Yokohama IT Operations Management

Zuletzt aktualisiert: 06.05.2025

Automatische Übersetzung

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

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

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

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

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

Automatische Übersetzung

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

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

Inhaltsverzeichnis

IT Operations Management 5
ITOM/OT SU-Lizenzierung und -Abonnements 9
ITOM/OT SU-Lizenzierung erkunden 10
ITOM/OT SU-Lizenzierung konfigurieren 20
ITOM/OT SU-Lizenzierung verwenden 21
ITOM/OT SU-Lizenzierung – Referenz 27
ITOM Store-Upgrades 32
ITOM Cloud Accelerate 32
Cloud-Services-Katalog 34
Bewertung der Cloud-Migration 105
Governance für Cloud-Konfigurationen 138
Bibliothek von Cloud-Aktionen 188
ITOM Cloud Accelerate-Referenz 220
ITOM-Transparenz 223
Referenz zu ITOM-Transparenz und CSDM 227
Durch ITOM-Transparenz erfasste Daten 233
Discovery 561
Zertifikatsbestand-Management 1154
Umgebung für die automatisierte Zertifikatverwaltung 1207
Service-Mapping 1219
Von ITOM-Transparenz verwendete Erkennungsmuster 1661
ITOM Content Service 2116
Tag-Governance 2124
Arbeitsbereich für Cloud-Vorgänge 2147
ITOM-Transparenz-Referenz 2161
ITOM-Integrität 2166
ITOM-Integrität – Anwendungsfall 2167
Ereignismanagement 2168
Health Log Analytics 2741
Service Reliability Management 3007
Servicelevel-Zielmanagement 3089
Service-Beobachtbarkeit 3107
Service Operations-Arbeitsbereich für ITOM 3128
Synthetische Überwachung 3326
CSDM-Richtlinien auf ITOM-Integrität anwenden 3343
Agent Client Collector 3353
Agent Client Collector Framework 3354
Agent Client Collector-Überwachung 3492
Agent Client Collector Visibility – Inhalt 3873

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

Agent Client Collector für Kubernetes – Transparenz....3902
Agent Client Collector Log Analytics....3923
Agent Client Collector Security Incident Response....3949
Live-CI-Daten mit Agent Client Collector anzeigen....3956
Metrikdaten....3958
Metrikdaten erkunden....3960
Metrikdaten konfigurieren....3983
Wird optimiert Metrikdaten....3990
Metrikdaten – Referenz....4019
ITOM-Optimierung....4020
Cloud Provisioning and Governance....4021
ITOM-Optimierung – Referenz....4541
Now Assist für IT Operations Management (ITOM)....4542
Now Assist für IT Operations Management (ITOM) erkunden....4544
Now Assist für IT Operations Management (ITOM) konfigurieren....4545
Now Assist für IT Operations Management (ITOM) verwenden....4546
Now Assist für IT Operations Management (ITOM) – Referenz....4553
Auf Cloud-Umgebungen für ITOM-Produkte zugreifen....4553
Installieren und konfigurieren Sie MID Servers für den Zugriff auf Cloud-Umgebungen....4553
Richten Sie ein Cloud-Servicekonto ein....4559

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

IT Operations Management

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

Mit IT Operations Management mehr sehen und mehr erreichen

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

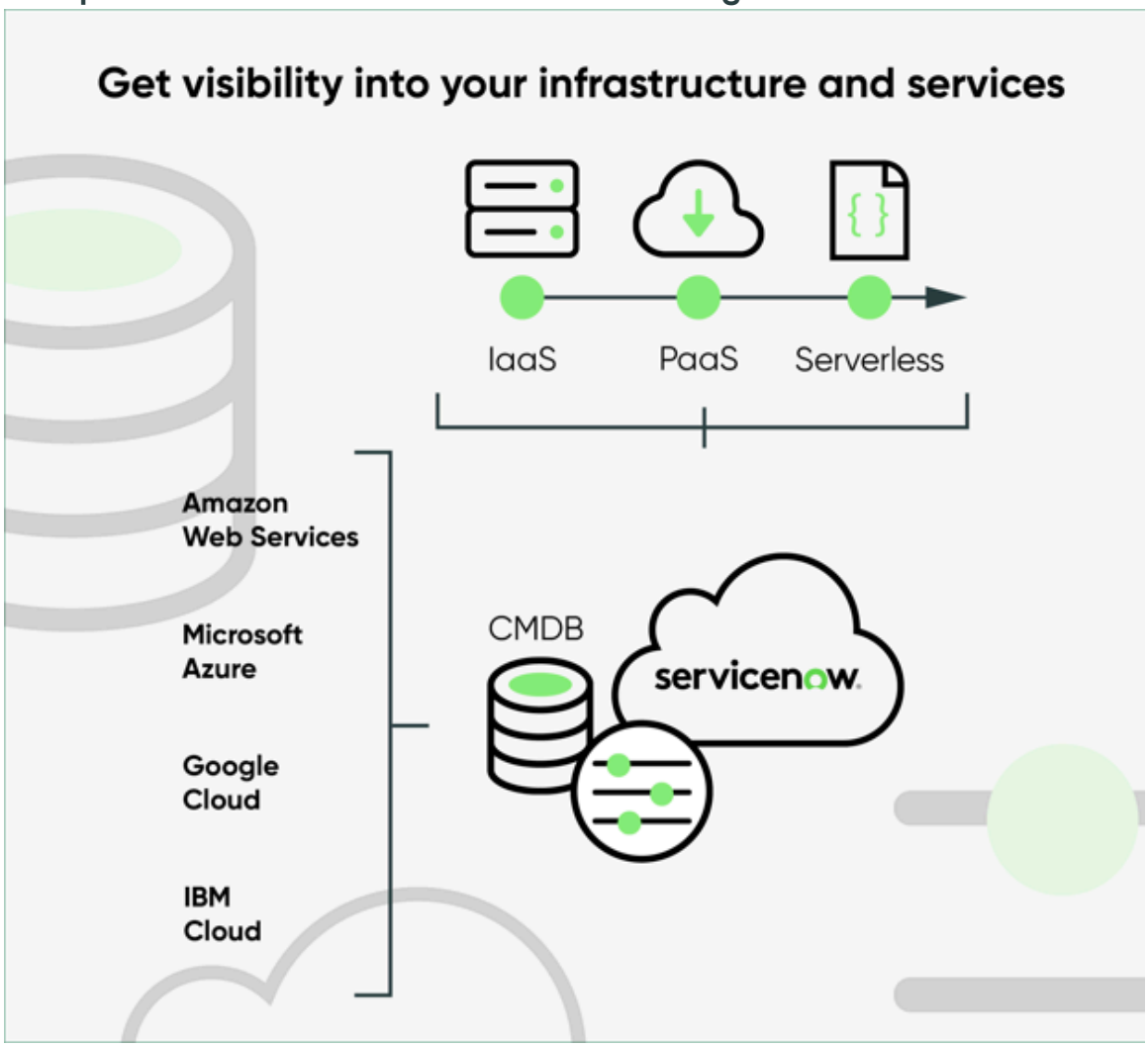
Hier können Sie die vollständige Infokarte anzeigen oder herunterladen , die eine Übersicht der wichtigsten Funktionen von IT Operations Management bietet.

	Transparenz Ihrer Infrastruktur und Services erlangen Übernehmen Sie mithilfe einer zentralen Lösung das Kommando über Ihre Infrastruktur und Services. Verbessern Sie die Servicequalität, stärken Sie Change-Prozesse, reduzieren Sie Risiken, optimieren Sie Ihre Infrastrukturausgaben, und minimieren Sie Compliance-Probleme mit der Software.
	Serviceprobleme wirksam vermeiden und lösen Entlasten Sie mit AIOps Ihre IT-Mitarbeiter von zeitaufwändigen, fehleranfälligen Aufgaben, und verringern Sie die Anzahl der Serviceausfälle. Beschleunigen Sie die Problemlösung mit relevanten und kontextbezogenen Change-, Problem- und Incident-Daten.

Automatische Übersetzung

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

Transparenz Ihrer Infrastruktur und Services erlangen

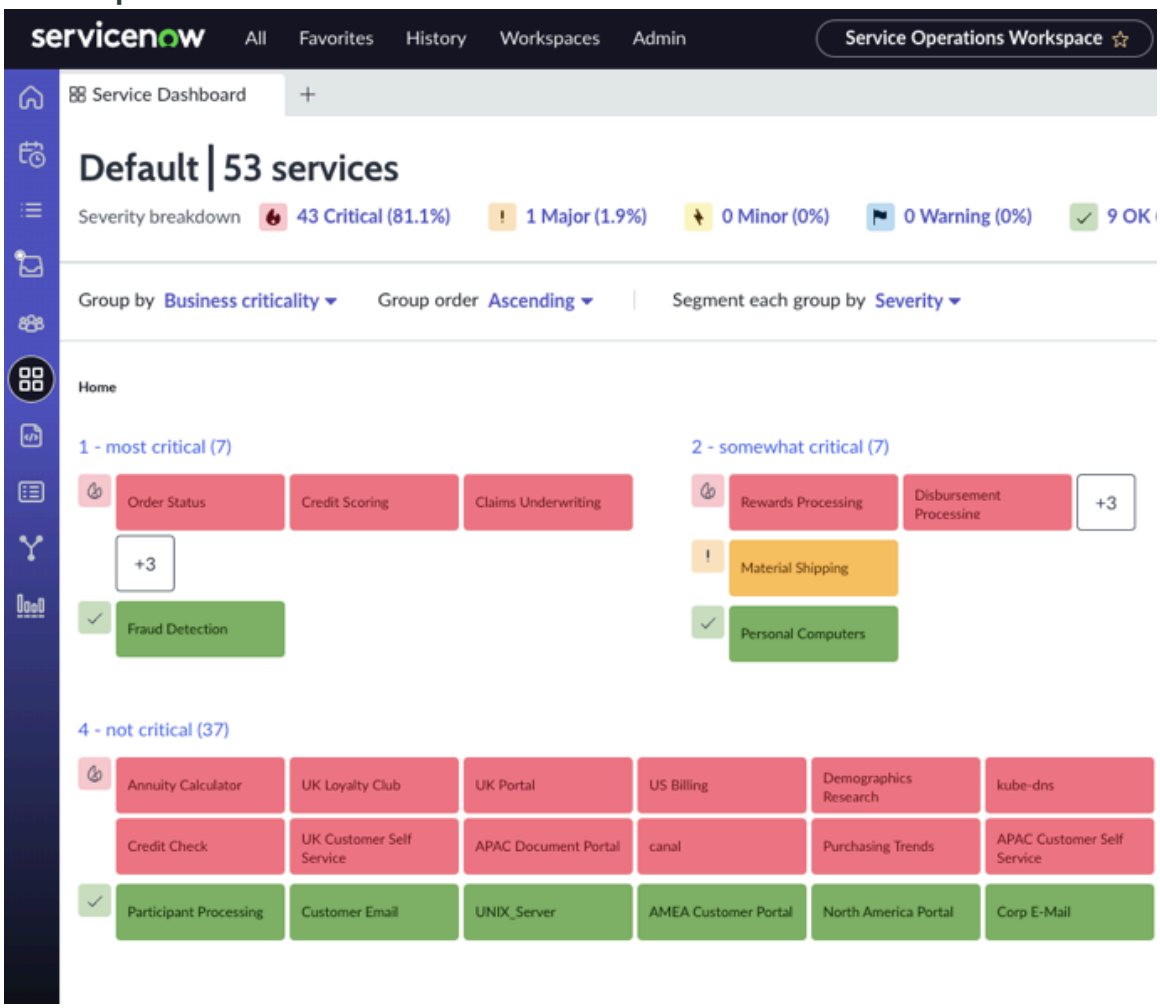


Sie können sofort die Auswirkungen von Infrastrukturproblemen und Changes auf den Service sehen, die Ursachenanalyse vereinfachen und die durchschnittliche Zeit bis zur Reparatur (MTTR) reduzieren. End-to-End-Erkennung und -Servicezuordnung bieten Ihnen eine genaue, aktuelle CMDB-Ansicht der IT-Infrastruktur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

Automatische Übersetzung

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

Serviceprobleme wirksam vermeiden und lösen



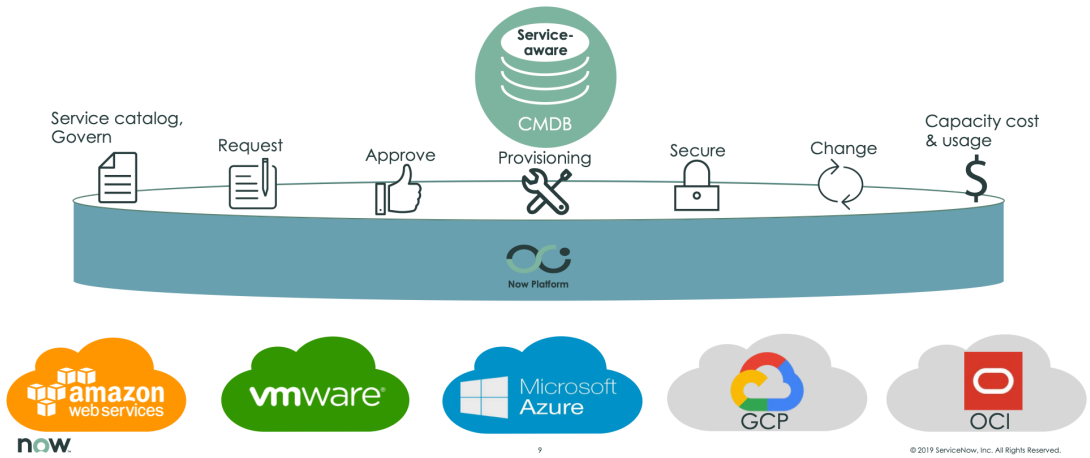
ITOM-Integrität nutzt die Möglichkeiten von AIOps, um Events in verwertbare Warnungen zu verwandeln. Erkennen Sie Serviceprobleme präzise, und identifizieren und beheben Sie die Ursachen im Handumdrehen. Im Gegensatz zu veralteten Event Management-Systemen, die statisch und regelbasiert sind, wendet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

Automatische Übersetzung

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

Cloud-Strategie beschleunigen und Kosten senken

Consistent cloud operating model on single platform



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

Unabhängig davon, ob es sich um eine Bewertung der Cloud-Migration oder eine Prüfung der Cloud-Ressourcenkonfiguration handelt, bietet ITOM Governance Workflows zur Aktivierung des Prozesses und ermöglicht Ihnen gleichzeitig die Korrektur von Cloud-Tags und ungültigen Konfigurationen. Die Kombination der Stärken agiler und innovativer Fähigkeiten in der Cloud mit ITOM und dem etablierten ServiceNow -Framework gewährleistet einen erfolgreichen Übergang.

IT Operations Management Produktlizenzierung

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

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

Erste Schritte

- Arbeiten Sie mit einem Implementierungsspezialisten zusammen, um Ihre gewünschten Geschäftsergebnisse zu erzielen. Weitere Informationen hierzu finden Sie im Customer Success Center .
- Wählen Sie im ServiceNow University Center die für Sie am besten geeignete Schulung.

Automatische Übersetzung

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

Mehr erfahren

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

Anwendungen und Funktionen

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

ITOM/OT SU-Lizenzierung und -Abonnements

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

Einheitliche Statistiken für alle ITOM-Produkte

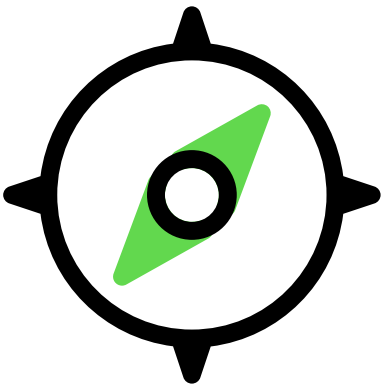
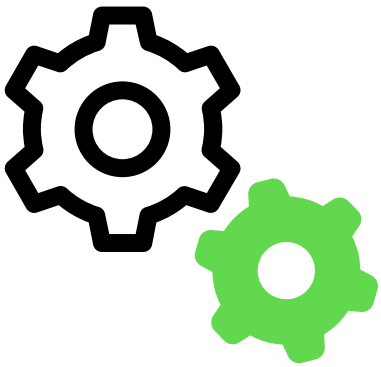
Verwenden Sie das Lizenzierungsmodul ITOM, um abonnementbezogene Informationen für alle ITOM -Produkte anzuzeigen: ServiceNow® ITOM-Transparenz, ServiceNow® ITOM Discovery, ServiceNow® ITOM-Integrität, ServiceNow® Health Log Analytics, ServiceNow® ITOM-OptimierungServiceNow® ITOM Cloud Accelerate] , , ServiceNow® Digitale Endanwender-Experience (DEX) und ServiceNow® Service Observability.

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

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

Verbrauchsniveau

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

Untersuchen	Installieren	Referenzen
		
Erkunden Sie ITOM/ OT SU-Lizenzierung und Abonnements	Erfahren Sie, wie installiert wird ITOM/ OT SU-Lizenzierung	Erfahren Sie mehr über das Planen von Aufgaben, Tabellen, das Abonnementformular und das Dashboard

Informationen zu Lizenzierungen und Abonnements für Operational Technology-Management (OTM) finden Sie unter Abonnementformular für die OTM-Produkte .

ITOM/OT SU-Lizenzierung erkunden

Erfahren Sie mehr über ServiceNow® ITOM/OT SU-Lizenzierung, die verschiedenen enthaltenen ITOM -Abonnements und die damit verbundenen Vorteile.

ITOM/OT SU-Lizenzierung – Übersicht

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

ITOM/OT SU-Lizenzierung – Vorteile

Vorteil	Funktion	Anwender
Zeigen Sie die Nutzung von ITOM -Anwendungen an, um fundierte Entscheidungen zu Ihren ITOM -Abonnements zu treffen und so die	Ressourcennutzung gegenüber den zugeteilten	Administrator

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

Vorteil	Funktion	Anwender
Ressourcenzuteilung Ihres Unternehmens effektiver zu optimieren.	Abonnementeinheiten überprüfen	
Dashboard-Berichte erleichtern Ihnen die Analyse der Ressourcennutzung und des Status im Vergleich zu Ihren gekauften Abonnements. Diese Berichte stellen sowohl die Anzahl der täglichen Nutzung als auch den durchschnittlichen Verbrauch von Abonnementeinheiten über einen Zeitraum von 90 Tagen visuell dar.	ITOM/OT SU-Lizenzierung-Dashboard	Administrator

Abonnements für IT Operations Management

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

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

- Container
- PaaS
- FaaS
- Server
- Nicht gelöstes Überwachungsobjekt
- Nicht kategorisiertes Objekt
- enduser_devices
- Netzwerkgeräte
- Netzwerkgeräte – erweitert
- IoT

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

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

ITOM-Transparenz

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

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

Automatische Übersetzung

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

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

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

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

ITOM Discovery

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

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

ITOM-Integrität

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

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

Health Log Analytics

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

ITOM Cloud Accelerate

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

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

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

ITOM-Optimierung

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

Zugehörige Informationen

Abonnement-Management

Sammlung und Zusammenfassung von Daten für den Lizenzierungsprozess

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

ServiceNow berechnet Gebühren für verschiedene ITOM -Anwendungen, einschließlich ITOM-Transparenz, ITOM Discovery, ITOM-Integrität, Health Log Analytics, ITOM Cloud Accelerateund ITOM-Optimierung. Genaue Informationen zu den Produkten und Funktionen, die von -Abonnements ITOM abgedeckt werden, finden Sie unter Abonnements für IT Operations Management.

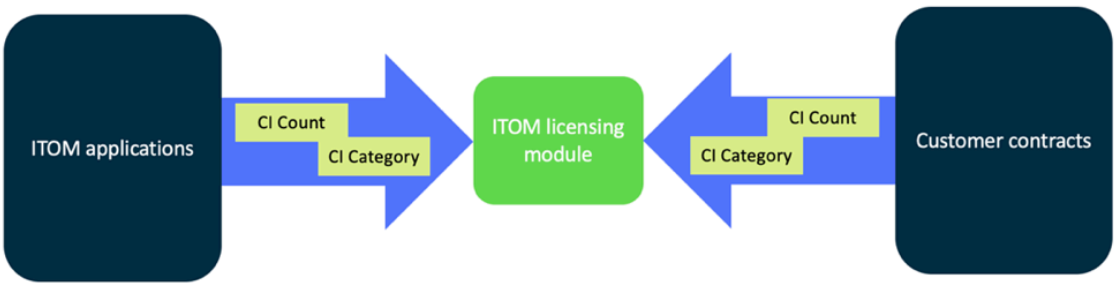
Das Sammeln und Aggregieren von Informationen für Lizenzierungszwecke umfasst die folgenden Schritte:

1. Der ITOM -Lizenzierungsmechanismus zählt täglich die Configuration Items (CIs), die von den einzelnen ITOM -Produkten verwaltet werden, und kategorisiert sie in lizenzierbare CI-Kategorien. Weitere Informationen finden Sie unter KB0748149: ITOM Subscription Unit license calculation logic (Lizenzberechnungslogik für ITOM-Abonnementeinheiten).
2. Wenn dieselben CIs von verschiedenen Funktionen innerhalb derselben ITOM -Produkte verwaltet werden, wird die CI-Anzahl angepasst, um Duplikate zu vermeiden. Wenn beispielsweise Discovery und Service-Mapping dieselben CIs erkennen, werden diese CIs nur einmal in der CI-Anzahl angezeigt.
3. Das Lizenzierungsmodul aggregiert CI-Anzahlen aus den Anwendungen ITOM, um die durchschnittliche tägliche CI-Anzahl für die letzten 90 Tage zu bestimmen.
4. Das Lizenzierungsmodul vergleicht dann die täglichen durchschnittlichen CI-Anzahlen für die letzten 90 Tage aus den Anwendungen ITOM mit den Lizenzierungsinformationen im Kundenvertrag, um Lizenzstatistiken zu generieren.

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

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

ITOM Flow für Anwendungslizenzen



ITOM/OT SU-Lizenzierung Abonnementtypen

Erwerben Sie Lizenzabonnements für ITOM -Produkte einzeln (à la carte), bündeln Sie mehrere -Produkte oder entscheiden Sie sich für einzelne und gebündelte Abonnements.

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

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

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

ITOM/OT SU-Lizenzierung Paketabonnement

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

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

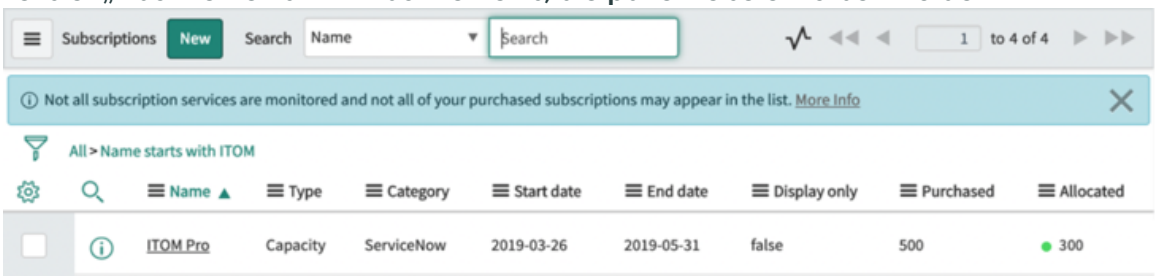
Wenn Sie Abonnements in einem Paket erwerben, erhalten Sie dieselbe Anzahl von Abonnementeinheiten für alle ITOM-Anwendungen, die vom Paket abgedeckt werden. Wenn Sie beispielsweise ein Paket von 500 Einheiten für ITOM-Transparenz und ITOM-Integrität kaufen, erhält Ihr Unternehmen 500 Einheiten für jede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

Hinweis: Sie können jeweils nur ein Bündel kaufen.

Automatische Übersetzung

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

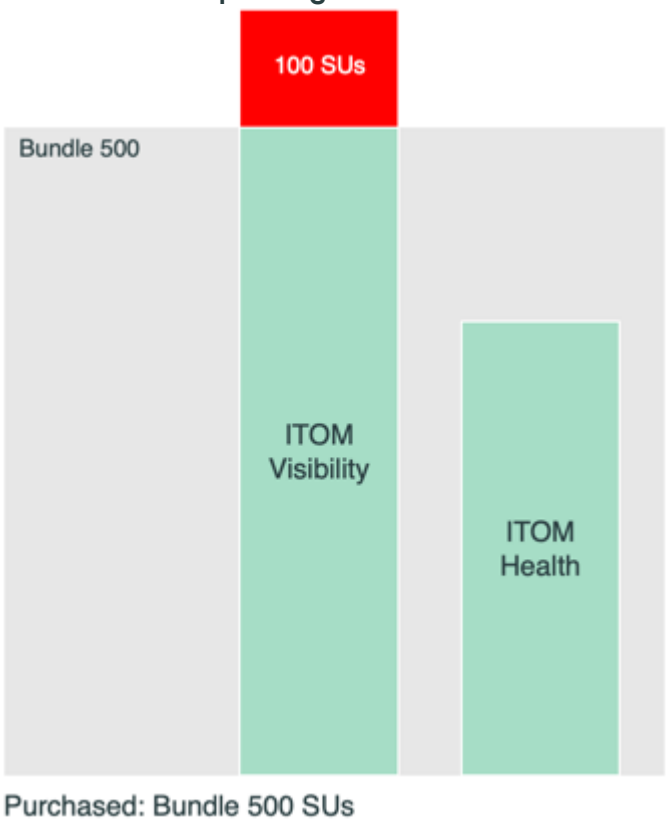
Fenster „Abonnements“ mit Abonnements, die paketweise erworben wurden



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

Die Verbrauchsstufe des Bündels wird durch die höchste Nutzung unter den im Bündel enthaltenen Produkten bestimmt.

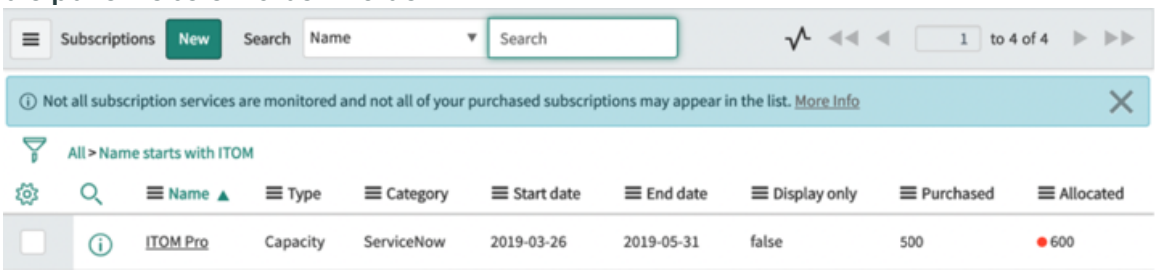
Automatische Anpassung des Pakets an den tatsächlichen Verbrauch



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

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

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



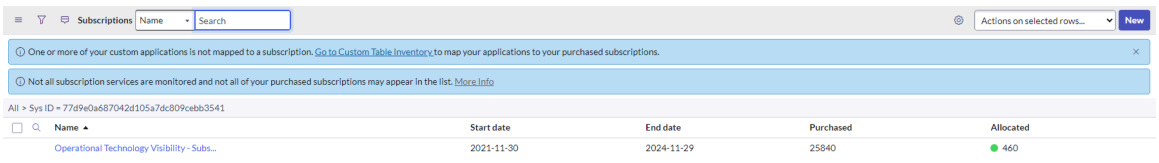
ITOM/OT SU-Lizenzierung Individuelles Abonnement (à la carte).

Sie können -Abonnements für einzelne ITOM -Anwendungen (à la carte) erwerben.

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

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

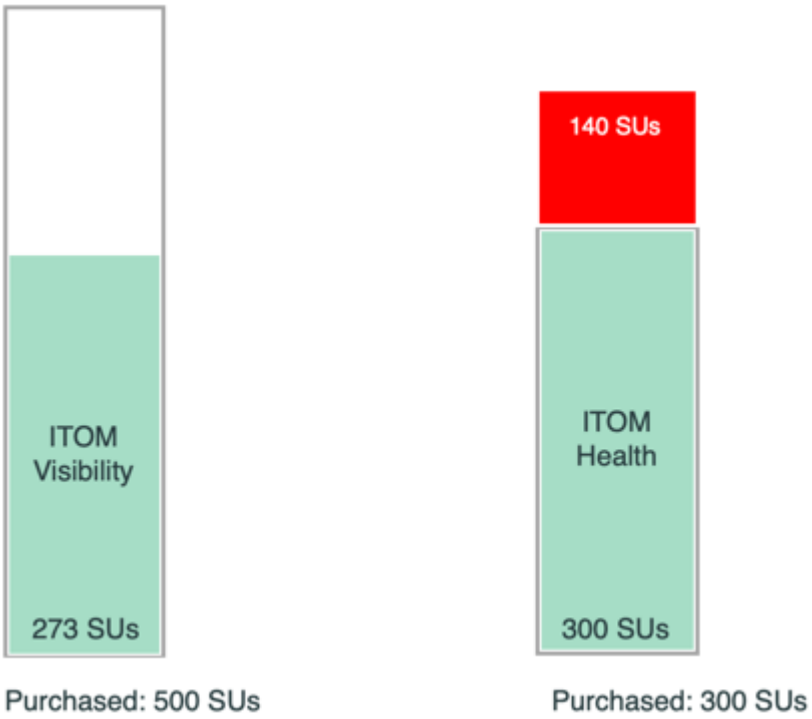
Fenster „Abonnements“, in dem à la carte erworbene Abonnements angezeigt werden



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

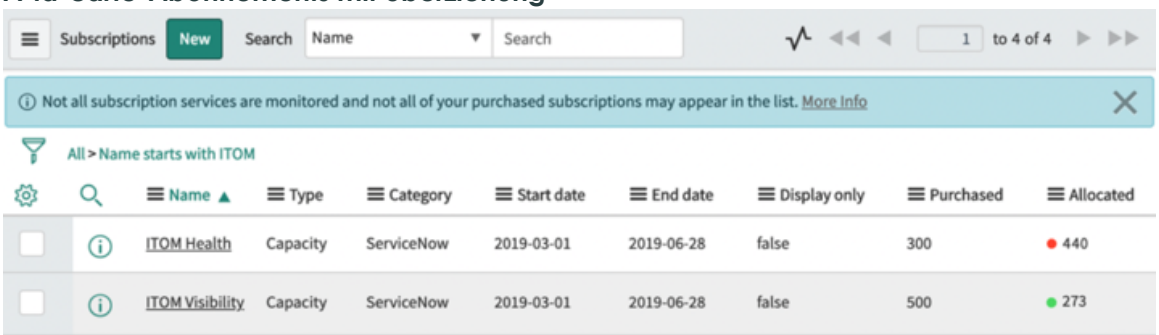
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Berechnung der à-la-carte-Abonnements



Wenn Ihre Organisation die Gesamtanzahl der erworbenen Abonnementeinheiten überschreitet, zeigt das Fenster Abonnements das entsprechende Abonnement à la carte als überzogen an. In der folgenden Abbildung hat ITOM-Integrität mehr Abonnements verbraucht, als dafür erworben wurden.

À-la-carte-Abonnements mit Überziehung



ITOM/OT SU-Lizenzierung Paket- und Einzelabonnement (à la carte).

Sie können Abonnements für einzelne ITOM -Anwendungen (à la carte) oder als Paket mit mehreren ITOM -Anwendungen erwerben.

Die Anwendung ITOM/OT SU-Lizenzierung berechnet die Abonnementnutzung für Produkte ITOM vom Typ und zeigt sie an. Zeigt die -Produkte ITOM einzeln oder als Teil eines Pakets an, je nach Abonnement. Wenn Ihre Organisation Abonnements ITOM sowohl als Paket als auch einzeln (à la carte) erworben hat, zieht das Lizenzierungsmodul die verbrauchten Abonnements zuerst vom Paket ab und dann von den einzeln erworbenen Abonnements.

Wenn Ihre Organisation die zugeteilte Anzahl von Abonnementeinheiten überschreitet, zeigt das Fenster Abonnements an, dass die entsprechenden Abonnements überzogen sind. Wenn die Gesamtzahl der Abonnements aus Paket- und Abonnementoptionen die Zuteilung überschreitet, identifiziert das Lizenzierungsmodul den Überschuss als aus dem Abonnement Abonnement übernommen. Wenn außerdem die Gesamtzahl der Abonnements für eine Anwendung, die ausschließlich von dem Paket abgedeckt wird, die

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

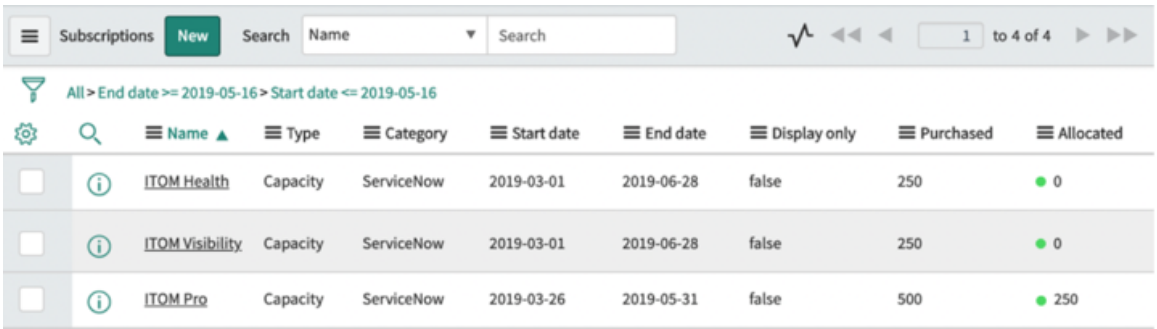
Zuteilung überschreitet, zeigt das Fenster „Abonnements“ das Paket als überzeichnet an, ohne die einzelne Anwendung separat aufzulisten.

Abonnementabzugsprozess: Bundle-Nutzung und À-la-carte-Szenario

Wenn Sie Abonnements ITOM als Paket und zusätzlich Abonnements à la carte für eine im Paket enthaltene Anwendung erworben haben, zieht das Lizenzierungsmodul die verbrauchten Abonnements vom Paket ab, bevor es von den separat erworbenen Abonnements subtrahiert.

Im folgenden Beispiel hat eine Organisation alle vom Paket ITOM Pro zugewiesenen Abonnements für ITOM-Integritätverwendet. Anschließend wird das Lizenzierungsmodul von den Abonnements à la carte für ITOM-Integritätabgezogen.

Abonnementverbrauch nach Paketen



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

Abonnementanzeige: Anwendung, die von Paket- und à la carte-Abonnements abgedeckt wird

Wenn Ihre Organisation die Gesamtzahl der Abonnements sowohl im Paket als auch in den Abonnements à la carte überschreitet, betrachtet das Lizenzierungsmodul dies als überzeichnet im Abonnement à la carte. Wenn Ihre Organisation jedoch die Abonnements speziell für eine Anwendung überschreitet, die ausschließlich vom Paket abgedeckt wird, gilt sie als im Paket überzeichnet.

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

Das Lizenzierungsmodul berechnet Bündel-Abonnements und Abonnements à la carte für dieselben ITOM -Anwendungen

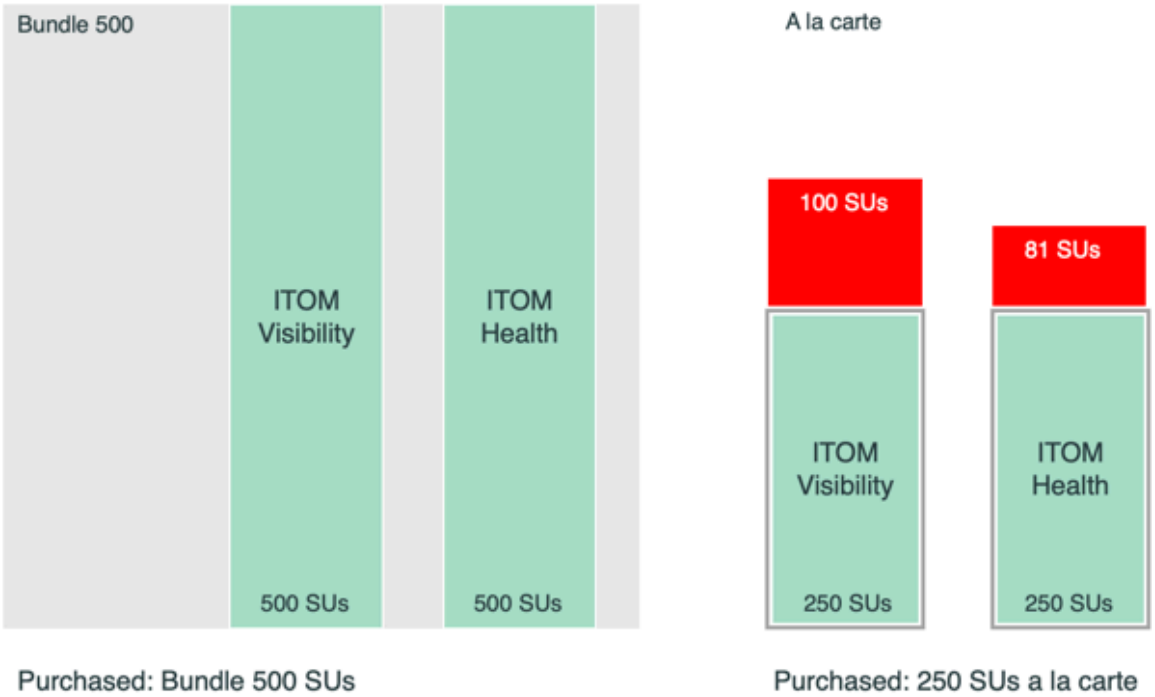
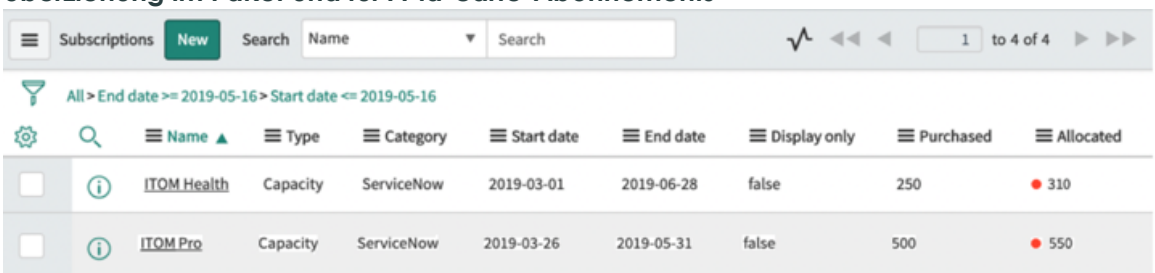


Abbildung der Abonnementberechnung: Bündel- und à la carte-Zuteilung

Das Diagramm veranschaulicht, wie das Lizenzierungsmodul Abonnements über Paket- und À-la-carte-Methoden für bestimmte Anwendungen berechnet, die vom Paket abgedeckt werden.

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



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

In der angegebenen Abbildung hat ITOM-Integrität 810 Abonnements verbraucht und damit die vom Paket (500) und à la carte (250) bereitgestellten Abonnements übertroffen. Daher zeigt das Fenster „Abonnements“ das Abonnement ITOM-Integrität à la carte als überzogen an.

Für ITOM-Transparenz, das 550 Abonnements verbraucht hat und für das keine Abonnements à la carte erworben wurden, wird das Paket ITOM Pro, das ITOM-Transparenz abdeckt, als überzogen angezeigt.

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

Abonnements für Operational Technology-Management

Die Plattform ServiceNow verwendet Operational Technology-Management (OTM), um Lizenzen für die verarbeitende Industrie zu verwalten. OTM enthält die Lizenzen, die in IT Operations Management enthalten sind, sowie spezifische Lizenzen für OTM.

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

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

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

ITOM/OT SU-Lizenzierung konfigurieren

Gewinnen Sie die Fähigkeit, ITOM -Abonnements innerhalb des ServiceNow -Frameworks effizient zu verwalten und zu optimieren, um den Betrieb zu optimieren.

Konfiguration – Übersicht

Beginnen Sie mit der Installation von ServiceNow® ITOM/OT SU-Lizenzierungund legen Sie damit den Grundstein für ein umfassendes Verständnis der Verwaltung von ITOM -Abonnements.

ServiceNow® ITOM/OT SU-Lizenzierung aktualisieren

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

Vorbereitungen

- Stellen Sie sicher, dass in Ihrer Instanz ITOM das Produkt ServiceNow] installiert ist, damit die Anwendung ITOM/OT SU-Lizenzierung funktioniert. Die Installation der Anwendung ITOM/OT SU-Lizenzierung ist nicht erforderlich, da das System die Anwendung automatisch zusammen mit jedem ITOM -Produkt installiert.
- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfen Sie die Anwendungsliste ITOM/OT-SU-Lizenzierung im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen sowie zur Releasekompatibilität.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie erhalten Benachrichtigungen, wenn Updates für die Anwendung ITOM/OT SU-Lizenzierung für ServiceNow Storeverfügbar sind.

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

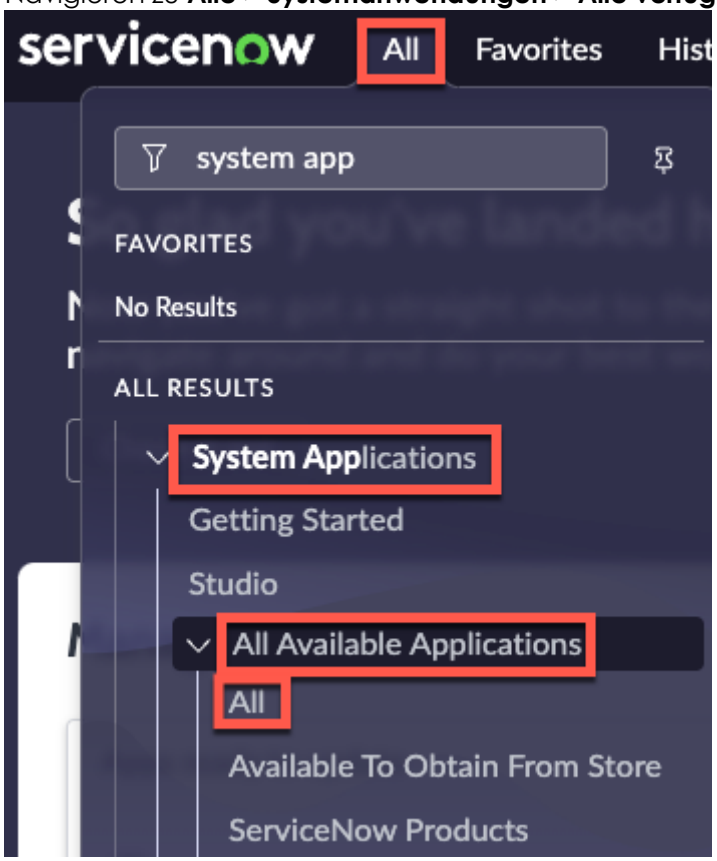
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

- Regelmäßige Aufgaben
- Tabellen

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

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung ServiceNow ITOM/OT SU-Lizenzierung (sn_itom_licensing).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen.

3. Wählen Sie auf der Registerkarte **Updates** die Anwendung ServiceNow ITOM/OT SU-Lizenzierung aus.
4. Wählen Sie **Mit der Aktualisierung fortfahren aus**.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die installiert werden, wenn die Anwendung aktualisiert wird.

5. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
6. Wählen Sie die Version aus, auf die Sie aktualisieren möchten, und wählen Sie **Installieren**.

ITOM/OT SU-Lizenzierung verwenden

Stellen Sie sicher, dass ITOM die -Abonnements Ihrer Organisation optimal genutzt werden, indem Sie die Ressourcennutzung Ihrer ITOM -Produkte analysieren.

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

Übersicht über ITOM/OT SU-Lizenzierung verwenden

Erfahren Sie, wie Sie Abonnements für ITOM -Anwendungen anzeigen und nachverfolgen und die Ressourcennutzung für zugeteilte Abonnementeinheiten analysieren, um eine optimale Nutzung sicherzustellen. Überprüfen Sie die Anzahl der Configuration Items (CIs), die für ITOM -Abonnements verwendet werden, und identifizieren Sie, welche CI-Typen speziell ITOM -Abonnementeinheiten erfordern. Generieren Sie abschließend Listen, die die aktuell zählbaren CIs für jede Anwendung ITOM anzeigen, sodass Sie deren Verbrauch an Abonnementeinheiten visualisieren können.

Abonnementstatistiken für ITOM anzeigen

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

Vorbereitungen

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

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

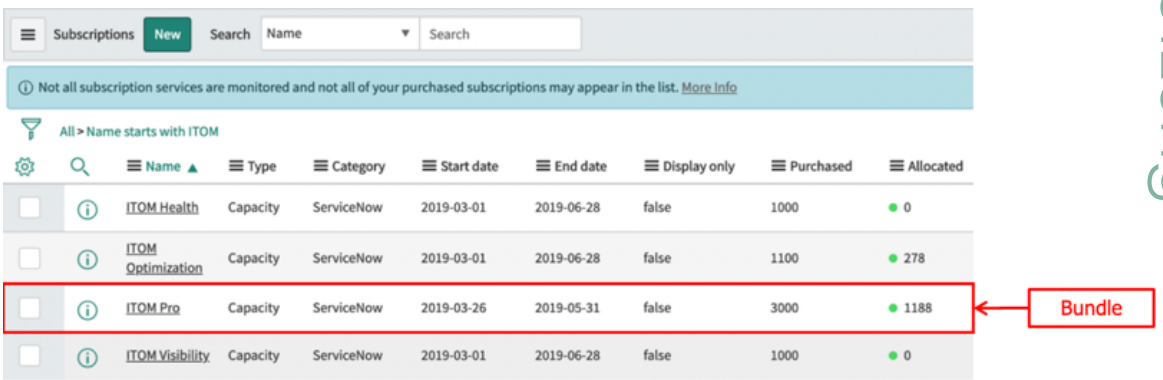
Erforderliche Rolle: sn_itom_license.reader

Warum und wann dieser Vorgang ausgeführt wird

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

Prozedur

1. Um Abonnementinformationen für IT Operations Management -Abonnements anzuzeigen, die einzeln und in Paketen erworben wurden, navigieren Sie zu **ITOM-Lizenz** > **Lizenzzusammenfassung**.
   Verwenden Sie Abonnementnamen, um zwischen Abonnements, die in Paketen und à la carte erworben wurden, zu unterscheiden.



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

Zugehörige Informationen

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

Abonnements für IT Operations Management

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

Ressourcennutzung gegenüber den zugeteilten Abonnementeinheiten überprüfen

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

Vorbereitungen

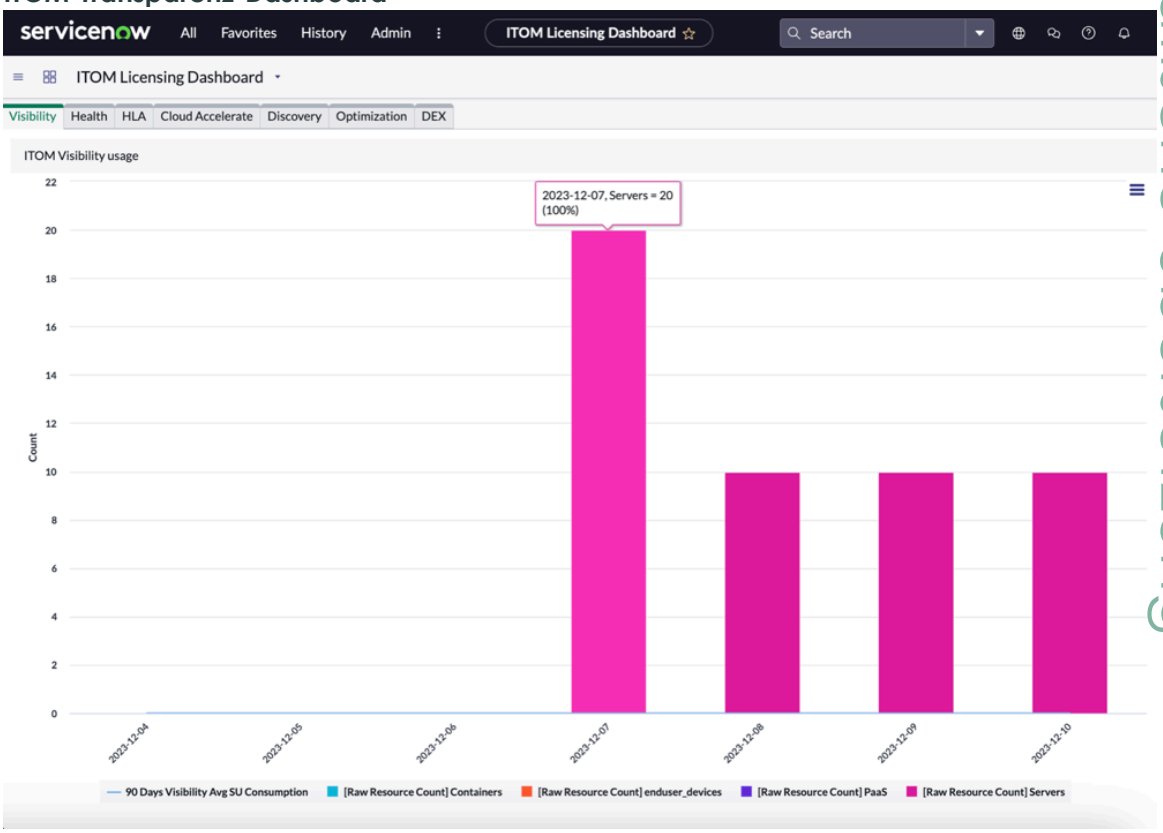
Erforderliche Rolle: Administrator

Zeigen Sie mit dem Lizenzierungs-Dashboard ITOMITOM detaillierte Lizenzierungsdaten im Zeitverlauf an. Zeigen Sie die täglichen CI-Anzahlen oder den Durchschnitt der letzten 90 Tage an. Domänenspezifische Informationen und spezifische CI-Auflistungen für jede tägliche Zählung ermöglichen Ihnen die Überwachung und Analyse der Ressourcennutzung.

Prozedur

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

ITOM-Transparenz-Dashboard



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

Für ITOM-Abonnements verwendete CI-Anzahl prüfen

Zeigen Sie tägliche CI-Anzahl oder den Durchschnitt der letzten 90 täglichen Anzahl an.

Automatische Übersetzung

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

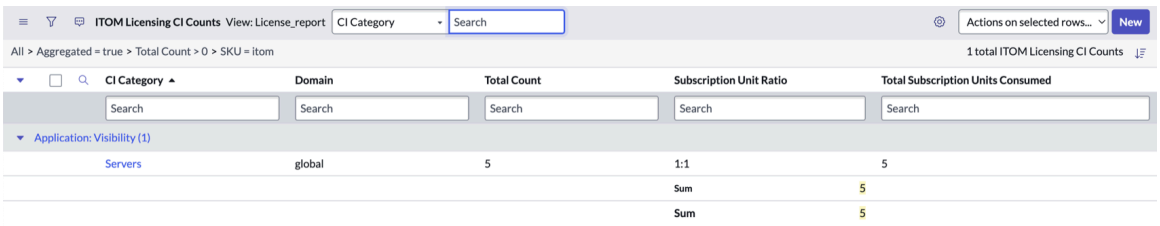
Vorbereitungen
Vergewissern Sie sich, dass Ihre Organisation ITOM-Abonnements erworben hat. Sie können die Informationen im **ITOM-Lizenz**-Modul nicht ohne Abonnements anzeigen.

Erforderliche Rolle: sn_itom_license.reader

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

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

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



   Weitere Informationen zu den Feldern im Lizenzbericht-Fenster finden Sie unter Formular „Lizenzbericht“.
2. Zeigen Sie in der Spalte **„Gesamtanzahl“** die durchschnittliche tägliche CI-Anzahl für die letzten 90 Tage an.
3. Zeigen Sie die tägliche CI-Anzahl auf eine der folgenden Arten an.
   - Legen Sie die Filterbedingung **Aggregiert** auf **[Aggregiert] [ist] [falsch]** fest, und wählen Sie **Ausführen**.
   - Navigieren zu **ITOM-Lizenz** > **Tägliche Lizenznutzungsanzahl**.

Überprüfen, welche CI-Typen ein ITOM-Abonnement erfordern

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

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

Erforderliche Rolle: sn_itom_license.reader

Warum und wann dieser Vorgang ausgeführt wird
Für Lizenzierungszwecke werden lizenzierbare Ressourcen CI-Kategorien zugewiesen. Die Lizenznutzung wird mithilfe von Abonnementeinheiten gemessen, die je nach CI-

Automatische Übersetzung

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

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

- Container
- PaaS
- FaaS
- Server
- Nicht gelöstes Überwachungsobjekt
- Nicht kategorisiertes Objekt
- enduser_devices
- Netzwerkgeräte
- Netzwerkgeräte – erweitert
- IoT

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

Prozedur

1. Überprüfen Sie, welche CI-Kategorie lizenzierbar ist:

   a. Navigieren zu **Alle** > **ITOM-Lizenz** > **Lizenzzusammenfassung**.

   b. Wählen Sie das entsprechende ITOM -Abonnement aus.
   Beispiel: **ITOM-Transparenz**.

   c. Scrollen Sie nach unten, und wählen Sie die Registerkarte **ITOM-CI – Abonnement-Einheiten-Verhältnis** aus.
   Auf der Registerkarte werden lizenzierbare CI-Kategorien aufgelistet, die aus dem Kundenvertrag generiert wurden. Dies sind die lizenzierbaren CI-Kategorien.

   d. Notieren Sie sich die lizenzierbaren CI-Kategorien, die für dieses Abonnement ITOM bereitgestellt werden.

   e. Wahlweise: Kehren Sie zur Liste **Lizenzzusammenfassung** zurück, und prüfen Sie die für andere ITOM-Abonnements generierten CI-Kategorien.

2. Navigieren zu **Alle** > **ITOM-Lizenz** > **Lizenzen nach CI-Typ**.

> **Wichtig:** Die Tabelle „ITOM-Lizenzierung – MetaData“ [itom_lu_metadata] enthält alle CI-Kategorien, einschließlich Kategorien von CIs, die keine ITOM-Abonnementeinheiten erfordern.

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

3. Prüfen Sie die Liste, um lizenzierbare CI-Kategorien zu identifizieren, die auf der Registerkarte **ITOM-CI – Abonnement-Einheiten-Verhältnis** der Liste **Lizenzzusammenfassung** angezeigt werden.
4. Wählen Sie den Pfeil neben der lizenzierbaren CI-Kategorie, um sie zu erweitern und auf die zugehörigen CI-Typen zuzugreifen.

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

ITOM-Abonnementeinheiten verbrauchende CIs anzeigen

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

Vorbereitungen

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

Erforderliche Rolle: sn_itom_license.reader

Warum und wann dieser Vorgang ausgeführt wird

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

Prozedur

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

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

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

ITOM/OT SU-Lizenzierung – Referenz

Referenzthemen enthalten zusätzliche Informationen zu geplanten Aufgaben, Tabellen, Abonnementformularen und dem Dashboard, die Sie zum Konfigurieren und Verwalten von ITOM/OT SU-Lizenzierungverwenden.

Mit ITOM/OT SU-Lizenzierung installierte Komponenten

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

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
ITOM Update Store für Ausschlusstabellen	Aktualisiert die Ausschlussliste.
ITOM Aggregator Store für Lizenzierung	Berechnet die täglichen durchschnittlichen CI-Anzahlen der letzten 90 Tage.
ITOM Licensing Cloud Accelerate CI Listing Store	Erstellt die Liste der lizenzierbaren CIs für ITOM Cloud Accelerate.
ITOM Cloud Accelerate Lizenzierungsnutzungsanzahlspeicher	Berechnet die täglichen CI-Anzahlen für ITOM Cloud Accelerate.
Event Management – Speichern der Knotenanzahl	Berechnet die in Ereignismanagement verwendete Knotenanzahl.
ITOMHealthCIReporterWithOTOMCountITOMStore	Kompiliert die Liste von lizenzierbaren CIs für ITOM.
ITOMHealthCIReporterWithOTOMCountOTOMStore	Kompiliert die Liste von lizenzierbaren CIs für Operational Technology Management (OTM).
ITOM Nutzungsanzahlspeicher für Integritätslizenzierung	Berechnet die tägliche CI-Anzahl für ITOM-Integrität.
ITOM Nutzungsanzahlspeicher für Optimierungslizenzierung	Berechnet die tägliche CI-Anzahl für ITOM-Optimierung.
ITOM Lizenzierungsoptimierung – CI-Listenspeicher	Kompiliert die Liste von lizenzierbaren CIs für ITOM-Optimierung.
OTOM-Lizenzierung – Speichern der CI-Auflistung für ITOM Visibility	Kompiliert die Liste von lizenzierbaren CIs für ITOM-Transparenz (OTM).
ITOM Discovery-CI-Listenspeicher für Lizenzierung	Kompiliert die Liste von lizenzierbaren CIs für Discovery.
ITOM Lizenzierung – Transparenz-CI-Listen-Store	Kompiliert die Liste von lizenzierbaren CIs für ITOM-Transparenz.
ITOM Transparenzlizenzierungs-Nutzungsanzahlspeicher	Berechnet die tägliche CI-Anzahl für ITOM-Transparenz.
OTOM-Lizenzierung – Speichern der CI-Auflistung für Discovery	Kompiliert die Liste von lizenzierbaren CIs für Discovery (OTM).
ITOM DEX Lizenzierungsnutzungsanzahlspeicher	Berechnet die täglichen CI-Anzahlen für ITOM DEX.

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

Regelmäßige Aufgabe	Beschreibung
ITOM Lizenzierung DEX CI Listing Store	Erstellt die Liste der lizenzierbaren CIs für ITOM DEX.

Installierte Tabellen

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

Tabelle	Beschreibung
ITOM LU-Discovery-Quellenzuordnung [itom_lu_discovery_source_mapping]	Enthält die Liste der lizenzierbaren Discovery-Quellen für jede Kategorie.
ITOM LU – Zuordnung der Governance-App [itom_lu_governance_app_mapping]	Liste der Datensätze, die die Zuordnung von Governance-Anwendungen zu den jeweiligen lizenzierbaren CIs enthalten.
ITOM LU-Governance-CIs [itom_lu_governance_ci]	Enthält die Liste der CIs, die unter der Governance-Lizenz gezählt werden.
ITOM Lizenzausschlussmetadaten itom_license_exclusion_metadata	Enthält die Liste der Ausschlussregeln, die für verschiedene Lizenzen gelten.
Lizenzausschlüsse [license_exclusion_list]	Enthält die Liste der CIs, die gemäß der Ausschlussregel von der Lizenzzählung ausgeschlossen werden müssen.
Sichtbarkeit LU Temporär [visibility_lu_temp]	Enthält die Liste der CIs, die unter der Discovery-Lizenz gezählt werden.
ITOM Metadaten der Lizenzierungskategorie [itom_lu_category_metadata]	Enthält Lizenzierungsmetadaten.
ITOM Lizenzierung von Discovery-Quellen [itom_lu_discovery_sources]	Enthält die Kategorien für alle Discovery-Quellen.
ITOM LU DEX CIs [sn_itom_licensing_itom_lu_dex_ci]	Enthält die Liste der CIs, die unter der Lizenz DEX gezählt werden.

Abonnementformular für die ITOM-Produkte

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

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

ITOM Formularfelder für Produktabonnement

Feld	Beschreibung
Name	Name des Abonnementpakets oder der Anwendung ITOM, wenn Ihre Organisation Abonnements separat pro Anwendung (à la carte) erworben hat.
Startdatum	Datum, an dem das Abonnement aktiviert wurde.
Enddatum	Datum, bis zu dem das Abonnement gültig ist.
Gekauft	Anzahl der gekauften Abonnements pro Paket oder Anwendung (à la carte).
Zugewiesen	Anzahl der verbrauchten Abonnementeinheiten aus einem Paket oder einer Anwendung (à la carte). Für Pakete wird in diesem Feld die höchste Anzahl der verbrauchten Abonnementeinheiten nach Anwendungen angezeigt, die Teil des Pakets sind. Beispiel: Wenn ITOM-Transparenz 300 Abonnementeinheiten und ITOM-Integrität 200 Abonnementeinheiten verbraucht hat, wird in diesem Feld der Wert 300 für das Paket angezeigt, das diese Anwendungen abdeckt. Der Farbcode gibt den Prozentsatz der Abonnementeinheiten an, die Ihr Unternehmen verbraucht hat. Standardmäßig lautet der Schwellenwert für den Farbcode 90 %. • Grün: Ihre Organisation hat weniger als 10 % der gekauften Abonnements verwendet. • Gelb: Ihre Organisation hat mehr als 90 %, aber weniger als 100 % der erworbenen Abonnements verwendet. • Rot: Ihre Organisation hat 100 % oder mehr verwendet und die Anzahl der erworbenen Abonnements überschritten. Die erworbenen Abonnements sind überzogen.

ITOM/OT SU-Lizenzierung-Dashboard

Verwenden Sie das ITOM Licensing Dashboard (ITOM-Lizenzierungsdashboard), um die Statistiken zum Ressourcenverbrauch und zum Status Ihrer erworbenen Abonnements zu überprüfen. Dieses Dashboard enthält Berichte für jede ITOM-Anwendung. Die Berichte bieten eine Visualisierung der täglichen Nutzungsanzahl und des durchschnittlichen Verbrauchs von Abonnementeinheiten für 90 Tage. Das Dashboard ITOM Lizenzierung ist Teil der ITOM Lizenzierungsanwendung Version 4.0, die unter ServiceNow Storeverfügbar ist.

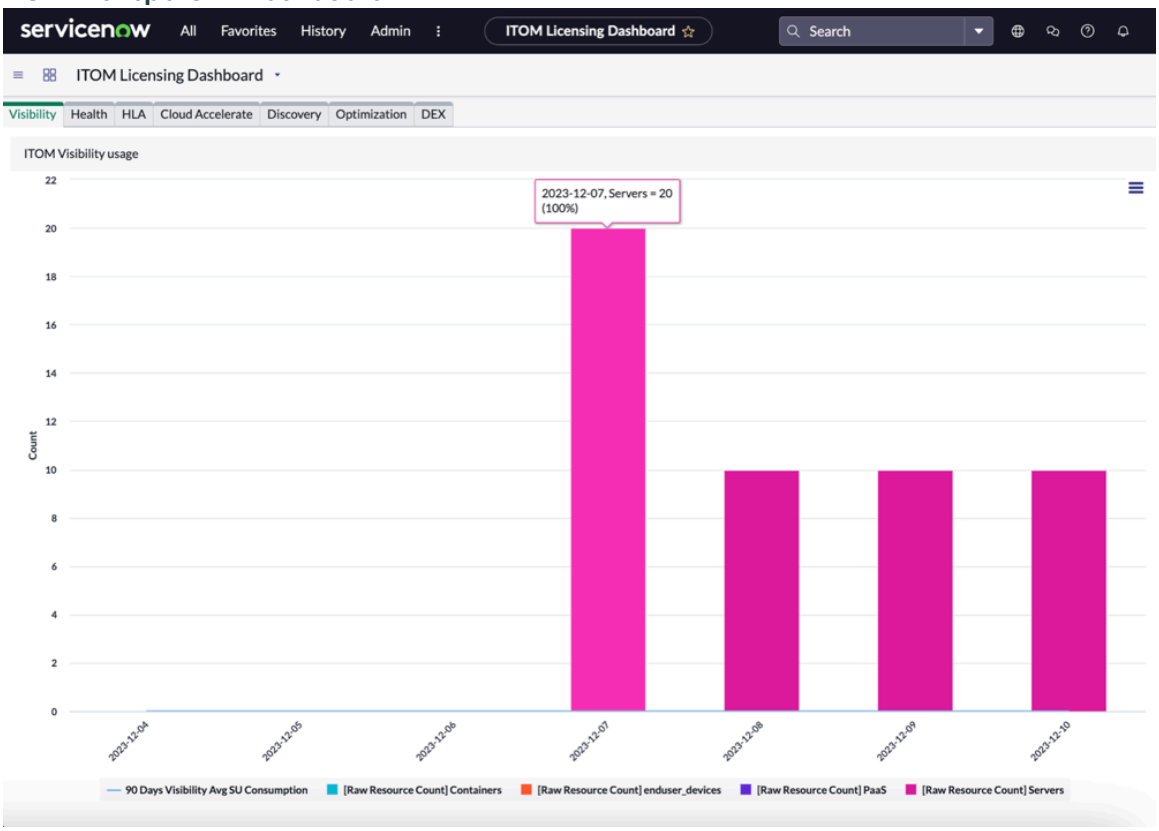
Erforderliche Rolle: Administrator

Bewertungs-Dashboard aufrufen

Vergewissern Sie sich, dass Sie über eine Administratorrolle verfügen, um auf das Lizenzierungsdashboard ITOM zugreifen zu können, das sich unter befindet **Alle** > **ITOM-Lizenz** > **ITOM-Lizenzierungsdashboard**.

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

ITOM-Transparenz-Dashboard



Anwendungsfälle

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

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

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

Datenvisualisierung

Das Dashboard enthält die folgende Visualisierung:

Monatlich	Typ	Quelltabelle	Beschreibung
• ITOM-Transparenz • ITOM-Integrität • Health Log Analytics	Vertikaler Balken	ITOM-Lizenzierungs-CI-Anzahlen [itom_lu_ci_counts] und UsageAnalytics-Anzahlen für Tabellen [usageanalytics_count]	Zeigt Balken an, die die Anzahl der CIs verschiedener lizenzierbarer Kategorien für die letzten 120 Tage pro ITOM-Anwendung

Automatische Übersetzung

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

Monatlich	Typ	Quelltabelle	Beschreibung
• ITOM Cloud Accelerate • ITOM Discovery • ITOM-Optimierung • ITOM Digitale Endanwender-Experience (DEX)			darstellen. Auf dem Dashboard wird auch die Zeile angezeigt, die den durchschnittlichen Verbrauch von Abonnementeinheiten in den letzten 90 Tagen darstellt.

Formular „Lizenzbericht“

Beschreibung der Felder im Formular „Lizenzbericht“.

Formularfelder „Lizenzbericht“

Feld	Beschreibung
CI-Kategorie	Gruppierung von Configuration Items (CIs) in jeder Anwendung auf Grundlage gemeinsamer Merkmale oder Attribute
Domäne	Domäne, zu der das CI gehört.
Gesamtanzahl	Durchschnitt von 90 täglichen Anzahlen von CIs, kategorisiert nach CI-Typen, in jeder Anwendung ITOM **Hinweis:** Die Gesamtzahl entspricht der obigen Definition nur dann, wenn die Bedingung **Aggregiert** im Filter auf **true**festgelegt ist. Wenn die Bedingung **Aggregiert** auf **false**festgelegt ist, stellt die Gesamtanzahl die tägliche Anzahl für eine bestimmte Anwendung und Kategorie an diesem Tag dar.
Abonnement-Einheiten-Verhältnis	Anzahl der CIs in einer bestimmten Kategorie, die ein Abonnement benötigen.
Insgesamt verbrauchte Abonnementeinheiten	Gesamtzahl der Abonnementeinheiten, die von ITOM Anwendungen innerhalb eines bestimmten Zeitraums verbraucht wurden. Diese Zahl wird vom Lizenzierungsmodul berechnet, indem das Abonnementeinheitenverhältnis mit der Anzahl der CIs in jeder CI-Kategorie verwendet wird.
Summe	Gesamtverbrauch an Abonnementeinheiten durch die Anwendung und alle ITOM Anwendungen. Wird unter Insgesamt verbrauchte Abonnementeinheiten hervorgehoben.

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

ITOM Store-Upgrades

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

Was sind Store-Upgrades?

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

Apps im Store anfordern

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

Liste der Store-Upgrades

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

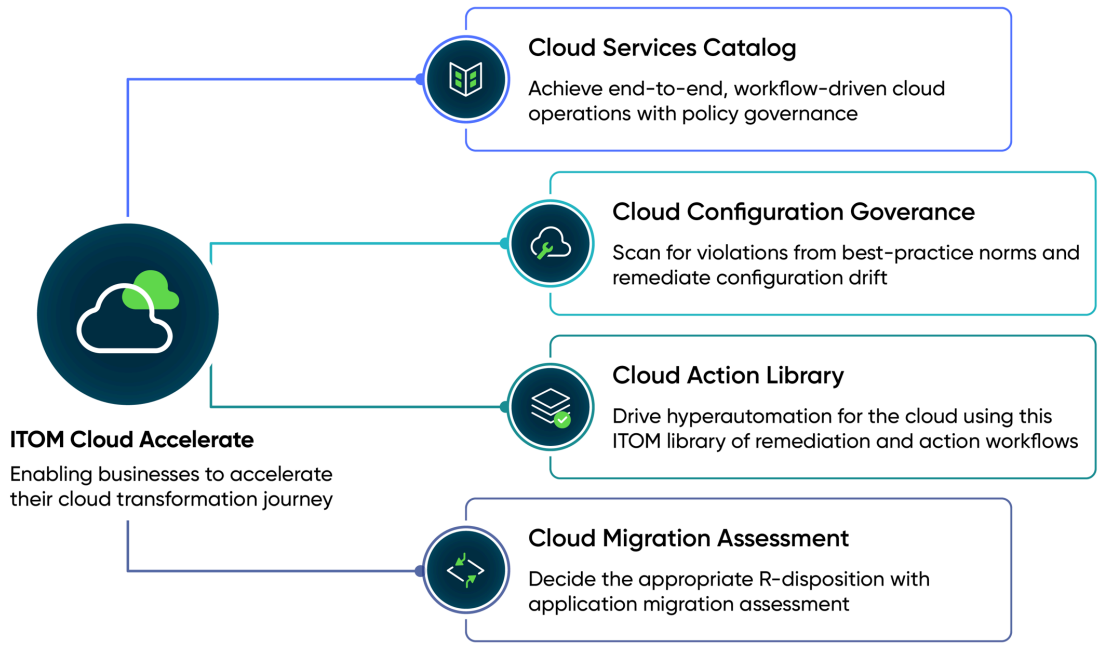
ITOM Cloud Accelerate

ITOM Cloud Accelerate -Workflows optimieren die Cloud-Automatisierung auf dem gesamten Weg zur Cloud-Einführung über Selfservice-Kataloge und kontrollierte Workflows. Es beschleunigt die Anwendungsmigration, indem es die Bewertung, Planung und Nachverfolgung der Ressourcenmigration erleichtert.

Funktionen von ITOM Cloud Accelerate

ITOM Cloud Accelerate Mit können Unternehmen ihre Cloud-Assets anhand vordefinierter Standards validieren und etwaige Abweichungen korrigieren.

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



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

Cloud-Services-Katalog

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

Bewertung der Cloud-Migration

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

Governance für Cloud-Konfigurationen

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

Bibliothek von Cloud-Aktionen

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

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

ITOM Cloud Accelerate Lizenzierung

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

ITOM Cloud Accelerate bereitstellen

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

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

Guided Setup zum Implementieren von IT Operations Management-Anwendungen

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

Cloud-Services-Katalog

Mit der Anwendung ServiceNow® Cloud-Services-Katalog können Sie eine vereinfachte Schnittstelle für den Zugriff auf Cloud-Ressourcen verwenden. Sie können Cloudangebote in einem Katalog veröffentlichen und die Nutzung und den Lebenszyklus dieser Ressourcen verwalten.

Durch die Integration mit Cloud-Anbietern, einschließlich Amazon Web Services, Microsoft Azure Google Cloud Platformund Cloud-Services-Katalog (CSK), können Sie die Azure DevOps- und CI-CD-Pipeline-Integrationverwenden. Sie können Ansible mit Cloud-Services-Katalog als Tag-1-Aktivität integrieren, um eine Ansible-Auftragsvorlage über ein ServiceNow-Katalogelement bereitzustellen. Nutzen Sie die Multi-Repository-Unterstützung mit Terraform Connector IaC Discover-Fähigkeiten, um die hierarchische Struktur mehrerer Repositorys zu verbessern.

Die sofort einsatzbereiten Kataloge für AWS, Azure und Google Cloud Platform sind in dieser Version von Cloud-Services-Katalogverfügbar. Sie können entweder eines der Katalogelemente bestellen, wie in diesem Video gezeigt, oder eines erstellen.

Bestellen Sie ein Katalogelement.

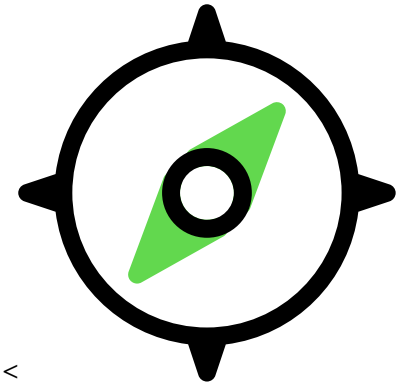
Erste Schritte

Erkunden	Konfigurieren	Verwenden Sie den Cloud-Servicekatalog

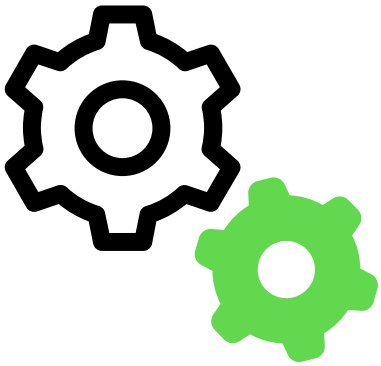
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Automatische Übersetzung

<



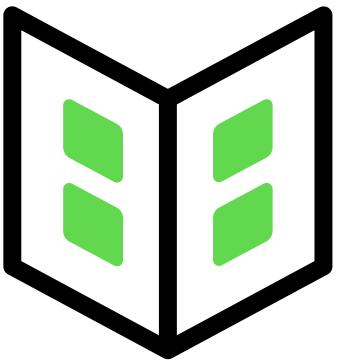
Erkunden Sie, und erfahren Sie, wie die Anwendung Cloud-Services-Katalog einen zentralen Ort zur Automatisierung von Cloud-Management-Tools bietet.



Konfigurieren Sie Cloud-Services-Katalog, und integrieren Sie ihn in andere Anwendungen.

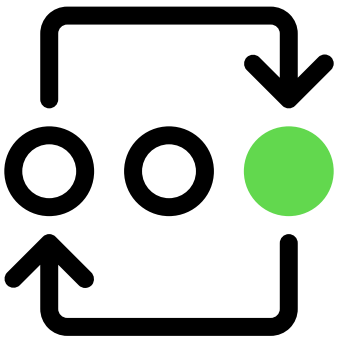
Verwenden Sie die Anwendung Cloud-Services-Katalog zum Suchen und Anfordern von Cloud-Services, zum Arbeiten mit Ihren Stapeln und Ressourcen usw.

Meine Stapel erkunden



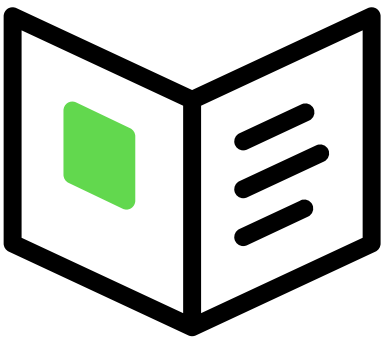
Meine Ressourcen erkunden

Bestellen Sie einen Katalog



Verwenden Sie die Anwendung Cloud-Services-Katalog, um aus einer Vielzahl von vordefinierten Katalogelementen, Aktionen und Richtlinien zu bestellen.

Referenz



Erhalten Sie weitere Informationen zu Berechtigungen und Problemumgehungen.

Automatische Übersetzung

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

Cloud-Services-Katalog erkunden

Die Anwendung Cloud-Services-Katalog ist der zentrale Ort, an dem Sie Cloud-Management-Tools automatisieren können. Es ersetzt und verbessert die Fähigkeiten, die von den Benutzer- und Administratorportalen Cloud Provisioning and Governance angeboten wurden.

Cloud-Services-Katalog – Übersicht

Auf der Seite Cloud-Services-Katalog Anforderung in Mitarbeiter-Center können Sie Cloud-Management-Aktionen anfordern. Sie können beispielsweise Bereitstellung (Tag 1), Patch- und Wartungsaktionen (Tag 2) oder Lebenszyklusvorgänge wie Starten, Stoppen oder Aufheben der Bereitstellung anfordern.

Cloud-Services-Katalog – Vorteile

In der folgenden Tabelle sind die Vorteile von Cloud-Services-Katalogaufgeführt.

Vorteile der Verwendung von Cloud-Services-Katalog

Leistung	Funktion
Unterstützung für Benutzer	Geführtes Setup
Vordefinierter Inhalt für die Anforderung Amazon AWS Cloud und die Automatisierung	AWS – Out-of-Box-Kataloge
Standardinhalte für die Anforderung und Automatisierung von Cloud-Services in Microsoft AzureMicrosoft Azure	Vordefinierte Azure-Kataloge
Standardinhalt für die Anforderung Google Cloud Platform .	Standardkataloge mit Cloud-Services-Katalog
Fordert den Prozess und die Seiten für die Bestellung von Cloud-Services an	Anforderungsprozess für Cloud-Services
Verwaltungsseite „Meine Stapel“ zum Anzeigen und Bearbeiten von Stapeln	Stapelverwaltung
Verwaltungsseite „Meine Ressourcen“ zum Anzeigen und Bearbeiten von Ressourcen	Ressourcenmanagement
Azure DevOps Pipeline-Integration für kontinuierliche Integration für kontinuierliche Bereitstellung (CICD).	Azure DevOps- und CI-CD-Pipeline-Integration
Integration von Ansible mit Cloud-Services	Integrieren Sie Ansible
Microsoft Azure - und Amazon AWS Cloud -Setup	Cloud-Setup
Multi-Repository-Unterstützung mit der App Terraform Connector .	Cloud Provisioning and Governance: Terraform Connector erkunden

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

Nächste Schritte

Unter Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate finden Sie die Liste der Plugins, die Sie mit Cloud-Services-Katalogaktivieren.

Cloud-Services-Katalog konfigurieren

Sie können die Anwendung Cloud-Services-Katalog so konfigurieren, dass Sie mit der Automatisierung von Cloud-Management-Tools beginnen können.

Konfiguration – Übersicht

Die Konfiguration erfolgt in einer sequenziellen Reihenfolge, wobei Sie zuerst die Voraussetzungen erstellen und einrichten und dann die Anmeldeinformationen mit Ihrem Cloud-Kontoprofil integrieren. Diese Setupschritte werden als Tag-1- und Tag-2-Aufgaben identifiziert.

Die Cloud-Services-Katalog Tag-1-Konfiguration umfasst Aufgaben wie das Erstellen von MID Servers, das Einrichten Ihrer Cloud-Anbieter, Amazon Web Servicesoder Microsoft Azure Cloud. Sie können es auch Ihrem Cloud-Konto zuordnen und die Discoverydes Rechenzentrums planen.

Eine Übersicht über den Setup-Prozess an „Tag 1“ finden Sie hier:

1. Fordern Sie bei Bedarf die Anwendung Cloud-Services-Katalog an.
2. Weisen Sie Ihren Cloud-Anwendern die entsprechenden Rollen zu.
3. Richten Sie die MID Servers ein, die die sichere Kommunikation mit den Provider-API-Endpunkten verarbeiten.
4. Erfassen Sie im Provider-Portal Ihre Kontoeinstellungen und die Anmeldeinformationen, die beim Discovery- Prozess (über ein MID-Server) für den Zugriff auf Ihre Provider-Konten verwendet werden.
5. Ordnen Sie die Kontoeinstellungen und Anmeldeinformationen sicher einem Servicekonto in Cloud-Services-Katalogzu.
6. Richten Sie einen Cloud-Account ein, der Ihre gesamte verwaltete Cloud-Infrastruktur darstellt, und richten Sie einen Serviceaccount ein, der mit einem Ihrer Provider-Accounts funktioniert.
7. Geben Sie die Rechenzentren im Servicekonto an, die im Cloud-Konto enthalten sein sollen.

An Tag 2 können Sie zusätzliche Cloud-Accounts und Serviceaccounts vom selben Provider oder anderen Providern einrichten.

1. Verwenden Sie die Daten Configuration Management Database (CMDB), um die Cloud-Ressourcen anzufordern und zu verwalten und Ihre Cloud-Infrastruktur zu verwalten.
2. Führen Sie den Discovery -Prozess manuell für jedes Rechenzentrum im Servicekonto aus, um CMDB mit den Ressourcendaten für alle Rechenzentren zu füllen.
3. Konfigurieren Sie Discovery für die regelmäßige Ausführung, um sicherzustellen, dass die Daten aktualisiert werden.

Geführtes Setup verwenden, um Cloud-Services-Katalogzu implementieren

Geführtes Setup stellt eine Reihe von Aufgaben bereit, mit denen Sie CSK in Ihrer Instanz ServiceNow von konfigurieren können. Um Geführtes Setup für Cloud-Services-Katalogzu öffnen, navigieren Sie zu **Alle** > **Cloud-Servicekatalog – Geführtes Setup** in Ihrer Instanz.

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

Weitere Informationen finden Sie unter Geführtes Setup .

Cloud-Services-Katalog installieren

Sie können die Anwendung Cloud-Services-Katalog installieren, die Sie bei ServiceNow® Storeerworben haben, um sie in Ihrer -Instanz verfügbar zu machen.Die Anwendung enthält auch Demodaten und Demoinstallationen im Zusammenhang mit ServiceNow -Anwendungen und -Plugins, falls Sie diese noch nicht installiert haben.

Vorbereitungen

- AnwendungCloud-Services-Katalog aus ServiceNow® Store.
- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow® Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Siehe Berechtigungen für ein Produkt oder eine Anwendung von ServiceNow anfordern .

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

Warum und wann dieser Vorgang ausgeführt wird

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

- Plugins
- Out-of-Box-Katalog
- Rollen

Tipp:

Wenn Sie ein vorhandener Benutzer von Cloud-Services-Katalog oder CSK Innovation Labs sind:

- Ein Upgrade von der vorherigen Version wird derzeit nicht unterstützt. Um eine vorhandene Instanz mit den Apps Cloud-Services-Katalog oder CSK zu aktualisieren, gehen Sie wie folgt vor:

- ◦ Deinstallieren Sie die zuvor installierten CSK Apps mit Tabellenbereinigungen (InhaltspaketCSK und CSK in der Reihenfolge).
  ◦ Installieren Sie neue CSK Apps (CSK und CSK Inhaltspaket in derselben Reihenfolge).
  ◦ Da das geführte Setup nur einmal pro Instanz ausgeführt werden kann, platzieren Sie neue Terraform-Vorlagen manuell im Feld Terraform, aktualisieren Sie den Konfigurations-Provider der vordefinierten Terraform entsprechend, und führen Sie Discoveryaus.

Weitere Informationen finden Sie unter den Komponentenlinks.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendung** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Suchen Sie anhand des Namens oder der ID nach der Anwendung.
   Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über ServiceNow® Storeanfordern. CSK ist als separates Abonnement verfügbar und erfordert das Plugin Cloud Provisioning and Governance (com.snc.cloud.mgmt).
3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.
   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die mit der Anwendung installiert werden.

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

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zu ServiceNow® Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Cloud-Services-Katalog Setup für die Konfigurationsaufgabe „Tag 1“.

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

Sie müssen die Setup-Schritte Cloud-Services-Katalog der Reihe nach ausführen. An Tag 1 richten Sie den Cloud-Service für Zugriffs-, Sicherheits- und Abrechnungszwecke für Amazon Web Services und Microsoft Azure Cloud ein.

Bevor Sie diese Aufgaben lösen können, müssen Sie Cloud-Services-Katalog mit Ihrer Amazon Web Services - oder Microsoft Azure -Cloud integrieren und mit den Tag-2-Konfigurationsaufgaben fortfahren.

Wenn Sie alle Aufgaben für Tag 1 und Tag 2 abgeschlossen haben, finden Sie im Administrationsleitfaden des Cloud-Servicekatalogs weitere Informationen zur Verwendung der Anwendung Cloud-Services-Katalog in Ihrer Organisation.

Amazon Web Services auf Cloud-Services-Katalogeinrichten

Integrieren Sie Cloud-Services-Katalog mit Ihrem Konto Amazon Web Services im Rahmen der Tag-1-Konfigurationsaufgabe zur erstmaligen Einrichtung der Anwendung.

Vorbereitungen

Erfassen Sie Ihre Kontoeinstellungen und Anmeldeinformationen aus dem Anbieterportal. Diese Einstellungen und Anmeldeinformationen helfen Ihnen, die Ressourcen in einem Account von denen in einem anderen Account zu unterscheiden und sich bei AWSanzumelden oder zu authentifizieren. Berechtigungsrichtlinien legen Ihre Genehmigungen innerhalb der Ressourcen im Account fest.

Erforderliche Rolle:

- Administrator für den Betrieb in der -Verwaltungskonsole AWS oder AWS .
- Rolle „sn_cmp.cloud_admin“ für Vorgänge in Cloud-Services-Katalog

Prozedur

1. Weisen Sie den AWS -Benutzern von Cloud-Services-Katalog und einzelnen Benutzern Rollen anhand ihrer Aktivitäten und Zuständigkeiten zu.
   Weitere Informationen finden Sie unter Weisen Sie AWS-Benutzern von Rollen zu Cloud-Services-Katalog.
2. Installieren und konfigurieren Sie MID Servers für Cloud-Discovery und Cloud Provisioning and Governance.

   Um eine sichere und zuverlässige Kommunikation zu gewährleisten, kommuniziert der Prozess Discovery mit Ihren Cloud Provider-Konten und Cloud-Ressourcen über einen oder mehrere MID Servers. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie MID Servers für Cloud-Discovery und Cloud-Bereitstellung und Governance.

3. Richten Sie MID-Server in Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke ein, und konfigurieren Sie es für Cloud-Services-Katalog zur Verwendung eines Proxy-Servers. Durch die Verwendung eines Proxy-Servers werden alle cloudbasierten Aktivitäten unterstützt, z. B. das Ausführen von Discovery, das Abrechnen von Downloads, das

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

Bereitstellen virtueller Computer und das Ausführen von Lebenszyklusvorgängen auf virtuellen Computern.

4. Konfigurieren Sie für jedes Rechenzentrum mindestens einen MID Servers, um eine hohe Leistung und Sicherheit zu gewährleisten.
   Daten werden zum MID-Server sowie zwischen dem MID-Server und dem API-Endpunkt verschlüsselt.
5. Konfigurieren Sie MID-Server, auch wenn Sie bereits andere MID Servers konfiguriert haben, während Sie Cloud-Services-Katalog für einen anderen Cloud-Anbieter eingerichtet haben.
6. Konfigurieren Sie den Zugriff auf die Konten AWS mithilfe von permanenten AWS -Anmeldeinformationen.

   - Für den sicheren Zugriff auf Daten im Provider-Konto müssen im Prozess Discovery die entsprechenden Anmeldeinformationen bereitgestellt werden.
   - Damit die Anmeldeinformationen für Discovery und Cloud-Services-Katalogverfügbar sind, erstellen Sie zuerst einen Benutzer mit programmgesteuertem Zugriff auf die AWS -Verwaltungskonsole.
   - Sie können die Anmeldeinformationen sicher in einem Servicekonto unter Now Platform® speichern.
   - Weitere Informationen hierzu finden Sie unter Zugriff auf AWS-Accounts mit permanenten AWS-Anmeldeinformationen konfigurieren.
7. Richten Sie einen Cloud-Account und einen Serviceaccount für AWSein.

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

Einrichtung von Google Cloud Platform im Cloud-Servicekatalog

Integrieren Sie Cloud-Services-Katalog mit Ihrem Konto Google Cloud Platform als Teil der Konfigurationsaufgabe für Tag 1 zur erstmaligen Einrichtung CSK von .

Vorbereitungen

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

Erforderliche Rolle:

- Administrator für den Betrieb in Google Cloud oder Google Cloud Management Console
- Rolle „sn_cmp.cloud_admin“ für Vorgänge in CSK

Erfahren Sie mehr über das Einrichten von Google cloud mit der App Terraform Connector zum ersten Mal finden Sie unter Setup-Leitfaden für Tag 1 für Cloud Provisioning and Governance: Google Cloud Connector.

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

Prozedur

1. Weisen Sie Google Cloud-Anwendern von CSK und einzelnen Anwendern Rollen nach ihren Aktivitäten und Zuständigkeiten zu.

   Weitere Informationen finden Sie unter Rollen an Google Cloud Platform-Benutzer zuweisen.

2. Installieren und konfigurieren Sie MID-Server für Cloud-Discovery und Cloud Provisioning and Governance.
   Damit eine sichere und zuverlässige Kommunikation gewährleistet ist, findet eine Kommunikation zwischen dem Discovery-Prozess und Ihren Cloud Provider-Konten und Cloud-Ressourcen über mindestens einen MID Server statt. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie MID Servers für den Zugriff auf Cloud-Umgebungen.
3. Richten Sie den MID-Server in Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke ein, und konfigurieren Sie ihn für CSK zur Verwendung eines Proxy-Servers.
   Durch die Verwendung eines Proxy-Servers werden alle cloudbasierten Aktivitäten unterstützt, z. B. Ausführen von Discovery, Abrechnungsdownloads, Bereitstellen virtueller Computer und Ausführen von Lebenszyklusvorgängen auf virtuellen Computern.
4. Konfigurieren Sie einen oder mehrere MID-Server für jedes Rechenzentrum, um eine hohe Leistung und Sicherheit zu gewährleisten.
   Daten werden sowohl auf dem MID-Server als auch zwischen dem MID-Server und dem API-Endpunkt verschlüsselt.
5. Konfigurieren Sie den MID-Server auch dann, wenn Sie bereits andere MID-Server konfiguriert haben, als Sie Cloud-Services-Katalog für einen anderen Cloud-Anbieter eingerichtet haben
6. Erstellen Sie den Service-Account und die Schlüssel (Anmeldeinformationen) in Google Cloud, falls Sie ihn nicht haben.
   Sie können die Anmeldeinformationen sicher in einem Servicekonto speichern.
   Sie benötigen die IAM-Rolle „Service-Account-Schlüsseladministrator“ (roles/iam.serviceAccountKeyAdmin) für das Projekt oder den Service-Account, dessen Schlüssel Sie verwalten möchten. Diese Berechtigungen können vom Administrator vergeben werden. Für den sicheren Zugriff auf Daten im Provider-Konto müssen im Discovery-Prozess die entsprechenden Anmeldeinformationen bereitgestellt werden.

   Weitere Informationen finden Sie unter Richten Sie Servicekonten für die Google Cloud Platform ein.

7. Richten Sie einen Cloud-Account und einen Serviceaccount für Google Cloud Platformein.

   - Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert werden. Discovery greift mithilfe dieser Informationen auf Ihren Provider-Account zu, um die Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.
   - Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud-Services-Katalog. Ein Cloud-Account kann mehrere Service-Accounts enthalten, einschließlich der Service-Accounts verschiedener Anbieter. Für jedes Servicekonto geben Sie an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

   Weitere Informationen finden Sie unter Richten Sie Cloud-Konto und Servicekonto für ein Google Cloud Platform.

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

Microsoft Azure Cloud in Cloud-Services-Katalogeinrichten

Integrieren Sie Cloud-Services-Katalog mit Ihrem Konto Microsoft Azure als Teil der Konfigurationsaufgabe für Tag 1 zur erstmaligen Einrichtung CSK von .

Vorbereitungen

Erfassen Sie Ihre Kontoeinstellungen und Anmeldeinformationen aus dem Anbieterportal. Diese Einstellungen und Anmeldeinformationen helfen Ihnen, die Ressourcen in einem Account von denen in einem anderen Account zu unterscheiden und sich bei Microsoft Azureanzumelden oder zu authentifizieren. Berechtigungsrichtlinien legen Ihre Genehmigungen innerhalb der Ressourcen im Account fest.

Erforderliche Rollen:

- Microsoft Azure oder Microsoft Azure AD-Administrator (Active Directory).
- Anwendungsadministrator
- Anwendungsentwickler
- Cloud-Anwendungsadministrator und die Rolle „Beitragender für Ressourcenrichtlinien“ zum Erstellen oder Ändern der Ressourcenrichtlinien.
- Rolle „sn_cmp.cloud_admin“ für Vorgänge in Cloud-Services-Katalog

Prozedur

1. Weisen Sie Azure Anwendern von Cloud Provisioning and GovernanceRollen zu.

   Cloud Provisioning and Governance -Rollen weisen Sie den -Benutzergruppen und einzelnen Benutzern basierend auf den Benutzeraktivitäten und Zuständigkeiten zu. Weitere Informationen hierzu finden Sie unter Azure-Benutzern von Cloud Provisioning and Governance Rollen zuweisen.

2. Installieren und konfigurieren Sie MID Servers für Cloud-Discovery und Cloud Provisioning and Governance.

   Um eine sichere und zuverlässige Kommunikation zu gewährleisten, kommuniziert der Prozess Discovery mit Ihren Cloud Provider-Konten und Cloud-Ressourcen über einen oder mehrere MID Servers. Weitere Informationen finden Sie unter Installieren und konfigurieren Sie MID Servers für den Zugriff auf Cloud-Umgebungen.

3. Richten Sie MID Servers in Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke ein. Daten werden zum MID-Server sowie zwischen dem MID-Server und dem API-Endpunkt verschlüsselt.
4. Konfigurieren Sie mindestens einen MID Servers für jedes verwaltete Rechenzentrum, um eine hohe Leistung und Sicherheit zu gewährleisten.
   Konfigurieren Sie MID-Server, auch wenn Sie bereits andere MID Servers beim Einrichten von Cloud-Services-Katalog für einen anderen Cloud-Anbieter konfiguriert haben.
5. Erstellen Sie einen Microsoft Azure -Serviceprinzipal.

   Für den sicheren Zugriff auf die Ressourcen und Abrechnungsdaten in Ihrem Konto Microsoft Azure müssen vom Prozess Discovery entsprechende Anmeldeinformationen für das Konto Microsoft Azure bereitgestellt werden. Um die erforderlichen Anmeldeinformationen zu generieren, erstellen Sie ein spezielles programmatisches Konto – einen Microsoft Azure -Serviceprinzipal. Weitere Informationen finden Sie unter Microsoft Azure-Serviceprinzipal erstellen.

6. Speichern Sie die Anmeldeinformationen des Azure -Serviceprinzipals in der -Instanz.

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

Für den sicheren Zugriff auf die Daten im Provider-Konto müssen im Prozess Discovery die entsprechenden Anmeldeinformationen bereitgestellt werden. Damit die Anmeldeinformationen für Discoveryverfügbar sind, erstellen Sie zuerst die Anmeldeinformationen des Serviceprinzipals Microsoft Azure für im Portal Azure. Anschließend können Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz speichern. Weitere Informationen hierzu finden Sie unter Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern.

7. Fügen Sie ein Servicekonto Azure hinzu. Fügen Sie ein Azure-Servicekonto hinzu

   Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert werden. Discovery verwendet die Informationen für den Zugriff auf Ihren Provider-Account, um Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Weitere Informationen finden Sie unter Azure-Service-Account hinzufügen.

8. Erkennen Sie alle Rechenzentren in einem Servicekonto.

   Discovery verwendet die Informationen im Servicekonto, um alle dem Anbieterkonto zugeordneten logischen Rechenzentren zu identifizieren.

9. Richten Sie einen Cloud-Account für Azureein.

   Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud-Services-Katalog. Ein Cloud-Account kann mehrere Service-Accounts enthalten, einschließlich der Service-Accounts verschiedener Anbieter. Für jedes Servicekonto geben Sie an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen. Weitere Informationen finden Sie unter Cloud-Account für Azure einrichten.

10. Legen Sie die Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen fest.

    Kapazitätsgrenzen schränken die Attribute der Cloud-Ressourcen ein, z. B. die Anzahl der virtuellen Computer, virtuellen CPUs oder Aggregatspeicher. Sie können die Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

Azure DevOps und die Pipeline für kontinuierliche Integration/kontinuierliche Bereitstellung werden integriert

Sie können die Release-Anforderung aus dem Workflow Cloud-Services-Katalog mit Azure DevOps für die End-to-End-Automatisierung des Entwicklungsprozesses, einschließlich der Bereitstellung der Ressourcen sowie der Bereitstellung und Überwachung der Anwendungen, verarbeiten.

Die Pipelineintegration von Azure DevOps und kontinuierliche Integration – kontinuierliche Bereitstellung (CI-CD-Tool) ist ein Release-Bereitstellungsprozess. Sie können Cloud-Services-Katalog und das CI-CD-Tool verwenden, um die bereitgestellten Ressourcen in Configuration Management Database (CMDB)direkt über Flows und Aktionen zu verwalten.

Vorteile von Azure DevOps -Pipelines mit Cloud-Services-Katalog

Durch die Verwendung der Pipelines Azure DevOps mit Cloud-Services-Katalogbietet Ihre Organisation die folgenden Vorteile:

- Fähigkeit, mit CI-CD-Pipelines unabhängig von den zugrunde liegenden Sprachen zu arbeiten, die in den Pipelines verwendet werden (JavaScript, Java, Node.js oder Python).
- Unterstützung für alle gängigen Versionskontrollsysteme wie GitHub, GitLab, Azure DevOps, Atlassian Bitbucket oder Team Foundation Version Control (TFVC).
- Unterstützung für die Cloud-Services Amazon Web Services und Microsoft Azure.

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

- Fähigkeit, die Anwendung überall (in der Cloud oder lokal, in Containern oder auf virtuellen Computern) oder in jeder Umgebung bereitzustellen. Weitere Informationen finden Sie unter ADO und Release- und Lebenszyklus-Management.
- Fähigkeit, Kubernetes, Platform as a Service (PaaS) usw. bereitzustellen, ohne dass eine Entwicklungsänderung erforderlich ist.
- Automatische Aktualisierungen von CMDB über die erforderlichen Tags.
- Genehmigungen und Governance-Schritte, die in den Workflow integriert sind.

Wichtige Schritte bei der Integration von Azure DevOps und CI-CD-Pipelines

1. Verwenden Sie die Release-Pipelines und Azure DevOps von Cloud-Services-Katalog.
2. Richten Sie die Konsole Microsoft Azure DevOps ein.
3. Führen Sie Discovery auf dem Konfigurations-Provider Azure DevOps aus.
4. Bestellen Sie ein Microsoft Azure DevOps -Katalogelement.

Release-Pipelines und Azure DevOps nach Cloud-Services-Katalog

Azure DevOps verfügt über Release-Pipelines, z. B. die Pipelines für kontinuierliche Integration/kontinuierliche Bereitstellung (CI-CD), die einen Build-, Test- und Bereitstellungsansatz bieten. Sie können diese vollständig automatisierten Prozesse verwenden, um Build-Anforderungen schnell in der Produktionsumgebung bereitzustellen.

Cloud-Services-Katalog stellt die Release-Pipeline Azure DevOps als CI-CD-Tool bereit, mit dem Sie Anwendungen für den gesamten Entwicklungslebenszyklus über verschiedene Plattformen und Cloud-Anbieter hinweg erstellen, testen und bereitstellen können.

Azure DevOps in Cloud-Services-Katalog bietet zusätzliche Funktionen für die Verwaltung von Arbeitselementen, Versionskontrolle, Projektmanagement und Berichterstellung. Ressourcenanforderungen über Pipelines Azure DevOps werden nach Genehmigung durch den Governance- und Anpassungs-Workflow verarbeitet.

Richten Sie die Konsole Microsoft Azure DevOps ein

Richten Sie die Konsole Microsoft Azure DevOps als ersten Schritt ein, bevor Sie Discovery ausführen und ein Katalogelement in der Anwendung Cloud-Services-Katalog bestellen.

Vorbereitungen

1. Fügen Sie den Pipelines Microsoft Azure DevOps in Ihrer Organisation eine Variable „deploymentID“ hinzu. Die Microsoft Azure DevOps -Integration erkennt nur Pipelines mit einer „deploymentID“-Variablen.
2. Kennzeichnen Sie alle bereitgestellten Ressourcen mit einem „deploymentID“-Schlüssel in der Pipeline, damit Sie die Ressourcen nach der Bereitstellung erkennen können.

Die „subscriptionID“ ist für die Vorlagen Azure DevOps und Ansible nicht erforderlich.

Erforderliche Rolle: keine

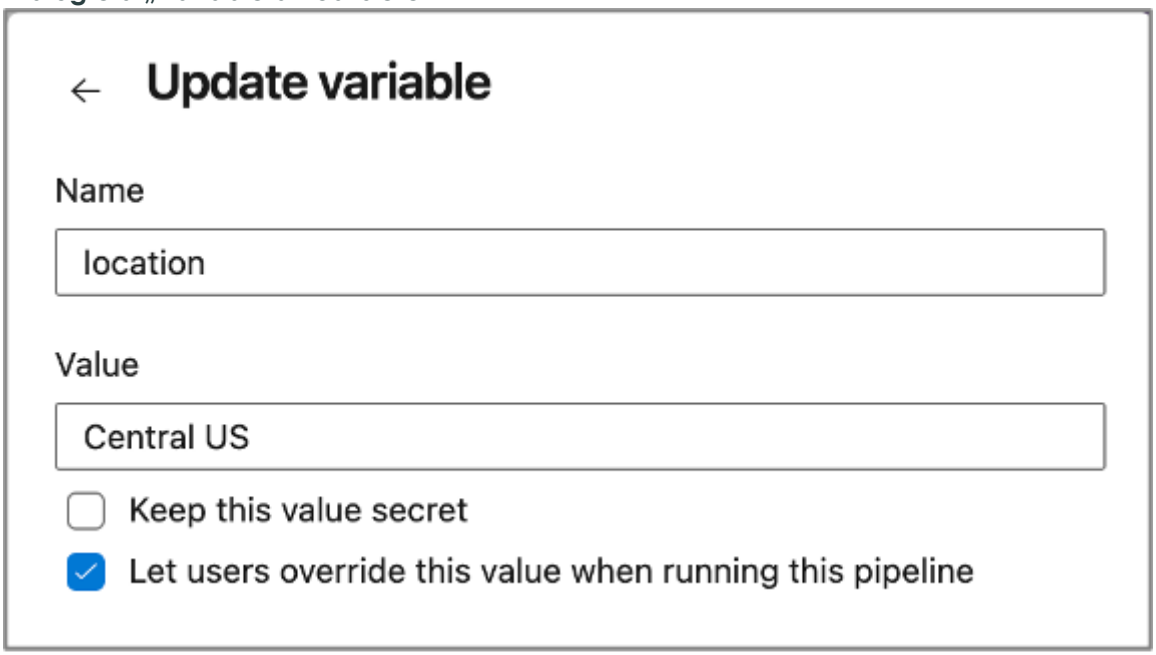
Prozedur

1. Benennen Sie eine Pipeline-Variable für „deploymentID“, die Sie für den Verweis auf Discovery verwenden können, um die Ressourcen in CMDBzu aktualisieren.
2. Erstellen Sie PAT-Anmeldeinformationen (Personal Access Token), die Sie in Azure DevOps Discoveryverwenden können.

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

3. Überschreiben Sie im Dialogfeld **„Variable aktualisieren“** die Pipelinevariablen, indem Sie das Kontrollkästchen **Diesen Wert von Anwendern beim Ausführen dieser Pipeline überschreiben** aktivieren.

Dialogfeld „Variable aktualisieren“



Die -Pipeline funktioniert mit dem -Katalogelement CSK DevOps-Integration. Die Microsoft Azure DevOps -Integration erkennt Pipelines mit der Variable „deploymentID“.

Führen Sie Discovery auf dem Konfigurations-Provider Azure DevOps aus

Fügen Sie den Konfigurations-Provider Azure DevOps hinzu, und führen Sie Discovery aus, um mithilfe der Anwendung Cloud-Services-Katalog alle Projekte, Pipelines und Pipeline-Variablen in einer Organisation zu erkennen.

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

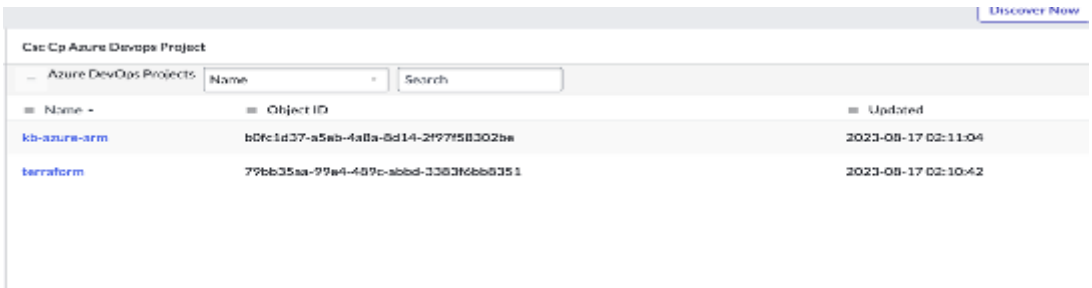
1. Navigieren Sie zum **Administratorportal**, und wählen Sie **VerwaltenAnmeldeinformationen**.
2. Fügen Sie die **API Key-** Anmeldeinformationen hinzu, die Sie mit den Anmeldeinformationen des Personal Access Token (PAT) erstellt haben.
3. Stellen Sie den Anmeldeinformationen für das persönliche Zugriffstoken (PAT) gerade Anführungszeichen („:“) voran, und codieren Sie sie im Base64-Format.
4. Stellen Sie der codierten Formatzeichenfolge eine Standardzeichenfolge voran. Beispiel: Basic encoded base 64(:PAT).
5. Fügen Sie einen erforderlichen Alias hinzu.
6. Navigieren zu **Verwalten** > **Konfigurationsverwaltung** und fügen Sie einen Konfigurations-Provider hinzu.

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

Wichtig:

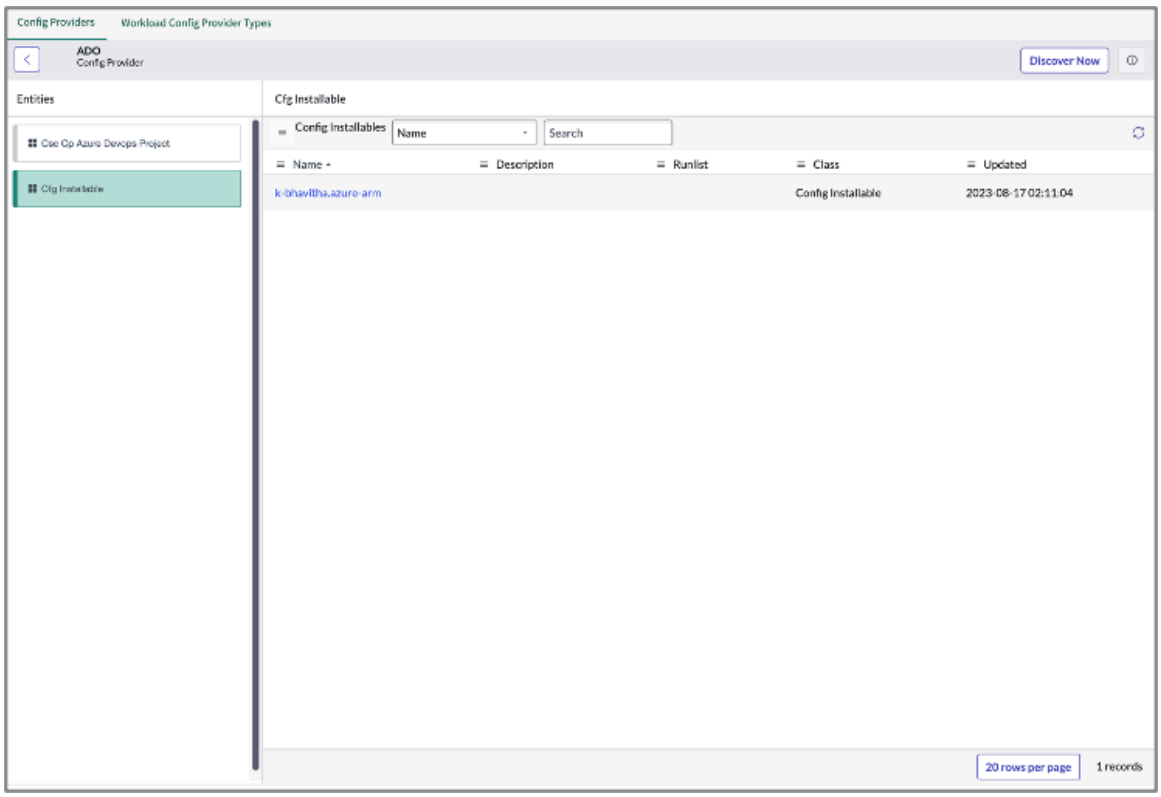
Infrastructure as Code (IaC) Discovery wird unterstützt. Sie können die Auftragsvorlagen der Azure DevOps -Pipeline Ansible erkennen, indem Sie eine geplante Discovery einrichten.

7. Erkennen Sie alle Projekte, Pipelines und Pipelinevariablen in einer Organisation, indem Sie Discoveryausführen.



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

8. Suchen Sie die installierbaren Konfigurationselemente unter dem ausgewählten Projekt Azure DevOps.



Ergebnisse

Sie können jetzt ein Azure DevOps -Katalogelement über das Azure DevOps -Katalogbestellformular unter Mitarbeiter-Centerbestellen.

Bestellen Sie ein Microsoft Azure DevOps -Katalogelement

Stellen Sie den Katalog Microsoft Azure DevOps mithilfe des Katalogbestellformulars Microsoft Azure DevOps in der Anwendung Cloud-Services-Katalog bereit.

Vorbereitungen

Um Microsoft Azure DevOps für Cloud-Services-Katalogzu verwenden, weisen Sie dem MID-Server die Funktionen Azure DevOps und Cloud-Management zu. Weitere Informationen finden Sie unter MID-Server-Fähigkeiten konfigurieren .

Legen Sie diebereitstellungs-ID als Variablen in den Pipelines AWS fest, die erkannt werden sollen. Die „subscriptionID“ ist für die Pipelines Microsoft Azure nicht erforderlich.

Alle Ressourcen mit dem Schlüssel „deploymentID“ kennzeichnen.

Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

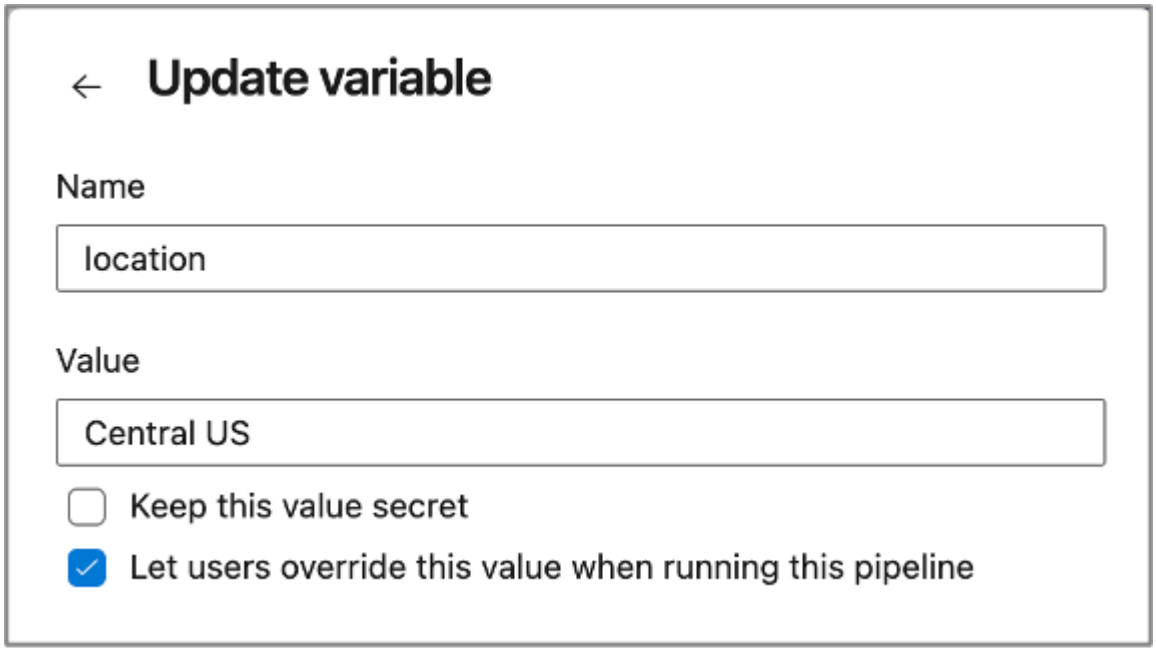
https://players.brightcove.net/6274575390001/nUx4EKfUz_default/index.html?videoId=6351050870112

Folgen Sie diesem kurzen Video, um zu erfahren, wie Sie ein Azure DevOps-Katalogelement bestellen.

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

Prozedur

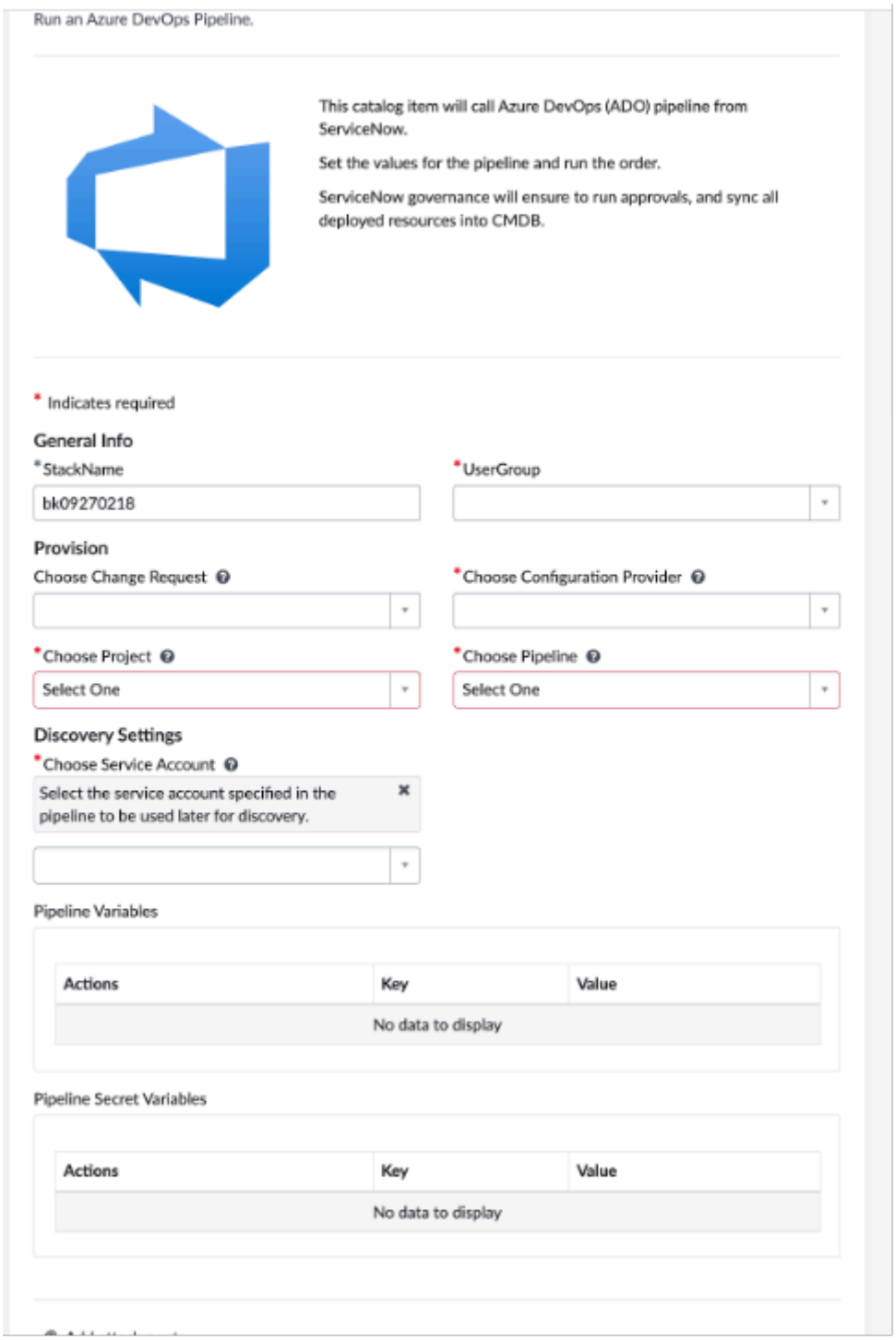
1. Überschreiben Sie im Dialogfeld **„Variable aktualisieren“** die Pipelinevariablen, indem Sie das Kontrollkästchen **Diesen Wert von Anwendern beim Ausführen dieser Pipeline überschreiben** aktivieren.



2. Navigieren zu **Mitarbeiter-Center** > **Cloudservices** > **Integrationen** > **CSC DevOps-Integration**.

   Verwenden Sie dieses Azure DevOps -Katalogelement-Bestellformular, um eine ADO-Pipeline aufzurufen.

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



3. Füllen Sie im Formular die Felder **UserGroup** und **Change Request** aus.
4. Wählen Sie in der Liste Konfigurationsanbieter auswählen den Konfigurationsanbieter aus, der der Organisation Azure DevOps zugeordnet ist.
5. Wählen Sie das -Projekt und die zugehörige Pipeline in der Organisation aus.

   Die Pipelinevariablen werden automatisch ausgefüllt. Sie können die Variablen ändern. Obwohl beispielsweise die geheimen Pipeline-Variablen maskiert sind, können Sie diese Werte ändern.

6. Wählen Sie den **Serviceaccount**aus. Dies ist dieselbe Option, die Sie als Serviceverbindung in der Pipeline Azure DevOps ausgewählt haben.

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

- Für Amazon Web Serviceswird eine Standortliste angezeigt, wenn Sie **Serviceaccount**auswählen.
- Sie können den Standort oder die Region einer Pipeline-Variablen verfügbar machen und in einer Pipeline für die Bereitstellung verwenden. Diese Pipeline-Variable wird von dem Wert überschrieben, den Sie in der Standortliste ausgewählt haben, um sicherzustellen, dass sich Bereitstellung und Discovery am selben Standort befinden.
- Für Discovery in Microsoft Azureist ein Standort erforderlich, daher wird keine Liste angezeigt, wenn Sie **Serviceaccount**auswählen. Diese Einstellungen stellen sicher, dass die richtigen Ressourcen, die sich auf den Stapel beziehen, in CMDBausgefüllt sind. Basierend auf diesen Einstellungen können Sie Discovery ausführen.

7. Wenn der Speicherort für die Pipeline AWS vorab ausgefüllt ist, wählen Sie den gleichen Speicherort im Katalog für Discoveryaus.
8. Richten Sie die identifizierenden Tags für die bereitgestellten Ressourcen ein.
   Das Feld DeploymentID ist schreibgeschützt und wird für den Auftrag automatisch generiert. Die DeploymentID wird allen bereitgestellten Ressourcen als Tag zugewiesen, wenn Sie sie als Tag in der Pipelinevorlage Azure DevOps der Stapel in der Cloud hinzugefügt haben. Die DeploymentID wird dem Stapel auch als Tag zugewiesen. Wenn die Pipeline eine dieser drei Variablen hat (Anwendung, BusinessService oder Kosten-Center), werden sie in den Allgemeine Informationen in der Anwenderoberfläche Azure DevOps angezeigt.
9. Wählen Sie aus der Liste die Feldwerte aus, die in den Pipelinevariablen aktualisiert werden sollen.

   Diese Einträge werden nur für den aktuellen Auftrag berücksichtigt.

   Hinweis: Sie können diese schreibgeschützten Variablen nicht im Abschnitt Pipeline-Variable ändern. Diese Variablen werden dem Stapel in der Cloud als Tags hinzugefügt und auch in die Schlüsselwerttabelle CMDB eingefügt. Sie können nur die Aktionen auf Ressourcenebene auf einem bereitgestellten Stapel ausführen, da die Aktion auf Stapelebene deaktiviert ist. Der vorherige Stapel wird als veraltet markiert, wenn Sie die Pipeline erneut ausführen, obwohl die Ressourcen in der Cloud verbleiben.

Nächste Maßnahme

Stellen Sie sicher, dass eine Blueprint-Genehmigungsrichtlinie (CSK Inhaltsgenehmigungsrichtlinie ADO Integration) auf den Katalog Microsoft Azure DevOps angewendet wird. Diese Richtlinie schreibt vor, dass eine Genehmigung von der Change-Managementgruppe eingeholt werden muss, bevor eine Bereitstellung stattfinden kann.

Ansible mit Cloud-Services-Katalog integrieren

Integrieren Sie Ansible mit Cloud-Services-Katalog als Tag-1-Aktivität. Mit dieser Aktivität können Sie eine Ansible -Auftragsvorlage über ein ServiceNow -Katalogelement bereitstellen.

Als cloud_service_user können Sie auf den Konfigurations-Provider und Auftragsvorlagen zugreifen und eine Auftragsvorlage über ein Katalogelement bereitstellen.

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

Support ab Tag 0	Support ab 1 Tag	Support ab Tag 2
1. Rufen Sie die -Ressourcen aus der Cloud ab, und aktualisieren Sie die CMDB 2. Stellen Sie sicher, dass keine Fehler vorliegen. Wenn Fehler angezeigt werden, ist die Bereitstellung von Discovery oder der Auftragsvorlage fehlgeschlagen	1. Bestellen Sie eine Ansible -Auftragsvorlage bei Servicekatalog 2. Verweisen Sie auf die erkannten Microsoft Azure -Pipelines, die für Ansiblespezifisch sind. 3. Wählen Sie Eingaben aus, die für die Release-Bereitstellungs-Pipeline erforderlich sind 4. Übermitteln Sie einen Katalog 5. Veröffentlichen Sie ein vordefiniertes Katalogelement als Cloud-Services-Katalog -Inhalt 6. Wählen Sie die Auftragsvorlagen aus, auf die Sie Zugriff haben, und stellen Sie sie bereit	1. Korrigieren Sie die Zuordnung von „Out-of-Box über Cloud-Services-Katalog -Inhalt 2. Aktualisiert die Dokumentation zum Einschränken der Ausführung der Auftragsvorlage auf einem bestimmten Host 3. Testen und dokumentieren Sie, wie die Bereitstellung der Auftragsvorlage auf nicht verwalteten Knoten unterstützt wird 4. Starten Sie Ihren Tag-2-Support für Ansible AWX
In CMDB als referenzierbare Objekte speichern.	1. Warten Sie auf die Auftragsgenehmigung 2. Verfolgen Sie den Fortschritt Ihrer Vorlagenbestellung 3. Aktualisieren Sie CMDB mit den bereitgestellten Ressourcen	1. Stellen Sie sicher, dass alle Support-Aktionen für Tag 2 erfolgreich ausgeführt werden 2. Zwischen blauer (aktuelle Anwendung) und grüner (neue Anwendung) Umgebung wechseln

Richten Sie Ansible als Tag-1-Aufgabe ein

Richten Sie die Konsole Ansible als Tag-1-Aufgabe ein, bevor Sie Discovery ausführen und eine Auftragsvorlage über ein ServiceNow -Katalogelement mithilfe der Anwendung Cloud-Services-Katalog bereitstellen.

Vorbereitungen

Legen Sie die „deploymentID“ für die zusätzlichen Variablen für Auftragsvorlagen Ansible fest.

Wählen Sie die Option **Beim Start auffordern** neben dem Abschnitt „Variablen“ in der Vorlage aus. Wenn Sie diese Aktion nicht ausführen, können Sie die standardmäßigen extra_vars, die mit den Werten aus dem Katalogbestellformular definiert sind, nicht aktualisieren oder überschreiben, während Sie die Vorlage starten.

Markieren Sie alle Ressourcen mit dem Schlüssel „deploymentID“, um Discovery nach der Bereitstellung zu aktivieren.

Erforderliche Rolle: Administrator

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

Prozedur

1. Speichern Sie die zusätzlichen Variablen lokal im JSON-Format, um Configuration Management Database (CMDB)zu erkennen und zu aktualisieren.
2. Erstellen Sie Ansible Tower-Anmeldeinformationen, die in Ansible Discoveryverwendet werden sollen.
   Weitere Informationen finden Sie unter Ansible Tower-Benutzernamen und -Passwort konfigurieren.
3. Zulassen, dass die zusätzlichen Variablen und Auftragsvorlagen überschrieben werden. Die Standardauftragsvorlage Ansible muss überschrieben werden, damit die Pipeline mit einem Cloud-Services-Katalog Ansible -Automatisierungskatalogelement funktioniert.

Führen Sie Discovery für den Konfigurations-Provider Ansible aus

Fügen Sie den Konfigurations-Provider Ansible hinzu, und führen Sie Discovery aus, um den Inhalt des Bestands, die Hostgruppe und die verfügbaren Auftragsvorlagen zu ermitteln.

Vorbereitungen

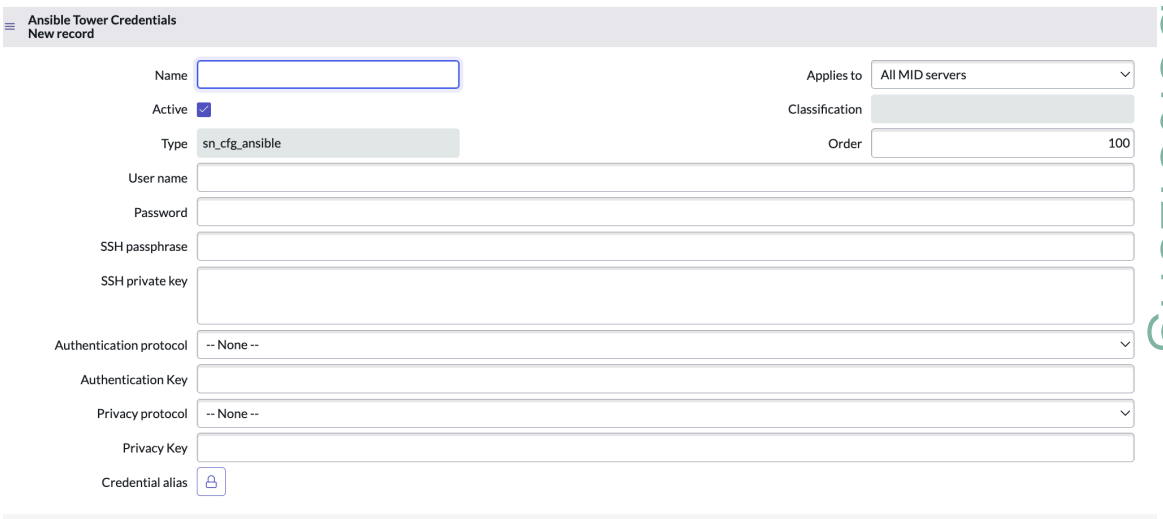
Führen Sie dieses Verfahren nur aus, wenn Sie über die Tower-Anmeldeinformationen Ansible verfügen.

Erforderliche Rolle: keine

Prozedur

1. Navigieren zu **Cloud-Adminportal** > **Verwalten** > **Anmeldeinformationen** > **Neu** > **Ansible Tower-Anmeldeinformationen**.
2. Füllen Sie die Felder des Formulars gemäß den Informationen aus, die Sie vom Ansible Tower erhalten haben.

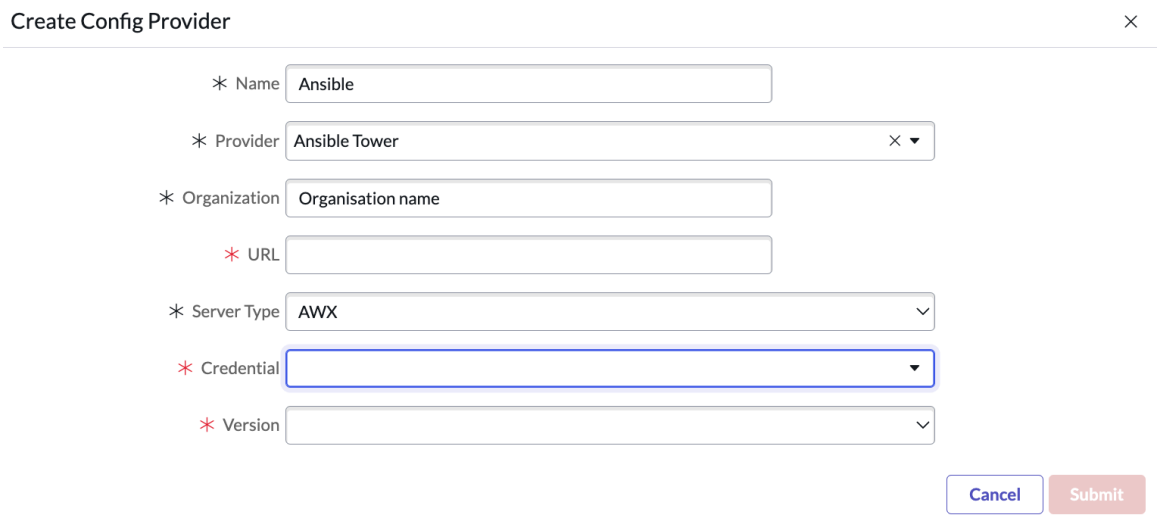
Ansible Tower-Anmeldeinformationen



3. Wählen Sie **Absenden**.
4. Erstellen Sie einen Konfigurations-Provider, indem Sie **Neu**auswählen.

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

Formular für Konfigurationsprovider erstellen

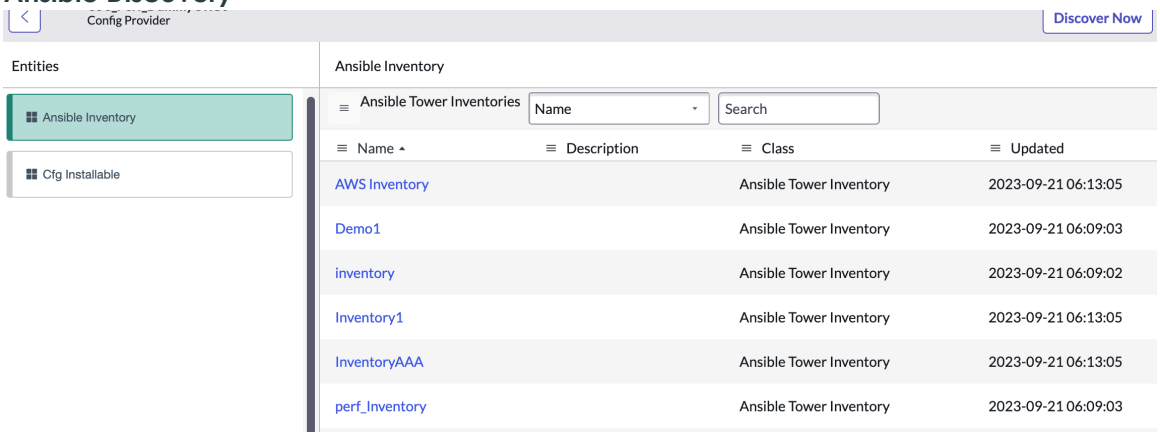


Wichtig:

Infrastructure as Code (IaC) Discovery wird unterstützt. Sie können Auftragsvorlagen, Bestand und Gruppen erkennen.

5. Führen Sie Discovery aus, um alle Projekte und zusätzlichen Variablen in einer Organisation zu erkennen.

Ansible Discovery



Ergebnisse

Sie sind bereit, die nächsten Schritte auszuführen, um einen Ansible -Artikel zu bestellen.

Bestellen Sie eine Ansible -Auftragsvorlage

Verwenden Sie Cloud-Services-Katalog, um eine Ansible -Auftragsvorlage zu bestellen, die aus dem Katalogelement aufgerufen wird.

Vorbereitungen

Erforderliche Rolle: cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird

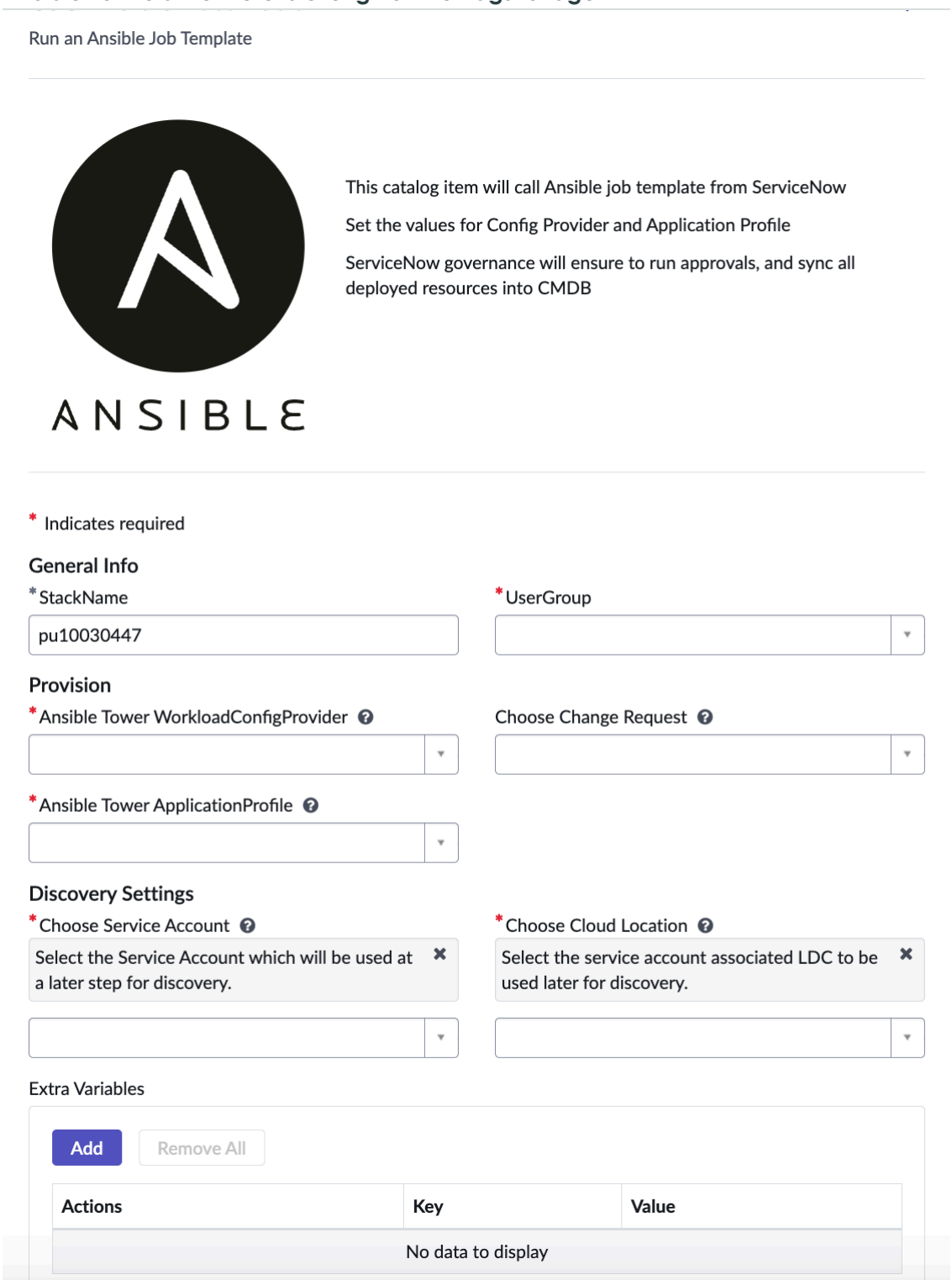
Sie können das Bereitstellungsformular für Auftragsvorlagen Ansible verwenden, um eine Auftragsvorlage Ansible aufzurufen und über ein ServiceNow -Katalogelement zur Bereitstellung auszuführen.

Automatische Übersetzung

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

Prozedur

1. Navigieren zu **Mitarbeiter-Center** > **Cloudservices** > **Integrationen** > **CSC Ansible-Automatisierung**.



Automatische Übersetzung

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

Ansible Vorlagenformularfelder

Felder	Beschreibung
UserGroup	Benutzergruppe, die dem Benutzer zugewiesen ist.
Bereitstellung	Bereitstellungsdetails. Wählen Sie den Workload Config-Provider und ApplicationProfile aus dem Ansible Tower aus.
Service-Account wählen	Pipeline Für Amazon Web Serviceswird die Standortliste angezeigt, wenn Sie **Serviceaccount**auswählen. Der Speicherort ist für Discovery in Microsoft Azurenicht erforderlich. **Tipp:** Sie können eine zusätzliche Variable verfügbar machen, die in einem JSON-Format am Tower-Standort oder in der Region Ansible gespeichert wurde, und sie in der Vorlage für die Bereitstellung verwenden. Diese zusätzliche Variable wird durch den Wert überschrieben, den Sie in der Liste Standort ausgewählt haben. Durch die Verwendung dieser zusätzlichen Variable stellen Sie sicher, dass sich Bereitstellung und Discovery am selben Ort befinden. Diese Einstellungen stellen sicher, dass die richtigen Ressourcen, die sich auf den Stapel beziehen, in CMDBausgefüllt sind. Basierend auf diesen Einstellungen können Sie Discovery ausführen.
Cloud-Standort wählen	Service-Account, der ein zugeordnetes logisches Rechenzentrum (LDC) für Discovery ist.
Zusätzliche Variablen	Zusätzliche Variablen, die Sie ändern können, auch wenn die Werte automatisch ausgefüllt und maskiert werden.

2. Richten Sie die identifizierenden Tags ein.
   Das Feld DeploymentID ist schreibgeschützt und wird für den Auftrag automatisch generiert. Die DeploymentID wird allen bereitgestellten Ressourcen als Tag zugewiesen, wenn Sie sie als Tag in der Pipelinevorlage Azure DevOps der Stapel in der Cloud hinzugefügt haben. Die DeploymentID wird dem Stapel auch als Tag zugewiesen. Wenn die Pipeline eine dieser drei Variablen hat (Anwendung, BusinessService oder Kostenstelle), werden sie in den Allgemeine Informationen auf der Anwenderoberfläche des Formulars Ansible Auftragsvorlage angezeigt.

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

3. Wählen Sie die Feldwerte aus der Liste aus, die in den Pipelinevariablen aktualisiert werden sollen.

   Diese Einträge werden nur für den aktuellen Auftrag berücksichtigt.

   Hinweis: Sie können nur die Aktionen auf Ressourcenebene auf einem bereitgestellten Stapel ausführen, da die Aktion auf Stapelebene deaktiviert ist. Der vorherige Stapel wird als veraltet markiert, wenn Sie die Pipeline erneut ausführen, obwohl die Ressourcen in der Cloud verbleiben.

Nächste Maßnahme
Vergewissern Sie sich, dass eine Blueprint-Genehmigungsrichtlinie (CSK Inhaltsgenehmigungsrichtlinie Ansible) angewendet wird. Diese Richtlinie schreibt vor, dass die Genehmigung von der Change-Managementgruppe eingeholt werden muss, bevor eine Bereitstellung stattfinden kann.

Cloud-Services-Katalog-Administrationsleitfaden

Nachdem Sie die Anwendung Cloud-Services-Katalog eingerichtet haben, müssen Sie einige zusätzliche Elemente einrichten, damit Ihre Benutzer beliebige Cloud-Ressourcen anfordern und verwalten können.

Governance wird konfiguriert

Sie können Governance-Tools verwenden, um die Bereitstellung von Cloud-Ressourcen wie Kontingente und Richtlinien einzuschränken. Sie können beispielsweise den Genehmigungs-Workflow konfigurieren, der verwendet wird, nachdem ein Benutzer eine Cloud-Ressource angefordert hat, ob eine E-Mail gesendet wird, nachdem eine Cloud-Ressource angehalten wurde, und welches Rechenzentrum automatisch ausgewählt wird, wenn ein Benutzer eine Ressource von einem Cloud-Anbieter auswählt. Weitere Informationen zu Kontingenten, Richtlinien und anderen Governance-Typen finden Sie unter Cloud-Governance.

Füllen von aus Cloud-Services-Katalog

Nachdem Sie die Governance-Kontingente und -Richtlinien angewendet haben, müssen Sie Cloud-Services-Katalog -Elemente erstellen. Sie haben folgende Möglichkeiten, um ein Katalogelement zu erstellen:

1. Importieren Sie eine Vorlage aus Amazon Web Services, Microsoft Azure oder Google Cloud Platform.
2. Verwenden oder ändern Sie ein sofort einsatzbereites Katalogelement.
3. Verwenden Sie eine Terraform-Vorlage.

Informationen zu Domain Separation, zur Unterstützung mehrerer Repositorys mit der App Terraform, zu Cloud-Accounts, zum Cloud-Adminportal oder zur Cloud-API finden Sie in den folgenden Themen:

- Verwenden Sie die Struktur aus mehreren Repositorys mit der App Terraform Connector .
- Domain Separation und Cloud-Services-Katalog: Zusätzliche Informationen zu Domain Separation abrufen.
- Cloud-Accounts: Erfahren Sie mehr über die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance.

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

- Cloud-Adminportal: Über dieses Portal können Sie alle Ihre Cloud-Ressourcen verwalten, entwerfen, steuern, betreiben und analysieren.
- Cloud-API (CAPI): Integrieren Sie Cloud Provisioning and Governance mit Cloud-Anbieter mithilfe von REST APIs.

Cloud-Services-Katalog und Terraform Connector

Verwenden Sie die App Cloud-Services-Katalog mit Terraform Connector-Unterstützung mit all ihren Funktionen, die bei der Bereitstellung und Verwaltung von Cloud-Ressourcen in verschiedenen Public und Private Clouds helfen.

Schlüsselfunktionen von Terraform Connector:

- Verwenden Sie Terraform als Konfigurationsanbieter, um Ressourcen in den folgenden Clouds bereitzustellen:
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Google Cloud-Anbieter
- Erkennen Sie die IaC-Vorlagen (Infrastructure as Code), um die IaC-Vorlagen (Terraform) aus der Umgebung Terraform zu erkennen.
- Generieren Sie Katalogelemente mit den -Vorlagen Terraform und verwenden Sie sie, um Ressourcen in verschiedenen Cloud-Umgebungen bereitzustellen.
- Nutzen Sie die Unterstützung der Struktur mehrerer Repositorys mit der App Terraform. Weitere Informationen finden Sie unter Verwenden Sie die Struktur aus mehreren Repositorys mit der App Terraform Connector ..

Weitere Informationen zu Terraform Connector, zur Konfiguration der erweiterten Funktionen und zu ihrer Verwendung finden Sie unter Cloud Provisioning and Governance: Terraform Connector erkunden.

Berechtigungsmanagement für Cloud-Services-Katalog

Berechtigungen sind Ihre Zugriffsrechte auf Gruppenebene für Funktionen und Aktionen in Cloud-Services-Katalog.

Die Berechtigungsrichtlinien im Benutzerportal Cloud Provisioning and Governance steuern die Aktionen, die für Benutzer basierend auf der -Benutzergruppe zulässig oder eingeschränkt sind. Informationen zu Berechtigungstypen und -ideen finden Sie unter Berechtigungsverwaltung.

Dies gilt derzeit nicht für die Katalogbereitstellung in Cloud-Services-Katalog. Für CSKkönnen standardmäßig alle Benutzer mit Rollenberechtigung auf die Kataloge zugreifen, sie anzeigen und sie bereitstellen.

Richtlinien und Berechtigungsebenen für Services

Konfigurieren Sie Richtlinien mit der erforderlichen Berechtigungsebene, um Zugriff auf die Services AWS, Azure, ADO, Ansible und Google Cloud zu gewähren.

- Cloud-Services-Katalog Sofort einsatzbereite AWS-Katalogberechtigungen
  - Amazon Web Services Sofort einsatzbereite EC2-Linux-Berechtigungen
  - AWS EC2 Windows OOB-Berechtigungen
  - AWS Dynamo DB-Berechtigungen
  - AWS S3-Bucket

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

- Azure OOB-Katalogberechtigungen
- Ansible-Berechtigungen
- ADO-Berechtigungen
- Cloud-Services-Katalog Sofort einsatzbereite Katalogberechtigungen für Google Cloud Platform
  - Google Cloud Platform (GCP) Out-of-Box-Berechtigungen für Big Query
  - Google Cloud Platform Out-of-Box-Berechtigungen für Cloud SQL
  - Google Cloud Platform Out-of-Box-Berechtigungen für Linux
  - Google Cloud Platform Standardmäßige Lastenausgleichsmodul-Berechtigungen
  - CSK GCP Windows OOB-Berechtigungen

Cloud-Services-Katalog verwenden

Die Anwendung Cloud-Services-Katalog ist ein dynamisches Portal für alle Ihre täglichen Cloud-Aktivitäten. Sie können damit Stapel verwalten, mit Anforderungen arbeiten und auf sofort einsatzbereite Katalogelemente und andere beliebte Themen zugreifen.

Sie können Cloud-Services erkunden, indem Sie eine Suche auf der Plattform Now Platform® durchführen. Sie finden dort auch zugehörige Links wie **Cloud-Katalog durchsuchen** und **CSC – Geführtes Setup**.

Cloud-Services werden auch in der Symbolleiste Mitarbeiter-Center als neue Registerkarte angezeigt. Suchen Sie nach den bereitgestellten Optionen, oder navigieren Sie zu **Cloud-Services durchsuchen,** um Cloud-Services-Katalogzu erfahren.

Die Anwendung Cloud-Services-Katalog zeigt die Funktionen in der folgenden Tabelle an.

Funktionen von Cloud Services

Funktion	Beschreibung
Meine Stapel	Listet alle Ihnen zugewiesenen Stapel auf. Wählen Sie ein Katalogelement aus, um die vom Element gestarteten Stapel anzeigen zu lassen. Wählen Sie einen Stapel aus, um Details wie alle Ressourcen, Ressourceneigenschaften, Aktivitäten und Lebenszyklusvorgänge anzuzeigen.
Themen für Cloud-Services	Stellt Quick-Links zu beliebten und relevanten Themen bereit.
Durchsuchen Sie Cloud-Services	Stellt die Suchfunktion bereit, die auf KI-Suchebasiert. Sie gibt relevante Cloud-Services zurück, stellt Filter bereit und sortiert Ergebnisse, mit denen Sie den gewünschten Cloud-Service vergrößern können. Diese Funktion ist getrennt von der globalen Suche auf der Zielseite Mitarbeiter-Center. 1. Verwenden Sie Filtern nach und Sortieren nach, um Ihre Suche einzugrenzen. 2. Sie können je nach Bedarf auch die Karten- oder Listenansicht verwenden.

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

Funktionen von Cloud Services (Fortsetzung)

Funktion	Beschreibung
	3. Wählen Sie eine der Quellen aus, um die Suchergebnisse zu filtern. **4.** Verwenden Sie einen Themenfilter, um die Ergebnisse einzugrenzen.
Letzte Stapel	Listet alle Stapel mit den letzten Aktivitäten auf, die dafür ausgeführt wurden.
Meine Ressourcen	Beobachtet die erkannten Ressourcen und interagiert mit ihnen.

Cloud-Services werden angefordert

Senden Sie eine Anforderung für eines der verfügbaren Servicekatalogelemente in Cloud-Services. Sie finden die Kataloge unter **Cloud-Services durchsuchen**.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Navigieren Sie auf der Seite des Mitarbeiterzentrale-Portals in Cloud-Services-Katalogzu **Cloud-Services durchsuchen** unter **Cloud-Services**.
2. Suchen Sie ein geeignetes Katalogelement aus den angezeigten Optionen.
3. Wählen Sie **Anforderung**aus.
   Dadurch wird das Anforderungsformular mit den bereitzustellenden Informationen und Anhängen geöffnet.
4. Geben Sie die Details in die zu bestellenden Formularfelder ein.
   Wenn Sie eine Anforderung für ein Element an den Servicekatalog übermitteln, stellt das System den Stapel in der Regel sofort bereit. Manchmal muss die Anforderung zuerst genehmigt werden.

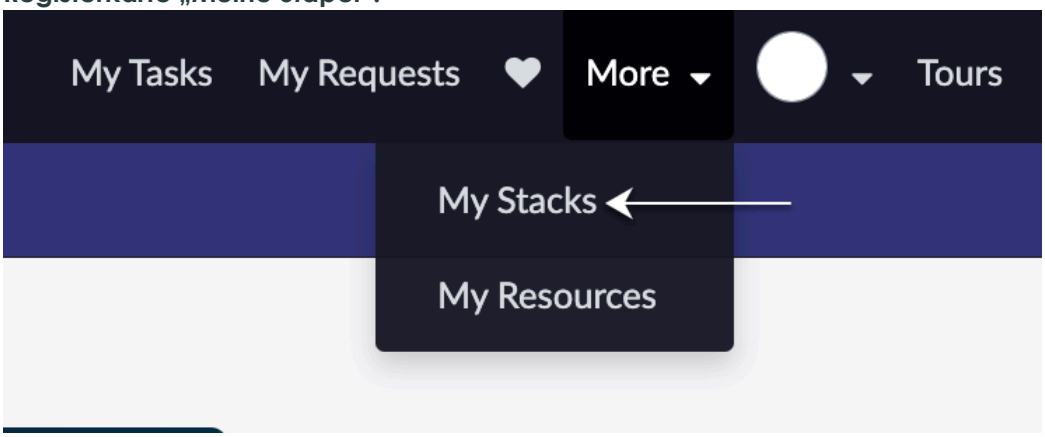
Erkunden Sie die Registerkarte „My Stacks“ (Meine Stapel).

Sortieren, Anzeigen oder Verwalten Ihres Stapels von Cloud-Ressourcen und Services im Rahmen der Tag-2-Aktivitäten mithilfe der Registerkarte **Meine Stapel** in der Symbolleiste Mitarbeiter-Center in Cloud-Services-Katalog.

Die Registerkarte „My Stacks“ **(Meine Stapel)** bietet mehrere Optionen, mit denen Sie Ihre Stapel kategorisieren, sortieren oder mit einem anderen verwalteten Status anzeigen können. Das folgende Beispiel zeigt, wie die Registerkarte **My Stacks (Meine** Stapel) auf Mitarbeiter-Centeraussieht.

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

Registerkarte „Meine Stapel“.



Auf der Registerkarte **„My Stacks“ (Meine Stapel**) werden die folgenden Status angezeigt:

- Verwaltete Stapel: Alle Stapel in allen Servicekategorien.
- Stapel nach Katalogelementen: Stapel, die nach dem Katalogelement aufgelistet sind.
- Stapel mit Problemen: Stapel mit Fehlern aufgrund unvollständiger oder nicht genehmigter Elemente.
- Stapel mit Folgeaktionen: Stapel, für die eine Folgeaktion aussteht.
- Erkannte Stapel (unverwaltet): Stapel, denen kein Katalog zugeordnet ist.

Suchen Sie die Registerkarte **„My Stacks“ (Meine Stapel**) am Ende des Menübands „My Stacks“ (Meine Stapel), um auf eine der folgenden Ansichten zuzugreifen:

- Stapel in meinem Besitz: Stapel, die Sie erstellt haben.
- Stapel im Besitz von Gruppen, denen ich angehöre: Stapel, die von Ihnen und allen Gruppen erstellt werden, denen Sie zugeordnet sind.
- Stapel im Besitz einer beliebigen Person: Alle Stapel in der Instanz.

Meine Stapel verwalten

Verwenden Sie die Registerkarte **„My Stacks“ (Meine Stapel**), um auf alle Stapeleigenschaften wie Erstellungs-, Aktualisierungs- und Löschdetails zuzugreifen.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Greifen Sie auf die Seite „Stapel“ zu, indem Sie zur Symbolleiste oder Homepage wechseln.

   - Wählen Sie in der Symbolleiste die Registerkarte **Meine Stapel**.
   - Wählen Sie auf der Homepage „My Stacks“ (Meine Stapel) die Registerkarte **Zuletzt verwendete Stapel** aus.

     Standardmäßig werden alle Stapel in allen Servicekategorien mit Ausnahme des Status Veraltet aufgelistet.

2. Verwenden Sie im Navigationsbereich eine Filterkategorie, um die übereinstimmenden Stapel anzuzeigen.
   Die Filter werden als bearbeitbare Bedingungen angezeigt.

Automatische Übersetzung

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

Ergebnisse
Die Stapel werden mit den Eigenschaften angezeigt, die in der folgenden Tabelle aufgeführt sind.

Stapeleigenschaften

Eigenschaftsname	Beschreibung
Name	Name, den Sie bei der Anforderung des Stapels angegeben haben.
Servicekatalogelement	Service, der erstellt wurde, als Sie den Katalog bestellt haben, der zu diesem Stapel geführt hat.
Stapelstatus	Status des Stapels: • Wird initialisiert • Aktiv (bereitgestellte Stapel) • Fehler • Wird verarbeitet (Stapel werden verarbeitet) • Wird beendet • Beendet (Stapel mit aufgehobener Bereitstellung) • Nicht verwaltet (erfasste Stapel) • Fehler wird behoben (Stapel mit Fehlern) • Nachverfolgung erforderlich • Veraltet
Eigentum von	Benutzername der anfordernden Person.
Besitzergruppe	Gruppenname, dem der Stapel zugewiesen ist.
Serviceanforderungselement	Datensatz, der in der Tabelle „Anforderungselement“ erstellt wurde, als Sie den Katalog bestellt haben, der zu diesem Stapel geführt hat.
Anforderung	Anforderungsnummer, die dem Anforderungselement zugeordnet ist.
Erstellt	Datum und Uhrzeit, zu der der Stapel angefordert wurde.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Stapeldetails.

Arbeiten Sie mit Stapeln

Starten Sie Ihre Tag-2-Vorgänge, indem Sie Ihre Stapel starten, anhalten, die Bereitstellung aufheben oder sie ändern.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_user.root_admin, admin oder sn_cmp.cloud_admin

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

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen Lebenszyklusvorgang für einen Stapel oder eine Ressource anfordern, wird vom System eine Change-Anforderung erzeugt. In einer Genehmigungsrichtlinie ist festgelegt, dass der Change entweder automatisch genehmigt wird oder dass ein Benutzer auf der Genehmigerliste den Change genehmigen muss. Weitere Informationen finden Sie unter .

Prozedur

1. Wählen Sie im Navigationsbereich im Feld **Name** einen Stapel aus, und wählen Sie dann **Vorgänge nachverfolgen**aus.
2. Zeigen Sie den Anforderungsstatus und den Status der Stapel an, indem Sie **Status**auswählen.
3. Zeigen Sie die Eigenschaften und Anforderungsparameter an, indem Sie **Anforderungsdetails**wählen.
   Sie können die Stapeldetails auch in einem Popup-Fenster anzeigen, indem Sie **Vollständige Details anzeigen**auswählen.
4. Suchen und sortieren Sie alle von Ihnen durchgeführten Vorgänge, indem Sie **Stapelvorgänge**auswählen.

Zeigen Sie die Stapelabhängigkeit an

Erkunden Sie die Details der Konfigurationselemente, Services und anderer Aufgaben, die den Stapeln und Ressourcen zugeordnet sind, indem Sie Abhängigkeit anzeigen verwenden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

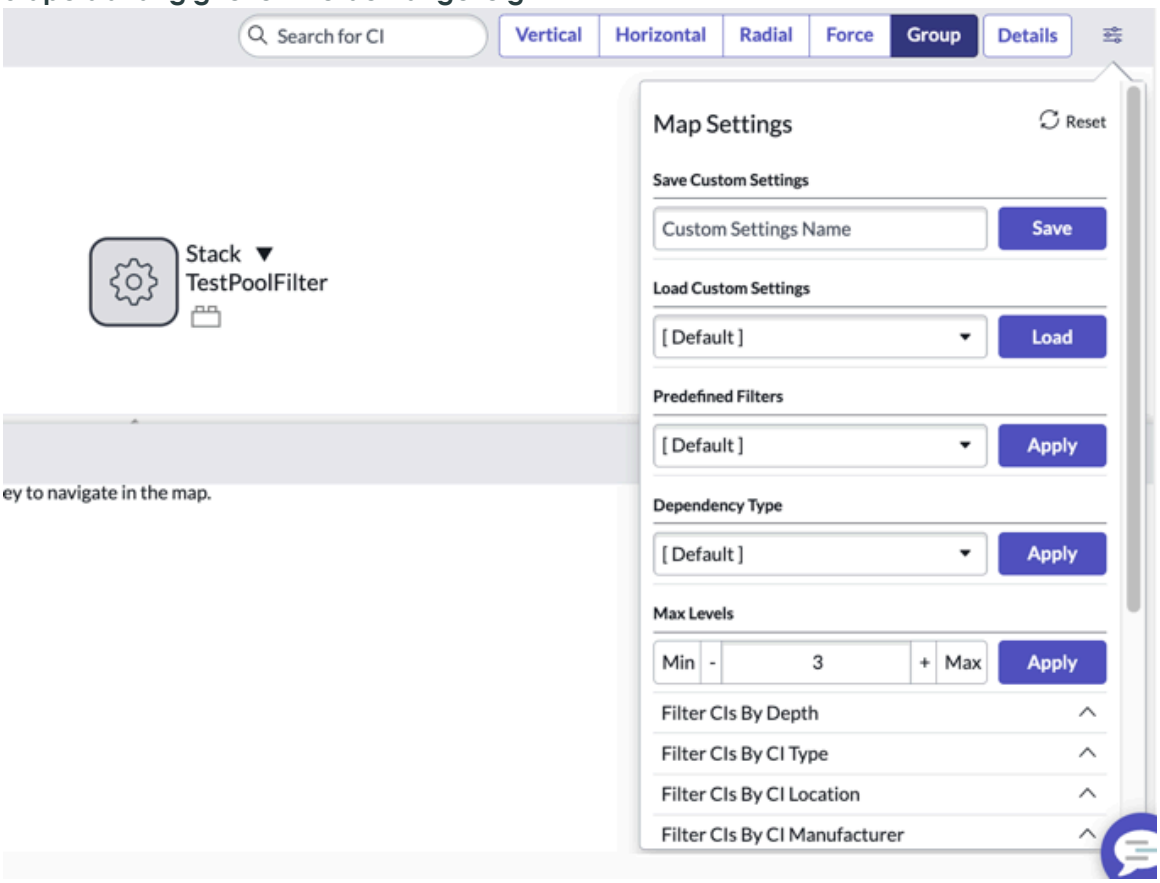
Ein Stapel kann von mehreren Stapeln abhängig sein, und mehrere Stapel können von einem einzelnen Stapel abhängen. Stapel, die mehrere Configuration Items (CIs) und Services enthalten, bilden die Stapelabhängigkeiten in der Anwendung Cloud-Services-Katalog. Die Abhängigkeitsübersicht bietet eine einfache und detaillierte grafische Darstellung dieser komplexen Einstellungen. Sie können durch die Referenzen navigieren, um die Auswirkungen des Ereignisses nachzuvollziehen, die eine Verzweigung auf eine andere hat.

Prozedur

1. Wählen Sie auf der Seite „Verwaltete Stapel“ einen Stapel aus, um die Seite mit den Stapelvorgängen zu öffnen.
2. Wählen Sie im Menüband Vollständige Details anzeigen die **Option Abhängigkeit anzeigen aus**.
3. Geben Sie im **Feld Nach CI suchen**ein CI ein, um die Abhängigkeitsübersicht anzuzeigen.
4. Füllen Sie die Felder des Formulars aus.
   Das folgende Beispiel zeigt die Einstellungen zum Anzeigen der Stapelabhängigkeiten. Die Einstellungen umfassen „Anwenderdefinierte Einstellungen speichern“, „Anwenderdefinierte Einstellungen laden“, „Vordefinierte Filter“, „Abhängigkeitstyp“ und „Maximale Ebenen“.

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

Stapelabhängigkeiten werden angezeigt



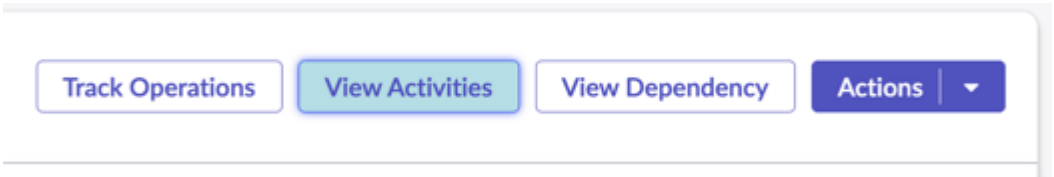
5. Machen Sie alle CI-Filterauswahlen rückgängig, und setzen Sie die Zuordnungseinstellung zurück, indem Sie **Zurücksetzen**wählen.

Ansicht „Stapelaktivitäten“.

Zeigen Sie die Cloud-Aktionen für Ihre Stapel und Ressourcen mithilfe der Registerkarte **Aktivitäten** anzeigen an.

Sie können im Stapellebenszyklus mehrere Aktionen ausführen, z. B. Vorgänge nachverfolgen, Aktivitäten anzeigen, Abhängigkeit anzeigen und Aktionen ausführen. Das folgende Beispiel zeigt die Stapelaktivitäten, die Sie ausführen können, und die folgende Tabelle beschreibt die Aktivitäten.

Stapelaktivitäten



Stapelaktivitäten

Aktivität	Beschreibung
Change-Anforderungen	Change-Anforderungen, die für Stapel oder Ressourcen eingereicht wurden, die Ihnen zugewiesen sind. Das System generiert Change-Anforderungen, wenn Sie

Automatische Übersetzung

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

Stapelaktivitäten (Fortsetzung)

Aktivität	Beschreibung
	Lebenszyklusvorgänge an einem Stapel oder einer Ressource durchführen.
Incidents	Incidents für Stapel und die zugehörigen Ressourcen, die Ihnen zugewiesen sind.
Aufgaben	Katalogaufgaben, die erstellt werden, wenn eine Anforderung für einen Stapel nicht bereitgestellt werden kann.
Geplante Vorgänge	Liste der geplanten Vorgänge, die Stapeln zugeordnet sind und als diese Funktionen angezeigt werden: • Betriebszeit • Ziel • Vorgang • Status

Aktionen für Stapel

Greifen Sie auf einen bestimmten Stapel zu, um Tag-2-Vorgänge oder Lebenszyklusvorgänge wie Stoppen, Starten, Deprovisionieren, ModifyLease oder ModifySchedule auszuführen.

Wenn Sie einen Lebenszyklusvorgang für einen Stapel oder eine Ressource anfordern, wird vom System eine Change-Anforderung erzeugt. Eine Genehmigungsrichtlinie gibt an, dass der Change automatisch genehmigt wird oder dass ein Benutzer auf der Genehmigerliste den Change genehmigen muss.

Stapel und Ressourcen durchlaufen Lebenszyklusvorgänge, beginnend mit dem Start, der Bereitstellung, der Aufhebung der Bereitstellung und dem Stoppen. Manchmal müssen Sie den Zeitplan einer bestimmten Ressource bei Konfigurationsproblemen aktualisieren oder anhalten. Sie können einen Stapel oder eine Ressource auswählen, um diese Vorgänge auszuführen. Die Aktionen umfassen nur die entsprechenden Vorgänge für die ausgewählte Ressource oder den ausgewählten Stapel. Nicht alle Vorgänge werden standardmäßig für alle Anbieter oder für alle Servicekategorien (Ressourcentypen) unterstützt.

Das folgende Beispiel zeigt die Aktionen, die die Anwendung Cloud-Services-Katalog für Stapel unterstützt. Die Aktionen sind stop, start, deprovision, ModifyLease oder ModifySchedule.

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

Aktionen für Stapel

In der folgenden Tabelle sind die Vorgänge aufgeführt, die die Anwendung Cloud-Services-Katalog als Aktionen für Stapel unterstützt.

Aktion	Funktion
Stoppen	Stoppt den ausgewählten virtuellen Computer (VM). Der Ressourcenstatus ändert sich in „Aus“. Keine Einstellung ist erforderlich.
Starten	Startet den ausgewählten VM. Der Ressourcenstatus ändert sich in in. Keine Einstellung ist erforderlich.
Aufheben der Bereitstellung	Beendet den ausgewählten Stapel und sendet eine Benachrichtigung an den Stapelbesitzer. Keine Einstellung erforderlich.
ModifyLease	Ändert das Enddatum der Miete.
ModifySchedule	Ändert das Zeitplanprofil und die Zeitplanzeitzone.

Umleitung zu „Meine Stapel“

Sie können die Umleitung zur Registerkarte **„My Stacks** “ (Meine Stapel) als alternative, aber vereinfachte Methode verwenden, um einen Stapel über die Registerkarte **„My Requests“ (Meine Anforderungen)** zu finden. Sie können beispielsweise die Umleitung verwenden, während Sie nach einem Stapel suchen, der kürzlich bereitgestellt wurde.

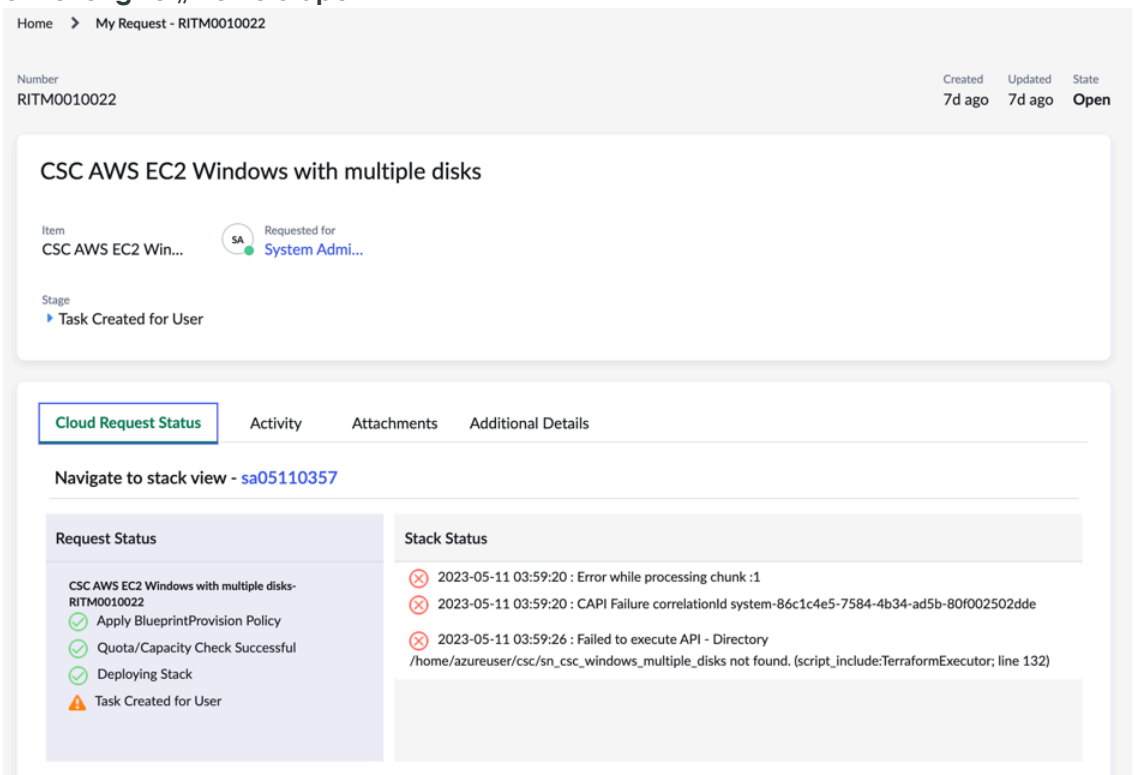
Sie können alle Ihre Stapel mit jedem relevanten Status anzeigen, die angezeigte Liste kann jedoch lang sein.

Durch die Weiterleitung zu den Stapeldetails über die Registerkarte „My Requests“ (**Meine Anforderungen**) in Mitarbeiter-Center können Sie den angeforderten Stapel anhand des angeforderten Elements (RITM) finden. Verwenden Sie die Registerkarte **Cloud-Anforderungsstatus** in der Anwendung Cloud-Services-Katalog, um die Anforderungsdetails und den Status der Stapel anzuzeigen.

Das folgende Beispiel zeigt, wie Sie von der Registerkarte **„My** Requests“ **(Meine Anforderungen**) zur Registerkarte „My Stacks“ (Meine Stapel) umleiten können, anstatt auf der Homepage „Stapel“ eine umfassende Liste von Stapeln anzuzeigen.

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

Umleitung zu „Meine Stapel“



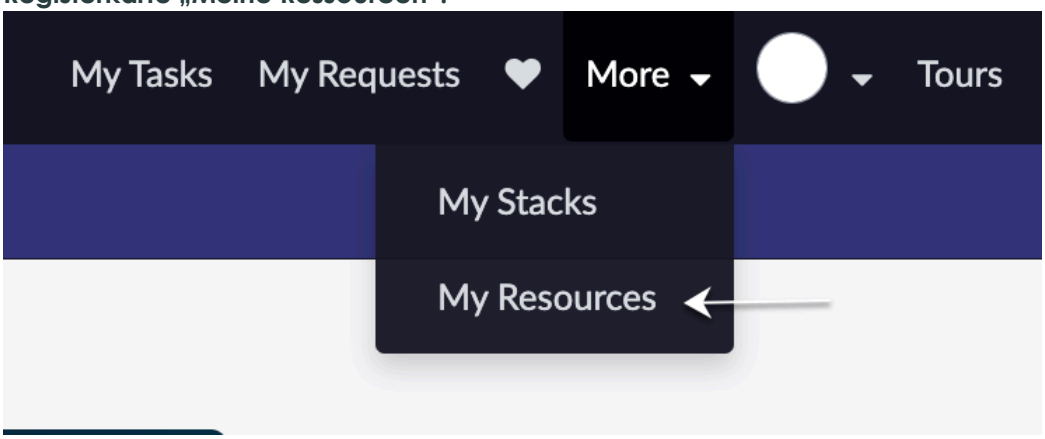
Meine Ressourcen erkunden

Über die Option **Meine Ressourcen** auf der Registerkarte **Mehr**in der Symbolleiste Mitarbeiter-Center können Sie erkannte Ressourcen beobachten und mit ihnen interagieren.

Sie können die Operatoren oder Besitzer für die identifizierten Ressourcen bestimmen, damit sie diese Ressourcen mit standardmäßigen Tag-2-Vorgängen handhaben können. Indem Sie diese Aktionen über Now Platform der Anwendung Cloud-Services-Katalog ausführen, können Sie die Workflows für ordnungsgemäßes Change-Management, Audit-Trails und allgemeine Governance nutzen.

Das folgende Beispiel zeigt die Registerkarte **Meine Ressourcen**.

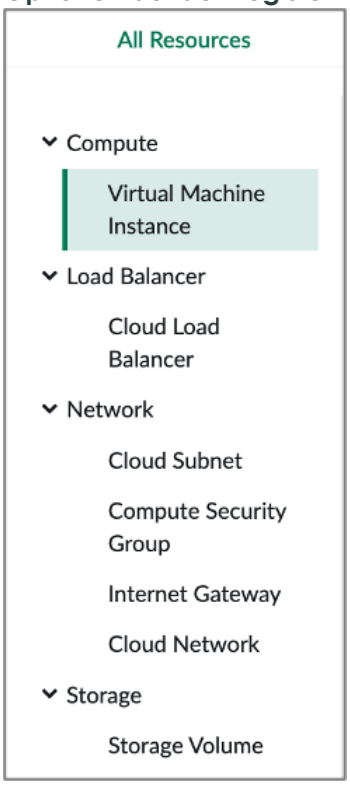
Registerkarte „Meine Ressourcen“.



Das folgende Beispiel zeigt eine Liste der Ressourcenkategorien und Filter, mit denen Sie auf die relevante Ressource zugreifen und andere Funktionen ausführen können, z. B. Speichern und Exportieren.

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

Optionen auf der Registerkarte Alle Ressourcen



Die Cloud-Ressourcen sind wie oben kategorisiert. Sie können auf eine der Kategorien zugreifen, um sie zu verwalten.

Verwalten Sie „Meine Ressourcen“ und Ressourcenfilter

Greifen Sie mit dem Ressourcenfilter auf Ihre eigenen Ressourcen, Ressourcen im Besitz einer Gruppe oder die Ressourcen beliebiger Personen zu. Sie können dann die benötigten Informationen mithilfe von Sortierfunktionen, Bedingungen, Kategorien und Stichwörtern finden.

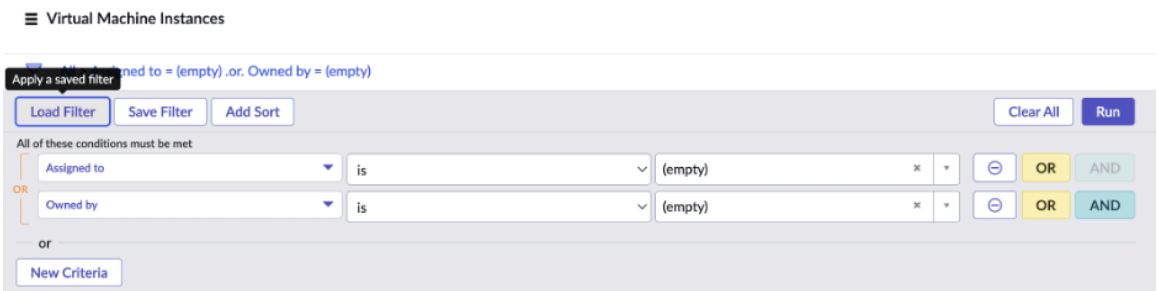
Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

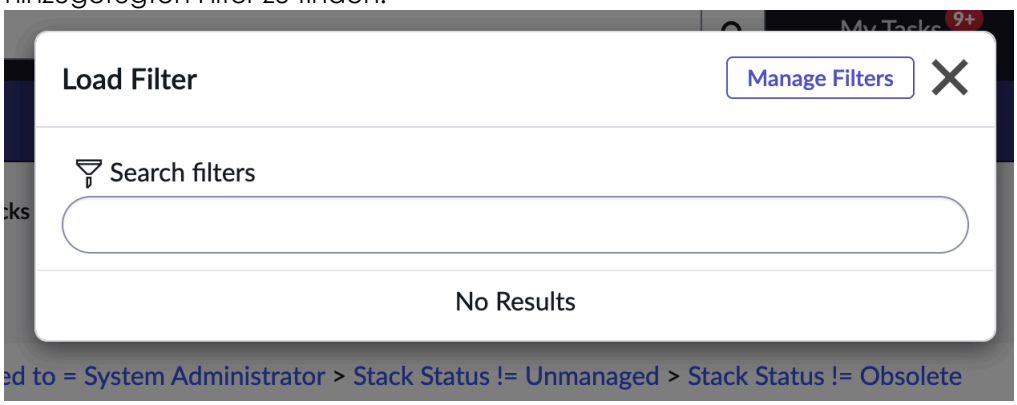
1. Wählen Sie im Navigationsbereich die Ressourcenkategorie aus, wenden Sie einen Filter (bereits hinzugefügt oder neu) an, und wählen Sie **Ausführen**, um eine Reihe von Ressourcen anzuzeigen und zu exportieren.
2. Sortieren Sie, zeigen Sie die Details an, und exportieren Sie sie nach Bedarf.

Filteroptionen für Ressourcen

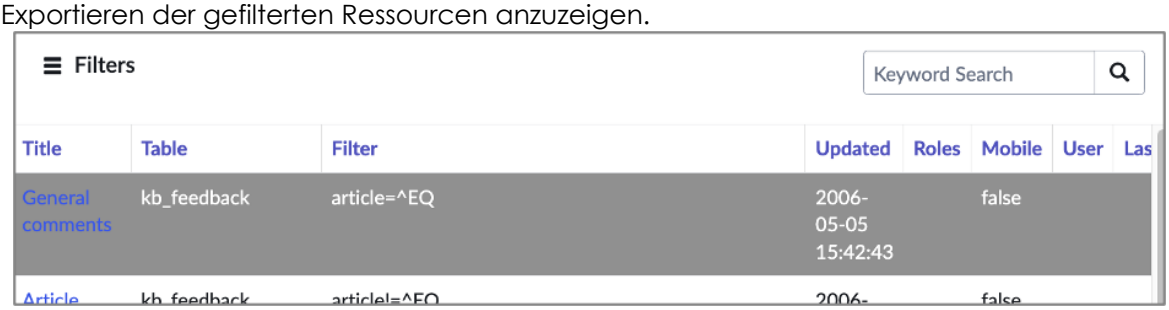


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

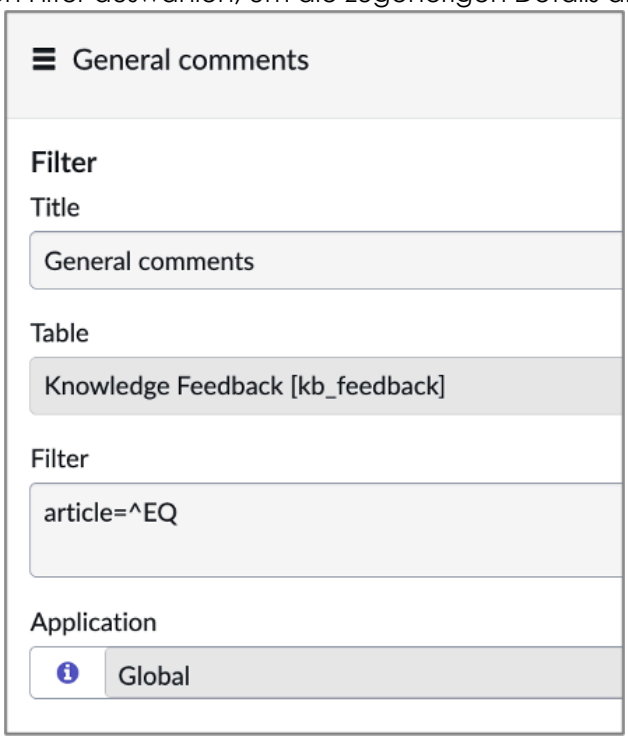
3. Wenden Sie einen vorhandenen oder einen gespeicherten Filter an, indem Sie **Filter laden**auswählen.
4. Wählen Sie im Fenster „Filter laden“ **die Option Filter verwalten aus**, um die Liste der zuvor hinzugefügten Filter zu finden.



5. Wählen Sie die Menüoption neben **Filter** aus, um die verschiedenen Optionen zum Exportieren der gefilterten Ressourcen anzuzeigen.

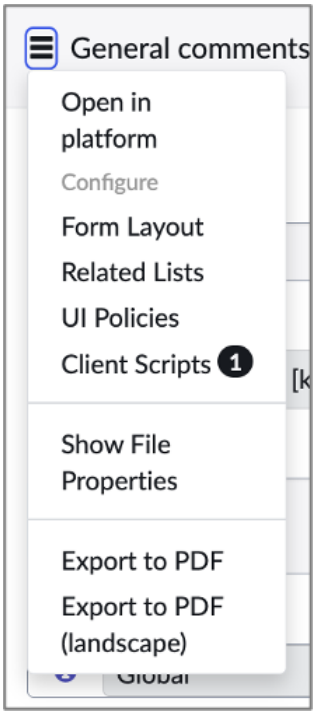


6. Sie können auch einen Filter auswählen, um die zugehörigen Details anzuzeigen.



7. Zeigen Sie weitere Optionen und Details zu dem von Ihnen ausgewählten Filter an, indem Sie die Menüoption neben Allgemeine Kommentare auswählen.

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



Sie können die Stichwortsuche verwenden, um einen Filter direkt anhand von Stichwörtern zu finden. Sie können Exportoptionen wie PDF, Excel oder CSV wählen.

8. Erstellen und fügen Sie einen oder mehrere Bedingungssätze hinzu, indem Sie zu navigieren **Neues Kriterium** > **Einen weiteren Satz Bedingungen erstellen**.
9. Speichern Sie den erstellten Filter, indem Sie **Filter speichern**wählen.
10. Weisen Sie in den Feldern Name, Abfrage und Sichtbarkeit den Namen, die Abfrage und die Sichtbarkeit zu.
    Sie können auch Sortieroptionen hinzufügen, indem Sie **Sortierung hinzufügen**wählen.
11. Weisen Sie eine Sortierreihenfolge aus der Liste zu, und wählen Sie **Speichern**aus.
12. Wählen Sie in den Ansichtsoptionen eine der folgenden Optionen aus:
    - Eigene Ressourcen: Diese Option ist standardmäßig ausgewählt
    - Ressourcen im Besitz von Gruppen, denen ich angehöre: Mit dieser Option werden alle Gruppen angezeigt, denen Sie angehören.
    - Ressourcen im Besitz von beliebiger Person: Diese Option zeigt alle Ressourcen in der ausgewählten Kategorie in Configuration Management Database (CMDB)und zugewiesen an.

Standardkataloge mit Cloud-Services-Katalog

Cloud-Services-Katalog verfügt über vordefinierte Katalogelemente, Aktionen und Richtlinien, die Sie nach Bedarf rendern können.

Verwenden Sie vordefinierte Katalogelemente für Azure-, GCP - und Amazon Web Services -Cloud-Service-Anforderungen und -Automatisierungen. Sie können entweder eines der Katalogelemente bestellen oder Flow Designer-basierte Aktionen verwenden oder Richtlinien bereitstellen.

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

Hinweis: Verwenden Sie die Katalogelemente unverändert, und ändern oder aktualisieren Sie sie nicht. Vorgenommene Änderungen oder Anpassungen ändern das Standardverhalten des Katalogs und liefern nicht die erwarteten Ergebnisse. Dies wirkt sich auch auf ihre Upgrades aus. Sie können eine Kopie der Vorlagen erstellen und Ihre Katalogelemente unter Berücksichtigung des vordefinierten Inhalts neu erstellen.

Bestellen Sie aus diesen Cloud-Services-Katalog Out-of-Box-Katalogelementen:

Amazon Web Services Vordefinierte EC2 Linux-Katalogelemente

Cloud-Services-Katalog Linux-VM mit Agent Client Collector (ACC), bis zu 10 zusätzlichen Datenträgern auf EC2 oder mit Sicherheitsgruppen.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Linux-Instanz eines beliebigen Instanztyps von Amazon EC2 angefordert werden kann.

Bestellung einer AWS EC2 Linux-VM Das Video zeigt, wie Sie eine virtuelle Amazon Web Services EC2 Linux-Maschine bestellen.

Reihenfolgen und Funktionen von Linux-VMs:

Auftrag	Funktionen
Bestellen Sie einen virtuellen Linux-Computer auf EC2, der die Installation von Agent Client Collector unterstützt. ACC ist für Produktionsinstanzen obligatorisch. Für andere VM-Größen als t2.nano und t2.micro ist eine Genehmigung erforderlich. Zur Compliance-Überprüfung wird ein Cloud-Konfigurationsscan ausgeführt.	Für andere Instanztypen als t2.nano und t2.micro ist die Genehmigung durch den Administrator gemäß Richtlinie erforderlich. Das Katalogelement verfügt über integrierte Client-Regeln, um eine ACC-Installation (Agent Client Collector) zu steuern, wenn die Bereitstellungsumgebung für die Produktion markiert ist. Zur Auswahl des Aliasschlüssels für Anmeldeinformationen für die ACC-Bereitstellung ab MID müssen dem Benutzer die entsprechenden Berechtigungen für die ACC-Administratorrolle gewährt werden. Informationen zu den Voraussetzungen finden Sie unten unter „ACC-* in Post-Bereitstellung bereitstellen“. Die Workflow-Automatisierung führt einen CCG-Scan für die bereitgestellte Linux-Instanz aus und überprüft die Richtlinienregel mit der Konfiguration der VM. Bei einem Verstoß wird der Stapel auf den Status „Nachverfolgung erforderlich“ gesetzt, um zu melden, dass die Stapelbereitstellung nicht den Normen entspricht.
Bestellen Sie einen virtuellen Linux-Computer auf EC2, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu 2 Datenträger ist keine Genehmigung erforderlich. Für alles, was darüber hinausgeht, ist eine Genehmigung einzuholen.	Dieses Katalogelementformular ermöglicht das Bestellen von bis zu 10 zusätzlichen Datenträgern (Volumes) unterschiedlicher Größe und Art, die an die VM angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, holen Sie gemäß Richtlinie die Genehmigung des Administrators ein.

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

Auftrag	Funktionen
Bestellen Sie einen sicheren virtuellen Linux-Computer mit erhöhter Sicherheit, indem Sie eine Netzwerk-Sicherheitsgruppe zuweisen, um die höchste Sicherheitsstufe zu gewährleisten.	Mit diesem Katalogelementformular kann der Compute-Instanz eine Netzwerksicherheitsgruppe zugewiesen werden, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und die ausgewählten Subnetze aufgelistet.

Hinweis:

Tag (Schlüssel-Wert) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden.

Der Schlüsselwert wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der Public Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Amazon Web Services Sofort einsatzbereite EC2-Linux-Berechtigungen

Amazon Web Services EC2 Linux OOB-Katalogelementberechtigungen

Katalogelement	Services	Berechtigungen
CSK AWS EC2 Linux-VM	AWS EC2-Bereitstellung	**1.** DescribeVolumes **2.** DescribeImages **3.** DescribeInstances **4.** DescribeVolumes **5.** DescribeInstanceCreditSpecifications **6.** DescribeInstanceAttribute **7.** DescribeInstances **8.** DescribeTags **9.** DescribeInstanceTypes **10.** DescribeInstances **11.** DescribeVpcs **12.** RunInstances **13.** DescribeImages **14.** GetCallerIdentity
	AWS EC2-Instanz: stoppen	**1.** DescribeInstances **2.** StopInstances
	AWS EC2-Instanz: Start	**1.** DescribeImages **2.** DescribeInstances **3.** Startinstanzen

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

Katalogelement	Services	Berechtigungen
	AWS EC2-Instanz: Bereitstellung der VM aufheben **Hinweis:** Dadurch wird auch die Bereitstellung des Speichervolumes aufgehoben.	**1.** DescribeAddresses **2.** TerminateInstances
	AWS EC2-Instanz: Deprovisionierungsstapel **Hinweis:** Beendet alles, einschließlich NIC.	**1.** GetCallerIdentity **2.** DescribeInstances **3.** DescribeImages
CSK AWS EC2 Linux mit mehreren Datenträgern	AWS EC2 Linux-Bereitstellung mit mehreren Datenträgern	**1.** DescribeVolumes **2.** DescribeImages **3.** DescribeInstances **4.** AttachVolume **5.** DescribeInstances **6.** CreateVolume **7.** DescribeInstanceCreditSpecifications **8.** DescribeInstanceAttribute DescribeVPCS **9.** DescribeInstanceTypes **10.** DescribeTags-Ausführungsinstanzen **11.** GetCallerIdentity
	AWS EC2 Linux mit mehreren Datenträgern anhalten	**1.** DescribeInstances **2.** StopInstances
	AWS EC2 Linux mit mehreren Datenträgern wird gestartet	**1.** DescribeImages **2.** DescribeInstances **3.** Startinstanzen
	AWS EC2 Linux-Aufhebung der Stapelbereitstellung für mehrere Datenträger – beendet alle Ressourcen	**1.** DescribeInstances **2.** TerminateInstances **3.** ModifyInstanceAttribute **4.** DescribeVolumes **5.** Volume löschen

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

Katalogelement	Services	Berechtigungen
		6. GetCallerIdentity **7.** DetachVolume **8.** DescribeInstanceCreditSpecifications **9.** DescribeVpcs **10.** DescribeInstanceTypes **11.** DescribeTags **12.** DescribeImages
CSK AWS EC2 Linux mit Sicherheitsgruppen	AWS EC2 Linux mit Sicherheitsgruppen – Bereitstellung	**1.** DescribeVolumes **2.** DescribeImages **3.** DescribeInstances **4.** DescribeInstanceCreditSpecifications **5.** DescribeInstanceAttribute **6.** DescribeVolumes **7.** DescribeTags **8.** DescribeVpcs **9.** DescribeInstanceTypes **10.** RunInstances **11.** GetCallerIdentity
	AWS EC2 Linux mit Sicherheitsgruppen anhalten	**1.** DescribeInstances **2.** StopInstances
	AWS EC2 Linux mit Sicherheitsgruppen starten	**1.** DescribeInstances **2.** DescribeImages **3.** Startinstanzen
	AWS EC2 Linux mit Sicherheitsgruppen – Stapelaufhebung, bei der alle Ressourcen beendet werden	**1.** DescribeInstances **2.** TerminateInstances **3.** ModifyInstanceAttribute **4.** GetCallerIdentity **5.** DescribeInstanceCreditSpecifications **6.** DescribeInstanceAttribute **7.** DescribeVolumes **8.** DescribeTags **9.** DescribeInstanceTypes

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

Katalogelement	Services	Berechtigungen
		10. DescribeVpcs **11.** DescribeImages

Amazon Web Services EC2: vordefinierte Microsoft Windows-Katalogelemente

Cloud-Services-Katalog Windows-VM, bis zu 10 zusätzliche Datenträger auf EC2 oder mit Sicherheitsgruppen.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Windows-Instanz eines beliebigen Instanztyps von Amazon EC2 angefordert werden kann. Diese obligatorischen Schritte sind für die Bereitstellung erforderlich:

1. Fügen Sie im Feld Terraform die PEM-Datei des privaten Schlüssels hinzu, die für die Bereitstellung verwendet wird.
2. Kopieren Sie den Pfad der PEM-Datei aus dem Feld Terraform, und aktualisieren Sie diesen Pfad im Standardwert der Schlüsselpfad-Variablen für Management.

Auftrag	Funktionen
Bestellen Sie einen virtuellen Microsoft Windows-Computer auf EC2. Zur Compliance-Überprüfung wird ein Cloud-Konfigurationsscan ausgeführt.	Für andere Instanztypen als t2.nano und t2.micro ist die Genehmigung durch den Administrator gemäß Richtlinie erforderlich. Die Workflow-Automatisierung führt einen CCG-Scan für die bereitgestellte Linux-Instanz aus und überprüft die Richtlinienregel mit der Konfiguration der VM.
Bestellen Sie einen virtuellen Windows-Computer auf EC2, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu zwei Datenträger ist keine Genehmigung erforderlich; bei mehr als 2 Datenträgern ist eine Genehmigung jedoch erforderlich.	Dieses Katalogelementformular ermöglicht das Bestellen von bis zu 10 zusätzlichen Datenträgern (Volumes) unterschiedlicher Größe und Art, die an die VM angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, holen Sie gemäß Richtlinie die Genehmigung des Administrators ein.
Bestellen Sie einen sicheren virtuellen Windows-Computer auf EC2, und weisen Sie Sicherheitsgruppen zu. Wählen Sie so viele aus, wie für die höchste Sicherheitsstufe erforderlich sind.	Mit diesem Katalogelementformular können Sie der Compute-Instanz eine oder mehrere Sicherheitsgruppen (Firewall-Port-Regeln) zuweisen, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und die ausgewählten Subnetze aufgelistet.

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

Hinweis:

Tag (Schlüssel-Wert) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden. Der Schlüsselwert wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der Public Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Der Bereitstellungs-Workflow benachrichtigt die anfordernde Person per E-Mail über das Windows-Administratorpasswort. Es kann mindestens vier Minuten dauern, bis Sie das Windows-Administratorpasswort von Amazon Web Serviceserhalten.

Amazon Web Services Sofort einsatzbereite EC2-Windows-Berechtigungen

Amazon Web Services EC2 Windows OOB-Katalogelementberechtigungen

Katalogelement	Services	Berechtigungen
CSK AWS EC2 Microsoft Windows-VM	AWS EC2-Bereitstellung	**1.** Passwortdaten abrufen **2.** DescribeInstanceCreditSpecifications **3.** DescribeInstanceAttribute **4.** DescribeInstances **5.** DescribeTags **6.** DescribeInstanceTypes **7.** DescribeVolumes **8.** DescribeVpcs **9.** RunInstances **10.** GetCallerIdentity **11.** DescribeImages
	AWS EC2-Instanz: stoppen	**1.** DescribeInstances **2.** StopInstances
	AWS EC2-Instanz: Start	**1.** DescribeImages **2.** DescribeInstances **3.** Startinstanzen
	AWS EC2-Instanz: Aufhebung der Bereitstellung	**1.** DescribeInstances **2.** GetCallerIdentity **3.** ModifyInstanceAttribute **4.** TerminateInstances **5.** Passwortdaten abrufen **6.** DescribeInstanceAttribute **7.** DescribeInstanceCreditSpecifications **8.** DescribeImages

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

Katalogelement	Services	Berechtigungen
		9. DescribeTags **10.** DescribeVolumes **11.** DescribeInstanceTypes **12.** DescribeVpcs
CSK CSC AWS EC2 Windows mit mehreren Datenträgern	AWS EC2 Windows-Bereitstellung mit mehreren Datenträgern	**1.** DescribeVolumes **2.** DescribeVolumes **3.** AttachVolume **4.** DescribeInstances **5.** Passwortdaten abrufen **6.** CreateVolume **7.** DescribeInstanceAttribute **8.** DescribeInstanceCreditSpecifications **9.** DescribeTags **10.** DescribeVpcs **11.** DescribeInstanceTypes **12.** RunInstances **13.** DescribeImages **14.** GetCallerIdentity
	Amazon Web Services EC2 Windows hält mehrere Datenträger an	**1.** DescribeInstances **2.** StopInstances
	AWS EC2 Windows-Start mit mehreren Datenträgern	**1.** DescribeImages **2.** DescribeInstances **3.** Startinstanzen
	AWS EC2 Windows-Aufhebung der Bereitstellung mehrerer Datenträger	**1.** DescribeInstances **2.** TerminateInstances **3.** ModifyInstanceAttribute **4.** DescribeVolumes **5.** Volume löschen **6.** DetachVolume **7.** GetCallerIdentity **8.** DescribeVpcs **9.** DescribeInstanceAttribute **10.** DescribeInstanceTypes

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

Katalogelement	Services	Berechtigungen
		11. DescribeTags 12. DescribeInstanceCreditSpecifications 13. Passwortdaten abrufen 14. DescribeImages
CSK AWS EC2 Windows mit Sicherheitsgruppen	AWS EC2 Windows mit Sicherheitsgruppen – Bereitstellung	1. Passwortdaten abrufen 2. DescribeVolumes 3. DescribeInstanceAttribute 4. DescribeInstance 5. DescribeInstanceTypes 6. DescribeVpcs 7. DescribeTags 8. DescribeInstanceCreditSpecifications 9. RunInstances 10. GetCallerIdentity 11. DescribeImages
	AWS EC2 Windows mit Sicherheitsgruppen anhalten	1. DescribeInstances 2. StopInstances
	AWS EC2 Windows mit Sicherheitsgruppen wird gestartet	1. DescribeInstances 2. DescribeImages 3. Startinstanzen
	AWS EC2 Windows mit aufgehobener Bereitstellung von Sicherheitsgruppen	1. DescribeInstances 2. TerminateInstances ModifyInstanceAttribute 3. GetCallerIdentity 4. DescribeInstanceAttribute 5. DescribeInstanceCreditSpecifications 6. DescribeVpcs 7. DescribeVolumes 8. DescribeTags 9. Passwortdaten abrufen 10. DescribeImages 11. DescribeInstanceTypes

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

Amazon Web Services Vordefinierte DynamoDB-Katalogelemente

Cloud-Services-Katalog AWS DynamoDB-Tabelle für hoch skalierbare NoSQL-Datenbank.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, das zum Bestellen einer Dynamo DB-Tabelle verwendet werden kann – einer Name-Wert-Datenbanktabelle in der Cloud Amazon Web Services oder AWS. Die anzugebenden Standardeingaben sind der Tabellenname, der Partitionsschlüssel und die Namen des Sortierschlüssels. Die Details der Dynamo-DB werden in den zurückgegebenen Stapeldetails angezeigt.

Bestellen Sie eine AWS DynamoDB-Tabelle, die ein Schlüssel-Wert-Speicher ist, mit Primärschlüsseln und Sekundärindizes. Dies ist nützlich für Entwickler, die eine hoch skalierbare und vollständig verwaltete NoSQL-Datenbank benötigen.

Amazon Web Services Out-of-Box-Berechtigungen für DynamoDB

Amazon Web Services Berechtigungen für DynamoDB OOB-Katalogelemente. DynamoDB unterstützt nur die Bereitstellung und Aufhebung der Bereitstellung.

Katalogelement	Services	Berechtigungen
Cloud-Services-Katalog AWS DynamoDB	AWS DynamoDB-Bereitstellung	**1.** DescribeTimeToLive **2.** DescribeTable **3.** Beschreiben SieKontinuierliche Sicherungen **4.** RessourcenListeTagsRessource **5.** UpdateTimeToLive **6.** Aktualisieren SieKontinuierliche Sicherungen **7.** GetCallerIdentity **8.** CreateTable **9.** GetCallerIdentity
	AWS Aufhebung der DynamoDB-Bereitstellung	**1.** DescribeTable **2.** DeleteTable **3.** GetAnruferIdentität **4.** RessourcenListeTagsRessource **5.** Beschreiben SieKontinuierliche Sicherungen **6.** DescribeTimeToLive **7.** DescribeTable

Amazon Web Services Vordefinierte S3-Bucket-Katalogelemente

Cloud-Services-Katalog AWS S3-Bucket mit sicherem Zugriff und Verschlüsselung.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, das zum Bestellen eines Objektspeicher-Buckets beim S3-Service der Amazon-Cloud verwendet werden kann. Der Bucket-Name wird validiert, um sicherzustellen, dass die S3-Benennungsrichtlinie eingehalten

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

wird. Die zugrunde liegende Terraform-Vorlage wird verwendet, um den öffentlichen Zugriff auf den Bucket zu verhindern und die Standardverschlüsselung für Daten einzurichten.

Bestellen Sie einen AWS S3-Speicher-Bucket, der Sicherheitsmaßnahmen wie die Verhinderung des öffentlichen Zugriffs und die serverseitige Verschlüsselung mit von Amazon S3 verwalteten Schlüsseln (SSE-S3) umfasst. Diese Sicherheitsfunktionen stellen sicher, dass die im Bucket gespeicherten Daten geschützt und sicher sind.

Amazon Web Services Sofort einsatzbereite S3-Bucket-Berechtigungen

AWS Berechtigungen für OOB-Katalogelemente für S3-Bucket. S3 Bucket unterstützt nur die Bereitstellung und Aufhebung der Bereitstellung.

Katalogelement	Services	Berechtigungen
CSK AWS S3-Bucket	AWS S3-Bucket-Bereitstellung	**1.** GetBucketPolicy **2.** BucketPublicAccessBlock setzen **3.** GetBucketLifecycle **4.** GetBucketReplication **5.** BucketTagging abrufen **6.** CreateBucket **7.** GetBucketLogging **8.** BucketÖffentlichenZugriffsblock abrufen **9.** GetBucketRequestPayment **10.** GetBucketAcl **11.** GetBucketWebsite **12.** GetAccelerateConfiguration **13.** GetBucketVersioning **14.** GetBucketEncryption **15.** GetBucketCors **16.** BucketObjectLockConfiguration abrufen **17.** BucketEncryption **18.** GetCallerIdentity
	AWS S3-Bucket-Bereitstellung aufheben	**1.** DeleteBucketEncryption **2.** DeleteBucketPublicAccessBlock **3.** DeleteBucket **4.** BucketObjectLockConfiguration abrufen **5.** GetBucketLifecycle **6.** GetBucketEncryption **7.** GetBucketReplication DescribeTable

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

Google Cloud Platform (GCP) Große Abfrage

Cloud-Services-Katalog mit Google Cloud Platform BigQuery Serverless Data Warehouse.

BigQuery Serverless Data Warehouse ist ein voll funktionsfähiges Beispielkatalogelement, das den Prozess der Bestellung einer auf BigQuery basierenden Data Warehouse-Lösung beim Google Cloud-Anbieter optimiert.

Auftrag	Funktionen
Bestellen Sie ein serverloses, kosteneffektives Multi-Cloud-Data Warehouse mit BigQuery für das Echtzeit-Streaming von Daten mit integriertem maschinellen Lernen, und geben Sie Analytics mit nur wenigen Klicks frei.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, das den Prozess der Bestellung einer serverlosen, kosteneffektiven Multi-Cloud-Data Warehouse-Lösung basierend auf BigQuery vom Google Cloud-Anbieter optimiert. Mit wenigen Klicks können Sie Echtzeit-Daten-Streaming und die Freigabe von Analysen einrichten. Die serverlose Architektur von BigQuery ermöglicht die SQL-basierte Datenanalyse und bietet Anpassungsoptionen für die Skalierbarkeit.

Google Cloud Platform (GCP) Out-of-Box-Berechtigungen für Big Query

Berechtigungen für vordefinierte GCP Big Query-Katalogelemente

GCP-Berechtigungen

Katalogelement	Services	Berechtigung
CSK GCP BigQuery	Bereitstellung	• Bigquery.datasets.create • Bigquery.tables.create • Speicher.Objekte.Abrufen
	Punkt-Discovery	• Bigquery.tables.list • Bigquery.datasets.get
	Aufheben der Bereitstellung	• Bigquery.tables.delete • Bigquery.datasets.delete • Bigquery.Routinen.Löschen • Bigquery.models.delete

Google Cloud Platform Cloud SQL

Cloud-Services-Katalog mit GCP Cloud SQL Database.

Die Cloud SQL-Datenbank ist ein Beispielkatalogelement, mit dem Sie eine Cloud SQL-Datenbanklösung bestellen können.

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

Auftrag	Funktionen
Bestellen Sie eine Cloud SQL-Datenbanklösung, die sich in Google Cloud-Services integrieren lässt.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, das zum Bestellen einer Cloud SQL-Datenbanklösung verwendet werden kann, die sich in Google Cloud-Services integrieren lässt, um innerhalb weniger Minuten Ihre erste skalierbare Datenbank zu erstellen und eine Verbindung damit herzustellen. Nach Abschluss werden in den Stapeldetails umfassende Details zur Cloud SQL-Konfiguration bereitgestellt. Sie automatisiert wichtige Funktionen wie Sicherungen, Replikation, Patchen, Verschlüsselung und Anpassungen der Speicherkapazität und stellt sicher, dass Anwendungen von verbesserter Zuverlässigkeit, Skalierbarkeit und verbesserten Sicherheitsmaßnahmen profitieren.

Google Cloud Platform Out-of-Box-Berechtigungen für Cloud SQL

Google Cloud Platform Cloud SQL: Berechtigungen für vordefinierte Katalogelemente

GCP-Berechtigungen

Katalogelement	Services	Berechtigung
CSK GCP Cloud SQL	Bereitstellung	• cloudql.instances.create • cloudsql.instances.get • cloudql.users.delete
	Punkt-Discovery	• cloudsql.databases.list • cloudsql.instances.list • cloudql.users.list • compute.regions.list • „compute.zones.list“
	Aufheben der Bereitstellung	cloudsql.instances.delete

Google Cloud Platform Vordefinierte Linux-Katalogelemente

Cloud-Services-Katalog Linux-VM mit Agent Client Collector (ACC), bis zu 10 zusätzlichen Datenträgern oder sicherer Linux-Bereitstellung.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Linux-Instanz eines beliebigen Instanztyps von Google Cloud Platform angefordert werden kann.

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

Reihenfolgen und Funktionen von Linux-VMs:

Auftrag	Funktionen
CSK GCP Linux-VM: Bestellen Sie eine virtuelle Linux-Maschine, die die Installation von Agent Client Collector unterstützt. ACC ist für Produktionsinstanzen obligatorisch. Für andere VM-Größen als e2-micro und e2-small ist eine Genehmigung erforderlich.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Linux-Instanz eines beliebigen Instanztyps vom Google Cloud-Anbieter angefordert werden kann. Für andere Instanztypen als e2-micro und e2-small ist die Genehmigung durch den Administrator gemäß Richtlinie erforderlich. Das Katalogelement verfügt über integrierte Client-Regeln für die Steuerung einer ACC-Installation (Agent Client Collector), wenn die Bereitstellungsumgebung für die Produktion markiert ist. Um den Aliasschlüssel für Anmeldeinformationen für die ACC-Bereitstellung ab MID auszuwählen, müssen dem Benutzer die entsprechenden Berechtigungen für die ACC-Administratorrolle gewährt werden.
CSK GCP Mehrere Linux-Datenträger: Bestellen Sie einen virtuellen Linux-Computer, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu zwei Datenträger ist keine Genehmigung erforderlich; bei mehr als 2 Datenträgern ist eine Genehmigung jedoch erforderlich.	Dieses Katalogelementformular ermöglicht das Bestellen von bis zu 10 zusätzlichen Datenträgern (Volumes) unterschiedlicher Größe und Art, die an die VM angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, holen Sie gemäß Richtlinie die Genehmigung des Administrators ein.
CSK GCP Linux-Cloud-Firewall: Bestellen Sie einen sicheren virtuellen Linux-Computer mit erweiterter Sicherheit, um Datenverkehr zu und von Ihren VM-Instanzen basierend auf Ihrer angegebenen Konfiguration für höchste Sicherheit zuzulassen oder abzulehnen.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Linux-Instanz eines beliebigen Instanztyps vom Google Cloud-Anbieter angefordert werden kann. Mit diesem Katalogelementformular können Sie der Compute-Instanz eine oder mehrere Sicherheitsgruppen (Firewall-Port-Regeln) zuweisen, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und die ausgewählten Subnetze aufgelistet.

Hinweis:

Tag (Schlüssel-Wert) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden.

Der Schlüsselwert wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der Public Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Google Cloud Platform Out-of-Box-Berechtigungen für Linux

Google Cloud Platform Berechtigungen für sofort einsatzbereite Linux-Katalogelemente

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

GCP-Berechtigungen

Katalogelement	Services	Berechtigung
CSK GCP Linux-VM	Bereitstellung	• „compute.disks.create“ • compute.disks.get • berechnen.Instanzen.Erstellen • compute.instances.get • „compute.instances.setMetadata“ • „compute.networks.get“ • „compute.subnetworks.get“ • „compute.subnetworks.use“. • „compute.subnetworks.useExternalIp“ • berechnen.zonen.abrufen
	Punkt-Discovery	• compute.disks.list • „compute.images.list“ • „compute.instanceTemplates.list“ • compute.instances.list • „compute.computerTypes.list“ • „compute.snapshots.list“ • „compute.zones.list“ • compute.regions.list
	Tag 2 – VM: Virtueller Server – StopNode	• compute.instances.stop • „compute.regions.get“ • berechnen.maschineTypen.abrufen
	Virtueller Server: StartNode	compute.instances.start
	Virtueller Server: Größe ändern	• compute.instances.stop • berechnen.maschineTypen.abrufen • „compute.regions.get“ • „compute.instances.setMachineType“ • compute.instances.start
	Virtueller Server: Bereitstellung aufheben	• compute.instances.delete • „compute.regions.get“

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

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
	Aufheben der Stapelbereitstellung	• compute.instances.delete • compute.disks.delete **Hinweis:** Tag-2-Datenträgerberechtigungen sind ebenfalls erforderlich. Diese entsprechen Linux-Mehrfachdatenträgern.
CSK GCP Linux mit mehreren Datenträgern	Bereitstellung	• „compute.disks.create“ • compute.disks.get • „compute.disks.use“. • berechnen.Instanzen.Erstellen • compute.instances.get • „compute.instances.setMetadata“ • „compute.networks.get“ • „compute.subnetworks.get“ • „compute.subnetworks.use“. • „compute.subnetworks.useExternalIp“ • berechnen.zonen.abrufen • „compute.zoneOperations.get“
	Punkt-Discovery	• compute.disks.list • „compute.images.list“ • „compute.instanceTemplates.list“ • compute.instances.list • „compute.computerTypes.list“ • „compute.snapshots.list“ • „compute.zones.list“ • compute.regions.list
	Tag 2 Festplattenspeicher – Speicher – Trennen	„compute.instances.detachDisk“
	Speicher-Deprovisionierung	compute.disks.delete
	Speicher – Verbundener Datenträger	„compute.instances.attachDisk“

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

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
	Aufheben der Stapelbereitstellung	• compute.instances.delete • compute.disks.delete **Hinweis:** VM-Berechtigungen für Tag 2 sind ebenfalls erforderlich. Diese entsprechen der Basis-Linux-VM.
CSK GCP Sichere Linux-Bereitstellung	Bereitstellung	• „compute.disks.create“ • compute.disks.get • berechnen.Instanzen.Erstellen • compute.instances.get • „compute.instances.setMetadata“ • „compute.instances.setTags“ • „compute.firewalls.create“ • „compute.firewalls.get“ • „compute.networks.get“ • „compute.networks.updatePolicy“ • „compute.subnetworks.get“ • „compute.subnetworks.use“. • „compute.subnetworks.useExternalIp“ • berechnen.zonen.abrufen
	Punkt-Discovery	• compute.disks.list • „compute.images.list“ • „compute.instanceTemplates.list“ • compute.instances.list • „compute.computerTypes.list“ • „compute.snapshots.list“ • „compute.zones.list“ • compute.regions.list • „compute.networks.list“ • „compute.firewalls.list“
	Aufheben der Stapelbereitstellung	• „compute.firewalls.delete“ • „compute.networks.updatePolicy“ • compute.instances.delete • compute.disks.delete

Automatische Übersetzung

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

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
		Hinweis: Tag-2-VM-Datenträgerberechtigungen sind ebenfalls erforderlich.

Google Cloud Platform Lastenausgleichsmodul

Cloud-Services-Katalog mit Google Cloud Platform HTTP Load Balancer für Hochverfügbarkeit

Dies ist ein Beispielkatalogelement, das den Prozess der Bereitstellung eines HTTP-Lastenausgleichsmoduls vom Google Cloud-Anbieter optimieren soll. Das primäre Ziel besteht darin, Leistungsprobleme zu minimieren und die Anwender-Experience durch die effiziente Verwaltung des eingehenden Datenverkehrs zu verbessern.

Auftrag	Funktionen
Bestellen Sie ein HTTP-Lastenausgleichsmodul, um den Anwenderdatenverkehr auf mehrere Instanzen der Anwendungen zu verteilen und so das Risiko von Leistungsproblemen zu verringern.	Dieses voll funktionsfähige Katalogelement erstellt ein Classic Application Load Balancer – global. Als globale Lastenausgleichsmodule sind nur externe Lastenausgleichsmodule verfügbar. Wählen Sie ein globales Lastenausgleichsmodul aus, wenn das Lastenausgleichsmodul global verteilt werden soll. Jedes globale Lastenausgleichsmodul wird auf alle Regionen verteilt. Zonen- und Regionalausfälle haben keine Auswirkungen.

Google Cloud Platform Standardmäßige Lastenausgleichsmodul-Berechtigungen

Google Cloud Platform Standardmäßige HTTP-Lastenausgleichsmodul-Berechtigungen

GCP-Berechtigungen

Katalogelement	Services	Berechtigung
CSK GCP HTTP-Lastenausgleichsmodul	Bereitstellung	• „compute.backendServices.create“ • „compute.backendServices.get“ • „compute.backendServices.use“. • „compute.globalAddresses.create“ • „compute.globalAddresses.get“ • „compute.globalAddresses.use“. • „compute.globalForwardingRules.create“ • „compute.globalForwardingRules.get“ • „compute.healthChecks.create“ • „compute.healthChecks.get“

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

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
		• „compute.healthChecks.useReadOnly“ • „compute.instanceGroups.create“ • „compute.instanceGroups.get“ • „compute.instanceGroups.update“ • „compute.instanceGroups.use“. • berechnen.instanzen.verwenden • „compute.targetHttpProxies.create“ • „compute.targetHTTPProxies.get“ • „compute.targetHttpProxies.use“. • „compute.urlMaps.create“ • „compute.urlMaps.get“ • „compute.urlMaps.use“ • „compute.networks.get“
	Punkt-Discovery	• „compute.backendServices.list“ • „compute.forwardingRules.list“ • „compute.healthChecks.list“ • „compute.httpHealthChecks.list“ • „compute.httpsHealthChecks.list“. • „compute.instanceGroupManagers.list“ • „compute.instanceGroups.list“ • compute.instances.list • „compute.targetHttpProxies.list“ • „compute.targetHttpsProxies.list“ • „compute.targetSslProxies.list“ • „compute.targetTcpProxies.list“ • „compute.urlMaps.list“ • compute.regions.list • „compute.zones.list“
	LB: Aufheben der Bereitstellung	• „compute.globalForwardingRules.delete“ • „compute.targetHttpProxies.delete“ • „compute.urlMaps.delete“
	Stapel: Bereitstellung aufheben	• „compute.globalAddresses.delete“ • „compute.backendServices.delete“

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

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
		• „compute.healthChecks.delete“ • „compute.instanceGroups.delete“ • „compute.globalForwardingRules.delete“ • „compute.targetHttpProxies.delete“ • „compute.urlMaps.delete“

Google Cloud Platform Vordefinierte Windows-Katalogelemente

Cloud-Services-Katalog Windows-VM, bis zu 10 zusätzliche Datenträger auf Google Cloud Platform oder mit Cloud-Firewall.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Windows-Instanz eines beliebigen Typs von Google Cloud Platformangefordert werden kann.

Reihenfolgen und Funktionen von Linux-VMs:

Auftrag	Funktionen
CSK GCP Windows-VM: Bestellen Sie eine virtuelle Windows-Maschine, die die Installation von Agent Client Collector unterstützt. Für andere VM-Größen als e2-micro und e2-small ist eine Genehmigung erforderlich.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Windows-Instanz eines beliebigen Instanztyps vom Google Cloud-Anbieter angefordert werden kann. Für andere Instanztypen als e2-micro und e2-small ist die Genehmigung durch den Administrator gemäß Richtlinie erforderlich. Die Windows-Anmeldeinformationen werden vom Benutzer im Katalogbestellformular angegeben. Die Anmeldeinformationen zur Erfüllung der Komplexitätsanforderung basierend auf der Windows-Version. Die Workflow-Automatisierung führt einen CCG-Scan auf der bereitgestellten Windows-Instanz aus und überprüft die Richtlinienregel mit der Konfiguration der VM. Bei einem Verstoß wird der Stapel auf den Status „Nachverfolgung erforderlich“ gesetzt, um zu melden, dass die Stapelbereitstellung nicht den Normen entspricht.
CSK GCP Windows mit mehreren Datenträgern: Bestellen Sie einen virtuellen Windows-Computer, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu zwei Datenträger ist keine Genehmigung erforderlich; bei	Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Windows-Instanz eines beliebigen Instanztyps vom Google Cloud-Anbieter angefordert werden kann. Dieses Katalogelementformular ermöglicht das Bestellen von bis zu 10 zusätzlichen Datenträgern (Volumes) unterschiedlicher Größe und Art, die an die VM angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, ist

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

Auftrag	Funktionen
mehr als 2 Datenträgern ist eine Genehmigung jedoch erforderlich.	gemäß Richtlinie die Genehmigung des Administrators erforderlich. Die Windows-Anmeldeinformationen werden vom Benutzer im Katalogbestellformular angegeben. Die Anmeldeinformationen zur Erfüllung der Komplexitätsanforderung basierend auf der Windows-Version.
CSK GCP Windows-Cloud-Firewall: Bestellen Sie einen sicheren virtuellen Windows-Computer mit erweiterter Sicherheit, um Datenverkehr zu und von Ihren VM-Instanzen basierend auf Ihrer angegebenen Konfiguration für höchste Sicherheit zuzulassen oder abzulehnen.	Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Windows-Instanz eines beliebigen Instanztyps vom Google Cloud-Anbieter angefordert werden kann. Mit diesem Katalogelementformular können Sie der Compute-Instanz eine oder mehrere Sicherheitsgruppen (Firewall-Port-Regeln) zuweisen, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und die ausgewählten Subnetze aufgelistet. Die Windows-Anmeldeinformationen werden vom Benutzer im Katalogbestellformular angegeben. Die Anmeldeinformationen zur Erfüllung der Komplexitätsanforderung basierend auf der Windows-Version.

Hinweis:

Tag (Schlüssel-Wert) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden.

Der Schlüsselwert wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der Public Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

CSK GCP Windows OOB-Berechtigungen

Google Cloud Platform Sofort einsatzbereite Windows-Berechtigungen

GCP-Berechtigungen

Katalogelement	Services	Berechtigung
CSK GCP Windows-VM	Bereitstellung	• „compute.disks.create“ • compute.disks.get • berechnen.Instanzen.Erstellen • compute.instances.get • „compute.instances.setMetadata“ • „compute.networks.get“ • „compute.subnetworks.get“ • „compute.subnetworks.use“.

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

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
		• „compute.subnetworks.useExternalIp“ • berechnen.zonen.abrufen
	Punkt-Discovery	• compute.disks.list • „compute.images.list“ • „compute.instanceTemplates.list“ • compute.instances.list • „compute.computerTypes.list“ • „compute.snapshots.list“ • „compute.zones.list“ • compute.regions.list
	Tag 2 – VM: Virtueller Server – StopNode	• compute.instances.stop • „compute.regions.get“ • berechnen.maschineTypen.abrufen
	Virtueller Server: StartNode	compute.instances.start
	Virtueller Server: Größe ändern	• compute.instances.stop • berechnen.maschineTypen.abrufen • „compute.regions.get“ • „compute.instances.setMachineType“ • compute.instances.start
	Virtueller Server: Bereitstellung aufheben	• compute.instances.delete • „compute.regions.get“
	Aufheben der Stapelbereitstellung	• compute.instances.delete • compute.disks.delete **Hinweis:** Tag-2-Datenträgerberechtigungen sind ebenfalls erforderlich. Diese sind mit mehreren Windows-Datenträgern identisch.

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

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
CSK GCP Windows mit mehreren Datenträgern	Bereitstellung	• „compute.disks.create“ • compute.disks.get • „compute.disks.use“. • berechnen.Instanzen.Erstellen • compute.instances.get • „compute.instances.setMetadata“ • „compute.networks.get“ • „compute.subnetworks.get“ • „compute.subnetworks.use“. • „compute.subnetworks.useExternalIp“ • berechnen.zonen.abrufen • „compute.zoneOperations.get“
	Punkt-Discovery	• compute.disks.list • „compute.images.list“ • „compute.instanceTemplates.list“ • compute.instances.list • „compute.computerTypes.list“ • „compute.snapshots.list“ • „compute.zones.list“ • compute.regions.list
	Tag 2 Festplattenspeicher – Speicher – Trennen	„compute.instances.detachDisk“
	Speicher-Deprovisionierung	compute.disks.delete
	Speicher – Verbundener Datenträger	„compute.instances.attachDisk“
	Aufheben der Stapelbereitstellung	• compute.instances.delete • compute.disks.delete **Hinweis:** VM-Berechtigungen für Tag 2 sind ebenfalls erforderlich. Diese entsprechen der grundlegenden Windows-VM.

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

GCP-Berechtigungen (Fortsetzung)

Katalogelement	Services	Berechtigung
CSK GCP Sichere Windows-Bereitstellung	Aufheben der Stapelbereitstellung	• „compute.firewalls.delete“ • „compute.networks.updatePolicy“ • compute.instances.delete • compute.disks.delete **Hinweis:** Tag-2-VM-Datenträgerberechtigungen sind ebenfalls erforderlich.

Microsoft Azure Vordefinierte Linux-Katalogelemente

Cloud-Services-Katalog Linux-VM mit Agent Client Collector (ACC), bis zu 10 zusätzlichen Datenträgern, Sicherheitsgruppen oder mit skalierbaren Webservern oder mit Sicherheitsgruppen.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Linux-Instanz eines beliebigen Instanztyps von Microsoft Azureangefordert werden kann.

Auftrag	Funktionen
Bestellen Sie einen virtuellen Linux-Computer bei Microsoft Azure, der die Installation von Agent Client Collector unterstützt. ACC ist für Produktionsinstanzen obligatorisch. Andere VM-Größen als „Standard_A1_v2“ und „Standard_A2_v2“ erfordern eine Genehmigung. Zur Compliance-Überprüfung wird ein Cloud-Konfigurationsscan ausgeführt.	Für andere Instanztypen als Standard_A1_v2 und Standard_A2_v2 ist die Genehmigung durch den Administrator gemäß Richtlinie erforderlich. Das Katalogelement verfügt über integrierte Client-Regeln zum Steuern einer ACC-Installation (Agent Client Collector), wenn die Bereitstellungsumgebung für die Produktion markiert ist. Zur Auswahl des Aliasschlüssels für Anmeldeinformationen für die ACC-Bereitstellung ab MID müssen dem Benutzer die entsprechenden Berechtigungen für die ACC-Administratorrolle gewährt werden. Die Workflow-Automatisierung führt einen CCG-Scan für die bereitgestellte Linux-Instanz aus und überprüft die Richtlinienregel mit der Konfiguration der VM. Bei einem Verstoß wird der Stapel auf den Status „Nachverfolgung erforderlich“ gesetzt, um zu melden, dass die Stapelbereitstellung nicht den Normen entspricht.
Bestellen Sie eine virtuelle Linux-Maschine, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu 2 Datenträger ist keine Genehmigung erforderlich. Für	Dieses Katalogelementformular ermöglicht das Bestellen von bis zu 10 zusätzlichen Datenträgern (Volumes) unterschiedlicher Größe und Art, die an die VM angehängt

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

Auftrag	Funktionen
alles, was darüber hinausgeht, ist eine Genehmigung einzuholen.	sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, holen Sie gemäß Richtlinie die Genehmigung des Administrators ein.
Bestellen Sie einen sicheren virtuellen Linux-Computer, und weisen Sie Sicherheitsgruppen zu. Wählen Sie so viele aus, wie Sie für die höchste Sicherheitsstufe benötigen.	Mit diesem Katalogelementformular können Sie der Compute-Instanz eine oder mehrere Sicherheitsgruppen (Firewall-Port-Regeln) zuweisen, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und die ausgewählten Subnetze aufgelistet.
Bestellen Sie einen Skalierungssatz für Linux-VMs, um identische virtuelle Computer bereitzustellen, die automatisierte Skalierung zu ermöglichen und hohe Verfügbarkeit sicherzustellen.	Dieses Katalogelement bietet die Möglichkeit, identische virtuelle Computer mithilfe einer Skalierungsgruppe für virtuelle Linux-Computer bereitzustellen, die die automatisierte Skalierung für eine höhere Verfügbarkeit unterstützt. E-Mail-URL wird als Vorgang nach der Bereitstellung hinzugefügt, der die Endpunkt-URL der bereitgestellten Anwendung per E-Mail an die anfordernde Person sendet.

Hinweis:

Tag (Schlüssel-Wert) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden.

Der Schlüsselwert wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der Public Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Microsoft Azure Vordefinierte Windows-Katalogelemente

Cloud-Services-Katalog Windows-VM, bis zu 10 zusätzliche Datenträger auf Microsoft Azure oder mit Sicherheitsgruppen.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem eine Windows-Instanz eines beliebigen Instanztyps von Microsoft Azureangefordert werden kann.

Auftrag	Funktionen
Bestellen Sie eine Microsoft Windows-VM, die die Installation von Agent Client Collector unterstützt. Andere VM-Größen als „Standard_A1_v2“ und „Standard_A2_v2“ erfordern eine Genehmigung. Zur Compliance-Überprüfung wird ein Cloud-Konfigurationsscan ausgeführt.	Für andere Instanztypen als Standard_A1_v2 und Standard_A2_v2 ist die Genehmigung durch den Administrator gemäß Richtlinie erforderlich. Die Workflow-Automatisierung führt einen CCG-Scan für die bereitgestellte Linux-Instanz aus und überprüft die Richtlinienregel mit der Konfiguration der VM.

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

Auftrag	Funktionen
Bestellen Sie einen virtuellen Windows-Computer bei Microsoft Azure, und geben Sie bis zu 10 zusätzliche Datenträger an. Für bis zu zwei Datenträger ist keine Genehmigung erforderlich; bei mehr als 2 Datenträgern ist eine Genehmigung jedoch erforderlich.	Dieses Katalogelementformular ermöglicht das Bestellen von bis zu 10 zusätzlichen Datenträgern (Volumes) unterschiedlicher Größe und Art, die an die VM angehängt sind. Wenn der Anforderung mehr als zwei zusätzliche Datenträger hinzugefügt werden, holen Sie gemäß Richtlinie die Genehmigung des Administrators ein. Das Windows-Administratorpasswort wird zum Zeitpunkt der Erstellung von Microsoft Azure abgerufen.
Bestellen Sie einen sicheren virtuellen Windows-Computer unter Microsoft Azure, und weisen Sie Sicherheitsgruppen zu. Wählen Sie so viele aus, wie für die höchste Sicherheitsstufe erforderlich sind.	Mit diesem Katalogelementformular können Sie der Compute-Instanz eine oder mehrere Sicherheitsgruppen (Firewall-Port-Regeln) zuweisen, sodass der Netzwerkzugriff auf die VM eingeschränkt wird. Sicherheitsgruppen werden für die ausgewählte VPC und die ausgewählten Subnetze aufgelistet.

Hinweis:

Tag (Schlüssel-Wert) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden. Der Schlüssel-Wert wird derzeit nur in der Tabelle „cmdb_key_value“ aktualisiert, nicht in der Public Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Microsoft Azure Out-of-Box-Berechtigungen

Cloud-Services-Katalog Microsoft Azure Berechtigungen für vordefinierte Katalogelemente.

Services	Ressourcen
Microsoft.Compute	1. virtuelleMaschinen/* 2. Datenträger/* 3. Verfügbarkeitssätze/* 4. Images/* 5. virtualMachineScaleSets/* 6. Standorte/* 7. VM-Größe/* 8. registrieren/Aktion/* 9. Registrierung aufheben/Aktion/* 10. capacityReservationGroups/* 11. cloudServices/* 12. diskAccesses/privateEndpointConnectionsApproval/* 13. diskEncryptionSets/*

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

Services	Ressourcen
	14. Galerien/* **15.** hostGruppen/* **16.** näherungsPlatzierungsGruppen/* **17.** wiederherstellenPunktsammlungen/* **18.** sshPublicKeys/* **19.** SharedVMExtensions/* **20.** SharedVMImages/* **21.** skus/Snapshots lesen/*
Microsoft.Network	**1.** registrieren/Aktion/* **2.** Registrierung aufheben/Aktion/* **3.** checkTrafficManagerNameAvailability/Aktion/* **4.** internalNotify/Aktion/* **5.** getDnsResourceReference/action/* **6.** checkFrontDoorNameAvailability/Aktion/* **7.** privateDnsZonesInternal/Aktion/* **8.** applicationGateways/* **9.** ExpressRouteCircuits/* **10.** Lastenausgleichsmodule/* **11.** networkInterfaces/* **12.** NetzwerkSicherheitsgruppen/* **13.** privateDnsZonen/* **14.** publicIPAddresses/* **15.** Standorte/* **16.** virtuelleNetzwerke/* **17.** virtualNetworks/subnets **18.** virtualNetworks/virtualNetworkPeerings/* **19.** NAT-Gateways/* **20.** localnetworkgateways/* **21.** Verbindungen/* **22.** RouteTabellen/* **23.** Subnetze/*
Microsoft.Storage	**1.** registrieren/Aktion/* **2.** Registrierung aufheben/Aktion/*

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

Services	Ressourcen
	3. Speicherkonten/* **4.** Blobs/*
Microsoft.Ressourcen	**1.** Tags/* **2.** resourceGroups/* **3.** Abonnements/* **4.** Ressourcen/* **5.** Anbieterbereitstellungen/*
Microsoft.Sql	**1.** Server/* **2.** Server/Datenbanken/* **3.** Standorte/*/lesen
Microsoft.Ressourcenintegrität	Verfügbarkeitsstatus/*
Microsoft.ContainerService	**1.** verwalteteCluster/* **2.** Flotten/*
Microsoft.Web	**1.** serverFarms/* **2.** Sites/*
Microsoft.RessourceGraph	Ressourcen/*

Microsoft Azure Funktionen-App-Katalogelemente

Cloud-Services-Katalog Microsoft Azure Funktions-App mit nutzungsbasierter Preisgestaltung.

Dies ist ein voll funktionsfähiges Beispielkatalogelement, mit dem Benutzer eine Windows-Instanz eines beliebigen Instanztyps von Microsoft Azureanfordern können.

Auftrag	Funktionen
Bestellen Sie eine Funktions-App, um kleine, ereignisgesteuerte Funktionen zu erstellen und bereitzustellen, ohne die Infrastruktur verwalten zu müssen. Sie bietet eine serverlose Computing-Experience mit nutzungsbasierten Preisen.	Dieses Katalogelement stellt eine NodeJS-Basisanwendung „Hello World“ in der bereitgestellten Funktions-App Microsoft Azure bereit. Die unterstützten Versionen von NodeJS entsprechen denen im Azure-Portal. Das Windows-Administratorpasswort wird zum Zeitpunkt der Erstellung von Microsoft Azure abgerufen.

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

Hinweis:

Tag (Schlüssel-Wert) ist allen bereitgestellten Ressourcen zugewiesen. Beispiel: VM, Netzwerk, Speicher wie im Stapel vorhanden. Der Schlüsselwert wird nur in der Tabelle „cmdb_key_value“ aktualisiert, derzeit nicht in der Public Cloud. Dies wird in zukünftigen Releases behoben, um die Tags in der Cloud zu aktualisieren.

Vordefinierte Aktionen

Die sofort einsatzbereiten Aktionen umfassen OOB-Bereitstellungs-, Tagging-, Abruf- und Nachbereitstellungsvorgänge. Alle diese Aktionen basieren auf Flow Designer und sind als Integration Hub-Subflows implementiert.

Aktionen	Name des Flow Designer-Subflows	Beschreibung
Stellen Sie ACC-* nach der Bereitstellung bereit	CSK Inhalt – Nachbereitstellung – Stellen Sie ACC in Stapel-VMs bereit	ACC (Agent Client Collector) wird über eine Flow Designer-Aktion bereitgestellt. Dies wird als Schritt nach der Bereitstellung für das grundlegende Linux-VM-Bereitstellungskatalogelement bezeichnet. Voraussetzungen: **1.** Der ACC-Listener muss in einem beliebigen MID-Serverkonfiguriert werden. Dadurch werden ein MID-Webserver-Endpunkt und ein MID-Server API-Schlüssel generiert. **2.** In den Betriebsparametern nach der Bereitstellung des Basis-Linux-VM-Katalogs werden diese beiden Parameter – Webserverendpunkt (normalerweise im Format wss://)<IP_Address> :3389/ws/events) und MID-Server API-Schlüssel, müssen festgelegt werden. Standardmäßig enthalten diese Parameter leere Werte.

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

Aktionen	Name des Flow Designer-Subflows	Beschreibung
		Hinweis: Wenn die generierte WS-Endpunkt-URL die private IP von MID-Serverzurückgibt, muss diese private IP für die Internetbasierte Konnektivität durch die öffentliche IP der VM MID-Server ersetzt werden. **3.** Es muss eine Konnektivität über den SSH-Port von MID-Server zur bereitgestellten VM bestehen. Im Falle eines Fehlers bei der Installation des Agent auf der bereitgestellten VM wird eine Aufgabe erstellt, und der Stapel wird auf den Status „Folgeaufgabe erforderlich“ gesetzt und automatisch aktiviert, sobald alle Folgeaufgaben geschlossen wurden.
CCG-Scan nach der Bereitstellung	CSK Inhalt: CCG-Richtlinienscan für Stapelelemente erstellen	„Scannen mit dem standardmäßigen OOB-Richtliniensatz in CCG“ wird mit der einfachen Windows- und Linux-Bereitstellung aufgerufen. Wenn ein CCG-Scan aufgrund eines Verstoßes fehlschlägt, wird der Stapel auf den Status „Nachverfolgung erforderlich“ gesetzt. Der Operator muss sicherstellen, dass der Verstoß behoben wird, und die Verstoßaufgabe schließen. Sobald alle Folgeaufgaben geschlossen sind, wird der Stapel automatisch in den Status „Aktiv“ versetzt und kann von der anfordernden Person verwendet werden.

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

Aktionen	Name des Flow Designer-Subflows	Beschreibung
Tagging-Aktion	CSK Inhalt – Nachbereitstellung – Schlüsselwerte in CMDB aktualisieren	Für alle Katalogelemente wird eine Tagging-Aktion als Schritt nach der Bereitstellung ausgeführt. Diese Aktion aktualisiert nur die Schlüssel-Wert-Einträge in CMDB, nicht in der Cloud. Die aktualisierten Standard-Tags sind StackName, Application, CostCenter und BusinessService. Felder mit leeren Werten werden nicht als Schlüssel-Wert-Datensätze gespeichert.
Ruft das Windows-Passwort ab	CSK Inhalt – Nachbereitstellung – Windows-Passwort abrufen	Alle Windows-Kataloge verfügen über eine Aktion zum Abrufen von Passwörtern, die dem Administrator das Passwort der bereitgestellten Windows-VM per E-Mail an die anfordernde Person sendet. Das Passwort wird von AWS abgerufen, nachdem die Bereitstellung abgeschlossen ist. Verwenden Sie eine SSH-Schlüsseldatei („pem“), um das Passwort zu entschlüsseln. Führen Sie die folgenden Schritte aus, um diese PEM-Datei auf dem Terraform Linux-Server einzurichten: **1.** Stellen Sie sicher, dass die Anmeldeinformationen für den privaten SSH-Schlüssel für die VM mit installierter Terraform CLI dem Anmeldeinformationsalias „TFO Server-Anmeldeinformationsalias“ zugeordnet sind. Dieser Alias wird bereits mit der Installation des Inhaltspakets CSK erstellt. Dieser Alias wird für eine SSH-Verbindung zum Terraform-Server verwendet, um das

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

Aktionen	Name des Flow Designer-Subflows	Beschreibung
		Windows-Passwort aus der Ausgabevariablen abzurufen. **2.** Stellen Sie sicher, dass im Variablensatz „Bereitstellung“ des Katalogs für die Variable „keypath“ der Standardwert auf den Pfad des Verwaltungsschlüssels (der Schlüssel, der das Passwort entschlüsseln kann) auf der Terraform-VM festgelegt ist. **3.** Stellen Sie sicher, dass die anfordernde Person die E-Mail eingerichtet hat **Hinweis:** Für anwenderdefinierte Kataloge ist dieser Vorgang nur zur Verwendung mit Terraform Opensource-basierten Katalogelementen verfügbar.
E-Mail-URL für Microsoft Azure Skalierbare Webserveranwendung	CSK Inhalt: E-Mail-URL für Microsoft Azure Skalierbare Webserveranwendung	Diese Aktion wird als Vorgang nach der Bereitstellung im Katalogelement „CSK Microsoft Azure Linux mit skalierbarem Webserver“ hinzugefügt, das die Endpunkt-URL der bereitgestellten Anwendung per E-Mail an die anfordernde Person sendet. Die URL wird von Microsoft Azure abgerufen, nachdem die Bereitstellung abgeschlossen ist. Stellen Sie sicher, dass die anfordernde Person die E-Mail eingerichtet hat.
Rufen Sie den Hostnamen der Microsoft Azure Funktions-App ab	CSC-Inhalt – Nachbereitstellung – Hostname der Funktions-App Microsoft Azure abrufen	Diese Aktion wird als Vorgang nach der Bereitstellung in „CSK

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

Aktionen	Name des Flow Designer-Subflows	Beschreibung
		Microsoft Azure Funktions-App-Katalogelement hinzugefügt, das den Hostnamen der bereitgestellten Funktions-App für die anfordernde Person abruft.

Out-of-Box-Richtlinien

Die Cloud-Services-Katalog sofort einsatzbereiten Richtlinien umfassen Genehmigungs-, Benennungs-, Leasing- und Kontingentbereitstellungsrichtlinien.

Bereitstellungsrichtlir	Beschreibung
Genehmigung	ServiceNow-Genehmigungsaktion, die zu bestimmten Anlässen über den Richtlinienauslöser aufgerufen wird. Beispiel: Wenn eine anfordernde Person eine VM eines anderen Typs als t2.micro und t2.nano bestellt oder wenn mehr als zwei zusätzliche Datenträger für bestimmte Katalogelemente angefordert werden.
Benennungsrichtlinie	Ein guter Ansatz für Ressourcen, die als Teil einer einzelnen Anforderung bereitgestellt werden, besteht darin, die Ressourcen mit einem allgemeinen Namen zu kennzeichnen, z. B. dem Namen des Stapels. Wenn der Stapelname der Standardkonvention entspricht, ist das nützlich, um die Identifizierung der Besitzer und das Alter zu erleichtern. Die standardmäßig enthaltene Benennungsrichtlinie ist für alle Cloud-Katalogelemente aktiviert. Wenn die Richtlinie aktiv ist, wird ein Stapelname in einem bestimmten Benennungsformat für das Feld Stapelname im Formular vorgeschlagen. Das Benennungsformat verwendet eine Kombination aus den Anfangsbuchstaben des Namens der anfordernden Person, gefolgt vom aktuellen Datum und der aktuellen Uhrzeit im Format „mm dt hh mm“. Beispiel: Wenn der Name der anfordernden Person John Smith ist und Datum/Uhrzeit 10:30 Uhr am 15. Mai sind, wird der Stapelname als „js05151030“ generiert.
Mietvertrag	Die Lease-Richtlinie wird verwendet, um die Aufhebung der Bereitstellung nicht verwendeter/unerwünschter Stapel auszulösen, um Kosten in der Cloud zu sparen. Die Mietrichtlinie hebt die Bereitstellung aktiver Stapel nach Ablauf des Mietzeitraums auf. Eine Woche vorher werden Erinnerungen an Stapelbesitzer gesendet, in denen angegeben wird, dass der Stapel abläuft.
Kontingentrichtlinie	Die Kontingentrichtlinie wird verwendet, um zu entscheiden, ob eine Anforderung, die ausgeführt wird, sobald das Kontingent überschritten wird, genehmigt oder abgebrochen werden soll. Siehe Steuerungen für Ressourcenbestellungen für vorlagenbasierte Cloud-Katalogelemente

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

CSC-Referenzen

Referenzthemen enthalten zusätzliche Informationen zu den Listen und Formularen, die Sie zum Konfigurieren, Verwalten und Verwenden von Cloud-Services-Katalogverwenden.

Domain Separation und Cloud-Services-Katalog

Die Domänentrennung wird in Cloud-Services-Katalog unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Empfehlungen für Domain Separation in Cloud-Services-Katalog

Empfehlungen zur Domänentrennung in Cloud-Services-Katalog:

CSK Geführtes Setup

CSK Das geführte Setup sollte nur vom Systemadministrator innerhalb der globalen Domäne ausgeführt werden. Es ist wichtig zu beachten, dass die lokale Domäne nicht die geeignete Umgebung für diese Aufgabe ist.

Terraform Open Source in globaler Domäne

Alle Kataloge und Konfigurations-Provider werden mit der Installation des Plugins Cloud-Services-Katalog in der globalen Domäne installiert. Daher funktionieren die vordefinierten Kataloge auch nur, wenn Sie die Terraform Opensource(TFO)-Konfiguration und die Anmeldeinformationen in der globalen Domäne und nicht in einer bestimmten Domäne erstellen. Dadurch können die Anwender von Managed Service Providern (MSP) auch einen einzelnen TFO-Server für mehrere Domänen verwenden.

Anmeldeinformationen des Service Providers

Die Anmeldeinformationen für Service Provider (AWS, Microsoft Azure und Google Cloud Platform müssen domänenspezifisch sein. Die installierbaren Konfigurationselemente Azure DevOps) und Ansible müssen sich jedoch für die Bereitstellung in der globalen Domäne befinden.

MID-Server in der globalen Domäne

Automatische Übersetzung

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

Legen Sie den MID-Server in der globalen Domäne als TFO fest, und die zugehörige Konfigurationsverwaltung wird ebenfalls im globalen Kontext festgelegt. Dies ermöglicht eine genaue globale Discovery.

MSP-Anwender können globale MID-Server einrichten und für Tag 1 auch domänenspezifische MID-Server für verschiedene Service Provider verwenden.

Nächste Schritte

Weitere Informationen zur Funktionsweise der Domänentrennung in Cloud Provisioning and Governancefinden Sie unter Domain Separation und Cloud Provisioning and Governance.

Zugehörige Informationen

Domänentrennung für Service Provider

Azure DevOps Berechtigungen

Azure DevOps Discovery- und Bereitstellungsberechtigungen.

Berechtigungstyp	Beschreibung	PAT-Zugriff
Cloud-Services-Katalog Azure DevOps Discovery	Erkennt Projekte und Pipelines in der Organisation Azure DevOps und fügt CMDBhinzu.	# Build (Lesen)
Cloud-Services-Katalog Azure DevOps Bereitstellung	Bereitstellung über die Pipeline Azure DevOps, ausgelöst über Cloud-Services-Katalog den DevOps-Integrationskatalog.	Build-Anzahl (Lesen und ausführen)
Cloud-Services-Katalog Azure DevOps tag:Ressourcen-Berechtigung abrufen	Erkennen Sie AWS -Ressourcen, die über die Pipeline Azure DevOps bereitgestellt werden.	Nicht zutreffend

Ansible Berechtigungen

Ansible Konfigurations-Provider, Ansible-Katalog und Betriebsberechtigungen.

Ansible Berechtigungen für Tag 0, Tag 1 und Tag 2

Berechtigungstyp	Beschreibung
Ansible Konfigurations-Provider Discovery an Tag 0	1. Referenzlink zum Konfigurieren der Anmeldeinformationen für Ansible : https://docs.ansible.com/ansible-tower/latest/html/userguide/credentials.html 2. Erstellen von Ansible Tower-Anwendern: https://docs.ansible.com/ansible-tower/3.2.5/html/userguide/users.html 3. Rollen/Berechtigungen können Tower-Anwendern Ansible pro Projekt/Bestand/Auftragsvorlage/Anmeldeinformationen nach Bedarf gewährt werden. Weitere Details: https://docs.ansible.com/ansible-tower/latest/html/userguide/users.html#users-permissions

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

Ansible Berechtigungen für Tag 0, Tag 1 und Tag 2 (Fortsetzung)

Berechtigungstyp	Beschreibung
	4. CAPI verwendet einen auf Token basierenden Mechanismus für die Standardauthentifizierung, der die Anmeldeinformationen des Tower-Benutzers Ansible verwendet. OAuth-Token basierend auf den Anmeldeinformationen für die Standardauthentifizierung werden generiert. **5.** Projekte, die die GitHub-Anmeldeinformationen des Playbooks enthalten (hier sind .yml-Dateien vorhanden), werden manuell unter Ansiblekonfiguriert. Weitere Informationen: https://docs.ansible.com/ansible-tower/latest/html/userguide/credentials.html#source-control **6.** Verwendet Ansible Anmeldeinformationen für Discovery von Bestand, Projekten, installierbaren cfg-Auftragsvorlagen (Playbooks und ihre zusätzlichen Variablen abrufen) unter Verwendung von CAPI.
Ansible Katalogbereitstellung/-aufhebung der Bereitstellung an Tag 1	Verwendet Ansible Tower-Anwenderanmeldeinformationen und Servicekonto-Anmeldeinformationen von Amazon Web Services/Azure, die in der Auftragsvorlage Ansible angegeben sind.
Ansible tag:Ressourcen für Discovery abrufen	Verwendet `tag:GetResources` Berechtigung zum Erkennen von AWS -Ressourcen, die über Ansible die -Pipeline bereitgestellt werden.
Ansible Tag-2-Vorgänge	Verwendet Ansible Tower-Anmeldeinformationen, Anmeldeinformationen für das Servicekonto von Amazon Web Services/Azure und ein privates SSH-Schlüsselpaar oder Windows-Anwendername/Passwort, um eine Verbindung zu der jeweils bereitgestellten Cloud-Ressource herzustellen.

Phasen von Azure DevOps in Release-Lebenszyklusmanagement

Die Komponenten und Phasen einer Pipeline Azure DevOps sind umfassend und hochgradig anpassbar. Mit Cloud-Services-Katalogkönnen Sie mehrere Phasen, Aufgaben und Integrationen basierend auf Ihren spezifischen Anforderungen und Ihrem Technologiestapel definieren.

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

Support ab Tag 0	Support ab 1 Tag	Support ab Tag 2
1. Scannen Sie die -Projekte und -Pipelines 2. Erfassen Sie Pipelinevariablen aus Azure DevOps	1. Bestellen Sie aus dem Servicekatalog 2. Referenz aus erkannten Azure DevOps -Projekten und -Pipelines 3. Wählen Sie Eingaben aus, die für die Release-Bereitstellungs-Pipeline erforderlich sind 4. Übermitteln Sie den Katalog	1. SRE-Vorgänge: Patchen, Sichern usw. für Produktionsressourcen 2. Tägliche Wartung – Neustart, Neustart, Anhalten usw. 3. Ressourcen mit Tags versehen, Härtung wird ausgeführt usw.
In CMDB als referenzierbare Objekte speichern	1. Auf Genehmigung warten 2. Verfolgen Sie den Fortschritt 3. Aktualisieren Sie CMDB mit bereitgestellten Ressourcen	1. Stellt Resilienz in der Produktion sicher. 2. Zwischen blauer und grüner Umgebung wechseln

Problemumgehung für bekannte Probleme

In der Knowledge Base wurden Schritte zur Problemumgehung für einige der bekannten Probleme zusammengestellt und beschrieben.

Workaround	Verknüpfung
Cloud-Services-Katalog: Bekannte Probleme und Problemumgehungen	https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1362282

Zugehörige Informationen

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1362282

Bewertung der Cloud-Migration

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

Ressourcenmigration vorbereiten

Gruppieren Sie Server, erstellen Sie Migrationsbewertungsaufgaben und schulen und überzeugen Sie Stakeholder, um eine bessere Entscheidung für die Migration in die Cloud zu ermöglichen. Mit dieser App können Sie die gesammelten Informationen zu Hardware, Apps und Serverkonfiguration verwenden, um die Migrationsansätze zu bewerten: die Migrationsstrategien und die Anzahl der erforderlichen Migrationswellen. Nutzen Sie die kombinierten Denkanstöße der Stakeholder, um eine Orientierungshilfe für den besten Ansatz zu erhalten.

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

Untersuchen	Konfigurieren	Referenz
Erfahren Sie mehr über die Bewertung der Cloud-Migration.	Installieren oder aktualisieren Sie die Bewertung der Cloud-Migration.	Rufen Sie Details zu Komponenten wie Feldern, Tabellen und Eigenschaften ab.

Verwenden
Planen Sie den Migrationsprozess, erstellen Sie Migrationsaufgaben, weisen Sie Aufgaben Ressourcen zu, und überwachen Sie den Migrationsfortschritt.

Bewertung der Cloud-Migration erkunden

Verstehen Sie den typischen Bewertung der Cloud-Migration-Workflow und allgemeine Aufgaben.

Bewertung der Cloud-Migration ist verfügbar im ServiceNow Store.

Automatische Übersetzung

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

Apps im Store anfordern

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

Bewertung der Cloud-Migration enthält Informationen zu IT-Ressourcen, die von ITOM-Transparenz erkannt und in der CMDB gespeichert wurden. Wenn mit Ihrer ServiceNow-Lösung Erkennungstools von Drittanbietern bereitgestellt werden, werden in Bewertung der Cloud-Migration die von diesen Tools erkannten Informationen angezeigt.

Um Bewertung der Cloud-Migration für Planung und Überwachung des Migrationsprozesses zu verwenden, führen Sie die folgenden Aufgaben aus:

1. Bewertung der Cloud-Migration installieren.
2. Planen Sie den Migrationsprozess.
3. Erstellen Sie Bewertungsaufgaben und ordnen Sie sie Migrationswellen zu.
4. Bewertungsaufgaben in Konfigurierbarer Arbeitsbereich Ressourcen zuweisen.
5. Benachrichtigen Sie für den Migrationsprozesses verantwortliche Mitarbeiter, dass sie mit dem Migrieren von Ressourcen beginnen können.
6. Fortschritt der Cloud-Migration in Konfigurierbarer Arbeitsbereich überwachen.

Bewertung der Cloud-Migration konfigurieren

Installieren Sie Bewertung der Cloud-Migration aus dem ServiceNow Store.

Bewertung der Cloud-Migration installieren

Sie können die Anwendung Bewertung der Cloud-Migration (com.sn_cloud_migration) installieren, wenn Sie über die Administratorrolle verfügen. Die Anwendung enthält Demodaten und installiert die zugehörigen ServiceNow® Store-Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfen Sie die -Anwendungsliste im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Releasekompatibilität.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Von Bewertung der Cloud-Migration wird das ITOM Cloud Accelerate-Abonnement verwendet.

Die Anwendung Cloud Migration Base (com.sn_cloud_mig_base) wird automatisch aktiviert, wenn Sie die Anwendung Bewertung der Cloud-Migration (com.sn_cloud_migration) installieren.

Die folgenden Elemente werden mit Bewertung der Cloud-Migration installiert:

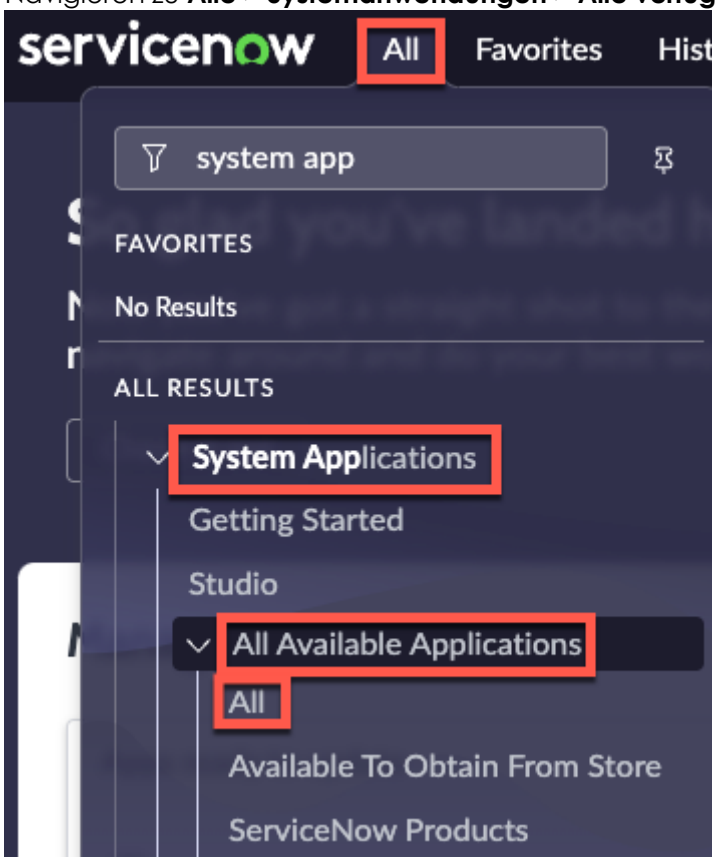
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

- Plugins
- Rollen
- Regelmäßige Aufgaben
- Tabellen
- Eigenschaften

Weitere Informationen finden Sie unter Mit Bewertung der Cloud-Migration installierte Komponenten.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Bewertung der Cloud-Migration (com.sn_cloud_migration).

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

   Die verfügbaren Versionen können Sie der Liste neben der Schaltfläche **Installieren** entnehmen.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.

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

5. Wahlweise: Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.
   Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für die gängigen Anwendungsfälle veranschaulichen. Laden Sie die Demodaten, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

   Wichtig: Wenn Sie die Demodaten nicht während der Installation laden, stehen sie nicht zum späteren Laden zur Verfügung.

6. Wählen Sie **Installieren** aus.

Zugehörige Informationen

Abonnements für IT Operations Management

Bewertung der Cloud-Migration in Konfigurierbarer Arbeitsbereich verwenden

Bewertung der Cloud-Migration-Operatoren überprüfen IT-Ressourcen, weisen sie Bewertungsaufgaben zu und ordnen Aufgaben Migrationswellen zu.

Migrationsprozess planen

Berücksichtigen Sie Aspekte der aktuellen IT-Infrastruktur, antizipieren Sie mögliche Auswirkungen der Migration und entscheiden Sie sich für die Migrationsstrategie.

Die Cloud-Migration erfordert eine sorgfältige Analyse und Planung.

Aktuelle Infrastruktur analysieren

Berücksichtigen Sie Aspekte der aktuellen IT-Infrastruktur und antizipieren Sie die Auswirkungen, um sich auf die Cloud-Migration vorzubereiten. Treffen Sie Entscheidungen zum Migrationsumfang: Welche IT-Ressourcen müssen in welcher Kapazität und wie schnell migriert werden? Darüber hinaus können Sie die Migration verwenden, um die Nutzung von IT-Ressourcen zu optimieren. Analysieren Sie die Ressourcennutzung, um redundante, nicht ausgelastete oder überstrapazierte Ressourcen zu identifizieren.

Verwenden Sie die folgenden Fragen, um über den Ansatz zu entscheiden und den Migrationsprozess zu planen, einschließlich Umfang, Zeitrahmen und Ressourcen:

- Woraus besteht die aktuelle IT-Infrastruktur?
  - Wie viele Server gibt es?
  - Gibt es Server, die nicht dauerhaft oder vorübergehend migriert werden können?
  - Wie viele IT-Ressourcen befinden sich bereits in der Cloud?
  - Was sind die Hardwareanforderungen, z. B. CPU-Durchsatz, Betriebszeit, Latenz?
  - Was sind die Software-Anforderungen?
  - Werden alle Server, Anwendungen und Services vollständig erkannt? Welche Konsequenzen hat die Migration dieser Ressourcen und Services? Was sind die potenziellen Fallstricke?
- Welche Teams könnten von der Migration betroffen sein?
  - Sind allen Teams die bevorstehenden Änderungen bekannt?
  - Wurden alle Serviceverantwortlichen identifiziert?
  - Gibt es Services, die von den Services anderer Teams abhängig sind?
- Was sind die Vor- und Nachteile einer Migration?

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

- Wie hoch wären die Kosten für die Migration zu verschiedenen Cloud-Providern?
- Welcher Cloud-Provider bietet das beste Preis-Leistungs-Verhältnis?
- Ist es möglich, basierend auf den Preismodellen mehrere Anbieter zu verwenden?

- Gibt es Möglichkeiten, die aktuelle IT-Infrastruktur vor der Migration zu optimieren?

  Es gibt Möglichkeiten, die Ressourcennutzung zu bewerten. In Umgebungen, in denen VMware bereitgestellt wird, können von Bewertung der Cloud-Migration VMware-Statistiken erfasst werden. Alternativ dazu können Sie die Anwendung Cloud-Einblicke bereitstellen, die Nutzungsmetriken verfügbar macht.

  - Gibt es Anwendungen, Server oder Services, die nicht mehr verwendet werden? Ist es möglich, solche Ressourcen zusammenzuführen, zu entfernen oder stillzulegen?
  - Gibt es Services, die derzeit eine übermäßige Abonnementnutzung bzw. übermäßige Nutzung aufweisen (ca. 90 % der Lizenzen sind vergeben)?
  - Gibt es Services, die derzeit eine zu geringe Abonnementnutzung bzw. Nutzung aufweisen (ca. 30 % der Lizenzen sind vergeben)?
  - Ist es möglich, den aktuellen Ressourcenverbrauch auszugleichen und anzupassen?
  - Ist es möglich, die Anzahl der Services zu konsolidieren?
  - Gibt es Server oder Services, bei denen End-of-Life-Software verwendet wird und die aktualisiert oder ersetzt werden müssen?

Aktuelle Infrastruktur mit Bewertung der Cloud-Migration überprüfen

Verwenden Sie die ganzheitliche Ansicht aller erkannten Ressourcen, um Ihre Infrastruktur zu bewerten. Sie können auch Detailinformationen zu allen erkannten Ressourcen anzeigen. Zu verstehen, welche Ressourcen Ihre Organisation verwendet, ist ein wichtiger Schritt bei der Planung des Migrationsprozesses.

Vorbereitungen

Stellen Sie sicher, dass von Discovery die horizontale Erkennung für das relevante Segment Ihrer IT-Infrastruktur erfolgreich ausgeführt wurde.

Wenn Erkennungsanwendungen von Drittanbietern vorhanden sind, stellen Sie sicher, dass die erkannten Informationen von ihnen in die Configuration Management Database (CMDB) eingespeist wurden.

Erforderliche Rolle: sn_cloud_migration.operator

Warum und wann dieser Vorgang ausgeführt wird

Bewertung der Cloud-Migration baut auf den Informationen auf, die von Discovery gefunden und in der CMDB gespeichert werden. Außerdem werden von der Anwendung Probes dazu verwendet, die für den Cloud-Migrationsprozess erforderlichen Informationen zu erfassen. Von Bewertung der Cloud-Migration können die Informationen angezeigt werden, die von Erkennungsanwendungen von Drittanbietern gefunden werden. Wenn Ihre Organisation solche Anwendungen bereitstellt, erhalten Sie einen umfassenden Überblick über Ihre Infrastruktur.

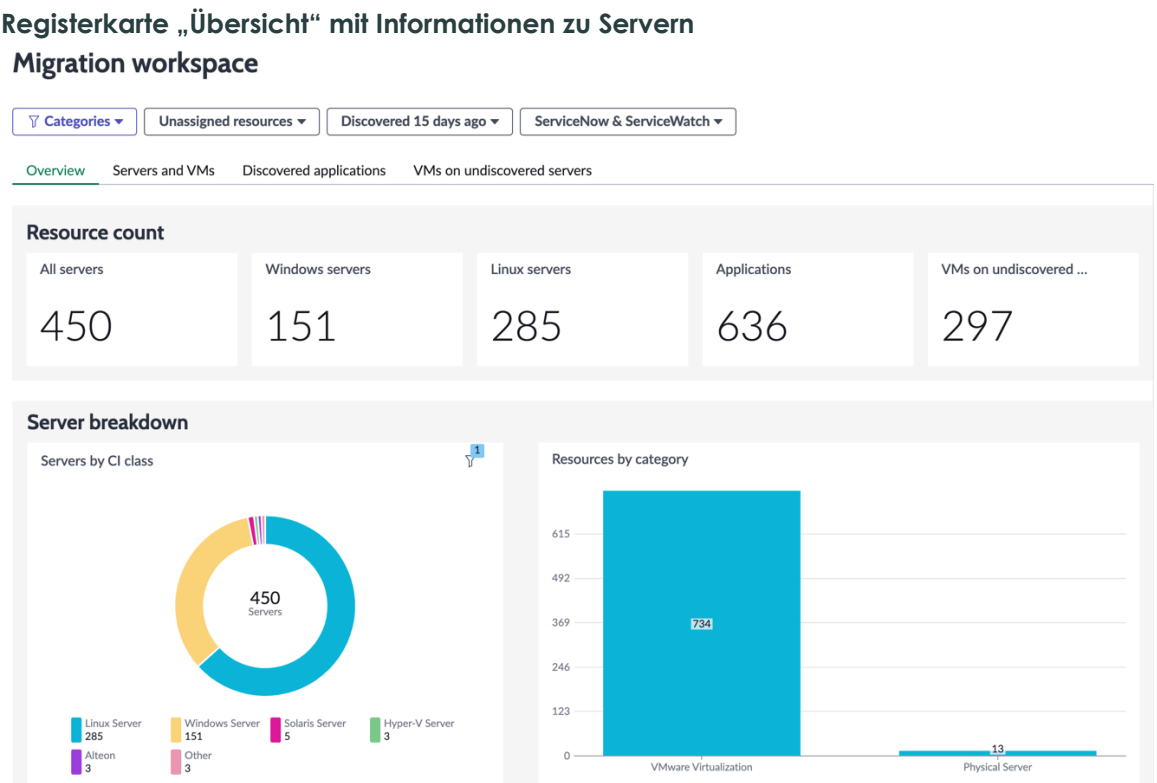
Sie können die Anzahl der bereitgestellten Server, Anwendungen und virtuellen Computer (Virtual Machine, VM) auf einen Blick sehen. Die Registerkarte „Übersicht“ zeigt Server nach Klasse.

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

Prozedur

1. Navigieren zu **Alle** > > **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration**.
2. Überprüfen Sie die Zusammenfassung der erkannten Ressourcen auf der Registerkarte **Übersicht**.

Registerkarte „Übersicht“ mit Informationen zu Servern



Standardmäßig werden auf der Registerkarte **Übersicht** nur die Kategorien angezeigt, für die Informationen erkannt wurden. Die Kategorie wird ausgeblendet, sofern keine zugehörigen Informationen zum Anzeigen vorhanden sind. Wenn beispielsweise keine erkannten Informationen zu Amazon AWS Cloud-Ressourcen vorhanden sind, wird die Kategorie AWS unter dem Filter **Kategorien** nicht angezeigt.

3. Wahlweise: Verwenden Sie Filter, um die relevanten Informationen auf der Registerkarte **Übersicht** anzuzeigen:

Filter	Beschreibung
Kategorien	
Alle Ressourcen	Ressourcen aller Kategorien
All on-premise resources (Alle lokalen Ressourcen)	Ressourcen, die lokal vorhanden sind, nicht in der Cloud
Physical server (Physischer Server)	Physische Server
Virtueller Server	Virtualisierungslösung: VMware-Virtualisierung, IBM HMC-Virtualisierung, HyperV-Virtualisierung, Hutanix-Virtualisierung, Solaris-Virtualisierung, Openstack-Virtualisierung
Cloud-Ressourcen	Ressourcen in der Cloud

Automatische Übersetzung

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

Filter	Beschreibung
AWS	Ressourcen in AWS
Azure	Ressourcen in Microsoft Azure Cloud
GCP	Ressourcen in Google Cloud Platform (GCP)
IBM	Ressourcen in IBM Cloud Platform
VMware Cloud	Ressourcen, die sich in Ihrer lokalen Umgebung befinden
Alle Ressourcen	Ressourcen, die Bewertungsaufgaben zugewiesen wurden und deren Zuweisung aufgehoben wurde
Nicht zugewiesene Ressourcen	Ressourcen, die nicht Bewertungsaufgaben zugewiesen sind
All discovered times (Alle erkannten Zeiten)	Ressourcen, die jederzeit erkannt wurden
Discovered 15 days ago (Vor 15 Tagen erkannt)	Vor 15 Tagen erkannte Ressourcen
Discovered 30 days ago (Vor 30 Tagen erkannt)	Vor 30 Tagen erkannte Ressourcen
All discovery sources (Alle Discovery-Quellen)	Ressourcen, die von Discovery und anderen mit der Now Platform® integrierten Erkennungstools von Drittanbietern erkannt wurden
ServiceNow & ServiceWatch	Von Discovery erkannte Ressourcen

Auf der Registerkarte **Übersicht** werden nur die Informationen angezeigt, die den von Ihnen ausgewählten Kategorien entsprechen. Alle Listen, auf die Sie zugreifen können, indem Sie andere Registerkarten und Kacheln auf dieser Seite auswählen, werden ebenfalls nach denselben Kategorien gefiltert. Wenn Sie beispielsweise unter **Kategorien** die Option **Physical servers** (Physische Server) ausgewählt haben, werden in der Liste auf der Registerkarte **Servers and VMs** (Server und VMs) nur physische Server angezeigt.

4. Wahlweise: Blenden Sie im Kreisdiagrammbericht **Server breakdown** (Serveraufgliederung) und im Balkendiagrammbericht **Resources by category** (Ressourcen nach Kategorie) irrelevante Server-CI-Klassen aus, indem Sie deren Namen in der Diagrammlegende auswählen.

Detaillierte Serverinformationen in Konfigurierbarer Arbeitsbereich überprüfen

Überprüfen Sie die Informationen zu den erkannten Ressourcen, um zu verstehen, wie sie in Ihrer aktuellen Infrastruktur bereitgestellt werden. Die Analyse und Bewertung Ihrer aktuellen Infrastruktur ist der erste Schritt im Cloud-Migrationsprozess.

Vorbereitungen

Erkennen Sie mit Discovery und Cloud-Discovery Ressourcen in Ihrer aktuellen Infrastruktur. Wenn Ihre Organisation andere Lösungen für die Erkennung verwendet, stellen Sie sicher, dass die erkannten Informationen in der CMDB verfügbar sind.

Erforderliche Rolle: sn_cloud_migration.operator

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

Warum und wann dieser Vorgang ausgeführt wird

Im Kontext der Bewertung der Cloud-Migration ist eine Ressource ein Server und ein virtueller Computer (Virtual Machine, VM), der diesen verwendet. Von Bewertung der Cloud-Migration werden Ressourcen identifiziert, indem erkannte Server und virtuelle Computer mit einer gegenseitigen Beziehung in der CMDB gesucht werden.

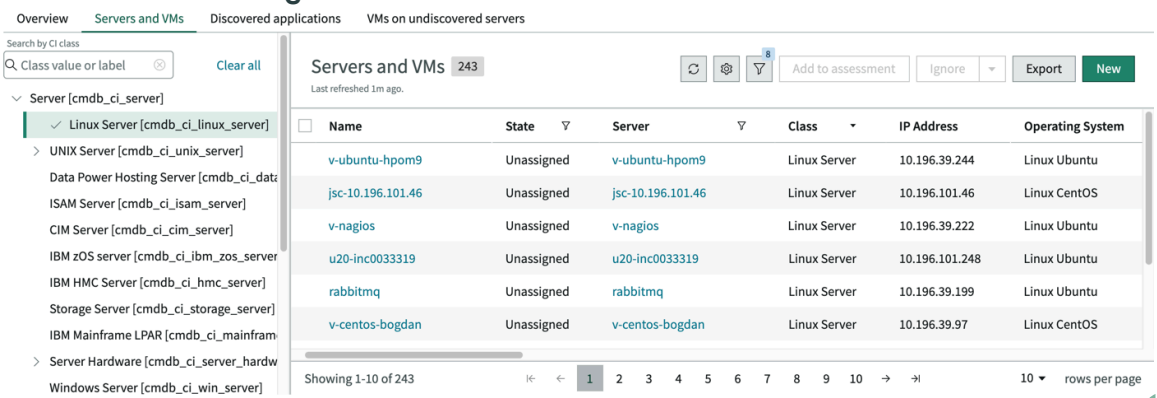
Prozedur

1. Navigieren zu **Alle** > > **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration**.
2. Wahlweise: Filtern Sie die Informationen im Fenster der Migrations-Flows, indem Sie die entsprechende Kategorie aus der Liste **Kategorien** auswählen.

   Example
   Wählen Sie beispielsweise **Physical Server** (Physischer Server) aus, um nur Informationen im Zusammenhang mit physischen Servern anzuzeigen. Alternativ können Sie **AWS** auswählen, um zu sehen, welche Ressourcen sich bereits in der Amazon AWS Cloud befinden.
   Alle Informationen im Fenster der Migration-Flows stimmen mit dem ausgewählten Filter überein.
3. Wählen Sie eine der Kacheln im Bereich **Server counts** (Serveranzahl) aus, um die Liste der Server anzuzeigen:
   - **Alle Server**
   - **Windows-Server**
   - **Linux-Server**

   Die Liste **Server and VMs** (Server und VMs) wird geöffnet und zeigt die Informationen, die entsprechend der im Fenster **Übersicht** ausgewählten Kategorie gefiltert wurden.

Gefilterte Liste der ausgeführten Server und VMs mit Linux



4. Wählen Sie den Servernamen in der Spalte **Server** aus.
   Die neue Registerkarte wird geöffnet und zeigt die erkannten Attribute für den ausgewählten Server an.
5. Wählen Sie den Ressourcennamen in der Spalte **Name** aus, um Details zu diesem Server und der darauf ausgeführten VM anzuzeigen.
   Die neu geöffnete Registerkarte zeigt die erkannten Attribute für die ausgewählte Ressource.
6. Wahlweise: Ändern Sie die Listenansicht oder exportieren Sie die Liste mithilfe der Listenschaltflächen.

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

Schaltfläche	Beschreibung
Liste neu laden	Aktualisiert die Liste, damit die neuesten Informationen angezeigt werden
Listenaktionen	Wählt Aktionen aus, die für diese Liste unterstützt werden: ◦ **Spalten bearbeiten** – Passt die Liste so an, dass die erforderlichen Spalten in der von Ihnen ausgewählten Reihenfolge angezeigt werden. ◦ **Speichern unter** – Erstellen Sie eine Kopie dieser Liste und speichern Sie sie unter **Meine Listen**. ◦ **Breiten zurücksetzen** – Setzt die Spaltenbreite auf den Standardwert zurück.
Filterbereich anzeigen	Zeigt den Filterbereich auf der rechten Seite an. Wenn Filter auf die Liste angewendet werden, enthält die Schaltfläche „Filter anzeigen“ die Anzahl der aktiven Filter.
Export	Speichert die Liste in einem der unterstützten Formate: Excel, CSV, JSON, PDF

7. Um eine Ressource auszublenden, die Sie aus keiner der Listen in Bewertung der Cloud-Migration migrieren möchten, wählen Sie diese Ressource aus und klicken Sie dann auf die Schaltfläche **Ignorieren**.

Zugehörige Informationen

Im Arbeitsbereich mit Listen arbeiten

Detaillierte Informationen zu virtuellen Computern in Konfigurierbarer Arbeitsbereich überprüfen

Überprüfen Sie die Informationen zu den erkannten virtuellen Computern (Virtual Machine, VM), um zu verstehen, wie sie in Ihrer aktuellen Infrastruktur bereitgestellt werden. Die Analyse und Bewertung Ihrer aktuellen Infrastruktur ist der erste Schritt im Cloud-Migrationsprozess.

Vorbereitungen

Erkennen Sie mit Discovery und Cloud-Discovery Ressourcen in Ihrer aktuellen Infrastruktur. Wenn Ihre Organisation andere Lösungen für die Erkennung verwendet, stellen Sie sicher, dass die erkannten Informationen in der CMDB verfügbar sind.

Erforderliche Rolle: sn_cloud_migration.operator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die horizontale Erkennung von Discovery verwenden, werden VMs zusammen mit ihren Beziehungen zu den Servern erkannt. Von Cloud-Discovery werden VMs ohne die zugehörigen Server gefunden.

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

Prozedur

1. Navigieren zu **Alle** > > **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration**.
2. Filtern Sie die Informationen im Fenster der Migrations-Flows, indem Sie die entsprechende Kategorie aus der Liste **Kategorien** auswählen.

   Example
   Wählen Sie beispielsweise **Physical Server** (Physischer Server) aus, um nur Informationen im Zusammenhang mit physischen Servern anzuzeigen. Alternativ können Sie **AWS** auswählen, um zu sehen, welche Ressourcen sich bereits in der Amazon AWS Cloud befinden.
   Alle Informationen im Fenster der Migration-Flows stimmen mit dem ausgewählten Filter überein.
3. Um die Informationen zu von Cloud-Discovery erkannten VMs zu überprüfen, wählen Sie die Kachel **VMs on undiscovered servers** (VMs auf nicht erkannten Servern) aus.
   Alternativ dazu können Sie VMs, die zusammen mit den zugehörigen Servern erkannt wurden, wie in Detaillierte Serverinformationen in Konfigurierbarer Arbeitsbereich überprüfen beschrieben überprüfen.
   Die Liste **VMs on undiscovered servers** (VMs auf nicht erkannten Servern) wird geöffnet und entsprechend der Kategorie gefiltert, die Sie im Fenster **Übersicht** ausgewählt haben.
4. Um eine Ressource auszublenden, die Sie aus keiner der Listen in Bewertung der Cloud-Migration migrieren möchten, wählen Sie diese Ressource aus und klicken Sie dann auf die Schaltfläche **Ignorieren**.
5. Wahlweise: Ändern Sie die Listenansicht oder exportieren Sie die Liste mithilfe der Listenschaltflächen.

Schaltfläche	Beschreibung
Liste neu laden	Aktualisiert die Liste, damit die neuesten Informationen angezeigt werden
Listenaktionen	Wählt Aktionen aus, die für diese Liste unterstützt werden: ◦ **Spalten bearbeiten** – Passt die Liste so an, dass die erforderlichen Spalten in der von Ihnen ausgewählten Reihenfolge angezeigt werden. ◦ **Speichern unter** – Erstellen Sie eine Kopie dieser Liste und speichern Sie sie unter **Meine Listen**. ◦ **Breiten zurücksetzen** – Setzt die Spaltenbreite auf den Standardwert zurück.
Filterbereich anzeigen	Zeigt den Filterbereich auf der rechten Seite an. Wenn Filter auf die Liste angewendet werden, enthält die Schaltfläche „Filter anzeigen“ die Anzahl der aktiven Filter.
Export	Speichert die Liste in einem der unterstützten Formate: Excel, CSV, JSON, PDF

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

Detaillierte Anwendungsinformationen in Konfigurierbarer Arbeitsbereich überprüfen

Überprüfen Sie die Informationen zu erkannten Anwendungen, um zu verstehen, wie sie in Ihrer aktuellen Infrastruktur bereitgestellt werden. Die Analyse und Bewertung Ihrer aktuellen Infrastruktur ist der erste Schritt im Cloud-Migrationsprozess.

Vorbereitungen

Erkennen Sie mit Discovery und Cloud-Discovery Ressourcen in Ihrer aktuellen Infrastruktur. Wenn Ihre Organisation andere Lösungen für die Erkennung verwendet, stellen Sie sicher, dass die erkannten Informationen in der CMDB verfügbar sind.

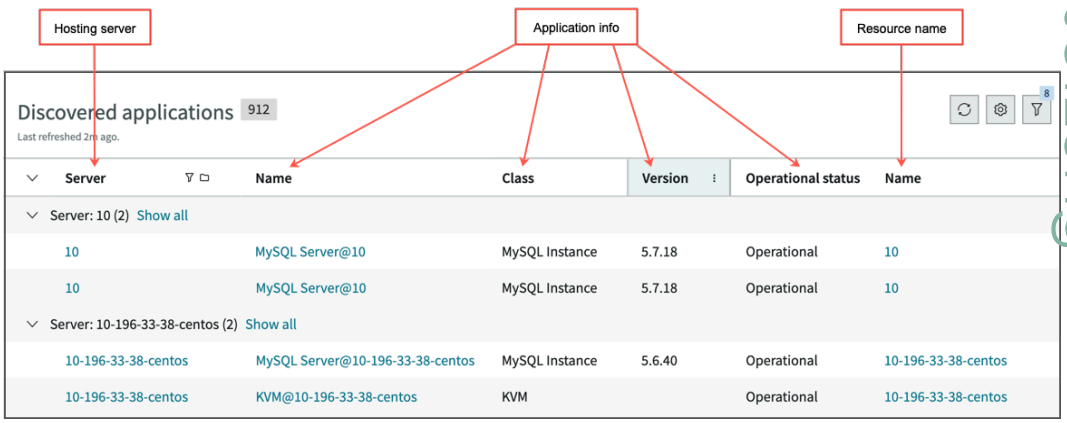
Erforderliche Rolle: cloud_migration_operator

Prozedur

1. Navigieren zu **Alle** > > **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration**.
2. Filtern Sie die Informationen im Fenster der Migrations-Flows, indem Sie die entsprechende Kategorie aus der Liste **Kategorien** auswählen.

   Example
   Wählen Sie beispielsweise **Physical Server** (Physischer Server) aus, um nur Informationen im Zusammenhang mit physischen Servern anzuzeigen. Alternativ können Sie **AWS** auswählen, um zu sehen, welche Ressourcen sich bereits in der Amazon AWS Cloud befinden.
   Alle Informationen im Fenster der Migration-Flows stimmen mit dem ausgewählten Filter überein.
3. Wählen Sie die Kachel **Anwendungen** aus.
   Die Liste **Discovered applications** (Erkannte Anwendungen) wird geöffnet und entsprechend der Kategorie gefiltert, die Sie im Fenster **Übersicht** ausgewählt haben.
   Ausführliche Informationen finden Sie unter Anwendungsliste in Bewertung der Cloud-Migration.

Erkannte Anwendungen, gefiltert nach der Kategorie „VMware-Virtualisierung“



4. Wahlweise: Bearbeiten Sie die Liste nach Bedarf mithilfe der Listenschaltflächen.

Schaltfläche	Beschreibung
Liste neu laden	Aktualisiert die Liste, damit die neuesten Informationen angezeigt werden

Automatische Übersetzung

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

Schaltfläche	Beschreibung
Listenaktionen	Wählt Aktionen aus, die für diese Liste unterstützt werden: ◦ **Spalten bearbeiten** – Passt die Liste so an, dass die erforderlichen Spalten in der von Ihnen ausgewählten Reihenfolge angezeigt werden. ◦ **Speichern unter** – Erstellen Sie eine Kopie dieser Liste und speichern Sie sie unter **Meine Listen**. ◦ **Breiten zurücksetzen** – Setzt die Spaltenbreite auf den Standardwert zurück.
Filterbereich anzeigen	Zeigt den Filterbereich auf der rechten Seite an. Wenn Filter auf die Liste angewendet werden, enthält die Schaltfläche „Filter anzeigen“ die Anzahl der aktiven Filter.

5. Wählen Sie den Anwendungsnamen aus, um detaillierte Informationen und Metriken für diese Anwendung zu überprüfen.
   Eine neue Registerkarte wird geöffnet und zeigt die Anwendungsinformationen an.
6. Wahlweise: Wählen Sie den Namen des Servers aus, um die Informationen zum Server anzuzeigen, auf dem die fragliche Anwendung ausgeführt wird.
7. Schließen Sie die Registerkarte.

Zugehörige Informationen

Im Arbeitsbereich mit Listen arbeiten

Migrationsstrategie auswählen

Nachdem Sie die aktuelle IT-Infrastruktur und die IT-Anforderungen Ihrer Organisation überprüft haben, betrachten Sie die Migrationsmethode und die Zielarchitektur.

- Wählen Sie die Art der Migration für verschiedene Ressourcen aus:

  Rehosting – „Lift and Shift“

  Sie hosten Ihre Anwendung mit einer anderen Hardwareumgebung neu, ohne die Anwendungsarchitektur zu ändern. Normalerweise eignet sich diese Strategie für große Legacy-Anwendungen oder Szenarien, in denen die Migration schnell und effektiv durchgeführt werden muss.

  Replatforming – „Lift, Tinker and Shift“

  Sie behalten die ursprüngliche Architektur der Anwendung bei, während Sie nur wenige Optimierungen vornehmen, um die Vorteile der Cloud-Infrastruktur zu nutzen. Replatforming kann länger dauern als Rehosting, eignet sich aber perfekt für Fälle, in denen Sie ein gewisses Maß an Kosteneffektivität, Funktionalität und Zeitersparnis ohne die erheblichen Ressourcenanforderungen des Refactoring benötigen.

  Retiring (Stilllegen)

  Sie verwenden einige Geräte oder Produkte in Ihrer aktuellen Infrastruktur nicht mehr. Sie könnten beispielsweise beschließen, veraltete Server oder Anwendungen mit wenigen Benutzern nicht zu migrieren.

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

Retaining (Beibehalten) – „Revisit“ (Erneut prüfen)

Migrationsstrategische Entscheidungen erfordern viel Überlegung und Forschung. In einigen Fällen möchten Sie die Entscheidung möglicherweise zurückstellen und später die wichtigsten oder problematischsten Aspekte Ihrer Infrastruktur erneut prüfen.

Refactoring – „Rearchitecturing“

Sie überprüfen und überarbeiten die Architektur der aktuellen Infrastruktur, um Cloud-Funktionen und -Flexibilität zu nutzen. Restrukturieren Sie Ihre Infrastruktur oder ihre Komponenten, um eine Skalierung, Leistung oder Agilität zu erreichen, die die Anwendung mit der vorhandenen Architektur nicht erreichen kann. Diese Strategie ist möglicherweise die teuerste, kann aber auch die perfekte Lösung sein, insbesondere wenn Ihr Ziel eine serviceorientierte Infrastruktur ist.

Repurchasing (Neukauf) – „Drop and Shop“

Sie wechseln von Ihrer aktuellen Anwendung zu einem Service oder einer Appliance, den/die der Cloud Provider anbietet. In einigen Fällen ist es einfacher und profitabler, ein neues Cloud-Produkt zu verwenden, anstatt in die Migration eines alten zu investieren. Dies ist der Fall, wenn Ihre Organisation über selbst entwickelte Produkte oder eine branchenspezifische Anwendung verfügt, die nicht für Cloud-Infrastrukturen geeignet ist.

- Abhängig von den Anforderungen Ihres Unternehmens können Sie alle Ihre IT-Ressourcen auf dieselbe Cloud-Plattform verschieben oder mehrere Plattformen verwenden. Treffen Sie Entscheidungen zur Zielarchitektur für verschiedene Ressourcen:

  IaaS

  Mit Infrastructure-as-a-Service wird nur eine grundlegende Infrastruktur bereitgestellt, die virtuelle Computer (Virtual Machines, VMs), Software Defined Network (SDN) und Network-Attached Storage (NAS) umfasst.

  SaaS

  Software-as-a-Service wird auch als On-Demand-Software bezeichnet. Cloud-Anbieter verwalten Anwendungen und stellen den Kunden Anwendungen über einen Webbrowser bereit.

  PaaS

  Platform-as-a-Service bietet eine Plattform, mit der Kunden ihre Anwendungen bereitstellen und ausführen können, ohne die Infrastruktur verwalten zu müssen.

  Hybrid

  In einer Hybridlösung befindet sich die IT-Infrastruktur in einer Public Cloud, während einige Ressourcen weiterhin lokal und in Private Cloud Workloads unterstützt und ausgeführt werden.

  Service Portal-Container

  Container-as-a-Service ist eine containerbasierte Virtualisierung. Cloud-Anbieter verwenden diesen Typ, um den Kunden containerbezogene Komponenten bereitzustellen: Container Engines, Orchestrierung und die zugrunde liegenden Rechenressourcen.

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

- Legen Sie Ihre Ziele und den Zeitrahmen fest. Für Migrationswellen in Bewertung der Cloud-Migration werden Geschäftsquartale verwendet.
- Identifizieren Sie Personengruppen und Einzelpersonen, die direkt für bestimmte Migrationsaufgaben verantwortlich sind, und solche innerhalb Ihres Unternehmens und auf Seiten des Cloud-Providers, die benachrichtigt werden müssen.

Bewertungsaufgaben für die Cloud-Migration in Konfigurierbarer Arbeitsbereich erstellen

Erstellen Sie Bewertungsaufgaben und verknüpfen Sie sie mit Migrationswellen für das Migrationsmanagement.

Vorbereitungen
Erforderliche Rolle: sn_cloud_migration.operator.

Prozedur

1. Navigieren zu **Alle** > > **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration**.
2. Wählen Sie das **Bewertungs-Dashboard** und dann **Bewertung erstellen** aus.

   Alternativ können Sie **Listen** wählen und zu navigieren**Bewertungsaufgaben** > **Aufgaben**und wählen Sie **Neu**.
3. Füllen Sie die Werte im Formular „Create New Cloud Migration Assessment Task“ (Neue Bewertungsaufgabe für Cloud-Migration erstellen) aus.
4. Wahlweise: Anhänge hinzufügen

   a. Wählen Sie im Abschnitt **Anhänge** die Option **Durchsuchen** aus.

   b. Navigieren Sie zu einer Datei und wählen Sie sie aus.

   c. Wählen Sie **Hochladen** aus.
   Die angehängte Datei wird unter „Anhänge“ angezeigt.
5. Wählen Sie **Speichern**.

Nächste Maßnahme
Bewertungsaufgaben in Konfigurierbarer Arbeitsbereich Ressourcen zuweisen

Bewertungsaufgaben in Konfigurierbarer Arbeitsbereich Ressourcen zuweisen

Sobald Sie geplant haben, wie Ressourcen in die Cloud migriert werden, können Sie die Ressourcen Bewertungsaufgaben zuweisen.

Vorbereitungen
Erforderliche Rolle: sn_cloud_migration.operator

Warum und wann dieser Vorgang ausgeführt wird
Ressourcen können nur zu einer einzigen Bewertungsaufgabe gehören.

Da Anwendungen von den Servern abhängen, auf denen sie gehostet werden, können Sie nur die Hostserver Bewertungsaufgaben zuweisen.

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

Prozedur

1. Aktivieren Sie in einer Ressourcenliste ein Kontrollkästchen neben der Ressource, die Sie einer Bewertungsaufgabe hinzufügen möchten.
   Auf der Schaltfläche **Add to assessment** (Zu Bewertung hinzufügen) wird die Anzahl der ausgewählten Ressourcen angezeigt.
2. Wählen Sie **Add to assessment** (Zu Bewertung hinzufügen) aus.
   Das Dialogfeld **Assign a resource to an assessment task** (Ressource einer Bewertungsaufgabe zuweisen) wird geöffnet.
3. Führen Sie einen der folgenden Schritte aus:
   - Um die Ressource einer vorhandenen Aufgabe hinzuzufügen, wählen Sie den entsprechenden Aufgabenlink in der Spalte **Nummer** aus und wählen Sie **Add to CAS** (Zu CAS hinzufügen) aus.
   - Um die Ressource einer neuen Aufgabe hinzuzufügen, wählen Sie **Bewertung erstellen** aus.

   Vom System wird die ausgewählte Ressource der Bewertungsaufgabe hinzugefügt. Die Bewertungsaufgabe wird auf einer neuen Registerkarte angezeigt.

Zugehörige Informationen

Bewertungsaufgaben für die Cloud-Migration in Konfigurierbarer Arbeitsbereich erstellen

Mit Bewertungsaufgaben in Konfigurierbarer Arbeitsbereich verknüpfte Anwendungen überprüfen

Verstehen Sie die Softwareanforderungen für Ressourcen, die Bewertungsaufgaben zugewiesen sind. Die meisten Ressourcen hosten Anwendungen. Überprüfen Sie die Aufgabenliste, die gefiltert ist, um anwendungsbezogene Informationen anzuzeigen.

Vorbereitungen

Erforderliche Rolle: sn_cloud_migration.operator

Prozedur

1. Navigieren zu **Alle** > > **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration**.
2. Wählen Sie **Listen**, navigieren Sie zu **Anwendungen** > **Softwareanforderungen**.
3. Überprüfen Sie die Informationen in der Liste der Softwareanforderungen.
4. Wahlweise: Wählen Sie Schaltflächen über der Liste für zusätzliche Aktionen aus.

Schaltfläche	Aktion
Liste neu laden	Aktualisiert die Liste, damit die neuesten Informationen angezeigt werden
Listenaktionen	Wählt Aktionen aus, die für diese Liste unterstützt werden: ◦ **Spalten bearbeiten** – Passt die Liste so an, dass die erforderlichen Spalten in der von Ihnen ausgewählten Reihenfolge angezeigt werden.

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

Schaltfläche	Aktion
	◦ **Speichern unter** – Erstellen Sie eine Kopie dieser Liste und speichern Sie sie unter **Meine Listen**. ◦ **Breiten zurücksetzen** – Setzt die Spaltenbreite auf den Standardwert zurück.
URL kopieren	Kopiert die URL für diese Liste
Filterbereich anzeigen	Zeigt den Filterbereich auf der rechten Seite an. Wenn Filter auf die Liste angewendet werden, enthält die Schaltfläche „Filter anzeigen“ die Anzahl der aktiven Filter.
Export	Speichert die Liste in einem der unterstützten Formate: Excel, CSV, JSON, PDF

5. Um detaillierte Informationen zur Bewertungsaufgabe anzuzeigen, wählen Sie den entsprechenden Link in der Spalte „Bewertungsaufgabe“ aus.
   Das Formular „Bewertungsaufgabe“ wird geöffnet.

Fortschritt der Cloud-Migration in Konfigurierbarer Arbeitsbereich überwachen

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

Vorbereitungen
Erforderliche Rolle: sn_cloud_migration.operator

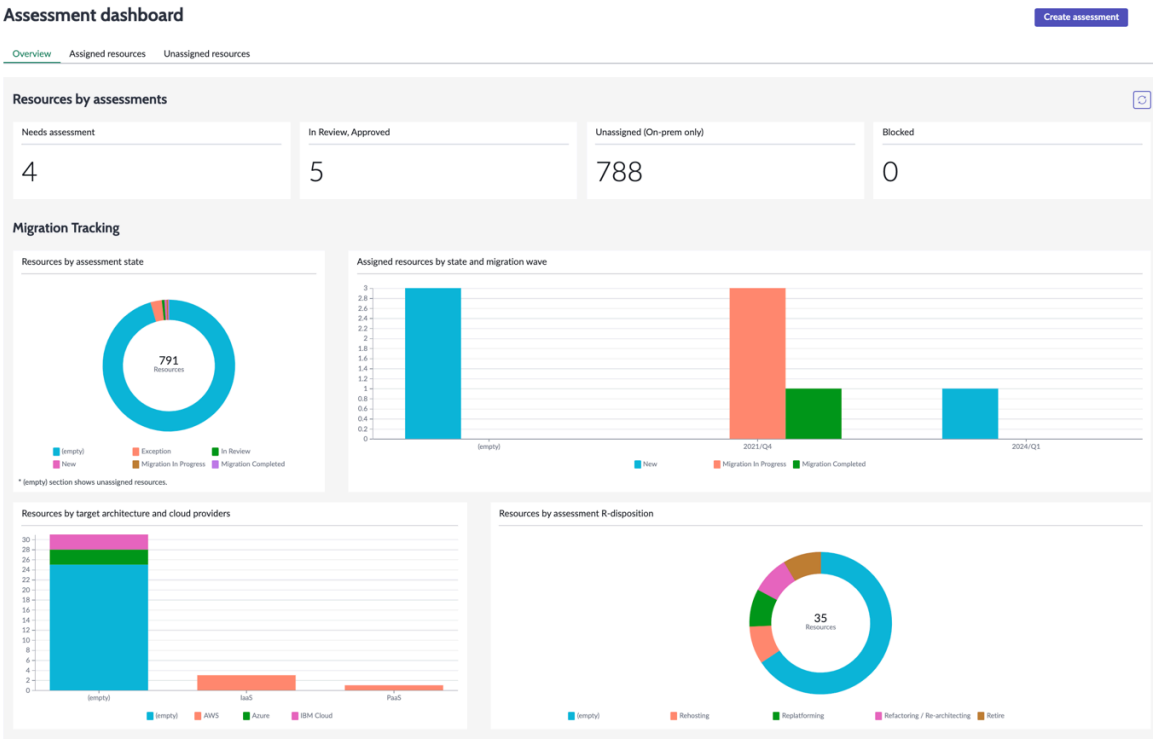
Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > > **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration**.
2. Wählen Sie das **Assessment Dashboard (Bewertungs-Dashboard)** aus.

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

3. Überprüfen Sie die Fortschrittsstatistiken anhand der Indikatoren und Berichte im Dashboard, wie unter Assessment Dashboard (Bewertungs-Dashboard) in Konfigurierbarer Arbeitsbereich von Bewertung der Cloud-Migration beschrieben.



Bewertung der Cloud-Migration-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Zuordnen und Optimieren von Anwendungsservices mithilfe von Bewertung der Cloud-Migration-Listen und -Formularen.

Mit Bewertung der Cloud-Migration installierte Komponenten

Bei Aktivierung des Bewertung der Cloud-Migration-Plugins werden mehrere Arten von Komponenten installiert, zum Beispiel Tabellen, Benutzerrollen und regelmäßige Aufgaben.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
sn_cloud_migration.admin	Konfiguriert erweiterte Parameter, um das Standardverhalten von Bewertung der Cloud-Migration anzupassen.	cloud_migration_operator
sn_cloud_migration.operator	Überprüft die Informationen zu den erkannten IT-Ressourcen, weist diese Ressourcen Bewertungsaufgaben zu und verfolgt den Migrationsfortschritt.	itil, canvas_user

Automatische Übersetzung

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

Regelmäßige Aufgaben installiert

Regelmäßige Aufgabe	Beschreibung
Cloud Migration – Populate Resources (Cloud-Migration – Ressourcen ausfüllen)	Wird täglich ausgeführt Füllt die Tabelle „Migrationsressource“ [sn_cloud_migration_resource] mit Informationen zu Servern und virtuellen Computern.
Cloud Migration – Update Application Counters (Cloud-Migration – Anwendungszähler aktualisieren)	Wird bei Bedarf ausgeführt. Aktualisiert die Anwendungsanzahl jeder Ressource um die Anzahl der Anwendungen, die auf jeder Ressource ausgeführt werden.
Cloud Migration Assessment-Lizenzierung – Verwendungsanzahl	Wird täglich ausgeführt Zählt alle Ressourcen in der Anwendung Bewertung der Cloud-Migration, die einer Aufgabe zugewiesen sind. Von der Anwendung ServiceNow® ITOM SU Licensing werden diese Informationen zum Zählen von lizenzierbaren CIs verwendet.

Installierte Tabellen

Tabelle	Beschreibung
Metrik der Migrations-VM [sn_cloud_migration_vm_metrics]	Enthält die Informationen zu virtuellen Maschinen und deren Metriken, die für die Bewertung der IT-Infrastruktur erforderlich sind.
Software Requirement for Migration [sn_cloud_migration_software_requirement] (Softwareanforderung für Migration)	Enthält die Liste der Anwendungen, die auf Servern ausgeführt werden, die Bewertungsaufgaben zugewiesen sind.
Cloud Migration Assessment Task [sn_cloud_migration_task] (Bewertungsaufgabe für Cloud-Migration)	Enthält die Informationen zu einer Migrationsaufgabe für Ressourcen, die für die Migration in die Cloud vorgesehen sind.
Base Migration Assessment Task [sn_cloud_migration_task_base] (Bewertungsaufgabe für Basismigration)	Dient als Basistabelle für verschiedene Migrationsaufgaben, die diese Tabelle erweitern.
Assigned Resource for Migration [sn_cloud_migration_task_resource_m2m] (Zugewiesene Ressource für Migration)	Enthält Informationen über die Zuweisung von Ressourcen zu Aufgaben.
Migration Resource [sn_cloud_migration_resource] (Migrationsressource)	Enthält die Informationen zu virtuellen Computern, Servern sowie Servern und virtuellen Computern, die zusammen mit den Servern erkannt wurden.
Migration Wave [sn_cloud_migration_wave] (Migrationswelle)	Sammelt die Bewertungsaufgaben und Migrationswellen.
Governance-Lizenzierung für Cloud Migration Assessment [itom_lu_cloud_migration_assessment_ci]	Enthält lizenzierbare CIs für Bewertung der Cloud-Migration.

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

Installierte Eigenschaften

Hinweis: Um die Tabelle „Systemeigenschaft“ [sys_properties] zu öffnen, geben Sie im Navigationsfilter `sys_properties.list` ein.

Eigenschaft	Beschreibung
sn_cloud_migration.os.exclusion_list	Kommagetrennte Deny-Liste von Betriebssystemen. Server, deren Betriebssystem hier aufgeführt ist, werden vom Migrationsprozess ausgeschlossen. • **Typ**: Zeichenfolge • **Standardwert**: ESX, Windows XP, Windows 7 Enterprise, Windows 7 Ultimate, Windows 10 Enterprise 2016 LTSB. • **Standort**: **Cloud-Migration** > **Administration** > **Eigenschaften**.
sn_cloud_migration.vm_state.inclusion_list	Kommagetrennte Allow-Liste von VM-Instanzstatus für Bewertung der Cloud-Migration. Am Migrationsprozess können nur Server mit einem hier aufgeführten Installationsstatus teilnehmen. • **Typ**: Zeichenfolge • **Andere mögliche Werte**: Ein, Aus, Angehalten, Geplant, Wird gestartet, Wird gestoppt, Stillgelegt, Beendet, Fehler, Abgebrochen, Wird angehalten, Wird beendet. • **Standardwert**: Ein • **Standort**: **Cloud-Migration** > **Administration** > **Eigenschaften**
sn_cloud_migration.server_status.inclusion_list	Kommagetrennte Allow-Liste des Serverstatus für Bewertung der Cloud-Migration. Am Migrationsprozess können nur Server mit einem hier aufgeführten Installationsstatus teilnehmen. • **Typ**: Zeichenfolge • **Standardwert**: 1 • **Andere mögliche Werte**: Installiert = 1, Bestellt = 2, In Wartung = 3, Ausstehende Installation = 4, Ausstehende Reparatur = 5, Auf Lager = 6, Stillgelegt = 7, Gestohlen = 8, Abwesend = 100. • **Standort**: **Cloud-Migration** > **Administration** > **Eigenschaften**

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

Eigenschaft	Beschreibung
sn_cloud_migration.categories.inclusion_list	Kommagetrennte Allow-Liste von Kategorien für Bewertung der Cloud-Migration. Am Migrationsprozess können nur Ressourcen teilnehmen, die hier aufgelisteten Kategorien zugewiesen sind. • **Typ**: Zeichenfolge • **Standardwert**: Physisch, VMware, HyperV, IBM HMC, OpenStack, Solaris, Nutanix, Amazon AWS, Microsoft Azure, Google Cloud, IBM Cloud • **Standort**: **Cloud-Migration** > **Administration** > **Eigenschaften**

Zusätzlich zu den aufgeführten Komponenten enthält Bewertung der Cloud-Migration die folgende VMware-Probe: VMWare – vCenter VM Performance. Weitere Informationen finden Sie unter vCenter-Probes und Probe-Parameter.

Assessment Dashboard (Bewertungs-Dashboard) in Konfigurierbarer Arbeitsbereich von Bewertung der Cloud-Migration

Verwenden Sie die Anwendung ServiceNow® Bewertung der Cloud-Migration, um den Prozess der Verlagerung von IT-Ressourcen und Arbeitslasten Ihres Unternehmens auf Cloud-Plattformen zu planen, zu organisieren und nachzuverfolgen. Analysieren Sie die IT-Ressourcen mithilfe von Dashboards, in denen Informationen zu Ressourcen nach verschiedenen Kategorien visualisiert und zusammengefasst werden. Verwenden Sie das Assessment Dashboard (Bewertungs-Dashboard), um die Statistiken der Migrationsaufgaben zu überprüfen und den Migrationsfortschritt zu überwachen.

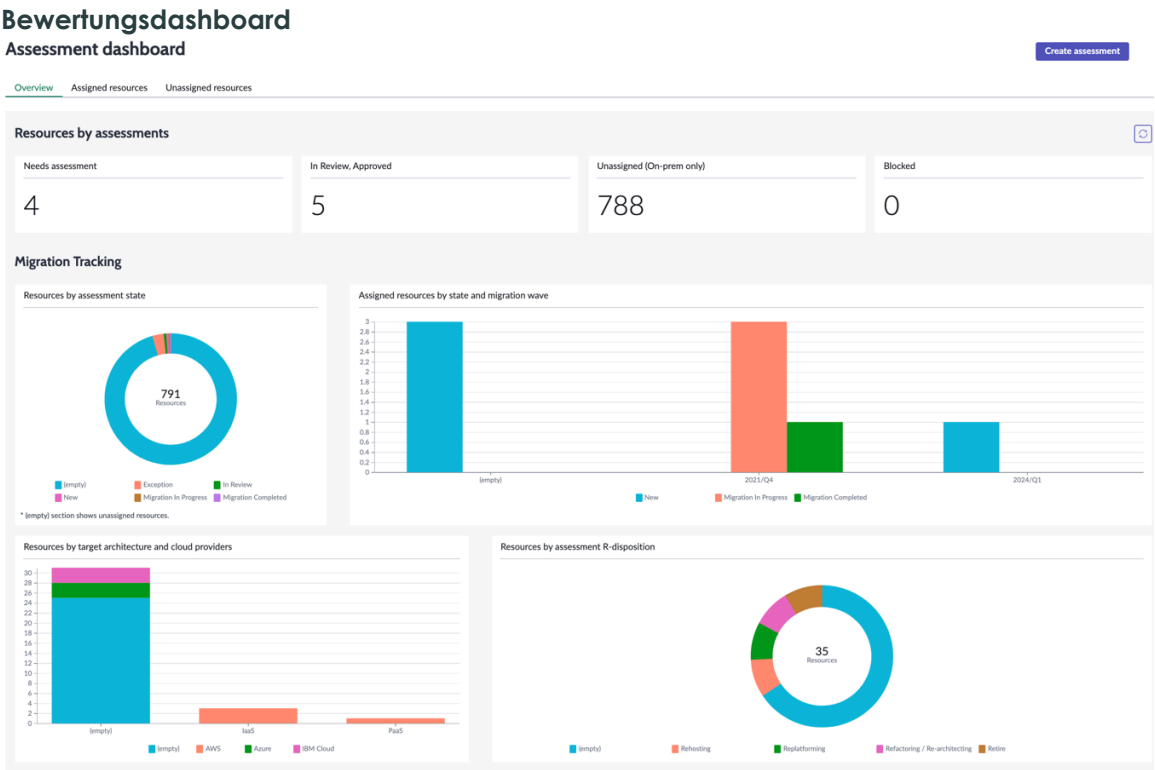
Erforderliche Now Platform-Rollen

sn_cloud_migration.operator, verwendet Bewertung der Cloud-Migration.

Bewertungs-Dashboard aufrufen

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > > **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration**und wählen Sie dann **Bewertungs-Dashboard** .

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



Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
sn_cloud_migration.operator	Überprüfen Sie die Statistiken der Migrationsaufgaben und überwachen Sie den Migrationsfortschritt. Zeigen Sie Detailinformationen für Ressourcen in relevanten Kategorien an.

Indikatoren

Ressourcen in neuen Bewertungen

Die Ressourcen aller Kategorien, die Bewertungsaufgaben im Status **Neu** zugewiesen sind

Ressourcen in der Überprüfung und genehmigte Ressourcen

Die Ressourcen aller Kategorien, die Aufgaben im Status **Prüfung** oder **Genehmigt** zugewiesen sind

Nicht zugewiesene lokale Ressourcen

Die Ressourcen, die Sie keinen Bewertungsaufgaben zugewiesen haben

Blockierte Ressourcen

Die Ressourcen aller Kategorien, die Aufgaben im Status **Blockiert** zugewiesen sind

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

Datenvisualisierungen

Die folgenden Visualisierungen sind auf der Registerkarte Übersicht von Bewertung der Cloud-Migrationverfügbar.

Titel	Typ	Quelltabelle	Beschreibung
Ressourcen nach Bewertungsstatus		Assigned Resource for Migration [sn_cloud_migration_task_resource_m2m] (Zugewiesene Ressource für Migration)	Ein Ring-Bericht, in dem Ressourcen nach ihrem Bewertungsaufgabenstatus angezeigt werden
Zugewiesene Ressourcen nach Status und Migrationswelle	Balken	Assigned Resource for Migration [sn_cloud_migration_task_resource_m2m] (Zugewiesene Ressource für Migration)	Ein Balkenbericht, in dem Ressourcen nach Status und Migrationswelle dargestellt werden
Ressourcen nach Zielarchitektur und Cloud-Anbieter	Balken	Assigned Resource for Migration [sn_cloud_migration_task_resource_m2m] (Zugewiesene Ressource für Migration)	Ein Balkenbericht, in dem Ressourcen nach Zielarchitektur und Cloud Provider dargestellt werden
Ressourcen nach R-Disposition für Bewertung		Assigned Resource for Migration [sn_cloud_migration_task_resource_m2m] (Zugewiesene Ressource für Migration)	Ein Ring-Bericht, in dem Ressourcen nach ihre jeweiligen Bewertungen ausgewählten Migrationsstrategie (R-Disposition) angezeigt werden

Formular „Bewertungsaufgabe“ in Konfigurierbarer Arbeitsbereich

Das Formular zum Erstellen oder Ändern einer Bewertung der Cloud-Migration-Bewertungsaufgabe zeigt detaillierte Informationen zur Bewertung an.

Tab „Details“

Geben Sie die Informationen auf der Registerkarte „Details“ ein, um eine Bewertungsaufgabe zu erstellen oder zu ändern.

Registerkarte „Details“ des Bewertung der Cloud-Migration-Formulars „Bewertungsaufgabe“

Feld	Beschreibung
Abschnitt „Bewertung“	
Nummer	Der eindeutige Name der Bewertungsaufgabe

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

Registerkarte „Details“ des Bewertung der Cloud-Migration-Formulars „Bewertungsaufgabe“ (Fortsetzung)

Feld	Beschreibung
Zugewiesen an	Der Benutzer, der direkt für die Migration von Ressourcen verantwortlich ist, die dieser Aufgabe zugeordnet sind
Zuweisungsgruppe	Die Benutzergruppe, der die Bewertungsaufgabe zugewiesen ist
Erstellt von	Der Benutzer, der diese Bewertungsaufgabe erstellt hat
List of Contacts (Liste der Kontakte)	Die Personen innerhalb und außerhalb Ihrer Organisation, die benachrichtigt werden müssen. Vom System werden automatische Benachrichtigungen gesendet, wenn diese Aufgabe erstellt oder aktualisiert wird.
Migration Start Date (Startdatum der Migration)	Datum, an dem mit der Migration der dieser Bewertungsaufgabe zugewiesenen Ressourcen begonnen wird
Migration Completion Date (Abschlussdatum der Migration)	Das Datum, an dem die Migration der dieser Bewertungsaufgabe zugewiesenen Ressourcen abgeschlossen sein soll
Erstellt	Das Erstellungsdatum der Bewertungsaufgabe
Aktualisiert	Das Änderungsdatum der Bewertungsaufgabe
Status	Der Status der Bewertungsaufgabe: • Neu • Wird überprüft • Genehmigt • Ausnahme • Migration wird ausgeführt • Migration abgeschlossen
Target Cloud Provider (Ziel-Cloud-Provider)	Der Cloud Provider, der Ressourcen hostet, die dieser Bewertungsaufgabe nach Abschluss der Migration zugewiesen sind
Target Architecture (Zielarchitektur)	Die Cloud-Servicemodelle, die für die Migration von Ressourcen verwendet werden, die dieser Bewertungsaufgabe zugewiesen sind: IaaS, PaaS, Hybrid (IaaS und PaaS), Container und SaaS
Dringlichkeit	Die Dringlichkeitsstufe: hoch, mittel oder niedrig
R-Disposition	Der Migrationstyp:

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

Registerkarte „Details“ des Bewertung der Cloud-Migration-Formulars „Bewertungsaufgabe“ (Fortsetzung)

Feld	Beschreibung
	Rehosting – „Lift and Shift“ Sie hosten Ihre Anwendung mit einer anderen Hardwareumgebung neu, ohne die Anwendungsarchitektur zu ändern. Normalerweise eignet sich diese Strategie für große Legacy-Anwendungen oder Szenarien, in denen die Migration schnell und effektiv durchgeführt werden muss. Replatforming – „Lift, Tinker and Shift“ Sie behalten die ursprüngliche Architektur der Anwendung bei, während Sie nur wenige Optimierungen vornehmen, um die Vorteile der Cloud-Infrastruktur zu nutzen. Replatforming kann länger dauern als Rehosting, eignet sich aber perfekt für Fälle, in denen Sie ein gewisses Maß an Kosteneffektivität, Funktionalität und Zeitersparnis ohne die erheblichen Ressourcenanforderungen des Refactoring benötigen. Retiring (Stilllegen) Sie verwenden einige Geräte oder Produkte in Ihrer aktuellen Infrastruktur nicht mehr. Sie könnten beispielsweise beschließen, veraltete Server oder Anwendungen mit wenigen Benutzern nicht zu migrieren. Retaining (Beibehalten) – „Revisit“ (Erneut prüfen) Migrationsstrategische Entscheidungen erfordern viel Überlegung und Forschung. In einigen Fällen möchten Sie die Entscheidung möglicherweise zurückstellen und später die wichtigsten oder problematischsten Aspekte Ihrer Infrastruktur erneut prüfen. Refactoring – „Rearchitecturing“

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

Registerkarte „Details“ des Bewertung der Cloud-Migration-Formulars „Bewertungsaufgabe“ (Fortsetzung)

Feld	Beschreibung
	Sie überprüfen und überarbeiten die Architektur der aktuellen Infrastruktur, um Cloud-Funktionen und -Flexibilität zu nutzen. Restrukturieren Sie Ihre Infrastruktur oder ihre Komponenten, um eine Skalierung, Leistung oder Agilität zu erreichen, die die Anwendung mit der vorhandenen Architektur nicht erreichen kann. Diese Strategie ist möglicherweise die teuerste, kann aber auch die perfekte Lösung sein, insbesondere wenn Ihr Ziel eine serviceorientierte Infrastruktur ist. Repurchasing (Neukauf) – „Drop and Shop“ Sie wechseln von Ihrer aktuellen Anwendung zu einem Service oder einer Appliance, den/die der Cloud Provider anbietet. In einigen Fällen ist es einfacher und profitabler, ein neues Cloud-Produkt zu verwenden, anstatt in die Migration eines alten zu investieren. Dies ist der Fall, wenn Ihre Organisation über selbst entwickelte Produkte oder eine branchenspezifische Anwendung verfügt, die nicht für Cloud-Infrastrukturen geeignet ist.
Migration wave (Migrationswelle)	Die Migrationswelle, die diese Bewertungsaufgabe enthält. Migrationswellen sind mit Bewertung der Cloud-Migration vorkonfiguriert.
Kurzbeschreibung	Die Kurzbeschreibung dieser Bewertungsaufgabe
Beschreibung	Die Beschreibung dieser Bewertungsaufgabe
Abschnitt „Notizen“	
Beobachtungsliste	Die Beobachtungsliste für diese Bewertungsaufgabe
Beobachtungsliste Arbeitshinweisen	Die Kommentare im Freitext

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

Registerkarte „Details“ des Bewertung der Cloud-Migration-Formulars „Bewertungsaufgabe“ (Fortsetzung)

Feld	Beschreibung
Zusätzliche Kommentare (sichtbar für Kunden)	Die Kommentare im Zusammenhang mit dieser Bewertungsaufgabe
Arbeitsnotizen (privat)	Die zugehörigen Arbeitsnotizen, die für Kunden nicht sichtbar sind

Serverliste in Bewertung der Cloud-Migration

Bewertung der Cloud-Migration stellt Informationen zu Serverressourcen in mehreren Listen dar: Alle Server, Windows-Server und Linux-Server.

In der Serverliste in Bewertung der Cloud-Migration verfügbare Informationen

Spalte (von links nach rechts)	Beschreibung
Name	Der Name der Ressource: Der Server oder der Server zusammen mit seiner VM.
Server	Der Servername.
IP-Adresse	Die IP-Adresse des Servers.
Betriebssystem	Das Betriebssystem des Servers.
Hersteller	Der Hersteller des Servers.
Discovery-Quelle	Die Anwendung, die den Server erkannt hat: • ServiceNow – horizontale Erkennung durch Discovery. • ServiceWatch – Erkennung von oben nach unten durch Service-Mapping. • Andere Optionen, wenn Anwendungen von Drittanbietern bereitgestellt werden.
CPU-Anzahl	Die Anzahl der Server-CPUs.
Cluster	Der Name des Clusters, der den Server enthält.
Status	Die Serverzuweisung: • Zugewiesen – Der Server ist einer Bewertungsaufgabe zugewiesen. • Nicht zugewiesen – Der Server ist keiner Bewertungsaufgabe zugewiesen. • Ignoriert – Der Server wird in den Listen ausgeblendet.
IT-Umgebung	Die aktuelle IT-Umgebung, die diesen Server enthält:

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

Spalte (von links nach rechts)	Beschreibung
	• Vor Ort • Cloud
Kategorie	Die Serverkategorie: • Physischer Server • VMware-Virtualisierung • Hyper-V-Virtualisierung • IBM HMC-Virtualisierung • OpenStack-Virtualisierung • Solaris-Virtualisierung • Nutanix-Virtualisierung • AWS • Microsoft Azure • Google Cloud • IBM Cloud
VM-Instanz	Die VM-Instanz, die auf dem Server registriert ist.
IP-Adresse	IP-Adresse der VM-Instanz.
Hersteller	Der Hersteller der VM.
CPUs	Die Anzahl der VM-Instanz-CPUs.
Arbeitsspeicher (MB)	Die Größe des Serverspeichers.

Listenaktionen

Schaltfläche	Aktion
Liste neu laden	Aktualisiert die Liste, damit die neuesten Informationen angezeigt werden
Listenaktionen	Wählt Aktionen aus, die für diese Liste unterstützt werden: • **Spalten bearbeiten** – Passt die Liste so an, dass die erforderlichen Spalten in der von Ihnen ausgewählten Reihenfolge angezeigt werden.

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

Schaltfläche	Aktion
	• **Speichern unter** – Erstellen Sie eine Kopie dieser Liste und speichern Sie sie unter **Meine Listen**. • **Breiten zurücksetzen** – Setzt die Spaltenbreite auf den Standardwert zurück.
URL kopieren	Kopiert die URL für diese Liste
Filterbereich anzeigen	Zeigt den Filterbereich auf der rechten Seite an. Wenn Filter auf die Liste angewendet werden, enthält die Schaltfläche „Filter anzeigen“ die Anzahl der aktiven Filter.
Export	Speichert die Liste in einem der unterstützten Formate: Excel, CSV, JSON, PDF

Zugehörige Informationen

Bewertungsaufgaben in Konfigurierbarer Arbeitsbereich Ressourcen zuweisen

Bewertungsaufgaben für die Cloud-Migration in Konfigurierbarer Arbeitsbereich erstellen

Detaillierte Serverinformationen in Konfigurierbarer Arbeitsbereich überprüfen

Anwendungsliste in Bewertung der Cloud-Migration

Bewertung der Cloud-Migration enthält Informationen zu Anwendungsressourcen in den folgenden Listen: „Anwendungen“ und „Erkannte Anwendungen“.

In den Listen „Anwendungen“ und „Erkannte Anwendungen“ verfügbare Informationen

Spalten (von links nach rechts)	Beschreibung
Server	Die Bezeichnung des Servers, auf dem die Anwendung gehostet wird.
Name	Der Anwendungsname.
Klasse	Die Anwendungsklasse.
Version	Die Anwendungsversion.
Betriebsstatus	Der Betriebsstatus der Anwendung: • Operativ • Nicht funktionsfähig • Reparatur in Bearbeitung • DR-Standby • Bereit • Stillgelegt

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

Spalten (von links nach rechts)	Beschreibung
Name	Der Name des Servers, auf dem die Anwendung gehostet wird.
Cluster	Der Name des Clusters, in dem sich der Server befindet. Dieses Feld ist in der Liste „Anwendungen“ verfügbar.
IT-Umgebung	Die aktuelle IT-Umgebung, in der die Anwendung bereitgestellt wird: vor Ort oder Cloud. Dieses Feld ist in der Liste „Anwendungen“ verfügbar.
Kategorie	Die Kategorie des Servers, auf dem die Anwendung gehostet wird. Beispiel: Physischer Server.
Status	Der Status des Servers, auf dem die Anwendung gehostet wird: Einer Bewertungsaufgabe zugewiesen, Keiner Bewertungsaufgabe zugewiesen oder Ignoriert.

Listenaktionen

Schaltfläche	Beschreibung
Liste neu laden	Aktualisiert die Liste, damit die neuesten Informationen angezeigt werden
Listenaktionen	Wählt Aktionen aus, die für diese Liste unterstützt werden: • **Spalten bearbeiten** – Passt die Liste so an, dass die erforderlichen Spalten in der von Ihnen ausgewählten Reihenfolge angezeigt werden. • **Speichern unter** – Erstellen Sie eine Kopie dieser Liste und speichern Sie sie unter **Meine Listen**. • **Breiten zurücksetzen** – Setzt die Spaltenbreite auf den Standardwert zurück.
URL kopieren	Kopiert die URL für diese Liste
Filterbereich anzeigen	Zeigt den Filterbereich auf der rechten Seite an. Wenn Filter auf die Liste angewendet werden, enthält die Schaltfläche „Filter anzeigen“ die Anzahl der aktiven Filter.

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

Zugehörige Informationen

Bewertungsaufgaben für die Cloud-Migration in Konfigurierbarer Arbeitsbereich erstellen

Bewertungsaufgaben in Konfigurierbarer Arbeitsbereich Ressourcen zuweisen

Detaillierte Anwendungsinformationen in Konfigurierbarer Arbeitsbereich überprüfen

Liste „VMs auf nicht erkannten Servern“ in Bewertung der Cloud-Migration

Bewertung der Cloud-Migration zeigt Informationen zu virtuellen Computern an, die auf nicht erkannten Servern gehostet werden.

In der Liste „VMs auf nicht erkannten Servern“ verfügbare Informationen

Spalte (von links nach rechts)	Beschreibung
Name	Der Name der VM-Instanz.
VM-Instanz	Der Name der VM-Instanz. Bei VMs, die ohne einen Server erkannt wurden, auf dem sie gehostet werden, sind die Felder „VM-Instanz“ und „Name“ gleich.
Status	Status der VM • An • Aus • Angehalten • Geplant • Wird gestartet • Wird gestoppt • Stillgelegt • Beendet • Fehler • Abgebrochen • Wird pausiert • Wird beendet
Status	Der Serverzuweisungsstatus: • Zugewiesen – Der Server ist einer Bewertungsaufgabe zugewiesen. • Nicht zugewiesen – Der Server ist keiner Bewertungsaufgabe zugewiesen. • Ignoriert – Der Server befindet sich in der Liste „Ignoriert“.
IP-Adresse	Die IP-Adresse des Servers.
Hersteller	Der Hersteller des Servers.
CPUs	Die Anzahl der Server-CPUs.

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

Spalte (von links nach rechts)	Beschreibung
Arbeitsspeicher (MB)	Die VM-Arbeitsspeichergröße.
IT-Umgebung	Die aktuelle IT-Umgebung, die diese VM-Instanz enthält. • Vor Ort • Cloud
Kategorie	Die Serverkategorie: • Physischer Server • VMware-Virtualisierung • Hyper-V-Virtualisierung • IBM HMC-Virtualisierung • OpenStack-Virtualisierung • Solaris-Virtualisierung • Nutanix-Virtualisierung • AWS • Microsoft Azure • Google Cloud • IBM Cloud

Listenaktionen

Schaltfläche	Aktion
Liste neu laden	Aktualisiert die Liste, damit die neuesten Informationen angezeigt werden
Listenaktionen	Wählt Aktionen aus, die für diese Liste unterstützt werden: • **Spalten bearbeiten** – Passt die Liste so an, dass die erforderlichen Spalten in der von Ihnen ausgewählten Reihenfolge angezeigt werden. • **Speichern unter** – Erstellen Sie eine Kopie dieser Liste und speichern Sie sie unter **Meine Listen**. • **Breiten zurücksetzen** – Setzt die Spaltenbreite auf den Standardwert zurück.
URL kopieren	Kopiert die URL für diese Liste

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

Schaltfläche	Aktion
Filterbereich anzeigen	Zeigt den Filterbereich auf der rechten Seite an. Wenn Filter auf die Liste angewendet werden, enthält die Schaltfläche „Filter anzeigen“ die Anzahl der aktiven Filter.
Export	Speichert die Liste in einem der unterstützten Formate: Excel, CSV, JSON, PDF

Liste „Softwareanforderungen“ in Bewertung der Cloud-Migration

Die Liste der Softwareanforderungen zeigt die Liste der Anwendungen, die den Bewertungsaufgaben zugeordnet sind.

In der Liste der Softwareanforderungen verfügbare Informationen

Spalten (von links nach rechts)	Beschreibung
Bewertungsaufgabe	Der Link zur Bewertungsaufgabe.
Software-Produktname	Der Anwendungsname.
Softwareherausgeber	Der Name des Unternehmens, das die Anwendung erstellt hat.
Softwareversion	Die Anwendungsversion.
BYOL unterstützt	Der Name der eigenen Lizenz (BYOL, Bring Your Own License).
Open Source	Die Anwendung wird als Open Source entwickelt.
Open Source-Lizenztyp	Der Lizenzierungstyp der Anwendung, die als Open Source entwickelt wird.
Anwendung	Die Anwendung, die auf einem der Bewertungsaufgabe zugewiesenen Server ausgeführt wird, im folgenden Format:<application name>@<server>.

Listenaktionen

Schaltfläche	Aktion
Liste neu laden	Aktualisiert die Liste, damit die neuesten Informationen angezeigt werden
Listenaktionen	Wählt Aktionen aus, die für diese Liste unterstützt werden: • **Spalten bearbeiten** – Passt die Liste so an, dass die erforderlichen Spalten in der von Ihnen ausgewählten Reihenfolge angezeigt werden.

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

Schaltfläche	Aktion
	• **Speichern unter** – Erstellen Sie eine Kopie dieser Liste und speichern Sie sie unter **Meine Listen**. • **Breiten zurücksetzen** – Setzt die Spaltenbreite auf den Standardwert zurück.
URL kopieren	Kopiert die URL für diese Liste
Filterbereich anzeigen	Zeigt den Filterbereich auf der rechten Seite an. Wenn Filter auf die Liste angewendet werden, enthält die Schaltfläche „Filter anzeigen“ die Anzahl der aktiven Filter.
Export	Speichert die Liste in einem der unterstützten Formate: Excel, CSV, JSON, PDF

Governance für Cloud-Konfigurationen

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

Erkunden

Governance für Cloud-Konfigurationen erkunden

Einrichten

- Cloud Configuration Governance installieren
- CCG Inhaltspaket installieren
- Cloud Configuration Governance für AWS einrichten
- Cloud Configuration Governance für Microsoft Azure einrichten

Verwalten

- Richtlinien
- Scan-Konfiguration
- Fehlerkorrektur

Verwenden

- Scan-Konfiguration ausführen
- Dashboard anzeigen
- Korrektur ausführen

Entwickeln

- Entwicklerschulungen
- Entwicklerdokumentation

Problembehandlung und Hilfe

- Fragen stellen oder beantworten im Governance für Cloud-Konfigurationen-Forum der ServiceNow Community

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

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Governance für Cloud-Konfigurationen erkunden

Verstehen Sie den typischen Governance für Cloud-Konfigurationen-Workflow und allgemeine Aufgaben.

Um Governance für Cloud-Konfigurationen für die Verwaltung der Konfiguration der Cloud-Ressourcen zu verwenden, führen Sie die folgenden Aufgaben aus:

1. Installieren Sie Governance für Cloud-Konfigurationen. Weitere Informationen finden Sie unter Cloud Configuration Governance installieren.
2. Installieren Sie das CCG-Inhaltspaket, um auf die Inhalte des Basissystems Governance für Cloud-Konfigurationen zuzugreifen. Weitere Informationen finden Sie unter CCG Inhaltspaket installieren.
3. Weisen Sie Benutzern Governance für Cloud-Konfigurationen-Rollen zu. Weitere Informationen zu den Governance für Cloud-Konfigurationen-Rollen finden Sie unter Cloud Configuration Governance-Rollen und -Systemeigenschaften.
4. Informationen zum Verwalten der Konfiguration der Ressourcen von Amazon Web Services (AWS) über Governance für Cloud-Konfigurationen finden Sie unter Cloud Configuration Governance für AWS einrichten.
5. Informationen zum Verwalten der Konfiguration der Microsoft Azure-Ressourcen über Governance für Cloud-Konfigurationen finden Sie unter Cloud Configuration Governance für Microsoft Azure einrichten.
6. Erstellen Sie eine Scan-Konfiguration, um die Cloud-Ressourcen anhand mindestens eines Richtliniensatzes zu scannen und die Richtlinienverstöße zu identifizieren. Weitere Informationen finden Sie unter Scan-Konfiguration erstellen.
7. Führen Sie die entsprechende Korrekturaktion aus, um die nicht konforme Cloud-Konfiguration zu beheben, die während der Scan-Ausführung identifiziert wurde. Weitere Informationen finden Sie unter Korrektur ausführen.

Nächste Schritte

Unter Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate finden Sie die Liste der Plugins, die Sie mit Governance für Cloud-Konfigurationenaktivieren.

Governance für Cloud-Konfigurationen installieren

Sie können die Anwendung Governance für Cloud-Konfigurationen (com.sn.itom.ccg) installieren, wenn Sie über die Administratorrolle verfügen. Die Anwendung installiert die zugehörigen ServiceNow® Store-Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .

Erforderliche Rolle: admin

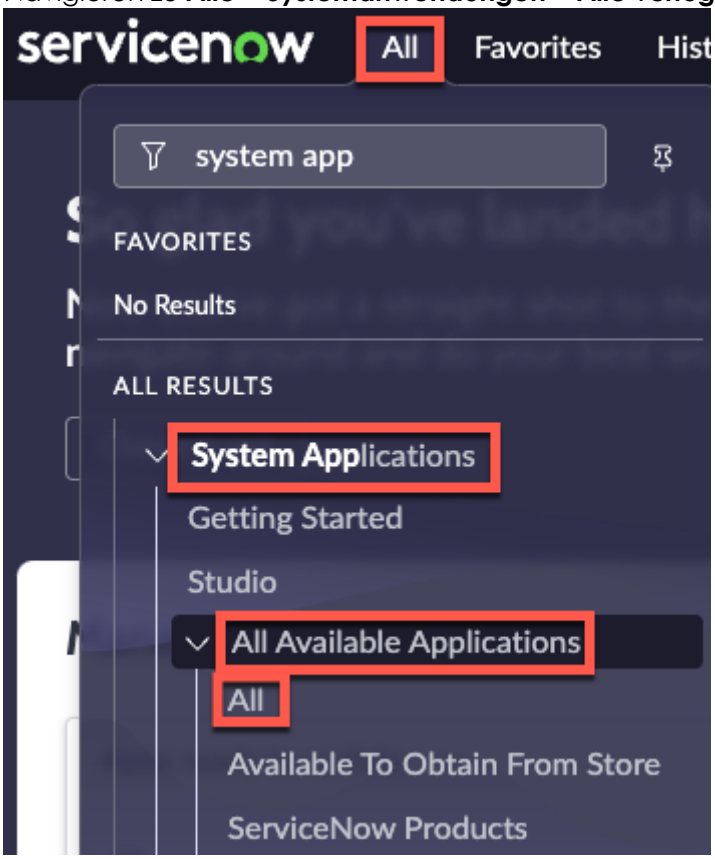
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Warum und wann dieser Vorgang ausgeführt wird

Von Governance für Cloud-Konfigurationen wird das ServiceNow® ITOM Cloud Accelerate-Abonnement verwendet. Wenn Sie diese Anwendung installieren, werden automatisch mehrere Rollen und die Anwendung ServiceNow® Bibliothek von Cloud-Aktionen (sn.itom.cal) installiert.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Governance für Cloud-Konfigurationen (com.sn.itom.ccg).

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

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

3. Überprüfen Sie im Dialogfeld „Anwendungsinstallation" die Anwendungsabhängigkeiten.

   Abhängige Plugins und Anwendungen werden aufgelistet, wenn sie installiert werden sollen, derzeit installiert sind oder installiert werden müssen. Wenn die Installation von Plugins oder Anwendungen erforderlich ist, müssen Sie sie installieren, bevor Sie Governance für Cloud-Konfigurationen installieren können.

4. Wählen Sie **Installieren** aus.

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

Nächste Maßnahme

Für den Zugriff auf Basissysteminhalte wie Richtlinien, Konfigurationssammler, Fehlerkorrekturen und mehr installieren Sie die Anwendung CCG Inhaltspaket. Weitere Informationen finden Sie unter CCG Content Pack installieren.

CCG Inhaltspaket installieren

Mit der Administratorrolle können Sie die Anwendung CCG Inhaltspaket (sn_itom_ccg_cp) installieren.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfen Sie die CCG Content Pack -Anwendungsliste im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

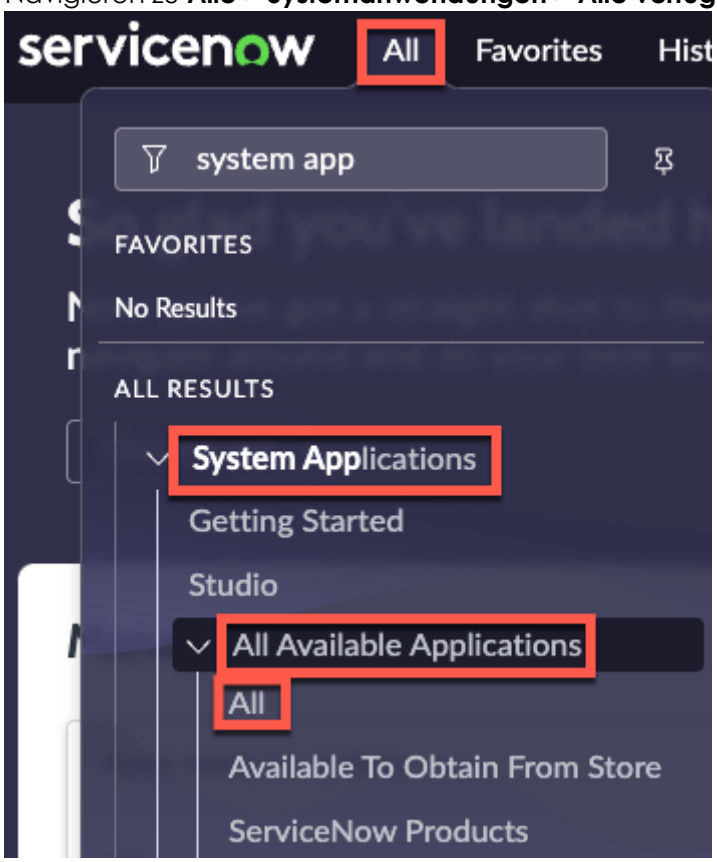
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

CCG Inhaltspaket stellt die Basissysteminhalte wie Richtlinien, Ressourcensammler, Konfigurationssammler und Korrekturaktionen für die App Governance für Cloud-Konfigurationen bereit.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung CCG Inhaltspaket (sn_itom_ccg_cp).

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

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

In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
4. Wählen Sie **Installieren** aus.

Governance für Cloud-Konfigurationen for AWS einrichten

Richten Sie in Governance für Cloud-Konfigurationen Zugriff auf die AWS-Cloud-Konten (Amazon Web Services) ein, um die Interaktion zwischen der Anwendung und der Cloud zu ermöglichen. Die Anwendung erfordert Zugriff auf die Cloud-Konten, damit die Cloud-Ressourcen auf nicht konforme Konfigurationen gescannt und nicht konforme Konfigurationen korrigiert werden können.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.scheduling_admin

Warum und wann dieser Vorgang ausgeführt wird
Im Zusammenhang mit der Konfiguration des Zugriffs für AWS-Konten werden die folgenden Begriffe verwendet:

Vertrauende Konten

Vertrauende Konten haben keine permanenten AWS-Anmeldeinformationen. Sie konfigurieren die Vertrauensstellung für IAM-Rollen in diesen Konten so, dass sie für den Zugriff auf andere Konten zurückgreifen.

Vertrauenswürdige Konten

Die vertrauenswürdigen Konten werden von den vertrauenden Konten für den Zugriff verwendet. In der Benutzeroberfläche von ServiceNow werden die vertrauenswürdigen Konten als Accounts des Zugriffsberechtigten bezeichnet.

Verwenden Sie eine der folgenden Methoden, um den Zugriff auf die Konten AWS zu konfigurieren:

- Konfigurieren Sie die permanenten Anmeldeinformationen in Now Platform für die Verbindung mit den eigenständigen AWS -Accounts (diskrete Accounts). Die Tabelle „Cloud-Servicekonto“ [cmdb_ci_cloud_service-account] enthält die Informationen zum Servicekontotyp wie Verwaltungskonto oder Mitgliedskonto und deren Anmeldeinformationen.
- Konfigurieren Sie die Mitgliedskonten so, dass sie für den Zugriff auf das Verwaltungskonto zurückgreifen. Konfigurieren Sie die permanenten Anmeldeinformationen des Verwaltungskontos in diesem Fall auf der Now Platform.
- Konfigurieren Sie die Konten so, dass für den Zugriff ein vertrauenswürdiges Konto verwendet wird (lateraler Zugriff innerhalb derselben AWS-Organisation oder über verschiedene AWS-Organisationen hinweg). Konfigurieren Sie die permanenten Anmeldeinformationen des vertrauenswürdigen Kontos in diesem Fall auf der Now Platform.

Hinweis: Governance für Cloud-Konfigurationen verwendet kein MID-Server-basiertes Setup für die Rollenübernahme, um auf die vertrauenden Accounts zuzugreifen.

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

Prozedur

1. Erstellen Sie Anmeldeinformationen für die AWS-Servicekonten.

   a. Navigieren zu **Verbindung und Anmeldeinformationen** > **Anmeldeinformationen**.

   b. Wählen Sie **Neu** und dann **AWS-Anmeldeinformationen** aus.

   c. Füllen Sie die Felder des Formulars aus.

   Formular für AWS-Anmeldeinformationen

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.
Zugangsschlüssel-ID	Die Zugriffsschlüssel-ID, die Sie in der AWS-Verwaltungskonsole erstellt haben
Geheimer Zugangsschlüssel	Der geheime Zugriffsschlüssel, den Sie in der AWS-Verwaltungskonsole erstellt haben

   d. Wählen Sie **Speichern**.

2. Wählen Sie den Anmeldeinformationsalias **sn_itom_cal.Aws_Creds_Alias** aus, oder erstellen Sie einen Anmeldeinformationsalias.

   a. Entsperren Sie den Anmeldeinformationsalias.

   b. Suchen Sie nach einem Anmeldeinformationsalias.

   c. Wählen Sie **Neu**.

   d. Füllen Sie die Felder des Formulars aus.

   Formular „Verbindungs- und Anmeldeinformationsalias“

Feld	Beschreibung
Name	Eindeutiger Name des Alias
Typ	Typ des Anmeldeinformationsalias. Wählen Sie in der Dropdown-Liste „Typ“ die Option **Anmeldeinformationen** aus.

   e. Wählen Sie **Absenden** aus.

3. Legen Sie das Feld **Authentifizierungsalgorithmus** auf **AWS Authenticator** fest.
4. Wählen Sie **Absenden** aus.
5. Richten Sie ein AWS-Servicekonto ein.

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

a. Navigieren zu **Cloud Provisioning and Governance** > **Servicekonten**.

b. Wählen Sie **Neu**.

c. Füllen Sie die Felder des Formulars aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger Name des Servicekontos
Account-ID	12-stellige Nummer des Benutzerkontos. Erweitern Sie die Liste unter dem Kontonamen in der AWS-Verwaltungskonsole, um die Nummer anzuzeigen. **Wichtig:** Entfernen Sie im Feld **Konto-ID** die Bindestriche (-) aus der Nummer.
Discovery-Anmeldeinformationen	Anmeldeinformationen, die für ServiceNow -Anwendungen erforderlich sind, um auf den Cloud-Account zuzugreifen. Sie können die Discovery-Anmeldeinformationen zu einem späteren Zeitpunkt konfigurieren, während Sie den Zugriff auf die Konten AWS konfigurieren. ▪ Wenn Sie ein unabhängiges Servicekonto oder ein Verwaltungskonto einrichten, wählen Sie die zugehörigen AWS-Anmeldeinformationen aus. ▪ Um andere AWS -Accounts für den Zugriff auf diesen Account zu verwenden, lassen Sie das Feld leer. Beispielsweise müssen Sie die Anmeldeinformationen AWS nicht für Konten angeben, die IAM-Rollen (Identity and Access Management) übernehmen, oder für Mitgliedskonten, die ihr Verwaltungskonto für den Zugriff verwenden.
Rechenzentrums-URL	URL des Rechenzentrums. Lassen Sie dieses Feld leer.
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie **AWS-Rechenzentrum** aus.
Rechenzentrums-Discovery-Status	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Übergeordneter Account	Name des Verwaltungskontos, das die AWS-Organisation darstellt, zu der dieses Mitgliedskonto gehört. Dieses Feld wird angezeigt, wenn Sie „AWS-Rechenzentrum“ auswählen. Wenn der Account keiner AWS -Organisation angehört, lassen Sie dieses Feld leer.
Ist Master-Konto	Kennzeichnung des Verwaltungskontos.

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

Feld	Beschreibung
	Dieses Kontrollkästchen wird angezeigt, wenn Sie in der Dropdown-Liste „Rechenzentrumstyp“ die Option „AWS-Rechenzentrum“ auswählen. Aktivieren Sie das Kontrollkästchen, um das AWS-Servicekonto dem Verwaltungskonto zuzuordnen. Aktivieren Sie dieses Kontrollkästchen nur für Konten, die Sie zuvor als Verwaltungskonten konfiguriert haben und zu denen einige Mitgliedskonten gehören. Weitere Informationen zur Organisation AWS finden Sie unter AWS Dokumentation .
Account des Zugriffsberechtigten	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, bei denen keine permanenten AWS-Anmeldeinformationen verwendet werden und bei denen IAM-Rollen für den Zugriff genutzt werden.

d. Wählen Sie **Absenden** aus.

6. Führen Sie eine der folgenden Aktionen aus.

Option	Beschreibung
Erstellen Sie eine Konfiguration für die Rollenübernahme für das Verwaltungskonto	Wenn Sie ein Verwaltungskonto verwenden möchten, um die Mitgliedskonten der Organisation AWS zu scannen, erstellen Sie eine Konfiguration für die Rollenübernahme für das Verwaltungskonto. **a.** Wenn Sie OrganizationAccountAccessRole nicht für den Zugriff auf den Mitgliedsaccount verwenden möchten, konfigurieren Sie den vertrauenden Account für Governance für Cloud-Konfigurationen. Weitere Informationen finden Sie unter Konfigurieren Sie das vertrauende Konto für Governance für Cloud-Konfigurationen und Bibliothek von Cloud-Aktionen. **b.** Wiederholen Sie Schritt 6.a für alle Mitgliedskonten, die über das Verwaltungskonto gescannt werden müssen, ohne die OrganizationAccountAccessRole zu verwenden. **c.** Wenn Sie die OrganizationAccountAccessRole verwenden möchten, um auf das Mitgliedskonto zuzugreifen, erstellen

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

Option	Beschreibung
	Sie eine Konfiguration für die Übernahme von Rollen für das Verwaltungskonto. Weitere Informationen finden Sie unter Konfiguration für die Übernahme von Rollen erstellen.
Konfigurieren Sie das vertrauende Konto für Governance für Cloud-Konfigurationen	Wenn Sie ein vertrauenswürdiges Konto zum Scannen des vertrauenden Kontos verwenden möchten, konfigurieren Sie das vertrauende Konto für Governance für Cloud-Konfigurationen. **a.** Konfigurieren Sie das vertrauende Konto für Governance für Cloud-Konfigurationen. Weitere Informationen finden Sie unter Konfigurieren Sie das vertrauende Konto für Governance für Cloud-Konfigurationen und Bibliothek von Cloud-Aktionen. **b.** Wiederholen Sie Schritt 6.a für alle vertrauenswürdigen Konten, die über das vertrauenswürdige Konto gescannt werden müssen.

7. Installieren und konfigurieren Sie die MID Servers.
   Weitere Informationen finden Sie unter MID-Server installieren und konfigurieren.
8. Führen Sie die Rechenzentrumserkennung aus, um die mit den Servicekonten verbundenen Rechenzentren zu identifizieren.
   Weitere Informationen finden Sie unter Rechenzentrumserkennung ausführen.

Konfigurieren Sie das vertrauende Konto für Governance für Cloud-Konfigurationen und Bibliothek von Cloud-Aktionen

Konfigurieren Sie das vertrauende Konto, auf dessen Ressourcen zugegriffen werden muss, so, dass es über die Identity and Access Management (IAM)-Rolle auf das vertrauenswürdige Konto zurückgreift.

Vorbereitungen

- Machen Sie sich mit der Amazon-Dokumentation zum Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer vertraut.
- Entscheiden Sie, welcher Amazon Web Services (AWS)-Account der vertrauenswürdige Account sein soll. Sie verwenden den vertrauenswürdigen Account zur Konfiguration temporärer Anmeldeinformationen für Governance für Cloud-Konfigurationen mithilfe von IAM-Rollen. Der vertrauenswürdige Account, den Sie für den Zugriff auf andere Accounts mit IAM-Rollen verwenden, wird als Account eines Zugriffsberechtigten bezeichnet.
- Richten Sie das vertrauenswürdige und das vertrauende Konto wie in Governance für Cloud-Konfigurationen for AWS einrichtenbeschrieben ein.

Erforderliche Rolle: sn_itom_ccg.scheduling_admin

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

Prozedur

1. Erstellen Sie eine IAM-Rolle für das vertrauende Konto, und konfigurieren Sie die Vertrauensstellung zwischen dem Benutzer, der diese Rolle übernimmt, und dem vertrauenswürdigen Konto (Account des Zugriffsberechtigten).

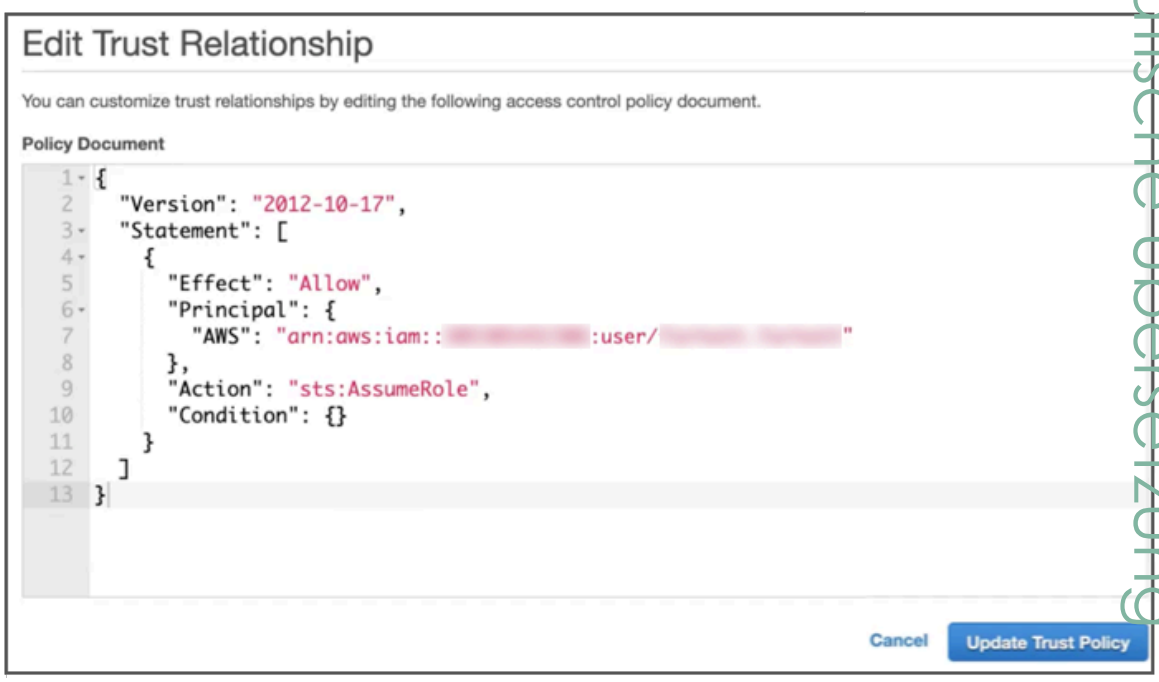
   a. Melden Sie sich in der AWS-Managementkonsole bei dem vertrauenden Account an.

   b. Erstellen und konfigurieren Sie die IAM-Rolle, indem Sie im Feld **Account ID** die ID des vertrauenswürdigen Kontos (des Accounts des Zugriffsberechtigten) angeben. Informationen zum Erstellen von AWS -Rollen finden Sie unter Amazon Dokumentation .

   c. Wählen Sie auf der Seite „Zusammenfassung“ für die IAM-Rolle die Registerkarte **Trust Relationships** (Vertrauensstellungen).

   d. Klicken Sie auf **Edit trust relationship** (Vertrauensstellung bearbeiten).
   Die Seite zum Bearbeiten der Vertrauensstellung wird geöffnet und zeigt das Richtliniendokument an.

   e. Legen Sie den Parameter *AWS* auf den vollständigen Benutzer-ARN des vertrauenswürdigen Accounts (des Zugriffsberechtigten) fest.



   f. Verifizieren Sie, ob der *Action*-Wert auf *sts:AssumeRole* festgelegt ist.

   g. Klicken Sie auf **Update Trust Policy** (Vertrauensrichtlinie aktualisieren).

2. Konfigurieren Sie den vertrauenswürdigen Serviceaccount für das vertrauende Konto auf der Now Platform.

   a. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**.

   b. Öffnen Sie das vertrauende Konto.

Automatische Übersetzung

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

c. Geben Sie im Formular „Cloud-Servicekonto“ den Namen des vertrauenswürdigen Kontos im Feld **Account des Zugriffsberechtigten** ein.

d. Wählen Sie **Aktualisieren**.

3. Erstellen Sie für das vertrauende Konto eine Konfiguration für die Übernahme von Rollen. Weitere Informationen finden Sie unter Konfiguration für die Übernahme von Rollen erstellen.

Konfiguration für die Übernahme von Rollen erstellen

Erstellen Sie ein Servicekonto, um die Rollenkonfiguration zu übernehmen, um den kontoübergreifenden Zugriff zu erleichtern, von einem Verwaltungskonto zu einem Mitgliedskonto oder von einem vertrauenswürdigen Konto zu einem vertrauenden Konto.

Vorbereitungen

Stellen Sie sicher, dass die Anmeldeinformationen für den Account des Zugriffsberechtigten in Now Platformkonfiguriert sind.

Erforderliche Rolle: sn_itom_ccg.scheduling_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn für das Mitgliedskonto keine permanenten Anmeldeinformationen definiert sind, wird von Governance für Cloud-Konfigurationen die Tabelle für die Konfiguration der Rollenübernahme für Cloud-Servicekonten [sn_itom_ccg_service_account_assume_role_config] überprüft, damit die spezielle Konfiguration identifiziert werden kann, die dem Verwaltungskonto zugeordnet ist. Dann werden die Anmeldeinformationen des Verwaltungskontos dazu verwendet, temporäre Anmeldeinformationen für die Mitgliedskonten zu generieren. Wenn die Konfiguration in der Tabelle vorhanden ist, verwendet Governance für Cloud-Konfigurationen die temporären Anmeldeinformationen, die durch Angabe einer Rolle und ihrer Konfiguration in der Aktion AssumeRole (Sicherheitstoken-Services-API) Amazon Web Services (AWS) abgerufen wurden.

Prozedur

1. Navigieren zu **Alle** > **Governance für Cloud-Konfigurationen** > **Rollenkonfiguration übernehmen**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Werte im Formular Konfiguration der Rollenübernahme für Servicekonto aus. Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen Formular „Konfiguration der Rollenübernahme für Servicekonto“..
4. Wählen Sie **Absenden**.

Governance für Cloud-Konfigurationen for Microsoft Azure einrichten

Richten Sie in Governance für Cloud-Konfigurationen Zugriff auf die Microsoft Azure Cloud-Konten ein, um die Interaktion zwischen der Anwendung und der Cloud zu ermöglichen. Die Anwendung erfordert Zugriff auf die Cloud-Konten Ihrer Organisation, damit die Cloud-Ressourcen auf nicht konforme Konfigurationen gescannt und nicht konforme Konfigurationen korrigiert werden können.

Vorbereitungen

Erforderliche Rolle: sn_itom_ccg.scheduling_admin

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

Prozedur

1. Erstellen Sie Microsoft Azure-Anmeldeinformationen für den Zugriff auf das Microsoft Azure-Konto.
   Weitere Informationen finden Sie unter Azure Cloud-Anmeldeinformationen erstellen.
2. Erstellen Sie eine IntegrationHub-Verbindung für Microsoft Azure.

   a. Navigieren zu **Prozessautomatisierung** > **Flow Designer**, und wählen Sie die Registerkarte **Verbindungen**.

   b. Wählen Sie auf der Kachel **Azure Connection** (Azure-Verbindung) die Option **Verbindung hinzufügen** aus.

   c. Füllen Sie die Felder des Formulars aus.

   Formular „Scan-Zeitplan“

Feld	Beschreibung
Verbindungsname	Name der Verbindung
OAuth-Client-ID	Microsoft Azure-Anwendungs-ID
OAuth-Client-Geheimnis	Microsoft Azure-Anwendungsschlüssel
OAuth-Token-URL	Mandanten-ID des Microsoft Azure-Kontos Ersetzen Sie `{tenant}` durch die Microsoft Azure-Mandanten-ID.

   d. Wählen Sie **OAuth-Token erstellen und abrufen** aus.

3. Führen Sie die Rechenzentrumserkennung aus, um die mit den Servicekonten verbundenen Rechenzentren zu identifizieren.
   Weitere Informationen finden Sie unter Rechenzentrumserkennung ausführen.

Domain Separation und Governance für Cloud-Konfigurationen

Domänentrennung wird in Governance für Cloud-Konfigurationen nicht unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Zugehörige Informationen

Domänentrennung für Service Provider

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

Arbeiten mit Governance für Cloud-Konfigurationen

Governance für Cloud-Konfigurationen bietet eine Reihe von sofort einsatzbereiten Richtlinien. Sie können entweder diese Richtlinien verwenden, um die nicht konformen Cloud-Ressourcenkonfigurationen in Ihrer Cloud-Organisation zu identifizieren, oder benutzerdefinierte Richtlinien erstellen. Nachdem Sie die nicht konformen Cloud-Ressourcenkonfigurationen identifiziert haben, können Sie die Fehlerkorrekturfunktion der Anwendung verwenden, um die Verstöße zu beheben.

Hinweis: Ab Governance für Cloud-Konfigurationen Version 1.3.7 wird der Inhalt des Basissystems in das Verzeichnis CCG Inhaltspaketverschoben. Installieren Sie CCG Inhaltspaket, um auf die Inhalte des Basissystems Governance für Cloud-Konfigurationen zuzugreifen.

Scan-Konfiguration

Die Scan-Konfiguration definiert die verschiedenen Einstellungen für den Governance für Cloud-Konfigurationen-Scan.

Wenn Sie eine Scan-Konfiguration ausführen, werden von Governance für Cloud-Konfigurationen die Ziel-Cloud-Ressourcentypen aus den Richtliniensätzen identifiziert, die der Scan-Konfiguration angefügt sind. Anschließend werden die entsprechenden Ressourcensammler und Konfigurationssammler aufgerufen, damit die Konfigurationsdaten der Zielressourcentypen importiert werden können. Nach dem Import der Konfigurationsdaten werden die importierten Konfigurationsdaten von Governance für Cloud-Konfigurationen mit den nicht konformen Konfigurationen verglichen, die in den Richtlinien definiert sind. Wird von Governance für Cloud-Konfigurationen eine Übereinstimmung erkannt, wird ein Verstoß im Audit-Verstoßbericht gemeldet.

Sie können die Menge der in das System importierten Konfigurationsdaten reduzieren, indem Sie eine Reihe von Kombinationen aus Servicekonto und Rechenzentrum für die Scan-Konfiguration angeben. Sind solche angegeben, werden von Governance für Cloud-Konfigurationen nur die Daten aus den angegebenen Kombinationen aus Servicekonto und Rechenzentrum importiert. Darüber hinaus können Sie auch Tag-basierte Cloud-Ressourcenfilter verwenden, um die Cloud-Ressourcen zu identifizieren, deren Konfigurationsdaten für den Scan importiert werden müssen.

Weitere Informationen zum Erstellen von Scan-Konfigurationen finden Sie unter Scan-Konfiguration erstellen.

Scan-Konfiguration erstellen

Erstellen Sie in Governance für Cloud-Konfigurationen eine Scan-Konfiguration, um die Cloud-Ressourcen anhand mindestens eines Richtliniensatzes zu scannen und die Richtlinienverstöße zu identifizieren.

Vorbereitungen

- Vergewissern Sie sich, dass ein geeigneter Richtliniensatz für den Scan verfügbar ist. Mit dem Richtliniensatz wird ein bestimmter Sicherheits- oder Organisationsstandard durchgesetzt. Weitere Informationen zum Erstellen des Richtliniensatzes finden Sie unter Richtliniensatz erstellen.
- Erforderliche Rolle: sn_itom_ccg.scheduling_admin

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

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Ab Governance für Cloud-Konfigurationen Version 1.3.7 wird der Inhalt des Basissystems in das Verzeichnis CCG Inhaltspaketverschoben. Installieren Sie CCG Inhaltspaket, um auf die Inhalte des Basissystems Governance für Cloud-Konfigurationen zuzugreifen.

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Scan-Konfigurationen**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Werte im Formular „Scan Configuration“ (Scan-Konfiguration) aus. Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen-Formular zum Konfigurieren von Scans.
4. Wählen Sie **Absenden** aus.
5. Um einen Zeitplan für die Ausführung der Scan-Konfiguration zu erstellen, wählen Sie **Setup Schedule** (Zeitplan einrichten) aus.

   a. Wahlweise: Legen Sie Kriterien zum Abbrechen von Scans fest, die längere Zeit dauern. Zum Importieren der Konfigurationsdaten der Cloud-Ressourcen verwenden Governance für Cloud-Konfigurationen-Ressourcensammler und -Konfigurationssammler Flow Designer-Subflows. Manchmal schlägt der Subflow fehl, und der Fehler wird nicht gemeldet. In solchen Fällen kann die Scan-Ausführung unbegrenzt ausgeführt werden. Das Festlegen von Abbruchkriterien hilft beim Abbrechen solcher Scans.

Nächste Maßnahme

Führen Sie die Scan-Konfiguration aus, um die Ressourcenkonfiguration der angegebenen Cloud anhand der angegebenen Richtliniensätze auszuwerten und die Richtlinienverstöße zu identifizieren. Weitere Informationen finden Sie unter Scan-Konfiguration ausführen.

Scan-Konfiguration ausführen

Führen Sie eine Scan-Konfiguration aus, um die Ressourcenkonfiguration der angegebenen Cloud anhand der angegebenen Richtliniensätze auszuwerten und die Richtlinienverstöße zu identifizieren. Die identifizierten Richtlinienverstöße werden von Governance für Cloud-Konfigurationen als Audit-Ergebnisse gemeldet.

Vorbereitungen

Erforderliche Rolle: sn_itom_ccg.scheduling_admin

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Scan-Konfigurationen**.
2. Öffnen Sie die Scan-Konfiguration, die Sie ausführen möchten.
3. Wählen Sie **Ausführen** aus.

Scan-Ausführung

Jede Ausführung einer Scan-Konfiguration wird als Scan-Ausführung bezeichnet. Das Modul „Scan Run“ (Scan-Ausführungen) zeigt eine Liste aller Scan-Ausführungen an.

In Governance für Cloud-Konfigurationen werden die folgenden Informationen für jede Scan-Ausführung in einer zugehörigen Liste angezeigt:

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

- **Scan-Status**: Auf dieser Registerkarte wird der Datenerfassungsstatus auf Servicekonto-Ebene angezeigt. Öffnen Sie den Scan-Ausführungsdatensatz, um den Konfigurationsdaten-Erfassungsstatus für jedes im Scan abgedeckte Rechenzentrum anzuzeigen. Verwenden Sie den Flow-Ausführungskontext, um Probleme bei der Ausführung der Richtlinie zu beheben.
- **Policy Run Status** (Richtlinienausführungsstatus): Auf dieser Registerkarte werden Informationen zu den während der Scan-Ausführung ausgeführten Richtlinien und der Status ihrer Ausführung angezeigt. Verwenden Sie den Flow-Ausführungskontext, um Probleme bei der Ausführung der Richtlinie zu beheben.
- **Run Resource Assocs** (Ressourcenzuordnungen ausführen): Auf dieser Registerkarte werden Informationen zu den Ressourcen und deren Konfigurationsdaten angezeigt, die während der Scan-Ausführung importiert wurden. Sie können eine beliebige Ressource auswählen, um die folgenden Informationen anzuzeigen:
  - Konfigurationseinstellungen der Ressource
  - Ressourcenattribute
  - Audit-Ergebnisse für die Ressource

Registerkarte **Scan Run Logs** (Scanausführungsprotokolle): Hier wird die Ablaufverfolgung der Scan-Ausführung angezeigt.

Zugehörige Informationen

Scan-Konfiguration

Governance für Cloud-Konfigurationen-Richtlinien

Eine Governance für Cloud-Konfigurationen-Richtlinie definiert die nicht konformen Konfigurationen für einen bestimmten Cloud-Ressourcentyp.

Jede Governance für Cloud-Konfigurationen-Richtlinie enthält die folgenden Informationen:

- Die Cloud, in der die Ressource bereitgestellt wird
- Den Cloud-Ressourcentyp
- Definition der nicht konformen Konfiguration. Zum Beispiel unverschlüsselte S3-Buckets von Amazon Web Services (AWS) oder unsichere IAM-Konten (Identity and Access Management)
- Definition des Audit-Verstoßberichts (Richtlinienverstoß)

Hinweis: Ab Governance für Cloud-Konfigurationen Version 1.3.7 wird der Inhalt des Basissystems in das Verzeichnis CCG Inhaltspaketverschoben. Installieren Sie CCG Inhaltspaket, um auf die Inhalte des Basissystems Governance für Cloud-Konfigurationen zuzugreifen.

Von Governance für Cloud-Konfigurationen werden mehrere Basissystemrichtlinien bereitgestellt. Sie können entweder diese Richtlinien verwenden oder benutzerdefinierte Richtlinien gemäß den Anforderungen Ihrer Organisation erstellen. Je nach Bedarf und Vertrautheit mit der Now Platform können Sie eine der folgenden Methoden zum Erstellen der Richtlinie verwenden:

- Richtlinie mit dem Bedingungsgenerator erstellen
- Richtlinie mit dem IntegrationHub-Flow erstellen
- Richtlinie per Skript erstellen

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

Um die Richtlinie zu verwenden, fügen Sie die Richtlinie einem Richtliniensatz hinzu. Jeder Richtliniensatz kann eine oder mehr Richtlinie(n) enthalten. Weitere Informationen zum Erstellen von Richtliniensätzen finden Sie unter Richtliniensatz erstellen.

Basissystemrichtlinien

Name	Typ	Beschreibung
AWS IAM User Activity policy (AWS IAM-Benutzeraktivitätsrichtlinie)	Condition Builder	Richtlinie zur Überprüfung, ob das Passwort für den AWS IAM-Benutzer aktiviert ist. Um diese Richtlinie zu verwenden, stellen Sie sicher, dass das AWS IAM-Benutzerkonto über die folgenden Berechtigungen verfügt: • Iam:GetCredentialReport • Iam:GenerateCredentialReport
AWS S3 Enforce Bucket encryption (AWS-S3-Bucket-Verschlüsselung erzwingen)	Condition Builder	Richtlinie zur Überprüfung, ob die AWS-S3-Buckets verschlüsselt sind
AWS Sample flow policy (Beispiel für eine AWS-Flow-Richtlinie)	IntegrationHub-Flow	Richtlinie zur Veranschaulichung einer IntegrationHub-Flow-basierten Richtlinie
AWS VM HardwareType	Condition Builder	Richtlinie zur Überprüfung, ob von den bereitgestellten EC2-VMs nur die genehmigten Hardwaretypen verwendet werden
AWS VM IPAddress	Skript	Richtlinie zur Überprüfung, ob die IP-Adresse der EC2-VM mit dem Datensatz der Configuration Management Database (CMDB) übereinstimmt
AWS VM Monitoring State (Überwachungsstatus für VMs)	Condition Builder	Richtlinie zur Überprüfung, ob die detaillierte Überwachung für die EC2-VM aktiviert ist
Azure VM HardwareType	Condition Builder	Richtlinie zur Überprüfung, ob von den bereitgestellten Azure-VMs nur die genehmigten Hardwaretypen verwendet werden
Azure VM IP Address (Azure-VM-IP-Adresse)	Skript	Richtlinie zur Überprüfung, ob die IP-Adresse der Azure-VM mit dem Datensatz der CMDB übereinstimmt
Azure VM Monitoring State (Überwachungsstatus für VMs)	Condition Builder	Richtlinie zur Überprüfung, ob die detaillierte Überwachung für die Azure-VM aktiviert ist

Richtlinie mit dem Bedingungsgenerator erstellen

Verwenden Sie den Bedingungsgenerator, um eine Governance für Cloud-Konfigurationen-Richtlinie zu erstellen, ohne Code zu schreiben. Verwenden Sie diese Option, um die Kriterien für die Identifizierung und Meldung nicht konformer Cloud-Ressourcenkonfigurationen anzugeben.

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

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.governor

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Richtlinien**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars „Richtlinie“ aus.

   Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen-Formular „Richtlinie“.

   Sehen Sie sich eine der Richtlinien, die auf dem Bedingungsgenerator des Basissystems basieren, als Beispiel für die Erstellung der benutzerdefinierten Richtlinie an.
4. Wählen Sie **Absenden** aus.

Nächste Maßnahme
Testen Sie die Richtlinie, um sich zu vergewissern, dass sie ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter Richtlinie testen.

Richtlinie mit IntegrationHub-Subflow erstellen

Verwenden Sie den IntegrationHub-Subflow, um eine Governance für Cloud-Konfigurationen-Richtlinie zu erstellen. In einem IntegrationHub-Subflow werden grafische Codierungsmechanismen dazu verwendet, die Richtlinienbedingungen anzugeben. Der Subflow bietet eine größere Flexibilität in Audit-Verstoßberichten als der Bedingungsgenerator. Das heißt, Sie können dieselbe Richtlinie verwenden, um verschiedene Arten von Problemen zu melden.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird
Sehen Sie sich die **Sample flow policy** (Beispiel-Flow-Richtlinie) des Basissystems als Beispiel für das Erstellen neuer Richtlinien mit dem IntegrationHub-Subflow an.

Prozedur

1. Erstellen Sie einen IntegrationHub-Subflow für die Richtlinie.

   a. Kopieren Sie den Subflow **CCG – Flow Policy Template** (CCG – Flow-Richtlinienvorlage). Weitere Informationen zum Kopieren des Subflows finden Sie unter IntegrationHub-Subflow-Vorlage kopieren.

   b. Um die Konfigurationsdaten zu lesen, fügen Sie die Aktion **CCG – Read Config Setting** (CCG – Konfigurationseinstellung lesen) hinzu.
   Weitere Informationen zur Aktion **CCG – Read Config Setting** (CCG – Konfigurationseinstellung lesen) finden Sie unter Governance für Cloud-Konfigurationen-Aktionsreferenz.

   c. Wiederholen Sie Schritt 1.b für alle Konfigurationsschlüssel, die Sie in der Richtlinie verwenden möchten.

   d. Fügen Sie die Flow-Logik hinzu.

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

e. Weisen Sie Subflow-Ausgaben zu.
Die Einstellungen der Subflow-Ausgabe definieren, wie Audit-Verstöße von Governance für Cloud-Konfigurationen gemeldet werden. Weitere Informationen zum Zuweisen der Subflow-Ausgabe finden Sie unter Governance für Cloud-Konfigurationen-Aktionsreferenz.

f. Wahlweise: Wenn Sie die Option **Vorfall melden** im Formular **Subflow-Ausgaben zuweisen** nicht ausgewählt haben, fügen Sie eine Aktion unter der Aktion **Subflow-Ausgaben zuweisen** hinzu und fügen Sie dann die Aktion **Datensatz erstellen** hinzu. Weitere Informationen zur Aktion **Datensatz erstellen** finden Sie unter Governance für Cloud-Konfigurationen-Aktionsreferenz.

g. Speichern Sie den Subflow.

2. Navigieren zu **Governance für Cloud-Konfigurationen** > **Richtlinien**.
3. Wählen Sie **Neu**.
4. Füllen Sie die Felder des Formulars „Richtlinie“ aus.
Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen-Formular „Richtlinie“.
5. Wählen Sie **Absenden** aus.

Nächste Maßnahme
Testen Sie die Richtlinie, um sich zu vergewissern, dass sie ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter Richtlinie testen.

Richtlinie per Skript erstellen

Verwenden Sie den nativen Skriptmechanismus der ServiceNow-Plattform, um die Richtlinienbedingung zu definieren. Sie können die Entscheidungsfindung für Skripteinbindungen externalisieren und den Code für verschiedene Richtlinien wiederverwenden.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.governor

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Richtlinien**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars „Richtlinie“ aus.

   Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen-Formular „Richtlinie“.

   Sehen Sie sich eine der auf Skripten des Basissystems basierenden Richtlinien als Beispiel für die Erstellung der benutzerdefinierten Richtlinie an.

4. Wählen Sie **Absenden** aus.

Nächste Maßnahme
Testen Sie die Richtlinie, um sich zu vergewissern, dass sie ordnungsgemäß funktioniert. Weitere Informationen finden Sie unter Richtlinie testen.

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

Richtlinie testen

Testen Sie die Governance für Cloud-Konfigurationen-Richtlinie anhand der Konfigurationsdaten, die für eine vorherige Scan-Ausführung importiert wurden. Testen Sie die Richtlinie, um sich zu vergewissern, dass sie ordnungsgemäß funktioniert.

Vorbereitungen

- Vergewissern Sie sich, dass eine Scan-Ausführung verfügbar ist, die die Konfigurationsdaten enthält, die Sie über die Richtlinie überprüfen möchten.
- Erforderliche Rolle: sn_itom_ccg.governor

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Richtlinie**.
2. Öffnen Sie die Richtlinie.
3. Wählen Sie **Test Policy** (Richtlinie testen) aus.
4. Wählen Sie die entsprechende Scan-Ausführung aus.
5. Wählen Sie **OK** aus.

Konfigurationsschlüssel erstellen

Erstellen Sie einen Konfigurationsschlüssel in Governance für Cloud-Konfigurationen, um ihn in den Richtlinien zu verwenden. Der Konfigurationsschlüssel gibt den Ressourcensammler und den Konfigurationssammler an, die zum Importieren der Konfigurationsdaten aus der Cloud verwendet werden. Er gibt auch den Datentyp des Konfigurationswerts an.

Vorbereitungen

- Vergewissern Sie sich, dass ein Ressourcensammler für den im Konfigurationsschlüssel genannten Ressourcentyp verfügbar ist. Wenn der Ressourcensammler nicht verfügbar ist, können Sie ihn erstellen. Weitere Informationen finden Sie unter Ressourcensammler erstellen.
- Erforderliche Rolle: sn_itom_ccg.governor

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Konfigurationsschlüssel**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars „Konfigurationsschlüssel“ aus.
   Eine Beschreibung der Formularfelder finden Sie unter Governance für Cloud-Konfigurationen-Formular „Konfigurationsschlüssel“.
4. Wählen Sie **Absenden** aus.

Ressourcensammler erstellen

Erstellen Sie einen Ressourcensammler, um festzulegen, wie von Governance für Cloud-Konfigurationen alle Ressourcen eines bestimmten Typs importiert werden.

Vorbereitungen

Erforderliche Rolle: sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird

Die Cloud-Ressourcen sind unter einem Servicekonto oder einer Kombination aus Servicekonto und Rechenzentrum verfügbar. Vom Ressourcensammler werden

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

IntegrationHub-Subflows dazu verwendet, die Ressourcenliste aus der Cloud zu importieren. Erstellen Sie nur einen Ressourcensammler pro Ressourcentyp.

Prozedur

1. Erstellen Sie einen IntegrationHub-Subflow für den Konfigurationssammler.

   a. Kopieren Sie den Subflow **CCG – Collector Template** (CCG – Sammlervorlage). Weitere Informationen zum Kopieren von Subflow-Vorlagen finden Sie unter Kopieren Sie eine IntegrationHub Subflow-Vorlage.

   b. Fügen Sie die entsprechende Bibliothek von Cloud-Aktionen(CAL)-Aktion und die Flow-Logik hinzu, um die Ressourcendaten zu lesen.

      Weitere Informationen zu verfügbaren CAL-Aktionen finden Sie unter Bibliothek von Cloud-Aktionen-Aktionsreferenz.

      Wenn die CAL nicht über die erforderliche Aktion verfügt, können Sie auf eine vorhandene CAL-Aktion verweisen und die IntegrationHub-Datenstromaktion verwenden, um die benutzerdefinierte Aktion zu implementieren. Alternativ dazu können Sie auch den REST-Schritt verwenden. Weitere Informationen finden Sie unter Datenstromaktionen und Paginierung und REST-Schritt .

   c. Fügen Sie die Aktion **CCG – Insert Resource Record** (CCG – Ressourcendatensatz einfügen) hinzu und wählen Sie dann die entsprechenden Eingaben aus, um die Konfigurationsdaten in die Configuration Management Database (CMDB) einzufügen. Weitere Informationen zur Aktion **CCG – Insert Resource Record** (CCG – Ressourcendatensatz erstellen) finden Sie unter Governance für Cloud-Konfigurationen-Aktionsreferenz.

   d. Wählen Sie **Veröffentlichen** aus.

2. Navigieren zu **Governance für Cloud-Konfigurationen** > **Ressourcensammler**.
3. Wählen Sie **Neu**.
4. Füllen Sie die Felder des Formulars aus.
   Eine Beschreibung der Feldwerte finden Sie unter Governance für Cloud-Konfigurationen-Formular „Resource collector“ (Ressourcensammler).
5. Wählen Sie **Absenden** aus.

Nächste Maßnahme

- Wenn die erforderlichen Konfigurationsdaten auf Cloud-Ressourcenebene nicht verfügbar sind, siehe Konfigurationsschlüssel erstellen.

- Wenn Sie in der Anwendung Governance für Cloud-Konfigurationen einen neuen Ressourcentyp erstellt haben, können Sie optional eine CI-Finder-Zuordnung für den neu angelegten Ressourcentyp erstellen. Weitere Informationen finden Sie unter CI-Finder-Zuordnung erstellen.

Konfigurationssammler erstellen

Erstellen Sie einen Konfigurationssammler, um festzulegen, wie die Konfigurationsdaten von Governance für Cloud-Konfigurationen aus der Cloud importiert werden.

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

Vom Konfigurationssammler werden IntegrationHub-Subflows dazu verwendet, die Konfigurationsdaten aus der Cloud zu importieren.

Vorbereitungen

- Vergewissern Sie sich, dass Governance für Cloud-Konfigurationen geeignete Konfigurationsschlüssel für alle Konfigurationswerte enthält, die Sie aus der Cloud importieren möchten. Erstellen Sie einen Konfigurationsschlüssel, wenn er in der Anwendung nicht verfügbar ist. Weitere Informationen finden Sie unter Konfigurationsschlüssel erstellen.

Erforderliche Rolle: sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird

Für einige Cloud-Ressourcen sind die erforderlichen Konfigurationsdaten auf Cloud-Ressourcenebene verfügbar. Erstellen Sie deshalb nur dann einen Konfigurationssammler, wenn die erforderlichen Konfigurationsdaten auf Cloud-Ressourcenebene nicht verfügbar sind.

Beispielsweise sind die meisten Konfigurationsdaten des Ressourcentyps **VM-Instanz** auf der Cloud-Ressourcenebene verfügbar. Daher ist kein Konfigurationssammler zum Importieren dieser Konfigurationen implementiert.

Sehen Sie sich einen Basissystem-Konfigurationssammler als Beispiel für das Erstellen der Konfigurationssammler an.

Prozedur

1. Erstellen Sie einen IntegrationHub-Subflow für den Konfigurationssammler.

   a. Kopieren Sie den Subflow **CCG – Collector Template** (CCG – Sammlervorlage). Weitere Informationen zum Kopieren von Vorlagen finden Sie unter IntegrationHub-Subflow-Vorlage kopieren.

   b. Fügen Sie die Aktion **CCG – Get Resources** (CCG – Ressourcen abrufen) hinzu und füllen Sie die Felder aus.

   c. Fügen Sie die entsprechende Bibliothek von Cloud-Aktionen(CAL)-Aktion und die Flow-Logik hinzu, um die Konfigurationsdaten zu lesen.

   Hinweis:

   Weitere Informationen zu verfügbaren CAL-Aktionen finden Sie unter Bibliothek von Cloud-Aktionen-Aktionsreferenz.

   Wenn die CAL nicht über die erforderliche Aktion verfügt, können Sie auf eine vorhandene CAL-Aktion verweisen und den IntegrationHub-REST-Schritt verwenden, um die benutzerdefinierte Aktion zu implementieren. Weitere Informationen finden Sie unter REST-Schritt .

   d. Fügen Sie die Aktion **CCG – Insert Configuration Settings** (CCG – Konfigurationseinstellungen einfügen) hinzu, um die Konfigurationsdaten in der Configuration Management Database (CMDB) einzufügen.

   e. Wählen Sie **Veröffentlichen** aus.

2. Navigieren zu **Governance für Cloud-Konfigurationen** > **Konfigurationssammler**.

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

3. Wählen Sie **Neu**.
4. Füllen Sie die Felder des Formulars aus.

Formular „Configuration Collector“ (Konfigurationssammler)

Feld	Beschreibung
Provider-Typ	Cloud, in der die über die Richtlinien zu scannenden Ressourcen gehostet werden
Flow	Konfigurationssammler, von dem die Konfigurationsdaten aus der Cloud importiert werden können
Ressourcentyp	Cloud-Ressourcentyp, dessen Konfiguration Sie importieren möchten
Name	Name des Konfigurationssammlers
Beschreibung	Kurzbeschreibung des Konfigurationssammlers

5. Wählen Sie **Absenden** aus.

CI-Finder-Zuordnung erstellen

Verwenden Sie die CI-Finder-Zuordnung, um die von den Scan-Ausführungen ServiceNow Governance für Cloud-Konfigurationen abgerufenen Ressourcen mit den entsprechenden Configuration Management Database (CMDB) Configuration Items (CIs) zu verknüpfen, falls verfügbar. Nachdem Sie die Zuordnung erstellt haben, können Sie die gemeldeten Konfigurationsverstöße den CIs zuordnen, zu denen sie gehören.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.scheduling_admin oder sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird
Nachdem Sie einen Ressourcentyp in Governance für Cloud-Konfigurationen erstellt haben, können Sie optional eine CI-Finder-Zuordnung für den neuen Ressourcentyp erstellen. Von Cloud Configuration Governance wird das CI-Finder-Zuordnungsskript für alle von den Scan-Ausführungen abgerufenen Ressourcen aufgerufen.

Prozedur

1. Navigieren zu **Alle** > **Governance für Cloud-Konfigurationen** > **Zuordnungen des CI-Finders**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Zuordnungen des CI-Finders“

Feld	Beschreibung
Provider-Typ	Cloud-Service Provider, der die Ressource hostet.
Ressourcentyp	Ressourcentyp der Cloud-Ressource.
Skript	Skript, über das die von der Anwendung Governance für Cloud-Konfigurationen abgerufenen Ressourcen mit dem vorhandenen CI verknüpft werden.

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

Feld	Beschreibung
	Verwenden Sie ein vorhandenes CI-Finder-Zuordnungsskript als Beispiel, um ein Skript für den neuen Ressourcentyp zu erstellen. Governance für Cloud-Konfigurationen bietet mehrere Objekte und Variablen zur Verwendung im Skript. Weitere Informationen finden Sie unter Governance für Cloud-Konfigurationen-Skriptreferenz.

Richtliniensatz erstellen

Erstellen Sie einen Richtliniensatz in Governance für Cloud-Konfigurationen, um Richtlinien zu gruppieren, die einen bestimmten Sicherheits- oder Organisationsstandard durchsetzen. Wenn der Richtliniensatz von der Scan-Konfiguration ausgeführt wird, werden die Cloud-Ressourcen identifiziert, die nicht den festgelegten Standards entsprechen. Ein Richtliniensatz kann eine oder mehrere Richtlinie(n) enthalten.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.governor

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Richtliniensätze**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Policy Sets“ (Richtliniensätze)

Feld	Beschreibung
Name	Name des Richtliniensatzes
Provider-Typ	Cloud, in der die Ressourcen gehostet werden, die über die dem Richtliniensatz angehängten Richtlinien zu scannen sind
Beschreibung	Kurzbeschreibung des Richtliniensatzes
Richtlinien	Richtlinien, die Sie gruppieren möchten, um einen bestimmten Sicherheits- oder Organisationsstandard durchzusetzen. Der Richtliniensatz kann mehr als eine Richtlinie enthalten.

4. Wählen Sie **Absenden** aus.

IntegrationHub-Subflow-Vorlage kopieren

Kopieren Sie eine IntegrationHub-Subflow-Vorlage, um Subflows für die Anwendung Governance für Cloud-Konfigurationen zu erstellen.

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Prozessautomatisierung** > **Flow Designer**.
2. Wählen Sie **Subflow** aus.

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

3. Suchen Sie in der Spalte „Name“ nach der erforderlichen Subflow-Vorlage und öffnen Sie sie.
4. Wählen Sie das Symbol „Weitere Aktionen“ (“) und wählen Sie dann **Subflow kopieren** aus dem Menü aus.
5. Geben Sie im Feld **Neuer Subflow-Name** einen eindeutigen und beschreibenden Namen für den kopierten Subflow ein.
6. Wählen Sie **Kopieren**.
   Der neue Subflow wird erstellt und als Registerkarte im Subflow-Designer geöffnet.

Fehlerkorrektur

Verwenden Sie die Korrekturaktionen in Governance für Cloud-Konfigurationen, um damit die nicht konformen Cloud-Ressourcenkonfiguration zu beheben, die während der Scan-Ausführungen identifiziert wurden.

Das Modul „Remediationen“ zeigt eine Liste aller verfügbaren Korrekturaktionen für den Satz von Verstoßtypen (Verstoßdefinitionen) an. Governance für Cloud-Konfigurationen bietet mehrere Basissystem-Korrekturaktionen. Wenn die Anwendung die erforderliche Korrekturaktion nicht enthält, können Sie benutzerdefinierte Aktionen erstellen. Weitere Informationen finden Sie unter Korrekturkatalogelement erstellen und Korrekturaktion erstellen.

Da die Korrekturaktionen für die Cloud-Ressourcen von Governance für Cloud-Konfigurationen durchgeführt werden, können Sie optional zusätzliche Genehmigungsanforderungen für die Aktion erzwingen. Immer, wenn der sn_itom_ccg.ccg_operator eine Nachbesserungsanforderung sendet, die eine Genehmigung erfordert, wird von der Anwendung eine Change-Anforderung zum Nachverfolgen der Genehmigung erstellt. Sie können die Liste aller Change-Anforderungen im Modul für Nachbesserungsanforderungen überprüfen.

Hinweis: Ab Governance für Cloud-Konfigurationen Version 1.3.7 wird der Inhalt des Basissystems in das Verzeichnis CCG Inhaltspaketverschoben. Installieren Sie CCG Inhaltspaket, um auf die Inhalte des Basissystems Governance für Cloud-Konfigurationen zuzugreifen.

Korrekturkatalogelement erstellen

Erstellen Sie in Governance für Cloud-Konfigurationen ein anwenderdefiniertes Korrekturkatalogelement für die Korrekturen, die zusätzliche Eingabeparameter erfordern.

Vorbereitungen

Erforderliche Rolle: sn_itom_ccg.governor

Warum und wann dieser Vorgang ausgeführt wird

Einige Korrekturaktionen erfordern zusätzliche Betriebsinformationen, z. B. den Hardwaretyp der Ressource, damit sie ausgeführt werden können. Erstellen Sie für solche Fälle ein Korrekturkatalogelement mit benutzerdefinierten Eingabeparametern oder -variablen, und ordnen Sie es der entsprechenden Korrekturaktion und dem Verstoßtyp zu. Nachdem Sie das Korrekturkatalogelement erstellt haben, kann ein Benutzer mit der Rolle sn_itom_ccg.ccg_operator damit eine Korrekturanforderung stellen.

Prozedur

1. Navigieren zu **Alle** > **Governance für Cloud-Konfigurationen** > **Nachbesserungskatalog**.
2. Öffnen Sie den Datensatz „CCG-Fehlerkorrektur – Standardkatalog“.
3. Wählen Sie **Kopieren**, um das Katalogelement zu kopieren.

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

4. Füllen Sie die Felder des Formulars aus.

Datensatzerstellerformular

Feld	Beschreibung
Name	Name des Governance für Cloud-Konfigurationen-Katalogelements.
Tabellenname	Die Tabelle, in der der Datensatzersteller Datensätze erstellt. Behalten Sie den Standardwert bei.
Besitzer	Besitzer des Katalogelements, der Bearbeitungszugriff darauf hat.
Kurzbeschreibung	Geschäftszweck des Korrekturkatalogelements. In Governance für Cloud-Konfigurationen wird dem Benutzer die Kurzbeschreibung angezeigt.
Aktivieren	Status des Katalogelements. Das kopierte Katalogelement ist standardmäßig aktiv.

5. Wählen Sie **Aktualisieren**.
   Der Datensatzersteller erstellt die folgenden Elemente:
   - Eine Flow Designer-Aktion mit dem Namen <Catalog item name>_Action.
   - Einen Flow Designer-Subflow mit dem Namen <Catalog item name>_Subflow.
   - Einen Nachbesserungsdatensatz für das Katalogelement. Der Nachbesserungsdatensatz ist dem Katalogelement und dem <Catalog item name>_Subflow zugeordnet.
6. Wahlweise: Definieren Sie Katalogelementvariablen, um zusätzliche Informationen durch das Katalogelementformular zu erfassen.
   a. Wählen Sie in der zugehörigen Liste „Variablen " **Neu**.
   b. Füllen Sie die Felder des Formulars aus.
      Weitere Informationen zu Katalogvariablen finden Sie unter Servicekatalogvariablen .
   c. Speichern Sie das Formular.
7. Ordnen Sie das Korrekturkatalogelement dem Verstoßtyp zu.
   a. Wählen Sie in der zugehörigen Liste „Remediationen" die Option **Neu** aus.
   b. Doppelklicken Sie auf die Zelle „Violation (Verstoß)".
   c. Wählen Sie den Verstoßtyp aus.
   d. Wählen Sie das Speichern-Symbol ( ).
8. Aktualisieren Sie die <Catalog item name>_Action zur Interaktion mit der Cloud-Ressource.

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

Von Governance für Cloud-Konfigurationen wird eine IntegrationHub-Aktion dazu verwendet, die Korrektur für die Cloud-Ressource auszuführen. Da geschäftliche Anforderungen die Korrekturlogik vorgeben, wird vom Datensatzersteller nur ein Standardbaustein für die <Catalog item name>_Action erstellt. Sie müssen die <Catalog item name>_Action gemäß den Geschäftsanforderungen implementieren.

a. Navigieren zu **Alle** > **Flow Designer**.

b. Wählen Sie die Registerkarte **Aktionen** aus.

c. Öffnen Sie die <Catalog item name>_Action.

d. Lesen Sie in der Dokumentation des Cloud-Anbieters nach, und implementieren Sie die <Catalog item name>_Action gemäß den Geschäftsanforderungen Ihrer Organisation. Weitere Informationen zum Erstellen von IntegrationHub -Aktionen finden Sie unter Anwenderdefinierte Aktionen erstellen .

e. Speichern Sie die aktualisierte <Catalog item name>_Action.

f. Testen Sie die <Catalog item name>_Action.
Weitere Informationen finden Sie unter Aktion testen .

g. Veröffentlichen Sie die <Catalog item name>_Action.

9. Verknüpfen Sie die <Catalog item name>_Action mit dem <Catalog item name>_Subflow. Von Governance für Cloud-Konfigurationen werden die IntegrationHub-Subflows dazu verwendet, die IntegrationHub-Aktion auszulösen und die zurückgegebenen Daten zu verarbeiten.

a. Navigieren Sie zur Homepage Flow Designer, indem Sie das Flow Designer-Startseitensymbol ( ) wählen.

b. Wählen Sie die Registerkarte **Subflows** aus.

c. Öffnen Sie den <Catalog item name>_Subflow.

d. Wählen Sie **Aktion, Flow-Logik oder Subflow hinzufügen** aus.

e. Wählen Sie **Aktion** aus.

f. Suchen Sie nach `<Catalog item name>_Action`, und wählen Sie die Aktion aus.

g. Fügen Sie die entsprechende Flow-Logik hinzu.

h. Weisen Sie die Ausgabe des Subflows der Ausgabevariablen zu.

i. Testen Sie den <Catalog item name>_Subflow.

j. Veröffentlichen Sie den <Catalog item name>_Subflow, um ihn zu aktivieren.

Nächste Maßnahme

Führen Sie die Korrekturaktion aus, um den erkannten Verstoß zu beheben. Weitere Informationen finden Sie unter Korrektur ausführen.

Korrekturaktion erstellen

Erstellen Sie in Governance für Cloud-Konfigurationen eine Korrekturaktion für die Fehlerkorrekturen, für die keine zusätzlichen Eingabeparameter erforderlich sind.

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

Vorbereitungen
Erforderliche Rolle: sn_itom_ccg.ccg_governer

Warum und wann dieser Vorgang ausgeführt wird
Von Governance für Cloud-Konfigurationen werden IntegrationHub-Subflows dazu verwendet, Fehlerkorrekturen durchzuführen.

Prozedur
1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Fehlerkorrekturen**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Remediationen“

Feld	Beschreibung
Minimum permission required (Erforderliche Mindestberechtigung)	Zum Ausführen der Fehlerkorrektur mindestens erforderliche Cloud-Berechtigungen. Von Governance für Cloud-Konfigurationen werden die Berechtigungsinformationen aus diesem Feld nicht gelesen. Verwenden Sie dieses Feld, um die Berechtigungsinformationen als zukünftige Referenz zu speichern.
Aktion	Korrektur-Flow, mit dem der ausgewählte Verstoß behoben werden kann
Violation (Verstoß)	Verstoß, den Sie beheben möchten
Genehmigung erforderlich	Option zum Erzwingen der Genehmigung für die Korrekturaktion. Weitere Informationen zu Genehmigungen finden Sie unter Genehmigungen .
Beschreibung	Kurze Beschreibung der Korrekturaktion
Korrekturkatalogelement	Name des Korrekturkatalogelements, das zum Auslösen einer Nachbesserungsanforderung verwendet werden kann. Wählen Sie den CCG-Fehlerkorrektur – Standardkatalog aus.

4. Wählen Sie **Absenden** aus.

Nächste Maßnahme
Führen Sie die Korrekturaktion aus, um den erkannten Verstoß zu beheben. Weitere Informationen finden Sie unter Korrektur ausführen.

Korrektur ausführen

Führen Sie die entsprechende Korrekturaktion aus, um die nicht konforme Cloud-Konfiguration zu beheben, die während der Scan-Ausführung von Governance für Cloud-Konfigurationen identifiziert wurde.

Vorbereitungen
- Die Scan-Ausführung ist abgeschlossen.
- Erforderliche Rolle: sn_itom_ccg.ccg_operator

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

Prozedur

1. Navigieren zu **Governance für Cloud-Konfigurationen** > **Scan-Ausführung**.
2. Öffnen Sie die Scan-Ausführung, in der von **Cloud Configuration Governance** die Audit-Probleme gemeldet wurden.
3. Wählen Sie **Audit-Ergebnisse anzeigen** aus.
4. Wählen Sie den Verstoßtyp aus, den Sie beheben möchten.
   Von Governance für Cloud-Konfigurationen werden die Verstöße nach dem Verstoßtyp gruppiert. Während der Ausführung einer Fehlerkorrektur können Sie nur Verstöße desselben Typs beheben.
5. Wählen Sie mindestens einen Verstoß aus.
6. Wählen Sie **Beheben** aus.

   Hinweis: Sie können **Vorerst ignorieren** auswählen, um das Problem zu ignorieren. Wenn Sie ein Problem ignorieren, wird das Problem von Governance für Cloud-Konfigurationen nicht als Verstoß gemeldet und nicht in den Dashboard-Berichten dargestellt.

7. Überprüfen Sie die Liste der für die Fehlerkorrektur ausgewählten Ressourcen.
8. Wählen Sie die Korrekturaktion aus.
9. Wählen Sie **OK** aus.

Ergebnisse

Nächste Maßnahme

Wählen Sie in der zugehörigen Liste „Ausführungen der Fehlerkorrektur“ die Change-Anforderung aus, und überprüfen Sie den Status der Fehlerkorrektur. Sie können auch die Liste aller Nachbesserungsanforderungen im Modul für Nachbesserungsanforderungen anzeigen.

Governance für Cloud-Konfigurationen-Referenz

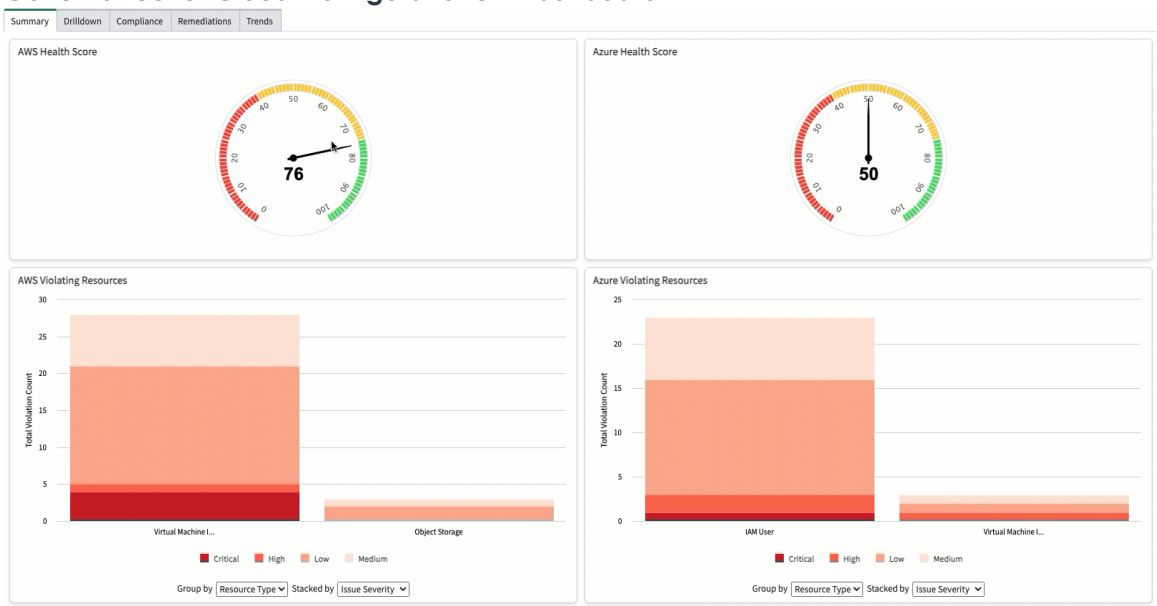
Referenzthemen enthalten zusätzliche Informationen zur Anwendung Governance für Cloud-Konfigurationen.

Governance für Cloud-Konfigurationen-Dashboard

Governance für Cloud-Konfigurationen ist ein Tool zum Verwalten der Konfiguration der Cloud-Ressourcen gemäß Ihren Organisationsstandards und etablierten Sicherheitsstandards. Verwenden Sie das Dashboard, um die Integritätspunktzahl der Cloud, Statistiken zu Richtlinienverstößen, Trends bei Richtlinienverstößen, Fehlerkorrekturen und mehr zu überprüfen.

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

Governance für Cloud-Konfigurationen-Dashboard



Erforderliche Now Platform-Rollen

zum Anzeigen des Dashboards und seiner Widgets ist die Rolle sn_itom_ccg.ccg_operator oder sn_itom_ccg.report_viewer erforderlich.

Zugriff auf das Dashboard von Governance für Cloud-Konfigurationen

Um das Dashboard zu öffnen, wechseln Sie zu: **Governance für Cloud-Konfigurationen** > **Dashboard**.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
sn_itom_ccg.ccg_operator oder sn_itom_ccg.report_viewer	• Cloud-Integritätspunktzahl überprüfen • Zur Korrektur der identifizierten Richtlinienverstöße eingesetzte Zeit • Den Trend des Richtlinienverstoßes nachvollziehen

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Cloud health score (Cloud-Integritätspunktzahl)	Tachodiagramm	sn_itom_ccg_scan_summary	Prozentsatz der gescannten Cloud-Ressourcen, für die kein Audit-Problem vorliegt

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

Titel	Typ	Quelltabelle	Beschreibung
Violating resources (Verstoßende Ressourcen)	Gestapeltes Balkendiagramm	sn_itom_ccg_scan_summary	Schweregrad der erkannten Audit-Probleme pro Cloud-Ressourcentyp
Violations count (Verstoßanzahl)	Ringdiagramm	sn_itom_ccg_violation_stats	Verstoß pro Schweregrad des Audit-Problems
Scanned resources (Gescannte Ressourcen)	Ringdiagramm	sn_itom_ccg_scan_summary	Anzahl der pro Cloud-Ressourcentyp gescannten Cloud-Ressourcen. Verwenden Sie die **CCG-Drilldown-Filter**, um die Daten zu filtern und die gewünschten Daten zu visualisieren.
Probleme	Horizontales Balkendiagramm	sn_itom_ccg_audit_stats	Anzahl der pro Verstoßdefinition gemeldeten Verstöße. Im Diagramm können maximal 10 Balken angezeigt werden, d. h. einer pro Verstoßdefinitionstyp. Wenn die Daten mehr als 10 Verstoßdefinitionstypen enthalten, werden alle zusätzlichen Verstoßdefinitionstypen im Balken **Sonstige** zusammengeführt. Verwenden Sie die **CCG-Drilldown-Filter**, um die Daten zu filtern und die gewünschten Daten zu visualisieren.
Richtlinien-Compliance	Eingebettete Listen	sn_itom_ccg_policy_compliance_stats	Zeigt die folgenden Informationen für die angegebene Richtlinie an:

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

Titel	Typ	Quelltabelle	Beschreibung
			• Anzahl der konformen Ressourcen • Anzahl der nicht konformen Ressourcen
Policy set compliance (Richtliniensatz-Compliance)	Eingebettete Listen	sn_itom_ccg_policy_set_compliance_stats	Zeigt die folgenden Informationen für den angegebenen Richtliniensatz an: • Anzahl der konformen Ressourcen • Anzahl der nicht konformen Ressourcen
Total issues remediated (Gesamtzahl der korrigierten Probleme)	Halbes Ringdiagramm	sn_itom_ccg_remediation_daily_trend	Anzahl der Korrekturen nach Verstoßdefinitionstyp
Remediations by type (Fehlerkorrekturen nach Typ)	Kreisdiagramm	sn_itom_ccg_remediation_daily_trend	Anzahl der Korrekturen pro Cloud-Ressourcentyp
Remediated on (Korrigiert in)	Halbes Ringdiagramm	sn_itom_ccg_remediation_daily_trend	Zeit, die zum Korrigieren der Verstöße benötigt wurde
Trend	Liniendiagramm	sn_itom_ccg_daily_trend	Trend der Meldung von Verstößen im Zeitverlauf

Filter

Name	Typ	Beschreibung
CCG-Drilldown-Filter	Auswahlbasierter Filter	Verwenden Sie diesen Filter, um den Cloud Provider, das Cloud-Konto und die Regionen für die Visualisierung der gescannten Ressourcen und Problemdaten auszuwählen.

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

Governance für Cloud-Konfigurationen-Rollen und -Systemeigenschaften

Benutzer von Governance für Cloud-Konfigurationen benötigen die entsprechenden Rollen und Systemeigenschaften, um verschiedene Aktivitäten auszuführen. Diese Rollen und Systemeigenschaften werden mit der Aktivierung der Anwendung installiert.

Nur Benutzer mit der Rolle user_admin oder admin können Benutzer mit diesen Rollen erstellen:

Governance für Cloud-Konfigurationen-Rollen

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Verschachtelte Rollen
sn_itom_ccg.scheduling_admin	Ein Planungsadministrator kann die folgenden Aktionen ausführen: • Scan-Zeitpläne erstellen. • CI-Finder-Zuordnungen erstellen.	discovery_admin
sn_itom_ccg.governor	Ein Benutzer mit der Rolle „Kontrolle“ kann die folgenden Aktionen ausführen: • Richtlinien über Bedingungsgenerator, IntegrationHub-Flows oder Skript erstellen • Erstellt einen Richtliniensatz. • Ressourcensammler erstellen • Konfigurationsschlüssel erstellen • Fehlerkorrektur erstellen • CI-Finder-Zuordnungen erstellen.	• flow_designer • action_designer • catalog_admin
sn_itom_ccg.ccg_operator	Ein Operator kann die folgenden Aktionen ausführen: • Audit-Problemberichte anzeigen • Korrektur ausführen • Scan-Konfigurationen ausführen • Dashboard anzeigen	• flow_operator • sn_change_write
sn_itom_ccg.report_viewer	Ein Berichtbetrachter kann folgende Aktionen ausführen: • Audit-Problemberichte anzeigen • Dashboard anzeigen	

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

Governance für Cloud-Konfigurationen-Systemeigenschaften

Name der Eigenschaft	Beschreibung
snc_af.log_level	Wenn Sie diese Eigenschaft aktivieren, werden die Protokolle von Governance für Cloud-Konfigurationen in das Syslog geschrieben. Die folgenden Protokollebenen werden unterstützt: • DEBUG • INFO • WARN • ERROR • AUS Vergewissern Sie sich, dass der Anwendungsbereich **Global** ist, wenn Sie diese Eigenschaft festlegen oder löschen.

Zugehörige Informationen

Einem Benutzer eine Rolle zuweisen

Governance für Cloud-Konfigurationen-Formular zum Konfigurieren von Scans

Im Governance für Cloud-Konfigurationen-Formular zum Konfigurieren von Scans werden detaillierte Informationen zur Scan-Konfiguration angezeigt.

Feld	Beschreibung
Name	Name, der die Scan-Konfiguration eindeutig identifiziert
Beschreibung	Kurze Beschreibung der Scan-Konfiguration.

Konfigurationsregisterkarte

Legen Sie die Konfigurationseinstellungen fest, z. B. Cloud Provider, Richtliniensätze, Zielservicekonten und Rechenzentren für den Scan.

Feld	Beschreibung
Cloud provider type (Typ des Cloud Providers)	Cloud, die die zu scannenden Ressourcen hostet.
Policy sets (Richtliniensätze)	Richtliniensätze für den Scan. Wählen Sie mindestens einen Richtliniensatz für den Scan aus und speichern Sie das Formular.
Rechenzentrumsfilter	Servicekonto oder Kombination aus Servicekonto und Rechenzentrum für den Scan.

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

Feld	Beschreibung
	1. Doppelklicken Sie in der leeren Zeile der Liste „Rechenzentrumsfilter“ auf die Zelle des Servicekontos und wählen Sie dann ein Servicekonto aus. Sie können ein Verwaltungskonto für Amazon Web Services (AWS) auswählen und dann der Scan-Konfiguration alle zugehörigen Mitgliedskonten hinzufügen, sofern die folgenden Bedingungen erfüllt sind: ◦ Für das Verwaltungskonto ist eine Konfiguration für die Übernahme von Rollen vorhanden. ◦ Von Cloud-Discovery wurde die Rechenzentrumserkennung für die Mitgliedskonten abgeschlossen. Weitere Informationen zum Erstellen von Konfigurationen für die Übernahme von Rollen finden Sie unter Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren. **2.** Speichern Sie das Formular. **3.** Doppelklicken Sie in der leeren Zeile der Liste „Rechenzentrumsfilter“ auf die Zelle des Rechenzentrums und wählen Sie dann ein Rechenzentrum aus. (Optional) Wenn Sie kein Rechenzentrum auswählen, werden von Governance für Cloud-Konfigurationen alle Rechenzentren gescannt, die dem Servicekonto zugeordnet sind.

Registerkarte „Filter“

(Optional) Geben Sie Kriterien zum Filtern der Cloud-Ressourcen an und importieren Sie dann ihre Konfigurationsdaten aus der Cloud. Wenn angegeben, werden von Governance für Cloud-Konfigurationen ausschließlich die Konfigurationen der Ressourcen abgerufen, die den Filterkriterien entsprechen. Andernfalls werden die Konfigurationen aller Cloud-Ressourcen abgerufen.

Feld	Beschreibung
Tag-Filter	Cloud-Ressourcen-Tags zum Filtern der Cloud-Ressourcen • Geben Sie den Tag-Namen in das Feld **Name** ein. • Geben Sie den Tag-Wert in das Feld **Wert** ein.
Freihandform	Option zur Angabe einer kommagetrennten Liste von Cloud-Bezeichnern zum Filtern der Cloud-Ressourcen
Ressourcen	Kommagetrennte Liste der Cloud-Bezeichner. Dieses Feld wird nur angezeigt, wenn die Option **Freihandform** ausgewählt ist.

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

Governance für Cloud-Konfigurationen-Formular „Richtlinie“

Im Governance für Cloud-Konfigurationen-Formular „Richtlinie“ werden detaillierte Informationen zur Richtlinie angezeigt, z. B. Cloud Provider, Ressourcentyp, Richtlinientyp und Einstellungen für die Meldung von Richtlinienverstößen.

Feld	Beschreibung
Richtlinienname	Name, der die Richtlinie eindeutig identifiziert
Beschreibung	Kurzbeschreibung der Richtlinie

Ressourcentyp

Definieren Sie den Ressourcentyp, für den Sie die Richtlinie erstellen möchten.

Feld	Beschreibung
Cloud Provider	Cloud, die die zu scannenden Ressourcen hostet.
Ressourcentyp	Cloud-Ressourcentyp, der über die Richtlinie gescannt werden soll. Wenn der erforderliche Ressourcentyp nicht verfügbar ist, können Sie einen Ressourcentyp erstellen. Weitere Informationen finden Sie unter Ressourcensammler erstellen.

Richtlinienbedingung

Definieren Sie den Richtlinientyp und die nicht konforme Ressourcenkonfiguration.

Feld	Beschreibung
Typ	Governance für Cloud-Konfigurationen unterstützt die folgenden Typen: • **Bedingungsgenerator**: Die Methode ohne Code zum Erstellen von Richtlinien. • **IntegrationHub-Flow**: Die Methode mit wenig Code zum Erstellen von Richtlinien. • **Skript**: Die code-basierte Methode zum Erstellen von Richtlinien. Wählen Sie das Symbol zum Anzeigen verfügbarer Schlüssel ( ) aus, um die Liste aller verfügbaren Konfigurationsschlüssel für den ausgewählten Ressourcentyp anzuzeigen. Sie können einen beliebigen Schlüssel in der Richtlinie verwenden.
Bedingung	Bedingungen für die Meldung der nicht konformen Cloud-Ressourcenkonfiguration. Geben Sie immer den Schlüssel und den Wert als Paar an. Verwenden Sie die Operatoren **ODER** und **UND**, um logische Operationen in der Richtlinienbedingung auszuführen. **Syntax**

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

Feld	Beschreibung

	`Key is <key_name>`
	`<data_type> Value <condition> <value>`
	
	Beispiel:
	
	`Key is AWS:IAM:User:PasswordEnabled`
	`Boolean Value is true`
	
	Dieses Feld wird nur angezeigt, wenn im Feld **Typ** die Option **Bedingungsgenerator** ausgewählt wird.

Konfigurationsschlüssel	Konfigurationsschlüssel für die Richtlinie. Dieses Feld wird nur angezeigt, wenn für das Feld **Typ** die Option **IntegrationHub Flow** ausgewählt wird.
Integration flow (Integrations-Flow)	Der entsprechende IntegrationHub-Flow. Dieses Feld wird nur angezeigt, wenn für das Feld **Typ** die Option **IntegrationHub Flow** ausgewählt wird.
Bedingungsskript	Skript, mit dem die Richtlinienbedingungen zum Identifizieren und melden von Richtlinienverstößen implementiert werden. Governance für Cloud-Konfigurationen enthält mehrere skriptfähige Objekte und Variablen zur Verwendung in den Richtlinienskripts. Weitere Informationen finden Sie unter Skriptreferenz. Sie können Skripteinbindungen erstellen, um die Entscheidungsfindung zu externalisieren und den Code für verschiedene Skripts wiederverwenden. Weitere Informationen zum Erstellen der Skripteinbindungen finden Sie unter Skripteinbindungen . **Hinweis:** Wenn Sie einen benutzerdefinierten Audit-Ergebnisdatensatz über das Skript erstellen, wird die in der Richtlinie definierte Konfiguration für **Audit Violation Reporting** (Audit-Verstoßberichte) nicht wirksam. Dieses Feld wird nur angezeigt, wenn im Feld **Typ** die Option **Skript** ausgewählt wird.

Audit-Verstoßberichte

Definieren Sie, der Richtlinienverstoß von Governance für Cloud-Konfigurationen gemeldet wird.

Feld	Beschreibung
Report violation	Verstoßdefinition, die in den Audit-Verstoßbericht aufgenommen werden soll. Von Governance für Cloud-Konfigurationen wird die Verstoßdefinition dazu verwendet, die Nichteinhaltung von Richtlinien zu melden.

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

Feld	Beschreibung
as (Verstoß melden als)	Wenn keine geeignete Verstoßdefinition verfügbar ist, können Sie wie folgt eine erstellen: **1.** Wählen Sie das Symbol „Nachschlagen mit Liste“ ( ) aus. **2.** Wählen Sie **Neu**. **3.** Geben Sie einen Namen ein, der die Verstoßdefinition eindeutig identifiziert. Von Governance für Cloud-Konfigurationen wird der Name der Verstoßdefinition in den Audit-Problembericht aufgenommen. **4.** Wählen Sie den Standardschweregrad für die Verstoßdefinition aus. **5.** (Optional) Geben Sie eine kurze Beschreibung des Verstoßes ein.
Schweregrad	Schweregrad des Verstoßes. Wenn Sie den Schweregrad in der Richtlinie nicht auswählen, verwendet Governance für Cloud-Konfigurationen den in der Verstoßdefinition definierten Standardschweregrad.

Governance für Cloud-Konfigurationen-Formular „Konfigurationsschlüssel“

Das Formular „Konfigurationsschlüssel“ enthält detaillierte Informationen zum Konfigurationsschlüssel.

Formular „Konfigurationsschlüssel“

Name	Beschreibung
Name	Name, der den Konfigurationsschlüssel eindeutig identifiziert.
Beschreibung	Kurze Beschreibung des Konfigurationsschlüssels.
Provider-Typ	Cloud, in der die über die Richtlinien zu scannenden Ressourcen gehostet werden
Ressourcentyp	Cloud-Ressourcentyp.
Werttyp	Datentyp des Konfigurationswerts, der dem Konfigurationsschlüssel zugeordnet ist.
Resource collector (Ressourcensammler)	Ressourcensammler, der die Konfigurationsdaten für den ausgewählten Ressourcentyp erfassen kann.
Configuration collector (Konfigurationssammler)	(Optional) Konfigurationssammler, von dem die Konfigurationsschlüssel importiert werden können. Wenn die erforderlichen Konfigurationsdaten nicht auf Cloud-Ressourcenebene verfügbar sind, wählen Sie den Konfigurationssammler aus, von dem die Konfigurationsschlüssel importiert werden können. Wenn kein geeigneter Konfigurationssammler verfügbar ist, erstellen Sie einen Konfigurationssammler und wählen Sie ihn aus. Weitere Informationen zum Erstellen des Konfigurationssammlers finden Sie unter Konfigurationssammler erstellen.

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

Governance für Cloud-Konfigurationen-Formular „Resource collector“ (Ressourcensammler)

Das Formular „Ressourcensammler“ (Ressourcensammler) enthält detaillierte Informationen zum Ressourcensammler.

Formular „Resource collector“ (Ressourcensammler)

Feld	Beschreibung
Name	Name, der den Konfigurationsschlüssel eindeutig identifiziert.
Scan mode (Scan-Modus)	Ebene, auf der die Ressource vom Ressourcensammler aus der Cloud importiert wird. Folgende Werte werden unterstützt: • **Run per LDC** (Ausführung pro LRZ): Importieren Sie die Ressource auf Rechenzentrumsebene. Das heißt, einmal aus jedem Rechenzentrum. • **Run per service account** (Ausführung pro Servicekonto): Importieren Sie die Ressource auf Servicekontoebene.
Provider-Typ	Cloud, in der die zu importierenden Ressourcen gehostet werden
Ressourcentyp	Cloud-Ressourcentyp, den Sie über den Ressourcensammler importieren möchten. Wenn Governance für Cloud-Konfigurationen nicht den erforderlichen Ressourcentyp enthält, können Sie ihn wie folgt erstellen: **1.** Wählen Sie das Symbol „Nachschlagen mit Liste“ ( ) aus. **2.** Wählen Sie **Neu**. **3.** Geben Sie im Feld **Name** den Cloud-Ressourcentyp ein. **4.** Wählen Sie **Absenden** aus.
Flow	Ressourcensammler-Flow, mit dem der angegebene Ressourcentyp importiert werden kann

Governance für Cloud-Konfigurationen Formular „Konfiguration der Rollenübernahme für Servicekonto“.

Das Formular Governance für Cloud-Konfigurationen Konfiguration der Rollenübernahme für Service-Account zeigt detaillierte Informationen über die Konfiguration der Rollenübernahme für den Zugriff auf das vertrauende Konto an.

Formular „Konfiguration der Rollenübernahme für Servicekonto“.

Feld	Beschreibung
Name der Zugriffsrolle	Name der IAM-Rolle (Identity and Access Management), die für das vertrauende Konto erstellt wurde und dem vertrauenswürdigen Konto (Zugriffsberechtigten) den Zugriff auf das vertrauende Konto ermöglicht. Um die Mitgliedskonten mithilfe des Verwaltungskontos zu scannen, geben Sie in dieses Feld OrganizationAccountAccessRole ein. Wenn Sie

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

Formular „Konfiguration der Rollenübernahme für Servicekonto“. (Fortsetzung)

Feld	Beschreibung
	OrganizationAccountAccessRole nicht für den Zugriff auf den Mitgliedsaccount verwenden möchten, geben Sie den Namen der IAM-Rolle ein, die für den Mitgliedsaccount erstellt wurde. Um das vertrauende Konto durch Verwendung des vertrauenswürdigen Kontos zu scannen, geben Sie den Namen der IAM-Rolle ein, die für das vertrauende Konto erstellt wurde.
Service-Account	Name des Service-Accounts, in dem die Rolle „Annehmen“ vorhanden ist.
Name der Rollensitzung	Ein Bezeichner für die Sitzung mit übernommener Rolle. Ändern Sie den Standardwert nicht.
Anmeldeinformationsalias	Optional: Anmeldeinformationsalias für die AWS -Anmeldeinformationen.

Governance für Cloud-Konfigurationen-Skriptreferenz

Von Governance für Cloud-Konfigurationen werden mehrere Objekte und Variablen bereitgestellt, mit denen Sie skriptbasierte Richtlinien und CI-Finder-Zuordnungsskripts erstellen können.

Skriptingreferenz für die Governance für Cloud-Konfigurationen-Richtlinien

Governance für Cloud-Konfigurationen-Objekte

Name	Beschreibung	Schema
`configSettings`	Stellt die aus der Cloud importierten Konfigurationsdaten dar.	`[ { "config_key":"configuration_key", "type":"data_type", "value":"configuration_value" }, ... ]`
`current`	Stellt das aktuelle Glide-Datensatzobjekt für den ausgewählten Ressourcentyp dar.	Es enthält die folgenden Felder: • Name: Name der Ressource • Typ: Ressourcentyp

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

Governance für Cloud-Konfigurationen-Objekte (Fortsetzung)

Name	Beschreibung	Schema
		• Bezeichner: Eindeutiger Bezeichner der Cloud-Ressource • Details: cloudressourcenspezifische Details
`resourceInformation`	Ressourcendatensatz und seine Attribute.	`[ { "attribute": "Attribute name", "tableName" : "Referenced table", "documentId": "Referenced record", }, ... ]`
`auditResult`	Audit-Details, die in die Configuration Management Database (CMDB) geschrieben werden müssen.	`{ "details": "Violation definition "' "severity": "severity of the violation", "auditViolationName": "Violation name" };`

Governance für Cloud-Konfigurationen-Variablen

Name	Datentyp	Beschreibung
`answer`	Boolescher Wert	Mit dieser Variablen wird angegeben, ob gemäß der Richtlinie der Verstoß gemeldet wird oder nicht. • `true`: Verstoß melden. Erstellen Sie das Objekt auditResult, um einen benutzerdefinierten Audit-Ergebnisdatensatz in der CMDB zu erstellen. Wenn Sie kein Audit-Ergebnisobjekt erstellen, wird der Verstoß gemäß der in der Richtlinie angegebenen Verstoßdefinition von Governance für Cloud-Konfigurationen gemeldet. • `false`: Verstoß nicht melden.

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

Governance für Cloud-Konfigurationen-Variablen (Fortsetzung)

Name	Datentyp	Beschreibung
`violatingConfigSettings`	JSON	Grund des Richtlinienverstoßes. **Syntax** `{ "config_key": "value" };`

Skriptingreferenz für das CI-Finder-Zuordnungsskript

Governance für Cloud-Konfigurationen-Objekte

Name	Beschreibung	Schema
`attributes`	Eine Zuordnung, die den Ressourcenattributschlüssel und den Attributwert aus der Ressourcenattributtabelle für die angegebene Ressource enthält.	`{ "LogicalDatacenter": "Referenced record", "ServiceAccount": "Referenced record" }`

Governance für Cloud-Konfigurationen-Variablen

Name	Datentyp	Beschreibung
`Name`	Zeichenfolge	Name der Ressource
`Kennung`	Ressourcendatensatz	Bezeichner des Governance für Cloud-Konfigurationen-Ressourcendatensatzes.
`type`	Ressourcendatensatz	Ressourcentyp der Governance für Cloud-Konfigurationen-Ressource.
`answer`	JSON	CI-Klasse, der die Ressource zugeordnet werden muss. Die `Antwort` enthält die folgenden Informationen: • `sysId` der CI-Klasse. • `tableName` der CI-Klasse. Wenn die CI-Klasse mithilfe der CI-Finder-Zuordnung nicht identifiziert wird, legen Sie diese Variable auf `null` fest. **Syntax**

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

Governance für Cloud-Konfigurationen-Variablen (Fortsetzung)

Name	Datentyp	Beschreibung
		`{ sysId: "value", tableName: "value" }`

Governance für Cloud-Konfigurationen-Aktionsreferenz

Von Governance für Cloud-Konfigurationen (CCG) werden IntegrationHub-Subflows dazu verwendet, mit der Cloud zu interagieren und die Konfigurationsdaten in der Configuration Management Database (CMDB) zu aktualisieren.

CCG – Read Config Setting (CCG – Konfigurationseinstellung lesen)

Verwenden Sie diese Aktion, um die Konfigurationsdaten der Ressource zu lesen.

Um diese Aktion zu verwenden, fügen Sie eine Aktion ein, und navigieren Sie dann zu **Aktion** > **Governance für Cloud-Konfigurationen** > **Dienstprogramme** > **CCG – Read Config Setting (CCG – Konfigurationseinstellung lesen)**.

Aktion „CCG – Read Config Setting“ (CCG – Konfigurationseinstellung lesen)

Feld	Beschreibung
Ressource [Ressource]	Ressourcendatensatz, der die Konfigurationsdaten enthält.
Konfigurationsschlüssel [Konfigurationsschlüssel]	Konfigurationsschlüssel, den Sie lesen möchten.

Unterablauf-Ausgaben zuweisen

Formular „Subflow-Ausgaben zuweisen“

Feld	Beschreibung
Vorfall melden	Option, mit der der Audit-Verstoß über den Subflow gemeldet werden kann. Wählen Sie die Option **Vorfall melden** in der Spalte „Daten“ aus oder deaktivieren Sie dieses Kontrollkästchen, um dieses Feld festzulegen oder zu löschen. • Ausgewählt: Meldet das Problem gemäß der im Feld **Audit Violation Reporting** (Audit-Verstoßberichte) der Richtlinie ausgewählten Verstoßdefinition. • Deaktiviert: Der Verstoß wird von Governance für Cloud-Konfigurationen nicht gemeldet. Erstellen Sie einen benutzerdefinierten Datensatz für den Audit-Verstoß. Sie können Bedingungen angeben, um die Erstellung des Audit-Verstoßdatensatzes zu steuern.
Details	Verstoßdefinition, die Sie für den Verstoß melden möchten. Geben Sie die Definition des Verstoßes in der Spalte „Daten“ in das Feld **Details** ein. Dieses Feld ist erforderlich, wenn Sie die Option **Vorfall melden** ausgewählt haben.

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

Datensatz erstellen

Verwenden Sie diese Aktion, um einen Datensatz in der CMDB zu erstellen.

Um diese Aktion zu verwenden, fügen Sie eine Aktion ein, und navigieren Sie dann zu **Aktion** > **ServiceNow Core** > **Standard** > **Datensatz erstellen**.

Aktion „Datensatz erstellen“

Feld	Beschreibung
Tabelle	Name der Configuration Management Database (CMDB)-Tabelle, in der das Audit-Ergebnis gespeichert wird. Legen Sie dieses Feld auf „Audit-Ergebnis“ [sn_itom_ccg_audit_result] fest.
Felder	Details des Datensatzes, den Sie in der Configuration Management Database (CMDB) erstellen möchten. Fügen Sie die folgenden Felder hinzu und konfigurieren Sie die Eingabe für sie: • **Scan Run** (Scan-Ausführung): Scan-Ausführung, bei der das Audit-Problem von Governance für Cloud-Konfigurationen identifiziert wurde. • **Ist Testausführung**: Gibt an, ob das Audit-Problem während einer Testausführung von Governance für Cloud-Konfigurationen gemeldet wurde. • **Details**: Details des Verstoßes. • **Violation Definition** (Verstoßdefinition): Verstoßdefinition des Audit-Problems. • **Ressource**: Cloud-Ressource, für die das Audit-Problem von Governance für Cloud-Konfigurationen ausgelöst wurde. • **Schweregrad**: Schweregrad des Audit-Problems.

CCG – Insert Resource Record (CCG – Ressourcendatensatz einfügen)

Verwenden Sie diese Aktion, um einen Ressourcendatensatz in die Configuration Management Database (CMDB) einzufügen.

Um diese Aktion zu verwenden, fügen Sie eine Aktion ein, und navigieren Sie dann zu **Aktion** > **Governance für Cloud-Konfigurationen** > **Dienstprogramme** > **CCG – Insert Resource Record (CCG – Ressourcendatensatz einfügen)**.

Aktion „CCG – Insert Resource Record“ (CCG – Ressourcendatensatz einfügen)

Feld	Beschreibung
Scan-Ausführung	Scanausführung, für die der Ressourcendatensatz vom Subflow erstellt werden muss.
Servicekonto	Servicekonto, an das die Ressource angehängt ist.
Logisches Rechenzentrum	Logisches Rechenzentrum, an das die Ressource angehängt ist.
Bezeichner	Bezeichner des Ressourcendatensatzes.
Name	Name der Ressource

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

Aktion „CCG – Insert Resource Record“ (CCG – Ressourcendatensatz einfügen) (Fortsetzung)

Feld	Beschreibung
Typ	Ressourcentyp
Anbieter	Cloud Provider, der die Ressource hostet.
Details	Details des Objekts, das Sie im Ressourcendatensatz speichern möchten.
Attribute	Jedes zusätzliche Ressourcenattribut, das Sie in die CMDB importieren möchten.

Bibliothek von Cloud-Aktionen-Aktionsreferenz

Bibliothek von Cloud-Aktionen (CAL) bietet verschiedene Aktionen, mit denen Sie die IntegrationHub-Subflows für Governance für Cloud-Konfigurationen erstellen können.

Bibliothek von Cloud-Aktionen bietet die folgenden Aktionen:

- CAL – AWS generate credential report (CAL – AWS-Anmeldeinformationsbericht generieren)
- CAL – AWS S3 get encryption (CAL – AWS S3-Verschlüsselung abrufen)
- CAL – Azure VM monitoring metric data (CAL – Metrikdaten für Azure-VM-Monitoring)
- AWS turn off EC2 instance (AWS EC2-Instanz deaktivieren)
- CAL – AWS list VMs (CAL – VMs auflisten)
- CAL – AWS list S3 buckets (CAL – AWS S3-Buckets auflisten)
- AWS put S3 bucket encryption (AWS S3-Bucket-Verschlüsselung platzieren)
- AWS enable EC2 instance monitoring (AWS EC2-Instanz-Monitoring aktivieren)
- CAL – Azure VM IP metric (CAL – Azure-VM-IP-Metrik)
- Azure turn off virtual machine (Azure-VM ausschalten)
- AWS get IAM login profile (AWS IAM-Anmeldeprofil abrufen)
- Disable AWS IAM user (AWS IAM-Benutzer deaktivieren)
- AWS list images (AWS-Images auflisten)
- CAL – Azure list VMs (CAL – VMs auflisten)

Die Aktionen von Bibliothek von Cloud-Aktionen sind in den Kategorien **Standard** und **Extern** verfügbar.

Cloud-Berechtigungen, die zum Erfassen der Konfigurationsschlüssel des Governance für Cloud-Konfigurationen-Basissystems erforderlich sind

Governance für Cloud-Konfigurationen erfordert geeignete Cloud-Berechtigungen zum Erfassen der Konfigurationsschlüssel des Basissystems aus der Cloud. Daher müssen Sie die entsprechenden Berechtigungen in der Cloud entsprechend den Anforderungen Ihrer Organisation festlegen.

Hinweis: Ab Governance für Cloud-Konfigurationen Version 1.3.7 wird der Inhalt des Basissystems in das Verzeichnis CCG Inhaltspaketverschoben. Installieren Sie CCG Inhaltspaket, um auf die Inhalte des Basissystems Governance für Cloud-Konfigurationen zuzugreifen.

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

Amazon Web Services (AWS)-Rechenzentrum

Governance für Cloud-Konfigurationen verwendet die folgenden Elemente, um den Konfigurationsschlüssel für die Konfigurationsschlüssel des AWS-Rechenzentrums zu erfassen:

- Ressourcensammler: Cloud-Servicekonto
- Verwendete Cloud-API: Aktion: `DescribeRegions`
- Cloud-Berechtigungen: `ec2: DescribeRegions`

Konfigurationsschlüssel für AWS-Rechenzentrum

Konfigurationsschlüssel	Datentyp
AWS:EC2:VM:DescribeRegions	*String*

AWS Identity and Access Management (IAM)-Benutzer

Governance für Cloud-Konfigurationen verwendet die folgenden Elemente, um die Konfigurationsschlüssel für AWS IAM-Benutzer zu erfassen:

- Ressourcensammler: AWS IAM User Data Collector
- Verwendete Cloud-API:
  - Aktion: `GetCredentialReport` und `GenerateCredentialReport`
  - Service: `AWS IAM service`
- Cloud-Berechtigungen: `Iam:GetCredentialReport` und `Iam:GenerateCredentialReport`

Konfigurationsschlüssel für AWS IAM-Benutzer

Konfigurationsschlüssel	Datentyp
AWS:IAM:Policy:ARN	*String*
AWS:IAM:Policy:AttachmentCount	*String*
AWS:IAM:Policy:CreateDate	*String*
AWS:IAM:Policy:PolicyName	*String*
AWS:IAM:Policy:UpdateDate	*String*
AWS:IAM:User:AccessKey1.active	*Boolean*
AWS:IAM:User:AccessKey1.lastRotated	*Date*
AWS:IAM:User:AccessKey1.lastUsedDate	*Date*
AWS:IAM:User:AccessKey1.lastUsedRegion	*String*
AWS:IAM:User:AccessKey1.lastUsedService	*String*
AWS:IAM:User:AccessKey2.active	*Boolean*
AWS:IAM:User:AccessKey2.lastRotated	*Date*
AWS:IAM:User:AccessKey2.lastUsedDate	*Date*
AWS:IAM:User:AccessKey2.lastUsedRegion	*String*

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

Konfigurationsschlüssel für AWS IAM-Benutzer (Fortsetzung)

Konfigurationsschlüssel	Datentyp
AWS:IAM:User:AccessKey2.lastUsedService	*String*
AWS:IAM:User:Certificate1.active	*Boolean*
AWS:IAM:User:Certificate1.lastRotated	*Date*
AWS:IAM:User:Certificate2.active	*Boolean*
AWS:IAM:User:Certificate2.lastRotated	*Date*
AWS:IAM:User:CreationTime	*Date*
AWS:IAM:User:LoginProfile.active	*Boolean*
AWS:IAM:User:MfaEnabled	*Boolean*
AWS:IAM:User:PasswordEnabled	*Boolean*
AWS:IAM:User:PasswordLastChanged	*String*
AWS:IAM:User:PasswordLastUsed	*Date*
AWS:IAM:User:PasswordNextRotation	*String*

AWS-Objektspeicher

Governance für Cloud-Konfigurationen verwendet die folgenden Elemente, um die Konfigurationsschlüssel für AWS IAM-Benutzer zu erfassen:

- Konfigurationssammler: AWS S3 Encryption Metric Collector
- Ressourcensammler: AWS S3 Resource Collector
- Verwendete Cloud-API: Aktion: *ListBuckets* und *GetBucketEncryption* im S3-Service
- Cloud-Berechtigungen: *s3:ListBucket* und *s3:GetEncryptionConfiguration*

Konfigurationsschlüssel für AWS-Objektspeicher

Konfigurationsschlüssel	Datentyp
AWS:S3:Encryption:BucketKeyEnabled	*Boolean*
AWS:S3:Encryption:KMSMasterKeyID	*String*
AWS:S3:Encryption:ServerSideEncryptionEnabled	*Boolean*
AWS:S3:Encryption:SSEAlgorithm	*String*

- Konfigurationssammler: AWS S3 ACL Permission Metric Collector
- Ressourcensammler: AWS S3 Resource Collector
- Verwendete Cloud-API: Aktion: *GetBucketAcl*
- Cloud-Berechtigungen: *s3:GetBucketAcl*

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

Konfigurationsschlüssel für AWS-Objektspeicher

Konfigurationsschlüssel	Datentyp
AWS:S3:ACL:AuthnUsersListing	*Boolean*
AWS:S3:ACL:AuthnUsersReadACL	*Boolean*
AWS:S3:ACL:AuthnUsersWrite	*Boolean*
AWS:S3:ACL:AuthnUsersWriteACL	*Boolean*
AWS:S3:ACL:OwnerFullControl	*Boolean*
AWS:S3:ACL:OwnerId	*String*
AWS:S3:ACL:OwnerListing	*Boolean*
AWS:S3:ACL:OwnerName	*String*
AWS:S3:ACL:OwnerReadACL	*Boolean*
AWS:S3:ACL:OwnerWrite	*Boolean*
AWS:S3:ACL:OwnerWriteACL	*Boolean*
AWS:S3:ACL:PublicListing	*Boolean*
AWS:S3:ACL:PublicReadACL	*Boolean*
AWS:S3:ACL:PublicWrite	*Boolean*
AWS:S3:ACL:PublicWriteACL	*Boolean*

AWS-VM-Instanz

Governance für Cloud-Konfigurationen verwendet die folgenden Elemente, um die Konfigurationsschlüssel der AWS-VM-Instanz zu erfassen:

- Ressourcensammler: AWS VM Data Collector
- Verwendete Cloud-API: Aktion: *DescribeInstances* and *AWS EC2 resource*
- Cloud-Berechtigungen: *ec2:DescribeInstances*

AWS-Konfigurationsschlüssel für VM-Instanz

Konfigurationsschlüssel	Datentyp
AWS:EC2:VM:CapacityReservationPreference	*String*
AWS:EC2:VM:CpuOptionsCoreCount	*Numeric*
AWS:EC2:VM:CpuOptionsThreadsPerCore	*Numeric*
AWS:EC2:VM:EbsOptimized	*Boolean*
AWS:EC2:VM:HardwareType	*String*
AWS:EC2:VM:ImageId	*String*
AWS:EC2:VM:InstanceState	*String*
AWS:EC2:VM:KeyName	*String*
AWS:EC2:VM:LaunchTime	*Date*

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

AWS-Konfigurationsschlüssel für VM-Instanz (Fortsetzung)

Konfigurationsschlüssel	Datentyp
AWS:EC2:VM:MonitoringState	*String*
AWS:EC2:VM:Platform	*String*
AWS:EC2:VM:PrivateDnsName	*String*
AWS:EC2:VM:PrivateIpAddress	*String*
AWS:EC2:VM:PublicDnsName	*String*
AWS:EC2:VM:PublicIPAddress	*String*
AWS:EC2:VM:SecurityGroups	*String*
AWS:EC2:VM:SubnetId	*String*
AWS:EC2:VM:Tags	*Map*
AWS:EC2:VM:UsageOperation	*String*
AWS:EC2:VM:VpcId	*String*

AWS-Profil mit minimalen Berechtigungen

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "iam:GenerateCredentialReport",
                "s3:GetEncryptionConfiguration",
                "ec2:DescribeInstances",
                "s3:ListBucketVersions",
                "ec2:DescribeRegions",
                "s3:ListBucket",
                "iam:GetCredentialReport"
            ],
            "Resource": "*"
        }
    ]
}
```

Microsoft Azure-VM-Instanz

Governance für Cloud-Konfigurationen verwendet die folgenden Elemente, um die Konfigurationsschlüssel der Azure-VM-Instanz zu erfassen:

- Ressourcensammler: Azure VM Data Collector
- Verwendete Cloud-API: *Microsoft.ResourceGraph/resources*
- Cloud-Berechtigungen: *Microsoft.ResourceGraph/resources*

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

Azure-Konfigurationsschlüssel für VM-Instanz

Konfigurationsschlüssel	Datentyp
Azure:VM:HardwareType	*String*
Azure:VM:NICID	*String*
Azure:VM:OSDiskCaching	*String*
Azure:VM:OSDiskCreateoption	*String*
Azure:VM:OSDiskDeleteoption	*String*
Azure:VM:OSDiskId	*String*
Azure:VM:OSDiskName	*String*
Azure:VM:OSDiskOSType	*String*
Azure:VM:OSDiskSizeGB	*String*
Azure:VM:OSProfileAllowExtensionOperations	*Boolean*
Azure:VM:OSProfileComputerName	*String*
Azure:VM:OSProfileLinuxConfigurationDisablePasswordAuthentication	*Boolean*
Azure:VM:OSProfileLinuxConfigurationPatchSettingsAssessmentMode	*String*
Azure:VM:OSProfileLinuxConfigurationPatchSettingsPatchMode	*String*
Azure:VM:OSProfileLinuxConfigurationProvisionVmAgent	*Boolean*
Azure:VM:OSProfileLinuxConfigurationSSHKeyData	*Map*
Azure:VM:OSProfileLinuxConfigurationSSHPath	*Map*
Azure:VM:OSProfileRequireGuestProvisionSignal	*Boolean*
Azure:VM:OSWindowsConfigurationEnableAutomaticUpdates	*Boolean*
Azure:VM:OSWindowsConfigurationPatchSettingsAssessmentMode	*String*
Azure:VM:OSWindowsConfigurationPatchSettingsEnableHotpatching	*Boolean*
Azure:VM:OSWindowsConfigurationPatchSettingsPatchMode	*String*
Azure:VM:OSWindowsConfigurationProvisionVMAgent	*Boolean*
Azure:VM:PowerState	*String*
Azure:VM:ProvisioningState	*String*
Azure:VM:ResourceGroup	*String*
Azure:VM:StorageProfileDataDisksCaching	*String*
Azure:VM:StorageProfileDataDisksCreateOption	*String*
Azure:VM:StorageProfileDataDisksDeleteOption	*String*
Azure:VM:StorageProfileDataDisksDetachOption	*String*
Azure:VM:StorageProfileDataDisksDiskIopsReadWrite	*String*
Azure:VM:StorageProfileDataDisksDiskMBpsReadWrite	*String*
Azure:VM:StorageProfileDataDisksDiskSizeGb	*Numeric*
Azure:VM:StorageProfileDataDisksImage	*String*

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

Azure-Konfigurationsschlüssel für VM-Instanz (Fortsetzung)

Konfigurationsschlüssel	Datentyp
Azure:VM:StorageProfileDataDisksLun	*Numeric*
Azure:VM:StorageProfileDataDisksManagedDiskDiskEncryptionSet	*String*
Azure:VM:StorageProfileDataDisksManagedDiskId	*String*
Azure:VM:StorageProfileDataDisksManagedDiskResourceGroup	*String*
Azure:VM:StorageProfileDataDisksManagedDiskStorageAccountType	*String*
Azure:VM:StorageProfileDataDisksManagedStorageAccountType	*String*
Azure:VM:StorageProfileDataDisksName	*String*
Azure:VM:StorageProfileDataDisksToBeDetached	*Boolean*
Azure:VM:StorageProfileDataDisksVhd	*String*
Azure:VM:StorageProfileDataDisksWriteAcceleratorEnabled	*Boolean*
Azure:VM:StorageProfileImageReferenceExactVersion	*String*
Azure:VM:StorageProfileImageReferenceId	*String*
Azure:VM:StorageProfileImageReferenceOffer	*String*
Azure:VM:StorageProfileImageReferencePublisher	*String*
Azure:VM:StorageProfileImageReferenceSharedGalleryImageId	*String*
Azure:VM:StorageProfileImageReferenceSku	*String*
Azure:VM:StorageProfileImageReferenceVersion	*String*
Azure:VM:Tags	*Map*
Azure:VM:VMId	*String*

- Ressourcensammler: Azure VM Data Collector
- Configuration collector (Konfigurationssammler): Azure VM Metric Collector
- Verwendete Cloud-API: *Microsoft.ResourceGraph/resources*
- Cloud-Berechtigungen: *Microsoft.ResourceGraph/resources*

Azure-Konfigurationsschlüssel für VM-Instanz

Konfigurationsschlüssel	Datentyp
Azure:VM:PublicIPAddress	*String*
Azure:VM:PublicIPId	*String*

- Ressourcensammler: Azure VM Data Collector
- Configuration collector (Konfigurationssammler): Azure VM Monitoring Metric Collector
- Verwendete Cloud-API: *Microsoft.Compute/virtualMachines/{vmName}/instanceView*
- Cloud-Berechtigungen: *Microsoft.Compute/virtualMachines/{vmName}/instanceView*

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

Konfigurationsschlüssel für Azure-VM-Instanz

Konfigurationsschlüssel	Datentyp
Azure:VM:MonitoringState	*String*

Hinweis: Verwenden Sie *scope=https://graph.microsoft.com/.default* und *scope=https://management.azure.com/.default*, um das oAuth-Token für Azure-Ressourcen abzurufen.

Azure-Profil mit minimalen Berechtigungen

```
{
    "properties": {
        "roleName": "CCGAzureMinimalPermission",
        "description": "Grants access to scan compute resources from azure
subscription",
        "assignableScopes": [
            "/subscriptions/${subscription_id}"
        ],
        "permissions": [
            {
                "actions": [
                    "Microsoft.ResourceGraph/resources/read",
                    "Microsoft.Compute/virtualMachines/instanceView/read"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```

Bibliothek von Cloud-Aktionen

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

Erkunden	Einrichten	Entwickeln
Untersuchen Bibliothek von Cloud-Aktionen	• Installieren Bibliothek von Cloud-Aktionen • Einrichten Bibliothek von Cloud-Aktionen für Amazon Web Services (AWS) • Einrichten Bibliothek von Cloud-Aktionen für Microsoft Azure	• Entwicklerschulungen • Entwicklerdokumentation • Bibliothek von Cloud-Aktionen Referenz

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

Problembehandlung und Hilfe
• Fragen stellen oder beantworten im Bibliothek von Cloud-Aktionen-Forum der ServiceNow Community • Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen • Kontakt Kundenservice und Support

Bibliothek von Cloud-Aktionen erkunden

Machen Sie sich mit dem typischen Bibliothek von Cloud-Aktionen-Workflow und allgemeinen Aufgaben vertraut.

Führen Sie die folgenden Aufgaben aus, um die Bibliothek von Cloud-Aktionen-Aktionen und -Workflows für die Interaktion mit den Cloud-Ressourcen zu verwenden:

1. Installieren Sie Bibliothek von Cloud-Aktionen. Weitere Informationen finden Sie unter Installieren Bibliothek von Cloud-Aktionen.
2. Informationen zur Verwendung von Bibliothek von Cloud-Aktionen für Interaktionen mit Ressourcen vom Amazon Web Services Typ (AWS) finden Sie unter Einrichten Bibliothek von Cloud-Aktionen für AWS.
3. Informationen zur Verwendung Bibliothek von Cloud-Aktionen von für Interaktionen mit Ressourcen Microsoft Azure finden Sie unter Einrichten Bibliothek von Cloud-Aktionen für Microsoft Azure.

Bibliothek von Cloud-Aktionen installieren

Sie können die Anwendung Bibliothek von Cloud-Aktionen (sn.itom.cal) installieren, wenn Sie über die Administratorrolle verfügen. Die Anwendung installiert die zugehörigen ServiceNow® Store-Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfung des folgenden Elements: Bibliothek von Cloud-Aktionen Anwendungsliste in ServiceNow Store, um Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Releasekompatibilität zu erhalten.

Erforderliche Rolle: Administrator

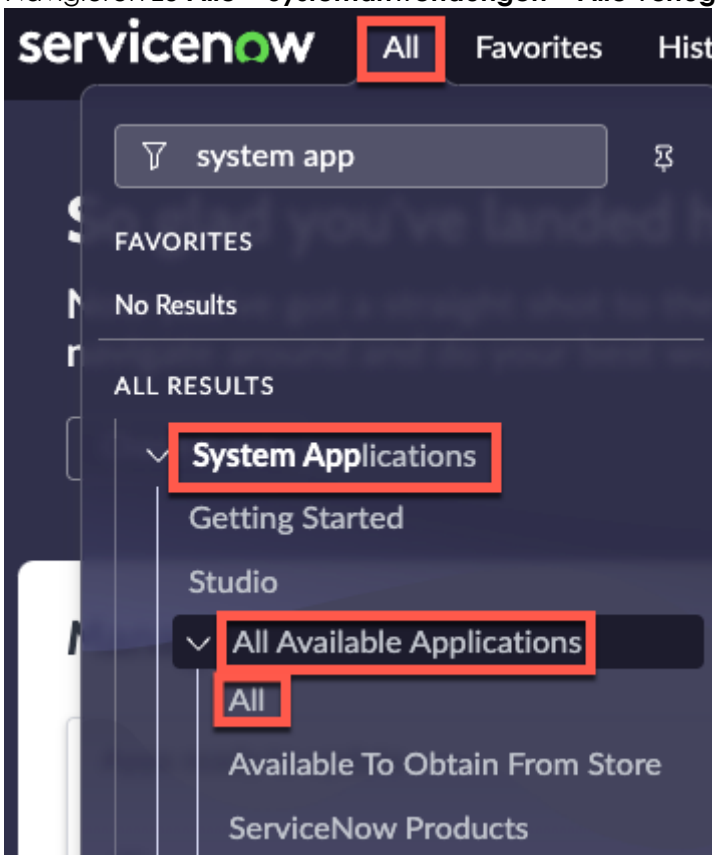
Warum und wann dieser Vorgang ausgeführt wird

Mit der Anwendung Bibliothek von Cloud-Aktionen werden mehrere Plugins installiert. Weitere Informationen finden Sie unter Bibliothek von Cloud-Aktionen .

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

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Bibliothek von Cloud-Aktionen (sn.itom.cal).

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

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Bibliothek von Cloud-Aktionen for AWS einrichten

Richten Sie in Bibliothek von Cloud-Aktionen Zugriff auf die AWS-Cloud-Konten (Amazon Web Services) ein, um die Interaktion zwischen der Anwendung und der Cloud zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: Administrator

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

Warum und wann dieser Vorgang ausgeführt wird

Im Zusammenhang mit der Konfiguration des Zugriffs für AWS-Konten werden die folgenden Begriffe verwendet:

Vertrauende Konten

Vertrauende Konten haben keine permanenten AWS-Anmeldeinformationen. Sie konfigurieren die Vertrauensstellung für IAM-Rollen in diesen Konten so, dass sie für den Zugriff auf andere Konten zurückgreifen.

Vertrauenswürdige Konten

Die vertrauenswürdigen Konten werden von den vertrauenden Konten für den Zugriff verwendet. In der Benutzeroberfläche von ServiceNow werden die vertrauenswürdigen Konten als Accounts des Zugriffsberechtigten bezeichnet.

Verwenden Sie eine der folgenden Methoden, um den Zugriff auf die Konten AWS zu konfigurieren:

- Konfigurieren Sie die permanenten Anmeldeinformationen in Now Platform für die Verbindung mit den eigenständigen AWS -Accounts (diskrete Accounts). Die Tabelle „Cloud-Servicekonto“ [cmdb_ci_cloud_service-account] enthält die Informationen zum Servicekontotyp wie Verwaltungskonto oder Mitgliedskonto und deren Anmeldeinformationen.
- Konfigurieren Sie die Mitgliedskonten so, dass sie für den Zugriff auf das Verwaltungskonto zurückgreifen. Konfigurieren Sie die permanenten Anmeldeinformationen des Verwaltungskontos in diesem Fall auf der Now Platform.
- Konfigurieren Sie die Konten so, dass für den Zugriff ein vertrauenswürdiges Konto verwendet wird (lateraler Zugriff innerhalb derselben AWS-Organisation oder über verschiedene AWS-Organisationen hinweg). Konfigurieren Sie die permanenten Anmeldeinformationen des vertrauenswürdigen Kontos in diesem Fall auf der Now Platform.

Hinweis: Bibliothek von Cloud-Aktionen verwendet kein MID-Server-basiertes Setup für die Rollenübernahme, um auf die vertrauenden Accounts zuzugreifen.

Prozedur

1. Erstellen Sie Anmeldeinformationen für die AWS-Servicekonten.

   a. Navigieren zu **Verbindung und Anmeldeinformationen** > **Anmeldeinformationen**.

   b. Wählen Sie **Neu** und dann **AWS-Anmeldeinformationen** aus.

   c. Füllen Sie die Felder des Formulars aus.

Formular für AWS-Anmeldeinformationen

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.
Zugangsschlüssel-ID	Die Zugriffsschlüssel-ID, die Sie in der AWS-Verwaltungskonsole erstellt haben

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

Feld	Beschreibung
Geheimer Zugangsschlüssel	Der geheime Zugriffsschlüssel, den Sie in der AWS-Verwaltungskonsole erstellt haben

d. Wählen Sie **Speichern**.

2. Wählen Sie den Anmeldeinformationsalias **sn_itom_cal.Aws_Creds_Alias** aus, oder erstellen Sie einen Anmeldeinformationsalias.

a. Entsperren Sie den Anmeldeinformationsalias.

b. Suchen Sie nach einem Anmeldeinformationsalias.

c. Wählen Sie **Neu**.

d. Füllen Sie die Felder des Formulars aus.

Formular „Verbindungs- und Anmeldeinformationsalias“

Feld	Beschreibung
Name	Eindeutiger Name des Alias
Typ	Typ des Anmeldeinformationsalias. Wählen Sie in der Dropdown-Liste „Typ“ die Option **Anmeldeinformationen** aus.

e. Wählen Sie **Absenden** aus.

3. Legen Sie das Feld **Authentifizierungsalgorithmus** auf **AWS Authenticator** fest.

4. Wählen Sie **Absenden** aus.

5. Richten Sie ein AWS-Servicekonto ein.

a. Navigieren zu **Cloud Provisioning and Governance** > **Servicekonten**.

b. Wählen Sie **Neu**.

c. Füllen Sie die Felder des Formulars aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger Name des Servicekontos
Account-ID	12-stellige Nummer des Benutzerkontos. Erweitern Sie die Liste unter dem Kontonamen in der AWS-Verwaltungskonsole, um die Nummer anzuzeigen. **Wichtig:** Entfernen Sie im Feld **Konto-ID** die Bindestriche (-) aus der Nummer.
Discovery-Anmeldeinformationen	Anmeldeinformationen, die für ServiceNow -Anwendungen erforderlich sind, um auf den Cloud-Account zuzugreifen.

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

Feld	Beschreibung
	Sie können die Discovery-Anmeldeinformationen zu einem späteren Zeitpunkt konfigurieren, während Sie den Zugriff auf die Konten AWS konfigurieren. ▪ Wenn Sie ein unabhängiges Servicekonto oder ein Verwaltungskonto einrichten, wählen Sie die zugehörigen AWS-Anmeldeinformationen aus. ▪ Um andere AWS -Accounts für den Zugriff auf diesen Account zu verwenden, lassen Sie das Feld leer. Beispielsweise müssen Sie die Anmeldeinformationen AWS nicht für Konten angeben, die IAM-Rollen (Identity and Access Management) übernehmen, oder für Mitgliedskonten, die ihr Verwaltungskonto für den Zugriff verwenden.
Rechenzentrums-URL	URL des Rechenzentrums. Lassen Sie dieses Feld leer.
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie **AWS-Rechenzentrum** aus.
Rechenzentrums-Discovery-Status	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Übergeordneter Account	Name des Verwaltungskontos, das die AWS-Organisation darstellt, zu der dieses Mitgliedskonto gehört. Dieses Feld wird angezeigt, wenn Sie „AWS-Rechenzentrum“ auswählen. Wenn der Account keiner AWS -Organisation angehört, lassen Sie dieses Feld leer.
Ist Master-Konto	Kennzeichnung des Verwaltungskontos. Dieses Kontrollkästchen wird angezeigt, wenn Sie in der Dropdown-Liste „Rechenzentrumstyp“ die Option „AWS-Rechenzentrum“ auswählen. Aktivieren Sie das Kontrollkästchen, um das AWS-Servicekonto dem Verwaltungskonto zuzuordnen. Aktivieren Sie dieses Kontrollkästchen nur für Konten, die Sie zuvor als Verwaltungskonten konfiguriert haben und zu denen einige Mitgliedskonten gehören. Weitere Informationen zur Organisation AWS finden Sie unter AWS Dokumentation .
Account des Zugriffsberechtigten	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, bei denen keine permanenten AWS-Anmeldeinformationen verwendet werden und bei denen IAM-Rollen für den Zugriff genutzt werden.

d. Wählen Sie **Absenden** aus.

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

6. Wahlweise: Um ein Verwaltungskonto zum Scannen der Mitgliedskonten der AWS-Organisation zu verwenden, erstellen Sie eine Konfiguration für die Übernahme von Rollen für das Verwaltungskonto.

   a. Wahlweise: Wenn Sie nicht die OrganizationAccountAccessRole verwenden möchten, um auf das Mitgliedskonto zuzugreifen, konfigurieren Sie ein vertrauendes Konto für Bibliothek von Cloud-Aktionen.
   Weitere Informationen finden Sie unter Konfigurieren Sie das vertrauende Konto für Governance für Cloud-Konfigurationen und Bibliothek von Cloud-Aktionen.

   b. Wahlweise: Wiederholen Sie Schritt 6.a für jedes Mitgliedskonto, das über das Verwaltungskonto gescannt werden muss, ohne die OrganizationAccountAccessRole zu verwenden.

   c. Wahlweise: Wenn Sie die OrganizationAccountAccessRole verwenden möchten, um auf das Mitgliedskonto zuzugreifen, erstellen Sie eine Konfiguration für die Übernahme von Rollen für das Verwaltungskonto.
   Weitere Informationen finden Sie unter Konfiguration für die Übernahme von Rollen erstellen.

7. Wahlweise: Um ein vertrauenswürdiges Konto zum Scannen des vertrauenden Kontos zu verwenden, konfigurieren Sie das vertrauende Konto für Bibliothek von Cloud-Aktionen. Das vertrauenswürdige Konto und das vertrauende Konto können sich in verschiedenen AWS-Organisationen, aber auch in derselben AWS-Organisation befinden.

   a. Konfigurieren Sie ein vertrauendes Konto für Governance für Cloud-Konfigurationen.
   Weitere Informationen finden Sie unter Konfigurieren Sie das vertrauende Konto für Governance für Cloud-Konfigurationen und Bibliothek von Cloud-Aktionen.

   b. Wiederholen Sie Schritt 7.a für jedes vertrauende Konto, das über das vertrauenswürdige Konto gescannt werden muss.

Bibliothek von Cloud-Aktionen for Microsoft Azure einrichten

Richten Sie in Bibliothek von Cloud-Aktionen Zugriff auf die Microsoft Azure Cloud-Konten ein, um die Interaktion zwischen der Anwendung und der Cloud zu ermöglichen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Erstellen Sie Microsoft Azure-Anmeldeinformationen für den Zugriff auf das Microsoft Azure-Konto.
   Weitere Informationen finden Sie unter Azure Cloud-Anmeldeinformationen erstellen.
2. Erstellen Sie eine IntegrationHub-Verbindung für Microsoft Azure.

   a. Navigieren zu **Prozessautomatisierung** > **Flow Designer**, und wählen Sie die Registerkarte **Verbindungen**.

   b. Wählen Sie auf der Kachel **Azure Connection** (Azure-Verbindung) die Option **Verbindung hinzufügen** aus.

   c. Füllen Sie die Felder des Formulars aus.

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

Formular „Scan-Zeitplan“

Feld	Beschreibung
Verbindungsname	Name der Verbindung
OAuth-Client-ID	Microsoft Azure-Anwendungs-ID
OAuth-Client-Geheimnis	Microsoft Azure-Anwendungsschlüssel
OAuth-Token-URL	Mandanten-ID des Microsoft Azure-Kontos Ersetzen Sie `{tenant}` durch die Microsoft Azure-Mandanten-ID.

d. Wählen Sie **OAuth-Token erstellen und abrufen** aus.

Domain Separation und Cloud-Aktionsbibliothek

Domänentrennung wird in Bibliothek von Cloud-Aktionen nicht unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Zugehörige Informationen

Domänentrennung für Service Provider

Bibliothek von Cloud-Aktionen-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Bibliothek von Cloud-Aktionen.

AWS Aktivieren Sie die Aktion zur Überwachung der EC2-Instanz

Aktion, mit der die Überwachung für die ausgewählte VM-Instanz von Amazon Web Services (AWS) aktiviert wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

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

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *ec2:MonitorInstances* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Instanzen

Datentyp: *String*

AWS-Instanz-ID. Geben Sie die durch Kommata getrennte Liste von AWS-Instanz-IDs ein.

Beispiel: i-1234567890abcdef0, i-1234567761abcdek1

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Gov Cloud

Datentyp: *True/False*

Nicht unterstützt.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: *True/False*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

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

Fehlermeldung

Datentyp: *String*

Fehlermeldung für den fehlgeschlagenen Anruf zurückgegeben.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

AWS Aktion „IAM-Anmeldeprofil abrufen“.

Aktion, durch die der Benutzername für den angegebenen Identity Access Management-Benutzer (IAM) von Amazon Web Services (AWS) abgerufen wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *iam:GetLoginProfile* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

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

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Gov Cloud

Datentyp: *True/False*

Nicht unterstützt.

IAM-Account

Datentyp: *String*

AWS IAM-Benutzername.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

AWS Aktion „Images auflisten“.

Aktion, die die angegebenen Images (AMIs, AKIs und ARIs), die für Sie verfügbar sind, oder alle für Sie verfügbaren Images beschreibt.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *ec2:DescribeImages* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Standort

Datentyp: *String*

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

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Version

Datentyp: *String*

Version der AWS-API.

Grenzwert

Datentyp: *Integer*

Anzahl der Seiten, die pro Aufruf zurückgegeben werden sollen.

Nächstes Token

Datentyp: *String*

Startseitentoken.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Filter

Datentyp: *Object*

Ein Filtername-Wert-Paar, das dazu verwendet wird, eine bestimmte Liste von Ergebnissen aus dem Beschreibungsvorgang zurückzugeben. Filter können dazu verwendet werden, eine Reihe von Ressourcen basierend auf Kriterien wie Tags, Attributen oder IDs abzugleichen.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *Object*

Ein komplexes Objekt, das Informationen zu den Images enthält.

AWS S3-Bucket-Verschlüsselungsaktion platzieren

Aktion, mit der die Standardverschlüsselung und der S3-Bucket-Schlüssel von Amazon Web Services (AWS) für einen vorhandenen Bucket konfiguriert werden.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

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

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *s3:PutEncryptionConfiguration* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Bucket-Name

Datentyp: *String*

Name des AWS S3-Bucket.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Gov Cloud

Datentyp: *True/False*

Nicht unterstützt.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: *String*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

Bucket-Region

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

Datentyp: *String*

Rechenzentrum, in dem der angegebene AWS S3-Bucket gehostet wird.

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

Weitergeleitet

Datentyp: *String*

Wenn der AWS S3-Bucket im angegebenen Rechenzentrum nicht verfügbar ist, gibt die Variable *Bucket Region* das Rechenzentrum des AWS S3-Bucket an.

Fehlermeldung

Datentyp: *String*

Fehlermeldung für den fehlgeschlagenen Anruf zurückgegeben.

AWS Deaktivieren Sie die Aktion der EC2-Instanz

Aktion, durch die der angegebene virtuelle AWS-Computer (Amazon Web Services) angehalten wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *ec2:StopInstances* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Instanzen

Datentyp: *String*

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

AWS-Instanz-ID. Geben Sie die durch Kommata getrennte Liste von AWS-Instanz-IDs ein.

Beispiel: i-1234567890abcdef0, i-1234567761abcdek1

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Gov Cloud

Datentyp: *True/False* Nicht unterstützt.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: *True/False*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

Fehlermeldung

Datentyp: *String*

Fehlermeldung für den fehlgeschlagenen Anruf zurückgegeben.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

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

Azure Aktion Virtuellen Computer deaktivieren

Aktion, durch die der angegebene virtuelle Microsoft Azure-Computer angehalten wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *Microsoft.Compute/virtualMachines/*/powerOff* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Gov Cloud

Datentyp: *True/False*

Nicht unterstützt.

VM-Bezeichner

Datentyp: *String*

URI der VM-Ressource.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

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

Ist „Zugriff verweigert“

Datentyp: *True/False*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

Fehlermeldung

Datentyp: *String*

Fehlermeldung für den fehlgeschlagenen Anruf zurückgegeben.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

CAL – AWS S3-Buckets auflisten – Aktion

Aktion, mit der eine Liste aller AWS-Buckets (Amazon Web Services) zurückgegeben wird, die dem authentifizierten Absender der Anforderung gehören.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *s3:ListBucket* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Nächstes Token

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

Datentyp: *String*

Startseitentoken.

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Grenzwert

Datentyp: *Integer*

Anzahl der Seiten, die pro Aufruf zurückgegeben werden sollen.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *Object*

Ein komplexes Objekt, das Informationen zu den Images enthält, die dem authentifizierten Absender der Anforderung gehören.

CAL – AWS-Liste der VMs – Aktion

Aktion, mit der eine Liste aller virtuellen AWS-Computer (Amazon Web Services) zurückgegeben wird, die zum angegebenen logischen Rechenzentrum gehören.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *ec2:DescribeInstances* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Standort

Datentyp: *String*

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

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Version

Datentyp: *String*

Version der AWS-API.

Grenzwert

Datentyp: *Integer*

Anzahl der Seiten, die pro Aufruf zurückgegeben werden sollen.

Nächstes Token

Datentyp: *String*

Startseitentoken.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Filter

Datentyp: *Object*

Ein Filtername-Wert-Paar, das dazu verwendet wird, eine bestimmte Liste von Ergebnissen aus dem Beschreibungsvorgang zurückzugeben. Filter können dazu verwendet werden, eine Reihe von Ressourcen basierend auf Kriterien wie Tags, Attributen oder IDs abzugleichen.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *Object*

Ein komplexes Objekt, das Informationen zu den VMs enthält, die im angegebenen logischen Rechenzentrum gehostet werden.

CAL – Azure-Liste der VMs – Aktion

Aktion, mit der die Liste der virtuellen Microsoft Azure-Computer zurückgegeben wird, die zum angegebenen logischen Rechenzentrum gehören.

Rollen und Verfügbarkeit

Abonnementanforderungen

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

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *Microsoft.ResourceGraph/resources* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Standort

Datentyp: *String*

Name des Rechenzentrums

Version

Datentyp: *String*

Version der Microsoft Azure-API.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die Microsoft Azure-Anmeldeinformationen.

Grenzwert

Datentyp: *Integer*

Anzahl der Seiten, die pro Aufruf zurückgegeben werden sollen.

Nächstes Token

Datentyp: *String*

Startseitentoken.

Filter

Datentyp: *Object*

Ein Filtername-Wert-Paar, das dazu verwendet wird, eine bestimmte Liste von Ergebnissen aus dem Beschreibungsvorgang zurückzugeben. Filter können dazu verwendet werden, eine Reihe von Ressourcen basierend auf Kriterien wie Tags, Attributen oder IDs abzugleichen.

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

Konto-ID

Datentyp: *String*

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

Microsoft Azure-Konto-ID.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *Object*

Ein komplexes Objekt, das Informationen zu den VMs enthält, die im angegebenen logischen Rechenzentrum gehostet werden.

CAL – Azure-VM-IP-Metrik – Aktion

Aktion, mit der die Details der IP-Adresse des angegebenen virtuellen Microsoft Azure-Computers zurückgegeben werden.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *Microsoft.ResourceGraph/resources* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die Microsoft Azure-Anmeldeinformationen.

Version

Datentyp: *String*

Version der Microsoft Azure-API.

VM

Datentyp: *Array.Object*

URI der VM-Ressource.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *Object*

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

Ein komplexes Objekt, das die IP-Adressdetails der angegebenen Microsoft Azure-VM enthält.

CAL – Metrikdaten für Azure-VM-Monitoring – Aktion

Aktion, mit der Überwachungsinformationen für den angegebenen virtuellen Microsoft Azure-Computer zurückgegeben werden.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *`Microsoft.Compute/virtualMachines/{vmName}/instanceView`* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *`Record`*

Anmeldeinformationsalias für die Microsoft Azure-Anmeldeinformationen.

Version

Datentyp: *`String`*

Version der Microsoft Azure-API.

VM

Datentyp: *`Object.Array`*

URI der VM-Ressource.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ergebnis

Datentyp: *`String`*

Die Ergebnisvariable enthält die Überwachungsinformationen für die angegebene Microsoft Azure-VM.

CAL – Ganzzahlstrom – Aktion

Aktion, mit der ein Array von Ganzzahlen im angegebenen Bereich zurückgegeben wird.

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

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Sie benötigen keine Cloud-Berechtigung, um diese Aktion auszuführen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

start

Datentyp: *Integer*

Eine Ganzzahl, die angibt, an welcher Position begonnen werden soll.

end

Datentyp: *Integer*

Eine Ganzzahl, die angibt, an welcher Stelle gestoppt werden soll. Der zurückgegebene Ganzzahl-Stream enthält nicht die End-Ganzzahl.

step

Datentyp: *Integer*

Eine Ganzzahl, die das Inkrementintervall für den Ganzzahl-Stream angibt.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ganzzahlstrom

Datentyp: *Array.Integer*

Ein Array von Ganzzahlen.

AWS IAM-Benutzer deaktivieren – Aktion

Aktion, mit der das Passwort für den angegebenen IAM-Benutzer gelöscht wird, wodurch der Zugriff des Benutzers auf AWS-Services (Amazon Web Services) über die AWS-Managementkonsole beendet wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diese Aktion in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

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

Diese Aktion erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieser Aktion muss die aufrufende Person über die Cloud-Berechtigung *iam:DeleteLoginProfile* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Standort

Datentyp: *String*

Name des Rechenzentrums

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Gov Cloud

Datentyp: *True/False*

Nicht unterstützt.

IAM-Account

Datentyp: *String*

AWS IAM-Benutzername.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: *String*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

error_code

Datentyp: *String*

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

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

Ergebnis

Datentyp: *True/False*

Status der Aktion.

- *True*: Erfolgreich
- *False*: Fehlgeschlagen

error_message

Datentyp: *String*

Fehlermeldung für den fehlgeschlagenen Anruf zurückgegeben.

CAL – AWS-Bericht zu Anmeldeinformationen erstellen – Subflow

Subflow, mit dem alle Benutzer in Ihrem Konto und der Status ihrer verschiedenen Anmeldeinformationen aufgelistet werden, einschließlich der Passwörter, Zugriffsschlüssel und MFA-Geräte.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diesen Subflow in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Dieser Subflow erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieses Subflows muss die aufrufende Person über die Cloud-Berechtigungen *Iam:GetCredentialReport* und *Iam:GenerateCredentialReport* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die für den Subflow erforderlich ist. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

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

API-Version

Datentyp: *String*

Version der AWS-API.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Subflows verwenden.

Fehler

Datentyp: *String*

Beschreibung des vom AWS-Endpunkt zurückgegebenen Fehlers.

credential_report_list

Datentyp: *Array.Object*

Komplexes Objekt, das alle Felder des Anmeldeinformationsberichts enthält.

CAL – AWS S3-Verschlüsselung abrufen – Subflow

Subflow, mit dem die Konfiguration der Standardverschlüsselung für einen S3-Bucket von Amazon Web Services (AWS) zurückgegeben wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diesen Subflow in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Dieser Subflow erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieses Subflows muss die aufrufende Person über die Cloud-Berechtigung *s3:GetEncryptionConfiguration* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die für den Subflow erforderlich ist. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Bucket-Name

Datentyp: *String*

Name des AWS S3-Bucket.

Anmeldeinformationsalias

Datentyp: *String*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

MID verwenden

Datentyp: *True/False*

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

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Subflows verwenden.

Ist „Zugriff verweigert“

Datentyp: *True/False*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

Ist verschlüsselt

Datentyp: *True/False*

Verschlüsselungsstatus der AWS-Ressource.

Bucket-Region

Datentyp: *String*

Rechenzentrum des AWS S3-Buckets.

KMS-Master-Schlüssel-ID

Datentyp: *String*

Kundenseitige Schlüssel-ID des AWS Key Management Service (KMS), die für die Standardverschlüsselung verwendet wird.

Verschlüsselungsalgorithmus

Datentyp: *String*

Serverseitiger Verschlüsselungsalgorithmus, der für die Standardverschlüsselung verwendet wird.

Bucket-Schlüssel aktiviert

Datentyp: *String*

Gibt an, ob von Amazon S3 ein S3-Bucket-Schlüssel mit serverseitiger Verschlüsselung mittels KMS (SSE-KMS) für neue Objekte im Bucket verwendet wird.

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

CAL – Anmeldeinformationsalias auflösen – Subflow

Subflow, mit dem der Anmeldeinformationsalias für die genannten Anmeldeinformationen zurückgegeben wird.

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

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diesen Subflow in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Dieser Subflow erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Sie benötigen keine Cloud-Berechtigung, um diese Aktion auszuführen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die für den Subflow erforderlich ist. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Service-Account

Datentyp: *Record*

Servicekonto, für das ein geeigneter Anmeldeinformationsalias gesucht wird.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Subflows verwenden.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Fehler

Datentyp: *String*

Wenn von der zugrunde liegenden CAL-Aktion (Bibliothek von Cloud-Aktionen) kein Anmeldeinformationsalias zurückgegeben wird, wird eine Fehlermeldung zurückgegeben, in der der Grund für den Fehler erläutert wird. Die Fehlervariable enthält die Fehlermeldung, die von der zugrunde liegenden CAL-Aktion zurückgegeben wird.

CAL – MID auflösen – Subflow

Subflow, mit dem basierend auf den angegebenen MID-Server-Auswahlkriterien ein geeigneter MID-Server zurückgegeben wird.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diesen Subflow in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

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

Dieser Subflow erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Sie benötigen keine Cloud-Berechtigung, um diese Aktion auszuführen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die für den Subflow erforderlich ist. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

Service-Account

Datentyp: *Record*

Servicekonto, für das ein geeigneter MID-Server gesucht wird.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Subflows verwenden.

MID-Server

Datentyp: *Record*

Aufgelöster MID-Server.

Fehler

Datentyp: *String*

Fehler, der bei der Identifizierung des MID-Servers aufgetreten ist.

CAL – AWS S3 ACL abrufen – Subflow

Subflow, mit dem die Details der Zugriffssteuerungsliste (Access Control List, ACL) für den angegebenen S3-Bucket von Amazon Web Services (AWS) abgerufen werden.

Rollen und Verfügbarkeit

Abonnementanforderungen

Um diesen Subflow in benutzerdefinierten Flows zu verwenden, müssen Sie ein IntegrationHub Enterprise-Abonnement oder ein App Engine-Abonnement erwerben. Weitere Informationen finden Sie unter Integrations-Hub anfordern .

Rollenanforderungen

Dieser Subflow erfordert Rollen, die von Delegated Development gewährt oder dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie unter Benutzerzugriff auf Flow Designer .

Cloud-Berechtigung

Zum Ausführen dieses Subflows muss die aufrufende Person über die Cloud-Berechtigung *s3:GetBucketAcl* verfügen.

Eingaben

Geben Sie einen Wert für jede Eingabe an, die Ihre Aktion benötigt. Um dynamische Werte hinzuzufügen, können Sie auch Datenpillen mit der Pillenauswahl auswählen.

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

Bucket-Name

Datentyp: *String*

Name des AWS S3-Bucket.

MID verwenden

Datentyp: *True/False*

Auswahl, mit der angegeben wird, ob ein MID-Server für die ausgehenden Anrufe verwendet werden soll.

MID-Server

Datentyp: *Record*

MID-Server für die ausgehenden Anrufe.

Anmeldeinformationsalias

Datentyp: *Record*

Anmeldeinformationsalias für die AWS-Anmeldeinformationen.

Ausgaben

Sie können diese Ausgaben als Eingaben für andere Aktionen verwenden.

Ist „Zugriff verweigert“

Datentyp: *True/False*

Serverautorisierungsstatus des Anrufs.

- *True*: Anruf wurde vom Server autorisiert
- *False*: Anruf wurde vom Server nicht autorisiert

Bucket-Region

Datentyp: *String*

Rechenzentrum, in dem der angegebene AWS S3-Bucket gehostet wird.

Fehlercode

Datentyp: *String*

Clientfehlercode für den fehlgeschlagenen Anruf zurückgegeben.

Besitzer Schreiben

Datentyp: *True/False*

Der Bucket-Besitzer kann in den Bucket schreiben.

Bucket-Besitzer Vollzugriff

Datentyp: *True/False*

Der Besitzer hat alle Berechtigungen für den Bucket.

Besitzerliste

Datentyp: *True/False*

Der Bucket-Besitzer kann den Inhalt des Buckets auflisten.

Öffentlicher Schreibzugriff

Datentyp: *True/False*

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

Jeder (öffentlicher Zugriff) kann in den Bucket schreiben.

Öffentliche Auflistung

Datentyp: *True/False*

Jeder (öffentlicher Zugriff) kann den Inhalt des Buckets auflisten.

Öffentliche vollständige Kontrolle

Datentyp: *True/False*

Jeder (öffentlicher Zugriff) verfügt über alle Berechtigungen.

Authentifizierte Anwender für Schreiben

Datentyp: *True/False*

Authentifizierte Benutzergruppen (Benutzer mit einem AWS-Konto) können in den Bucket schreiben.

Anwender mit vollem Zugriff authentifizieren

Datentyp: *True/False*

Authentifizierte Benutzergruppen (Benutzer mit einem AWS-Konto) verfügen über alle Berechtigungen für den Bucket.

Besitzer-Lese-ACL

Datentyp: *True/False*

Der Besitzer des Buckets kann die Bucket-ACL lesen.

Besitzer-Schreib-ACL

Datentyp: *True/False*

Der Besitzer des Buckets kann die Bucket-ACL schreiben oder aktualisieren.

Öffentlicher Lesezugriff ACL

Datentyp: *True/False*

Jeder (öffentlicher Zugriff) kann die Bucket-ACL lesen.

Öffentlicher Schreibzugriff ACL

Datentyp: *True/False*

Jeder (öffentlicher Zugriff) kann die Bucket-ACL schreiben oder aktualisieren.

Authentifizierte Benutzer für ACL Lesen

Datentyp: *True/False*

Authentifizierte Benutzergruppen (Benutzer mit einem AWS-Konto) können die Bucket-ACL lesen.

Authentifizierte Anwender für ACL Schreiben

Datentyp: *True/False*

Authentifizierte Benutzergruppen (Benutzer mit einem AWS-Konto) können die Bucket-ACL schreiben oder aktualisieren.

Anwenderliste authentifizieren

Datentyp: *True/False*

Authentifizierte Benutzergruppen (Benutzer mit einem AWS-Konto) können den Inhalt des Buckets auflisten.

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

Verantwortlichen-ID

Datentyp: *String*

Kanonische Benutzer-ID des AWS-Kontos.

Anzeigename des Besitzers

Datentyp: *String*

Anzeigename des Ressourcenbesitzers.

Bei der Verbundanmeldung wird vom Subflow kein Anzeigename des Besitzers zurückgegeben.

Cloud-Profile mit minimalen Berechtigungen für Bibliothek von Cloud-Aktionen-Aktionen und -Subflows

Sie benötigen entsprechende Cloud-Berechtigungen, um die Bibliothek von Cloud-Aktionen-Aktionen und -Subflows ausführen zu können. Bearbeiten Sie die JSON-Datei des Cloud-Berechtigungsprofils entsprechend den Anforderungen Ihrer Organisation.

AWS-Profil (Amazon Web Services) mit minimalen Berechtigungen

```
{
 "Version": "2012-10-17",
 "Statement": [{
  "Sid": "VisualEditor0",
  "Effect": "Allow",
  "Action": [
   "iam:GenerateCredentialReport",
   "s3:GetEncryptionConfiguration",
   "ec2:DescribeInstances",
   "s3:ListBucketVersions",
   "ec2:DescribeRegions",
   "s3:ListBucket",
   "iam:GetCredentialReport",
   "iam:DeleteLoginProfile",
   "ec2:MonitorInstances",
   "iam:GetLoginProfile",
   "ec2:DescribeImages",
   "s3:PutEncryptionConfiguration",
   "ec2:StopInstances",
   "s3:GetBucketAcl"
  ],
  "Resource": "*"
 }]
}
```

Microsoft Azure-Profil mit minimalen Berechtigungen

```
{
 "properties": {
  "roleName": "CCGAzureMinimalPermission",
  "description": "Grants access to scan compute resources from the Azure subscription",
```


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

```
  "assignableScopes": [
    "/subscriptions/${subscription_id}"
  ],
  "permissions": [{
    "actions": [
      "Microsoft.ResourceGraph/resources/read",
      "Microsoft.Compute/virtualMachines/instanceView/read",
      "Microsoft.Compute/virtualMachines/*/powerOff"
    ],
    "notActions": [],
    "dataActions": [],
    "notDataActions": []
  }]
 }
}
```

ITOM Cloud Accelerate-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Konfigurieren und Verwenden von ITOM Cloud Accelerate.

Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate

Tabellen, die die Plugins oder Anwendungen auflisten, die mit den -Anwendungen ITOM Cloud Accelerate installiert werden. Wenn Sie Ihre Anwendung aktualisieren, werden alle neu erforderlichen Anwendungsabhängigkeiten installiert.

Cloud-Services-Katalog

Das CSK Content Pack-Plugin (sn_itom_csc_cp) stellt den erforderlichen vordefinierten Inhalt für die Anwendung Cloud-Services-Katalog bereit. Dieser Inhalt enthält Governance-Richtlinien und -Aktionen zur Bereitstellung eines gesteuerten End-to-End-Bereitstellungs-Workflows.

Mit Cloud-Services-Katalog (sn_itom_csc) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Cloud Provisioning and Governance: Terraform Connector (sn_cmp_ Terraform)	Integriert Terraform Open Source, Terraform Enterpriseund Terraform Cloud mit ITOM Cloud Provisioning and Governance (CPG), sodass Sie Services in mehreren Clouds wie AWS, Azure, GCPund VMwarebereitstellen und verwalten können. Die Terraform -Vorlagen sind als Cloud-Vorlagenkataloge verschlüsselt, die Sie zum Bereitstellen von Cloud-Ressourcen verwenden können.
Arbeitsbereich für Cloud-Vorgänge (sn_cloud_ops_ws)	Bietet eine umfassende Lösung für die Verwaltung der Cloud-Vorgänge Ihres Unternehmens.
Cloud Provisioning and Governance (com.snc.cloud.mgmt)	Bietet eine einzige Oberfläche für den Zugriff auf Cloud-Ressourcen, die Veröffentlichung von Cloud-Angeboten in einem Katalog und die Verwaltung der Nutzung dieser Ressourcen.

Automatische Übersetzung

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

Mit Cloud-Services-Katalog (sn_itom_csc) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Geführtes Setup (sn_ads_setup)	Ermöglicht das schrittweise Durchlaufen der Erstkonfiguration von Produkten und Anwendungen, die ein Geführtes Setup -Modul bereitstellen. Geführtes Setup unterstützt Sie bei der Planung der Einführung eines Produkts und der Durchführung der grundlegenden Konfiguration, die für die Veröffentlichung erforderlich ist.
ITOM/OT SU-Lizenzierung sn_itom_licensing	Berechnet, wie viele Abonnements für ITOM-Anwendungen Ihr Unternehmen erworben und genutzt hat, und zeigt das Ergebnis an.

Mit dem Inhaltspaket CSK (sn_itom_csc_cp) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Cloud-Services-Katalog (sn_itom_csc)	Bietet eine vereinfachte Schnittstelle zur Automatisierung des Cloud-Managements und für den Zugriff auf Cloud-Ressourcen. Mit der Anwendung können Sie Cloud-Angebote in einem Katalog veröffentlichen und die Nutzung und den Lebenszyklus dieser Ressourcen verwalten.
ServiceNow IntegrationHub-Aktionsschritt – SSH (com.glide.hub.action_step.ssh)	Der SSH-Schritt führt über einen ServiceNow® MID-Server SSH-Befehle für ein externes *nix-System aus. Der Schritt speichert auch Skripts und Befehle für die *nix-Systeme.
Agent Client Collector Framework (sn_agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
CCG Inhaltspaket (sn_itom_ccg_cp)	Stellt optionale vordefinierte Inhalte für die AnwendungGovernance für Cloud-Konfigurationen bereit, z. B. Richtlinien, Ressourcensammler, Konfigurationssammler und Korrekturaktionen.
Flow Designer-Aktionsschritt – E-Mail (com.glide.hub.action_step.email)	Stellt den Schritt E-Mail senden bereit, um eine E-Mail an angegebene Benutzer oder Gruppen als Aktion in einem Flow zu senden.

Bewertung der Cloud-Migration

Mit Bewertung der Cloud-Migration (sn_cloud_migration) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
ITOM/OT SU-Lizenzierung sn_itom_licensing	Berechnet, wie viele Abonnements für ITOM-Anwendungen Ihr Unternehmen erworben und genutzt hat, und zeigt das Ergebnis an.

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

Mit Bewertung der Cloud-Migration (sn_cloud_migration) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.
Cloud-Migrationsbasis (com.sn_cloud_mig_base)	Ein Basis-Plugin zur Unterstützung der Anwendung Bewertung der Cloud-Migration.

Governance für Cloud-Konfigurationen

Das Plugin CCG Inhaltspaket (sn_itom_ccg_cp) bietet optionale vordefinierte Inhaltefür die Anwendung Governance für Cloud-Konfigurationen, z. B. Richtlinien, Ressourcensammler, Konfigurationssammler und Korrekturaktionen.

Mit Governance für Cloud-Konfigurationen (sn_itom_ccg) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Bibliothek von Cloud-Aktionen (sn_itom_cal)	Stellt vordefinierte Aktionen und Subflows bereit, um die Interaktion mit den Cloud-Ressourcen Ihrer Organisation zu ermöglichen. ServiceNow® ITOM Cloud Accelerate -Funktionen wie Governance für Cloud-Konfigurationen verwenden diese Aktionen, um zu arbeiten.

Mit CCG Inhaltspaket (sn_itom_ccg_cp) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Governance für Cloud-Konfigurationen (sn_itom_ccg)	Prüft die Konfigurationseinstellungen von Cloud-Ressourcen in Ihrer Organisation anhand einer Reihe von Richtlinien, um Verstöße zu identifizieren. Nachdem der Verstoß identifiziert wurde, können Sie Nachbesserungs-Workflows verwenden, um ihn zu minimieren.

Bibliothek von Cloud-Aktionen

Mit Bibliothek von Cloud-Aktionen (sn_itom_cal) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
ITOM/OT SU-Lizenzierung sn_itom_licensing	Berechnet, wie viele Abonnements für ITOM-Anwendungen Ihr Unternehmen erworben und genutzt hat, und zeigt das Ergebnis an.
Flow Designer-Aktionsschritt – Nutzlastgenerator (com.glide.hub.action_step.payload)	Ermöglichen Sie Aktionsdesignern, Name-/Wert-Paare mit dynamischen Daten einfach in JSON- und XML-Nutzlasten zu erstellen.

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

Mit Bibliothek von Cloud-Aktionen (sn_itom_cal) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
ServiceNow IntegrationHub-Aktionsschritt – Verbindungsinformationen abrufen (com.glide.hub.action_step.get_connection_info)	Stellt Details zu Verbindung und Anmeldeinformationen von einem anderen Schritt wie einem REST-Schritt (Representational State Transfer) zu anderen Schritten in Ihrer Aktion bereit.
ServiceNow IntegrationHub-Aktionsschritt – XML-Parser (com.glide.hub.action_step.xmlparser)	Aktiviert den XML-Parser-Aktionsschritt in Flow Designer.
ServiceNow IntegrationHub-Laufzeit (com.glide.hub.integration.runtime)	Ermöglicht die Ausführung von IntegrationHub-Aktionen und -Flows.
Cloud Provisioning and Governance Core (com.snc.cloud.core)	Enthält Ressourcenblöcke und Cloud API-Zuordnungen (Cloud Application Programming Interface) im Zusammenhang mit der Cloud API-basierten Erkennung und Ereignissen, die entweder durch Antwortzuordnungs- oder Aufrufmuster verarbeitet werden.
Flow Designer-Aktionsschritt – Skript auf MID (com.glide.hub.action_step.script_mid)	Stellt einen Aktionsschritt zum Ausführen von anwenderdefiniertem JavaScript innerhalb einer wiederverwendbaren Aktion für einen MID-Server bereit.
ServiceNow IntegrationHub-Aktionsschritt – REST (com.glide.hub.action_step.rest)	Aktiviert den REST-Aktionsschritt in Flow Designer.
ServiceNow IntegrationHub-Aktionsvorlage – Datenstrom (com.glide.hub.action_type.datastream)	Senden Sie REST-, SOAP- oder JDBC-Anforderungen von Flow Designer an APIs, die einen Stream von Antwortdaten größer als 10 MB oder paginierte Ergebnisse zurückgeben. Parsen Sie Streamdaten in eine Reihe komplexer Objektausgaben, und verwenden Sie die Datenpillen in anderen Aktionen in einem Flow.

Zugehörige Informationen

- Mit installierte Plugins oder Anwendungen ITOM-Transparenz
- Mit installierte Plugins oder Anwendungen ITOM-Integrität
- Mit aktivierte Plugins ITOM-Optimierung
- Mit Now Assist für ITOM installierte Anwendungen

ITOM-Transparenz

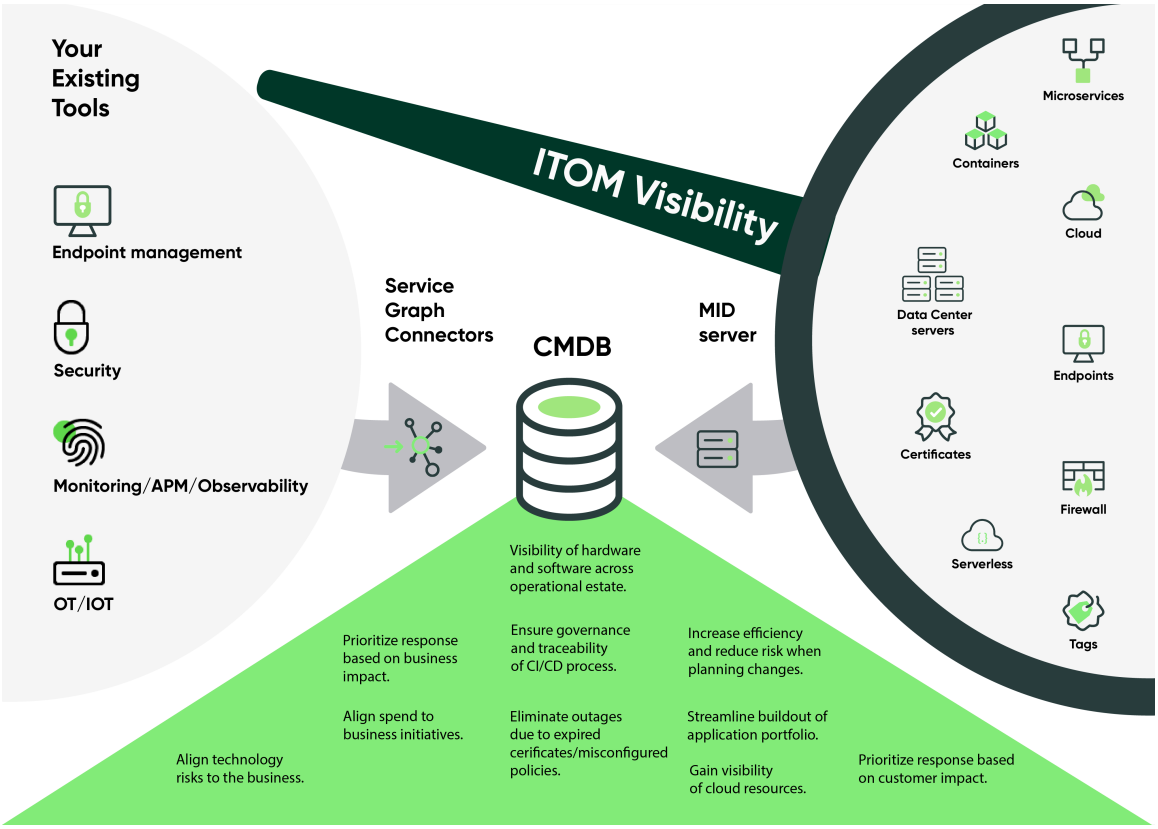
Das ProduktServiceNow® ITOM-Transparenz besteht aus ServiceNow® Discovery, ServiceNow® Service-Mapping, Zertifikatsbestand-Management, Service Graph Connectors, Multisource-CMDB sowie Firewall-Audits und Reporting. Discovery und Service-Mapping vermitteln Ihnen zusammen eine einheitliche, verbundene Ansicht Ihres gesamten IT-Netzwerks und der von ihm unterstützten Services.

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

ITOM-Transparenz – Benutzer

ITOM-Transparenz versetzt IT-Abteilungen von Unternehmen und Cloud-Unternehmen, die Platform-as-a-Service anbieten, in die Lage, ihre IT-Ressourcen zu erkennen.

ServiceNow® Configuration Management Database (CMDB) ist nicht nur einfach ein operatives Tool, sondern in der heutigen IT-Landschaft eine strategische Notwendigkeit. Die Gewährleistung einer genauen und vollständigen CMDB stellt die Grundlage zur Durchführung kritischer Services dar und bietet IT-Abteilungen eine Reihe von wichtigen Ergebnissen.



Die von ITOM-Transparenz erfassten Daten bilden die Grundlage für den Betrieb der folgenden Geschäftsbereiche und Produkte der Now Platform:

ITOM-Integrität

Verwenden Sie ITOM-Integrität, um die Integrität von Services in Ihrer Organisation nachzuverfolgen und zu verwalten. Von ITOM-Integrität werden Warnmeldungen zu Infrastruktur-Events gesammelt, die von Überwachungs-Tools von Drittanbietern erfasst wurden. Anschließend nutzt das Tool von Discovery gesammelte IT-bezogene Informationen, um Konfigurationselementen Warnungen zuzuordnen. Basierend auf den erfassten Informationen stellt ITOM-Integrität Dashboards bereit, die eine konsolidierte Ansicht aller Serviceeinfluss-Events anzeigen. Sie können ITOM-Integrität auch verwenden, um Ihre IT-Infrastruktur proaktiv zu analysieren und so Probleme zu erkennen und Serviceausfälle zu verhindern. Mithilfe von ausgereiftem maschinellem Lernen zur Analyse von Informationen über Ihre IT-Infrastruktur werden von der Anwendung automatisch dynamische Schwellenwerte ermittelt und Anomalien identifiziert, die auf potenzielle Serviceausfälle hindeuten.

ITOM-Optimierung

ITOM-Optimierung erhalten Sie Tools für die Bereitstellung von Private und Public Cloud-Infrastrukturen und -Services sowie für eine konsistente Verwaltung und

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

Kostentransparenz. Die Anwendung Cloud-Einblicke , die im ServiceNow Store verfügbar ist, hilft Ihnen bei der Analyse des gesamten Spektrums der mit Cloud-Assets zusammenhängenden Kosten, sodass Sie Möglichkeiten zur Kosteneinsparung und Betriebsoptimierung erkennen und entsprechende Maßnahmen ergreifen können.

Software Asset Management

Verschaffen Sie sich einen Überblick über die in Ihrer IT-Umgebung ausgeführten Software. Software Asset Management funktioniert zusammen mit der durch ITOM-Transparenz unterstützten CMDB. Verwenden Sie Software Asset Management, um Konfigurationen nachzuverfolgen, die sich auf die Nutzung von Softwarelizenzen in Ihren IT-Umgebungen und im Rechenzentrum auswirken.

Kundenservice-Management

Diagnostizieren Sie Probleme im Zusammenhang mit der IT-Infrastruktur, und beheben Sie sie auf effiziente Weise mit mithilfe von von ITOM-Transparenz bereitgestellten Echtzeitdaten.

IT Service Management

Verlassen Sie sich auf die von ITOM-Transparenz erkannte IT-Infrastruktur, um Services für Ihre Benutzer zu verwalten und bereitzustellen. Zeigen Sie Changes und Incidents an, die durch IT Service Management-Anwendungen in ITOM-Transparenz-Servicezuordnungen erstellt und verwaltet werden.

Strategisches Portfoliomanagement

Verwenden Sie die durch ITOM-Transparenz erfassten Daten, um umfassende Kenntnisse über die in Ihrem Unternehmen verwendeten Anwendungen zu erlangen.

Security Operations

Zeigen Sie Security Incidents im Kontext von ITOM-Transparenz an, um herauszufinden, welche Anwendungsservices gefährdet sind. Nutzen Sie diese Informationen, um Bedrohungen je nach Auswirkungen auf Ihr Unternehmen zu priorisieren und zu beheben.

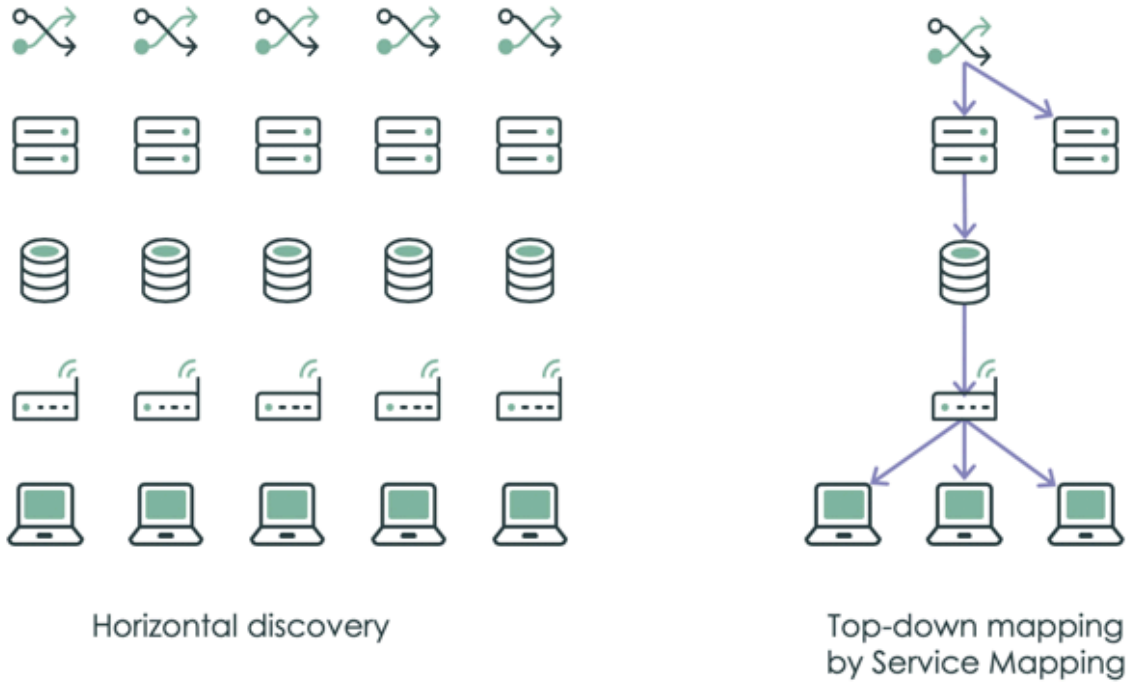
ITOM-Transparenz – Verwendung

Die Discovery-Funktion bietet eine replizierbare und zuverlässige Methode zur Identifizierung der IT-Infrastruktur von Unternehmen. Discovery kann Computer, Server, Software, Drucker, Router und Switches erkennen. Außerdem werden IP-fähige Geräte und die darauf ausgeführten Anwendungen sowie Ressourcen verschiedener Cloud-Anbieter und TLS-Zertifikate gefunden. Diese Methode wird in der Regel als horizontale Erkennung bezeichnet. Bei der horizontalen Erkennung werden keine Verbindungen zwischen Geräten und Anwendungen berücksichtigt.

Die Service-Mapping-Funktion ordnet Abhängigkeiten basierend auf einer Verbindung zwischen Geräten und Anwendungen zu. Diese Methode wird als Zuordnung von oben nach unten bezeichnet. Mithilfe der Zuordnung von oben nach unten können Sie sofort die Auswirkungen eines problematischen Objekts auf den Rest des Anwendungsservicevorgangs erkennen. Anwendungsservicezuordnungen zeigen Infrastrukturobjekte und semantische Verbindungen zwischen ihnen. Service-Mapping generiert Anwendungsservicezuordnungen regelmäßig neu, damit sie jederzeit aktuell und relevant sind. Alle fehlerhaften Objekte werden zusammen mit den betroffenen Geräten und Anwendungen angezeigt und geben so einen visuellen Überblick über den Status des Anwendungsservice.

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

Horizontale Erkennung und Erkennung von oben nach unten – Ergebnisse im Vergleich



Funktionsweise von ITOM-Transparenz

Discovery kann Skripts verwenden, um Daten auf einem Host zu sammeln und zu verarbeiten und dann CMDBzu aktualisieren. Skripts, die CIs in Ihrem Netzwerk erkunden oder untersuchen, werden als Probes bezeichnet. Sensoren entsprechen den Skripts, die die von den Probes zurückgegebenen Daten analysieren. Darüber hinaus setzt Discovery Erkennungsmuster ein. Ein Muster entspricht einer Folge von Vorgängen, die zum Erkennen von Attributen von Geräten sowie von Anwendungen und (bei Verwendung von Service-Mapping) deren ausgehenden Verbindungen dienen.

Service-Mapping kann unterschiedliche Methoden zum Erstellen von Anwendungsservices bereitstellen. Erkennungsmuster sind die von Service-Mapping hauptsächlich verwendete Methode. Sie können jedoch auch Anwendungsservices mithilfe von Tags sowie Datenverkehrverbindungen zwischen Geräten und Anwendungen zuordnen. Weitere Informationen finden Sie unter Richtige Methode zur Zuordnung von Anwendungsservices auswählen.

ITOM-Transparenz Lizenzierung

Bei der für Now Platform® verwendeten Lizenzierungsmethode zahlt Ihre Organisation für die Nutzung von ITOM-Transparenz Anwendungen. ITOM-Transparenz und Discovery sind als separate Lizenzen verfügbar. Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung und -Abonnements.

Was Sie wissen müssen, bevor Sie beginnen

ITOM-Transparenz ist verfügbar durch die Aktivierung des Plugins „Discovery“ (com.snc.discovery) und des Plugins „Service-Mapping“ (com.snc.service-mapping), die ein ITOM-Transparenz-Abonnement erfordern. Nähere Einzelheiten erfahren Sie unter Discovery anfordern und Service-Mapping anfordern. Um die volle Funktionalität

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

von ITOM-Transparenz nutzen zu können, müssen Sie die neuesten ITOM-Transparenz-Out-of-Band-Anwendungen aus dem ServiceNow Store installieren. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den „Release-Informationen zum Versionsverlauf“ im ServiceNow Store.

Definieren Sie Benutzer, und konfigurieren Sie Anmeldeinformationen, um ITOM-Transparenz Zugriff auf Anwendungen und Geräte in Ihrem Unternehmensnetzwerk zu ermöglichen. Details finden Sie unter Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping.

Referenz zu ITOM-Transparenz und CSDM

ITOM-Transparenz besteht aus zwei ServiceNow -Produkten: Discovery und Service-Mapping. Diese Produkte sind dafür verantwortlich, Configuration Items (CIs) in CMDB zu erstellen und miteinander zu verknüpfen. Diese Produktansicht soll Ihnen dabei helfen zu verstehen, wie ITOM-Transparenz mit dem Core-Framework CSDM funktioniert.

Aspekte von ITOM-Transparenz

Discovery

Discovery findet Computer, Server, Drucker, eine Vielzahl von IP-fähigen Geräten und die darauf ausgeführten Anwendungen. Anschließend können sie die CIs in Ihrem CMDB mit den gesammelten Daten aktualisieren.

Service-Mapping

Service-Mapping erkennt alle Anwendungsservices in Ihrer Organisation und erstellt eine umfassende Zuordnung aller Geräte, Anwendungen und Konfigurationsprofile, die die zugehörigen Business Services unterstützen.

Service-Mapping ordnet Abhängigkeiten basierend auf den Verbindungen zwischen Geräten und Anwendungen zu. Mit dieser Methode, die als Top Down-Zuordnung bezeichnet wird, können Sie sofort die Auswirkungen eines problematischen Objekts auf die restlichen Anwendungsservices erkennen.

CMDB -Daten werden implementiert

Einzelheiten zur Implementierung CMDB von -Daten entsprechend dem CSDM -Framework finden Sie unter Implementierung des Frameworks CSDM in Phasen .

Einzelheiten erfahren Sie von

Lernen Sie das Framework CSDM kennen .

Implementierung des Frameworks CSDM in Phasen .

Discovery-Grundlagen.

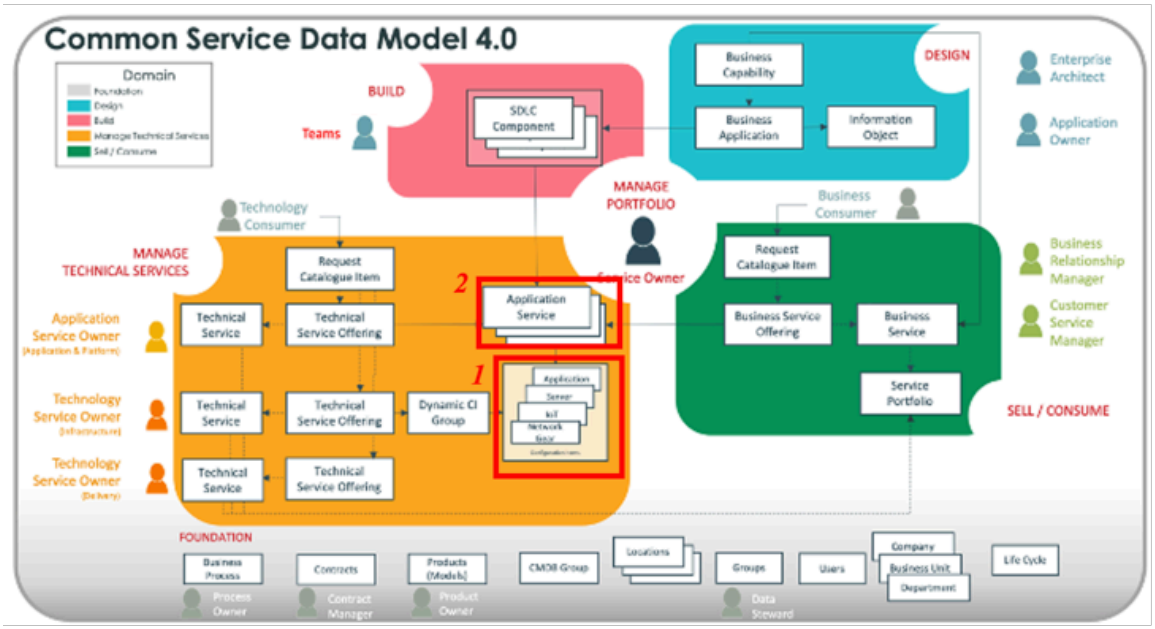
Service-Mapping.

ITOM-Transparenz und CMDB-Tabellen

ITOM-Transparenz verwaltet und verwendet CMDB-Tabellen. Mehrere ServiceNow-Produkte profitieren von ITOM-Transparenz und fügen der Anwendung Mehrwert hinzu.

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

Tabellen, die von ITOM-Transparenz verwaltet werden



Zugeordnete Anwendungsservicetabellen

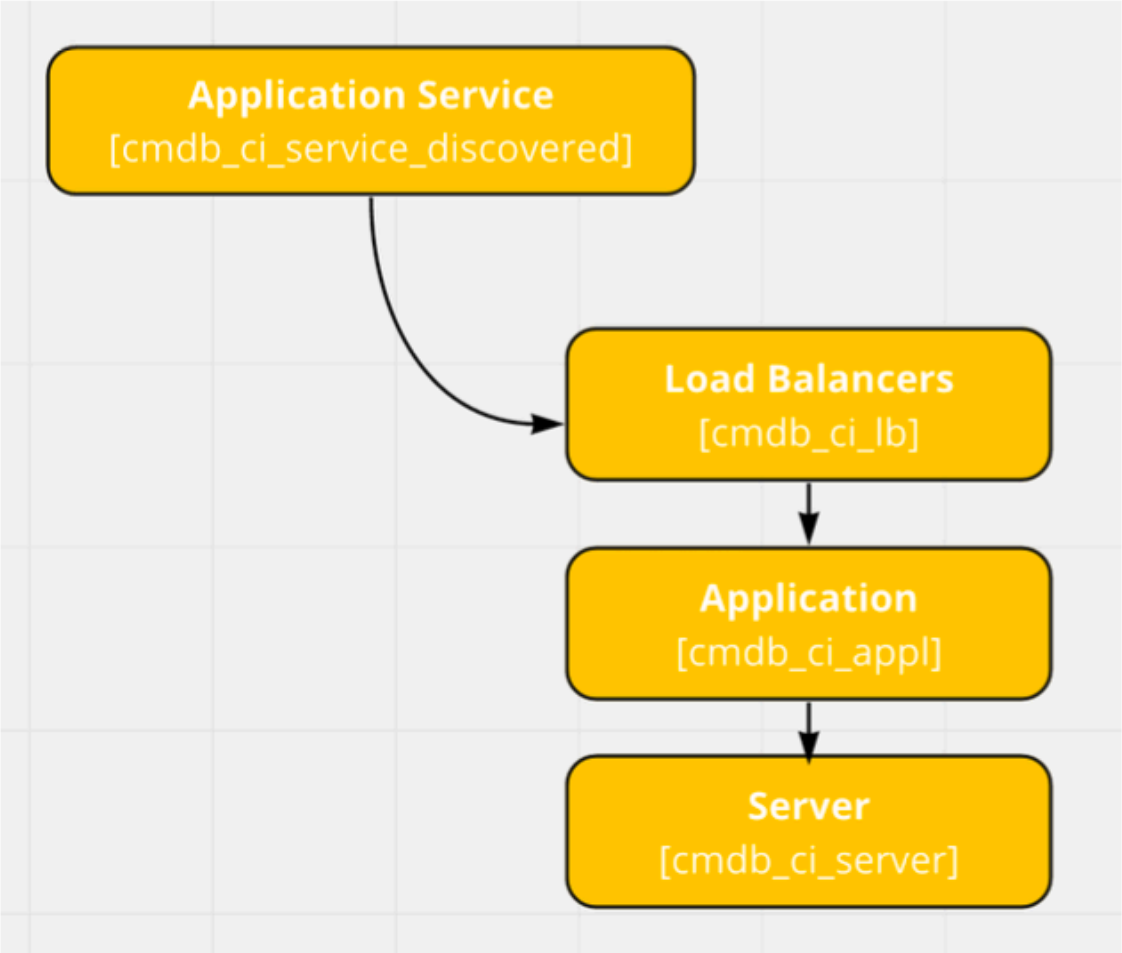
Die von ITOM-Transparenz verwalteten Tabellen hängen von der Methode ab, die zum Zuordnen des Anwendungsservice verwendet wird. Sie können den Assistenten für Anwendungsservices verwenden, um einen Anwendungsservice zu füllen.

- Ordnen Sie den Anwendungsservice mithilfe der Top Down-Discovery von CI-Verbindungen zu. Diese Methode erfordert Service-Mapping, die Rolle sm_admin, und die aktuelle Domäne muss eine untergeordnete Domäne sein. Dies ist die beste Option für Genauigkeit und vollständige Zuordnung. ITOM-Transparenz verwaltet die Tabelle „Zugeordneter Anwendungsservice“ [cmdb_ci_service_discovered]
- Ordnen Sie den Anwendungsservice mithilfe einer Tag-Liste oder Tag-Familie zu. Diese Methode erfordert Service-Mapping und wird für Public oder Private Clouds bevorzugt, in denen normalerweise Tags verwendet werden. ITOM-Transparenz verwaltet die Tabelle mit tagbasierten Zuordnungen [cmdb_ci_service_by_tags].
- Ordnen Sie den Anwendungsservice manuell zu. Diese Methode erfordert die Auswahl bestimmter CIs – es wird keine Automatisierung verwendet. ITOM-Transparenz verwaltet die Servicezuordnungstabelle [cmdb_ci_service_manual].
- Verwenden Sie Dynamischer Service, um manuell erstellte CI-Beziehungen mit einer Servicezuordnungsansicht zu synchronisieren.

Tabellen für Konfigurationselemente (CIs) [cmdb_ci_*]

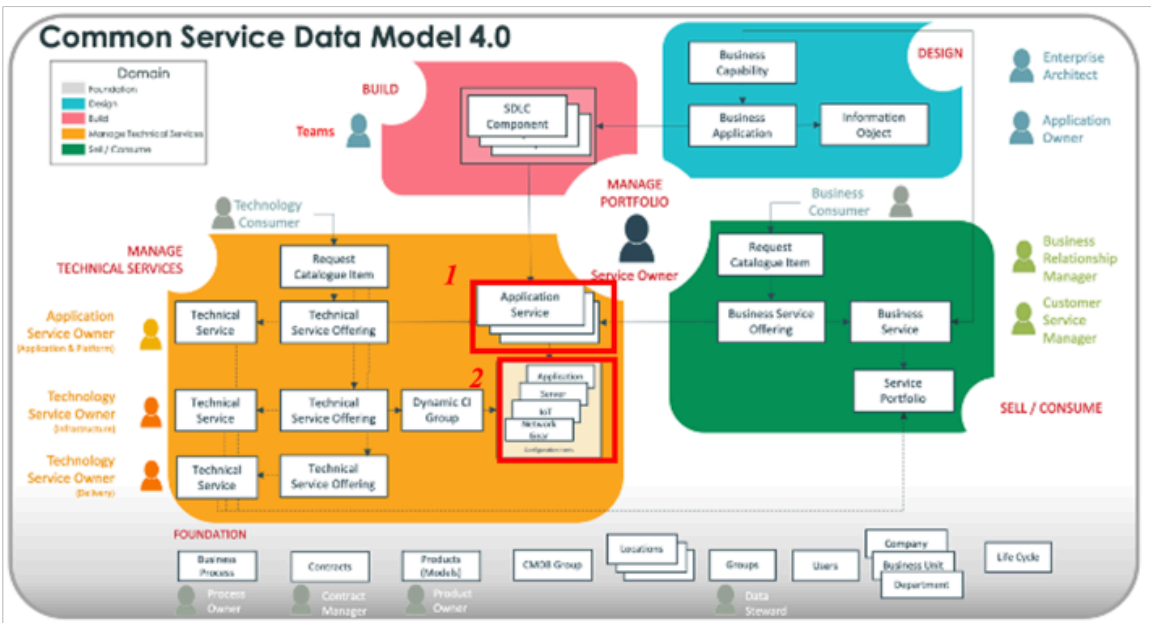
- Tabelle „Anwendung“ [cmdb_ci_appl]
- Tabelle „Server“ [cmdb_ci_server]
- Tabelle „Virtuelle Maschinen“ [cmdb_ci_vm_instance]
- Tabelle „Lastenausgleichsmodul“ [cmdb_ci_lb]
- Tabelle „Netzwerkgerät“ [cmdb_ci_netgear]

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



Tabellen, die von ITOM-Transparenz verwendet werden

1. Tabelle „Dynamische CI-Gruppe“ [cmdb_ci_query_based_service]
2. Produktmodelltabellen (für Technologie-Portfoliomanagement [TPM]) Software- und Hardwaremodelle



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

Produkte, die von ITOM-Transparenz profitieren

- IT Service Management
- Kundenservice-Management (CSM)
- Ereignismanagement
- Cloud-Management
- Asset-Management (Hardware Asset Management und Software Asset Management)
- Strategisches Portfoliomanagement (Finanzmanagement – Showback-Anweisungen, Anwendungs-Portfoliomanagement [APM])
- Security Operations (Reaktion auf Incidents, Software-Schwachstellenmanagement)

CMDB -Daten werden implementiert

Einzelheiten zur Implementierung CMDB von -Daten entsprechend dem CSDM -Framework finden Sie unter Implementierung des Frameworks CSDM in Phasen .

ITOM-Transparenz – Anwendungsfall

In diesem Abschnitt werden die Anwendungsfälle ITOM-Transparenz beschrieben.

Discovery – Anwendungsfall

- Verschaffen Sie sich mehr Transparenz über Ihre lokalen und cloudbasierten Ressourcen.
- Verfolgen Sie Änderungen an Ihrer lokalen, cloudbasierten und serverlosen Infrastruktur im Configuration Management Database (CMDB)nach.
- Stellen Sie eine starke Grundlage mit genauen Daten und Beziehungsansichten für ServiceNow -Produkte, einschließlich Change-Management, Software Asset Management, Kundenservice-Management (CSM)und Security Operations.

Hauptfunktionen des Anwendungsfalls für Discovery

- Richten Sie Discovery -Aufträge ein und verwalten Sie sie.
- IT-Ressourcen und Abhängigkeiten auf einen Blick sehen.
- Erstellen Sie Abfragen, um erkannte IT-Ressourcen zu validieren.
- Verwalten Sie Ihre PKI-Zertifikate (Public Key Infrastructure) in einem zentralen Dashboard.

Ergebnisse des Anwendungsfalls für Discovery

Das CSDM -Framework bietet Discovery ein vorgeschriebenes Modell dafür, wie sich Infrastruktur- und Software-CIs auf andere Bereiche beziehen, z. B. Anwendungsservices, Geschäftsanwendungen und Assets.

Service-Mapping – Anwendungsfall

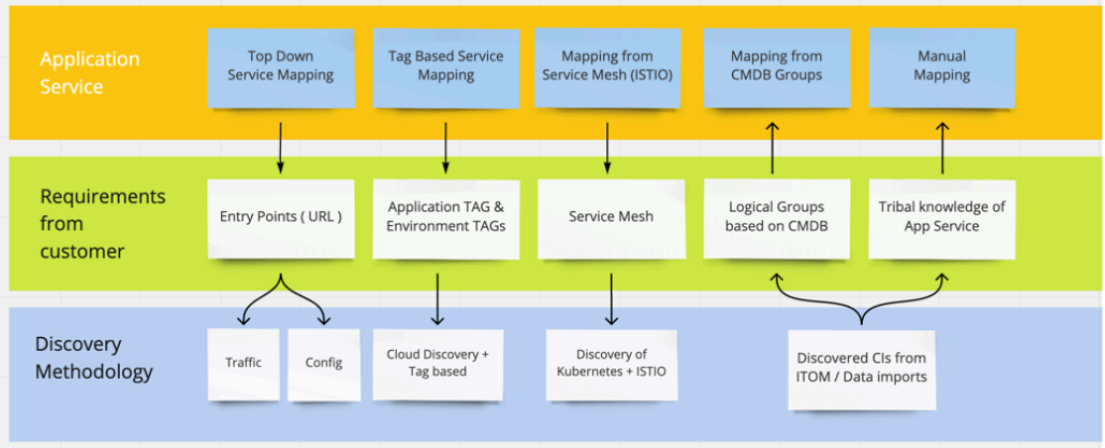
Sie können Anwendungsservices manuell, mithilfe einer API oder durch Erkennung durch Service-Mapping erstellen. Unabhängig von der Erstellungsmethode werden alle Anwendungsservices in der Tabelle „Zugeordneter Anwendungsservice“ [cmdb_ci_service_discovered] gespeichert.

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

Ergebnisse des Anwendungsfalls für Service-Mapping

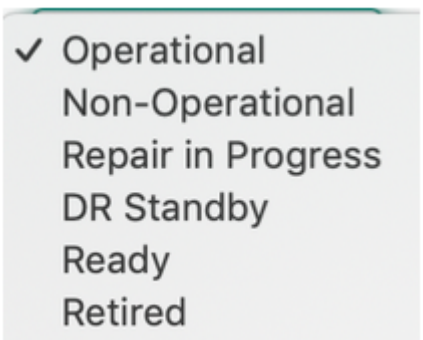
Service-Mapping automatisiert einen kritischen Aspekt von CSDM mit einem konsistenten, automatisierten Ansatz, um die logische Ebene des Modells CSDM mit den physischen Modell-CIs in CMDBzu verbinden. Mit diesem Ansatz können Sie Ihre Geschäftsanwendungen effektiver verwalten. Mit diesem Ansatz können Sie auch die Modellierung Ihrer Geschäftsanwendungen für die Folgenbewertung und -analyse automatisieren. Für Auswirkungsbewertungen und -analysen können Sie eine Reihe von ServiceNow -Produkten verwenden, einschließlich Change-Management, Incident-Managementoder der CMDB Abfragegenerator.

Flow für Anwendungsservices



Ansicht der Anwendungsservices in Betreiber-Arbeitsbereich

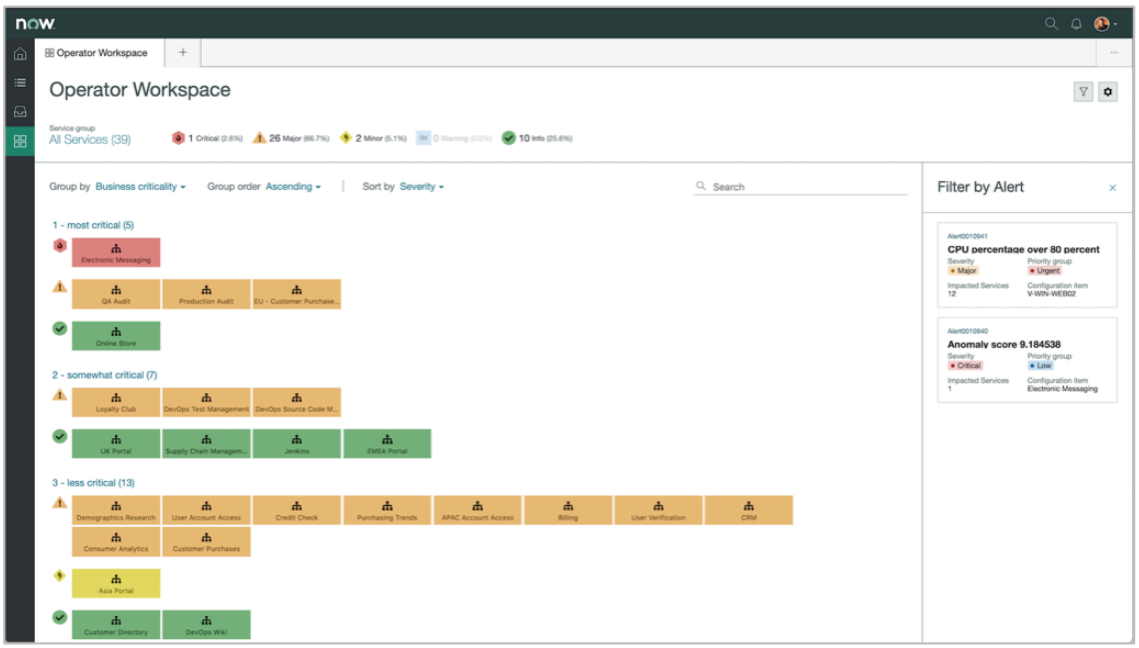
Sie können einen Lebenszyklusstatus für einen Anwendungsservice angeben. Anwendungsservices mit dem Lebenszyklusstatus „Operativ“ können für Servicezuordnungen für die relevanten Workflows verwendet werden, z. B. Workflows für künstliche Intelligenz im IT-Betrieb (AIOPs).



Informationen zu den Services, z. B. die Relevanz, können Sie im Betreiber-Arbeitsbereichanzeigen.

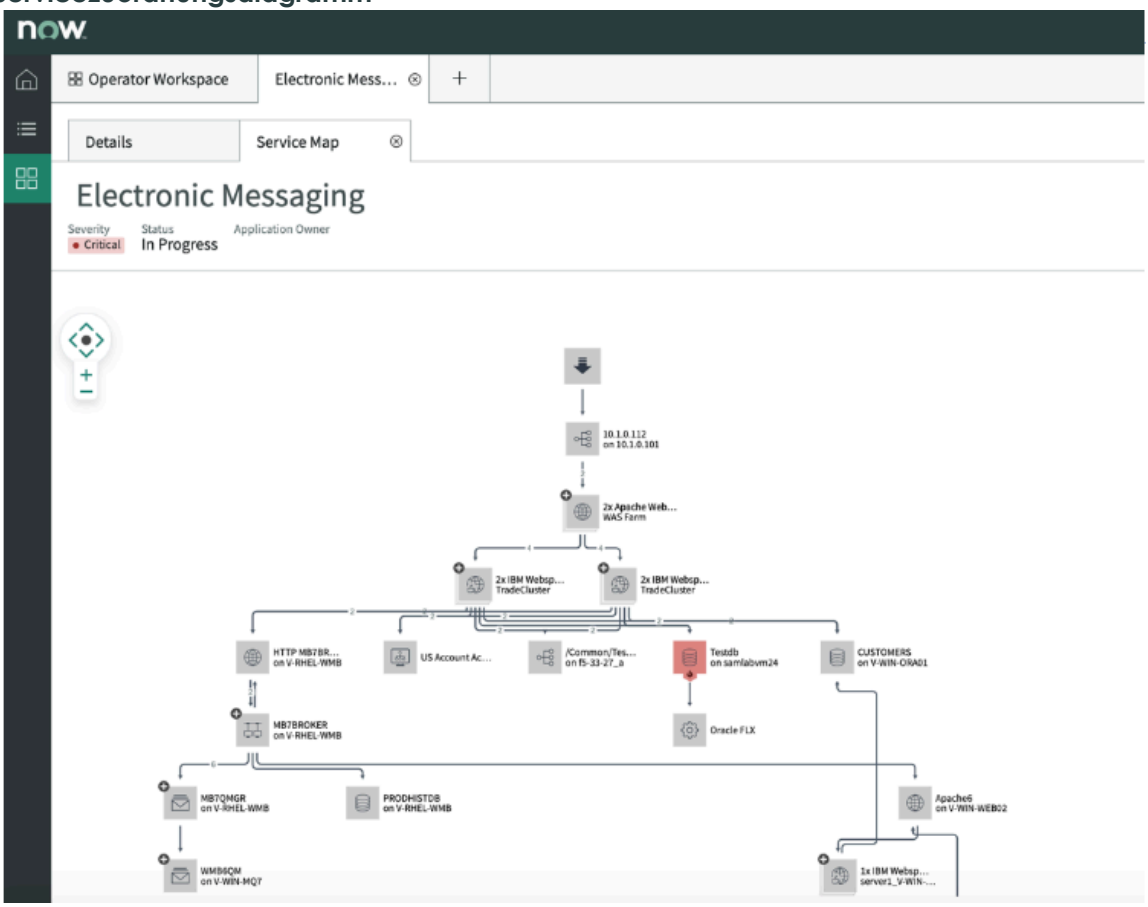
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Betreiber-Arbeitsbereich



Auf der Registerkarte Servicezuordnung wird eine visuelle Darstellung des Service angezeigt.

Servicezuordnungsdiagramm



Zugehörige Informationen

Dokumentlebenszyklus

Lebenszyklus der Hardware

Automatische Übersetzung

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

Lebenszyklus des Standorts

Logischer Lebenszyklus

Produktlebenszyklus

ITOM-Transparenz Überlegungen zum CSDM Framework

Berücksichtigen Sie bei der Implementierung des CSDM-Frameworks die folgenden Punkte.

Mit Service-Mapping können Sie Anwendungsservices definieren.

Nachstehend sind alternative Methoden zum Definieren von Anwendungsservices aufgeführt:

- Manuell definieren.
- Verwenden Sie eine dynamische CI-Gruppe, basierend auf einer Abfrage.
- Verwenden Sie einen Tag-basierten Ansatz (häufig für Cloud-Integrationen verwendet).

Weitere Informationen zum Erstellen von Anwendungsservices finden Sie unter Anwendungsservice erstellen .

Durch ITOM-Transparenz erfasste Daten

ITOM-Transparenz erfasst spezifische Daten für jeden Gerätetyp und speichert sie in dedizierten Tabellen, Feldern und Beziehungen.

Betriebssystem

Betriebssystem

Erkennen Sie Server und Computer abhängig vom Betriebssystem des Computers:

- Windows
- Solaris
- Linux
- Erkennung von OS/X (Mac)
- HPUX
- AIX

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

Virtualisierung

Virtualisierung

Erfassen Sie Informationen über Bereitstellungen, die Virtualisierung beinhalten:

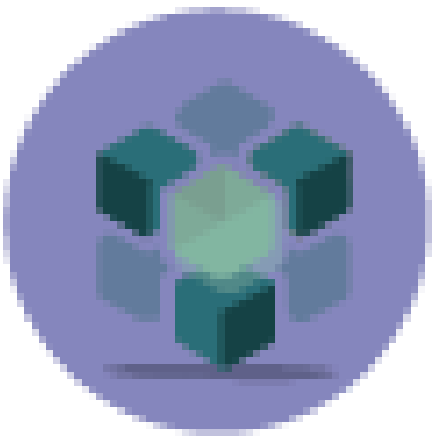
- Erkennung von Hyper-V
- Virtualisierung mit IBM
- Virtualisierung mit Red Hat
- Nutanix Acropolis
- VMware vCenter
- OpenStack-Virtualisierung

Cloud

Cloud

- Amazon Web Service (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- IBM-Cloud
- VMware Cloud

Container



Container

- Kubernetes und OpenShift
- Discovery von Amazon-ECS-Ressourcen
- Erkennung von Pivotal Cloud Foundry

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

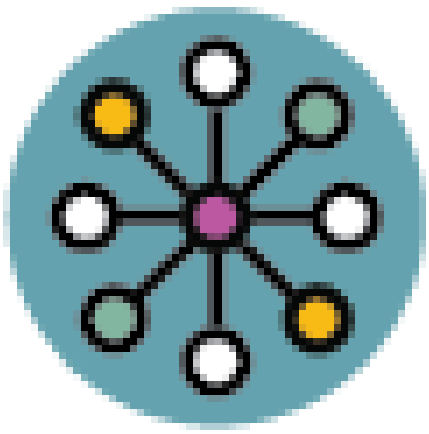
Software

Software

Erkennen Sie zahlreiche Softwareanwendungen, einschließlich:

- Apigee Edge
- ColdFusion
- HP Operations Manager
- IBM Websphere DataPower
- JBOSS unter Windows und Linux
- Web- und E-Mail-Server, einschließlich Microsoft IIS, Apache, Tomcat, Exchange-Postfach
- Puppet-Automatisierungssoftware
- Red Hat JBoss Fuse
- SAP-Anwendungen
- WebLogic- und WebSphere-Server
- Allgemeine Software

Geclusterte Anwendungen



Anwendungen in einem Cluster

- IBM PowerHA-Cluster (HACMP)
- Linux Red Hat-Cluster
- Erkennung von Veritas Cluster Server
- Windows-Servercluster

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

Datenbanken

Datenbanken

Erkennen Sie Datenbanken, einschließlich:

- Oracle
- MySQL
- MicrosoftMicrosoft Azure Event Hubs SQL
- MongoDB
- SAP HANA
- PostgreSQL
- Sybase
- Amazon DynamoDB
- Oracle-Datenbank 12c

Netzwerkgeräte

Netzwerkgeräte

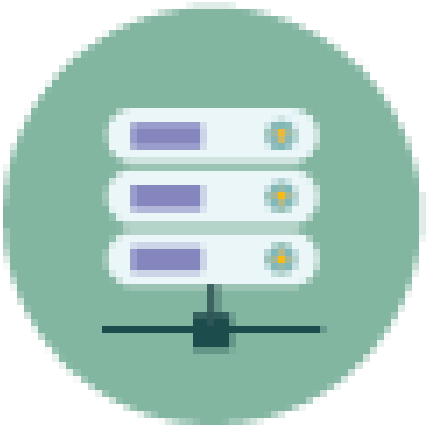
- Router und Switches
- Lastenausgleichsmodule:
  - A10
  - F5 BIG-IP
  - Cisco GSS
  - Cisco CSS
  - Citrix NetScaler
  - HAProxy
  - NGINX
  - Alteon
  - ACE
  - Radware-appDirector
  - Amazon AWS Application ELB Service-Erkennung
- Firewalls
  - Cisco-Firewall
  - Fortinet-Firewall
  - Juniper-Firewall
  - Palo Alto-Firewall
- IP-Netzwerke und bestimmte IP-Adressen
- Cisco UCS-Geräte

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

- Cisco Switch Wireless Access Point (WAP)
- Drucker und Netzgeräte
- IP-Services und -Daemons

Sie können Geräte auch basierend auf TCP-Verbindungen und mithilfe der Layer 2-Erkennung auf SNMP-Ebene finden.

Speicher



Speicher

Erkennen Sie die folgenden Typen von Speichergeräten:

- Pure Storage FlashBlade
- NetApp-Server
- Erkennung von Storage Area Networks (SAN)
- Direct Attached Storage (DAS)
- Network Attached Storage (NAS)
- Hostbusadapter (HBA)
- EMC Isilon

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Discovery und Service-Mapping können eine Vielzahl von Betriebssystemen und Anwendungen erkennen.

Discovery findet Computer, Server, Drucker, verschiedene IP-fähige Geräte und die Anwendungen, die darauf ausgeführt werden. Es kann dann die CIs in Ihrer CMDB mit den gesammelten Daten aktualisieren. Diese Erkennungsmethode wird als horizontale Erkennung bezeichnet. Service-Mapping Ordnet Abhängigkeiten basierend auf einer Verbindung zwischen Geräten und Anwendungen zu. Diese Methode wird als Zuordnung von oben nach unten bezeichnet. Mithilfe der Top Down-Zuordnung können Sie sofort die Auswirkungen eines problematischen Objekts auf den Rest des Serviceinstanzbetriebs erkennen.

Zusätzlich zu den standardmäßig unterstützten Hosts und Anwendungen können Sie zusätzliche Hosts und Anwendungen ermitteln, indem Sie im Store verfügbare Muster bereitstellen. Referenzinformationen zu im Store veröffentlichten Mustern finden Sie unter Verfügbare Erkennungsmuster.

Wenn Ihr Unternehmen Geräte oder Anwendungen verwendet, die nicht standardmäßig unterstützt werden oder Muster verwenden, die im ServiceNow Store verfügbar sind, können Sie Discovery und Service-Mapping so konfigurieren, dass die Erkennung wie unter Von ITOM-Transparenz verwendete Erkennungsmuster beschrieben erfolgt.

Cloud-Discovery Muster finden die Cloud-Ressourcen AWS, Azure, Google Cloud Platform (GCP), IBMund Oracle.

Wenn Sie die erforderlichen Musterbefehle vor dem Ausführen einer Discovery validieren möchten, verwenden Sie das Tool zur Validierung von Befehlen. Weitere Informationen finden Sie unter Validiert Befehle, die in der musterbasierten Discovery verwendet werden.

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

ITOM Content Service Verschafft Transparenz für Ihre Anwendungen durch die Verwendung von KI-Fähigkeiten, die laufende Anwendungsprozesse gruppieren und klassifizieren. Weitere Informationen finden Sie unter ITOM Content Service.

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
.Net Framework	Windows	1.x.x, 2.x.x, 3.x.x, 4.x.x	WMI WinRM	Von oben nach unten	.NET-Applikation
A10 (Lastenausgleichsmodul)	A10	N/V	REST	Horizontal	A10 Lastenausgleich
Adobe JRun	Windows UNIX	4.x	WMI WinRM SSH	Horizontal und von oben nach unten	JRun
Radware Alteon RadWare ADC	Alteon	v31, v29.5	SNMP	Horizontal und von oben nach unten	Alteon Load Balancer
Amazon AWS Discovery von Auto Scaling-Gruppen	AWS	N/V	REST	Horizontal	AWS Auto Scaling-Gruppen (LP) (Muster)
Amazon Relationaler Datenbankservice	AWS	N/V	REST	Horizontal und von oben nach unten	Amazon AWS Relational Database Service
Amazon Route53-Service	AWS	N/V	REST	Horizontal	Amazon AWS Route53 HD
Amazon ECS auf AWS Falgate	AWS	N/V	REST	Horizontal	AWS ECS/ Fargate

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Amazon Application Load Balancer Service	AWS	N/V	REST	Von oben nach unten	Amazon AWS Application ELB Service - TD
Amazon Simple Storage Service (AWS S3)	AWS	N/V	REST	Horizontal und von oben nach unten	AWS S3
Amazon DynamoDB	AWS	N/V	REST	Horizontal und von oben nach unten	Amazon AWS – DynamoDB (Muster)
AWS Lambda-Erkennung	AWS	N/V	REST	Horizontal und von oben nach unten	Amazon AWS Lambda
AWS MemoryDB für Redis	AWS	N/V	REST	Horizontal	AWS MemoryDB (Muster)
Ressourcenbestand von Amazon Web Services (AWS)	AWS	N/V	REST	Horizontal	AWS-Ressourcenbestand
Erkennung von AWS-DB-Clustern	AWS	N/V	REST	Horizontal und von oben nach unten	Amazon AWS DB-Cluster
Amazon Elastic Load Balancer-Service	AWS	N/V	REST	Von oben nach unten	Amazon AWS Classic ELB Service - TD
Erkennung von Amazon Kinesis	AWS	N/V	REST	Horizontal	• Amazon AWS – Kinesis Video Stream Services (LP) • Amazon AWS – Kinesis Data Stream

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					Services (LP) • Amazon AWS – Kinesis Firehose Stream Services (LP) • Amazon AWS – Kinesis Data Analytics Stream Services (LP)
Apache Cassandra-Datenbank und DataStax	UNIX	N/V	SSH	Horizontal und von oben nach unten	Cassandra
Apache HBase	UNIX	N/V	SSH	Horizontal	Sonden: • HBase - Version • HBase - Hauptklasse • HBase - Konfiguration
Apache HTTP Server	Windows UNIX	2.x	WMI WinRM SSH	Horizontal und von oben nach unten	Apache
Apache Kafka und Zookeeper	Apache Kafka	N/V	SSH	Horizontal	Kafka und Zookeeper
Apache HTTP-Webserver des Tomcat Servlet-Containers	Windows UNIX	6.x, 7.x, 8.x	WMI WinRM SSH	Horizontal und von oben nach unten	Tomcat
Apigee Edge Enterprise Edition	Linux	4.xx	SSH HTTP	Horizontal und von	APIGee

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
				oben nach unten	
Lastenausgleichsmodul Avi Vantage einschließlich Avi Controller und GSLB	VMware AWS Avi Networks	N/V	REST	Horizontal und von oben nach unten	AVI LB – Lastenausgleichsmodul Avi Vantage AVI LB – AVI von oben nach unten AVI Session – Avi Controller AVI-GSLB-Unterstützung
BMC Control-M	UNIX Windows	6.x	WMI WinRM SSH	Horizontal	Cntl-M Enterprise Manager
Verwendung der eigenen Lizenz (Bring Your Own License, BYOL)	Amazon AWS Cloud Microsoft Azure Cloud Google Cloud Platform (GCP)	N/V	REST Azure Resource Graph	Horizontal	Die gemeinsame Bibliothek „Image License“ ist eine Erweiterung der Muster: • Amazon AWS – Executable Template (LP) • Amazon AWS – Owned Template (LP) Die gemeinsame Bibliothek „Azure Virtual Machine License“ ist eine Erweiterung des Musters

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					„Azure – Virtual Machine (LP)“. Die gemeinsame Bibliothek „Google Cloud Platform (GCP) – VM-Lizenz“ ist eine Erweiterung des Musters „Google Cloud Platform (GCP) – Virtual Server“.
CA eTrust-Verzeichnisserver	Windows	7.x, 8.x	WMI WinRM	Von oben nach unten	CA eTrust-Verzeichnisserver
CA Identity Manager-Bereitstellungsserver	Windows	11.x, 12.x	WMI WinRM	Von oben nach unten	CA Identity Manager-Bereitstellungsserver für Windows
CA Introscope Enterprise Manager	Windows Unix	8.x, 9.x	WMI WinRM SSH	Von oben nach unten	CA Introscope Enterprise Manager
CA Policy-Server	Windows Unix	11.x	WMI WinRM SSH	Von oben nach unten	CA Policy-Server
CA Site Minder Agent	Windows Unix	11.x	WMI WinRM SSH	Horizontal und von oben nach unten	CA Site Minder Agent

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Cisco Lastenausgleichsmodul für Inhaltsservices-Switch	ACE	6.x	SNMP SSH	Horizontal und von oben nach unten	Cisco CSS SNMP
Cisco ACE-Anwendungssteuerungs-Engine	ACE	2.x	SSH	Horizontal und von oben nach unten	ACE Load Balancer
Cisco Call Manager	Cisco	3.x, 4.x	SNMP SSH	Von oben nach unten	Cisco CallManager
Cisco Fiber Connect	Cisco	Keine Daten	SNMP SSH	Von oben nach unten	Cisco Fibre Connect
Cisco Global Site Selector (Lastenausgleichsmodul)	ACE	3.x	SNMP SSH	Horizontal und von oben nach unten	Cisco GSS
Cisco Unified Computing System	UCS	3.x	REST	Horizontal	UCS - HD
Citrix Delivery Controller	Windows	7.x> 7,5, 8.x	WMI WinRM	Von oben nach unten	Delivery Controller
Citrix Netscaler Global Server Load Balancing (GSLB)	Netscaler	10.x	SNMP SSH NS.conf	Horizontal und von oben nach unten	Netscaler GLB
Citrix Netscaler Load Balancer	Netscaler	9.x, 10.x	SNMP SSH NS.conf	Horizontal und von oben nach unten	Citrix Netscaler
Citrix Netscaler SDX	Citrix NetScaler SDX	13	SSH	Horizontal	Citrix NetScaler SDX

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Citrix Lizenzserver	Windows	7.x	WMI	Horizontal	Lizenzserver
Citrix Xen Hyper-V	Xen Server	7.6	SSH	Horizontal	Citrix Xen Hyper-V
Cloudian-Speicher	Linux	7.x	SSH	Horizontal	Cloudian-Speicher-Discovery
APK verbinden	Windows	1.xx	WMI WinRM	Von oben nach unten	Connect-It Service
Container-Image-Scans für Softwarezerlegung	Linux		REST HTTP	Horizontal	Container-Image-Scan
Software-Stückliste (Software Bill of Material, SBOM)	Linux	N/V	REST HTTP	Horizontal	SBOM ist ein Erweiterungsabschnitt des Container-Image-Scan-Musters
Docker-Virtualisierung	Linux	N/V	N/V	Horizontal	Docker (Muster)
Epic Systems Corporation	UNIX	2014.xx, 2015.xx	SSH	Von oben nach unten	EPIC Cache
Discovery-Berichte von Database Administrator (DBA).	N/V	N/V	N/V	Horizontal	DBA ist ein Erweiterungsabschnitt der Muster: • Cassandra-DB • MSSQL-DB • MySQL-DB • Oracle-DB
Dell EMC PowerMax-Speicher-Discovery mit Mustern	Dell EMC	9 und 10	N/V	Horizontal	EMC PMAX Phase 1 (Muster) EMC PMAX Phase 2 (Muster)

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Dell EMC Data Domain-Speicher-Discovery mit Mustern	DD OS	DD OS 7.3 oder höher	REST	Horizontal	DELL EMC Data Domain (Muster)
Dell EMC XtremIO-Speicher-Array Discovery	Linux	6.3.0 und 6.3.1	REST	Horizontal	EMC XtremIO (Muster)
EMC Isilon	OneFS	8.0	SNMP REST	Horizontal	EMC Isilon
F5 BIG-IP Device Service Clustering	F5	11.x, 12.x	SNMP SSH REST	Horizontal	F5-Cluster
F5 BIG-IP	F5	11.x, 12.x	REST	Horizontal und von oben nach unten	F5-Lastenausgleichsmodul, F5-Lastenausgleichsmodul SSH
Fortinet Firewalls	Fortinet Firewall-Gerät	FortiOS 5.2.x, FortiOS 5.4.x, FortiOS 5.6.x, FortiOS 6.2.x, FortiOS 6.4.x, FortiOS 7.2.x	SNMP	Horizontal	Fortinet-Netzwerk-Firewall der nächsten Generation
Fortinet Firewalls und FortiGate VDOMs	Fortinet Firewall-Gerät	FortiOS 6.2.x, FortiOS 6.4.x, FortiOS 7.x	REST	Horizontal	Fortinet-Netzwerk-Firewall der nächsten Generation – REST
Google Cloud Apigee API-Plattform	Linux	4.xx	SSH	Horizontal und von oben nach unten	APIGee-Service
Google Cloud-Firebase	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) –

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					Firebase Realtime DB
Google Cloud Fire Store	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Firestore DB
Google Cloud-Speicher	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Memorystore DB
Google Cloud SQL	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Cloud SQL DB
Google Cloud BigQuery	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – BigQuery DB
Google Cloud Bigtable	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Bigtable DB
Google Cloud Platform	GCP	N/V	REST	Horizontal	Google Cloud Platform-(GCP-)Ressource
Google Cloud Platform (GCP) Asset-Bestand	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Ressourcenbestand
Google Cloud Platform (GCP) Organisation	GCP	N/V	REST	Horizontal	GCP-Organisation
Google Cloud Spanner	GCP	N/V	REST	Horizontal	Google Cloud Platform (GCP) – Spanner DB

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
HAProxy Lastenausgleichsmodule der Community-Edition	UNIX	1,5, 1,6, 1,7	SSH	Horizontal und von oben nach unten	HA-Proxy
HP Operations Manager	Windows Unix	9.x	WMI WinRM SSH	Horizontal und von oben nach unten	HP Operations Manager
HP Quality Center	Windows	10.x	WMI WinRM	Von oben nach unten	HP Quality Center on Windows
HP Servicemanager	Windows Unix	9.x	WMI WinRM SSH	Horizontal und von oben nach unten	HP Service Manager-Anwendungsserver
HP UCMDB	Windows	N/V	WMI WinRM	Horizontal und von oben nach unten	HP uCMDB on Windows
HP UX-Unix-Server	HPUX	11i	SSH	Horizontal	HP-UX Server
IBMAIX	UNIX	6.x, 7.x	SSH	Von oben nach unten	AIX-Server
IBM CICS Transaction Gateway	Windows UNIX	5.x	WMI WinRM SSH	Von oben nach unten	CTG
IBM Cloud Platform	IBM Cloud Platform	N/V	REST	Horizontal	IBM Cloud – Lastenausgleichsmodul, IBM Cloud – Standortgruppen, IBM Cloud – Netzwerk, IBM Cloud – Organisationen und Bereiche, IBM Cloud – Ressourcengruppen,

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					IBM Cloud – SSH-Schlüssel, IBM Cloud – Speicher, IBM Cloud – Virtual Server
IBM Customer Information Control System	Windows UNIX	4.x, 5.x	WMI WinRM	Von oben nach unten	CICS
IBM Db2 unter Unix	UNIX	8.x, 9.x, 10.x, 11.x	WMI WinRM SSH	Horizontal	DB2
IBM Db2 unter Windows	Windows	8.x, 9.x, 10.x, 11.x	WMI WinRM SSH	Horizontal	DB2
IBM-Virtualisierung und Hardware Management Console (HMC) – Komponenten	UNIX	N/V	SSH	Horizontal	IBM HMC-Server
IBM PowerHA-Cluster (HACMP)	IBM	N/V	REST	Horizontal	IBM PowerHA-Cluster (HACMP)
IBM Security Access Manager	ISAM	8.0.1	SNMP REST	Horizontal und von oben nach unten	ISAM-Server
IBM WebSEAL Discovery	ISAM	9.*,10.*.	REST	Horizontal und von oben nach unten	IBM WebSEAL
IBM Tivoli Access Manager	Windows UNIX	6.x	WMI WinRM SSH	Von oben nach unten	ITAM - Asset Center

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
IBM Tivoli WebSEAL	Windows UNIX	5.x, 6.x	WMI WinRM SSH	Von oben nach unten	Webseal (Muster)
IBM WebSphere Application Server	Windows UNIX	5.x, 6.x, 7.x, 8.x, 9.x	WMI WinRM SSH	Horizontal und von oben nach unten	Websphere
IBM WebSphere DataPower SOA-Appliance	DataPower	I40, I50	SNMP REST	Horizontal und von oben nach unten	DataPower
IBM WebSphere Message Queue	Windows UNIX	6.x, 7.x, 8.x, 9.x	WMI WinRM SSH	Horizontal und von oben nach unten	Die folgenden Muster: • WMQ unter Unix • WMQ unter Windows • WMQ-Warteschlange Unix • WMQ-Warteschlange Windows
IBM Discovery von WebSphere Message Broker (WMB) und WMB-HTTP-Listener	UNIX	6, 7, 8, 9, 10, 11, 12.	N/V	Horizontal und von oben nach unten	WMB unter UNIX (Muster)
IBM WebSphere Portal	Windows UNIX	6.x, 7.x, 8.x	WMI WinRM SSH	Horizontal und von oben nach unten	Websphere Portal On Windows
IBM Z-Mainframe	Z/OS	OS/390	SSH	Horizontal	IBM zOS Server

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Infini-Box		5.0.x	REST HTTP	Horizontal	InfiniBox
Interconnect Web Service	Windows	2014	WMI WinRM	Von oben nach unten	Inter Connect
Istio Service Mesh	Kubernetes	1.15 und höher	HTTP	Horizontal	ISTIO Service Mesh
Kubernetes	Kubernetes	1.21 – 1.30	REST HTTP	Horizontal	Kubernetes
Linux Server	UNIX	Ubuntu 16, RHEL 5.x, CentOS 7.x	SSH	Horizontal	Linux-Server
Linux Pacemaker-Cluster	Linux	N/V	SSH	Horizontal	Pacemaker Linux-Cluster
Microsoft Azure Cloud-Komponenten von MicrosoftMicrosoft Azure Event Hubs Azure WebSite-Service und -Datenbank	Microsoft Azure	N/V	REST	Horizontal	Muster: Azure WebSite Azure WebSite (LP) Erfassen Sie Azure-Datenbank-Tags und WebSite-Tags.
MicrosoftMicrosoft Azure Event Hubs Azure Database-Service	Microsoft Azure	N/V	REST	Horizontal und von oben nach unten	Azure DataBase (Muster)
Azure DNS Zonen-Discovery	Microsoft Azure	N/V	REST	Horizontal	Muster: Azure DNS Zones HD oder Azure DNS Zones (LP)

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
					Azure DNS Zone Recordsets (LP)
MicrosoftMicrosoft Azure Event Hubs Azure Functions	Microsoft Azure	N/V	REST	Horizontal und von oben nach unten	Muster: Azure Functions TD oder Azure Functions (LP)
Microsoft Azure Inventory-Ressourcen	Microsoft Azure	N/V	REST	Horizontal	Azure Inventory und Tags
Azure Virtual Machine Scale Sets (VMSS) Instanz-Discovery	Microsoft Azure	N/V	REST	Horizontal	Azure VM Scale Set Instance
Microsoft Azure LoadBalancer-Service	Microsoft Azure	N/V	REST	Horizontal und von oben nach unten	Azure LoadBalancer TD
MicrosoftMicrosoft Azure Event Hubs Azure SQL-Datenbank	Microsoft Azure	N/V	REST	Horizontal und von oben nach unten	Cloud-Datenbankinstanz
MicrosoftMicrosoft Azure Event Hubs BizTalk Orchestration-Server	Windows	2004, 2006, 2007, 2009, 2010	WMI WinRM	Von oben nach unten	BizTalk-Server
MicrosoftMicrosoft Azure Event Hubs Zertifizierungsstelle	MicrosoftMicrosoft Azure Event Hubs	N/V	WMI	Horizontal	MicrosoftMicrosoft Azure Event Hubs-Zertifizierungsstelle
MicrosoftMicrosoft Azure Event Hubs Dynamics CRM	Windows	2003, 2005, 2007, 2010	WMI WinRM	Von oben nach unten	Dynamic CRM-Komponente

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
MicrosoftMicrosoft Azure Event Hubs Schnellsuche	Windows	2005	WMI WinRM	Horizontal und von oben nach unten	Schnellsuche
MicrosoftMicrosoft Azure Event Hubs Hyper-V-Server	Windows	2008, 2012, 2016	WMI WinRM	Horizontal	Hyper-V-Server
MicrosoftMicrosoft Azure Event Hubs Identity Integration Server	Windows	2003	WMI WinRM	Von oben nach unten	IIFP On Windows Pattern
MicrosoftMicrosoft Azure Event Hubs Internet Information Services	Windows	6.0, 7.x, 8.x	WMI WinRM	Horizontal und von oben nach unten	IIS
MicrosoftMicrosoft Azure Event Hubs Message Queuing	Windows	3.x, 4.x, 5.x	WMI WinRM	Von oben nach unten	MSMQ (Muster)
MicrosoftMicrosoft Azure Event Hubs SharePoint	Windows	2003, 2007, 2010, 2013	WMI WinRM	Horizontal und von oben nach unten	Microsoft SharePoint
MicrosoftMicrosoft Azure Event Hubs SQL Server- und Cluster-Discovery	Windows	2014, 2016, 2017, 2019, 2022	WMI WinRM	Horizontal und von oben nach unten	MSSQL-DB unter Windows (Muster)
MicrosoftMicrosoft Azure Event Hubs SQL Server Analysis Services (SSAS)	Windows	2014, 2016, 2017, 2019, 2022	WMI WinRM	Horizontal und von oben nach unten	SSAS (Muster)
MicrosoftMicrosoft Azure Event Hubs Discovery von SQL Server Integration	Windows	2014, 2016, 2017, 2019, 2022	WMI WinRM	Von oben nach unten	SSIS (Muster)

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Services (SSIS).					
MicrosoftMicrosoft Azure Event Hubs SQL Server Reporting Services	Windows	2014, 2016, 2017, 2019, 2022	WMI WinRM	Von oben nach unten	SSRS (Muster)
MicrosoftMicrosoft Azure Event Hubs Windows-Desktops	Windows	2003, 2008, 2012,	WMI WinRM	Horizontal	Windows OS - Desktops
MicrosoftMicrosoft Azure Event Hubs Windows-Server	Windows	2003, 2008, 2012, 2016, 2022	WMI WinRM	Horizontal	Windows OS - Server
MongoDB	Windows UNIX	3.x.x	WMI WinRM SSH	Horizontal und von oben nach unten	Mongos-Server
Discovery für NetApp Server und Cluster	NetApp	7.x,8.x	SNMP	Horizontal	Muster: NetApp Storage 7-Modus NetApp Cluster SNMP
Discovery für NetApp Server und Cluster	NetApp	7.x,8.x,9.x	HTTP	Horizontal	NetApp Cluster HTTP (Muster)
NetApp SolidFire-Speichersystem	NetApp SolidFire	N/V	HTTP	Horizontal	NetApp SolidFire-Speichersystem
NGINX-Webserver	Windows UNIX	1.10, 1.10.1	WMI WinRM SSH	Von oben nach unten	Nginx-Muster
Nutanix Acropolis (AOS)	UNIX	N/V	REST	Horizontal	Nutanix-Komponenten

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Nutanix Prism Central	UNIX	N/V	REST	Horizontal	Nutanix-Komponenten
OpenText Documentum	Windows UNIX	6.x, 7.x	WMI WinRM SSH	Von oben nach unten	Muster für Lizenzserver
OpenStack-Ressourcen	OpenStack	N/V	REST	Horizontal	OpenStack (Muster)
Oracle Applikationsserver	Windows UNIX	9.x, 10.x	WMI WinRM SSH	Von oben nach unten	Oracle iAS
Oracle Concurrent Server	Windows UNIX	10.x, 11.x, 12.x	WMI WinRM SSH	Von oben nach unten	Concurrent Server
Oracle Cloud-Infrastruktur	Oracle	N/V	REST	Horizontal	Oracle Cloud-Infrastruktur
Oracle Clusterware	Linux	10.x, 11.x, 12.x	SSH	Horizontal	Oracle CRS
Oracle Datenbank	Windows UNIX	8.x.x, 9.x.x, 10.x.x, 11.x.x, 12.x.x	WMI WinRM SSH	Horizontal und von oben nach unten	Oracle-DB
Oracle Database Advanced Queuing	Windows UNIX	9.x.x, 10.x.x, 11.x.x, 12.x.x	WMI WinRM SSH	Von oben nach unten	Advanced Queue Queue
Oracle Datenbank 12c	Windows UNIX	N/V	WMI WinRM SSH	Horizontal	PDB/CDB
Oracle Discover Server	Windows	9.x, 10.x	WMI	Von oben nach unten	Discoverer Engine

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
	UNIX		WinRM SSH		
Oracle E-Business Suite	Windows UNIX	10.x, 11.x	WMI WinRM SSH	Von oben nach unten	E-Business Suite
Oracle Formulare	Windows UNIX	9.x, 10.x	WMI WinRM SSH	Von oben nach unten	Formulare-Engine
Oracle Fulfillment Server	Windows UNIX	9.x, 10.x	WMI WinRM SSH	Von oben nach unten	Fulfillment Server
Oracle GoldenGate	Windows UNIX	N/V	WMI SSH	Horizontal und von oben nach unten	Oracle GG
Oracle Global License Advisory Services (GLAS)	N/V	N/V	SSH	Horizontal	Oracle GLAS-Datenerfassung (Muster)
Oracle Java-Prozesse	JDK	Alle	N/V	Horizontal	Java-Installationsmuster ACC-basierte Discovery
Oracle Solaris LDOM	Solaris	10, 11	SSH	Horizontal	Solaris Logical Domain (LDOM)-Infrastruktur
Oracle HTTP Server	Windows UNIX	N/V	WMI WinRM SSH	Von oben nach unten	HTTP Server

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Oracle iPlanet Webserver	Solaris	4.x, 6.x, 7.x	SSH	Horizontal und von oben nach unten	Sun iPlanet Webserver
Oracle Java Enterprise System (JES)	Solaris	7.x	SSH	Von oben nach unten	Sun JES-Muster
Oracle-Listener	Linux	12.2.x.x	SSH	Horizontal	Oracle Listener HD
Oracle Metric Server	Windows UNIX	9.x, 10.x	WMI WinRM SSH	Von oben nach unten	Metric Server
Oracle MySQL Server	Windows UNIX	4.x, 5.x	WMI WinRM SSH	Horizontal und von oben nach unten	My SQL Server unter Windows und Linux (Muster)
Oracle Notification Server	Windows UNIX	9.x, 10.x	WMI WinRM SSH	Von oben nach unten	Oracle Benachrichtigungs-Server
Oracle Peoplesoft	Windows Unix	8.x	WMI WinRM SSH	Von oben nach unten	PeopleSoft-Applikationsserver
Oracle Prozessmanager	Windows Unix	9.x.x, 10.x.x	WMI WinRM SSH	Von oben nach unten	Prozessmanager
Oracle RAC	Windows UNIX	9.x.x, 10.x.x, 11.x.x, 12.x.x	WMI WinRM SSH	Von oben nach unten	App TNS-Dienst

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Oracle Berichtsserver	Windows UNIX	9.x.x, 10.x.x	WMI WinRM SSH	Von oben nach unten	Berichtsserver
Oracle Solaris Server	Solaris	9, 10, 11, SPARC	SSH	Horizontal	Solaris-Server
Oracle Solaris Infrastruktur für logische Domänen	Solaris	N/V	SSH	Horizontal	Solaris LDOM
Oracle WebLogic Application Server	Windows UNIX	8.x, 9.x, 10.x, 11.x, 12.x	WMI WinRM SSH	Horizontal und von oben nach unten	WebLogic
Pivotal Cloud Foundry	PCF	N/V	REST	Horizontal und von oben nach unten	Muster: Pivotal Cloud Foundry Bosh
Pivotal RabbitMQ	Windows UNIX	3.x.x	WMI WinRM SSH	Von oben nach unten	RabbitMQ Cluster Unix - Muster
PostgreSQL-DB	Windows UNIX	6.x, 7.x, 8.x	WMI WinRM SSH	Horizontal und von oben nach unten	PostgreSQL-DB
Puppet	UNIX	N/V	SSH	Horizontal	Sonden: • Puppet – Master-Info • Puppet – Zertifikatsanfragen • Puppet – Manifest • Puppet - Modules

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Discovery für reinen Speicher FlashArray .	Pure Storage	N/V	REST	Horizontal	Pure Flash Array Storage (Muster)
Pure Storage FlashBlade	Pure Storage	4.10.7	REST SSH	Horizontal	Pure Storage
RadWare AppDirector (Lastenausgleichsmodul)	Radware	N/V	SNMP	Horizontal und von oben nach unten	AppDirector Load Balancer
Red Hat Cluster Suite	Linux	RH 5.x, 6.x, 7.x	SSH	Horizontal	RH Cluster
Red Hat JBoss-Anwendungsserver	Windows UNIX	6.x, 7.x	WMI WinRM SSH	Horizontal und von oben nach unten	Jboss (Muster)
Red Hat JBoss Fuse-Erkennung	Windows UNIX	N/V	SSH	Horizontal und von oben nach unten	Jboss Fuse (Muster)
Red Hat OpenShift-Komponenten von Kubernetes	RHEL	API 1.x	REST	Horizontal	OpenShift-Infobibliothek sammeln, die als Erweiterungsabschnitt des Kubernetes-Musters verwendet wird
Red Hat Virtualisierung	RHV	N/V	REST	Horizontal	RHV
Rubrik-Cluster		N/V	HTTP HTTPS	Horizontal	Mehrere Muster
SAP Business Object XI Scheduler	Windows	2004, 2005, 2008	WMI WinRM	Horizontal und von oben nach unten	SAP BO BOXISchedule Router on Windows - Muster

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
SAP Crystal Management Server	Windows	2004, 2005, 2008	WinRM	Horizontal und von oben nach unten	SAP Business Objects CMS Server on Windows
SAP HANA	Windows UNIX	2015, 2016, 2017	WMI WinRM SSH	Horizontal und von oben nach unten	SAP HANA DB (Muster)
SAP HANA-Katalog	UNIX	N/V	N/V	Horizontal	SAP Hana 2.0 DB-Katalog (Muster)
SAP Sybase ASE-Erkennung	Windows UNIX	16	WMI WinRM SSH	Horizontal und von oben nach unten	Sybase (Muster)
SAP Sybase ASE-Erkennung-Katalog	UNIX	16	SSH	Horizontal	Sybase (Mustererweiterung)
Cisco Drahtlosen Zugriffspunkt (WAP) wechseln	Cisco Network Switch	N/V	SNMP	Horizontal	WAP
Sun Directory Proxy Server	Solaris	4.0.8	SSH	Von oben nach unten	Sun Directory-Proxy-Server
Sun Java System Directory Server	Solaris	6.3	SSH	Von oben nach unten	Sun Directory Server
Thunder ADC	A10	2.x, 4.x	SNMP/SSH	Horizontal und von oben nach unten	A10 Lastenausgleich
Tibco ActiveMatrix Adapter	UNIX	7.1.0	SSH	Von oben nach unten	Tibco-Adapter
Tibco BusinessWorks	Windows	5.7.2	WMI	Horizontal	ActiveMatrix BusinessWorks

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

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
	UNIX		WinRM SSH		
Tibco Enterprise Message Service (EMS)	Windows UNIX	5.x, 6.x	WMI WinRM SSH	Horizontal und von oben nach unten	Enterprise Message Service
Tibco Enterprise Message Service-(EMS-)Warteschlange	Windows UNIX	5.x, 6.x	WMI WinRM SSH	Horizontal und von oben nach unten	Enterprise Message Service
Tibco Hawk	UNIX	5.2.0	SSH	Von oben nach unten	TibcoHawk
Veritas Enterprise Vault	Windows	14.1	WMI WinRM	Von oben nach unten	Enterprise Vault
Veritas-Clusterserver	UNIX	6.xx	SSH	Horizontal und von oben nach unten	Veritas-Cluster
VMware NSX Advanced Load Balancer	VMware	1	REST-API	Horizontal und von oben nach unten	NSX

Erkennung von Betriebssystemen

Discovery identifiziert die folgenden Computer, Cluster und virtuellen Computer.

Erkennung von AIX-Servern

Discovery identifiziert und klassifiziert Informationen über AIX-Server.

Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen .

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

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

Verwenden Sie für AIX-Computer OpenSSH Version 7.5.102 und höher, da sich frühere Versionen von OpenSSH darauf auswirken können, welche Geräte von Discovery erkannt werden.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
AIX (UNIX-Klassifizierung)	• Probe „Horizontal Discovery“: Startet Muster • AIX - Installed Software^ • AIX - ADM^ • AIX - Identity* • AIX - CPU* • AIX - Hardware Model* • AIX - Memory* • AIX - OS Patches* • AIX - OS Release* • AIX - OS Revision* • UNIX - Find FQDN • UNIX - OS Filesystems • UNIX - OS Uptime	AIX-Server

*Diese Probes sind für die Klassifizierung nicht aktiv, da Discovery standardmäßig Muster für diese Erkennungen verwendet.

^Diese Probes bleiben standardmäßig aktiv, auch wenn Discovery die Muster-Discovery verwendet.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Bezeichnung	Tabellenname	Feldname	Quelle
Betriebssystem	cmdb_ci_computer	os	uname
BS-Version	cmdb_ci_computer	os_version	oslevel
BS-Service Pack	cmdb_ci_computer	os_service_pack	oslevel
Kurzbeschreibung	cmdb_ci_aix_server	short_description	uname

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

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_aix_server	Name	DNS, NBT
Hostname	cmdb_ci_aix_server	host_name	DNS, NBT
DNS-Domäne	cmdb_ci_aix_server	dns_domain	DNS
Startdatum	cmdb_ci_aix_server	start_date	uptime
CPU-Typ	cmdb_ci_computer	cpu_type	lsdev, lsattr
CPU-Geschwindigkeit (MHz)	cmdb_ci_computer	cpu_speed	lsdev, lsattr
CPU-Anzahl	cmdb_ci_computer	cpu_count	lsdev, lsattr
Hersteller	cmdb_ci_aix_server	manufacturer	lsattr
Modell-ID	cmdb_ci_aix_server	model_id	lsattr
RAM (MB)	cmdb_ci_computer	ram	lsdev, lsattr
Name	cmdb_ci_file_system	Name	df
Kapazität (MB)	cmdb_ci_file_system	Kapazität	df
Verfügbarer Speicherplatz (MB)	cmdb_ci_file_system	available_space	df
Bereitstellungspunkt	cmdb_ci_file_system	mount_point	df
Name	cmdb_ci_patches	Name	instfix
Name	cmdb_running_process	Name	ps
Befehl	cmdb_running_process	command	ps
Verbunden mit	cmdb_running_process	connects_to	lsof
Lauschen auf	cmdb_running_process	listening_on	lsof
Typ	cmdb_running_process	Typ	ps
PID	cmdb_running_process	pid	ps
Parameter	cmdb_running_process	parameters	ps
Name	cmdb_ci_network_adapter	Name	ifconfig, netstat
IP-Adresse	cmdb_ci_network_adapter	ip_address	ifconfig, netstat
MAC-Adresse	cmdb_ci_network_adapter	mac_address	ifconfig, netstat
Netzmaske	cmdb_ci_network_adapter	netmask	ifconfig, netstat

Die LPAR-Discovery für die AIX-Server-Mustererweiterung schlägt aufgrund des Fehlers MISSING_DEPENDENCY fehl

Wenn das Gebietsschema von AIX-Server ja_JP.UTF-8 ist, schlägt die LPAR-Discovery der AIX-Server-Mustererweiterung aufgrund des Fehlers MISSING_DEPENDENCY fehl und gibt die Suche in Japanisch zurück. Um dieses Problem zu beheben, befolgen Sie die Schritte im Muster „LPAR-Discovery in AIX-Server“ schlägt fehl mit MISSING_DEPENDENCY In der Nutzlast sind keine Beziehungen für die abhängige Klasse [cmdb_ci_lpar_instance] definiert, die mit

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

Containment-/Hosting-Regeln übereinstimmt: [cmdb_ci_lpar_instance >> Virtualized by >> cmdb_ci_ibm_frame] [KB0963418] Artikel in der Now Support Knowledge Base.

Azure Virtual Machine Scale Sets (VMSS) Instanz-Discovery

Azure Virtual Machine Scale Sets (VMSS) Mit können Sie eine Gruppe von VMs mit Lastenausgleich erstellen und verwalten. Die Anzahl der VM-Instanzen kann automatisch je nach Bedarf oder nach einem definierten Zeitplan erhöht oder verringert werden. Es gibt zwei Orchestration-Modi Flexible und Einheitlich.

- VMSS mit Flexible Orchestration erzielt hohe Verfügbarkeit im großen Umfang mit identischen oder mehreren VM-Typen. Mit der flexiblen Orchestrierung bietet Azure eine einheitliche Experience im gesamten VM-Ökosystem Azure von .
- VMSS mit Einheitliche Orchestrierung optimiert für große zustandslose Arbeitsauslastungen mit identischen Instanzen. VMSS mit einheitlicher Orchestrierung verwenden ein VM-Profil oder eine Vorlage, um auf die gewünschte Kapazität zu skalieren. Zwar besteht eine gewisse Möglichkeit, einzelne VM-Instanzen zu verwalten oder anzupassen, bei Einheitlich werden jedoch identische VM-Instanzen verwendet.

Beziehung in vorhandenem Muster VM (LP)

Übergeordnet	Beziehungstyp	Untergeordnetes Element
cmdb_ci_vm_instance	Verwaltet von: Verwaltet	cmdb_ci_instance_scale_set

Muster für einheitlichen Skalierungssatz der Azure-VM-Instanz füllen vorhandene Tabelle „cmdb_ci_vm_instance“ ausfüllen

Ausgefüllte Attribute: **Name**, **object_id**, **state**, **disks**, **disk_size**, **location**, **nics**, **vm_inst_id**, **image_id**

Beziehungen

Übergeordnet	Beziehungstyp	Untergeordnetes Element
cmdb_ci_instance_scale_set	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_vm_instance	Verwaltet von:Verwalten	cmdb_ci_instance_scale_set
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_vm_instance	Endpunkt verwenden bis: Endpunkt verwenden von	cmdb_ci_endpoint_vnic
cmdb_ci_endpoint_block	Implementierter Endpunkt bis:Implementierter Endpunkt von	cmdb_ci_storage_volume
cmdb_ci_vm_instance	Endpunkt verwenden bis: Endpunkt verwenden von	cmdb_ci_endpoint_block
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_compute_template
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_cloud_hardware_type
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_os_template

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

Beziehungen (Fortsetzung)

cmdb_ci_os_template	Gehostet auf: Host	cmdb_ci_azure_datacenter
cmdb_ci_storage_volume	Gehostet auf: Host	cmdb_ci_azure_datacenter

Apache-Erkennung von HBase-Instanzen

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz von HBase auf einem UNIX-Server erkannt wird.

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

In der folgenden Tabelle kann die Quelle `HBase Instance@`*`hostname`* die Information enthalten, ob es sich bei der Instanz um eine primäre oder eine sekundäre Instanz handelt. Der Name enthält *`Hmaster`*, wenn die Instanz eine primäre Instanz ist. Der Name einer Sekundärinstanz enthält *`HRegionServer`*.

Erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_db_hbase_instance	Name	HBase-Instanz@*`Hostname`*
Stammverzeichnis	cmdb_ci_db_hbase_instance	root_dir	hbase-site.xml
TCP-Port	cmdb_ci_db_hbase_instance	tcp_port	Laufender Prozess
Standort-XML	cmdb_ci_db_hbase_instance	site_xml	hbase-site.xml
Version	cmdb_ci_db_hbase_instance	Version	HBase-Shell
HBase-Homepage	cmdb_ci_db_hbase_instance	hbase_home	Laufender Prozess
ZooKeeper Quorum	cmdb_ci_db_hbase_instance	zookeeper	hbase-site.xml

Erkennung von HPUX

Discovery identifiziert und klassifiziert Informationen über HPUX-Computer.

Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen .

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

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

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
HP-UX (Unix-Klassifizierer)	• Probe „Horizontal Discovery“: Startet Muster • HP-UX - Installed Software^ • HP-UX - ADM^ • HP-UX - OS Patches* • HP-UX - CPU Speed* • HP-UX - Total Memory* • HP-UX - Hardware Model* • HP-UX - CPU Info* • HP-UX - Identity* • UNIX - Find FQDN* • UNIX - OS Filesystems* • UNIX - OS Uptime*	HP-UX Server

*Diese Probes sind für die Klassifizierung nicht aktiv, da Discovery standardmäßig Muster für diese Erkennungen verwendet.

^Diese Probes bleiben standardmäßig aktiv, auch wenn Discovery die Muster-Discovery verwendet.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Bezeichnung	Tabellenname	Feldname	Quelle
Betriebssystem	cmdb_ci_hpux_server	os	uname
Kurzbeschreibung	cmdb_ci_hpux_server	short_description	uname
Name	cmdb_ci_hpux_server	Name	DNS, NBT
Hostname	cmdb_ci_hpux_server	host_name	DNS, NBT
DNS-Domäne	cmdb_ci_hpux_server	dns_domain	DNS
Startdatum	cmdb_ci_hpux_server	start_date	uptime
Hersteller	cmdb_ci_computer	manufacturer	dmidecode
Seriennummer	cmdb_ci_hpux_server	serial_number	uname
CPU-Typ	cmdb_ci_hpux_server	cpu_type	cpuinfo

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

Bezeichnung	Tabellenname	Feldname	Quelle
CPU-Geschwindigkeit (MHz)	cmdb_ci_hpux_server	cpu_speed	adb
CPU-Anzahl	cmdb_ci_hpux_server	cpu_count	cpuinfo
Modell-ID	cmdb_ci_hpux_server	model_id	Modell
RAM (MB)	cmdb_ci_hpux_server	ram	adb
Name	cmdb_ci_file_system	Name	df
Kapazität (MB)	cmdb_ci_file_system	Kapazität	df
Verfügbarer Speicherplatz (MB)	cmdb_ci_file_system	available_space	df
Bereitstellungspunkt	cmdb_ci_file_system	mount_point	df
Name	cmdb_ci_patches	Name	swlist
Name	cmdb_running_process	Name	ps
Befehl	cmdb_running_process	command	ps
Typ	cmdb_running_process	Typ	ps
PID	cmdb_running_process	pid	ps
Parameter	cmdb_running_process	parameters	ps
Name	cmdb_ci_network_adapter	Name	hifconfig
IP-Adresse	cmdb_ci_network_adapter	ip_address	hifconfig
MAC-Adresse	cmdb_ci_network_adapter	mac_address	hifconfig
Netzmaske	cmdb_ci_network_adapter	netmask	hifconfig

Erkennung von Hyper-V

Die Anwendung ServiceNow Discovery sucht nach MicrosoftMicrosoft Azure Event Hubs Hyper-V-Hypervisoren in Ihrer Umgebung.

Hyper-V ist ein von MicrosoftMicrosoft Azure Event Hubs entwickelter Hypervisor, mit dem Sie virtuelle Maschinen (VMs) auf einem physischen Server oder Computer erstellen und verwalten können. Sie ermöglicht die Hardware-Virtualisierung, sodass mehrere virtuelle Computer auf einem physischen Computer ausgeführt werden und gleichzeitig die zugrunde liegenden Hardware-Ressourcen wie CPU, Arbeitsspeicher, Speicher und Netzwerk gemeinsam genutzt werden.

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Hyper-V unterstützt die folgende Funktionalität:

- Failoverclustering: Failover wird mit dem Failovercluster-Manager verwaltet.
- Live-Migration: Virtuelle Computer können zwischen Failovercluster-Knoten verschoben werden, ohne den virtuellen Computer herunterzufahren.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

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

Unterstützte Versionen

Discovery wird für folgende Versionen von Hyper-V Server unterstützt:

- 2008
- 2012
- 2012 R2
- 2016
- 2019

Wichtig: Die Discovery von Hyper-V unter Windows 2016 wird nurfür Muster unterstützt. Wenn Sie ein Upgrade durchgeführt haben und noch Probes und Sensoren für Discovery verwenden, finden Sie unter KB0694773 Anweisungen zum Konfigurieren von Hyper-V-Probes.

Anmeldeinformationen

Windows-Anmeldeinformationen mit Domänenadministratorrechten konfigurieren Sie sollten PowerShell auch für MID-Server aktivieren, die zur Erkennung von Hyper-V-Servern und -Instanzen verwendet werden.

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
Hyper-V-Server Die Klassifizierung gilt nur für eigenständige Hyper-V-Server (Server, die NICHT unter Windows 2008 ausgeführt werden).	• Probe „Horizontal Discovery“: Startet Muster • Windows - ADM^ • Windows - Installed Software^ • Hyper-V - Cluster* • Hyper-V - Resource Pools* • Hyper-V - Virtual Machines* • Hyper-V - Virtual Networks* • Mehrere andere Windows-Probes werden ebenfalls ausgeführt, zum Beispiel „Windows - Identity“ und „Windows - Software“.*	Hyper-V-Server

*Diese Probes sind für die Klassifizierung nicht aktiv, da Discovery standardmäßig Muster für diese Erkennungen verwendet.

^Diese Probes bleiben standardmäßig aktiv, auch wenn Discovery die Muster-Discovery verwendet.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

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

Von Discovery während der horizontalen Erkennung erfasste Daten

Virtuelle Instanzen

Bezeichnung	Feldname	Datenbeschreibung	Gespeichert in Tabelle
Objekt-ID ^	object_id	ID	cmdb_ci_hyper_v_instance
Name^	Name	Name	cmdb_ci_hyper_v_instance
Status	state	• An • Aus	CMDB_CI_Hyper_v_Instanz*
CPUs	CPUs	Anzahl	CMDB_CI_Hyper_v_Instanz*
Arbeitsspeicher	memory	Menge in MB	CMDB_CI_Hyper_v_Instanz*
Netzwerkadapter	nics	Anzahl	CMDB_CI_Hyper_v_Instanz*
Datenträger	disks	Anzahl+	CMDB_CI_Hyper_v_Instanz*
Datenträgergröße	disks_size	Kapazität in GB+	CMDB_CI_Hyper_v_Instanz*
Seriennummer virtuelle Hauptplatine	baseboard_serial	Virtuelle Seriennummer	cmdb_ci_hyper_v_instance
BIOS-Seriennummer	bios_serial	Virtuelle Seriennummer	cmdb_ci_hyper_v_instance
Gehäuse-Seriennummer	chassis_serial	Virtuelle Seriennummer	cmdb_ci_hyper_v_instance
BIOS-GUID	bios_guid	Global eindeutiger Bezeichner (GUID)	cmdb_ci_hyper_v_instance

*Attribute, die der Tabelle `cmdb_ci_hyper_v_instance` hinzugefügt werden, wenn das Muster „Hyper-V Server“ verwendet wird. Für Upgrades fügen Probes und Sensoren diese Attribute weiterhin der Tabelle `cmdb_ci_vm_instance` hinzu.

^Neu erkanntes Attribut bei Verwendung des Musters Hyper-V Server.

+Discovery kann diese Informationen nur zurückgeben, wenn die virtuelle Maschine ausgeführt wird.

Virtuelle Server

Bezeichnung	Feld	Gespeichert in Tabelle
Name	Name	cmdb_ci_hyper_v_server
Gehäusetyp	chassis_type	cmdb_ci_hyper_v_server
Beschreibung	short_description	cmdb_ci_hyper_v_server
OS-Adressbreite (Bit)	os_address_width	cmdb_ci_hyper_v_server

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

Virtuelle Server (Fortsetzung)

Bezeichnung	Feld	Gespeichert in Tabelle
Betriebssystem	BS	`cmdb_ci_hyper_v_server`
Host-Name	hostname	`cmdb_ci_hyper_v_server`
IP-Adresse	ip_address	`cmdb_ci_hyper_v_server`
BS-Version	os_version	`cmdb_ci_hyper_v_server`
BS-Service Pack	os_service_pack	`cmdb_ci_hyper_v_server`
Ist virtuell	virtual	`cmdb_ci_hyper_v_server`

Virtuelle Netzwerke

Bezeichnung	Feldname	Datenbeschreibung	Gespeichert in Tabelle
Name	Name	Name des virtuellen Netzwerks	`CMDB_CI_Hyper_v_Netzwerk` *
ID	object_id	Global eindeutiger Bezeichner (GUID)	`CMDB_CI_Hyper_v_Netzwerk` *

*Attribute, die zur Tabelle `cmdb_ci_hyper_v_network` hinzugefügt werden, wenn das Muster „Hyper-V Server“ verwendet wird. Für Upgrades fügen Probes und Sensoren diese Attribute weiterhin den Tabellen `cmdb_ci` (name) und `cmdb_ci_vm_object` (object_id) hinzu.

Ressourcenpools

Bezeichnung	Feldname	Datenbeschreibung	Gespeichert in Tabelle
Name^	Name	Name des Ressourcenpools	`cmdb_ci_hyper_v_resource_pool`
ID	object_id	Global eindeutiger Bezeichner (GUID)	`cmdb_ci_hyper_v_rpool_comp`
Kapazität	Kapazität	Maximaler Betrag der entsprechenden Zuteilungseinheit	`cmdb_ci_hyper_v_rpool_comp`
Zuordnungseinheiten	allocation_units	Verwendete Maßeinheiten (zum Beispiel MB oder GB)	`cmdb_ci_hyper_v_rpool_comp`
Ressourcentyp	resource_type	Typ der erkannten Ressource (zum Beispiel Arbeitsspeicher oder Festplattenspeicher)	`cmdb_ci_hyper_v_rpool_comp`

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

Cluster

Bezeichnung	Feldname	Datenbeschreibung	Gespeichert in Tabelle	Referenztabelle
Windows-Cluster	Name	Referenzfeld, in dem das Windows-Cluster angezeigt wird, in dem sich das Hyper-V-Cluster befindet	`cmdb_ci_hyper_v_cluster`	`cmdb_ci_win_cluster`

Beziehungen

Discovery erstellt Datensätze in CMDB für den Hostcomputer, die übergeordnete Partition, auf der Windows Server 2008 ausgeführt wird, und alle virtuellen Computer, die auf dem Hyper-V-Server ausgeführt werden. Discovery findet die gespeicherten Vorlagen und ordnet alle Beziehungen zwischen Komponenten zu.

Die Instanz ändert die folgenden Tabellen, damit sie für mehrere Virtualisierungsprodukte verwendet werden können:

Tabelle	Zweck
Virtualisierungsserver [cmdb_ci_virtualization_server]	Enthält Daten über alle erkannte Virtualisierungsserver
VM-Instanz [cmdb_ci_vm_instance]	Enthält Daten über alle erkannte Instanzen virtueller Computer
VM-Objekt [cmdb_ci_vm_object]	Enthält Daten über verschiedene Objekte, die einem Hyper-V-Server zugeordnet sind, zum Beispiel Partitionen, Netzwerke, Ressourcenpools und Cluster

Übergeordnete Tabelle	Beziehung	Untergeordnete Tabelle
Hyper-V-VM-Instanz [cmdb_ci_hyper_v_instance]	Registriert auf::Hat sich registriert	Hyper-V-Server [cmdb_ci_hyper_v_server]
Hyper-V-VM-Instanz [cmdb_ci_hyper_v_instance]	Verbunden von::Verbindet	Hyper-V-Netzwerk [cmdb_ci_hyper_v_network]
Hyper-V-Netzwerk [cmdb_ci_hyper_v_network]	Bereitgestellt::Stellt bereit	Hyper-V-Server [cmdb_ci_hyper_v_server]
Hyper-V-Ressourcenpool [cmdb_ci_hyper_v_resource_pool]	Definiert Ressourcen für:Erhält Ressourcen von	Hyper-V-Server [cmdb_ci_hyper_v_server]
Hyper-V-Ressourcenpoolkomponenten [cmdb_ci_hyper_v_resource_pool]	Enthalten in::Enthält	Hyper-V-Ressourcenpool [cmdb_ci_hyper_v_resource_pool]

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

Übergeordnete Tabelle	Beziehung	Untergeordnete Tabelle
Hyper-V-Cluster [cmdb_ci_hyper_v_cluster]	Mitglieder::Mitglied von	Hyper-V-Server [cmdb_ci_hyper_v_server]
Hyper-V-Server [cmdb_ci_hyper_v_server]	Wird ausgeführt auf::Wird ausgeführt	Windows-Server [cmdb_ci_win_server]
Windows-Server [cmdb_ci_win_server]	Instanziiert::Instanziiert von	Hyper-V-VM-Instanz [cmdb_ci_hyper_v_instance]
Windows-Server [cmdb_ci_win_server]	Virtualisiert von::Virtualisiert	Hyper-V-Server [cmdb_ci_hyper_v_server]

Virtuelle Hyper-V-Computer klonen

Stellen Sie beim Importieren (Klonen) von virtuellen Hyper-V-Computern sicher, dass jeder virtuelle Computer eine eindeutige ID aufweist. Discovery identifiziert virtuelle Computer mit identischen IDs als denselben Computer.

1. Exportieren Sie den virtuellen Computer vom Hyper-V-Server.
2. Importieren Sie den virtuellen Computer auf einen anderen Server, und wählen Sie eine der folgenden Optionen aus:
   - Move or restore the virtual machine (Virtuellen Computer verschieben oder wiederherstellen): Bei Auswahl dieser Option wird das Image mit derselben ID geklont und auf einen anderen Server verschoben. Das Original-Image bleibt auf dem Hyper-V-Server.
   - Copy the virtual machine (Virtuellen Computer kopieren): Bei Auswahl dieser Option wird der virtuelle Computer mit einer anderen ID kopiert und vom Hyper-V-Server verschoben. Das ist die beste Auswahl. Sie erfordert vor Ausführung von Discovery keine weitere Aktion.
3. Wenn Sie den Hyper-V-Klon mit der Option zum **Verschieben oder Wiederherstellen** importieren, müssen Sie das Original-Image vom Hyper-V-Server löschen.

   Wenn Discovery auf zwei virtuelle Computer mit denselben äquivalenten Seriennummern trifft, wird nur ein Konfigurationselement (CI) erstellt.

Erkennung von Red Hat JBoss-Servern

Discovery kann JBoss-Anwendungsserver erkennen, die unter Linux und Windows ausgeführt werden.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Anforderungen

Für JBoss-Anwendungsserver, die unter Linux ausgeführt werden:

- Legen Sie Probe-Berechtigungen zur Verwendung der folgenden Befehle der Bourne-Shell fest: *find*, *cat* und *dirname*.
- Aktivieren Sie SSH auf dem JBoss-Anwendungsserver. Die SSH-Anmeldeinformationen müssen auch Leseberechtigungen für die Dateien `web.xml` und `jboss-service.xml` beinhalten.

Aktivieren Sie für JBoss-Anwendungsserver, die unter Windows ausgeführt werden, PowerShell auf dem MID Server.

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

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Anmeldeinformationen

- Applicative-Anmeldeinformationen
- Windows-Anmeldeinformationen
- SSH-Anmeldeinformationen

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
JBoss-Server	• Horizontal Pattern: Startet Muster • Windows - JBoss Find web.xml List* • Windows - JBoss Get jboss-service.xml* • JBoss - Find web.xml List* • JBoss - Get jboss-service.xml*	JBoss

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Discovery füllt in der JBoss-Tabelle [cmdb_ci_app_server_jboss] die folgenden Felder:

Bezeichnung	Feldname
Name	Name
Kategorie	Kategorie
Version	Version
TCP-Port(s)	tcp_port

Discovery füllt in den Servertabellen für Webservices [cmdb_ci_web_service] und Webanwendungen [cmdb_ci_web_application] die folgenden Felder:

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

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_web_service	Name	jboss-service.xml
App-Server	cmdb_ci_web_service	app_server	Interne Referenz
Beschreibung	cmdb_ci_web_application	short_description	web.xml
Name	cmdb_ci_web_application	Name	web.xml
Dokumentenbasis	cmdb_ci_web_application	document_base	web.xml
App-Server	cmdb_ci_web_application	app_server	web.xml
Servlet-Name*	cmdb_ci_web_application	servlet_name	web.xml
Servlet-Klasse*	cmdb_ci_web_application	servlet_class	web.xml

*Nur Windows-Server

Beziehungen

Erstellte Beziehungen

Übergeordnete Klasse	Beziehung	Untergeordnete Klasse
cmdb_ci_web_service	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_windows_server
cmdb_ci_app_server_jboss	Enthält::Enthalten in	cmdb_ci_web_application
cmdb_ci_app_server_jboss	Wird ausgeführt:Wird ausgeführt auf	cmdb_ci_web_application
cmdb_ci_app_server_jboss	Wird ausgeführt:Wird ausgeführt auf	cmdb_ci_web_service

Veraltet: JBoss-Probes und -Sensoren

Discovery identifiziert einen Linux JBoss-Anwendungsserver mithilfe von Probes und Sensoren.

Linux

Dieser Prozess beschreibt die Verwendung von Probes, die bei einem Upgrade in Ihrer Instanz aktiv sind. Für neue Instanzen verwendet Discovery das Muster JBoss.

1. Die Probe „UNIX - Active Processes“ erkennt einen laufenden Prozess, der dem Einstiegspunktparameter *`org.jboss.main`* entspricht.
2. Bei einer Übereinstimmung wird ein Datensatz in der Tabelle „JBoss-Anwendungsserver“ [cmdb_ci_app_server_jboss] erstellt. Die folgenden Sonden werden ebenfalls aktiviert:
   - JBoss - Find web.xml list: Der Sensor dieses Tests füllt gegebenenfalls Informationen in die Tabelle der Webanwendung [cmdb_ci_web_application].
   - JBoss - jboss-service.xml abrufen: Der Sensor dieses Tests füllt die Informationen in der Tabelle "Web Service [cmdb_ci_web_service]" auf.
3. Der JBoss - Find web.xml Listentest sucht nach dem `web.xml`-Dateien des JBoss-Anwendungsservers. Von der Probe wird der Parameter *`classpath`* im ausgeführten Prozess verwendet. Dann wird im zugehörigen Verzeichnis `server\default\deploy` nach der JBoss-Installation gesucht.

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

4. Wenn sich zugehörige Webanwendungen im Verzeichnis `server\default\deploy` befinden, wird die Sonde JBoss - Get web.xml für jede Anwendung ausgelöst. Diese Sonde liest die `web.xml`-Datei für jede Webanwendung und der Sensor füllt zusätzliche Informationen in die Tabelle Web Service [cmdb_ci_web_service].
5. Von der Probe „Boss - Get jboss-service.xml“ wird der Parameter *`classpath`* im ausgeführten Prozess zum Suchen nach der `jboss-service.xml` -Datei im zugehörigen Verzeichnis `server\default\conf\` für die JBoss-Installation verwendet.
6. Wenn die Sonde die Datei `jboss-service.xml` im Verzeichnis `server\default\conf\` gefunden hat, liest der Sensor den Inhalt der XML-Datei. Anschließend erstellt er bei Bedarf zusätzliche Datensätze in der Tabelle Web Service [cmdb_ci_web_service].

Windows

Dieser Prozess beschreibt die Verwendung von Probes, die bei einem Upgrade in Ihrer Instanz aktiv sind. Für neue Instanzen verwendet Discovery das Muster JBoss.

1. Die Probe „Windows - Active Processes“ erkennt einen laufenden Prozess, der dem Einstiegspunktparameter *`org.jboss.main`* entspricht.
2. Bei einer Übereinstimmung wird ein Datensatz in der Tabelle „JBoss-Anwendungsserver“ [cmdb_ci_app_server_jboss] erstellt. Die folgenden Sonden werden ebenfalls aktiviert:
   - JBoss - Find web.xml list: Der Sensor dieses Tests füllt gegebenenfalls Informationen in die Tabelle der Webanwendung [cmdb_ci_web_application].
   - JBoss - jboss-service.xml abrufen: Der Sensor dieses Tests füllt die Informationen in der Tabelle "Web Service [cmdb_ci_web_service]" auf.
3. Der JBoss - Find web.xml Listentest sucht nach dem `web.xml`-Dateien des JBoss-Anwendungsservers. Von der Probe wird der Parameter *`classpath`* im ausgeführten Prozess verwendet. Dann wird im zugehörigen Verzeichnis `server\default\deploy` nach der JBoss-Installation gesucht.
4. Wenn sich zugehörige Webanwendungen im Verzeichnis `server\default\deploy` befinden, wird die Sonde JBoss - Get web.xml für jede Anwendung ausgelöst. Diese Sonde liest die `web.xml`-Datei für jede Webanwendung und der Sensor füllt zusätzliche Informationen in die Tabelle Web Service [cmdb_ci_web_service].
5. Von der Probe „Boss - Get jboss-service.xml“ wird der Parameter *`classpath`* im ausgeführten Prozess zum Suchen nach der `jboss-service.xml` -Datei im zugehörigen Verzeichnis `server\default\conf\` für die JBoss-Installation verwendet.
6. Wenn die Sonde die Datei `jboss-service.xml` im Verzeichnis `server\default\conf\` gefunden hat, liest der Sensor den Inhalt der XML-Datei. Anschließend erstellt er bei Bedarf zusätzliche Datensätze in der Tabelle Web Service [cmdb_ci_web_service].

Linux Discovery

Discovery identifiziert und klassifiziert Informationen über Computer Linux, die IPv4-Adressen und/oder IPv6-Adressen verwenden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Hinweis: Das Servermuster Linux kann nur Linuxin englischer Sprache erkennen.

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

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Unterstützte Linux Betriebssysteme

Für IPv4-Erkennung:

- Red Hat
- Fedora
- Debian
- SUSE
- CentOS
- Ubuntu

Für IPv6-Erkennung:

- CentOS 7
- Ubuntu 20

Einschränkungen der IPv6-Unterstützung

Die folgenden Betriebssysteme oder Geräte wurden für die IPv6-Erkennung nicht verifiziert:

- Red Hat-Cluster
- Oracle Clusterware
- Linux Pacemaker-Cluster
- Netzwerkspeicher

Erforderliche Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen. Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Mehrere IP-Adressen, die Netzwerkadaptern zugeordnet sind

Wenn Ihrer Umgebung mehrere IP-Adressen zugeordnet sind, die Netzwerkadaptern zugeordnet sind, können Sie die Eigenschaft `network_adapter_exclusion_list` verwenden, um die Erkennung Linux von auf bestimmte Netzwerkadapter und deren primäre IP-Adressen zu beschränken. Dadurch wird sichergestellt, dass nur die angegebenen Netzwerkadapter und ihre primären IP-Adressen während der Erkennung Linux von verwendet werden. Discovery sucht oder erstellt keine Beziehungen für sekundäre IP-Adressen, die nicht aufgeführt sind. Weitere Informationen finden Sie unter Sekundäre IP-Adressen des Netzwerkadapters in Discovery Linux auslassen.

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

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
Linux (Unix-Klassifizierung)	• Probe „Horizontal Discovery“: Startet Muster • Linux - Installed Software^ • Unix - ADM^ • Linux - Identity* • Linux - CPU* • Linux - Distribution* • Linux - Find FQDN* • Linux - Memory* • Linux - Memory Modules* • Linux - Network ARP Tables* • Linux - Storage* • Linux - Amazon EC2* • Unix - OS Uptime* • UNIX - OS Filesystems* • UNIX - Find FQDN* • Unix - ADM Enhanced*	Linux Server

*Diese Probes sind für die Klassifizierung nicht aktiv, da Discovery standardmäßig Muster für diese Erkennungen verwendet.

^Diese Probes bleiben standardmäßig aktiv, auch wenn Discovery die Muster-Discovery verwendet.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Der Klassifizierer **Linux** löst Probes aus, die die Erkennung ausführen. Während der Erkennung werden mehrere Proben gestartet. Eine Liste der ausgelösten Probes finden Sie unter dem Klassifizierer.

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Bezeichnung	Tabellenname	Feldname	Quelle
Betriebssystem	cmdb_ci_linux_server	os	uname -a
BS-Version	cmdb_ci_computer	os_version	uname -a or cat /etc/*release

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

Bezeichnung	Tabellenname	Feldname	Quelle
Kurzbeschreibung	cmdb_ci_linux_server	short_description	uname -a
Name	cmdb_ci_linux_server	Name	DNS, NBT
Hostname	cmdb_ci_linux_server	host_name	DNS, NBT
DNS-Domäne	cmdb_ci_linux_server	dns_domain	DNS
Startdatum	cmdb_ci_linux_server	start_date	uptime
Hersteller	cmdb_ci_computer	manufacturer	dmidecode
Seriennummer	cmdb_ci_computer	serial_number	dmidecode
CPU-Typ	cmdb_ci_linux_server	cpu_type	/proc/cpuinfo
CPU-Geschwindigkeit (MHz)	cmdb_ci_linux_server	cpu_speed	/proc/cpuinfo
CPU-Anzahl	cmdb_ci_linux_server	cpu_count	/proc/cpuinfo
Anzahl CPU-Kerne	cmdb_ci_computer	cpu_core_count	/proc/cpuinfo
CPU-Kern-Thread	cmdb_ci_computer	cpu_core_thread	/proc/cpuinfo
CPU-Hersteller	cmdb_ci_linux_server	cpu_manufacturer	/proc/cpuinfo
Modellnummer	cmdb_ci_computer	model_number	dmidecode
Modell-ID	cmdb_ci_computer	model_id	dmidecode
RAM (MB)	cmdb_ci_linux_server	ram	meminfo
Festplattenspeicher (GB)*	cmdb_ci_linux_server	disk_space	/proc/ide, /proc/scsi, /var/log/dmesg
Typ	cmdb_ci_disk	Typ	/proc/ide, /proc/scsi, /var/log/dmesg
Modell-ID	cmdb_ci_disk	model_id	/proc/ide, /proc/scsi, /var/log/dmesg
Festplattenspeicher (GB)	cmdb_ci_disk	disk_space	/proc/ide, /proc/scsi, /var/log/dmesg
Name	cmdb_ci_disk	Name	/proc/ide, /proc/scsi, /var/log/dmesg
Name	cmdb_ci_file_system	Name	df
Kapazität (MB)	cmdb_ci_file_system	Kapazität	df
Freier Speicherplatz in Byte (MB)	cmdb_ci_file_system	free_space_bytes	df
Bereitstellungspunkt	cmdb_ci_file_system	mount_point	df
Name	cmdb_running_process	Name	ps
Befehl	cmdb_running_process	command	ps
Typ	cmdb_running_process	Typ	ps
PID	cmdb_running_process	pid	ps
Parameter	cmdb_running_process	parameters	ps

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

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_network_adapter	Name	ifconfig oder ip address show
IP-Adresse	cmdb_ci_network_adapter	ip_address	ifconfig oder ip address show
MAC-Adresse	cmdb_ci_network_adapter	mac_address	ifconfig oder ip address show
Netzmaske	cmdb_ci_network_adapter	netmask	ifconfig oder ip address show
Standard-Gateway	cmdb_ci_hardware	default_gateway	route

* Der Wert im Feld **disk_space** ist eine Zusammenfassung der Gesamtkapazität (einschließlich belegtem Platz) für alle nicht entnehmbaren Festplatten, einschließlich Direct Attached Storage und SAN-Speicher.

Hinweis: Achten Sie darauf, eindeutige Seriennummern für die RAMs auf dem Server Linux zu definieren.

Discovery identifiziert und klassifiziert auch Informationen über Linux KVM. Discovery

identifiziert Kernel-basierte virtuelle Maschinen (KVM) Linux, wenn die Prozessklassifizierung erkennt, dass *libvirtd* auf einem Server Linux ausgeführt wird. Die Klassifizierung löst die Erstellung eines cmdb_ci_kvm-Datensatzes aus und startet die SSH-Befehlsprobes, um den Server Linux mit *Virsh*, dem Dienstprogramm *„libvert"* und den Konfigurationsdaten der virtuellen Maschine zu untersuchen.

Discovery erstellt einen [cmdb_ci_kvm_instance]-Datensatz für jede virtuelle Maschine auf dem Server und gleicht dann den [cmdb_ci_kvm_instance]-Datensatz anhand der MAC-Adressen der installierten Netzwerkadapter mit einem entsprechenden [cmdb_ci_computer]-Datensatz ab.

Von Discovery auf Linux KVM verwendete Tabellen

Tabellenname	Erweitert	Beschreibung	Quelle
cmdb_ci_kvm	cmdb_ci_vm	Ein Hypervisor, der Kernel-basierte virtuelle Computer (KVMs) verwaltet	Prozessklassifizierer erkennt libvirtd, das auf Linux-Servern ausgeführt wird
cmdb_ci_kvm_vm_instance	cmdb_ci_vm_instance	Eine VM-Instanz für diesen Hypervisor	Virsh-Befehl „list-all" und „dumpxml".
cmdb_ci_kvm_object	cmdb_ci_vm_object	Ein Objekt, das mit einer VM-Instanz verbunden ist	Elemente <network> , <storage pool> und <storage volume> des dumpxml-Befehls
cmdb_kvm_device	Nicht zutreffend	Ein Gerät, das mit einer VM-Instanz verbunden ist	Element <devices> des dumpxml-Befehls

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

Von Discovery auf Linux KVM gesammelte Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Linux-Host	cmdb_ci_kvm	linux_host	Verweis auf den cmdb_ci_linux_server, auf dem diese VM ausgeführt wird
Details	cmdb_ci_kvm	details_xml	dumpxml
Objekt-ID	cmdb_ci_kvm_vm_instance	object_id	virsh dumpxml
Status	cmdb_ci_kvm_vm_instance	state	Virsh-Liste – Alle
CPUs	cmdb_ci_kvm_vm_instance	CPUs	virsh dumpxml
Arbeitsspeicher	cmdb_ci_kvm_vm_instance	memory	virsh dumpxml
Datenträger	cmdb_ci_kvm_vm_instance	disks	virsh dumpxml
Datenträgergröße	cmdb_ci_kvm_vm_instance	disks_size	virsh domblkinfo
Netzwerkadapter	cmdb_ci_kvm_vm_instance	nics	virsh dumpxml
Name	cmdb_ci_kvm_vm_instance	Name	virsh dumpxml
Kurzbeschreibung	cmdb_ci_kvm_vm_instance	short_description	virsh desc
Details	cmdb_ci_kvm_object	details_xml	XML-Element aus dumpxml
KVM-Instanz	cmdb_kvm_device	kvm_instance	Verweis auf cmdb_ci_kvm_instance
Gerät	cmdb_kvm_device	Gerät	Datenträger, Controller, Schnittstelle usw
Typ	cmdb_kvm_device	Typ	hängt vom Gerät ab
Details	cmdb_kvm_device	details_xml	XML-Element aus dumpxml

Von Discovery über die KVM-Beziehung erfasste Daten

Beziehung	Übergeordnete Tabelle	Untergeordnete Tabelle
Registriert auf::Hat sich registriert	KVM [cmdb_ci_kvm]	Instanz der virtuellen KVM-Maschine [cmdb_ci_kvm_vm_instance]
Bereitgestellt von::Stellt bereit	KVM [cmdb_ci_kvm]	Netzwerk [cmdb_ci_kvm_network]
Definiert Ressourcen für:Erhält Ressourcen von	KVM [cmdb_ci_kvm]	Speicherpool [cmdb_ci_kvm_storage_pool]
Verbunden von::Verbindet	Instanz der virtuellen KVM-Maschine [cmdb_ci_kvm_vm_instance]	Netzwerk [cmdb_ci_kvm_network]

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

Von Discovery über die KVM-Beziehung erfasste Daten (Fortsetzung)

Beziehung	Übergeordnete Tabelle	Untergeordnete Tabelle
Instanziiert von::Instanziiert	Instanz der virtuellen KVM-Maschine [cmdb_ci_kvm_vm_instance]	Computer [cmdb_ci_computer]
Virtualisiert von::Virtualisiert	Computer [cmdb_ci_computer]	KVM [cmdb_ci_kvm]
Stellt Speicher bereit für::Gespeichert auf	Speicherpool [cmdb_ci_kvm_storage_pool]	Instanz der virtuellen KVM-Maschine [cmdb_ci_kvm_vm_instance]

Zugehörige Informationen

Erkennung von Linux Red Hat-Clustern

Sekundäre IP-Adressen des Netzwerkadapters in Discovery Linux auslassen

Erkennung von Linux Red Hat-Clustern

Discovery kann Linux Red Hat-Cluster erkennen, die hohe Verfügbarkeit und Lastenausgleich bieten.

Erforderliche Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen .

Zusätzliche Anforderungen

Sie benötigen außerdem Berechtigungen zum Lesen des Verzeichnisses `/etc/hosts/` und der Datei `/etc/cluster/cluster.conf`, die Hostnamen mit IP-Adressen verknüpft.

Die folgenden Befehle werden für Oracle-Clusterware ausgeführt:

Befehl
`ps -ef | grep-corosync | grep -v grep`
`clustat -x`
`ifconfig | grep 'inet addr:' |awk '{print $1, $2 }'`
`hostname -s`
`hostname -s`

Sudo-Berechtigung zur Ausführung: `sudo /u01/app/12.1.0.2/grid/bin/ocrcheck \| egrep -v 'error\|return code'`

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

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
Linux (Unix-Klassifizierung)	Probe „Horizontal Discovery“: Startet Muster	Die folgenden Muster stellen eine Erweiterung des Musters Linux Server dar: • UNIX-Cluster – Linux Red Hat-Cluster • Linux – Red Hat-Cluster Das Muster verwendet den Befehl `clustat -x` und untersucht die folgende Clusterkonfigurationsdatei: `/etc/cluster/cluster.conf`

Erfasste Daten

Tabelle	Bezeichnungen und Feldnamen
Unix-Cluster [cmdb_ci_unix_cluster]	Name [name] Clusterstatus [cluster_status] Clustertyp [cluster_type] IP-Adresse [ip_address] Cluster-ID [cluster_id] Clusterversion [cluster_version]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Name [name] Knotenzustand [node_state] IP-Adresse [ip_address] Knotenstatus [node_status]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Name [name] Ressourcentyp [resource_type] Ressourcenstatus [resource_status] Eigenschaften [properties]
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	Name [name]

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

Tabelle	Bezeichnungen und Feldnamen
	IP-Adresse [ip_address] Cluster-ID [cluster_id]

Beziehungen

CI	Beziehung	CI
Unix-Cluster [cmdb_ci_unix_cluster]	Virtualisiert::Virtualisiert von	Virtuelle Cluster-IP [cmdb_ci_cluster_vip]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	Verwendet::Verwendet von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Cluster von::Cluster	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Gehostet auf::Hostet	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Cluster [cmdb_ci_unix_cluster]	Hostet::Gehostet auf	Linux-Server [cmdb_ci_linux_server]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Gehostet auf::Hostet	Linux-Server [cmdb_ci_linux_server]

Sekundäre IP-Adressen des Netzwerkadapters in Discovery Linux auslassen

Beschränken Sie die Discovery Linux von auf bestimmte Netzwerkadapter und deren primäre IP-Adressen, um die Leistung zu verbessern, indem Sie sekundäre IP-Adressen ignorieren.

Warum und wann dieser Vorgang ausgeführt wird

Durch die Konfiguration der Systemeigenschaft *network_adapter_exclusion_list* wird sichergestellt, dass bei der Erkennung Linux von nur die angegebenen Netzwerkadapter und ihre primären IP-Adressen verwendet werden. Sekundäre IP-Adressen, die nicht benannt sind, werden automatisch ausgelassen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein.
2. Suchen Sie im Feld **Name** nach `network_adapter_exclusion_list`.
3. Wählen Sie die Eigenschaft *network_adapter_exclusion_list* aus.
4. Geben Sie im Feld **Wert** den Netzwerkadapter ein, der der NIC-IP-Adresse zugeordnet ist, um ihn vom Löschen auszuschließen.

   Der Netzwerkadapter muss in einem der in der folgenden Tabelle aufgeführten Formate eingegeben werden.

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

Format	Beschreibung
Einzelname	Einzelner Adaptername. Beispiel: `Bond0`.
Regulärer Ausdruck, der mehreren Adapternamen entspricht	Regulärer Ausdruck, der mehreren Adapternamen entspricht, die mit einer oder mehreren Ziffern enden. Beispiel: `Bond\d+`.
Mehrere Adapternamen	Mehrere Adapternamen, durch Kommas getrennt, einschließlich regulärem Ausdruck. Beispiel: `nic1,bond\d+`.

5. Wählen Sie **Aktualisieren**.

Ergebnisse

Wenn der vordefinierte Zeitplan die Discovery des Servers Linux auslöst oder eine geplante horizontale Discovery ausgeführt wird, werden nur die spezifischen Netzwerkadapter und ihre primären IP-Adressen in den Discovery-Prozess einbezogen.

Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Zugehörige Informationen

Linux Discovery

Netware-Erkennung

Discovery identifiziert und klassifiziert Informationen über Netware.

Erfasste Daten

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_netware_server	Name	snmp
Seriennummer	cmdb_ci_netware_server	serial_number	snmp
BS-Version	cmdb_ci_netware_server	os_version	snmp
RAM	cmdb_ci_netware_server	ram	snmp
CPU-Anzahl	cmdb_ci_netware_server	cpu_count	snmp

Erkennung von OS/X (Mac)

Discovery identifiziert und klassifiziert Informationen über Mac (OS/X)-Computer.

Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen .

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

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

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Erfasste Daten

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Bezeichnung	Tabellenname	Feldname	Quelle
Betriebssystem	cmdb_ci_computer	os	uname
BS-Version	cmdb_ci_computer	os_version	system_profiler
BS-Service Pack	cmdb_ci_computer	os_service_pack	system_profiler
Kurzbeschreibung	cmdb_ci_computer	short_description	uname
Name	cmdb_ci_computer	Name	DNS, NBT
Hostname	cmdb_ci_computer	host_name	DNS, NBT
DNS-Domäne	cmdb_ci_computer	dns_domain	DNS
Startdatum	cmdb_ci_computer	start_date	uptime
Hersteller	cmdb_ci_computer	manufacturer	Vermutlich Apple
Seriennummer	cmdb_ci_computer	serial_number	system_profiler
CPU-Typ	cmdb_ci_computer	cpu_type	system_profiler
CPU-Geschwindigkeit (MHz)	cmdb_ci_computer	cpu_speed	system_profiler
CPU-Anzahl	cmdb_ci_computer	cpu_count	system_profiler
Modell-ID	cmdb_ci_computer	model_id	system_profiler
RAM (MB)	cmdb_ci_computer	ram	system_profiler
Festplattenspeicher (GB)	cmdb_ci_computer	disk_space	system_profiler
Volume-Name	cmdb_ci_disk	volume_name	system_profiler
Volume-Seriennummer	cmdb_ci_disk	volume_serial_number	system_profiler
Festplattenspeicher (GB)	cmdb_ci_disk	disk_space	system_profiler
Name	cmdb_ci_disk	Name	system_profiler
Geräte-ID	cmdb_ci_disk	device_id	system_profiler
Freier Speicherplatz (GB)	cmdb_ci_disk	free_space	system_profiler
Dateisystem	cmdb_ci_disk	file_system	system_profiler
Name	cmdb_running_process	Name	ps
Befehl	cmdb_running_process	command	ps
Verbunden mit	cmdb_running_process	connects_to	lsof

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

Bezeichnung	Tabellenname	Feldname	Quelle
Lauschen auf	cmdb_running_process	listening_on	lsof
PID	cmdb_running_process	pid	ps
Parameter	cmdb_running_process	parameters	ps
Name	cmdb_ci_network_adapter	Name	system_profiler
IP-Adresse	cmdb_ci_network_adapter	ip_address	system_profiler
MAC-Adresse	cmdb_ci_network_adapter	mac_address	system_profiler
Netzmaske	cmdb_ci_network_adapter	netmask	system_profiler
MAC-Hersteller	cmdb_ci_network_adapter	mac_mfr	Vermutlich Apple
DHCP-fähig	cmdb_ci_network_adapter	dhcp_enabled	system_profiler

Solaris-Erkennung

Discovery identifiziert und klassifiziert Informationen über Solaris-Computer.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Unterstützte Betriebssysteme

- Oracle Solaris 10
- Oracle Solaris 11

Voraussetzungen

Discovery speichert Daten in der Tabelle [cmdb_running_process] mit Befehlszeilenparametern, die auf maximal 80 Zeichen beschnitten sind. Das kann dazu führen, dass mehrere Anwendungen in einem CI zusammengeführt werden. Um die vollständige Befehlszeile zu erhalten und dieses Problem zu vermeiden, führen Sie `pargs -a` aus, und analysieren Sie das Ergebnis.

Damit Discovery Muster für die Suche nach Solaris-Computern verwendet, müssen Sie SNEEP installieren. Andernfalls kann Discovery die Seriennummer nicht finden.

Bei Verwendung von Solaris-Zonen muss jede Zone so konfiguriert werden, dass sie einen eindeutigen Wert für die Seriennummer zurückgibt. Andernfalls gibt jede Zone dieselbe Nummer zurück, wodurch Probleme bei der CI-Identifizierung entstehen.

Hinweis: Die Solaris-Discovery unterstützt nur lokale Zonen, die auf dem gleichen Host wie die globale Zone installiert sind. Wenn die lokale Zone auf einem anderen Host als die globale Zone installiert ist, ruft der Befehl `zoneadm list -cip` den UUID für die lokale Zone nicht ab.

Die Probe „Solaris - ADM“ erfordert die Installation des LSQF-Befehls.

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen für die zu erkennenden Systeme.

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

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Klassifizierer, Probes und Muster

Klassifizierung	Probes	Muster
Solaris (UNIX-Klassifizierung)	• Probe „Horizontal Discovery“: Startet Muster • Solaris - Installed Software^ • Solaris - Identity* • Solaris - CPU* • Solaris - Hardware Model* • Solaris - Memory* • Solaris - Network ARP Tables* • Solaris - OS Patches* • Solaris - Storage* • Solaris - Zones* • Solaris - Disks* • DNS*	Solaris-Server

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

^Diese Probe bleibt standardmäßig aktiv, selbst wenn Discovery die Mustererkennung verwendet.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Betriebssystem	cmdb_ci_computer	os	uname
Kurzbeschreibung	cmdb_ci_solaris_server	short_description	uname
Name	cmdb_ci_solaris_server	Name	DNS, NBT
Hostname	cmdb_ci_solaris_server	host_name	DNS, NBT
DNS-Domäne	cmdb_ci_solaris_server	dns_domain	DNS
Startdatum	cmdb_ci_solaris_server	start_date	uptime

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

Bezeichnung	Tabellenname	Feldname	Quelle
CPU-Typ	cmdb_ci_computer	cpu_type	kstat
CPU-Geschwindigkeit (MHz)	cmdb_ci_computer	cpu_speed	kstat
CPU-Anzahl	cmdb_ci_computer	cpu_count	kstat
Anzahl CPU-Kerne	cmdb_ci_computer	cpu_core_count	kstat
CPU-Kern-Thread	cmdb_ci_computer	cpu_core_thread	kstat
Modellnummer	cmdb_ci_solaris_server	model_number	suntype
Modell-ID	cmdb_ci_solaris_server	model_id	suntype
RAM (MB)	cmdb_ci_computer	ram	prtconf
Festplattenspeicher (GB)	cmdb_ci_solaris_server	disk_space	iostat
Seriennummer	cmdb_ci_solaris_server	serial_number	sneep *
Hersteller	cmdb_ci_disk	manufacturer	iostat
Modell-ID	cmdb_ci_disk	model_id	iostat
Volume-Seriennummer	cmdb_ci_disk	volume_serial_number	iostat
Festplattenspeicher (GB)	cmdb_ci_disk	disk_space	iostat
Name	cmdb_ci_disk	Name	iostat
Name	cmdb_ci_file_system	Name	df
Kapazität (MB)	cmdb_ci_file_system	Kapazität	df
Verfügbarer Speicherplatz (MB)	cmdb_ci_file_system	available_space	df
Bereitstellungspunkt	cmdb_ci_file_system	mount_point	df
Name	cmdb_ci_patches	Name	showrev
Name	cmdb_running_process	Name	ps
Befehl	cmdb_running_process	command	ps
Verbunden mit	cmdb_running_process	connects_to	lsof
Lauschen auf	cmdb_running_process	listening_on	lsof
Typ	cmdb_running_process	Typ	ps
PID	cmdb_running_process	pid	ps
Parameter	cmdb_running_process	parameters	ps
Name	cmdb_ci_network_adapter	Name	ifconfig
IP-Adresse	cmdb_ci_network_adapter	ip_address	ifconfig
MAC-Adresse	cmdb_ci_network_adapter	mac_address	ifconfig
Netzmaske	cmdb_ci_network_adapter	netmask	ifconfig
Standard-Gateway	cmdb_ci_hardware	default_gateway	netstat

* Zum Erkennen von Fujitsu PRIMEPOWER-Geräten müssen Sie Oracle SNEEP installieren und die Solaris-Erkennung mit Root-Anmeldeinformationen ausführen.

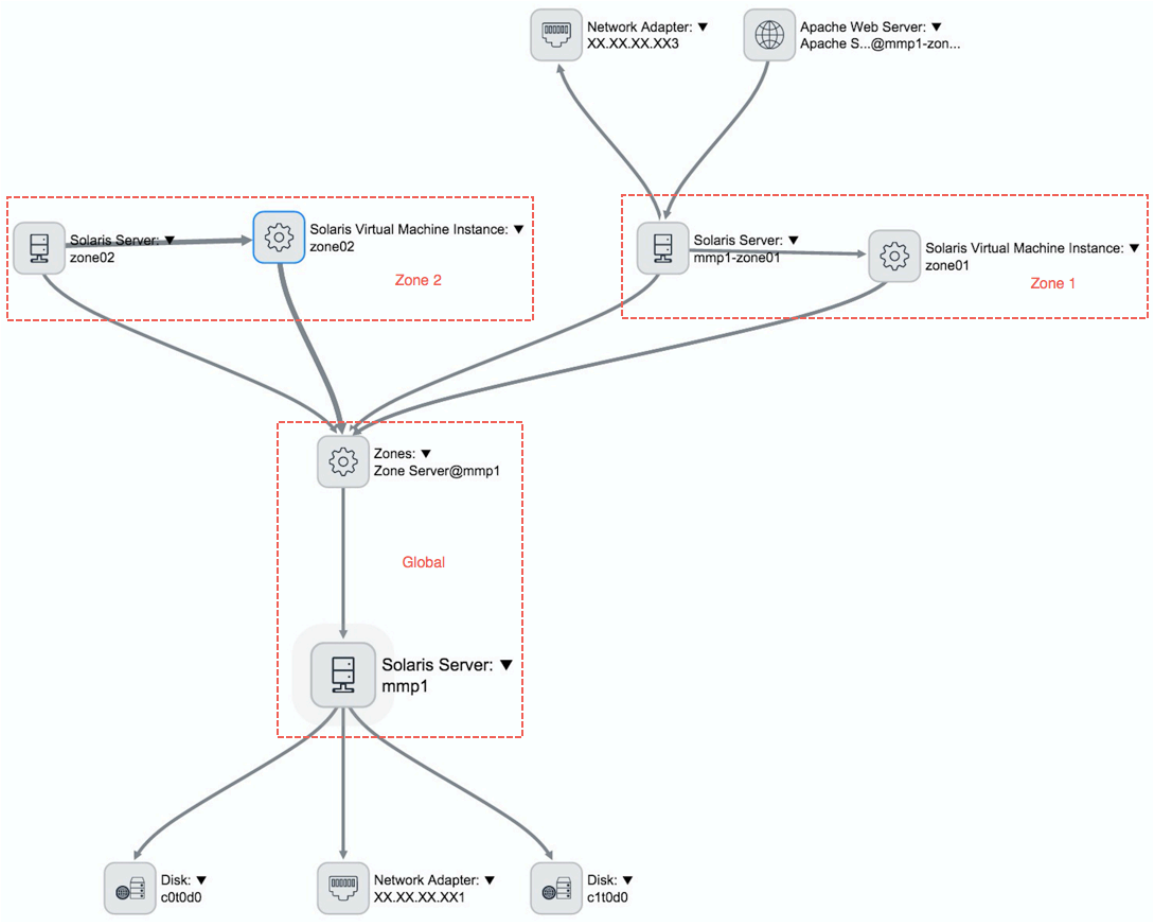
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Erkennung von Solaris-Zonen

Bei der Erkennung ordnet Discovery die Beziehungen zwischen globalen und lokalen Solaris-Zonen zu.

Im folgenden Beispiel enthält eine globale Solaris-Zone zwei lokale Zonen: zone01 und zone02. Jede lokale Zone wird durch einen physischen Solaris-CI-Datensatz und einen VM-Instanzdatensatz dargestellt. Jede der lokalen Zonen ist an einen Zonenserver gebunden, wodurch die Beziehung zwischen Virtualisierung und globaler Zone (mmp1) verdeutlicht wird.

Zuordnung der Solaris-Zonenbeziehungen



Die TCP-Verbindungs- und -Prozessinformationen für lokale Zonenserver müssen durch Ausführung von Befehlen in ihrer übergeordneten globalen Zone erfasst werden. Der Beziehungspfad zwischen den physischen Computern der lokalen und globalen Zone muss festgelegt werden, bevor TCP-Verbindungs- und -Prozessinformationen für lokale Zonenserver erfasst werden können.

Fall 1: Die globale Zone wird zuerst erkannt.

- Das System erstellt das CI für den Solaris-Server für die globale Zone.
- Discovery erkennt die lokalen Zonen und erstellt für jedes Solaris-Gerät in der lokalen Zone je einen Datensatz für den Hypervisor-Zonenserver und die VM-Instanz.
- Discovery erstellt die Beziehung zwischen dem Hypervisor-Datensatz und dem VM-Instanzdatensatz.

Fall 2: Die lokale Zone wird zuerst erkannt.

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

- Das System erstellt das CI für den Solaris-Server für die lokale Zone.
- Discovery legt die Korrelations-ID fest, damit sie bei späteren globalen Zonenerkennungen abgeglichen werden kann.

Fall 3: Die globale Zone wird nach der Erstellung von CIs für Solaris-Server der lokalen Zone erkannt.

- Die globale Zonenerkennung erkennt lokale Zonen.
- Discovery erstellt für jedes Solaris-Gerät in der lokalen Zone je einen Datensatz für den Hypervisor-Zonenserver und die VM-Instanz.
- Discovery erstellt die Beziehung zwischen dem Hypervisor-Datensatz und dem VM-Instanzdatensatz. Darüber hinaus wird die Beziehung zwischen dem virtuellen Computer der physischen lokalen Zone und dem entsprechenden Datensatz für die VM-Instanz hergestellt.
- Die globale Zone führt die Probe „Solaris - ADM“ für sich selbst aus, filtert nach der lokalen Zone und aktualisiert die physischen VMs der lokalen Zone mit diesen Daten.

Fall 4: Der Beziehungspfad zwischen physischen lokalen und globalen Zonencomputern wird eingerichtet.

Nachfolgende Erkennungen der globalen Zone aktualisieren die TCP-Verbindungs- und -Prozessinformationen für die enthaltenen lokalen Zonen.

Wenn das System eine globale Zone erkennt, löst die Probe „Solaris - Zones & ADM Launcher“ die Probe „Solaris - ADM“ aus, um die globale Zone und alle gefundenen lokalen Zonen zu untersuchen. Da die Probe „Solaris - ADM“ in der globalen Zone ausgeführt werden muss, um Informationen über TCP-Verbindungen und Prozesse aus ihren lokalen Zonen zu erkennen, werden möglicherweise mehrere ECC-Warteschlangen-Datensätze angezeigt, die identisch aussehen.

ECC-Warteschlangeneinträge zur Zonenerkennung

2016-01-13 02:02:29	mid.server.demouk	MultiProbe	Solaris - Application Dependency Mapping	10.196.39.206	input	processed	2016-01-13 02:02:31
2016-01-13 02:02:29	mid.server.demouk	MultiProbe	Solaris - Application Dependency Mapping	10.196.39.206	input	processed	2016-01-13 02:02:31
2016-01-13 02:02:29	mid.server.demouk	MultiProbe	Solaris - Application Dependency Mapping	10.196.39.206	input	processed	2016-01-13 02:02:31

Bei der Überprüfung der Nutzlast werden Sie jedoch feststellen, dass jede Probe tatsächlich auf ein anderes Zonen-CI abzielt, nach dem gefiltert und aktualisiert werden soll.

Nutzlast der lokalen Zone

```
<parameter name="sequence" value="1523a01c947000001
<parameter name="from host" value=""/>
<parameter name="zone" value="zone01"/>
<parameter name="sys_created_on" value="2016-01-13 (
<parameter name="used_by_discovery" value="true"/>
```

In Solaris-Zonen erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Version	cmdb_ci_vm_zones	Version	zoneadm, zonename
Zuordnungs-ID	cmdb_ci_vm_zones	correlation_id	zoneadm, zonename
Name	cmdb_ci_solaris_instance	Name	zoneadm, zonename
Übergeordnet	cmdb_ci_solaris_instance	parent	Intern

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

In Solaris-Zonen erfasste Daten (Fortsetzung)

Bezeichnung	Tabellenname	Feldname	Quelle
CMDB CI	`cmdb_ci_solaris_instance`	`cmdb_ci`	Intern
Zuordnungs-ID	`cmdb_ci_solaris_instance`	`correlation_id`	zoneadm, zonename

Hinweis: cmdb_ci_solaris_instance erweitert cmdb_ci_vm_instance.

Erkennung eines virtuellen Computers (VM).

Muster für Discovery und Service-Mapping Informationen über virtuelle Computer identifizieren und klassifizieren.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Nach dem Upgrade auf Discovery-Administratorarbeitsbereich Version 1.3.1 (Store August 2024) können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** und verwenden Sie das erweiterte Dashboard.

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Erfasste Daten

Bezeichnung	Tabellenname	Feldname
CPUs	cmdb_ci_vm_instance	CPUs
Datenträger	cmdb_ci_vm_instance	disks
Datenträgergröße	cmdb_ci_vm_instance	disks_size
Bildpfad	cmdb_ci_vmware_instance	image_path
Arbeitsspeicher	cmdb_ci_vm_instance	memory
Netzwerkadapter	cmdb_ci_vm_instance	nics
Status	cmdb_ci_vm_instance	state
Vorlage	cmdb_ci_vmware_instance	Vorlage
vCenter-Referenz	cmdb_ci_vmware_instance	vcenter_ref
vCenter-Referenz-UUID	cmdb_ci_vmware_instance	vcenter_uuid

VMware-Erkennung

Mit einem Discovery-Zeitplan können VMware vCenter- und ESX-Hosts sowie einzelne ESXi-Hosts erkannt werden, mit denen virtuelle Computer und zugehörige Komponenten ohne vCenter verwaltet werden.

Die folgenden Optionen sind zum Abrufen von VMware vCenter-Daten verfügbar:

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

- Discovery führt die Probe VMware - vCenter Datacenters aus und identifiziert einen VMware vCenter-Prozess, der auf einem Windows-Computer ausgeführt wird, oder erkennt Aktivität mit der Probe „vmapp port“.
- Klassische Orchestrierung kann alle vCenter-Probes aus einem Workflow ausführen.

Um VMware-Daten ohne vCenter zu erkennen, verwenden Sie die eigenständige ESXi-Discovery.

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Erkennung für VMware vCenter

Discovery kann den VMware vCenter-Prozess untersuchen, der auf einem Windows- oder Linux-Host ausgeführt wird. IPv6 wird für vCenter unterstützt.

Hinweis:

Wenn auf einem Windows- oder Linux-Server die Anwendung vCenter ausgeführt wird, wird nach dem Erstellen des vCenter-CI eine Beziehung vom Typ „Wird ausgeführt auf“ mit dem Windows- oder Linux-Serverhost erstellt.

Wenn vCenter auf einer dedizierten vCenter-Appliance ausgeführt wird, wird die Beziehung vom Typ „Wird ausgeführt auf“ zum vCenter-CI nicht erstellt.

Getestete vCenter-Versionen

Die ServiceNow® Platform unterstützt die vCenter-API Version 4.0 und höher. Die folgenden Versionen wurden mit Release Yokohama getestet:

- vCenter Version 7.0 und früher
- vCenter-Appliance Version 6.7 und früher

Für Installationen, die auf der vCenter-Appliance basieren, wird ein Server-CI für die vCenter-Appliance erstellt, und die folgenden Felder werden ausgefüllt:

- NameIP
- AddressMAC
- AddressDiscovery
- Quelle

Hinweis: Wenn SUSE Linux-Hosts für vCenter-Appliances, Version 6.0 und früher, erkannt werden, beachten Sie die folgenden SSH-Beschränkungen .

Unter Für VMware vCenter-Server erfasste Daten finden Sie eine Beschreibung der VMware-Architektur und der Komponentenbeziehungen.

Erkennungsprozess für vCenter

Nach der Klassifizierung von vCenter startet Discovery die Probe „VMware - vCenter Datacenters“, der wiederum spezifische Probes startet, die Informationen über ESX-Computer, virtuelle Computer und andere vCenter-Objekte zurückgeben. Die Probe „vmapp port“ ist auch zum Starten des Probe „VMware - vCenter Datacenters“ konfiguriert.

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

VMware-Anmeldeinformationen

Wenn Sie eine Domänenkonto für den Zugriff auf vCenter verwenden, geben Sie die Domäne mit dem Benutzernamen im Datensatz für die Anmeldeinformationen in einem der unterstützten Formate an, zum Beispiel **Domäne\Benutzername**. Die VMware-Anmeldeinformationen müssen in vCenter über Leseberechtigung und Lizenz-Administratorrechte verfügen.

Wichtig: Windows-Anmeldeinformationen sind für vCenter-Discovery nicht erforderlich, wenn gültige VMware-Anmeldeinformationen verwendet werden.

CMDB mit vCenter-Ereignissammlung aktualisieren

Neben der Suche nach vCenter-Daten über den standardmäßigen Discovery-Prozess kann Discovery die CMDB auch aktualisieren, indem vCenter-Ereignisse über eine MID-Servererweiterung namens vCenter Event Collector erkannt werden.

Mit dem Ereignissammler kann die CMDB zusätzlich zu den von Discovery erkannten Aktualisierungen mit Änderungen an virtuellen Maschinen (VMs) aktualisiert werden. Eine Änderung an einer VM wird vom vCenter-Server als Ereignis an den vCenter-Ereignissammler gesendet. Wenn ein Ereignis empfangen wird, wird die CMDB entsprechend aktualisiert. Full vCenter Discovery muss nicht erneut ausgeführt werden. Bei einigen Ereignissen, z. B. eingeschalteten und ausgeschalteten Ereignissen, muss Discovery nicht erneut ausgeführt werden. Bei den meisten Ereignissen wird Discovery nur auf der erforderlichen vCenter-Ressource ausgeführt.

Anweisungen zum Konfigurieren von vCenter-Ereignissen finden Sie unter Erweiterung der vCenter-Ereignissammlung konfigurieren und ausführen .

VM aus vCenter gelöscht

Beim Löschen der VM aus vCenter wird der Status von „cmdb_ci_vm_instance“ in „Beendet“ und der Wert des Statusfelds in „Deaktiviert“ geändert.

CIs aus vCenter entfernt

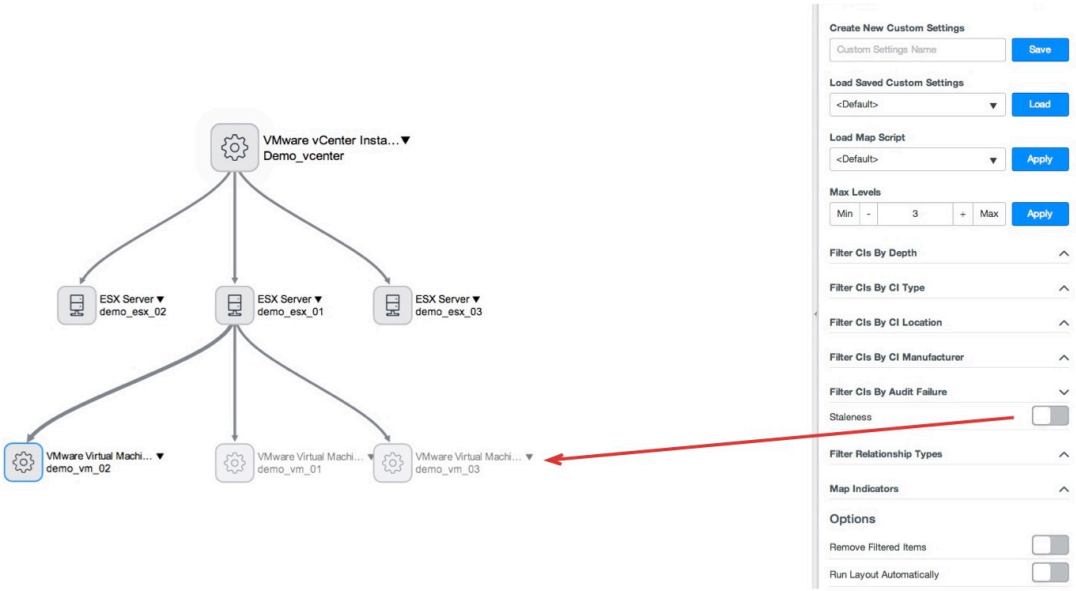
Wenn ein vCenter-CI wie ein virtueller Computer entfernt wird, wird es von der ServiceNow-Instanz in der CMDB mit einem der folgenden Verfahren als „veraltet“ markiert:

- Wenn Discovery ausgeführt wird, wird in der Tabelle „Mit CMDB-Integrität installierte Komponenten“ ein Audit-Datensatz für das fehlende CI erstellt und das CI als „veraltet“ markiert.
- Wenn die Instanz zum Erfassen von vCenter-Ereignissen konfiguriert ist, kann das System auch auf Basis des Ereignisses VmRemovedEvent einen „Veraltet“-Audit-Datensatz für das CI in der Tabelle „CMDB-Integritätsergebnis“ [cmdb_health_result] erstellen, ohne Discovery ausführen zu müssen.

Hinweis: Wenn die Einstellung **Veraltung** konfiguriert ist, werden in der Abhängigkeitsansicht (BSM-Zuordnung) veraltete CIs im Beziehungsdiagramm grau dargestellt, um anzugeben, dass sie aus vCenter entfernt wurden.

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

Als „veraltet“ markiertes vCenter-CI



Sie können eine CMDB-Korrekturregel erstellen, um automatisch einen Korrektur-Workflow auszuführen, der beispielsweise veraltete CIs löschen kann. Weitere Informationen zu veralteten CIs finden Sie unter CMDB-Integritätsmetriken .

Erkennung von vCenter auf Windows-Host

Windows-Anmeldeinformationen sind für vCenter Discovery nicht erforderlich, wenn gültige VMware-Anmeldeinformationen verwendet werden.

Alternativen Port für vCenter konfigurieren

Für die Probe „VMWare - vCenter Datacenters“ können Sie einen alternativen Port angeben.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig wird die Probe „VMware - vCenter Datacenters“ an Port 443 ausgeführt, dem Standardport für das https-Protokoll. Die Port-Probes für vCenter werden an den folgenden Ports ausgeführt:

- **vmapp6_https**: 9443
- **vmapp_https**: 5480

Prozedur

1. Hartcodieren Sie die Portinformationen.

   a. Navigieren zu **Alle** > **Konfiguration** > **VMware** > **vCenter**.

   b. Wählen Sie aus der Liste der Instanzen die gewünschte Instanz aus.

   c. Bearbeiten Sie das Feld **URL** so, dass der Port einbezogen wird.
   Beispiel: `https://10.0.0.1:444`

   d. Klicken Sie auf **Absenden**.

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

2. Geben Sie für die Probe „VMWare - vCenter Datacenters“ einen alternativen Port für vCenter an.
   a. Navigieren zu **Alle** > **Discovery** > **Probes**.
   b. Öffnen Sie den Probe-Datensatz **VMware - vCenter Datacenters**.
   c. Klicken Sie in der zugehörigen Liste **Probe Parameter** auf **Neu**.
   d. Geben Sie in das Feld **Name** des Probe-Parameterdatensatzes den Namen `vcenter_port` ein.
   e. Geben Sie in das Feld **Wert** die alternative Portnummer ein.
   f. Klicken Sie auf **Absenden**.

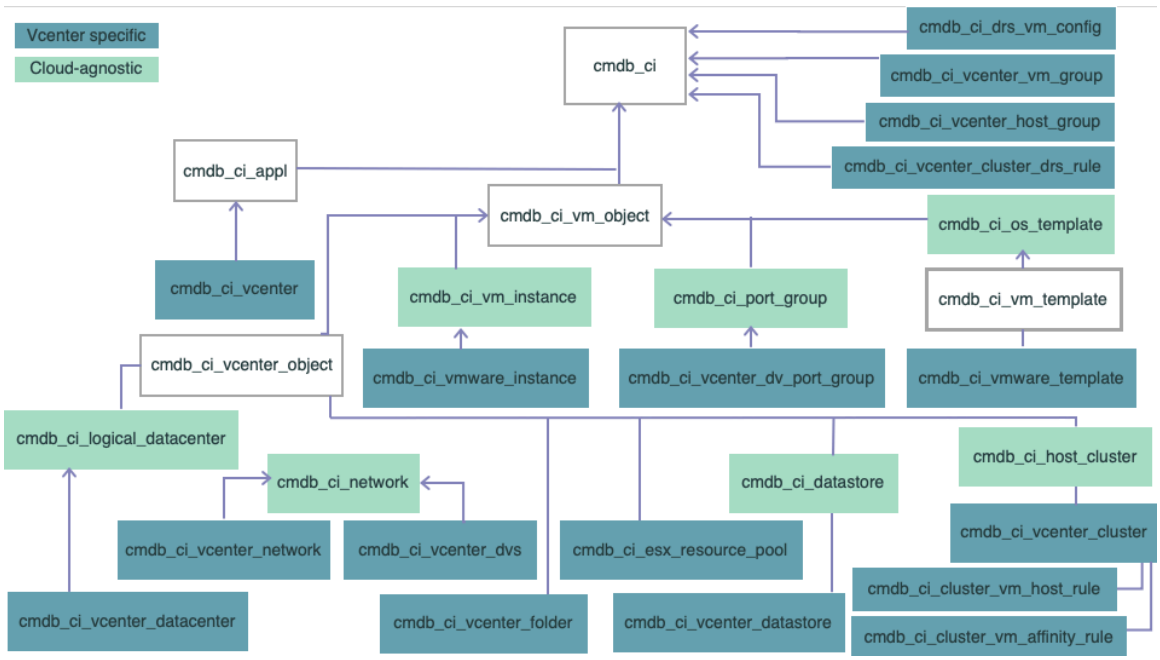
Für VMware vCenter-Server erfasste Daten

Discovery identifiziert und klassifiziert Informationen über VMware vCenter-Server.

vCenter-Tabellenschema

Im folgenden Diagramm wird das vCenter-Tabellenschema dargestellt:

vCenter-Tabellenschema



Bei mehreren Tabellen handelt es sich um Cloudagnostische Tabellen. Das heißt, dass sie für jede Cloud-Ressource gefüllt werden können, nicht nur für vCenter-Ressourcen. Suchen Sie in den untergeordneten Tabellen, die Erweiterungen der Cloudagnostischen Tabellen sind, nach erkannten CIs.

Cloudagnostische Tabelle	Entsprechende vCenter-spezifische Tabelle
VM-Instanz [cmdb_ci_vm_instance]	VMware-VM-Instanz [cmdb_ci_vmware_instance]
Betriebssystemvorlage [cmdb_ci_os_template]	Vorlage für virtuellen VMware-Computer [cmdb_ci_vmware_template]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]

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

Cloudagnostische Tabelle	Entsprechende vCenter-spezifische Tabelle
Cloud-Netzwerke [cmdb_ci_network]	VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]
Datenspeicher [cmdb_ci_datastore]	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]
Hostcluster [cmdb_ci_host_cluster]	VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]

vCenter-Daten

Mithilfe von mehreren vCenter-Probes erfasst Discovery Daten aus vCenter. Die Daten werden in Tabellen gespeichert, die Erweiterungen der Tabelle der Konfigurationselemente [cmdb_ci] darstellen.

VMware vCenter-Instanz [cmdb_ci_vcenter]

Feldbezeichnung	Spaltenname
Name	Name
Vollständiger Name	fullname
Instanz-UUID	instance_uuid
URL	url
Tatsächliche CPU	effectivecpu

Die Kombination der vCenter-Instanz in der Tabelle cmdb_ci_vcenter und der Objekt-ID in der Tabelle cmdb_ci_vm_object identifiziert ein bestimmtes vCenter.

Die Tabellen erweitern die Tabelle „VM-Objekte“ [cmdb_ci_vm_object], die Objekt-IDs für alle cloudbasierten Ressourcen mit Ausnahme von Virtualisierungsservern enthält.

DRS-VM-Konfiguration [cmdb_ci_drs_vm_config]

Feldbezeichnung	Spaltenname
Cluster	Cluster
DRS-Verhalten	drs_behavior
DRS-fähig	drs_enabled
Virtueller Computer	virtual_machine

In dieser Tabelle wird das DRS-Verhalten für die VMs gespeichert, das das Clusterverhalten überschreibt. Weitere Informationen zu DRS finden Sie in der VMware-Dokumentation zum verteilten Ressourcenplaner .

VMware vCenter-VM-Gruppe [cmdb_ci_vcenter_vm_group]

Feldbezeichnung	Spaltenname
Cluster	Cluster

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

Die Tabelle „VMware vCenter-VM-Gruppe“ [cmdb_ci_vcenter_vm_group] weist gegenüber „cmdb_ci_vmware_instance“ eine Beziehung vom Typ „Enthält::Enthalten in“ auf. Diese Gruppe verfügt über eine Reihe von VMs.

VMware vCenter-Hostgruppe [cmdb_ci_vcenter_vm_group]

Feldbezeichnung	Spaltenname
Cluster	Cluster

Die Tabelle „VMware vCenter-Hostgruppe“ [cmdb_ci_vcenter_host_group] weist gegenüber „cmdb_ci_vmware_instance“ eine Beziehung vom Typ „Enthält::Enthalten in“ auf. Diese Gruppe besitzt mehrere Hosts.

DRS-Regel für VMware vCenter-Cluster [cmdb_ci_vcenter_cluster_drs_rule]

Feldbezeichnung	Spaltenname
Regel-UUID	rule_uuid
Aktiv	active
Cluster	Cluster

VMware-VM-Instanz [cmdb_ci_vmware_instance]

Feldbezeichnung	Spaltenname
Name	Name
Vorlage	Vorlage
CPUs	CPUs
Datenträger	disks
Datenträgergröße (GB)	disks_size
Arbeitsspeicher (MB)	memory
Netzwerkadapter	nics
Bildpfad	image_path
Status	state
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref
Basisname	base_name
BIOS-UUID	bios_uuid
VM-Instanz-UUID	vm_instance_uuid
IP-Adresse	ip_address

Verteilte virtuelle VMware-Portgruppen [cmdb_ci_vcenter_dv_port_group]

Feldbezeichnung	Spaltenname
Name	Name

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

Verteilte virtuelle VMware-Portgruppen [cmdb_ci_vcenter_dv_port_group] (Fortsetzung)

Feldbezeichnung	Spaltenname
vCenter-Instanz-UUID	vcenter_uuid
Verweis auf verteilten virtuellen Switch	dvs_ref

Vorlage für virtuellen VMware-Computer [cmdb_ci_vmware_template]

Feldbezeichnung	Spaltenname
Name	Der Vorlagenname aus VMware
CPUs	CPUs
Datenträgergröße (GB)	disks_size
Gast-ID	guest_id
Arbeitsspeicher (MB)	memory
Bildpfad	image_path
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref
Netzwerkadapter	nics
Basisname	base_name
VM-Namensgeber	vm_namer
BIOS-UUID	bios_uuid
VM-Instanz-UUID	vm_instance_uuid

VMware vCenter-Objekt [cmdb_ci_vcenter_object]

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref

VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]*

Feldbezeichnung	Spaltenname
Region	region
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref
Ordner der obersten Ebene für VMs	folder_moreid
Ordner der obersten Ebene für Hosts	host_morid

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

*Die Tabelle „VMware vCenter-Rechenzentrum“ [cmdb_ci_vcenter_datacenter] ist eine Erweiterung der Tabelle [cmdb_ci_logical_datacenter].

VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]*

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref
Netzwerk, auf das von Hosts oder VM zugegriffen werden kann	accessible

*Die Tabelle „VMware vCenter-Netzwerk“ [cmdb_ci_vcenter_network] ist eine Erweiterung der Tabelle [cmdb_ci_network].

Verteilter virtueller VMware-Switch [cmdb_ci_vcenter_dvs]

Feldbezeichnung	Spaltenname
VMCount	vm_count
Hostanzahl	host_count

VMware vCenter-Ordner [cmdb_ci_vcenter_folder]

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
vCenter-Referenz	vcenter_ref
Vollständiger Pfad	fullpath

ESX-Ressourcenpool [cmdb_ci_esx_resource_pool]

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter
vCenter-Referenz	vcenter_ref
Besitzer	Eigentümer
Eigentümer verwaltetes Objekt Referenz-ID	owner_morid
CPU erweiterbar	cpu_expandable
CPU limitiert (MHz)	cpu_limit_mhz
CPU reserviert (MHz)	cpu_reserved_mhz
CPU Anteile	cpu_shares
Vollständiger Pfad	fullpath

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

ESX-Ressourcenpool [cmdb_ci_esx_resource_pool] (Fortsetzung)

Feldbezeichnung	Spaltenname
Arbeitsspeicher erweiterbar	mem_expandable
Arbeitsspeicher limitiert (MB)	mem_limit_mb
Arbeitsspeicher reserviert (MB)	mem_reserved_mb
Speicheranteile	mem_shares

VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
Zugänglich	accessible
vCenter-Referenz	vcenter_ref
Typ	Typ
Kapazität (GB)	Kapazität
Freier Speicherplatz (GB)	freespace
URL	url
Geclustert	clustered

*Die Tabelle „VMware vCenter-Datenspeicher“ [cmdb_ci_vcenter_datastore] ist eine Erweiterung der Tabelle [cmdb_ci_datastore].

VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]*

Feldbezeichnung	Spaltenname
Verwaltetes Objekt Referenz-ID	morid
vCenter-Instanz-UUID	vcenter_uuid
Effektive Hosts	effectivehosts
vCenter-Referenz	vcenter_ref
Tatsächliche CPU	effectivecpu
Tatsächlicher Speicher	effectivememory
Anzahl tatsächlicher Hosts	effectivehosts
Anzahl Hosts	numhosts
CPU gesamt	totalcpu
Speicher gesamt	totalmemory
Anzahl der CPU-Kerne	numcpucores
Anzahl der CPU-Kerne	numcputhreads
DRS-Verhalten	drs_behavior

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

VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]* (Fortsetzung)

Feldbezeichnung	Spaltenname
DRS aktiviert	drs_enabled
DRS-VMotion-Rate	drs_vmotion_rate

*Die Tabelle „VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]“ ist eine Erweiterung der Tabelle [cmdb_ci_host_cluster].

Informationen zur Clusterhostregel der VM [cmdb_ci_cluster_vm_host_rule]

Feldbezeichnung	Spaltenname
VM-Gruppe	vm_group
Hostgruppe	host_group
Obligatorisch	Obligatorisch
Affinität	affinity

Informationen zur Clusteraffinitätsregel der VM [cmdb_ci_cluster_vm_affinity_rule]

Feldbezeichnung	Spaltenname
Affinität	affinity

Die Tabelle „Informationen zur Clusteraffinitätsregel der VM“ [cmdb_ci_cluster_vm_affinity_rule] weist gegenüber „cmdb_ci_vmware_instance“ die Beziehung „Enthält::Enthalten in“ auf. Diese Gruppe besitzt mehrere VMs, auf die diese Affinität angewendet wird.

Verteilter virtueller VMware-Switch [cmdb_ci_vcenter_dvs]

Feldbezeichnung	Spaltenname
Name	Name
VMCount	vm_count
Hostanzahl	host_count

Discovery ordnet die Beziehungen auch VMs und verteilten virtuellen Portgruppen zu.

Verteilte virtuelle VMware-Portgruppe [cmdb_ci_vcenter_dv_port_group]

Feldbezeichnung	Spaltenname
Name	Name
vCenter-Instanz-UUID	vcenter_uuid
Verweis auf verteilten virtuellen Switch	dvs_ref

Discovery ordnet die Beziehungen auch dem verteilten virtuellen Switch zu.

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

Sie können die folgenden zugehörigen Listen hinzufügen, um zusätzliche erkannte Daten anzuzeigen:

- Speicher-Laufwerke

  Die virtuellen Datenträger für diesen virtuellen Computer. Diese Daten werden in der Tabelle „Speichervolume“ [cmdb_ci_storage_volume] mit dem Wert `type=v Disk` gespeichert.

Speichervolume [cmdb_ci_storage_volume]

Feldbezeichnung	Spaltenname
Name	Name
Größe	size

- Netzwerkadapter

  Die virtuellen Netzwerkadapter für die virtuellen Datenträger. Diese Daten werden in der Tabelle „Netzwerkadapter“ [cmdb_ci_network_adapter] gespeichert.

Netzwerkadapter [cmdb_ci_network_adapter]

Feldbezeichnung	Spaltenname
Name	Name
IP-Adresse	ip_address
MAC-Adresse	mac_address
Netzmaske	netmask

vCenter-Erkennung mit Software Asset Management

Wenn Software Asset Management aktiv ist, füllt Discovery diese vCenter-Tabellen mithilfe der Probe „VMware - vCenter ESX Hosts License“.

VMware-Lizenzschlüssel [samp_vmware_license_key]

Feldbezeichnung	Spaltenname
vCenter-Referenz	vcenter_ref
Kosteneinheit	cost_unit
Edition	Edition
Funktionen	features
Lizenzschlüssel	license_key
Produktname	product_name
Produktversion	product_version
Rechte im Besitz	rights_owned
Verwendete Rechte	rights_used

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

VMware-Lizenzschlüsselnutzung [samp_vmware_license_key_usage]

Feldbezeichnung	Spaltenname
Verwendete Rechte	rights_used
Ablaufdatum	expiration_date
Verwendete Funktionen	used_features
Lizenzschlüssel	license_key
Softwareinstallation	software_install
Verwendet von	used_by

vCenter-Beziehungen

Discovery erstellt mithilfe von Daten aus einer Schlüsselklasse automatisch Beziehungen für vCenter-Komponenten. Nachfolgende Erkennungen verwenden dieselbe Schlüsselklasse, um Beziehungen, die nicht mehr gültig sind, automatisch zu validieren und zu entfernen.

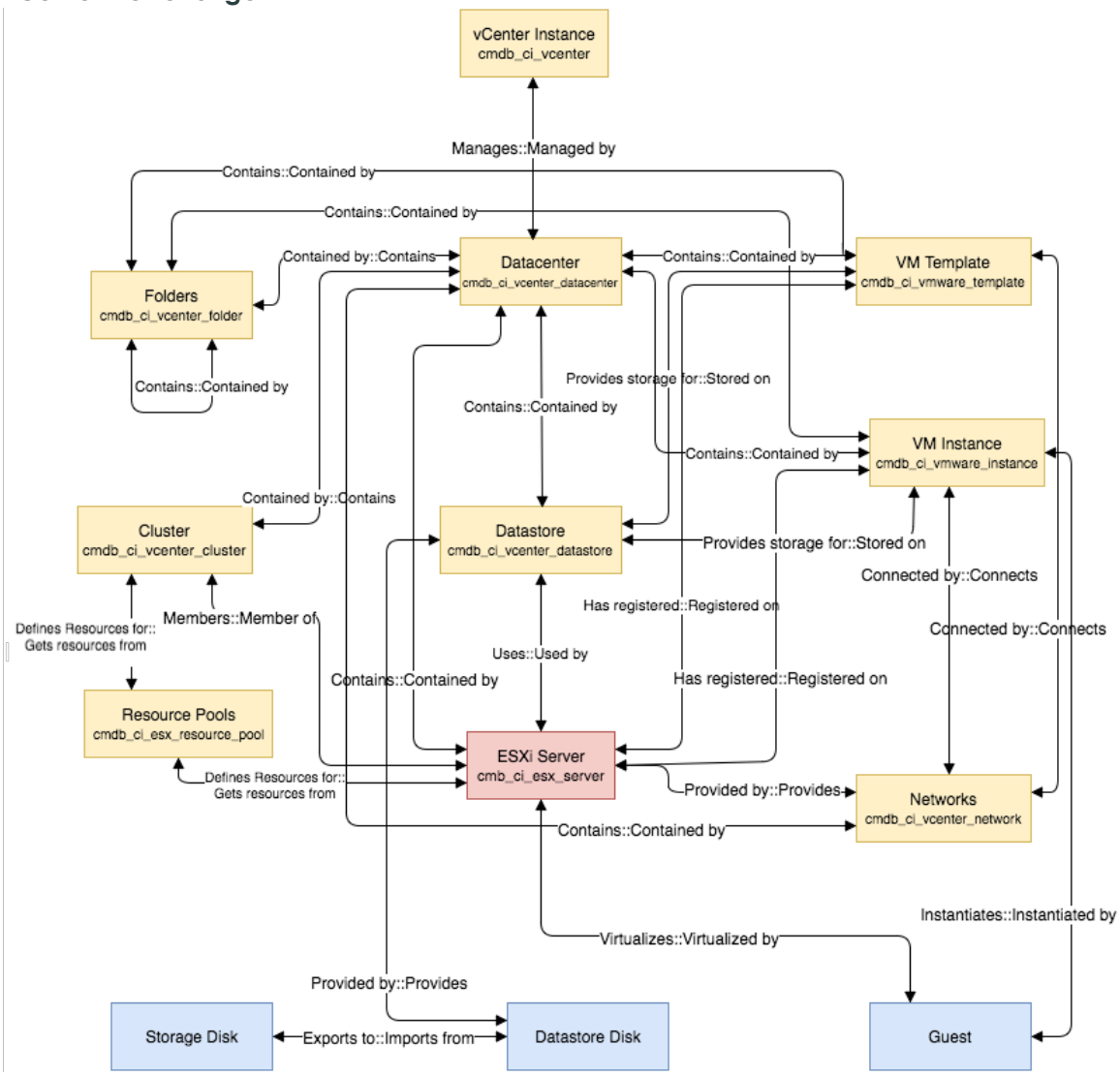
vCenter-CIs können Mitglieder von Ordnern oder Clustern sein, was sich darauf auswirkt, wie Discovery deren Beziehungen erstellt.

- Wenn sich ein CI in einem Ordner befindet, erstellt Discovery eine Beziehung zwischen diesem CI und dem Ordner. Befindet sich das CI nicht in einem Ordner, erzeugt Discovery die Beziehung zwischen dem CI und dem Rechenzentrum. Die folgenden vCenter-CIs können sich in einem Ordner befinden:
  - VM-Instanz
  - VM-Template
  - vCenter-Netzwerk
  - Datenspeicher
  - vCenter-Ordner
  - vCenter-Cluster
- Wenn sich ein ESX-Server in einem Cluster befindet, erstellt Discovery eine Beziehung zwischen dem ESX-Server und dem Cluster. Ist ein ESX-Server kein Mitglied eines Clusters, erzeugt Discovery eine Beziehung zum Rechenzentrum.
- Wenn sich ein Ressourcenpool in einem Cluster befindet, erstellt Discovery eine Beziehung zwischen dem Ressourcenpool und dem Cluster. Ist der Ressourcenpool kein Mitglied eines Clusters, erstellt Discovery eine Beziehung zum ESX-Server.

Das folgende Diagramm veranschaulicht vCenter-Beziehungen:

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

vCenter-Beziehungen



Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Computer [cmdb_ci_computer]	Virtualisiert von::Virtualisiert	ESX-Server [cmdb_ci_esx_server] **Hinweis:** Die vom ESX-Server und der VM-Instanz zum Gast erstellte Beziehung wird durch die Geschäftsregel „Überprüfung des virtuellen Computers“ erstellt. Der Gastcomputer muss erkannt werden, nachdem das VCenter erkannt wurde, um die Geschäftsregel auszulösen und entsprechende Beziehungen zu erstellen.
Computer [cmdb_ci_computer]	Instanziiert::Instanziiert von	VM-Instanz [cmdb_ci_vmware_instance]

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

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
		Hinweis: Die vom ESX-Server und der VM-Instanz zum Gast erstellte Beziehung wird durch die Geschäftsregel „Überprüfung des virtuellen Computers“ erstellt. Der Gastcomputer muss erkannt werden, nachdem das VCenter erkannt wurde, um die Geschäftsregel auszulösen und entsprechende Beziehungen zu erstellen.
VMware-VM-Instanz [cmdb_ci_vmware_instance]	Registriert auf::Hat sich registriert	ESX-Server [cmdb_ci_esx_server]
VMware-VM-Instanz [cmdb_ci_vmware_instance]	Verbunden von::Verbindet	VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]
Vorlage für virtuellen Computer [cmdb_ci_vmware_template]	Verbunden von::Verbindet	VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]
VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]	Bereitgestellt von::Stellt bereit	ESX-Server [cmdb_ci_esx_server]
VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Stellt Speicher bereit für::Gespeichert auf	VMware-VM-Instanz [cmdb_ci_vmware_instance]
VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Verwendet von::Verwendet	ESX-Server [cmdb_ci_esx_server]
VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Stellt Speicher bereit für::Gespeichert auf	Vorlage für virtuellen Computer [cmdb_ci_vmware_template]
VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]	Mitglieder::Mitglied von	ESX-Server [cmdb_ci_esx_server]
ESX-Ressourcenpool [cmdb_ci_esx_resource_pool]	Definiert Ressourcen für::Erhält Ressourcen von	VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]
ESX-Ressourcenpool [cmdb_ci_esx_resource_pool]	Definiert Ressourcen für::Erhält Ressourcen von	ESX-Server [cmdb_ci_esx_server]
VMware vCenter-Ordner [cmdb_ci_vcenter_folder]	Enthält::Enthalten in	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]
VMware vCenter-Ordner [cmdb_ci_vcenter_folder]	Enthält::Enthalten in	VMware vCenter-Ordner [cmdb_ci_vcenter_folder]
VMware vCenter-Ordner [cmdb_ci_vcenter_folder]	Enthält::Enthalten in	Vorlage für virtuellen Computer [cmdb_ci_vmware_template]

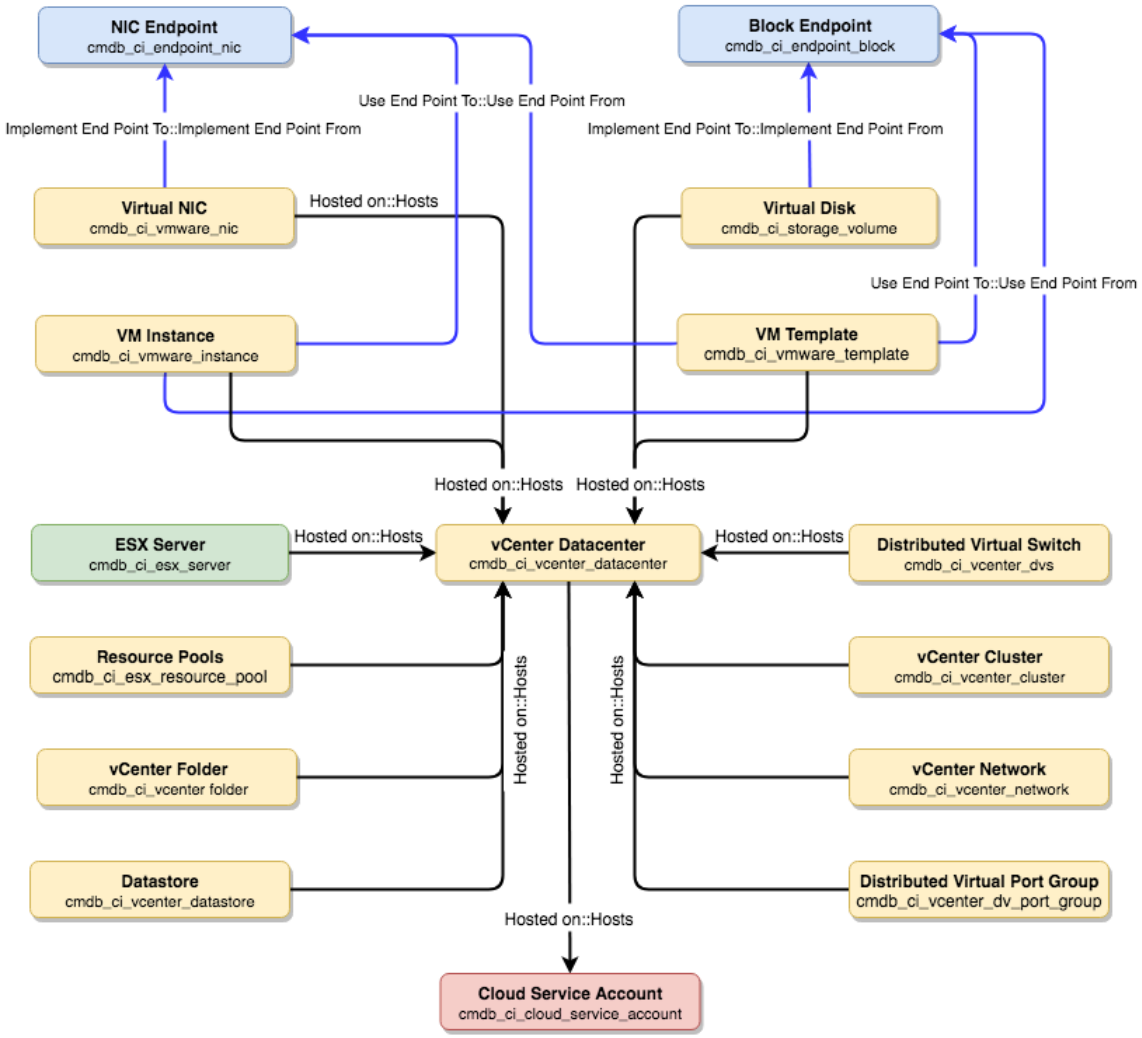
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
VMware vCenter-Ordner [cmdb_ci_vcenter_folder]	Enthält::Enthalten in	VMware-VM-Instanz [cmdb_ci_vmware_instance]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	VMware-VM-Instanz [cmdb_ci_vmware_instance]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	ESX-Server [cmdb_ci_esx_server]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	VMware vCenter-Ordner [cmdb_ci_vcenter_folder]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	VMware vCenter-Cluster [cmdb_ci_vcenter_cluster]
VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Enthält::Enthalten in	Vorlage für virtuellen Computer [cmdb_ci_vmware_template]

Cloud Management-Beziehungen

Die folgenden zusätzlichen Beziehungen werden erstellt, wenn Cloud Management (CMP) aktiv ist.

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



Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
ESX-Server [cmdb_ci_esx_server]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
vCenter-Ordner [cmdb_ci_vcenter folder]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
vCenter-Cluster [cmdb_ci_vcenter_cluster]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Ressourcenpools [cmdb_ci_esx_resource_pool]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
VM-Instanz [cmdb_ci_vmware_instance]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
VM-Vorlage [cmdb_ci_vmware_template]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
vCenter-Netzwerk [cmdb_ci_vcenter_network]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]

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

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
Verteilter virtueller Switch [cmdb_ci_vcenter_dvs]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Verteilte virtuelle Portgruppe [cmdb_ci_vcenter_dv_port_group]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Datenspeicher [cmdb_ci_vcenter_datastore]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Virtueller Datenträger [cmdb_ci_storage_volume]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
Virtuelle NIC [cmdb_ci_vmware_nic]	Gehostet auf::Hostet	vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]
VM-Vorlage [cmdb_ci_vmware_template]	Endpunkt verwenden an::Endpunkt verwenden von	Block-Endpunkt [cmdb_ci_endpoint_block]
VM-Instanz [cmdb_ci_vmware_instance]	Endpunkt verwenden an::Endpunkt verwenden von	Block-Endpunkt [cmdb_ci_endpoint_block]
Virtueller Datenträger [cmdb_ci_storage_volume]	Endpunkt implementieren in::Endpunkt implementieren von	Block-Endpunkt [cmdb_ci_endpoint_block]
Virtuelle NIC [cmdb_ci_vmware_nic]	Endpunkt implementieren in::Endpunkt implementieren von	NIC-Endpunkt [cmdb_ci_endpoint_nic]
VM-Vorlage [cmdb_ci_vmware_template]	Endpunkt verwenden an::Endpunkt verwenden von	NIC-Endpunkt [cmdb_ci_endpoint_nic]
VM-Instanz [cmdb_ci_vmware_instance]	Endpunkt verwenden an::Endpunkt verwenden von	NIC-Endpunkt [cmdb_ci_endpoint_nic]

VMware-Tags

Über die vSphere-Schnittstelle können Sie Tags an vSphere-Objekte (zum Beispiel virtuelle Computer) anhängen. Die Tags können dann in Kategorien gruppiert werden. Objekte mit Tags können basierend auf den Parametern, die Sie den Tags und Kategorien zuweisen, sortiert und durchsucht werden. Die Probe VMWare - vCenter VM Tags erkennt diese Tags. Die erkannten Tags können Sie anzeigen, indem Sie den VM-Datensatz in **cmdb_ci_vmware_instance** öffnen. Wechseln Sie dann zur Registerkarte **Schlüsselwerte**.

Schlüsselwerte [cmdb_key_value]

Feldbezeichnung und -name	Beschreibung
Konfigurationselement [configuration_item]	Referenzierte VM mit angehängtem Tag in vCenter
Schlüssel [key]	Kategoriename des Tag, das auf die Ressource in vCenter angewendet wird

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

Schlüsselwerte [cmdb_key_value] (Fortsetzung)

Feldbezeichnung und -name	Beschreibung
Tag [tag]	Quelle in vCenter, aus der Tags abgerufen werden. In diesem Fall lautet der Wert immer **Tags**.
Wert [value]	Name des Tag, das in vCenter auf die Ressource angewendet wird

Von Discovery erfasste Datenspeicherdaten

Discovery identifiziert jeden Datenspeicher im System und erstellt die Beziehungen zu den virtuellen Computern und den ESX-Servern, die diese Datenspeicher verwenden.

Datenspeicher

Discovery verwendet die Probe „VMware - vCenter Datastores“, um diese Daten aus Datenspeichern zu erfassen.

Feldbezeichnung	Tabellenname	Spaltenname	Beschreibung
Zugänglich	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	accessible	Angabe, ob der Datenspeicher erfasst wurde oder nicht
Kapazität (GB)	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Kapazität	Vom Datenspeicher bereitgestellter Speicherplatz
Geclustert	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	clustered	Angabe, ob der Datenspeicher geclustert ist (zu einem Speicher-Pod gehört)
Freier Speicherplatz (GB)	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	freespace	Im Datenspeicher noch verfügbarer Speicherplatz
Typ	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Typ	Typ des Dateisystemvolume, zum Beispiel WFS oder NFS
URL	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	url	Der eindeutige URL-Locator für den Datenspeicher

Host-Mounts

Discovery verwendet die Probes „VMWare - vCenter ESX Hosts“ und „VMWare - vCenter Datastores“, um Daten des Host-Mount für den Datenspeicher zu erfassen.

Feldbezeichnung	Tabelle	Spalte
Zugänglich	Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]	accessible

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

Feldbezeichnung	Tabelle	Spalte
Zugriffsmodus	Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]	access_mode
VMware vCenter-Datenspeicher	Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]	datastore
ESX-Server	Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]	esx_server
vCenter-Referenz	Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]	vcenter_ref

Erkennung von ESXi-Servern

Informationen über ESXi-Server und ESXi-Ressourcenpools identifiziert und klassifiziert Discovery nicht durch die direkte Erkennung von ESXi-Servern, sondern durch die Erkennung von vCenter.

Wichtig: Die Erkennung von ESXi-Servern erfolgt über vCenter. Geben Sie die IP-Adresse des ESXi-Servers nicht in einem Discovery-Zeitplan an. Führen Sie anhand des Erkennungszeitplans stattdessen eine Erkennung von vCenter durch.

Unter Für VMware vCenter-Server erfasste Daten finden Sie eine Beschreibung der VMware-Architektur und der Komponentenbeziehungen.

Eine Beschreibung, wie Discovery Informationen über Datenspeicher erfasst und die Beziehungen zwischen den ESXi-Hosts und den an die Datenspeicher angehängten Speicherdatenträgern herstellt, finden Sie unter Erkennung von Datenspeicher.

Erforderliche Rollen

Benutzer mit den Rollen *itil* und *asset* haben Zugriff auf Datensätze von ESXii- und ESXi-Konfigurationselementen (CIs). Zum Ausführen der Erkennung auf vCenter-Servern müssen Benutzer über die Rolle *discovery_admin* verfügen.

Berechtigungen

Zum Ausführen einer vollständigen Erkennung von vCenter-/ESXi-Servern benötigen Sie vCenter-Anmeldeinformationen. Wenn die Probe „vmapp port“ deaktiviert ist, müssen Sie mit Windows-Anmeldeinformationen auf den Windows-Host zugreifen, auf dem der vCenter-Server ausgeführt wird.

Hinweis: Stellen Sie sicher, dass Sie Anmeldeinformationen mit *VMware* als *Typ* auswählen.

Komponenten bei der Erkennung von ESXi-Servern

Discovery identifiziert ESXi-Server basierend auf der Korrelations-ID (BIOS-UUID), wenn sich der Hardwarehersteller auf einer zertifizierten Aufnahmeliste befindet. Befindet sich der Hersteller also in der Liste der kompatiblen Hersteller, muss die Korrelations-ID eindeutig sein. Wenn der Hersteller nicht auf der zertifizierten Aufnahmeliste steht, werden auch die verwaltete Objektreferenz-ID (MORID) und die Seriennummer überprüft. Nach der Ausführung der vCenter-Klassifizierung startet Discovery die Probe „VMware - vCenter Datacenters“, die die

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

Probes startet, die den ESXi-Server untersuchen. Die vollständige Liste der vCenter-Probes finden Sie unter Liste der Discovery-Probes.

Komponente	Name	Beschreibung
Klassifizierung	vCenter	Klassifiziert eigenständige vCenter-Server
Probe	VMWare - vCenter ESX Hosts	Erstellt Datensätze für ESXi-Server und Host-Mounts. Erstellt Beziehungen zwischen ESXi-Servern und vCenter-Komponenten. Löst Probes zur Speichererkennung aus
Probe	VMWare - vCenter ESX Hosts Storage	Erstellt Datensätze für ESXi-Hosthardware: Netzwerkadapter, Datenträger, HBAs, FC-Ports, iSCSI und FC-Datenträger. Erstellt Beziehungen zwischen DAS/iSCSI/FC-Datenträgern und Datenspeicher-Datenträgern

Erfasste Daten

Grundlegende Serverdaten von ESXi-Hosts werden mit der Probe „VMware - vCenter ESX-Hosts“ erfasst.

Von Discovery auf ESXi-Hosts erfasste Daten

Bezeichnung	Tabellenname	Feldname
Betriebssystem	cmdb_ci_esx_server	os
BS-Version	cmdb_ci_computer	os_version
Name	cmdb_ci_esx_server	Name
DNS-Domäne	cmdb_ci_esx_server	dns_domain
Hersteller	cmdb_ci_computer	manufacturer
Seriennummer	cmdb_ci_computer	serial_number
CPU-Typ	cmdb_ci_esx_server	cpu_type
CPU-Geschwindigkeit (MHz)	cmdb_ci_esx_server	cpu_speed
CPU-Anzahl	cmdb_ci_esx_server	cpu_count
Anzahl CPU-Kerne	cmdb_ci_computer	cpu_core_count
CPU-Hersteller	cmdb_ci_esx_server	cpu_manufacturer
Modell-ID	cmdb_ci_computer	model_id
RAM (MB)	cmdb_ci_esx_server	ram
Festplattenspeicher (GB)	cmdb_ci_esx_server	disk_space
Typ	cmdb_ci_disk	Typ
Modell-ID	cmdb_ci_disk	model_id
Festplattenspeicher (GB)	cmdb_ci_disk	disk_space
Name	cmdb_ci_disk	Name
Name	cmdb_ci_network_adapter	Name
IP-Adresse	cmdb_ci_network_adapter	ip_address

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

Von Discovery auf ESXi-Hosts erfasste Daten (Fortsetzung)

Bezeichnung	Tabellenname	Feldname
MAC-Adresse	cmdb_ci_network_adapter	mac_address
Netzmaske	cmdb_ci_network_adapter	netmask
Verwaltetes Objekt Referenz-ID	Virtualisierungsserver [cmdb_ci_virtualization_server]	morid
Seriennummer	Seriennummer [cmdb_serial_number]	serial_number

Beziehungen

Discovery erfasst die folgenden Beziehungsdaten für ESXi-Server.

Basisklasse	Beziehung	Abhängige Klasse
ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	Definiert Ressourcen für:Erhält Ressourcen von	ESXi-Server [cmdb_ci_esx_server]
VM-Instanz [cmdb_ci_vmware_instance]	Registriert auf::Hat sich registriert	ESXi-Server [cmdb_ci_esx_server]
ESXi-Server [cmdb_ci_esx_server]	Stellt Speicher bereit für::Gespeichert auf	VM-Vorlage [cmdb_ci_vmware_template]
ESXi-Server [cmdb_ci_esx_server]	Bereitgestellt von::Stellt bereit	Netzwerke [cmdb_ci_vcenter_network]
ESXi-Server [cmdb_ci_esx_server]	Mitglieder von::Mitglieder	Cluster [cmdb_ci_vcenter_cluster]
ESXi-Server [cmdb_ci_esx_server]	Enthält::Enthalten in	Rechenzentrum [cmdb_ci_vcenter_datacenter]

ESXi-Ressourcenpools

Ressourcenpools werden in vCenter konfiguriert. Sie definieren die maximale Menge an Ressourcen, die von virtuellen Computern in diesem Pool verwendet werden können. Eine ESXi-Servereigenschaft ermöglicht, dass Ressourcenpools bei Bedarf erweitert werden, wenn der ESXi-Server über zusätzliche Ressourcen verfügt. Die Felder **Name** und **Besitzer** jedes Ressourcenpools auf dem ESXi-Server müssen auf der Now Platform

in der Tabelle „ESXi-Ressourcenpool“ [cmdb_ci_esx_resource_pool] konfiguriert werden. Wenn Orchestration für VMware manuelle Bereitstellungsaufgaben ausführt, muss der Bereitsteller den richtigen Ressourcenpool für den angeforderten virtuellen Server auswählen. Discovery erkennt Ressourcenpools auf ESXi-Computern und füllt automatisch die Felder im Formular „ESXi-Ressourcenpool“. Weitere Informationen finden Sie unter ESXi-Ressourcenpools konfigurieren.

ESXi-Ressourcenpools erfordern das Plugin „Orchestration - VMware Support“.

Hinweis: Stellen Sie sicher, dass vCenter und der ESXi-Server vollständig konfiguriert wurden. Dies schließt die Erstellung der Vorlagen und Ressourcenpools ein.

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

Erfasste Daten

Bezeichnung	Tabelle	Feldname	Quelle
CPU erweiterbar	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	cpu_expendable	Probe „VMWare - vCenter Clusters“
CPU limitiert (MHz)	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	cpu_limit_mhz	Probe „VMWare - vCenter Clusters“
CPU reserviert (MHz)	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	cpu_reserved_mhz	Probe „VMWare - vCenter Clusters“
CPU Anteile	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	cpu_shares	Probe „VMWare - vCenter Clusters“
Vollständiger Pfad	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	fullpath	Probe „VMWare - vCenter Clusters“
Arbeitsspeicher erweiterbar	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	mem_expandable	Probe „VMWare - vCenter Clusters“
Arbeitsspeicher limitiert (MB)	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	mem_limit_mb	Probe „VMWare - vCenter Clusters“
Arbeitsspeicher reserviert (MB)	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	mem_reserved_mb	Probe „VMWare - vCenter Clusters“
Speicheranteile	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	mem_shares	Probe „VMWare - vCenter Clusters“
Besitzer	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	Eigentümer	Probe „VMWare - vCenter Clusters“
Eigentümer verwaltetes Objekt Referenz-ID	ESXi-Ressourcenpool [cmdb_ci_esx_resource_pool]	owner_morid	Probe „VMWare - vCenter Clusters“

ESXi-Ressourcenpools konfigurieren

Der ESXi-Server besitzt einen standardmäßigen Ressourcenpool namens „Ressourcen“, in dem normale Ressourcen für virtuelle Computer definiert werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Ressourcenebenen werden dynamisch aus Freigaben der gesamten Ressourcen generiert, die virtuellen Computern auf dem ESXi-Server zugewiesen sind. Ausführliche Informationen zur Berechnung dieser Ressourcen finden Sie in der VMware Knowledge Base https://www.vmware.com/ . ServiceNow Discovery erkennt diesen Standardressourcenpool und fügt dem Modul „ESXi-Ressourcenpools“ automatisch einen Datensatz hinzu. Wenn

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

Discovery nicht auf der ServiceNow-Instanz ausgeführt wird , erstellen Sie einen Datensatz für den Pool **Ressourcen**. Stellen Sie sicher, dass das Feld **Besitzer** korrekt ist, und lassen Sie die Ressourcenfelder leer. Wenn ein Bereitsteller bei der Bereitstellung eines virtuellen Servers den Pool **Ressourcen** auswählt, erstellt der ESXi-Server einen virtuellen Computer zur Verwendung unter normaler Last.

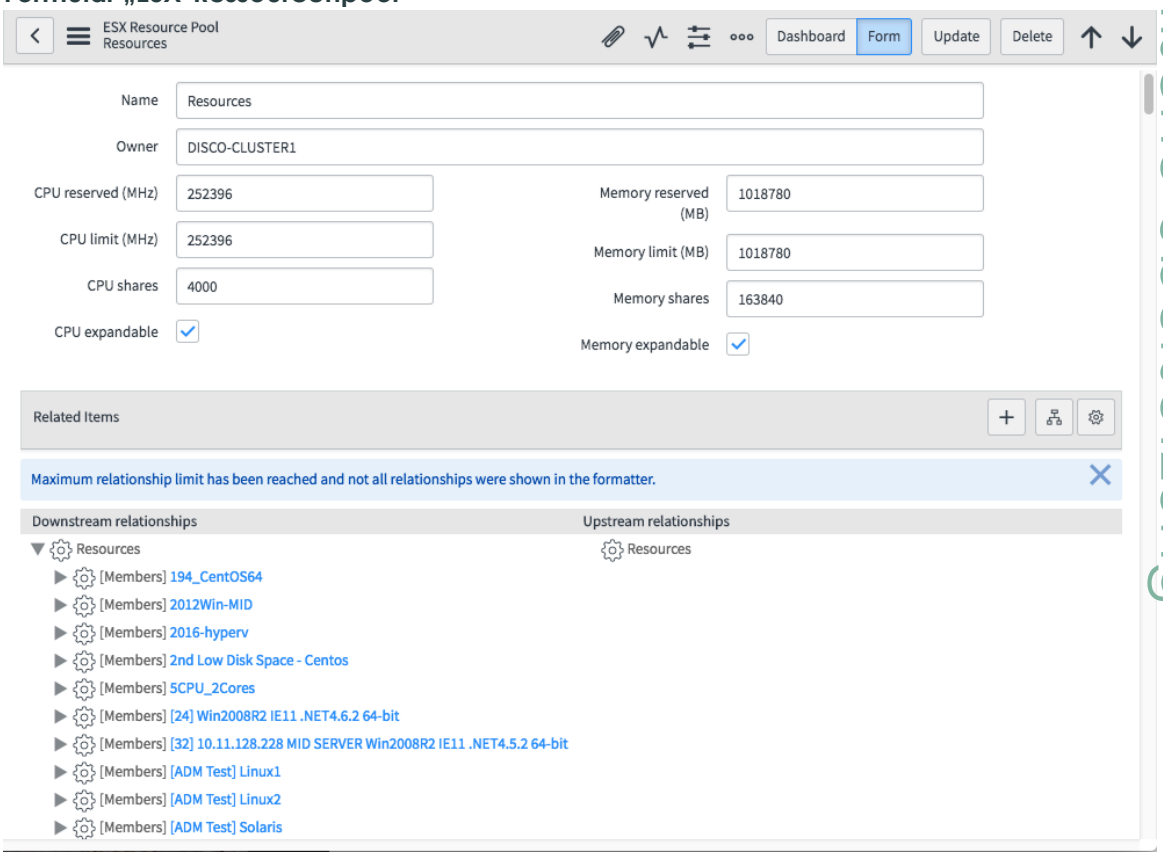
Prozedur

1. Navigieren zu **Alle** > **VMware Cloud** > **Konfiguration** > **ESX-Ressourcenpools**.
2. Klicken Sie in der Liste auf **Neu**.
3. Erstellen Sie einen neuen Datensatz für jeden Ressourcenpool auf dem ESXi-Server, und vergewissern Sie sich, dass die Felder **Name** und **Besitzer** korrekt ausgefüllt sind.
4. Aktivieren Sie die Kontrollkästchen **CPU erweiterbar** und **Arbeitsspeicher erweiterbar**, um bei Bedarf eine Erhöhung der CPU- und der Arbeitsspeicherlimits zu ermöglichen, wenn diese Ressourcen auf dem ESXi-Server verfügbar sind.

   Nach der Gewährung können diese zusätzlichen Ressourcen bei Bedarf widerrufen werden, um andere virtuelle Computer bereitzustellen. Die zusätzlichen Felder im Formular dienen nur zu Anzeigezwecken.

5. Klicken Sie auf **Absenden**.

Formular „ESX-Ressourcenpool“



Erkennung eigenständiger ESXi-Server

Mit der Erkennung eigenständiger ESXi-Server wird die Erkennung einzelner ESXi-Server unterstützt, auf denen virtuelle Computer (Virtual Machines, VMs) und zugehörige Komponenten ohne vCenter gehostet werden. Verschiedene CIs und Beziehungen werden im Rahmen eines Discovery-Zeitplans erkannt.

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

Erforderliche Rollen

Benutzer mit den Rollen *itil* und *asset* können auf ESXi-Configuration Item (CI)-Datensätze zugreifen. Zum Ausführen einer eigenständigen ESXi-Discovery benötigen Benutzer die Rolle *discovery_admin*.

VMware-Anmeldeinformationen

Zum Ausführen einer Erkennung eigenständiger ESXi-Server benötigen Sie VMware-Anmeldeinformationen. Erstellen Sie die Anmeldeinformationen, indem Sie zu navigieren **Discovery** > **Anmeldeinformationen** > **VMware-Anmeldeinformationen**

Wenn Sie ein Domänenkonto für den Zugriff auf den ESXi-Host verwenden, geben Sie die Domäne mit dem Benutzernamen im Datensatz für die Anmeldeinformationen in einem der unterstützten Formate an, zum Beispiel **Domäne\Benutzername**.

Hinweis: Die VMware-Anmeldeinformationen müssen auf dem ESXi-Host über eine Rolle mit Lesezugriff verfügen.

Anforderungen

- Stellen Sie sicher, dass das Plugin „Discovery“ (com.snc.discovery) installiert und aktiviert ist und dass Sie auf Release Yokohama oder höher aktualisiert haben.
- Aktivieren Sie die ESXi-Auslöser-Probe. Navigieren Sie zur Tabelle „Auslöser-Probe“ [trigger_probe_m2m]. Der esxi-Datensatz ist standardmäßig inaktiv. Markieren Sie „Aktiv“ als „true“, um die Erkennung eigenständiger ESXi-Server zu aktivieren.
- Erstellen Sie einen neuen Discovery-Zeitplan für den Host mit der entsprechenden IP-Adresse des ESXi-Hosts.

Hinweis: Wenn sowohl SSH als auch ESXi ausgelöst werden, wird SSH zuerst gestartet. Dies kann dazu führen, dass Discovery mit der Meldung „ESX-Discovery wird nur durch vCenter unterstützt“ abgeschlossen wird. Öffnen Sie in diesem Fall die Probe „Unix – Klassifizieren“, und legen Sie „ESX – OS“ inaktiv fest.

Komponenten bei der Erkennung von ESXi-Servern

Discovery identifiziert ESXi-Server basierend auf der Korrelations-ID (BIOS-UUID), wenn sich der Hardwarehersteller auf einer zertifizierten Aufnahmeliste befindet. Wenn der Hersteller in der Liste aufgeführt ist, muss die Korrelations-ID eindeutig sein. Wenn der Hersteller nicht auf der zertifizierten Aufnahmeliste steht, werden auch die verwaltete Objektreferenz-ID (MORID) und die Seriennummer überprüft.

Nach der Ausführung von Shazzam findet eine Suche nach der Port-Probe esxi statt. Anschließend startet Discovery die Probe „VMware - Standalone ESXi Server“, von der dann wiederum die Probes gestartet werden, mit denen der ESXi-Server untersucht wird. Andere vorhandene Discovery-Probes werden ebenfalls gestartet. Die vollständige Liste der Probes finden Sie unter Liste der Discovery-Probes.

Komponenten bei der Erkennung von ESXi-Servern

Komponente	Name	Beschreibung
IP-Service	ESXi	IP-Service ESXi - Die VMware VM-Konsole ist für Port 902 definiert.

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

Komponenten bei der Erkennung von ESXi-Servern (Fortsetzung)

Komponente	Name	Beschreibung
Port-Probe	esxi	Webbenutzeroberfläche der ESXi-Server-Appliance. Wird von IP Service ESXi ausgelöst und löst die Probe „VMware - Standalone ESXi Server“ aus.
Probe	VMware - Standalone ESXi Server	Probe, mit der Informationen zu einem ESXi-Server abgerufen werden
Probe	VMWare - vCenter ESX Hosts	Erstellt Datensätze für ESXi-Server und Host-Mounts. Löst andere Probes aus: • VMware - vCenter ESX Hosts Storage • VMware - vCenter Datastores • VMware - vCenter Networks • VMware - vCenter VMs
Probe	VMWare - vCenter ESX Hosts Storage	Erstellt Datensätze für ESXi-Hosthardware: Netzwerkadapter, Datenträger, HBAs, FC-Ports, iSCSI und FC-Datenträger. Erstellt Beziehungen zwischen DAS/iSCSI/FC-Datenträgern und Datenspeicher-Datenträgern

Grundlegende Serverdaten von ESXi-Hosts werden mit der Probe „VMware - vCenter ESX-Hosts“ erfasst.

Daten zu eigenständigen ESXi-Servern

Discovery nutzt mehrere vorhandene Probes, um diese Daten von ESXi zu erfassen. Die Daten werden in verschiedenen Tabellen gespeichert. Einige der CIs, die über das Feld „Server“ verfügen, beinhalten einen Verweis auf den ESXi-Host (z. B. cmdb_ci_esx_server).

VMware-VM-Instanz [cmdb_ci_vmware_instance]

Feldbezeichnung	Spaltenname
Name	Name
Arbeitsspeicher (MB)	memory
CPUs	CPUs
Datenträger	disks

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

VMware-VM-Instanz [cmdb_ci_vmware_instance] (Fortsetzung)

Feldbezeichnung	Spaltenname
Netzwerkadapter	nics
Objekt-ID	object_id
Server	Server
Status	state
Zuordnungs-ID	correlation_id
VM-Instanz-UUID	vm_instance_uuid
Status	install_status

VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]

Feldbezeichnung	Spaltenname
Name	Name
Kapazität (GB)	Kapazität
Freier Speicherplatz (GB)	freespace
Zugänglich	accessible
Typ	Typ
Objekt-ID	object_id
Server	Server
URL	url
Status	install_status

VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]

Feldbezeichnung	Spaltenname
Name	Name
Objekt-ID	object_id
Server	Server
Status	install_status

VMware-Netzwerkadapter [cmdb_ci_vmware_nic]

Feldbezeichnung	Spaltenname
Name	Name
MAC-Adresse	mac_address
IP-Adresse	ip_address
Netzmaske	netmask
Configuration Item	cmdb_ci

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

VMware-Netzwerkadapter [cmdb_ci_vmware_nic] (Fortsetzung)

Feldbezeichnung	Spaltenname
Objekt-ID	object_id
MAC-Hersteller	mac_manufacturer
DHCP aktiviert	dhcp_enabled
Status	install_status

Host-Mount des VMware-Datenspeichers [vcenter_datastore_hostmount]

Feldbezeichnung	Spaltenname
VMware vCenter-Datenspeicher	datastore
ESX-Server	esx_server
Zugänglich	accessible
Zugriffsmodus	access_mode

Datenspeicher-Datenträger [cmdb_ci_vcenter_datastore_disk]

Feldbezeichnung	Spaltenname
Name	Name
Hersteller	manufacturer
Standort	location
Beschreibung	short_description
Klasse	sys_class_name
Aktualisiert	sys_updated_on
Wartungsplan	maintenance_schedule
Zuordnungs-ID	correlation_id
Datenspeicher	datastore
Status	install_status

ESX-Ressourcenpool [cmdb_ci_esx_resource_pool]

Feldbezeichnung	Spaltenname
Name	Name
CPU reserviert (MHz)	cpu_reserved_mhz
CPU limitiert (MHz)	cpu_limit_mhz
CPU Anteile	cpu_shares
Arbeitsspeicher reserviert (MB)	mem_reserved_mb
Arbeitsspeicher limitiert (MB)	mem_limit_mb
Speicheranteile	mem_shares

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

ESX-Ressourcenpool [cmdb_ci_esx_resource_pool] (Fortsetzung)

Feldbezeichnung	Spaltenname
Objekt-ID	object_id
Server	Server
Verwaltetes Objekt Referenz-ID	morid
Status	install_status

ESX-Server [cmdb_ci_esx_server]

Feldbezeichnung	Spaltenname
Name	Name
Hersteller	manufacturer
Modell-ID	model_id
Betriebssystem	os
BS-Version	os_version
Beschreibung	short_description
Klasse	sys_class_name
Status	install_status

Netzwerkadapter [cmdb_ci_network_adapter]

Feldbezeichnung	Spaltenname
Name	Name
Mac-Adresse	mac_address
Netzmaske	netmask
Configuration Item	cmdb_ci
MAC-Hersteller	mac_manufacturer
DHCP aktiviert	dhcp_enabled
Status	install_status

Datenträger [cmdb_ci_disk]

Feldbezeichnung	Spaltenname
Name	Name
Computer	Computer
Größe	size
Hersteller	manufacturer
Modell-ID	model_id
Status	install_status

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

Speicher-HBA [cmdb_ci_storage_hba]

Feldbezeichnung	Spaltenname
Name	Name
Modell-ID	model_id
Computer	Computer
WWNN	wwnn
Status	install_status

Fibre-Channel-Port [cmdb_ci_fc_port]

Feldbezeichnung	Spaltenname
Name	Name
WWNN	wwnn
WWPN	wwpn
Geschwindigkeit	speed
Controller	controller
Computer	Computer
Status	install_status

iSCSI-Datenträger [cmdb_ci_iscsi_disk]

Feldbezeichnung	Spaltenname
Name	Name
Computer	Computer
Größe	size
Bereitgestellt von	provided_by
IQN	iqn
Geräte-LUN	device_lun
Speichertyp	storage_type
Status	install_status

Fibre Channel-Datenträger [cmdb_ci_fc_disk]

Feldbezeichnung	Spaltenname
Name	Name
Computer	Computer
Größe	size
Bereitgestellt von	provided_by
Geräte-LUN	device_lun

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

Fibre Channel-Datenträger [cmdb_ci_fc_disk] (Fortsetzung)

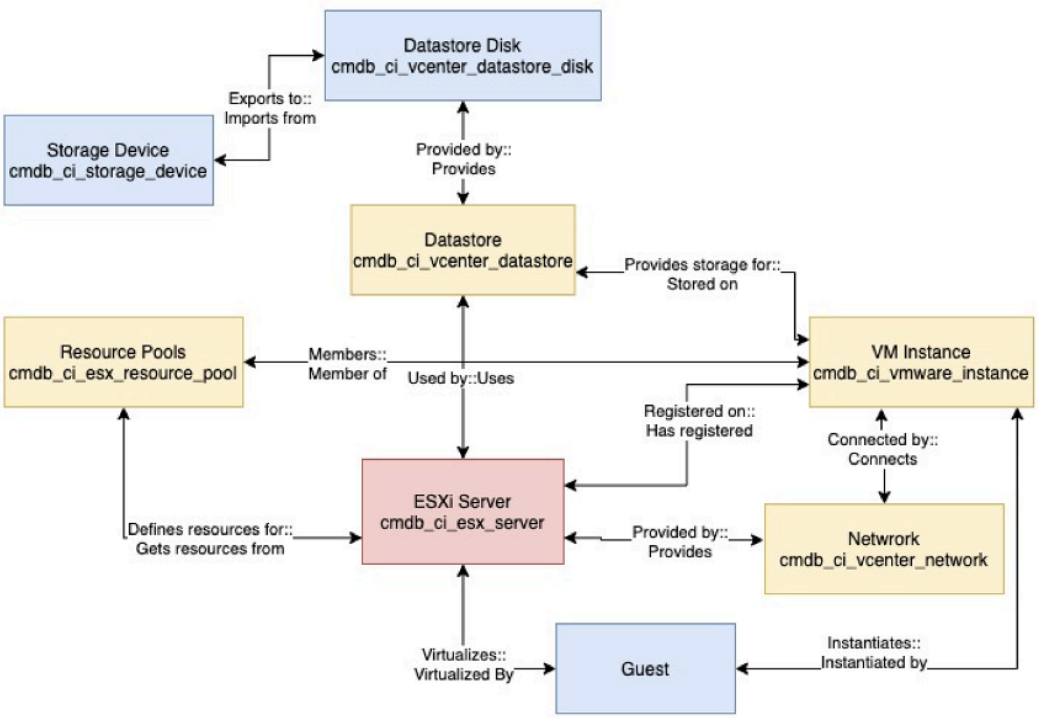
Feldbezeichnung	Spaltenname
WWN	wwn
Status	install_status

IP-Adresse [cmdb_ci_ip_address]

Feldbezeichnung	Spaltenname
IP-Adresse	ip_address
IP-Version	ip_version
Netzmaske	netmask
Nic	nic
Status	install_status

Beziehungen

Beziehungen bei der Erkennung eigenständiger ESXi-Server



Ressourcenpools

Bei der Erkennung eigenständiger ESXi-Server werden auch die Ressourcenpools auf dem Host abgerufen, einschließlich des Stammressourcenpools. Dieser Stammressourcenpool ist für jeden ESXi-Host immer ausgeblendet. Der Stammressourcenpool ist im vSphere-Webclient für den ESXi-Host möglicherweise nicht sichtbar, Sie können ihn jedoch mit dem MOB-Browser anzeigen.

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

Navigieren Sie zu dieser URL: **<domain name/or ip_address>/mob/?moid=ha-root-pool**.

Im Stammressourcenpool werden die Ressourcen des betreffenden Hosts gruppiert. Andere untergeordnete Ressourcenpools können auch aus dem Stammressourcenpool erstellt werden. Der Stamm wird auf dem ESXi-Host anhand der ID des verwalteten Objekts (ha-root-pool) identifiziert.

Zukunftssichere Migration

Wenn Sie die Erkennung eigenständiger ESXi-Server verwendet haben und derselbe ESXi-Server nun mit vCenter verwaltet wird, können Sie stattdessen die vCenter-Erkennung verwenden. Erstellen Sie einen vCenter-Discovery-Zeitplan, und lösen Sie diesen aus. Durch das Auslösen einer vCenter-Erkennung werden doppelte CIs in den folgenden Tabellen erstellt, da für eigenständige ESXi-Server und mit vCenter verwaltete ESXi-Server jeweils unterschiedliche Bezeichner für die betreffenden CIs verwendet werden:

- VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]
- ESX-Ressourcenpool [cmdb_ci_esx_resource_pool]
- VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]
- Datenspeicher-Datenträger [cmdb_ci_vcenter_datastore_disk]

Um Duplikate zu vermeiden, müssen Sie die von der Erkennung eigenständiger ESXi-Server erstellten CIs in den obigen vier Tabellen als „Deaktiviert“ markieren. Wenn die vCenter-Erkennung ausgelöst wird, prüft die Skripteinbindung vCenterESXHostsSensor für alle ESXi-Server, ob sie zuvor als eigenständige ESXi-Server erkannt wurden. Wenn ja, wird automatisch das Skript ESXMigrationUtil ausgelöst, sodass alle zuvor erkannten doppelten CIs als deaktiviert markiert werden.

Hinweis: Wenn Sie die Migration manuell auslösen möchten, führen Sie das folgende Skript aus dem Hintergrundskript aus: // @params esx_sys_ids – Array von sys-IDs aller ESXi-Server, die migriert werden müssen.

```
ESXMigrationUtil. retireCIsForESXForwardMigration(esx_sys_ids)
```

Sobald ein ESXi-Server zu vCenter migriert wurde, führt das Auslösen eines Discovery-Zeitplans für die Erkennung eigenständiger ESXi-Server auf demselben ESXi-Host zu einem Fehler. Die Erkennung wird mit einer Fehlermeldung abgebrochen, die besagt, dass dieser ESXi-Server Teil des Discovery-Zeitplans von vCenter <IP-Adresse von vCenter> ist und dass die Erkennung abgebrochen wird.

Virtuelle VMware-Computer

Discovery erfasst Informationen über virtuelle Computer, die von vCenter verwaltet werden.

Das Produkt Discovery kann Informationen aus VMware-Konfigurationselements (CIs) extrahieren, einschließlich ihrer Beziehungen. Discovery ist für den gemeinsamen Einsatz mit dem Plugin „Orchestration VMware Support“ konfiguriert, das das automatische Klonen von virtuellen Computern durch einen von vCenter verwalteten ESX-Server ermöglicht. Informationen zu Daten, die von Discovery in vCenter erfasst werden, finden Sie unter Für VMware vCenter-Server erfasste Daten.

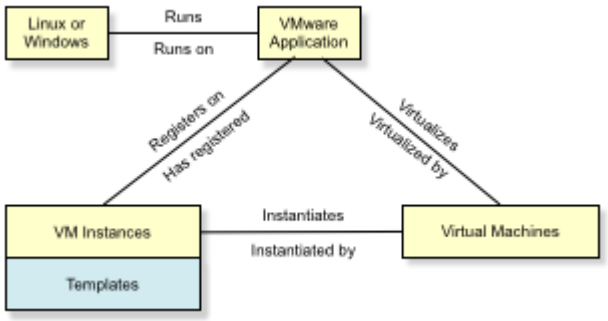
VMware-Workstation – Veraltet

Im VMware-Basissystem wird die VMware-Workstation auf einem Windows- oder Linux-Hostcomputer ausgeführt.

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

Dieses System kann Instanzen aus Vorlagen klonen, lässt sich jedoch nicht automatisieren. Die Beziehungen zwischen VMware-Komponenten für diesen Installationstyp sind im folgenden Diagramm dargestellt:

Beziehungen der VMware-Workstation



Beziehungen von Komponenten der VMware-Workstation

Komponente	Beziehungen
Windows- oder Linux-Server	Führt die VMware-Anwendung aus
VMware-Anwendung	• Wird auf einem Windows- oder Linux-Hostcomputer ausgeführt • Besitzt registrierte VM-Instanzen • Virtualisiert virtuelle Computer
VM-Instanzen (einschließlich Images und Vorlagen)	• Wird bei der VMware-Anwendung registriert • Wird von einzelnen virtuellen Computern instanziiert
Virtuelle Computer	• Instanziiert VM-Instanzen • Wird durch die VMware-Anwendung virtualisiert

Felder „Status“ und „Status“ der VM-Instanz

Diese Tabellen stellen den Status und Status von cmdb_ci_vm_instance in verschiedenen Flows dar, z. B. vCenter Discovery und vCenter Events sowie die Geschäftsregeln, die ausgelöst werden.

vCenter Discovery, das verschiedene Status und Statusfelder im Zusammenhang mit der VM-Instanz ändert

Quelle	Skript- oder Ereignisname	Feldname	Vorheriger VM-Status	Neuer VM-Status
vCenter Discovery	VCenterVMsSensor	Installationsstatus	Deaktiviert	Installiert
vCenter Discovery	vCenterDatacentersSensor	Installationsstatus Status	Installiert	Deaktiviert Beendet

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

vCenter Discovery, das verschiedene Status und Statusfelder im Zusammenhang mit der VM-Instanz ändert (Fortsetzung)

Quelle	Skript- oder Ereignisname	Feldname	Vorheriger VM-Status	Neuer VM-Status
		Betriebsstatus		Nicht funktionsfähig

vCenter-Ereignisse, die verschiedene Status und Statusfelder im Zusammenhang mit der VM-Instanz ändern

Quelle	Skript- oder Ereignisname	Feldname	Vorheriger VM-Status	Neuer VM-Status
vCenter-Ereignisse	vCenterVmStateUpdater PowerOnEvtsToUse = ['VmPoweredOffEvent', 'VmPowerOffOnIsolationEvent', 'VmSturdownOnIsolationEvent', 'VmAnhaltedEvent'],	Status „Installiert“. Status	Installiert Beliebig	Installiert EIN
vCenter-Ereignisse	PowerOffEvtsToUse = ['VmPoweredOnEvent', 'DrsVmPoweredOnEvent', 'VmRestartedOnAlterateHostEvent', 'VmAnhaltedEvent'],	Status „Installiert“. Status	Installiert Beliebig	Installiert AUS
vCenter-Ereignisse	ausgesetztEvtsToUse = ['VmPoweredOnEvent', 'DrsVmPoweredOnEvent', 'VmRestartedOnAlternatHostEvent', 'VmPoweredOffEvent', 'VmPowerOffOnIsolationEvent']	Status „Installiert“. Status	Installiert Beliebig	Installiert Angehalten
vCenter-Ereignisse	VmRemovedEvent	Status „Installiert“. Status	Installiert Beliebig	Deaktiviert Beendet

Business-Regeln, die verschiedene Status und Statusfelder im Zusammenhang mit der VM-Instanz und dem zugehörigen Server ändern

Business-Regel	Feldname	Plugin-Name
Betriebsstatus auf Server kaskadieren	Betriebsstatus	Musterdesigner
Kaskadieren Sie den Betriebsstatus an die VM-Instanz	Betriebsstatus	Musterdesigner

Automatische Übersetzung

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

Business-Regeln, die verschiedene Status und Statusfelder im Zusammenhang mit der VM-Instanz und dem zugehörigen Server ändern (Fortsetzung)

Business-Regel	Feldname	Plugin-Name
Synchronisierungsvorgangsstatus für CMDB-CI	Betriebsstatus Hardwarestatus Installationsstatus	CMDB

Erkennung von Datenspeicher

Ein Datenspeicher ist ein Speicherobjekt für virtuelle Computer, die auf einem ESXi-Server gehostet werden.

Ein Datenspeicher ist eine Sammlung von mindestens einem physischen Datenträger, zum Beispiel einem iSCSI-Datenträger, die von mehr als einem ESXi-Host verwendet werden kann. Ein physischer Datenträger kann jedoch nur eine Verbindung zu maximal einem Datenspeicher herstellen. Da Datenspeicher von ESXi-Hosts gemeinsam genutzt werden können, lässt sich der virtuelle Computer problemlos zwischen Hosts mit gemeinsamem Datenspeicher verschieben.

Hinweis: Aus der Perspektive eines virtuellen Computers, der an einen Datenspeicher angehängt ist, wird Speicher von einem einzelnen Datenträger bereitgestellt.

Die Verbindung eines Datenspeichers mit mehreren Datenträgern bietet folgende Vorteile:

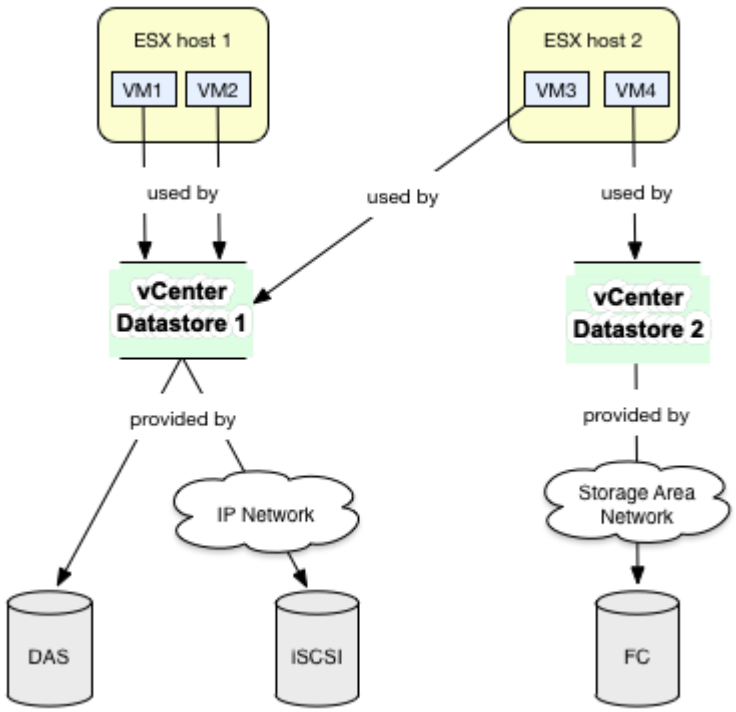
- Die Möglichkeit, die Datenträger zum Failover-Schutz zu spiegeln
- Das einfache Hinzufügen von Speicher zum Datenspeicher

Informationen über die Tabellen, die in Discovery zum Speichern der Daten für physische Datenträger und ihrer Beziehung zu Datenspeichern und ESXi-Hosts verwendet werden, finden Sie unter Erkennung von ESXi-Servern.

In dieser Beispielkonfiguration nutzen zwei ESXi-Hosts einen gemeinsamen Datenspeicher, der verschiedene Speichertypen verwendet.

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

Erkennung von Datenspeicher mit unterschiedlichen Speichertypen



Beziehungen

ServiceNow stellt Tabellen bereit, die die Beziehungen zwischen einem ESXi-Host und seinem Datenspeicher und den spezifischen Datenträgern enthalten, mit denen der Datenspeicher verbunden ist.

ServiceNow Discovery erkennt die Beziehungen zwischen einem Datenspeicher, den mit dem Datenspeicher verbundenen Datenträgern und dem ESXi-Server, auf dem die virtuellen Computer gehostet werden, die diesen Datenspeicher nutzen. Aus der Perspektive des ESXi-Hosts werden iSCSI- und Fibre Channel-Datenträger, die mit dem Datenspeicher verbunden sind, als physische Datenträger behandelt. Discovery zeigt nicht die direkte Beziehung der Speicherdatenträger zum ESX-Host an.

Hinweis: Speicher kann auf Computern gehostet werden, die nicht von Discovery erkannt werden. ESXi-Hosts werden über vCenter erkannt, und Speicher wird über CIM separat erkannt. Die Beziehung zwischen beiden kann nur hergestellt werden, wenn der Speicher vor dem ESXi-Host erkannt wird.

Datenspeichertabellen

Tabelle	Beschreibung
cmdb_ci_vcenter_datastore_disk	Speichert die Beziehung des physischen Datenträgers zum Datenspeicher
vcenter_datastore_hostmount	Speichert die Beziehung zwischen dem Datenspeicher und dem ESXi-Server, mit dem er verbunden ist
cmdb_ci_disk	Enthält die physischen Datenträger, die direkt mit dem Datenspeicher verbunden sind Diese Tabelle enthält auch einen Verweis auf den ESXi-Host.
cmdb_ci_fc_disk	Enthält die Fibre Channel-Datenträger in einem Storage Area Network (SAN), das mit dem Datenspeicher

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

Datenspeichertabellen (Fortsetzung)

Tabelle	Beschreibung
	verbunden ist Diese Tabelle enthält auch einen Verweis auf den ESXi-Host.
cmdb_ci_iscsi_disk	Enthält die iSCSI-Datenträger in einem IP-Netzwerk, das mit dem Datenspeicher verbunden ist Diese Tabelle enthält auch einen Verweis auf den ESXi-Host.

Erkennung von Windows

Discovery identifiziert und klassifiziert Informationen über Computer Windows, die IPv4-Adressen und/oder IPv6-Adressen verwenden.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Hinweis: Für die Erkennung von Windows ab Madrid P3 und höher ist der Freigabezugriff admin$ erforderlich.

Unterstützte Versionen Windows.

Für IPv4-Erkennung:

- Windows Arbeitsplatzrechner 7, 8, 10
- Windows Serverversionen:
  - 2008
  - 2008R2
  - 2012R2
  - 2016
  - 2019
  - 2022

Für IPv6-Erkennung:

- Windows 2019 (10.0.17763)
- Windows Server 2016
- Windows Desktop 10
- Windows 2019 Datacenter

Hinweis: Für die Fibre Channel-Discovery auf einem Windows 2008-Host muss das Microsoft Fibre Channel Information Tool (`fcinfo.exe`) auf diesem Computer installiert sein. Die ausführbare Datei `fcinfo` muss im Umgebungspfad verfügbar sein. Das Microsoft-Informationstool für Fibre Channel kann unter http://www.microsoft.com heruntergeladen werden.

Einschränkungen der IPv6-Unterstützung

Die folgenden Gerätetypen wurden nicht für die IPv6-Erkennung überprüft:

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

- Drucker
- Netzwerkspeicher (NFS, CIFS, NAS, FC, ISCSI)
- Virtuelle Azure-Computer (Der native IPv6-Modus wird von Microsoft nicht unterstützt.)

PowerShell-Anforderungen

ServiceNow bietet jetzt Unterstützung für PowerShell 3.0 bis 5.1.

Anmeldeinformationen

Konfigurieren Sie die Windows-Anmeldeinformationen . Der in den Anmeldeinformationen konfigurierte Benutzer muss lokalen Administratorzugriff auf den Computer Windows haben.

Die von Ihnen konfigurierten Anmeldeinformationen benötigen:

- Zugriff auf den WMI-Service für den aktuellen Namespace und die untergeordneten Namespaces
- Zugriff auf den Powershell-Service
- Mitgliedschaft in der lokalen Sicherheitsgruppe „Distributed COM-Benutzer“

Klassifizierer, Probes und Muster

Klassifizierungen	Probes	Muster
• Windows • Windows 2008-Server • Windows 2012-Server • Windows Server 2016	• Probe „Horizontal Discovery“: Startet Muster • WMIRunner-Windows - Installed Software^ • Multi-Probe-Windows - ADM^ • Windows - Identity* • Windows - Network ARP Table* • Windows - Network NDP Table* • Windows - OS Information* • Windows - Cluster* • Windows - CPU/Memory* • Windows - Installed Software* • Windows - Printers* • Windows - Storage 2008* • Windows - Storage 2012* • Windows - Amazon EC2* • Windows - Azure*	• Windows OS - Server • Windows OS - Desktops

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

Klassifizierungen	Probes	Muster
	• DNS* • SNMP - Routing*	
Windows Server 2019	N/V	Windows OS - Server

*Diese Probes sind für die Klassifizierung nicht aktiv, da Discovery standardmäßig Muster für diese Erkennungen verwendet.

^Diese Probes bleiben standardmäßig aktiv, auch wenn Discovery die Muster-Discovery verwendet.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Bezeichnung	Tabellenname	Feldname	Quelle
Zugewiesen an	cmdb_ci_win_server	assigned_to	wmi
Gehäusetyp	cmdb_ci_win_server	chassis_type	wmi
Befehl	cmdb_running_process	command	wmi
Verbunden mit	cmdb_running_process	connects_to	wmi
Anzahl CPU-Kerne*	cmdb_ci_computer	cpu_core_count	wmi
CPU-Kern-Thread*	cmdb_ci_computer	cpu_core_thread	wmi
CPU-Anzahl*	cmdb_ci_computer	cpu_count	wmi
CPU-Hersteller	cmdb_ci_computer	cpu_manufacturer	wmi
CPU-Name	cmdb_ci_computer	CPU-Name	wmi
CPU-Geschwindigkeit (MHz)	cmdb_ci_computer	cpu_speed	wmi
Standard-Gateway	cmdb_ci_win_server	default_gateway	wmi
Beschreibung	cmdb_ci_disk	short_description	wmi
Festplattenspeicher (GB)	cmdb_ci_computer	disk_space	wmi
Festplattenspeicher (GB)	cmdb_ci_disk	disk_space	wmi
DHCP-fähig	cmdb_ci_network_adapter	dhcp_enabled	wmi
DNS-Domäne	cmdb_ci_win_server	dns_domain	DNS
Freier Speicherplatz (GB)	cmdb_ci_file_system	free_space	wmi
Hostname	cmdb_ci_win_server	host_name	DNS, NBT
IP-Adresse	cmdb_ci_network_adapter	ip_address	wmi
Lauschen auf	cmdb_running_process	listening_on	wmi

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

Bezeichnung	Tabellenname	Feldname	Quelle
MAC-Adresse	cmdb_ci_network_adapter	mac_address	wmi
Hersteller	cmdb_ci_win_server	manufacturer	wmi
Modell-ID	cmdb_ci	model_id	wmi
Name	cmdb_ci_win_server	Name	DNS, NBT
Name	cmdb_ci_disk	Name	wmi
Name	cmdb_running_process	Name	wmi
Name	cmdb_ci_network_adapter	Name	wmi
Netzmaske	cmdb_ci_network_adapter	netmask	wmi
Betriebssystem	cmdb_ci_computer	os	wmi
BS-Domäne	cmdb_ci_computer	os_domain	NBT
BS-Service Pack	cmdb_ci_computer	os_service_pack	wmi
BS-Version	cmdb_ci_computer	os_version	wmi
Parameter	cmdb_running_process	parameters	wmi
PID	cmdb_running_process	pid	wmi
RAM (MB)	cmdb_ci_computer	ram	wmi
Seriennummer	cmdb_ci_win_server	serial_number	wmi
Kurzbeschreibung	cmdb_ci_win_server	short_description	wmi
Typ	cmdb_ci_disk	Typ	wmi

* Die Angaben für Anzahl der Kerne und Threads pro Kern sind aufgrund von Problemen mit der Microsoft-Berichterstellung möglicherweise nicht genau.

** Der Wert im Feld **disk_space** ist eine Zusammenfassung der Gesamtkapazität (einschließlich belegtem Platz) für alle nicht entnehmbaren Festplatten, einschließlich Direct Attached Storage und SAN-Speicher.

Windows-Registrierung

Discovery können Software finden, die auf einem Windows-Computer installiert wurde, indem Sie in der Windows-Registrierung suchen. Discovery kann die folgenden Attribute von erkannter Software finden:

- **Produktname**: Kombination aus Name und Version, zum Beispiel Windows Imaging Component 3.0
- **Name**: Name des Produkts ohne Version
- **Version**: Version des Produkts
- **Deinstallationszeichenfolge**: Pfad zum Deinstallationsprogramm, zum Beispiel `C:\Programme\Notepad ++\uninstall.exe`.
- **Teil von**: Update, von dem dies ein Teil ist, zum Beispiel Windows Internet Explorer 8 - Software Update
- **Installationsdatum**: Datum, an dem die Software installiert wurde Der Sensor „Windows - Installierte Software“ wendet einen Zeitstempel von 00:00:00 auf den in der Registrierung abgerufenen Wert „install_date“ ab. Die Installationszeit aller Windows -Software ist unabhängig von der Zeitzone und wird auf Mitternacht des Tages festgelegt, an dem sie

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

installiert wurde. Beispiel: Ein Installationsdatum von **2.19.2017** in der Registrierung Windows wird im Fenster CMDBals **2.19.2017 00:00:00** angezeigt.

- **Installiert auf**: Name des Asset, auf dem die Software installiert ist

Zugehörige Informationen

Windows Probes und Berechtigungen

Erkennung von Windows-Serverclustern

Discovery stellt die Beziehungen zwischen einem Windows -Servercluster und seinen Knoten her.

Wenn ein Windows -Server gefunden wird und Discovery erkennt, dass er Teil eines Clusters ist, startet das System die Windows – Cluster-Probe. Navigieren zu **Discovery-Definition** > **Probes** und öffnen Sie den Datensatz für die Windows-Cluster-Probe, um die spezifischen Daten anzuzeigen, die Discovery sammelt.

Hinweis: Discovery sammelt Clusterressourcen basierend auf der WMI-Klasse MSCluster_ResourceType. Eine Liste der standardmäßigen Clusterressourcen finden Sie unter Ressourcentypen . Informationen zum Zusammenhang von Clusterressourcen mit Prozessklassifizierern finden Sie unter Prozessklassifizierer mit Windows-Clusterressourcen verknüpfen.

Clusterdatentabellen

Discovery erstellt CIs für Cluster in diesen Tabellen:

- Windows Cluster [cmdb_ci_win_cluster]
- Windows Clusterressource(n) [cmdb_ci_win_cluster_resource]
- Windows Cluster-Knoten [cmdb_ci_win_cluster_node]
- Clusterknotenressourcen [cmdb_ci_cluster_node_resource]
- Virtuelle IPs des Clusters [cmdb_ci_cluster_vip]

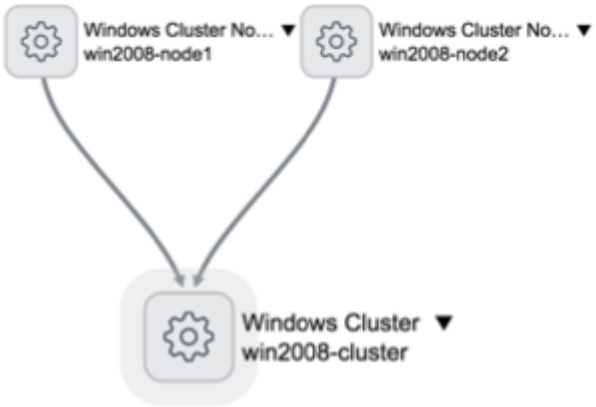
Clusterbeziehungen

Discovery erstellt für jeden Knoten einen CI-Beziehungsdatensatz [cmdb_rel_ci] mit den folgenden Beziehungen:

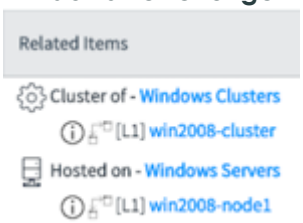
- **Cluster von::Cluster**: Beziehung zwischen den Clusterknoten und dem Cluster. Service Mapping verwendet diese Beziehung, um das Windows-Cluster und seine Knoten zuzuordnen.
- **Mitglieder::Mitglied von**: Beziehung zwischen dem Cluster und dem Clusterknoten
- **Gehostet auf::Hostet**: Beziehung zwischen den Clusterknoten und dem Windows-Server
- **Verwendet::Verwendet von**: Cluster VirtualIP und Windows-Clusterknoten.
- **Definiert Ressourcen für::Erhält Ressourcen von**: Windows Cluster-Ressourcen und Windows Cluster.
- **Definiert Ressourcen für::Erhält Ressourcen von**: Windows Cluster-Ressourcen und Windows Cluster-Knoten.

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

Windows Clusterzuordnung



Windows Beziehungen mit Clusterknoten



Clusterreferenzen

Discovery erstellt die folgenden Clusterreferenzen:

- Von Windows -Clusterknoten zum zugeordneten Windows -Cluster.
- Von Windows -Clusterressourcen zum zugeordneten Windows -Cluster
- Von virtuellen Cluster-IPs zum zugeordneten Windows -Cluster.
- Von Cluster-Knotenressourcen zum zugeordneten Windows -Clusterknoten.
- Von virtuellen Cluster-IPs zum zugeordneten Windows -Clusterknoten.

Hinweis: Referenzen werden in Discovery verwaltet, um die Abwärtskompatibilität für Systeme zu gewährleisten, die sie verwenden.

z/OS-Erkennung

Discovery sucht nach Computern, auf denen das Betriebssystem z/OS ausgeführt wird.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Anforderungen

Unter z/OS muss an Port 22 der USS-Service ausgeführt werden.

Die folgenden Befehle können auf dem Hostcomputer ausgeführt werden:

- uname
- hostname
- sysvar SYSNAME
- netstat
- df

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

- ls
- cat
- grep
- ps
- cut

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Anmeldeinformationen

Erstellen Sie SSH-Anmeldeinformationen . Der Anwender muss zum Schreiben in `/tmp`berechtigt sein, Lesezugriff auf alle Anwenderprozesse haben und REXX-Skripts ausführen können.

Klassifizierer, Probe und Muster

Klassifizierung	Auslöser-Probe	Muster
IBM z/OS	Horizontal Pattern: Startet Muster	IBM zOS Server

Erfasste Daten

Discovery füllt die Tabelle „IBM zOS-Server“ [cmdb_ci_ibm_zos_server] mit folgenden Informationen:

Bezeichnung	Feldname
Name	Name
BS-Version	os_version
Betriebssystem	os
Hersteller	manufacturer
Seriennummer	serial_number

Erkennung der Virtualisierung auf Betriebssystemebene (OSLV, Operating-System-Level Virtualization)

Discovery kann Image- und Containerinformationen von OSLV-Engines erfassen.

Discovery kann Containerstatus und -größe bestimmen sowie Images und deren Tags identifizieren, die durch Virtualisierung auf Betriebssystemebene bereitgestellt werden.

Hinweis: Derzeit unterstützt die ServiceNow® Platform nur die Erkennung von Docker-Virtualisierungscontainern.

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

Tabellenschema

Tabelle	Beschreibung
cmdb_ci_oslv_engine	Basistabelle für alle OSLV-Engines
cmdb_ci_oslv_image	Basistabelle für global eindeutige OSLV-Images
cmdb_ci_oslv_local_image	Basistabelle für lokale Instanzen von OSLV-Images
cmdb_ci_oslv_image_tag	Basistabelle für Tags in OSLV-Images
cmdb_ci_oslv_container	Basistabelle zum Speichern von auf dem Host gefundenen Containern

Erfasste Daten

Tabelle	Felder
Virtualisierungs-Engine auf Betriebssystemebene [cmdb_ci_oslv_engine]	Server [Server]
Virtualisierungs-Image auf Betriebssystemebene [cmdb_ci_oslv_image]	• Image-ID [image_id] • Image-Auszug [image_digest] • Image erstellt [image_created_at] • Größe (Byte) [size_bytes]
Lokales Image der Virtualisierung auf Betriebssystemebene [cmdb_ci_oslv_image]	Image-ID [image_id]
Image-Tag für Virtualisierung auf Betriebssystemebene [cmdb_ci_oslv_image_tag]	• Image-ID [image_id] • Repository [repository] • Tag [tag]
Container der Virtualisierung auf Betriebssystemebene [cmdb_ci_oslv_container]	• Container-ID [container_id] • Status [status] • Größe (Byte) [size_bytes] • Image-ID [image_id]

Docker-Virtualisierung

Discovery verwendet das *Docker Pattern*, um Daten über bestimmte Objekte in einer Docker-Engine zu erfassen, die auf einem Linux-Host ausgeführt wird.

Die ServiceNow® Platform unterstützt die Erkennung von Docker Release 1.11.0 oder höher.

Discovery führt den Prozessklassifizierer „Docker Engine“ im Netzwerk aus. Wenn der Klassifizierer den Prozess **dockerd** oder **docker daemon** identifiziert, löst der Klassifizierer die

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

Probe „Horizontal Pattern“ (HorizontalDiscoveryProbe) aus, die das Muster „Docker“ startet und mit dem Erfassen von Daten aus Docker-Komponenten beginnt.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Voraussetzungen

Benutzerrechte

Der Benutzer, dessen Anmeldeinformationen zum Ausführen der Docker Discovery verwendet werden, muss über Berechtigungen verfügen, die mit einer der folgenden Methoden definiert wurden:

- Erteilen Sie einem Benutzer erweiterte Rechte für die Ausführung von Befehlen, da der Docker-Daemon als Root-Benutzer ausgeführt wird. Das Docker-Muster unterstützt die Verwendung privilegierter Befehle wie *sudo* oder *pbrun*zur Ausführung als Root-Benutzer.
- Zuweisung zu einer Gruppe mit dem Namen **docker**, die über besondere Berechtigungen zum Ausführen von Docker-Befehlen verfügt. Anweisungen zum Einrichten einer Gruppe finden Sie in der Dokumentation zu Docker .

Neueste Muster

Stellen Sie die aktuelle Anwendung „Discovery and Service Mapping Patterns“ aus dem ServiceNow Store bereit.

Einschränkungen und Überlegungen für Docker

Beachten Sie bei Verwendung der Docker-Virtualisierung Folgendes:

- Der erste Prozess-Scan von Discovery kann eine Anwendung in einem Container identifizieren und korrekt klassifizieren. Nachfolgende Probes, die gestartet werden, um die Anwendung zu untersuchen, können jedoch nicht in den Container sehen und keine Details zur Anwendung zurückgeben.
- Discovery durchsucht alle gefundenen Container, einschließlich inaktiver Container. Dadurch kann Discovery verlangsamt werden. Daher sollten Sie nicht ausgeführte Container löschen.
- Bevor Sie die Eigenschaft *„sn_itom_pattern.manifest_digest_image_id"*auf **„wahr“** festlegen und Discovery ausführen: Verhindern Sie die Erstellung von doppelten Docker -Datensätzen, indem Sie alle Docker -Bilddatensätze löschen.
- Pro (physischem oder virtuellem) Computer ist nur eine Docker-Engine zulässig.

Von Discovery während der horizontalen Erkennung erfasste Daten

Zusätzlich zu den aus den übergeordneten OSLV-Tabellen abgeleiteten Attributen werden die folgenden Attribute erkannt.

Tabelle und Felder	Beschreibung
Docker-Engine [cmdb_ci_docker_engine]	
Name [name]	Speichert Informationen zu Instanzen der Docker-Engine.
BS-Architektur [os_arch]	
GIT-Commit [git_commit]	

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

Tabelle und Felder	Beschreibung
Erstellungsdatum [build_date]	
Version [version]	
API-Version [api_version]	
Go-Version [go_version]	
Ist geclustert [is_clustered]	
Laufender Prozess [running_process]	
Befehl für laufenden Prozess [running_process_command]	
Schlüsselparameter des laufenden Prozesses [running_process_key_parameters]	
Docker-Image [cmdb_ci_docker_image]	
Name [name]	Speichert Informationen zur global eindeutigen Darstellung von Docker-Images.
Image-ID [image_id]	
Image-Auszug [image_digest]	
Größe (Byte) [size_byte]	
Bild erstellt [Image_created_at]	
Lokales Docker-Image [cmdb_ci_docker_image]	
Name [name]	Speichert lokale Instanzen von Docker-Images
Image-ID [image_id]	
Docker-Image-Tag [cmdb_ci_docker_image_tag]	
Name [name]	Speichert Tags aus lokalen Docker-Images
Image-ID [image_id]	
Repository [repository]	
Tag [tag]	
Docker-Container [cmdb_ci_docker_container]	
Name [name]	Speichert Docker-Container, die auf dem Host gefunden wurden In Fällen, in denen doppelte Datensätze erstellt werden, werden Deduplizierungsaufgaben angezeigt, sobald Discovery ausgeführt wird. Informationen zur Lösung dieser Aufgaben finden Sie im Artikel Docker-Container-Bezeichner unabhängig machen [KB1443042] in der ServiceNow® Knowledge Base.
Image-ID [image_id]	
Container-ID [container_id]	
Größe (Byte) [size_bytes]	
Befehl [command]	
Container erstellt [container_created_at]	
Status [status]	

Diese Informationen werden vom Erweiterungsabschnitt *`Collect Container Repository`* erkannt.

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

Tabelle und Feld	Beschreibung
Container-Repository [cmdb_ci_container_repository]	
Name [name]	Der Name des Container-Repositorys.
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]	
Name [name]	Der Name des Container-Repository-Eintrags.
Kategorie [category]	Die Kategorie des Container-Repository-Eintrags.

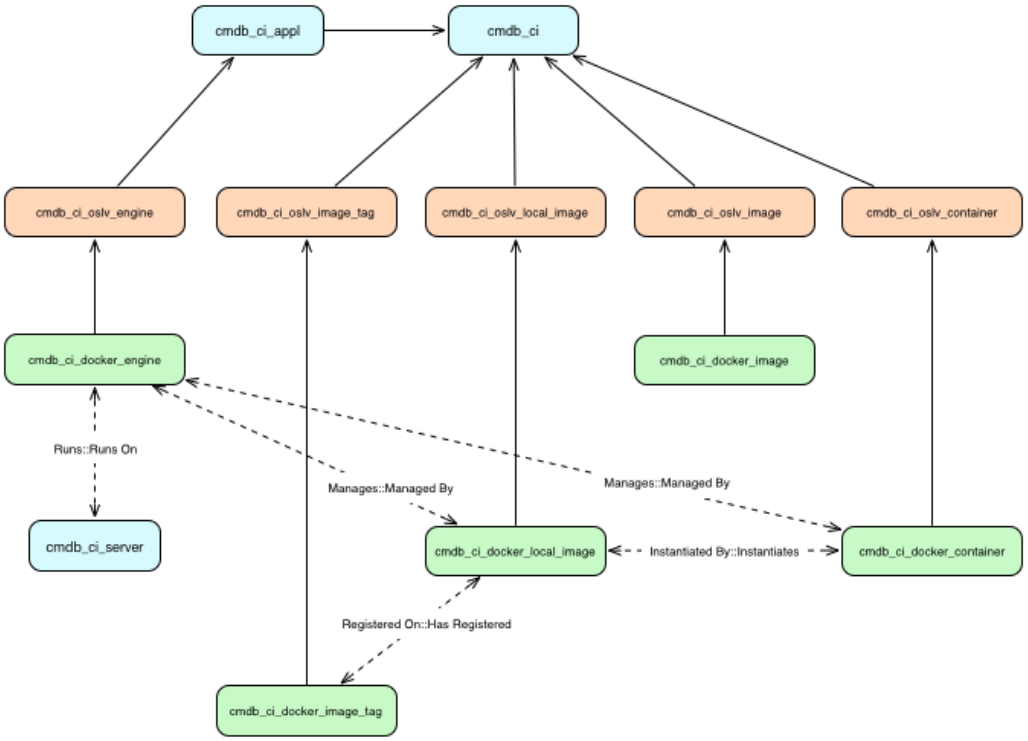
CI-Beziehungen

Die folgenden Beziehungen zwischen erkannten CIs werden vom Docker-Muster identifiziert.

CI	Beziehung	CI
cmdb_ci_server	Runs::Runs On	cmdb_ci_docker_engine
cmdb_ci_docker_engine	Manages::Managed By	cmdb_ci_docker_container
cmdb_ci_docker_engine	Verwaltet::Verwaltet Von	cmdb_ci_docker_local_image
cmdb_ci_docker_image	Instanziiert::Instanziiert Von	cmdb_ci_docker_container
cmdb_ci_docker_local_image **Hinweis:** Die Richtung dieser Beziehung ist für alle Store-Versionen vor 1.0.99, Februar 2023, umgekehrt.	Instanziiert::Instanziiert Von	cmdb_ci_docker_container
cmdb_ci_docker_image_tag	Registriert am::Hat registriert	cmdb_ci_docker_local_image
cmdb_ci_docker_local_image	Instantiates::Instantiated By	cmdb_ci_docker_image

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

Über- und untergeordnete Beziehungen für abhängige OSLV- und Docker-Tabellen



Der Erweiterungsabschnitt *Collect Container Repository* des Docker-Musters identifiziert diese Beziehungen.

CI	Beziehung	CI
Docker-Image [cmdb_ci_docker_image]	Bereitgestellt von::Bereitgestellt	Container-Repository-Eintrag [cmdb_ci_container_repository_entry]
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]	Gehostet auf::Hostet	Container-Repository [cmdb_ci_container_repository]

Identifizierungs-, Containment- und Hosting-Regeln

Discovery verwendet für die Suche nach der Docker-Engine einen Bezeichner für Anwendungsregeln und wendet dann andere Regeln an, um bestimmte Docker-Objekte zu identifizieren.

Bezeichner für Anwendungsregeln

Das System erstellt während der Prozessklassifizierung das Konfigurationselement (CI) cmdb_ci_docker_engine. Darauf aufbauend, verwendet Discovery den Bezeichner der Anwendungsregel in der Anwendungstabelle [cmdb_ci_appl], um die spezifische Docker-Engine zu identifizieren. Nach der Herstellung dieser Identität verwendet Discovery die Beziehungen, die in den Containment- und Hosting-Regeln definiert sind, um die einzelnen CIs der Docker-Komponente, die zu dieser Engine gehören, genau zu erstellen und zu aktualisieren.

Kennungen

Automatische Übersetzung

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

Name	Tabelle	Attribute
Docker-Container	Docker-Container [cmdb_ci_docker_container]	container_id
Globales Docker-Image	Docker-Image [cmdb_ci_docker_image]	image_id
Lokales Docker-Bild	Lokales Docker-Image [cmdb_ci_docker_image]	image_id
Docker-Bild-Tag	Docker-Image-Tag [cmdb_ci_docker_image_tag]	Repository, Tag

Containment- und Hosting-Regeln

Docker-Discovery verwendet diese Regeln zum Erstellen oder Bearbeiten einer Sammlung von Containment-Regeln und zum Erstellen oder Bearbeiten einer Sammlung von Hosting- Regeln, um Configuration Items (CI) aus den vom Docker-Muster zurückgegebenen Datenundzu erstellen. Nachdem Discovery die Docker-Engine anhand ihrer Beziehung zur Anwendungstabelle [cmdb_ci_appl] identifiziert hat, werden diese Regeln angewendet, um die spezifischen CIs, die mit dieser Engine verbunden sind, anhand ihrer Beziehungen zueinander zu identifizieren. Indem die Komponenten auf diese Weise (von der Anwendung nach unten, ausgehend von der Engine) verbunden werden, verhindert Discovery, dass doppelte CIs für Komponenten aus anderen Docker-Engines erstellt werden, die denselben Namen oder dieselbe image_id aufweisen.

Containment-Regel

Übergeordnet	Untergeordnetes Element	Beziehung
Lokales Docker-Bild	Docker-Bild-Tag	Hat sich registriert

Hosting-Regeln

Übergeordnet	Untergeordnetes Element	Beziehung
Docker-Container	Docker-Engine	Verwaltet von
Lokales Docker-Bild	Docker-Engine	Verwaltet von

Erkennung von Software

Discovery identifiziert mehrere Arten von Software.

Erkennung des Active Directory-Domänencontrollers

Die Anwendung Muster für Discovery und Service-Mapping verwendet das Muster „Active Directory-Domänencontroller unter Windows“, um Active Directory-Domänencontroller zu finden, die auf einem Windows -Server ausgeführt werden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

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

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das Muster „Active Directory-Domänencontroller unter Windows“ ausgeführt wird.

Active Directory-Domänencontroller [cmdb_ci_ad_controller]

Bezeichnung	Feldname
Name	name
Domänenname	domain_name
Domänencontrollername	domain_controller_name
Forest-Name	„forest_name“
Klasse	sys_class_name
TCP-Port(s)	tcp_port

Erkennung von Adobe JRun

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz von Adobe JRun erkannt wird.

Standardmäßig verwendet Discovery das Muster *Jrun*, um Discovery auszuführen.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Privilegierte Befehle

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Für Adobe JRun erfasste Daten

In der JRun-Tabelle `[cmdb_ci_app_server_jrun]` werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Version	Version
Installationsverzeichnis	install_directory
Konfigurationsverzeichnis	config_directory
Konfigurationsdatei	config_file

Erkennung von Apache-Webservern

Discovery identifiziert und klassifiziert Informationen über Apache-Webserver auf Windows- und Linux-Computern.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

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

Anmeldeinformationen

- Applicative-Anmeldeinformationen
- Windows-Anmeldeinformationen
- SSH-Anmeldeinformationen

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
Apache-Server	• Probe „Horizontal Discovery“: Startet Muster • Apache - Version* • Apache - Get Configuration* • Apache - Get JK ModuleApache - Get Proxy Module*	• Apache On Windows • Apache On Unix

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Mit Probes erfasste Daten

Für Unix und Windows erfasst Discovery in der Apache-Tabelle [cmdb_ci_apache_web_server] die folgenden Daten:

Bezeichnung	Feldname
Name	Name
Version	Version
Beschreibung	Beschreibung
TCP-Port(s)	tcp_port

Verbindungen, die von Service-Mapping während der Erkennung von oben nach unten gefunden werden

Service-Mapping verwendet Erkennungsmuster, um die folgenden Verbindungen zu erkennen:

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

- Alle Anwendungen, die Java verwenden
- Alle Anwendungen, die den LDAP-Port verwenden
- Oracle WebLogic-Modul und Oracle WebLogic Server (Version 10.3)
- (Nur unter Windows) Jiva-Anwendungen
- (Nur unter Windows) Tomcat-Server
- (Nur unter UNIX) Mit dem mod_jk-Prozess erkannte Anwendungen
- (Nur unter UNIX) Hosts, zu denen der Apache-Webserver eine Verbindung im Lastenausgleichsmodus herstellt
- (Nur unter UNIX) Anwendung Epic

Erkennung der Apache-Connectors mod_jk und mod_proxy

Discovery verwendet SSH für die Suche nach den Apache-Connectors mod_jk und mod_proxy.

Discovery verwendet die Probe **Unix - Active Processes**, um durch den Abgleich mit den folgenden Kriterien einen Apache-Webserverprozess zu identifizieren: Der **Name** des Prozesses lautet:

- `httpd` oder
- `apache` oder
- `httpd2` oder
- `httpd2-prefork`
- `httpd.worker`

Wenn für eines dieser Kriterien eine Übereinstimmung vorliegt, wird in der Tabelle „Webserver“ [cmdb_ci_web_server] ein Datensatz erstellt, falls für den ausgeführten Prozess noch keiner vorhanden ist.

Nach der Klassifizierung werden die folgenden Probes ausgelöst:

Probes für Apache-Webserver

Probe	Beschreibung	Befehle
Apache – Version	Der Sensor dieser Probe fügt dem Webserver-Datensatz die Apache-Versionsinformationen hinzu.	httpd
Apache – Get Configuration	Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der Apache-Konfigurationsdatei bestimmt. Der Sensor dieser Probe fügt dem Webserver-Datensatz einige zusätzliche Informationen hinzu.	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)

Die Sensorverarbeitung der Probe **Apache - Get Configuration** gibt an, ob die Module mod_jk und mod_proxy vorhanden sind, und löst die entsprechende Probe aus.

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

Probes für das Apache-Modul

Probe	Beschreibung	Befehle
Apache – Get JK Module	Wenn das Modul mod_jk als Lastenausgleichsmodul auf dem Server ausgeführt wird, fügt der Sensor dieser Probe die Informationen in die Tabellen „Load Balancer-Service“ [cmdb_ci_lb_service], „Load Balancer-Pool“ [cmdb_ci_lb_pool] und „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member] ein.	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)
Apache – Get Proxy Module	Wenn das Modul mod_proxy als Lastenausgleichsmodul auf dem Server ausgeführt wird, fügt der Sensor dieser Probe die Informationen in die Tabellen „Load Balancer-Service“ [cmdb_ci_lb_service], „Load Balancer-Pool“ [cmdb_ci_lb_pool] und „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member] ein.	grep, egrep (im Bourne-Shell-Skript)

Zusätzlich zur Datenauffüllung werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] die folgenden Beziehungen erstellt:

- Die Datensätze in der Tabelle cmdb_ci_lb_appl werden in den Datensätzen der Tabelle cmdb_ci_web_server ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool werden vom Datensatz der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool sind Mitglieder der Tabelle cmdb_ci_lb_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool_member sind Mitglieder der Tabelle cmdb_ci_lb_pool.

Veraltet: Sudo-Zugriff für die Probe „Unix - Active Processes“ hinzufügen

Für einen Apache-Webserver erfordert die Probe „Unix - Active Processes“ Sudo-Berechtigungen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Sie können die Probe „Unix - Active Processes“ zum Erweitern von Berechtigungen konfigurieren.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Probes**.
2. Suchen Sie im Feld **Suche** nach „Unix - Active Processes“.
3. Klicken Sie in das Feld, und suchen Sie nach „Unix - Active Processes“.
4. Klicken Sie in der zugehörigen Liste **Probe Parameter** auf**Neu**.
5. Klicken Sie auf **Neu**.
6. Verwenden Sie die folgenden Informationen, um das Formular auszufüllen:

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

Probe	Befehle
Name	must_sudo
Wert	Wahr

7. Klicken Sie auf **Absenden**.

Vom Modul mod_jk erfasste Daten

Das Apache-Modul mod_jk leitet Anforderungen vom Apache-Webserver an einen Servlet-Container wie Tomcat weiter.

Zusätzliche mod_jk-Direktiven können auch den Lastenausgleich verwalten. Discovery füllt die CMDB, wenn ein Apache-Server erkannt wird. Wenn der Prozess des Apache-Webservers erkannt wird und das Modul mod_jk auf dem Webserver als Lastenausgleichsmodul ausgeführt wird, werden die zugehörigen Informationen in die CMDB eingetragen.

- Das MID Server-Benutzerkonto zum Untersuchen des Zielservers muss Zugriff auf die Konfigurationsdatei httpd.conf im Ordner /etc/httpd/conf/ haben.
- Discovery verwendet SSH-Befehle (Secure Shell), um die folgenden zugeordneten Elemente zu identifizieren:
  - Apache Get Configuration
  - Apache Version
  - Apache Get JK Module
- Die folgenden Probes benötigen Ausführungsrechte, um Befehle auszuführen:

Probes, die Ausführungsberechtigungen erfordern

Probe	Befehl
Apache – Get Configuration	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)
Apache – Version	httpd
Apache – Get JK Module	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)

Sonden und Sensoren

Discovery verwendet die Probe „Unix - Active Processes“, um einen Apache-Server zu identifizieren, der das Modul mod_jk enthält:

1. Die Probe „Unix – Active Processes“ erkennt einen laufenden Prozess, der eines der folgenden Kriterien erfüllt:
   - Der Name des Prozesses lautet httpd.
   - Der Name des Prozesses lautet apache.
2. Wenn für eines dieser Kriterien eine Übereinstimmung vorliegt, wird in der Webserver-Tabelle [cmdb_ci_web_server] ein Datensatz erstellt, falls für den ausgeführten Prozess noch keiner vorhanden ist. Die folgenden Sonden werden ebenfalls aktiviert:

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

- Apache – Version: Der Sensor dieser Probe fügt dem Webserver-Datensatz die Apache-Versionsinformationen hinzu.
- Apache – Get Configuration: Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der Apache-Konfigurationsdatei bestimmt. Der Sensor dieser Probe fügt dem Webserver-Datensatz einige zusätzliche Informationen hinzu.

3. Die Sensorverarbeitung der Probe „Apache - Get Configuration“ löst die folgenden Probes aus, wenn das Modul mod_jk auf dem Webserver ausgeführt wird:

   Apache – JK Module: Wenn das Modul mod_jk als Lastenausgleichsmodul auf dem Server ausgeführt wird, füllt der Sensor dieser Probe die Informationen in den Tabellen „Load Balancer-Service“ [cmdb_ci_lb_service], „Load Balancer-Pool“ [cmdb_ci_lb_pool] und „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member].

Erfasste Daten

Für das Modul mod_jk ohne Lastenausgleichsmodul werden standardmäßig die folgenden Daten erfasst:

Von Discovery standardmäßig erfasste Daten

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_web_server	Name [name]	Apache – Get Configuration
cmdb_ci_web_server	Version [version]	Apache – Version
cmdb_ci_web_server	Beschreibung [short_description]	Apache – Version

Wenn das Modul mod_jk für den Lastenausgleich aktiviert ist, verknüpft Discovery die folgenden Daten:

Von Discovery erfasste Daten, wenn das Modul mod_jk als Lastenausgleichsmodul identifiziert wird

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_lb_appl	Name [name]	Apache – Apache - Get JK Module
cmdb_ci_lb_appl	IP-Adresse [ip_address]	Apache – Apache - Get JK Module
cmdb_ci_lb_appl	Zuletzt erkannt [last_discovered]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool_member	Name [name]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool_member	Zuletzt erkannt [last_discovered]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool_member	IP-Adresse [ip_address]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool_member	Load Balancer [load_balancer]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool_member	Port [port]	Apache – Apache - Get JK Module

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

Von Discovery erfasste Daten, wenn das Modul mod_jk als Lastenausgleichsmodul identifiziert wird (Fortsetzung)

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_lb_service	Eingabe-URL [Input_url]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	Zuletzt erkannt [last_discovered]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	IP-Adresse [ip_address]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	Name [name]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	Load Balancer [load_balancer]	Apache – Apache - Get JK Module
cmdb_ci_lb_service	Port [port]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool	Zuletzt erkannt [last_discovered]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool	Lastenausgleichsmethode [load_balancing_method]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool	Load Balancer [load_balancer]	Apache – Apache - Get JK Module
cmdb_ci_lb_pool	Name [name]	Apache – Apache - Get JK Module

Beziehungen

Zusätzlich zur Datenauffüllung werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] die folgenden Beziehungen erstellt:

- Die Datensätze in der Tabelle cmdb_ci_lb_appl werden in den Datensätzen der Tabelle cmdb_ci_web_server ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool werden vom Datensatz der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool sind Mitglieder der Tabelle cmdb_ci_lb_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool sind Mitglieder der Tabelle cmdb_ci_lb_pool.

Vom Modul mod_proxy erfasste Daten

Das Apache-Modul mod_proxy implementiert einen Proxy, ein Gateway oder einen Cache für den Apache-Webserver.

Ein zusätzlicher mod_proxy_balancer kann den Lastenausgleich ebenfalls verwalten. Discovery füllt die CMDB, wenn ein Apache-Server erkannt wird. Wenn der Prozess des Apache-Webservers erkannt wird und das Modul mod_proxy auf dem Webserver als

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

Lastenausgleichsmodul ausgeführt wird, werden die zugehörigen Informationen in die CMDB eingetragen.

Beachten Sie die folgenden Anforderungen für die Erkennung eines Apache-Servers, der das Modul mod_proxy enthält:

- Das MID Server-Benutzerkonto zum Untersuchen des Zielservers muss Zugriff auf die Konfigurationsdatei [httpd.conf] im Ordner /etc/httpd/conf/ haben.
- Discovery verwendet SSH-Befehle (Secure Shell), um die folgenden zugeordneten Elemente zu identifizieren:
  - Apache Get Configuration
  - Apache Version
  - Apache Get Proxy Module
- Die folgenden Probes benötigen Ausführungsrechte, um Befehle auszuführen:

Vom Modul mod_jk erfasste Daten

Probe	Befehle
Apache – Get Configuration	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)
Apache – Get Proxy Module	grep, egrep (im Bourne-Shell-Skript)
Apache – Version	httpd

Sonden und Sensoren

Discovery verwendet die Probe „Unix - Active Processes“, um einen Apache-Server zu identifizieren, der das Modul mod_proxy enthält: Die Probes und Sensoren funktionieren wie folgt:

1. Die Probe „Unix – Active Processes“ erkennt einen laufenden Prozess, der eines der folgenden Kriterien erfüllt:
   - Der Name des Prozesses lautet httpd.
   - Der Name des Prozesses lautet apache2.
2. Wenn für eines dieser Kriterien eine Übereinstimmung vorliegt, wird in der Webserver-Tabelle [cmdb_ci_web_server] ein Datensatz erstellt, falls für den ausgeführten Prozess noch keiner vorhanden ist. Die folgenden Sonden werden ebenfalls aktiviert:
   - Apache – Version: Der Sensor dieser Probe fügt dem Webserver-Datensatz [cmdb_ci_web_server] die Apache-Versionsinformationen hinzu.
   - Apache – Get Configuration: Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der Apache-Konfigurationsdatei bestimmt. Der Sensor dieser Probe fügt dem Webserver-Datensatz [cmdb_ci_web_server] einige zusätzliche Informationen hinzu.
3. Die Sensorverarbeitung der Probe „Apache - Get Configuration“ löst die folgenden Probes aus, wenn das Modul mod_proxy auf dem Webserver ausgeführt wird:

   Apache - Get Proxy Module: Wenn das Modul mod_proxy als Lastenausgleichsmodul auf dem Server ausgeführt wird, fügt der Sensor dieser Probe die Informationen in die Tabellen „Load Balancer-Service“ [cmdb_ci_lb_service], „Load Balancer-Pool“ [cmdb_ci_lb_pool] und „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member] ein.

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

Erfasste Daten

Für das Modul mod_proxy ohne Lastenausgleichsmodul werden standardmäßig die folgenden Daten erfasst:

Von Discovery standardmäßig erfasste Daten

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_web_server	Name [name]	Apache – Get Configuration
cmdb_ci_web_server	Version [version]	Apache – Version
cmdb_ci_web_server	Beschreibung [short_description]	Apache – Version

Wenn das Modul mod_proxy für den Lastenausgleich aktiviert ist, verknüpft Discovery die folgenden Daten:

Von Discovery erfasste Daten, wenn das Modul mod_proxy als Lastenausgleichsmodul identifiziert wird

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_lb_appl	IP-Adresse [ip_address]	Apache - Get Proxy Module
cmdb_ci_lb_appl	Zuletzt erkannt [last_discovered]	Apache - Get Proxy Module
cmdb_ci_lb_pool_member	Name [name]	Apache - Get Proxy Module
cmdb_ci_lb_pool_member	Zuletzt erkannt [last_discovered]	Apache - Get Proxy Module
cmdb_ci_lb_pool_member	IP-Adresse [ip_address]	Apache - Get Proxy Module
cmdb_ci_lb_pool_member	Load Balancer [load_balancer]	Apache - Get Proxy Module
cmdb_ci_lb_pool_member	Port [port]	Apache - Get Proxy Module
cmdb_ci_lb_service	Eingabe-URL [Input_url]	Apache - Get Proxy Module
cmdb_ci_lb_service	Zuletzt erkannt [last_discovered]	Apache - Get Proxy Module
cmdb_ci_lb_service	IP-Adresse [ip_address]	Apache - Get Proxy Module
cmdb_ci_lb_service	Name [name]	Apache - Get Proxy Module
cmdb_ci_lb_service	Load Balancer [load_balancer]	Apache - Get Proxy Module
cmdb_ci_lb_service	Port [port]	Apache - Get Proxy Module

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

Von Discovery erfasste Daten, wenn das Modul mod_proxy als Lastenausgleichsmodul identifiziert wird (Fortsetzung)

Tabellenname	Feld- und Bezeichnungsname	Probe
cmdb_ci_lb_pool	Zuletzt erkannt [last_discovered]	Apache - Get Proxy Module
cmdb_ci_lb_pool	Lastenausgleichsmethode [load_balancing_method]	Apache - Get Proxy Module
cmdb_ci_lb_pool	Load Balancer [load_balancer]	Apache - Get Proxy Module
cmdb_ci_lb_pool	Name [name]	Apache - Get Proxy Module

Beziehungen

Zusätzlich zur Datenauffüllung werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] die folgenden Beziehungen erstellt:

- Die Datensätze in der Tabelle cmdb_ci_lb_appl werden in den Datensätzen der Tabelle cmdb_ci_web_server ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool werden von den Datensätzen der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool sind Mitglieder der Datensätze der Tabelle cmdb_ci_lb_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_lb_pool_member sind Mitglieder der Datensätze der Tabelle cmdb_ci_lb_pool.

Anwendungszuordnung für UNIX-Erkennung

Für die Zuordnung, mit der die Anwendungsbeziehungen hergestellt werden, muss Discovery in der Lage sein, TCP-Verbindungen zu erkennen.

Dies lässt sich am besten erreichen, indem auf Zielcomputern der Befehl lsof ausgeführt wird. Für AIX-Computer ist Discovery so konfiguriert, dass die Probe für aktive Verbindungen für AIX-Ziele verwendet wird. Der Benutzer, der das Shell-Skript auf AIX-Computern ausführt, benötigt jedoch möglicherweise zusätzliche Berechtigungen, um im Skript verwendete Befehle wie kdb auszuführen.

Auf Linux-Computern verwendet Discovery zum Erkennen von TCP-Verbindungen den (unter Linux standardmäßig installierten) Befehl `lsof`. Die Linux-Klassifizierungs-Probe löst die Probe „Linux - Active Connections“ aus, der `lsof` zum Erkennen von Anwendungsbeziehungen verwendet und keine Unterbrechungen verursacht. Der Befehl `lsof` stellt die empfohlene Methode zur Rückgabe aktiver TCP-Verbindungen dar. Er kann auf Solaris- und AIX-Zielcomputern installiert werden, um alle durch das Shell-Skript verursachten Probleme zu beheben.

Hinweis: Unter HP-UX wird die Erkennung aktiver Verbindungen nicht unterstützt.

lsof-Befehl verwenden

Verwenden Sie den lsof-Befehl, um aktive TCP-Verbindungen zurückzugeben. Er kann auf Solaris- und AIX-Zielcomputern installiert werden.

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

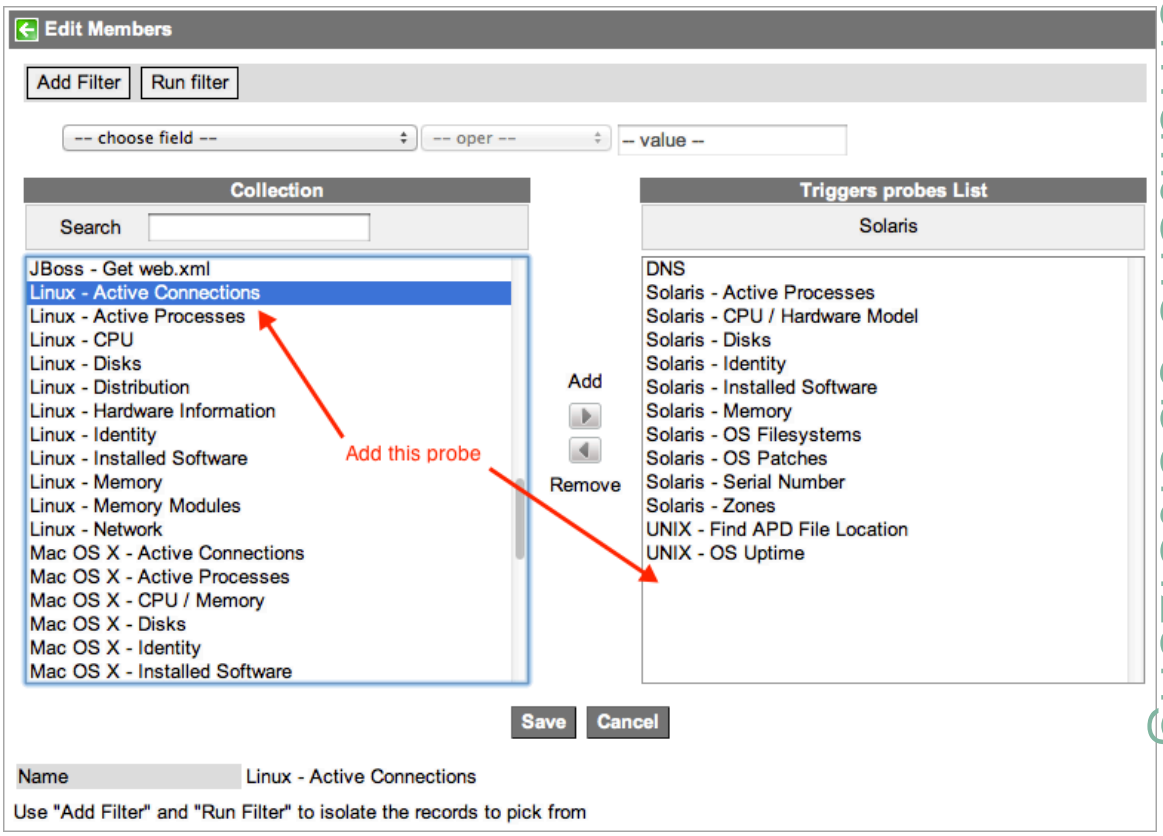
Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Installieren Sie `lsof` auf den Solaris- und AIX-Computern, auf denen Sie Daten über Anwendungsbeziehungen erfassen möchten.
2. Navigieren Sie in der Instanz zu **Discovery-Definition** > **CI-Klassifizierung** > **UNIX**.
3. Wählen Sie aus der Liste **Solaris** aus.
4. Wählen Sie im Formular „UNIX-Klassifizierung“ für Solaris die zugehörige Liste **Auslösertests** aus, und klicken Sie dann auf **Bearbeiten**.
5. Verschieben Sie **Linux - Active Connections** aus der Liste „Sammlungen“ in die Liste „Löst Probe aus“.
   Diese Probe ist für die Verwendung von `lsof` konfiguriert.

Example

Solaris Active Connections lsof



6. Klicken Sie auf **Speichern**.
7. Wiederholen Sie dieses Verfahren für die AIX-Klassifizierung-Probe.

Erkennung des Citrix-Lizenzservers und von Citrix Delivery Controller

Discovery kann Instanzen des Citrix-Lizenzservers und Komponenten von Delivery Controller finden, die auf Windows-Computern ausgeführt werden.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Automatische Übersetzung

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

Anforderungen

- Konfigurieren Sie die Windows-Anmeldeinformationen , um auf den Hostcomputer zuzugreifen.
- Stellen Sie sicher, dass PowerShell für Discovery auf Ihren MID Servern installiert ist. Für die für die Citrix-Discovery verwendeten Muster müssen PowerShell-Befehle ausgeführt werden können.
- Für Betriebssystembenutzer müssen Sie „Get-XDSite“ ausführen. Der Citrix Studio-Administrator muss Berechtigungen erteilen.
- (Optional) Für die Top Down-Discovery mit Service-Mapping installieren Sie auf dem Citrix Delivery Controller das Modul Citrix.Broker.
- (Optional) Für die Top Down-Discovery mit Service-Mapping, erstellen Sie einen Benutzer mit Berechtigung zum Ausführen von PowerShell-Befehlen.
- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

Muster

Zur Ausführung einer horizontalen Erkennung verwendet Discovery die folgenden Muster:

Muster	Erkannter Prozess
Citrix Lizenzserver	lmadmin.exe
Delivery Controller	BrokerService

Erfasste Daten und Beziehungen

Tabelle	Felder
Citrix-Lizenzserver [cmdb_ci_appl_license_server]	Name [name] TCP-Ports [tcp_port] Betriebsstatus [operational_status]
Citrix Delivery Controller [cmdb_ci_appl_delivery_controler]	Name [name] Version [version] TCP-Ports [tcp_port] Betriebsstatus [operational_status]

CI	Beziehung	CI
Citrix-Lizenzserver [cmdb_ci_appl_license_server]	Wird ausgeführt auf::Wird ausgeführt	Windows-Server [cmdb_ci_win_server]

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

CI	Beziehung	CI
Citrix Delivery Controller [cmdb_ci_appl_delivery_controler]	Wird ausgeführt auf::Wird ausgeführt	Windows-Server [cmdb_ci_win_server]

Erkennung geclusterter Anwendungen unter Windows

Ein Prozess und die entsprechenden Ressourceninformationen können verwendet werden, um zu bestimmen, ob es sich bei einem Prozess um einen geclusterten Prozess handelt.

Der Prozessklassifizierer **Microsoft SQL Server** im Lieferumfang Ihrer Instanz identifiziert geclusterte SQL-Server. Mit demselben Verfahren können Sie mithilfe von Discovery unter Windows auch andere geclusterte Anwendungen erkennen.

Um mit Discovery Windows-Clusteranwendungen zu erkennen, erstellen Sie einen Prozessklassifizierer, der erkennt, ob es sich bei einem Prozess um einen geclusterten Prozess handelt. Führen Sie die nachfolgenden Schritte durch:

Klassifizierer für geclusterte Prozesse erzeugen

Erstellen Sie zum Erkennen von geclusterten Windows-Anwendungen einen Prozessklassifizierer für diesen CI-Typ.

Vorbereitungen

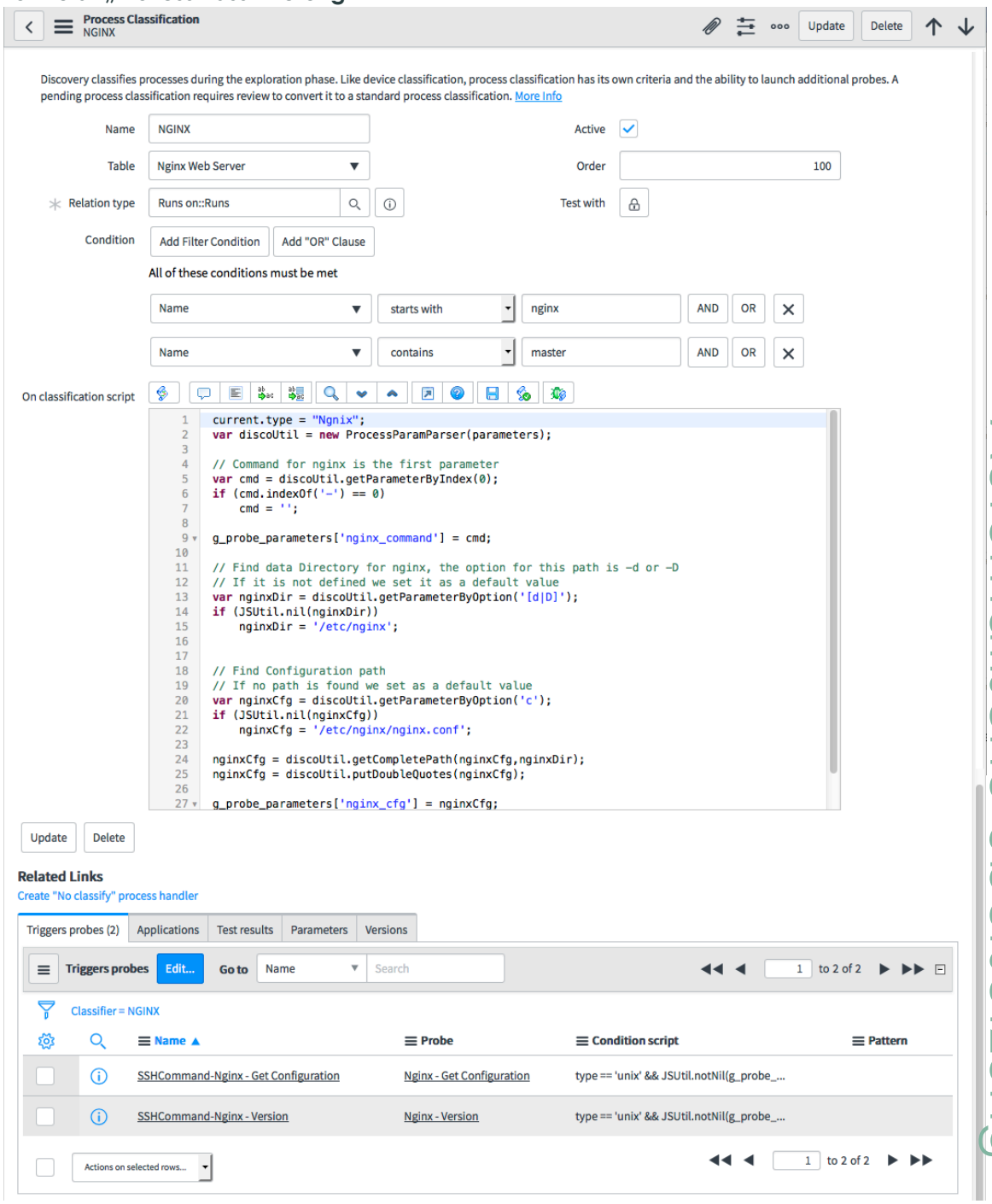
Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **Prozesse**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular mithilfe der Felder aus der Tabelle.
4. Klicken Sie auf **Absenden**.

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

Formular „Prozessklassifizierung“



Automatische Übersetzung

Formular „Prozessklassifizierung“

Feld	Beschreibung
Name	Ein eindeutiger Name für den Prozessklassifizierer
Tabelle	Wählen Sie **Anwendung** aus.
Beziehungstyp	Wählen Sie den CI-Beziehungstyp für diese Klassifizierung aus. Das Beziehungsfeld ist nur für Prozess- und Scan-Anwendungsklassifizierungen verfügbar. Für Erkennungsprozessklassifizierungen wird normalerweise einer der folgenden Beziehungstypen verwendet:

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

Feld	Beschreibung
	◦ **Wird ausgeführt auf::Wird ausgeführt**: Definiert die Beziehung einer Anwendung mit dem Host, auf dem sie ausgeführt wird. Diese Beziehung wird aus der Perspektive des Hosts und der Anwendung ausgedrückt. Beispiel: Meine Datenbankanwendung wird auf server001 ausgeführt::server001 führt meine Datenbankanwendung aus. ◦ **Abhängig von::Verwendet von**: Definiert die Beziehung einer Anwendung, die mit einer anderen Anwendung kommuniziert. Diese Beziehung wird aus der Perspektive der jeweiligen Anwendung ausgedrückt. Beispiel: Die Anwendung Tomcat ist von der Datenbank MySQL abhängig::Die Datenbank MySQL wird von Tomcat verwendet. ◦ **Virtualisiert von::Virtualisiert**: Definiert die Beziehung eines virtuellen Computers mit ihrem Host. Diese Beziehung wird aus der Perspektive des virtuellen Computers und des Hosts ausgedrückt. Beispiel: server001 wird virtualisiert von ServerESX::ServerESX virtualisiert server001. ◦ **Cluster von::Cluster**: Definiert die Beziehung eines Clusterknotens mit dem Cluster, dem er angehört. Diese Beziehung wird aus der Perspektive des Clusterknotens und des Clusters ausgedrückt. ◦ **Gehostet auf::Hostet**: Definiert die Beziehung eines Clusterknotens und des Windows-Hosts. Diese Beziehung wird aus der Perspektive des Clusterknotens und des Windows-Hosts ausgedrückt.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Prozessklassifizierung zu aktivieren. Deaktivieren Sie es, um sie zu deaktivieren.
Reihenfolge	Geben Sie die Reihenfolge ein, in der Discovery diese Prozessklassifizierung ausführen soll, wenn für eine Tabelle mehrere Klassifizierungen verfügbar sind. Discovery führt Prozessklassifizierungen von der niedrigsten zur höchsten Ordnungszahl aus.
Testen mit	Listet das Host-CI auf, bei dem die Bedingungen einer automatisch generierten Prozessklassifizierung erfüllt wurden. Verwenden Sie dieses Feld, um Änderungen an der Prozessklassifizierung zu testen. Auf diese Weise können Sie sicherstellen, dass sich die aktualisierte Klassifizierung wie erwartet verhält.
Bedingung	Konfigurieren Sie die gewünschte Bedingung. Im Beispiel-Screenshot wird diese Prozessklassifizierung ausgelöst, wenn der Prozessbefehl die Zeichenfolge `MSFT SQL Server 2000` enthält.

Prozessklassifizierer mit Windows-Clusterressourcen verknüpfen

Verknüpfen Sie im zweiten Schritt den Prozessklassifizierer mit den Informationen in der Tabelle „Windows-Clusterressourcen“.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Der Name der Tabelle Windows-Clusterressourcen lautet cmdb_ci_win_cluster_resource. Diese Beziehung wird über JavaScript erstellt.

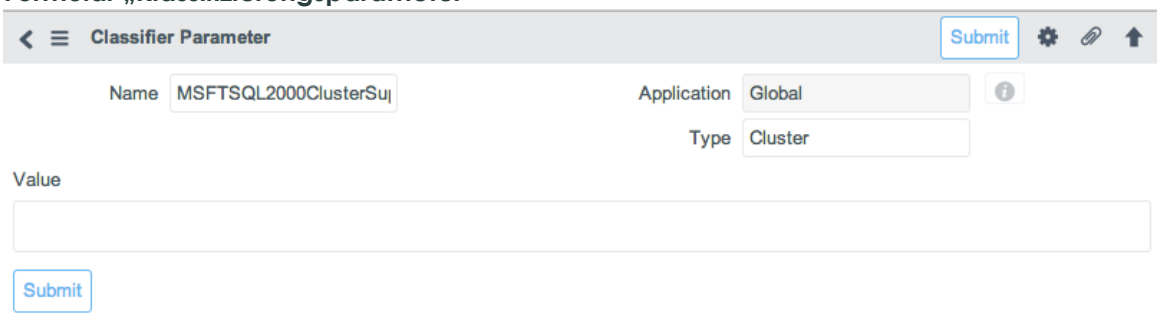
Prozedur

1. Navigieren Sie zurück zur gerade erstellten Prozessklassifizierung.
2. Klicken Sie auf die Registerkarte **Parameter**.

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

3. Klicken Sie auf **Neu**.
4. Füllen Sie die Felder im Formular in geeigneter Weise aus (siehe Tabelle).
5. Klicken Sie auf **Absenden**.

Formular „Klassifizierungsparameter“



Formular „Klassifizierungsparameter“

Feld	Beschreibung
Name	Wählen Sie einen eindeutigen Namen aus.
Applikation	Wählen Sie **Global** aus.
Typ	Geben Sie **Cluster** ein.
Wert	Dieses Feld definiert die beiden JavaScript-Objekte *resourceType* und *isMatch*. Weitere Informationen finden Sie unter Feld „Wert“ im Formular „Klassifizierungsparameter“ füllen.

Feld „Wert“ im Formular „Klassifizierungsparameter“ füllen

Dieses Feld definiert die beiden JavaScript-Objekte *resourceType* und *isMatch*.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Der Wert von *resourceType* verweist auf die Spalte „Ressourcentyp“ in der Tabelle „Windows-Clusterressourcen“ [cmdb_ci_win_cluster_resource]. Der Wert *resourceType* darf nicht leer oder NULL sein.

Prozedur

1. Navigieren Sie zu einer Windows-Clusterseite, um auf die Tabelle „Windows-Clusterressourcen“ zuzugreifen.
2. Klicken Sie auf die Registerkarte **Windows-Clusterressourcen**.

Example:

Mit dem Wert **isMatch** wird ausgewertet, ob es sich bei dem Prozess um einen geclusterten Prozess handelt.

- Wenn die Auswertung **true** ergibt, handelt es sich bei dem Prozess um eine geclusterte Anwendung, und der Prozess wird im Cluster als geclusterte Anwendung klassifiziert.
- Ergibt die Auswertung hingegen **false**, wird der Prozess als normale Anwendung klassifiziert, die auf dem Clusterknoten ausgeführt wird.

Automatische Übersetzung

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

Der Wert **isMatch** ist eine Funktion, die die beiden Eingabevariablen „process“ und „resource“ enthält:

- process: Der Prozess ist der GlideRecord der Prozessanwendung. Diese Variable wird durch das Feld **Tabelle** im Klassifizierer bestimmt. In diesem Beispiel wird für den Prozess, der klassifiziert wird, der GlideRecord-Eintrag der Anwendungstabelle (cmdb_ci_app) verwendet. Sie haben Zugriff auf alle Feldwerte für den CI-Typ, zum Beispiel Name oder Version.
- resource: Die Ressource ist der GlideRecord-Eintrag in der Tabelle „Windows-Clusterressourcen“, nachdem die resourceType-Bedingung angewendet wurde. Im Beispiel ist es der GlideRecord-Eintrag der sechsten Zeile.

JavaScript-Beispiele für das Feld „Wert“.

Im folgenden Beispielcode (resourceType: "SQL Server") filtert die Abfrage den Eintrag der Tabelle „Windows-Clusterressourcen“ für das Feld „Ressourcentyp“, das den Wert „SQL Server“ enthält. In der folgenden Beispieltabelle würde der sechste Datensatz zurückgegeben.

Das folgende Skript gibt an, dass der Prozess als geclusterte Anwendung klassifiziert ist, wenn eine Ressource vom Typ „SQL Server“ vorhanden ist.

```
resourceType: "SQL Server"
isMatch: function(process, resource) {
    return true;
}
```

Das folgende Skript gibt an, dass der Prozess als geclusterte Anwendung klassifiziert ist, wenn eine Ressource vom Typ „SQL Server“ vorhanden ist und der Anwendungsname dem Ressourcennamen entspricht.

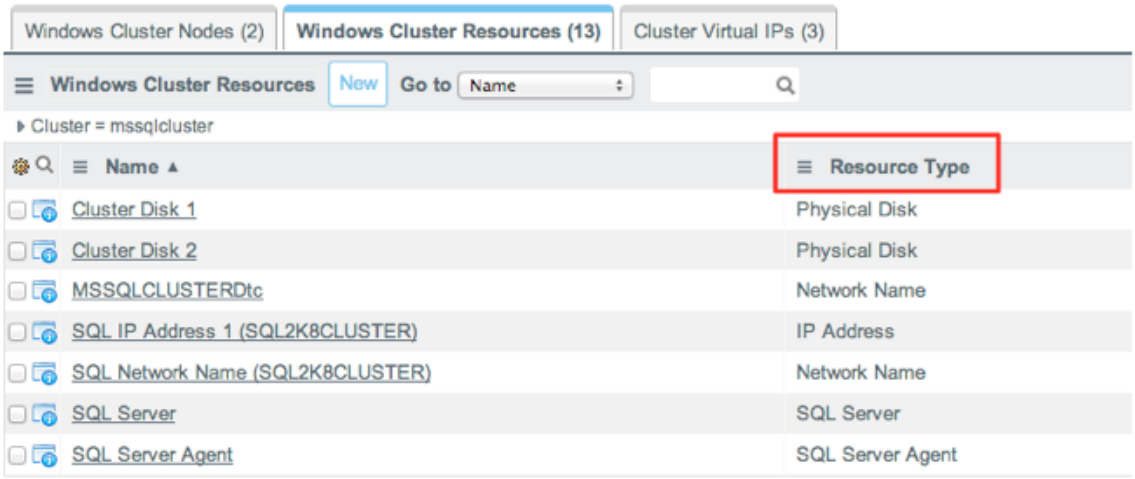
```
resourceType: "SQL Server"
isMatch: function(process, resource) {
    if (process.name == resource.name)
        return true;
}
```

Wenn mehrere Übereinstimmungen mit der resourceType-Bedingung vorhanden sind, wird die Abgleichfunktion mehrmals aufgerufen. Im folgenden Beispiel für resourceType wird die Abgleichfunktion zweimal aufgerufen, da in der Beispieltabelle „Windows-Clusterressourcen“ zwei Einträge vorhanden sind, die in der Spalte **Ressourcentyp** den Eintrag **Physical Disk** haben.

```
resourceType: "Physical Disk"
```


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

Registerkarte „Windows-Clusterressourcen“



Erkennung mit Software Asset Management

Die Tabellenstruktur zur Verwaltung von Softwareinstallationen verhält sich anders, wenn die Anwendung Software Asset Management (SAM) aktiviert ist.

Das Vorhandensein dieser Anwendung hat Einfluss darauf, wie Discovery die von einem Scan zurückgegebenen Softwareinstallationsdaten speichert. Dafür ist eine zusätzliche Konfiguration der Datensätze von Konfigurationselementen (CIs) erforderlich.

Die folgenden Tabellen werden erstellt, wenn das Plugin „Software Asset Management“ aktiviert ist:

- Software-Discovery-Modell [cmdb_sam_sw_discovery_model]
- Softwaremodell [cmdb_software_product_model]
- Softwareinstallation [cmdb_sam_sw_install]

Hinweis: Das von vorherigen Versionen verwendete ursprüngliche Schema ist nicht betroffen, wenn das Plugin „Software Asset Management“ nicht aktiviert ist.

Wenn es ausgeführt wird, füllt Discovery die Tabelle „Softwareinstallation“ [cmdb_sam_sw_install]. Das entsprechende Konfigurationselement (CI) verweist auf die Softwaredaten. Eine Geschäftsregel in dieser Tabelle wird ausgeführt und sucht nach einem übereinstimmenden Datensatz in der Tabelle „Software-Discovery-Modell“ [cmdb_sam_sw_discovery_model]. Wenn in der Tabelle „Software-Discovery-Modell“ ein Datensatz vorhanden ist, wird dieser anhand der Tabelle „Softwareinstallation“ aktualisiert. Wenn in der Tabelle „Software-Discovery-Modell“ kein Datensatz vorhanden ist, wird ein Datensatz erstellt.

Diese Tabellen werden nicht von Discovery mit Software Asset Management verwendet:

- Software [cmdb_ci_spkg]
- Softwaremodell [cmdb_software_product_model]

Wichtig: Wenn SAM installiert ist, stellt die Tabelle „Softwareinstallation“ [cmdb_sam_sw_install] die richtige Quelle für alle aktuellen Softwaredaten dar. Das bedeutet, dass Sie alle zugehörigen Listen und benutzerdefinierten Referenzfelder aktualisieren müssen, die Sie CI-Datensätzen hinzugefügt haben.

Ab der Kingston-Version füllt die Discovery die Tabellen mit dem VMWare-Lizenzschlüssel [samp_vmware_license_key] und dem VMWare-Lizenzschlüssel

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

[samp_vmware_license_key_usage] aus. Siehe Für VMware vCenter-Server erfasste Daten, für weitere Informationen dazu, wo Discovery vCenter-Daten speichert.

CI zur Anzeige von Software Asset Management-Daten konfigurieren

Nachdem Sie das Plugin „Software Asset Management“ aktiviert haben, konfigurieren Sie das Formular für alle Computer-CIs, die erkannt werden sollen, um ihre Daten aus der Tabelle „Softwareinstallation“ [cmdb_sam_sw_install] anzuzeigen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie einen beliebigen Computer-CI-Datensatz.
2. Konfigurieren Sie das Formular so, dass die zugehörige Liste **Softwareinstallation** hinzugefügt wird, und entfernen Sie die zugehörige Liste **Software installiert**.

Erkennung von Exchange-Clientzugriffsservern (CAS)

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz des Exchange-Clientzugriffsservers erkannt wird.

Standardmäßig verwendet Discovery das Muster *CAS On Windows*, um den Exchange-Clientzugriffsserver zu erkennen.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Von Discovery auf dem Exchange-Clientzugriffsserver erfasste Daten

In der Tabelle „Exchange-Clientzugriffsserver“ `[cmdb_ci_exchange_cas]` werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Version	Version
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn
IP-Adresse	ip_address
Installationsverzeichnis	install_directory
Typ	Typ

Erkennung von Exchange-Hub-Transport-Servern

Discovery erstellt oder aktualisiert einen Datensatz CMDB, wenn eine ausgeführte Instanz von Exchange Hub erkannt wird.

Standardmäßig verwendet Discovery das Muster „Hub-Transport-Server unter Windows“ zum Erkennen von Exchange-Hub-Transport-Servern.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

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

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das Muster „Hub-Transport-Server unter Windows“ ausgeführt wird.

ExchangeHub [cmdb_ci_exchange_hub]

Bezeichnung	Feldname
Name	Name
Version	Version
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn
IP-Adresse	ip_address
Installationsverzeichnis	install_directory
Typ	Typ

CI-Beziehungen

Das Muster „Hub-Transport-Server unter Windows“ erkennt keine Beziehungen.

Erkennung von Exchange-Postfächern

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz des Exchange-Postfachs erkannt wird.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Voraussetzungen

Auf dem Server, der erkannt werden soll, muss das Modul `Microsoft.Exchange.Management.PowerShell` installiert sein.

Auf dem Hostcomputer muss der Service `winRM` ausgeführt werden. Führen Sie im Powershell-Fenster den folgenden Befehl zur Überprüfung aus: `New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri "http://$hostname/PowerShell/" -Authentication Kerberos`

Muster

Standardmäßig verwendet Discovery das Muster *`MailBox On Windows`*, um das Exchange-Postfach zu erkennen.

Berechtigungen

Konfigurieren Sie die folgenden Anmeldeinformationen:

Anmeldeinformationstyp	Zusätzliche Hinweise
Applicative-Anmeldeinformationen	Der Benutzer muss in der Lage sein, PowerShell-Befehle für die Exchange-Hosts auszuführen.

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

Anmeldeinformationstyp	Zusätzliche Hinweise
	Verwenden Sie **Exchange-Postfach** als CI-Typ für die Applicative-Anmeldeinformationen. **Wichtig:** Verwenden Sie nicht den CI-Typ **Exchange-Postfachserver**.
Windows-Anmeldeinformationen	Der BS-Benutzer darf kein lokaler Benutzer für den Server, sondern muss ein Domänenbenutzer sein.

Erfasste Daten

In der Tabelle „Exchange-Postfächer“ [cmdb_ci_exchange_mailbox] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Version	Version
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn
IP-Adresse	ip_address
Installationsverzeichnis	install_directory
Typ	Typ

Erkennung von allgemeinen Softwarepaketen

Discovery identifiziert und klassifiziert Informationen über allgemeine Softwarepakete.

Von Discovery für allgemeine Softwarepakete erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_spkg	Name	Verschiedene
Version	cmdb_ci_spkg	Version	Verschiedene
Anzahl Installationen	cmdb_ci_spkg	install_count	Verschiedene
Lizenzanzahl	cmdb_ci_spkg	license_count	Verschiedene
Microsoft SMS-ID	cmdb_ci_spkg	msft_sms_id	Verschiedene
Installiert auf	cmdb_software_instance	installed_on	Verschiedene
Software	cmdb_software_instance	Software	Verschiedene

Erkennung von GlassFish-Servern

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz von GlassFish Server erkannt wird.

Standardmäßig verwendet Discovery zur Erkennung die folgenden Muster: *GlassFish Server* und *GlassFish WAR*.

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

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Von Discovery für GlassFish erfasste Daten

Die folgenden Daten werden in den Tabellen GlassFish [cmdb_ci_appl_ GlassFish] und GlassFish War [cmdb_ci_appl_ GlassFish_War] gesammelt:

Bezeichnung	Feldname
Name	Name
Version	Version
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn
IP-Adresse	ip_address
Installationsverzeichnis	install_directory
TCP-Port(s)	tcp_port
Konfigurationsverzeichnis	config_directory
Konfigurationsdatei	config_file

Erkennung von HP Operations Manager

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz von HP Operations Manager erkannt wird.

Standardmäßig verwendet Discovery das Muster *HP Operations Manager for Windows*, um HP Operations Manager zu erkennen.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Von Discovery für HP Operations Manager erfasste Daten

In der Tabelle „HP Operations Manager“ `[cmdb_ci_appl_hp_operations]` werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	name

Erkennung von HP Service Manager

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz von HP Service Manager erkannt wird.

Standardmäßig verwendet Discovery das Muster *HP Service Manager Application Server*, um HP Service Manager zu erkennen.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

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

Von Discovery für HP Service Manager erfasste Daten

In der Tabelle „HP Service Manager“ `[cmdb_ci_appl_hp_service]` werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Lieferant	Lieferant

IBM Discovery von WebSphere Message Broker (WMB) und WMB-HTTP-Listener

Discovery und Service-Mapping erstellen oder aktualisieren einen CMDB -Datensatz, wenn eine ausgeführte Instanz von IBM WMB und der WMB-HTTP-Listener für Linux und Windows erkannt werden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Standardmäßig verwendet Discovery die folgenden Muster für die Discovery:

- WMB Ein UNIX
- WMB Ein Windows
- WMB-HTTP-Listener ein UNIX
- WMB-HTTP-Listener ein Windows

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Informationen zu IBM WebSphere Message Broker (WMB) und den WMB-HTTP-Listener-Komponenten und -Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Stellen Sie sicher, dass die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- Visibility Content

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

Von Discovery für IBM WebSphere Message Brokers und IBM WMB HTTP-Listener erfasste Daten

Die folgenden Daten werden in der Tabelle IBM WebSphere Message Brokers `[cmdb_ci_appl_ibm_wmb]` und der Tabelle IBM WMB HTTP Listener `[cmdb_ci_appl_ibm_wmb_listener]` gesammelt:

Bezeichnung	Feldname
Name	Name
Klasse	sys_class_name
IP-Adresse	ip_address
Version	Version
Installationsverzeichnis	install_directory

IBM MQ-Erkennung

Die Anwendung ServiceNow Discovery verwendet die Muster „WMQ On Unix“ und „WMQ On Windows“, um IBM MQ-Ressourcen (früher IBM WebSphere MQ) zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

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

Discovery verwendet die folgenden Muster für eine horizontale Erkennung:

- *WMQ On Unix*
- *WMQ On Windows*

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Daten, die von Discovery für IBM MQ erfasst wurden

Discovery füllt die Daten in CMDB bei der Ausführung der WMQ-Muster aus.

IBM MQ Manager (früher IBM WebSphere MQ) [cmdb_ci_appl_ibm_wmq]

Bezeichnung	Feldname
Name	Name
Version	Version
Installationsverzeichnis	install_directory

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

IBM MQ Manager (früher IBM WebSphere MQ) [cmdb_ci_appl_ibm_wmq] (Fortsetzung)

Bezeichnung	Feldname
Klasse	sys_class_name

Erkennung von Microsoft IIS-Servern

Discovery identifiziert und klassifiziert Informationen über Microsoft IIS-Server.

Voraussetzungen

Installieren Sie IIS-Verwaltungsskripts und -tools auf einem Microsoft IIS-Server.

Berechtigungen

Konfigurieren Sie die folgenden Anmeldeinformationen:

- Applicative-Anmeldeinformationen
- Windows-Anmeldeinformationen

Klassifizierer, Muster und Probe

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Zur Erkennung von IIS verwendet Discovery die folgenden Klassifizierer, Probes und Muster:

Klassifizierung	Auslöser-Probes	Muster
Microsoft IIS Server	• Probe „Horizontal Discovery“: Startet Muster • Windows - Get IIS Information*	IIS

*Probes bei neuen Instanzen inaktiv

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Von Discovery für IIS-Webserver erfasste Daten

In der Tabelle „IIS-Webserver“ [cmdb_ci_microsoft_iis_web_server] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Version	Version
Typ*	Typ
Prozessbefehl wird ausgeführt	running_process_command
Zentrale Parameter des ausführenden Prozesses	running_process_key_parameters

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

*Der Typ lautet immer IIS.

In der Tabelle „Website“ [cmdb_ci_web_site] werden die folgenden Daten erfasst:

Bezeichnung	Feldname	Quelle
Name	Name	wmi
TCP-Port	tcp_port	wmi

Erkennung von Microsoft SharePoint

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine laufende Instanz von Microsoft SharePointerkannt wird.

Standardmäßig verwendet Discovery das Muster *`SharePoint`*, um Microsoft SharePointzu erkennen. Informationen zu unterstützten Microsoft SharePoint -Versionen finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Daten erfasst von Discovery für Microsoft SharePoint

In der Tabelle „SharePoints“ `[cmdb_ci_appl_sharepoint]` werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn
IP-Adresse	ip_address
Version	Version

Erkennung von NGINX-Webservern

NGINX ist ein Open Source-Webserver mit einem Lastenausgleichsmodul. Discovery erkennt den Webserver und Informationen über das Lastenausgleichsmodul.

Discovery identifiziert die Serversoftware NGINX mit dem folgenden Prozess:

1. Die NGINX-Prozessklassifizierung erkennt einen laufenden Prozess, der die folgenden Kriterien während der Durchsuchung eines Servers Linux erfüllt:
   - Name beginnt mit „nginx“
   - Name enthält „master“
2. Wenn es eine Übereinstimmung gibt:
   - In der Tabelle „NGINX-Webserver“ [cmdb_ci_nginx_web_server] wird ein Datensatz erstellt.
   - Die Beziehung Wird ausgeführt auf wird in der CI-Beziehungstabelle [cmdb_rel_ci] für einen Linux -Server (Linux Server [cmdb_ci_linux_server]) und für einen NGINX-Webserver (NGINX Web Server [cmdb_ci_nginx_web_server]) erstellt.

     Die folgenden beiden Probes werden ausgelöst:

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

- NGINX – Version: Diese Probe enthält ein Bourne-Shell-Skript. Er bestimmt die Version von NGINX und füllt die Tabelle „NGINX-Webserver“ [cmdb_ci_nginx_web_server].
- NGINX – Get Configuration: Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der NGINX-Konfigurationsdatei bestimmt. Die Probe identifiziert Konfigurationsparameter basierend auf Schlüsselwörtern in der Konfigurationsdatei und gibt sie als einzelnes Nutzlastergebnis zurück.

Der Sensor in der Instanz ServiceNow analysiert das Nutzlastergebnis und füllt die Instanz CMDBaus.

Zur Erkennung eines NGINX-Webservers müssen die folgenden Voraussetzungen erfüllt sein:

- NGINX ist auf dem Server installiert und wird ausgeführt.
- MID-Server hat Zugriff auf die NGINX-Konfigurationsdatei, die standardmäßig`/etc/nginx/nginx.conf` lautet.

Anforderungen

Für NGINIX-Server:

- NGINX ist auf dem Server installiert und wird ausgeführt.
- Gewähren Sie, dass MID-Server Zugriff auf die NGINX-Konfigurationsdatei hat, standardmäßig `/etc/nginx/nginx.conf`.
- Aktivieren Sie SSH-Befehle (Secure Shell), um die folgenden zugeordneten Elemente zu identifizieren:
  - NGINX - Version
  - NGINX - Get Configuration

Die folgenden Probes benötigen Ausführungsrechte, um Befehle auszuführen:

Befehle

Probe	Befehle
Nginx – Version	nginx
Nginx – Get Configuration	echo, sed, httpd, cut, grep, egrep (im Bourne-Shell-Skript)

Hinweis: Das Nginx-Muster führt eine Top Down-Discovery auf den Servern Windows und Linux durch. Informationen zu den Voraussetzungen für die Top Down-Discovery für NGINX-Webserver finden Sie unter Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping.

Probes und Sensoren

Discovery identifiziert die Serversoftware NGINX mit dem folgenden Prozess:

1. Der Prozessklassifizierer „Nginx“ erkennt einen laufenden Prozess, der während der Erkundung eines UNIX-Servers die folgenden Kriterien erfüllt:
   - Der Name des Prozesses beginnt mit `nginx`.
   - Der Name des Prozesses enthält `master`.
2. Wenn es eine Übereinstimmung gibt:

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

- In der Tabelle „Webserver“ [cmdb_ci_web_server] wird ein Datensatz erstellt.
- In der Tabelle „CI-Beziehung“ [cmdb_rel_ci] wird für den Linux-Server (Linux-Server [cmdb_ci_linux_server]) und für den Webserver (Webserver [cmdb_ci_web_server]) eine Beziehung vom Typ Wird ausgeführt auf erstellt.

3. Die folgenden beiden Probes werden ausgelöst:
   - **Nginx – Version**: Diese Probe enthält ein Bourne-Shell-Skript. Er bestimmt die Version von NGINX und füllt die Tabelle „Webserver“ [cmdb_ci_web_server].
   - **Nginx – Get Configuration**: Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der NGINX-Konfigurationsdatei bestimmt. Die Probe identifiziert Konfigurationsparameter basierend auf Schlüsselwörtern in der Konfigurationsdatei und gibt sie als einzelnes Nutzlastergebnis zurück.
4. Der Sensor in der Instanz ServiceNow verarbeitet die Nutzlast und füllt die Instanz CMDBaus.

Erfasste Daten

Discovery erstellt oder aktualisiert CMDB Datensätze, wenn ein laufender NGINX-Prozess erkannt wird. Die folgenden Daten werden erfasst.

Von Discovery für NGINX erfasste Daten

Tabellenname	Feld- und Bezeichnungsname	Probe
Name	cmdb_ci_lb_appl [name]	Nginx– Get Configuration
IP-Adresse	cmdb_ci_lb_appl [ip_address]	Nginx– Get Configuration
Zuletzt erkannt	cmdb_ci_lb_appl [last_discovered]	Nginx– Get Configuration
Version	cmdb_ci_lb_appl [version]	Nginx– Version
Name	cmdb_ci_lb_pool_member [name]	Nginx– Get Configuration
Zuletzt erkannt	cmdb_ci_lb_pool_member [last_discovered]	Nginx– Get Configuration
IP-Adresse	cmdb_ci_lb_pool_member [ip_address]	Nginx– Get Configuration
Lastenausgleich	cmdb_ci_lb_pool_member [load_balancer]	Nginx– Get Configuration
Vollqualifizierter Domänenname	cmdb_ci_lb_pool_member [fqdn]	Nginx– Get Configuration
Port	cmdb_ci_lb_pool_member [port]	Nginx– Get Configuration
Zuletzt erkannt	cmdb_ci_lb_service [last_discovered]	Nginx– Get Configuration
IP-Adresse	cmdb_ci_lb_service [ip_address]	Nginx– Get Configuration
Name	cmdb_ci_lb_service [name]	Nginx– Get Configuration

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

Von Discovery für NGINX erfasste Daten (Fortsetzung)

Tabellenname	Feld- und Bezeichnungsname	Probe
Lastenausgleich	cmdb_ci_lb_service [load_balancer]	Nginx– Get Configuration
Eingabe-URL	cmdb_ci_lb_service [input_url]	NGINX - Get Configuration

Beziehungen

In die Tabelle [cmdb_rel_ci] werden die folgenden Beziehungen eingefügt:

- Die Datensätze in der Tabelle cmdb_ci_lb_appl werden in den Datensätzen der Tabelle cmdb_ci_web_server ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_pool werden von den Datensätzen der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_pool sind Mitglieder der Tabelle cmdb_ci_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_pool_member sind Mitglieder der Tabelle cmdb_ci_pool.

Erkennung von Oracle Tuxedo

Die Anwendung ServiceNow Discovery verwendet das Tuxedo-Muster, um Oracle Tuxedo-Ressourcen zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

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

Discovery verwendet das **Tuxedo** -Muster zur Ausführung einer horizontalen Discovery.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Daten, die von Discovery für Oracle Tuxedo erfasst wurden

Discovery füllt die Daten in CMDB aus, wenn das Tuxedo-Muster ausgeführt wird.

Tuxedo [cmdb_ci_appl_tuxedo]

Name	Beschreibung
Port [port]	Der Netzwerkkommunikationsport, der von Oracle Tuxedo-Services und -Prozessen für die Netzwerkkommunikation verwendet wird.
Domäne [domain]	Die logische Gruppierung von Oracle Tuxedo-Komponenten und -Services, die in einer definierten Umgebung ausgeführt werden.

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

Tuxedo [cmdb_ci_appl_tuxedo] (Fortsetzung)

Name	Beschreibung
Installationsverzeichnis [install_directory]	Der Speicherort, der alle Binärdateien und Konfigurationsdateien enthält, die zum Ausführen von Oracle Tuxedo erforderlich sind.
Protokollverzeichnis [log_dir]	Das Verzeichnis, in dem alle von Oracle Tuxedo für Überwachung und Fehlerbehebung generierten Protokolldateien gespeichert werden.
Version [version]	Das spezifische Release von Oracle Tuxedo, das installiert ist und derzeit verwendet wird.
Modus [mode]	Die Definition des Interaktionsprotokolls zwischen Oracle Tuxedo und verschiedenen Clients oder anderen Domänen, z. B. Jelt, Workstation oder Domain Gateway, basierend auf der Betriebskonfiguration.

Erkennung der Automatisierungssoftware Puppet

Discovery identifiziert Puppet-Master, die auf UNIX-Servern ausgeführt werden.

Discovery verwendet SSH-Befehle (Secure Shell) zur Erfassung von Informationen.

Um auf Puppet Master-Datensätze zuzugreifen, navigieren Sie zu **Alle** > **Konfiguration** > **Automatisierungsserver** > **Master-Puppets**. Sie können die Ressourcen in der zugehörigen Liste des Puppet Master-Datensatzes anzeigen.

Funktionsweise der Probe „Puppet Master“

Discovery identifiziert Puppet Master mit dem folgenden Prozess:

1. Die Probe **UNIX - Active Processes** erkennt einen laufenden Prozess, der eines der folgenden Kriterien erfüllt:
   - Der Name des Prozesses lautet `pe-httpd`.
   - Der Name des Prozesses lautet `ruby`, und die Parameter des Prozesses enthalten *`puppet master`*.
2. Wenn eine Übereinstimmung mit einem der folgenden Kriterien vorliegt:
   - Ein Datensatz wird in der Puppet Master-Tabelle [cmdb_ci_puppet_master] erstellt, wenn für den ausgeführten Prozess noch kein Datensatz vorhanden ist.
   - Die Probe **Puppet - Master Info** wird ausgelöst. Der Sensor dieser Probe fügt dem Puppet Master-Datensatz [cmdb_ci_puppet_master] einige zusätzliche Informationen hinzu.

Anforderungen zum Erkennen eines Puppet-Masters

Standardmäßig erkennt Discovery auf UNIX-Servern ausgeführte Puppet-Master. Discovery verwendet SSH-Befehle (Secure Shell) zur Erfassung von Informationen.

Die zum Erkennen des UNIX-Servers verwendeten Anmeldeinformationen müssen über Berechtigungen zum Ausführen der folgenden Befehle verfügen. Die Verwendung von sudo wird unterstützt, Sie müssen der Probe jedoch den Parameter *`must_sudo`* hinzufügen.

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

Probe	Befehle
Puppet - Master Info	puppet, echo, hostname (im Bourne-Shell-Skript)
Puppet - Certificate Requests	puppet
Puppet - Manifests	echo, sed, find (im Bourne-Shell-Skript)
Puppet - Modules	puppet

Erfasste Daten

Daten, die Discovery standardmäßig für die Automatisierungssoftware Puppet erfasst

Name	Puppet-Master [cmdb_ci_puppet_master]	Name	Puppet - Master Info
Konfigurationsverzeichnis	Puppet-Master [cmdb_ci_puppet_master]	config_directory	Puppet - Master Info
Manifestverzeichnis	Puppet-Master [cmdb_ci_puppet_master]	manifestdir	Puppet - Master Info
Modulpfad	Puppet-Master [cmdb_ci_puppet_master]	modulepath	Puppet - Master Info
Vollqualifizierter Domänenname	Puppet-Master [cmdb_ci_puppet_master]	fqdn	Puppet - Master Info
IP-Adresse	Puppet-Master [cmdb_ci_puppet_master]	ip_address	Puppet - Master Info
Version	Puppet-Master [cmdb_ci_puppet_master]	Version	Puppet - Master Info

Puppet-Probes den Parameter must_sudo hinzufügen

Um Puppet-Probes mit sudo zu verwenden, müssen Sie jeder Probe, für die das erforderlich ist, den Parameter *must_sudo* hinzufügen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Fügen Sie allen Puppet-Probes den Parameter must_sudo hinzu.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Probes**.
2. Suchen Sie im Feld **Suchen** nach dem Namen **Puppet**.
3. Klicken Sie auf den Namen der Probe.
   Beispiel: **Puppet Master - Info**.
4. Wählen Sie im Bereich **Zugehörige Links** die Registerkarte **Probe Parameter** aus.
5. Klicken Sie auf **Neu**.
6. Geben Sie in das Feld **Name** den Namen `must_sudo` ein.

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

7. Im Feld **Wert** geben Sie `wahr` ein.
8. Klicken Sie auf **Absenden**.

Erkennung von SAP-Produkten

ITOM-Transparenz kann SAP Anwendungen, SAP HANA-Datenbank und SAP HANA DB-Katalogerkennen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Informationen zu den SAP -Komponenten und ihren Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

Muster für Discovery und Service-Mapping

Visibility Content

CMDB CI-Klassenmodelle

Überprüfen Sie die Konfiguration der Anmeldeinformationen

- (Beim Hosting auf UNIX-Server) Konfigurieren Sie auf der Now Platform die Applicative-Anmeldeinformationen und SSH-Anmeldeinformationen . Die SSH-Anmeldeinformationen werden dazu verwendet, Verbindungen von der SAP-Zentralinstanz zu anderen Anwendungen und Geräten herzustellen. Gewähren Sie dem Benutzer außerdem erhöhte Rechte, damit er Befehle ausführen kann, die einen privilegierten Benutzer erfordern: Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern.
- (Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform die Windows-Anmeldeinformationen , um Verbindungen von der SAP-Zentralinstanz zu anderen Anwendungen und Geräten herzustellen.
- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
- (Optional für Discovery von oben nach unten durch Service-Mapping) Erteilen Sie einem Benutzer die Berechtigung zum Ausführen von SOAP in der RFC-Tabellenlesefunktion.
- (Optional für Top Down-Discovery durch Service-Mapping) Wenn Ihre Organisation digitale SAP-Business-Services mithilfe von Webservices implementiert und Sie alle verbundenen Services zuordnen möchten, führen Sie die folgenden Aktionen aus:

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

- Konfigurieren Sie Applicative-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle: CVERS, DBCONS und RFCONS.
- Stellen Sie sicher, dass Sie über die Webservice-URL verfügen. Informationen zum Erstellen von Webservices finden Sie unter https://blogs.sap.com/2012/10/24/how-to-create-web-services-abap-based/ .

SAP HANA 2.0 DB-Katalog auf UNIX

Stellen Sie sicher, dass die Applicative-Anmeldeinformationen für **SAP HANA DB-App-Anmeldeinformationen** mit **„SAP HANA DB“ [cmdb_ci_appl_sap_hana_db]** als CI-Typ konfiguriert sind.

Überprüfen Sie die Berechtigungen zum Ausführen von Service-Mapping -Befehlen

Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern

Stellen Sie sicher, dass der Benutzer über die Berechtigungen zum Ausführen der Musterabfragen verfügt

Die folgenden Befehle werden beim Ausführen der SAP HANA DB- und SAP HANA DB-Katalogmuster ausgeführt.

- `* aus Schemas auswählen;`
- `* aus M_HOST_INFORMATION auswählen, wobei oberes Element (KEY) wie '%TIMEZONE%';`
- `Wählen Sie SCHEMA_NAME aus, und runden Sie (sum(TABLE_SIZE) /1024/1024) aus M_TABLES GROUP BY SCHEMA_NAME ab`

Der Abfragetyp	Fallback-Befehle, die der Reihe nach ausgeführt werden
Schemainformationen	**1.** `$hdbsql_path + " -n " + $entry_point.ip_address + ":" + $query_port + " -i " + $digits + " -u '$$username$$' -p '$$password$$' \"select * aus Schemas;\""` **2.** `$hdbsql_path + " -n " + $ip_address + ":" + $query_port + " -i " + $digits + " -u '$$username$$' -p '$$password$$' \"select * from schemas;\""` **3.** `$hdbsql_path + " -n " + $server_name + ":" + $query_port + " -i " + $digits + " -u '$$username$$' -p '$$password$$' \"select * from schemas;\""` **4.** `$hdbsql_path + " -n localhost -i " + $digits + " -u '$`

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

Der Abfragetyp	Fallback-Befehle, die der Reihe nach ausgeführt werden
	`$username$$' -p '$$password$$' \"* aus schemas auswählen; \""`
Zeitzone:	1. `$hdbsql_path + " -n " + $entry_point.ip_address + ":" + $query_port + " -i " + $digits + " -u '$$username$$' -p '$$password$$' \"select * aus „M_HOST_INFORMATION“, wobei „Upper(KEY)“ wie '%TIMEZONE%';\""` 2. `$hdbsql_path + " -n " + $ip_address + ":" + $query_port + " -i " + $digits + " -u '$$username$$' -p '$$password$$' \"select * from M_HOST_INFORMATION, wobei oberer (KEY) wie '%TIMEZONE%';\""` 3. `$hdbsql_path + " -n " + $server_name + ":" + $query_port + " -i " + $digits + " -u '$$username$$' -p '$$password$$' \"select * from M_HOST_INFORMATION, wobei oberer (KEY) wie '%TIMEZONE%';\""` 4. `$hdbsql_path + " -n localhost -i " + $digits + " -u '$$username$$' -p '$$password$$' \"select * aus M_HOST_INFORMATION wobei oberes (KEY) wie '%TIMEZONE%' lautet ;\""`
Datenträgergröße	1. `$hdbsql_path + " -n " + $entry_point.ip_address + ":" + $query_port + " -i " + $digits + " -u '$$username$$' -p '$$password$$' \"select SCHEMA_NAME, Round(sum(TABLE_SIZE) /1024/ 1024) von M_TABLES GROUP BY SCHEMA_NAME;\""` 2. `$hdbsql_path + " -n " + $ip_address + ":" + $query_port + " -i " + $digits + " -u '$$username$$' -p '$$password$$'`

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

Der Abfragetyp	Fallback-Befehle, die der Reihe nach ausgeführt werden
	\"select SCHEMA_NAME, Round(sum(TABLE_SIZE) /1024/ 1024) from M_TABLES GROUP BY SCHEMA_NAME;\"" 3. $hdbsql_path + " -n " + $server_name + ":" + $query_port + " -i " + $digits + " -u '$$username $$' -p '$$password$$' \"select SCHEMA_NAME, Round(sum(TABLE_SIZE) /1024/ 1024) from M_TABLES GROUP BY SCHEMA_NAME;\"" 4. $hdbsql_path + " -n localhost -i " + $digits + " -u '$ $username$$' -p '$$password $$' \"select SCHEMA_NAME, Round(sum(TABLE_SIZE) /1024/ 1024) from M_TABLES GROUP BY SCHEMA_NAME;\""

Überprüfen Sie die Konfiguration des Zeitplans Discovery .

Weitere Informationen finden Sie unter Erkennungen im Netzwerk ausführen

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
SAP ASCS [cmdb_ci_appl_sap_ascs]	
Name [name]	Für SAP Advanced Business Application Programming (ABAP) SAP Central Services (ASCS) gesammelte Daten
Version [version]	
Installationsverzeichnis [install_directory]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [confi_file]	
Instanzname [instance_name]	
Instanznummer [instance_number]	
System-ID [sid]	
Systemverzeichnis [system_directory]	
Systemtyp [system_type]	
Transportdomäne [transport_domain]	
SAP Business Objects CMS-Server [cmdb_ci_appl_sap_bo]	
Name [name]	Für SAP Business Objects CMS-Server erfasste Daten
Servername [server_name]	

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

Tabelle und Feld	Beschreibung
Version [version]	
Installationsverzeichnis [install_directory]	
SAP SCS-Anwendung [cmdb_ci_appl_sap_scs]	
Name [name]	Für SAP Central Services (SCS) erfasste Daten
Version [version]	
Installationsverzeichnis [install_directory]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Instanzname [instance_name]	
Instanznummer [instance_number]	
System-ID [sid]	
Systemverzeichnis [system_directory]	
Systemtyp [system_type]	
Transportdomäne [transport_domain]	
SAP CI-Anwendung [cmdb_ci_appl_sap_ci]	
Name [name]	Für SAP Convergent Invoicing (CI) erfasste Daten
Version [version]	
Installationsverzeichnis [install_directory]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Instanzname [instance_name]	
Instanznummer [instance_number]	
System-ID [sid]	
Systemverzeichnis [system_directory]	
Systemtyp [system_type]	
Transportdomäne [transport_domain]	
SAP DI-Anwendungen [cmdb_ci_appl_sap_di]	
Name [name]	Für SAP NetWeaver Development Infrastructure (DI) erfasste Daten
Version [version]	
Installationsverzeichnis [install_directory]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Instanzname [instance_name]	
Instanznummer [instance_number]	
System-ID [sid]	

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

Tabelle und Feld	Beschreibung
Systemverzeichnis [system_directory]	
Systemtyp [system_type]	
Transportdomäne [transport_domain]	
SAP ERS-Anwendung [cmdb_ci_appl_sap_ers]	
Name [name]	Für SAP Evaluated Receipt Settlement (ERS) erfasste Daten
Version [version]	
Installationsverzeichnis [install_directory]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Instanzname [instance_name]	
Instanznummer [instance_number]	
System-ID [sid]	
Systemverzeichnis [system_directory]	
Systemtyp [system_type]	
Transportdomäne [transport_domain]	
HANA-Datenbank [cmdb_ci_appl_sap_hana_db]	
Name [name]	Für SAP HANA-Datenbank erfasste Daten
IP-Adresse [id_address]	
Klasse [sys_class_name]	
Vollständig qualifizierter Domänenname [fqdn]	
Version [version]	
Installationsverzeichnis [install_directory]	
SAP-SID [cmdb_ci_sap_sid]	
Name [name]	Für SAP System Identification (SID) gesammelte Daten. Eine SID ist ein eindeutiger Identifizierungscode für eine SAP R/3-Installation. Eine SID ist ein dreistelliger Code wie D10, PRD oder E56. Eine R/3-Installation besteht aus einem Datenbankserver und mehreren Anwendungsservern. ITOM-Transparenz verwendet das Muster der gemeinsamen Bibliothek SID SAP, um SIDs für Anwendungen SAP von zu erkennen.
Version [version]	
Informationen zur Patch-Ebene [sap_patch_info]	

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

Daten, die vom Muster SAP „ HANA-DB-Katalog auf UNIX während der Horizontal-Discovery erfasst wurden

SAP HANA-Katalog [cmdb_ci_db_hana_catalog]

Feld	Beschreibung
Katalogbesitzer [catalog_owner]	Die Anwender-ID des Schemabesitzers.
Katalogerstellungszeit [catalog_create_time]	Die Katalogerstellungszeit.
Zugeteilte Datenträgergröße (MB) [disk_allocated_size_mb]	Die zugeteilte Datenträgergröße in MB.
Datenbankreferenz [database_Instanz]	Der Verweis auf die SAP HANA DB.

CI-Beziehungen

Das Muster der SAP SID-Gemeinschaftsbibliothek [] erstellt CI-Beziehungen zwischen allen wichtigen CI-Anwendungen und SAP der System-ID.

CI	Beziehung	CI
SAP ERS-Anwendung [cmdb_ci_appl_sap_ers]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]
SAP DI-Anwendungen [cmdb_ci_appl_sap_di]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]
SAP ASCS [cmdb_ci_appl_sap_ascs]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]
SAP CI-Anwendung [cmdb_ci_appl_sap_ci]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]
SAP SCS-Anwendung [cmdb_ci_appl_sap_scs]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]
SAP JC-Anwendung [cmdb_ci_appl_sap_jc]	Verwendet::Verwendet von	SAP-SID [cmdb_ci_sap_sid]

SAP HANA DB-Katalog für UNIX CI-Beziehungen

CI	Beziehung	CI
SAP HANA-DB [cmdb_ci_appl_sap_hana_db]	Enthält::Enthalten in	SAP HANA DB-Katalog [cmdb_ci_db_hana_catalog]

Einschränkungen

Service-Mapping kann pro Bereitstellung nur eine ASCS-Instanz zuordnen.

Das Muster des HANA-DB-Katalogs SAP kann nur unter UNIXausgeführt werden.

Ordnen Sie Anwendungsservices zu, die SAP-Anwendungen enthalten

Ordnen Sie einen für Service zu, der eine SAP-Anwendung enthält, und vergewissern Sie sich, dass Service-Mapping alle SAP-Komponenten richtig erkannt hat.

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

Vorbereitungen

Erforderliche Rolle: service_mapping_admin

Prozedur

1. Erstellen Sie eine Serviceinstanz.

   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**.

   b. Klicken Sie auf **Neu**.
   Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.

   c. Geben Sie im Feld **Name** einen beschreibenden Namen für die Serviceinstanz ein.

2. Definieren Sie den Einstiegspunkt für diesen Anwendungsservice:

   a. Wählen Sie die Kachel **SAP-Anwendung**.
   Die Option **Erkennbar durch Service Mapping** ist standardmäßig ausgewählt.

   b. Definieren Sie den Einstiegspunkt wie folgt:

   - Eine URL zu einem beliebigen SAP-Modul
   - Eine TCP-Verbindung zu einem beliebigen SAP-Modul
   - Zum Erkennen von Umgebungen mit verbundenen Services geben Sie die URL für den Webservice im folgenden Format an: .

   ```
   http://<hostname>:<port>/sap/bc/srt/scs/sap/z_servicenow_read?sap-client=003
   ```

   c. Klicken Sie auf **Hinzufügen**.

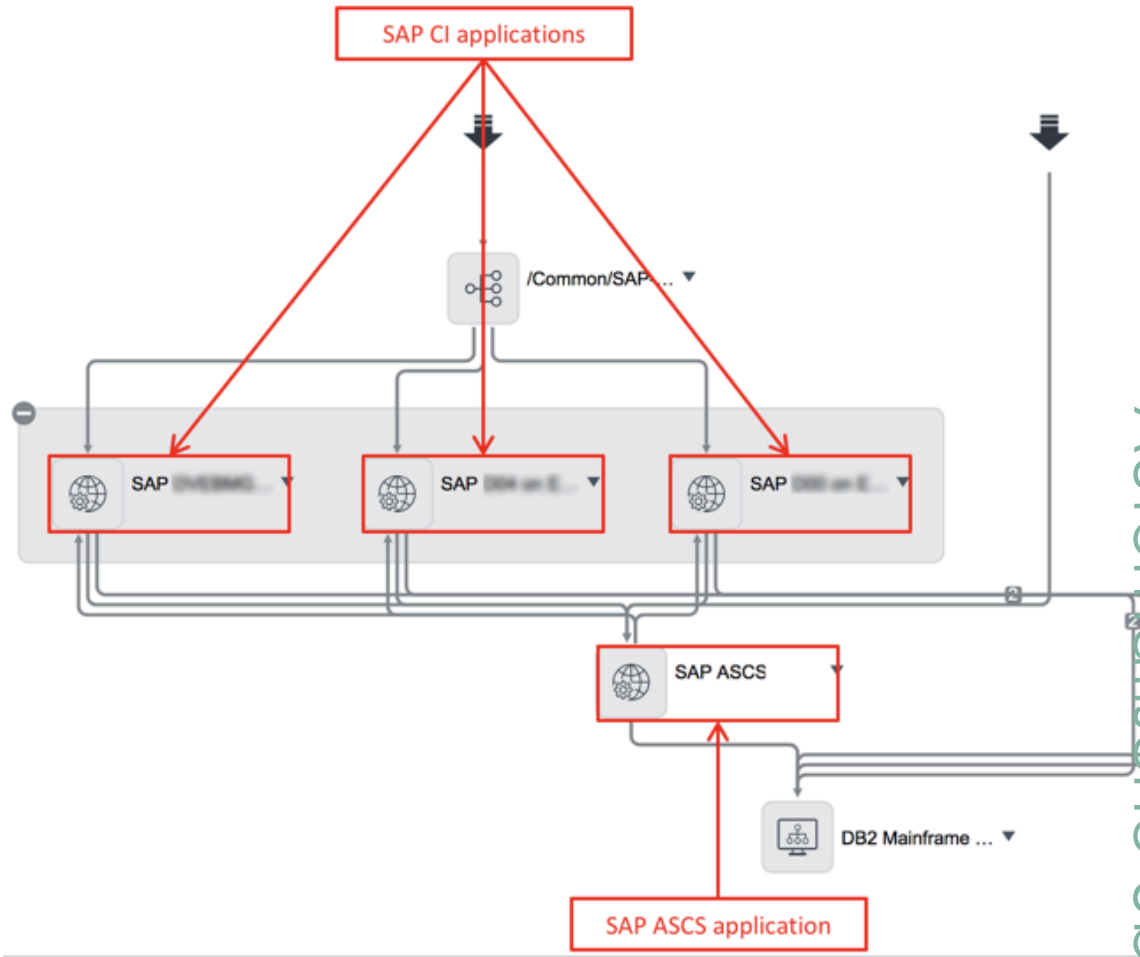
   d. Klicken Sie auf **Speichern**.

3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:

   a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist.
   Es kann einige Minuten dauern.

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

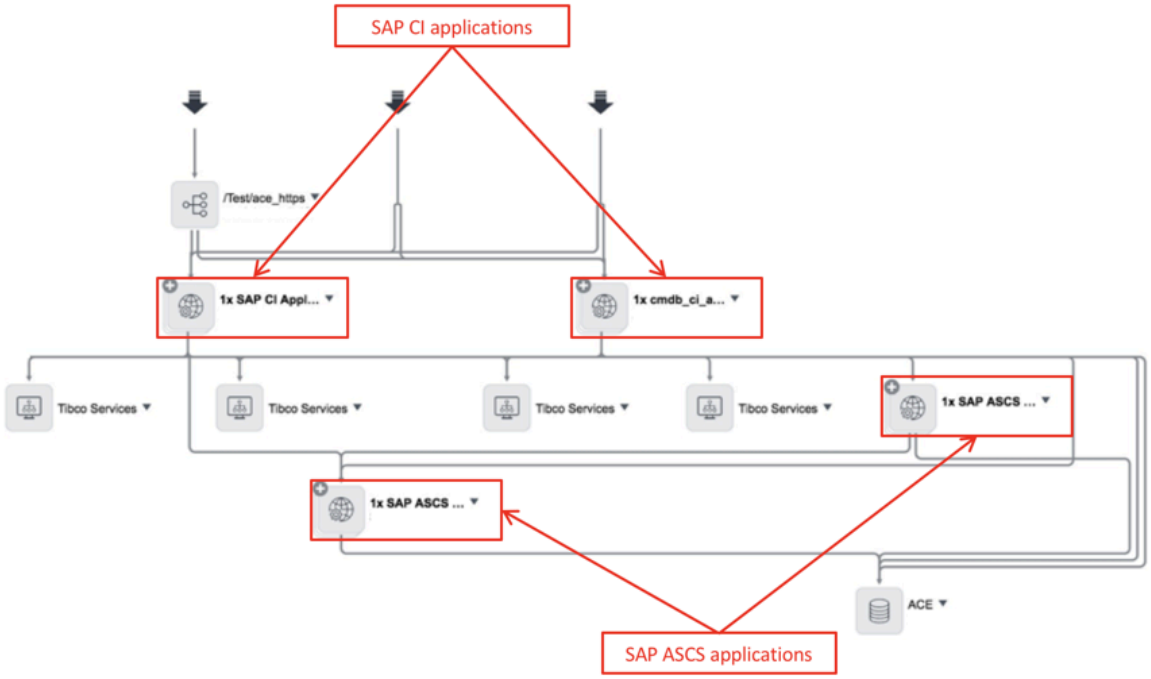
b. Überprüfen Sie die Zuordnung des Anwendungsservice, und stellen Sie sicher, dass das Servicelayout wie in den folgenden Beispielen aussieht.



Automatische Übersetzung

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

Wenn die SAP-Umgebung SAP-Komponenten mit Tibco-Services integriert, können Sie dieses Zuordnungsergebnis erwarten:



Problembehebung bei Anwendungsservices, die SAP-Anwendungen enthalten

Beheben Sie grundlegende Erkennungsprobleme basierend auf den Symptomen und Erkennungsmeldungen.

Symptom

In der Zuordnung des Anwendungsservice in Service-Mapping wird die folgende Meldung angezeigt: `Fehler beim Erkennen von <Name der SAP-Komponente>.`

Ursache

Das CI konnte nicht identifiziert werden, und die Prozesserkennung ruft die Prozessattribute ab.

Lösung

Führen Sie die nachfolgenden Schritte durch:

1. Öffnen Sie den fehlgeschlagenen Musterschritt im Debug-Modus:
   a. Klicken Sie in der Zuordnung des Business-Service oder der Serviceinstanz mit der rechten Maustaste auf die Fehlermeldung, und wählen Sie **Discovery-Protokoll anzeigen**aus.

      Das Fenster „Discovery-Protokoll“ wird geöffnet.

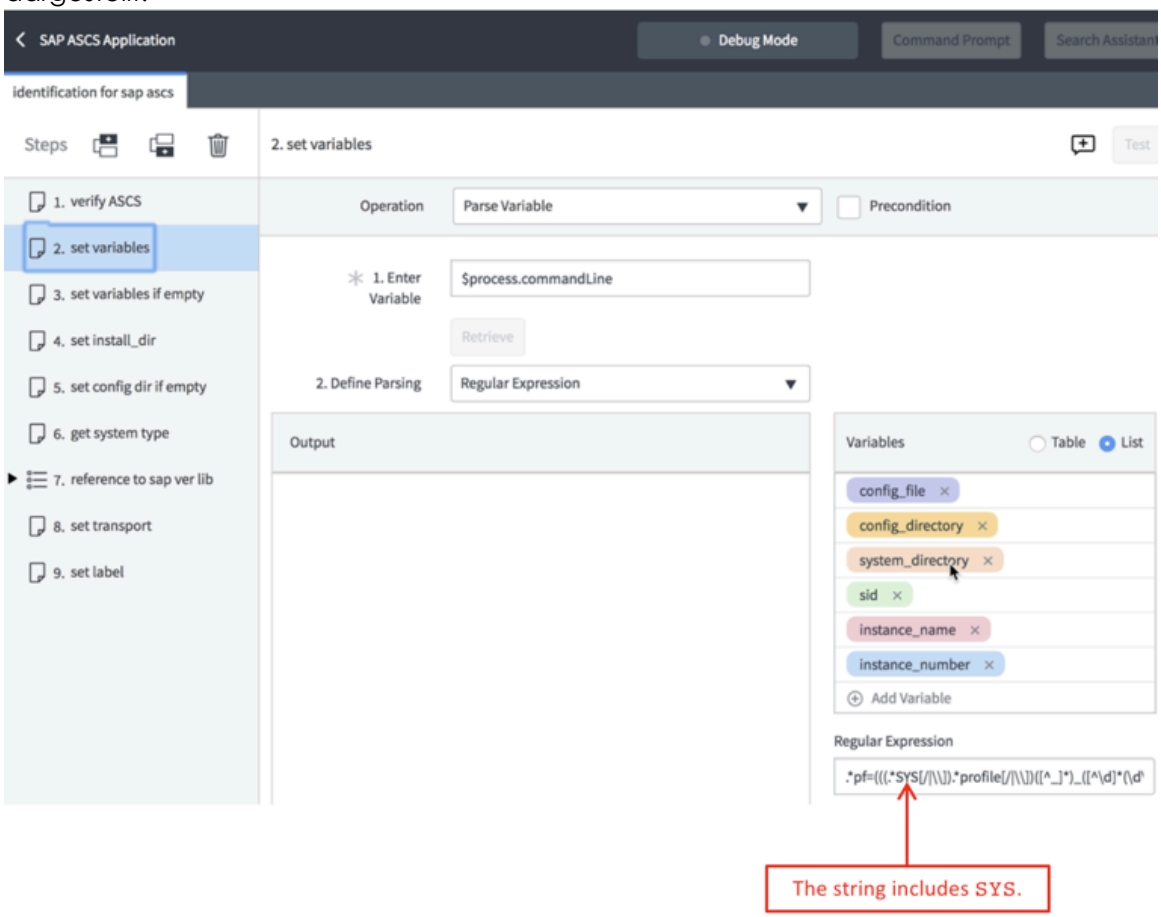
   b. Suchen Sie im rechten Bereich den fehlerhaften Identifikationsbereich und den fehlgeschlagenen Schritt innerhalb dieses Bereichs.
   c. Wählen Sie diesen fehlerhaften Identifikationsbereich aus und klicken Sie auf **Debuggen**.

      Das Fenster „Identifikationsbereich debuggen“ wird geöffnet.

   d. Füllen Sie ggf. die erforderlichen Angaben aus und klicken Sie auf **Verbinden**.

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

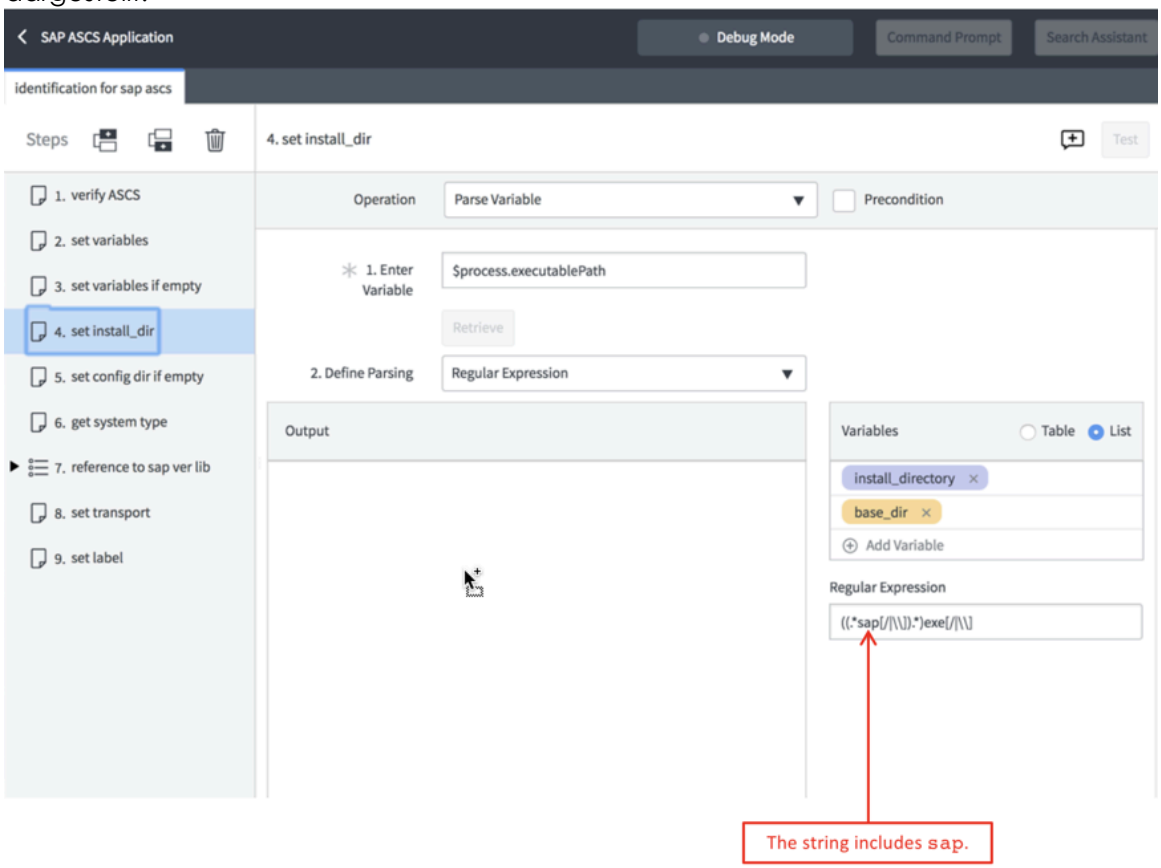
2. Klicken Sie unter **Schritte** auf den Schritt **Variablen festlegen**.
3. Stellen Sie sicher, dass der reguläre Ausdruck `SYS` enthält, wie in der folgenden Abbildung dargestellt.



4. Klicken Sie unter **Schritte** auf den Schritt **install_dir festlegen**.

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

5. Stellen Sie sicher, dass der reguläre Ausdruck `sap` enthält, wie in der folgenden Abbildung dargestellt.



Symptom

Service-Mapping erkennt den Webservice nicht, den Ihre Organisation für die Bereitstellung von SAP Digital Business Services verwendet.

Ursache 1

Das Muster schlägt bei der EVAL-Funktion zum Identifizieren des Webservice fehl.

Lösung 1

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass Sie die erforderlichen Applicative-Anmeldeinformationen wie im Zuordnungsverfahren beschrieben konfiguriert haben.
3. Überprüfen Sie, ob das Erkennungsprotokoll die folgende Nachricht enthält: GROOVE_CODE_FAILURE: Keine solche Eigenschaft: com für Klasse: Script1.
4. Öffnen Sie den fehlgeschlagenen Musterschritt im Debug-Modus:
   a. Klicken Sie in der Zuordnung des Business-Service oder der Serviceinstanz mit der rechten Maustaste auf die Fehlermeldung, und wählen Sie **Discovery-Protokoll anzeigen**aus.

      Das Fenster „Discovery-Protokoll“ wird geöffnet.

   b. Suchen Sie im rechten Bereich den fehlerhaften Identifikationsbereich und den fehlgeschlagenen Schritt innerhalb dieses Bereichs.

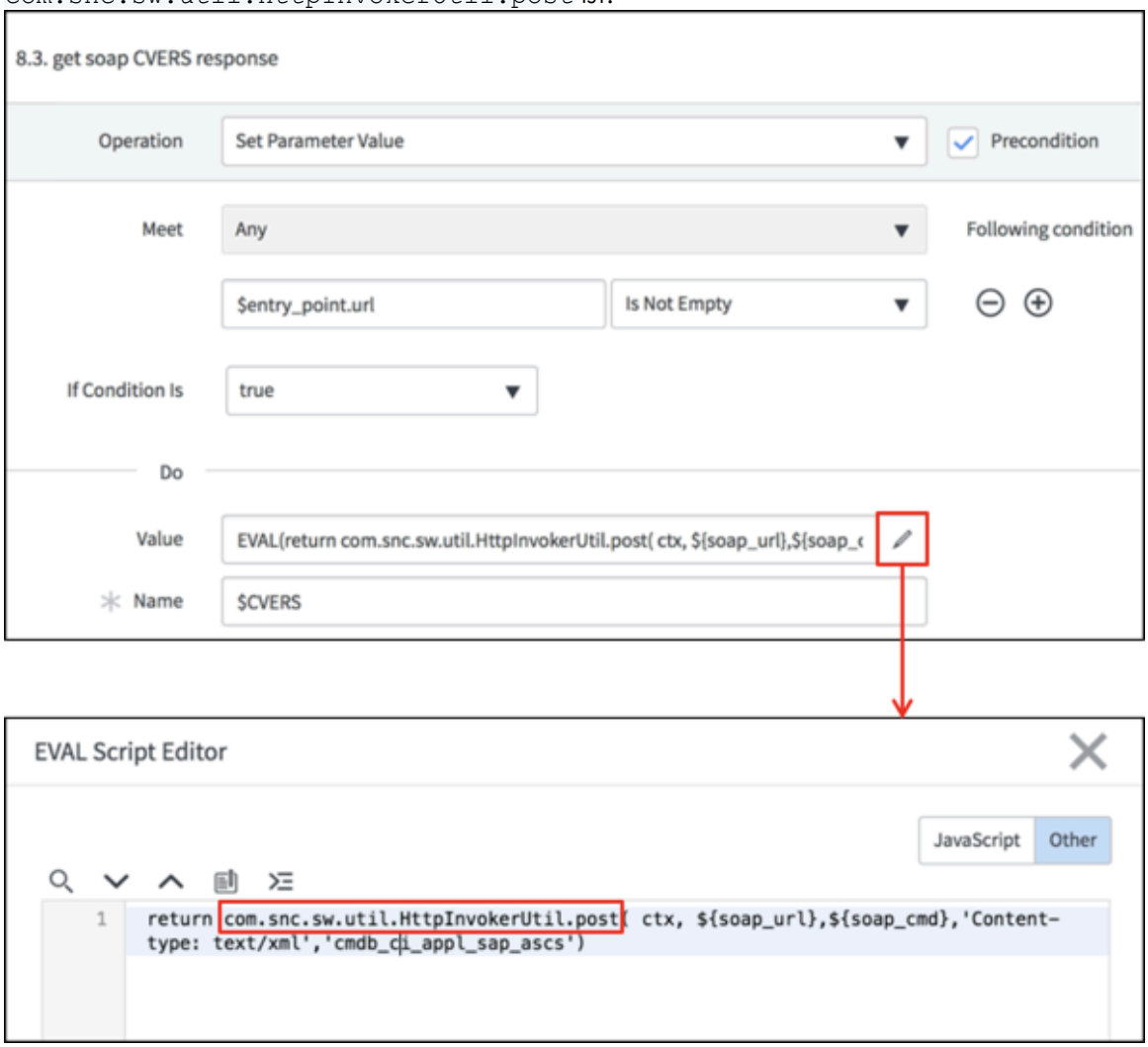
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

c. Wählen Sie diesen fehlerhaften Identifikationsbereich aus und klicken Sie auf **Debuggen**.

   Das Fenster „Identifikationsbereich debuggen“ wird geöffnet.

d. Füllen Sie ggf. die erforderlichen Angaben aus und klicken Sie auf **Verbinden**.

5. Der Musterdesigner wird mit dem ausgewählten Identifizierungsabschnitt geöffnet.
6. Wählen Sie rechts den fehlgeschlagenen Schritt aus.
7. Stellen Sie sicher, dass die auf EVAL ausgeführte Funktion `com.snc.sw.util.HttpInvokerUtil.post` ist.



8. Versuchen Sie, den Anwendungsservice erneut zuzuordnen, und überprüfen Sie das Ergebnis.

Ursache 2

Das Muster schlägt bei der EVAL-Funktion zum Identifizieren des Webservice fehl, weil der Webservice falsch konfiguriert wurde.

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

Lösung 2

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass Sie die erforderlichen Applicative-Anmeldeinformationen wie im Zuordnungsverfahren beschrieben konfiguriert haben.
3. Vergewissern Sie sich, dass das Erkennungsprotokoll die folgende Meldung enthält: „Debug-Ausführung fehlgeschlagen: Testschritt fehlgeschlagen. GROOVE_CODE_FAILURE: Alle Befehlsimplementierungen (HTTP) auf Host 10.xxx sind fehlgeschlagen. Host muss ausgefallen oder nicht erreichbar sein. ()"
4. Erstellen Sie den Webservice neu, wie in https://blogs.sap.com/2012/10/24/how-to-create-web-services-abap-based/ beschrieben.
5. Versuchen Sie, den Anwendungsservice erneut zuzuordnen, und überprüfen Sie das Ergebnis.

Ursache 3

Das Muster schlägt bei der EVAL-Funktion zum Identifizieren des Webservice fehl, da die im Einstiegspunkt konfigurierte URL nicht korrekt ist oder weil der MID-Server nicht auf diese URL zugreifen kann.

Lösung 3

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass Sie die erforderlichen Applicative-Anmeldeinformationen wie im Zuordnungsverfahren beschrieben konfiguriert haben.
3. Vergewissern Sie sich, dass das Erkennungsprotokoll die folgende Meldung enthält: „Debug-Ausführung fehlgeschlagen: Testschritt fehlgeschlagen. GROOVE_CODE_FAILURE: Alle Befehlsimplementierungen (HTTP) auf Host 10.xxx sind fehlgeschlagen. Host muss ausgefallen oder nicht erreichbar sein. ()"
4. Stellen Sie sicher, dass Sie die richtige URL für den Serviceeinstiegspunkt verwendet haben:
   a. Navigieren Sie im TCode SOAMANAGER zu **Vereinfachte Webservice-Konfiguration**.
   b. Suchen Sie auf der Registerkarte **Konfiguration** des Fensters „Vereinfachte Servicekonfiguration“ nach dem Webservice, der Teil des für Services ist.
   c. Klicken Sie auf das Kontrollkästchen unter **Benutzername/Passwort (Standard)** für diesen Webservice.
   d. Klicken Sie auf **Details anzeigen**.
   e. Überprüfen Sie im Fenster „Details“ der Servicedefinition die tatsächliche URL des Webservices unter WSDL-URLs.
   f. Korrigieren Sie ggf. die für den Einstiegspunkt konfigurierte URL, und versuchen Sie erneut, den für Service zuzuordnen.

Ursache 4

MID-Server kann nicht auf diese URL zugreifen, die im Einstiegspunkt des für Service konfiguriert wurde.

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

Lösung 4

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass Sie die erforderlichen Applicative-Anmeldeinformationen wie im Zuordnungsverfahren beschrieben konfiguriert haben.
3. Vergewissern Sie sich, dass das Erkennungsprotokoll die folgende Meldung enthält: „Debug-Ausführung fehlgeschlagen: Testschritt fehlgeschlagen. GROOVE_CODE_FAILURE: Alle Befehlsimplementierungen (HTTP) auf Host 10.xxx sind fehlgeschlagen. Host muss ausgefallen oder nicht erreichbar sein. ()"
4. Vergewissern Sie sich, dass Sie den MID-Server für den Zugriff auf die URL verwendet haben, die Sie im Serviceeinstiegspunkt konfiguriert haben:
   a. Melden Sie sich remote beim MID-Server-Host an.
   b. Öffnen Sie einen Browser.
   c. Fügen Sie die URL in die Adresszeile des Browsers ein, und drücken Sie die Eingabetaste.
   d. Wenn die Seite nicht geöffnet wird, liegt ein Netzwerkproblem vor, z. B. ist eine Firewall vorhanden, die verhindert, dass der MID-Server auf diese URL zugreift.
5. Beheben Sie das Netzwerkproblem, und stellen Sie sicher, dass der MID-Server wie in Schritt 4 beschrieben auf die URL zugreifen kann.

Ursache 5

MID-Server kann nicht auf diese URL zugreifen, die im Einstiegspunkt des für Service konfiguriert wurde.

Lösung 5

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass Sie die erforderlichen Applicative-Anmeldeinformationen wie im Zuordnungsverfahren beschrieben konfiguriert haben.
3. Vergewissern Sie sich, dass das Erkennungsprotokoll die folgende Meldung enthält: „Debug-Ausführung fehlgeschlagen: Testschritt fehlgeschlagen. GROOVE_CODE_FAILURE: Alle Befehlsimplementierungen (HTTP) auf Host 10.xxx sind fehlgeschlagen. Host muss ausgefallen oder nicht erreichbar sein. ()"
4. Überprüfen Sie, ob die Applicative-Anmeldeinformationen, die Sie auf der Now Platform für den Webservice konfiguriert haben, gültig sind:
   a. Melden Sie sich remote beim MID-Server-Host an.
   b. Öffnen Sie einen Browser.
   c. Fügen Sie die URL in die Adresszeile des Browsers ein, und drücken Sie die Eingabetaste.
   d. Die Browserseite zeigt das Popup-Fenster für die Anmeldeinformationen an.
   e. Geben Sie die Anmeldeinformationen ein, und überprüfen Sie, ob die Seite geöffnet wird.

      Die Seite wird nicht geöffnet, was bedeutet, dass die konfigurierten Applicative-Anmeldeinformationen falsch sind.
5. Ermitteln Sie die richtigen Anmeldeinformationen.

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

6. Überprüfen Sie die neuen Anmeldeinformationen wie in Schritt 4 beschrieben.
7. Wenn die Seite geöffnet wird, nachdem Sie die neuen Anmeldeinformationen verwendet haben, konfigurieren Sie diese Anmeldeinformationen als Applicative-Anmeldeinformationen auf der Now Platform.

Ursache 6

MID-Server kann nicht auf diese URL zugreifen, die im Einstiegspunkt des für Service konfiguriert wurde.

Lösung 6

1. Stellen Sie sicher, dass das Format des Einstiegspunkts die Webservice-URL ist, wie im Zuordnungsverfahren beschrieben.
2. Vergewissern Sie sich, dass das Erkennungsprotokoll die folgende Meldung enthält: „Debug-Ausführung fehlgeschlagen: Testschritt fehlgeschlagen. GROOVE_CODE_FAILURE: Fehlende gültige Applicative-Anmeldeinformationen für den CI-Typ <Name des CI-Typs>."
3. Vergewissern Sie sich, dass Sie wie in Ordnen Sie Anwendungsservices zu, die SAP-Anwendungen enthalten beschrieben Applicative-Anmeldeinformationen für das relevante CI definiert haben.

Erkennung von SQL Server Analysis Services (SSAS)

Die Anwendung Discovery und Service-Mapping verwenden das SSAS-Muster, um SQL Server Analysis Services in Ihrer Infrastruktur zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren..

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Voraussetzungen

Stellen Sie sicher, dass die Anwendungen aktuell sind.

Muster für Discovery und Service-Mapping

CMDB CI-Klassenmodelle

Visibility Content

Überprüfen Sie die Konfiguration der Anmeldeinformationen

Überprüfen Sie auf der Seite Now Platform®die Konfiguration der Anmeldeinformationen Windows. Weitere Informationen finden Sie unter Windows-Anmeldeinformationen

Während der horizontalen Erkennung erfasste Daten

Discovery füllt die folgenden Daten aus, wenn das SSAS-Muster ausgeführt wird.

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

SQL Server Analysis Services [cmdb_ci_db_mssql_analysis]		
Bezeichnung	**Feld**	**Beschreibung**
Name	name	Der Name des SSAS auf dem Server Windows
IP-Adresse	ip_address	Die SSAS-IP-Adresse
Version	version	Die SSAS-Version
Edition	Edition	Die SSAS-Edition
Installationsverzeichnis	install_directory	Das SSAS-Installationsverzeichnis
Instanzname	Instanz	Der Name der SSAS-Instanz
TCP-Port(s)	tcp_port	Der SSAS-TCP-Port

MicrosoftMicrosoft Azure Event Hubs Discovery von SQL Server Integration Services (SSIS).

Die Anwendung Discovery und Service-Mapping verwenden das SSIS-Muster, um SQL Server Integration Services (SSIS) in Ihrer Infrastruktur zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Voraussetzungen

Überprüfen Sie die Einrichtung der Plugins

Muster für Discovery und Service-Mapping

CMDB CI-Klassenmodelle

Visibility Content

Überprüfen Sie die Konfiguration der Anmeldeinformationen

Überprüfen Sie auf der Seite Now Platform®die Konfiguration der Anmeldeinformationen Windows. Weitere Informationen finden Sie unter Windows-Anmeldeinformationen

Daten, die während der horizontalen -Discovery erfasst wurden

Discovery füllt die folgenden Daten aus, wenn das SSIS-Muster ausgeführt wird.

SQL Server Integration Services [cmdb_ci_db_mssql_integration_list]		
Bezeichnung	**Feld**	**Beschreibung**
Name	name	Der Name von SSIS auf dem Server Windows
IP-Adresse	ip_address	Die SSIS-IP-Adresse
Version	version	Die SSIS-Version
Edition	Edition	Die SSIS-Edition

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

SQL Server Integration Services [cmdb_ci_db_mssql_integration_list]		
Bezeichnung	**Feld**	**Beschreibung**
Installationsverzeichnis	install_directory	Das SSIS-Installationsverzeichnis
Instanzname	Instanz	Der Name der SSIS-Instanz

Erkennung von Sun Java Enterprise System (JES)

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz von Sun JES erkannt wird.

Standardmäßig verwendet Discovery das Muster *Sun JES pattern*, um Sun Java Enterprise System zu erkennen.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Von Discovery für Sun Java Enterprise System erfasste Daten

In der JES-Tabelle `[cmdb_ci_email_server_jes]` werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Klasse	sys_class_name
Vollqualifizierter Domänenname	fqdn

Erkennung von Tomcat-Servern

Discovery identifiziert und klassifiziert Informationen über Tomcat-Server und Webanwendungen, die auf Unix-Computern ausgeführt werden.

Discovery kann Webanwendungen im Verzeichnis `CATALINA_BASE` oder im Verzeichnis `CATALINA_HOME` identifizieren und klassifizieren.

Der Klassifizierer verwendet für die Suche nach Tomcat-Serverprozessen die folgende Bedingung: [Parameter] [enthält] [org.apache.catalina.startup.Bootstrap].

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Berechtigungen

Konfigurieren Sie die folgenden Anmeldeinformationen:

- Applicative-Anmeldeinformationen
- SSH-Anmeldeinformationen

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

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

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
Tomcat	• Horizontal Pattern: Startet Muster • SSHCommand-Tomcat - Find web.xml List* • SSHCommand-Tomcat - Get server.xml* • SSHCommand-Tomcat - Get Version*	Tomcat

*Probes bei neuen Instanzen inaktiv

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Für Unix und Windows erfasst Discovery in der Tomcat-Tabelle [cmdb_ci_app_server_tomcat] die folgenden Daten:

Bezeichnung	Feldname	Quelle
Name	Name	server.info
Installationsverzeichnis	install_directory	server.xml
Version	Version	server.info
Serverport	server_port	server.xml
Attribute	attributes	server.xml

In der Tabelle „Tomcat Connector“ [cmdb_ci_tomcat_connector] werden für Unix und Windows die folgenden Daten erfasst:

Bezeichnung	Feldname	Quelle
Tomcat	tomcat	server.xml
Port	port	server.xml

In der Webanwendungs-Tabelle [cmdb_ci_web_application] werden für Unix und Windows die folgenden Daten erfasst:

Bezeichnung	Feldname	Quelle
Beschreibung	Beschreibung	web.xml
Dokumentenbasis	document_base	web.xml

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

Bezeichnung	Feldname	Quelle
App-Server	app_server	web.xml

Beziehungen

Übergeordnete Klasse	Beziehung	Untergeordnete Klasse
cmdb_ci_app_server_tomcat	Enthält::Enthalten in	cmdb_ci_web_application

Erkennung von WebLogic-Anwendungsservern

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine Instanz eines unter Windows oder Linux ausgeführten Oracle- oder BEA Weblogic-Anwendungsservers erkannt wird.

Anforderungen

Für Windows

- PowerShell muss auf dem MID Server aktiviert sein.
- Für die WebLogic-Administrationsserverinstanzen, die über WebLogic NodeManager starten, muss der Parameter *-Dweblogic.RootDirectory=<path>* beim Start des Servers definiert sein. Die Windows-Anmeldeinformationen müssen auch Leseberechtigungen für die Datei `config.xml` besitzen.

Für Linux

- Discovery erfordert die Verwendung der folgenden Bourne-Shell-Befehle:
  - `find`
  - `cat`
  - `dirname`
- Für WebLogic-Administrationsserverinstanzen, die über NodeManager gestartet wurden, muss der Parameter *-Dweblogic.RootDirectory=<path>* definiert und über den Linux-Befehl *ps process stat* (für jeden Administrationsserver) sichtbar gemacht werden, damit die CMDB mit den übrigen Informationen der Linux WebLogic-Anwendungsserver und -Webanwendungen gefüllt wird.
- Die folgende Konfiguration muss in der Datei sudorers festgelegt werden:

  ```
  User ALL=(root) NOPASSWD: /bin/sh *
  ```

  `User` entspricht dem Benutzernamen in den SSH-Anmeldeinformationen, die Sie für diese Erkennung erstellen.

- Der folgende Befehl muss ausgeführt werden können:

  ```
  /bin/sh /tmp/snc-*-findcat.sh * *"
  ```

  Nehmen Sie keine Änderungen an `findcat.sh` vor.

- Wenn Sie für die Weblogic-Erkennung Probes und keine Muster verwenden, müssen Sie in der Probe *Linux - Weblogic - Find config.xml* den folgenden Parameter und Wert angeben: *must_sudo = true*

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

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Anmeldeinformationen

- Applicative-Anmeldeinformationen
- Windows-Anmeldeinformationen
- SSH-Anmeldeinformationen

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
Weblogic-Server	• Horizontal Pattern: Startet Muster • Windows - Weblogic - Get web.xml* • Windows - Weblogic - Find config.xml* • Linux - Weblogic - Find config.xml*	WebLogic

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Unter Windows erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_app_server_weblogic	Name	Laufender Prozess
Version	cmdb_ci_app_server_weblogic	Version	config.xml
WebLogic-Domäne	cmdb_ci_app_server_weblogic	weblogic_domain	config.xml
TCP-Port(s)	cmdb_ci_app_server_weblogic	tcp_port	web.xml und laufender Prozess
Name	cmdb_ci_web_application	Name	config.xml
Dokumentenbasis	cmdb_ci_web_application	document_base	config.xml
Beschreibung	cmdb_ci_web_application	Beschreibung	web.xml
Servlet-Klasse	cmdb_ci_web_application	servlet_class	web.xml
Servlet-Name	cmdb_ci_web_application	servlet_name	web.xml
App-Server	cmdb_ci_web_application	app_server	config.xml

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

Bezeichnung	Tabellenname	Feldname	Quelle
TCP-Port(s)	cmdb_ci_web_application	tcp_port	web.xml

Unter Linux erfasste Daten

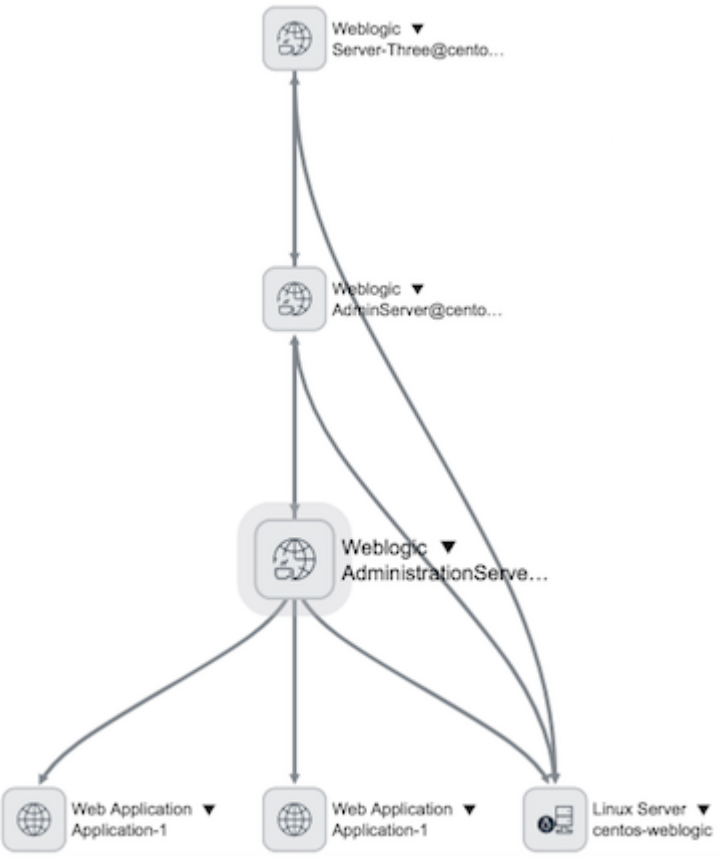
Tabelle	Feld	Quelle
cmdb_ci_app_server_weblogic	Name (name)	Laufender Prozess
cmdb_ci_app_server_weblogic	TCP-Port [tcp_port]	Laufender Prozess
cmdb_ci_app_server_weblogic	Version (version)	config.xml
cmdb_ci_app_server_weblogic	Weblogic-Domäne (weblogic_domain)	config.xml
cmdb_ci_web_application	Name (name)	config.xml
cmdb_ci_web_application	Kontextpfad (context_path)	config.xml
cmdb_ci_web_application	App-Server (app_server)	config.xml

Beziehung

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
cmdb_ci_app_server_weblogic	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_windows_server oder cmdb_ci_linux_server
cmdb_ci_app_server_weblogic	Enthält::Enthalten in	cmdb_ci_web_application
cmdb_ci_app_server_weblogic	Abhängig von::Verwendet von	cmdb_ci_app_server_weblogic Diese Beziehung wird zwischen einem Administrationsserver und allen von ihm gekapselten verwalteten Servern hergestellt.

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

Beispiel für Weblogic-Beziehungen



sudo-Zugriff für die Probe „Weblogic - Find config.xml“ hinzufügen

Wenn Sie das Weblogic-Muster nicht verwenden, können Sie unter Linux der Probe „Weblogic - Find config.xml“ sudo-Berechtigungen hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **Probes**.
2. Suchen Sie nach der Probe **Linux - Weblogic - Find config.xml**, und wählen Sie sie aus.
3. Klicken Sie in der zugehörigen Liste **Probe Parameter** auf **Neu**.
4. Füllen Sie das Formular mit den folgenden Informationen aus:

Probe	Befehle
Name	must_sudo
Wert	Wahr

5. Klicken Sie auf **Absenden**.

Windows WebLogic-Anwendungsserver identifizieren

Falls Sie das Weblogic-Muster nicht verwenden, folgt Discovery diesem Prozess, wenn die Probes „Windows - Active Processes“ und „Linux - Active Processes“ verwendet werden.

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

Dieser Prozess beschreibt die Verwendung von Probes, die bei einem Upgrade in Ihrer Instanz aktiv sind. Für neue Instanzen verwendet Discovery das Weblogic-Muster.

1. Die Probe „Windows - Active Processes“ oder „Linux - Active Processes“ erkennt einen laufenden Prozess, der eines der folgenden Kriterien erfüllt:
   - Die Parameter des Prozesses enthalten *`weblogic.Server`*.
   - Die Parameter des Prozesses enthalten *`-Dweblogic.name`*.
2. Wenn eine Übereinstimmung mit einem der folgenden Kriterien vorliegt:
   - Ein Datensatz wird in der BEA Weblogic-Tabelle [cmdb_ci_app_server_weblogic] erstellt. Der Datensatz wird mit dem Servernamen und dem TCP-Port gefüllt, die aus dem laufenden Prozess erfasst werden.
   - Die Probe „Windows - Weblogic - Find config.xml“ oder „Linux - Weblogic - Find config.xml“ wird ausgelöst. Der Sensor dieser Probe fügt dem BEA Weblogic-Datensatz [cmdb_ci_app_server_weblogic] und gegebenenfalls dem Webanwendungsdatensatz [cmdb_ci_web_application] zusätzliche Informationen hinzu.
3. Die Probe „Windows - Weblogic - Find config.xml“ oder „Linux - Weblogic - Find config.xml“ versucht wie folgt, die zugehörige Datei `config.xml` für den Server zu finden:
   - Mit dem im laufenden Prozess definierten Parameter *`-Dweblogic.RootDirectory=<path>`*.
   - [Windows] Durch Suche nach den `config.xml`-Dateien unter dem im laufenden Prozess definierten Parameter *`-Dplatform.home=<path>`* (nicht so effizient wie die Verwendung der Prozessparameter).
   - [Linux] Durch Suche nach dem übergeordneten Prozess, der den WebLogic-Server gestartet hat (nur möglich, wenn die WebLogic-JVM über *`startWeblogic.sh`* oder ein zugehöriges benutzerdefiniertes Skript und nicht über den init-Prozess gestartet wurde).
4. Wenn in der WebLogic-Datei `config.xml` zugehörige Webanwendungen gefunden werden, wird die Probe „Windows - Weblogic Find web.xml“ für jede Anwendung ausgelöst. Diese Probe liest die WebLogic-Datei `web.xml` für jede Webanwendung und den Sensor und fügt zusätzliche Informationen hinzu.

IBM WebSphere-Server-Discovery mithilfe von Probes

Der IBM WebSphere-Anwendungsserver ist ein Software-Framework mit Middleware, das Java-basierte Webanwendungen hostet. Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine Instanz eines unter Windows oder Linux ausgeführten WebSphere-Anwendungsservers erkannt wird.

Hinweis: Ab Visibility Content Version 6.1.0 ist die musterbasierte Discovery die Standardmethode zur Erkennung von IBM WebSphere Application Server. Die WebSphere-Proben sind standardmäßig deaktiviert. Weitere Informationen finden Sie unter IBM WebSphere Application Server-Discovery anhand von Mustern.

Websphere-Erkennung unter Windows

Anforderungen für die Erkennung:

Aktivieren Sie für WebSphere-Anwendungsserver, die unter Windows ausgeführt werden, PowerShell auf dem MID Server.

Websphere-Erkennung unter Linux

Anforderungen für die Erkennung:

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

- Aktivieren Sie SSH auf dem WebSphere-Anwendungsserver.
- Legen Sie Ausführungsrechte fest, damit die folgenden Probes Befehle ausführen können:
  - WebSphere - Get serverindex.xml: cat/read-Berechtigungen für die Datei `serverindex.xml`
  - WebSphere - Get cell.xml: cat/read-Berechtigungen für die Datei `cell.xml`
  - WebSphere - Get server.xml: cat/read-Berechtigungen für die Datei `server.xml`

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Sonden und Sensoren

Discovery verwendet den folgenden Prozess, um Linux WebSphere-Anwendungsserver zu identifizieren:

1. Die Probe „Unix - Active Processes“ erkennt einen laufenden Prozess, der *`com.ibm.ws.runtime.WsServer`* entspricht. Beispielsweise enthält die Ausgabe des Prozesses *`...com.ibm.ws.bootstrap.WSLauncher com.ibm.ws.runtime.WsServer`* den Parameter */opt/IBM/WPS/profiles/ccmdb/config localhostNode01Cell ccmdb01 server1*. Die Werte sind:
   - letzter Parameter = Servername = Server1
   - letzter Parameter - 1 = Knotenname = ccmdb01
   - letzter Parameter - 2 = cell_name = localhostNode01Cell
   - letzter Parameter - 3 = config_path = ‘/opt/IBM/WPS/profiles/ccmdb/config’
2. Bei Übereinstimmung wird ein Datensatz in der IBM Websphere-Tabelle [cmdb_ci_app_server_websphere] erstellt. Die folgenden Probes werden ausgelöst:
   - WebSphere - Cell
   - WebSphere - Web Applications
   - WebSphere –Web Services
3. Von der Probe „WebSphere - Cell“ wird nach der `cell.xml`-Datei für die Instanz gesucht, indem die Parameter im ausgeführten Prozess verwendet werden und dann im zugehörigen Verzeichnis `<config_path>\cells\<cell_name>\` gesucht wird.
4. Wenn die `cell.xml`-Datei von der Probe gefunden wurde, wird ihr Inhalt vom Sensor gelesen. Die zusätzlichen Tabellendatensätze der Tabelle [cmdb_ci_websphere_cell] werden nach Bedarf ausgefüllt.
5. Wenn die `serverindex.xml` -Datei von der Probe gefunden wurde, wird der Inhalt vom Sensor gelesen, und zusätzliche Datensätze der Webanwendungstabelle [cmdb_ci_web_application] werden nach Bedarf ausgefüllt.
6. Wenn die `server.xml`-Datei von der Probe gefunden wurde, wird ihr Inhalt vom Sensor gelesen, und zusätzliche Datensätze der Webservicetabelle [cmdb_ci_web_service] werden nach Bedarf ausgefüllt.

Discovery verwendet den folgenden Prozess, um Windows WebSphere-Anwendungsserver zu identifizieren:

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

1. Die Probe „Windows - Active Processes“ erkennt einen laufenden Prozess, der *com.ibm.ws.runtime.WsServer* entspricht. Beispielsweise enthält die Ausgabe des Prozesses *...com.ibm.ws.bootstrap.WSLauncher com.ibm.ws.runtime.WsServer* den Parameter */opt/IBM/WPS/profiles/ccmdb/config localhostNode01Cell ccmdb01 server1*. Die Werte sind:
   - letzter Parameter = Servername = Server1
   - letzter Parameter - 1 = Knotenname = ccmdb01
   - letzter Parameter - 2 = cell_name = localhostNode01Cell
   - letzter Parameter - 3 = config_path = ‘/opt/IBM/WPS/profiles/ccmdb/config’
2. Bei Übereinstimmung wird ein Datensatz in der IBM Websphere-Tabelle [cmdb_ci_app_server_websphere] erstellt. Die folgenden Probes werden ausgelöst:
   - Windows - WebSphere - Cell
   - Windows - WebSphere - Web Applications
   - Windows - WebSphere –Web Services
3. Die Probe „Windows - WebSphere - Cell“ sucht nach der Datei `cell.xml` für die Instanz, indem die Parameter im laufenden Prozess verwendet werden und dann im zugehörigen Verzeichnis `<config_path>\cells\<cell_name>\` gesucht wird.
4. Wenn die `cell.xml`-Datei von der Probe gefunden wurde, wird ihr Inhalt vom Sensor gelesen. Die zusätzlichen Tabellendatensätze der Tabelle [cmdb_ci_websphere_cell] werden nach Bedarf ausgefüllt.
5. Die Probe „Windows - WebSphere - Web Applications“ sucht nach der Datei `serverindex.xml` für die Instanz, indem die Parameter im laufenden Prozess verwendet werden und dann im zugehörigen Verzeichnis `<config_path>\cells\<cell_name>\nodes\<node_name>` gesucht wird.
6. Wenn die `serverindex.xml` -Datei von der Probe gefunden wurde, wird der Inhalt vom Sensor gelesen, und zusätzliche Datensätze der Webanwendungstabelle [cmdb_ci_web_application] werden nach Bedarf ausgefüllt.
7. Die Probe „Windows WebSphere - Web Services“ sucht nach der Datei `server.xml` für die Instanz, indem die Parameter im laufenden Prozess verwendet werden und dann im zugehörigen Verzeichnis `<config_path>\cells\<cell_name>\nodes\<node_name>\servers\<server_name>` gesucht wird.
8. Wenn die `server.xml`-Datei von der Probe gefunden wurde, wird ihr Inhalt vom Sensor gelesen, und zusätzliche Datensätze der Webservicetabelle [cmdb_ci_web_service] werden nach Bedarf ausgefüllt.

Erfasste Daten

Auf Websphere-Servern unter Windows erfasste Daten

Tabelle	Feld	Quelle
cmdb_ci_app_server_websphere	Name (name)	Laufender Prozess
cmdb_ci_websphere_cell	Name (name)	cell.xml
cmdb_ci_websphere_cell	Zellen-ID (cell_id)	cell.xml
cmdb_ci_websphere_cell	Zellentyp (cell_type)	cell.xml

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

Auf Websphere-Servern unter Windows erfasste Daten (Fortsetzung)

Tabelle	Feld	Quelle
cmdb_ci_websphere_cell	Zellenerkennungsprotokoll (cell_discovery_protocol)	cell.xml
cmdb_ci_web_service	Name (name)	server.xml
cmdb_ci_web_service	Service-ID (service_id)	server.xml
cmdb_ci_web_application	Name (name)	serverindex.xml

Auf Websphere-Servern unter Linux erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_websphere_cell	Name	server.xml
App-Server	cmdb_ci_web_service	app_server	Interne Referenz
Name	cmdb_ci_web_service	Name	server.xml
Name	cmdb_ci_web_application	Name	serverindex.xml
App-Server	cmdb_ci_web_application	app_server	serverindex.xml

Beziehungen

In der Tabelle „CI-Beziehungen“ [cmdb_rel_ci] werden die folgenden Beziehungen erstellt.

Übergeordnete Klasse	Beziehungstyp	Untergeordnete Klasse
cmdb_ci_app_server_websphere	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_linux_server
cmdb_ci_win_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_win_server
cmdb_ci_app_server_websphere	Enthält::Enthalten in	cmdb_ci_web_application
cmdb_ci_web_service	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_app_server_websphere
cmdb_ci_websphere_cell	Enthält::Enthalten in	cmdb_ci_app_server_websphere

Erkennung von Datenbanken

Discovery kann nach Datenbankanwendungen wie MySQL, Oracle und MongoDB suchen. Außerdem kann Discovery auch nach Software zur Datenbankverwaltung wie MSSQL Server suchen.

Erkennung von Datenbankkatalogen

Der Datenbankkatalog listet alle Katalogobjekte oder Datenbanken auf, die für eine Instanz einer Datenbank erkannt wurden.

Datenbanken und Kataloge im Vergleich

Die meisten Datenbankhersteller verwenden für eine Datenbank den Begriff Katalog, während Microsoft MSSQL den Begriff Datenbank verwendet. Datenbankkataloge können

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

über das Erkennungstool eines Drittanbieters in Ihre Instanz importiert, manuell in die Plattform eingegeben oder von Discovery erkannt werden.

Wichtig: Discovery unterstützt im Basissystem keine Katalog-Discovery für MySQL-Datenbanken. Die Muster für Oracle DB unter Unix und Oracle DB unter Windows erkennen Oracle-Katalogobjekte über die Mustererweiterung „Kataloginformationen abrufen“. Für die MSSQL-Discovery wird standardmäßig die Probe Windows – MSSQL für die MSSQL-Katalog-Discovery verwendet, während das Muster MSSQL-DB unter Windows MSSQL-Datenbanken erkennt. Beachten Sie, dass das Muster und die Probe nicht die gleichen Informationen füllen.

Um einen Datenbankkatalog anzuzeigen, navigieren Sie zu **Alle** > **Konfiguration** > **Datenbankkataloge** und wählen Sie eine Datenbank aus.

MSSQL-Nutzung von Katalogen

In MSSQL-Datenbankkatalogen werden Metadaten zu einer MSSQL-Datenbank in der Tabelle „MSFT SQL-Katalog“ [cmdb_ci_db_mssql_catalog] gespeichert, die nur von Probes verwendet wird. Im Basissystem enthält das Formular „MSFT SQL-Katalog“ zwei Felder: **Name** und **Datenbankinstanz**. Sie können das Formularlayout anpassen, um weitere Felder anzuzeigen.

So greifen Sie auf einen MSFT SQL-Katalogdatensatz zu:

1. Navigieren zu **Alle** > **Konfiguration** > **Datenbankinstanzen** > **MSSQL** und wählen Sie einen Datensatz aus.
2. Wählen Sie im Instanzdatensatz die zugehörige Liste **MSFT SQL-Kataloge** aus.
3. Öffnen Sie einen in der Liste vorhandenen Datensatz, oder klicken Sie auf **Neu**, um einen neuen Katalogdatensatz zu erstellen.

Discovery-Berichte von Database Administrator (DBA).

Discovery und Service-Mapping verwenden die Erweiterungsabschnitte Muster, um einen Datenbankadministratorbericht (DBA-Bericht) für die Datenbanken Apache Cassandra, MicrosoftMicrosoft Azure Event Hubs SQL, MySQL, MongoDB und Oracle bereitzustellen. Die Erweiterungsabschnitte für jedes DB-Muster füllen die zugehörigen Eintragstabellen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Voraussetzungen

Überprüfen Sie die Einrichtung der Plugins

- CMDB CI-Klassenmodelle 1.49.0 (September 2023)
- Muster für Discovery und Service-Mapping 1.8.0 (September 2023)

Vergewissern Sie sich, dass die Systemeigenschaften von aktiviert sind

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

Standardmäßig sind die Systemeigenschaften für DBA-Berichte auf **false**festgelegt. Stellen Sie zum Aktivieren der Berichtsammlung sicher, dass der Wert der Systemeigenschaften für jedes Muster auf **true**festgelegt ist.

Muster	Systemeigenschaft
Cassandra	cassandra_dba_report_enabled
MongoDB	mongo_dba_report_enabled
MSSQL-DB unter Windows	mssql_dba_report_enabled
My SQL server Unter Windows und Linux	mysql_dba_report_enabled
Oracle-DB	oracle_dba_report_enabled

Überprüfen Sie die Konfiguration der Anmeldeinformationen

Weitere Informationen finden Sie unter Applicative-Anmeldeinformationen .

MongoDB-Ausführungsbefehl	Applicative-Anmeldeinformationen müssen Lesezugriff haben, um `„getSiblingDB (databaseName)“`auszuführen.
Apache Cassandra Befehl ausführen	Discovery-Anmeldeinformationen müssen Lesezugriff auf `„nodetool“`haben.
MySQL-Tabellen und -Befehle ausführen	Discovery-Anmeldeinformationen müssen Lesezugriff auf Folgendes haben: • Tabelle`„information_schema.tables“` • Führen Sie den Befehl `„show databases“` aus
MicrosoftMicrosoft Azure Event Hubs SQL-Tabellen	Discovery-Anmeldeinformationen müssen Lesezugriff auf die folgenden Tabellen haben: • *master.sys.databases* • *sys.sysprocesses* • *sys.dm_os_sys_info* • *sys.dm_os_ring_buffers* • *msdb.dbo.backupset* • *master.dbo.sysdatabases* • *master..sysprocesses* • *msdb..sysjobactivity* • *sys.master_files* • *sys.dm_tran_session_transactions*

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

	• *sys.dm_os_sys_memory* • *sys.database_files*
Oracle DB-Tabellen und führen Sie Befehle aus	Discovery Anmeldeinformationen müssen Lesezugriff auf Folgendes haben: • Führen Sie die Befehle „`lsnrctl services`“ und „`sqlplus`“ aus • *dba_data_files* Tabelle • *dba_segments* Tabelle • *v$database* Tabelle • *gv$instance* Tabelle • *dba_hist_osstat* Tabelle • *dba_hist_snapshot* Tabelle • *v$asm_disk* Tabelle • *v$asm_diskgroup* Tabelle • *dba_audit_session* Tabelle • *gv$session_longops* Tabelle • *gv$session* Tabelle • *gv$sqlarea* Tabelle • *gv$process* Tabelle

Stellen Sie sicher, dass ein Zeitplan Discovery konfiguriert ist

Weitere Informationen finden Sie unter Discovery-Zeitplan erstellen

Daten, die vom Erweiterungsabschnitt des Musters Apache Cassandra gesammelt werden

Discovery füllt die folgenden Daten aus, wenn das Muster Apache Cassandra ausgeführt wird.

Hinweis: Im Abschnitt Voraussetzungen finden Sie wichtige Informationen zum Aktivieren der Systemeigenschaft.

Tabellenname	Tabellenbezeichnung	Felder
cassandra_health_report	Cassandra-Integritätsbericht	• database_host • local_write_latency • „read_latency“ • Snapshot_verwendeter_Bereich • Platz_verwendet • Tabelle

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

Tabellenname	Tabellenbezeichnung	Felder
		• Keyspace • ci

Daten, die vom Erweiterungsabschnitt des MongoDB-Musters erfasst wurden

Discovery füllt die folgenden Daten aus, wenn das MongoDB-Muster ausgeführt wird.

Hinweis: Im Abschnitt Voraussetzungen finden Sie wichtige Informationen zum Aktivieren der Systemeigenschaft.

Tabellenname	Tabellenbezeichnung	Felder
mongo_db_statistiken	Mongo DB-Statistiken	• database_host • database_name • fs_total_size • fs_used_size • scale_factor • index_size • index_count • Extents_count • storage_size • data_size • durchschn. Objektgröße • object_count • Sammlung_Anzahl • view_count • ci

Daten, die vom Erweiterungsabschnitt des MSSQL-Musters gesammelt wurden

Discovery füllt die folgenden Daten aus, wenn das MSSQL-Muster ausgeführt wird.

Hinweis: Im Abschnitt Voraussetzungen finden Sie wichtige Informationen zum Aktivieren der Systemeigenschaft.

Tabellenname	Tabellenbezeichnung	Felder
ms_sql_db_blocking_info	MSSQL-DB-Blockierungsinformationen	• database_host • database_instance • Definition • object_name

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

Tabellenname	Tabellenbezeichnung	Felder
		• Blocking_spid • spid • ci
ms_sql_db_cpu_util	MSSQL-DB-CPU-Dienstprogramm	• database_host • database_instance • load_date • other_process_cpu_util • other_process • system_idle_process • „sql_server_cpu_util“ • event_time • server_name • ci
ms_sql_db_not_backup	MSSQL-DB – kein BackUp	• database_host • database_instance • last_backup_date • database_name • ci
ms_sql_db_running_job	Ausgeführter MSSQL-DB-Auftrag	• database_host • database_instance • Anmeldename • nt_domain • cmd • hostname • name • status • open_tran • SPID • last_wait_type • „login_time“ • ci
ms_sql_disk_info	MSSQL-DB-Datenträgerinformationen	• database_host • database_instance

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

Tabellenname	Tabellenbezeichnung	Felder
		• Prozentsatz_freier_Speicherplatz • volume_free_space • volume_capacity • volume_label • volume_name • ci
ms_sql_files_space	MSSQL-DB-Dateibereich	• database_host • database_instance • database_name • Free_Space_MB • Dateigröße_MB • file_type • file_logic_name • ci
ms_sql_fregment_info	Informationen zur MSSQL-DB-Fragmentierung	• database_host • database_instance • index_status • page_count • avg_frag • index_name • object_name • schema_name • ci
ms_sql_last_restart	Letzter Neustart der MSSQL-DB	• database_host • database_instance • uptime_in_days • current_date • last_recycle • ci
ms_sql_long_trans	Lange MSSQL-DB-Transaktionen	• database_host • database_instance • blockiert • SQL

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

Tabellenname	Tabellenbezeichnung	Felder
		• cmd • Programmname • hostname • Anmeldename • status • last_batch • Dauer • „login_time“ • database_name • user_tran • trans_id • spid • ci
ms_sql_memory_info	Informationen zum MSSQL-DB-Arbeitsspeicher	• database_host • database_instance • system_memory_state_desc • percentage_used • available_page_file_mb • total_page_file_mb • available_physical_memory_mb • total_physical_memory_mb • ci
ms_sql_temp_files_space	MSSQL-DB-Temp-Dateibereich	• database_host • database_instance • percent_full • available_space_mb • file_physical_name • file_logic_name • database_name • ci

Vom Erweiterungsabschnitt des MySQL-Musters gesammelte Daten

Discovery füllt die folgenden Daten aus, wenn das MySQL-Muster ausgeführt wird.

Hinweis: Im Abschnitt Voraussetzungen finden Sie wichtige Informationen zum Aktivieren der Systemeigenschaft.

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

Tabellenname	Tabellenbezeichnung	Felder
mysql_table_schemas	MySQL-Tabellenschemas	• database_host • database_instance • data_index_länge • table_schema • ci

Daten, die vom Erweiterungsabschnitt des DB-Musters Oracle gesammelt werden

Discovery füllt die folgenden Daten aus, wenn das DB-Muster Oracle ausgeführt wird.

Hinweis: Im Abschnitt Voraussetzungen finden Sie wichtige Informationen zum Aktivieren der Systemeigenschaft.

Tabellenname	Tabellenbezeichnung	Felder
oracle_active_session	Oracle Aktive Sitzung	• database_host • database_instance • Key • sql_id • Programm • Modul • Aktion • status • last_call_et_hrs • sid • spid • Inst • ci
oracle_asm_info	Oracle, ASM-Datenträgerinformationen	• database_host • database_instance • used_gb • Free_GB • total_gb • state • Blockgröße

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

Tabellenname	Tabellenbezeichnung	Felder
		• asm • ci
oracle_asm_nodes_info	Oracle Datenträgerinformationen für ASM-Knoten	• database_host • database_instance • Redundanz • Free_GB • total_gb • state • asm_node • ci
oracle_cpu_usage	Oracle CPU-Auslastung	• database_host • database_instance • Leerlauf • io • sys • Sehr gut • user • SnapID • Inst • end_time • begin_time • ci
oracle_inactive_sessions	Oracle Inaktive Sitzungen	• database_host • database_instance • Schlüssel • status • spid • sid • Programm • Modul • last_call_et_hrs • Inst • ci

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

Tabellenname	Tabellenbezeichnung	Felder
oracle_instance_info	Oracle Instanzinformationen	• database_host • database_instance • Platform_name • current_scn • DBID • db_unique_name • log_mode • db_name • open_mode • ci
oracle_nodes_info	Oracle Knoteninformationen	• database_host • database_instance • instance_mode • instance_state • instance_role • instance_status • instance_version • hostname • instance_name • ci
oracle_table_space	Oracle Tabellenbereich	• database_host • database_instance • used_mb • Free_Prozent • Free_mb • Tabellenbereich • total_mb • ci
Oracle_top_10_queries	Oracle Top 10 Abfragen	• database_host • database_instance • Eindeutig • status • sql_id • spid

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

Tabellenname	Tabellenbezeichnung	Felder
		• sid • Programm • Modul • last_call_et_hrs • ci

MicrosoftMicrosoft Azure Event Hubs SQL Server- und Cluster-Discovery

Die Anwendung Discovery und Service-Mapping verwenden das Muster „MSSQL DB auf Windows “ , um MicrosoftMicrosoft Azure Event Hubs SQL DB-Server und -Cluster in Ihrer -Infrastruktur zu finden. Zum Erkennen dieser Ressourcen muss der Funktionssatz Muster für Discovery und Service-Mapping aus dem Element ServiceNow Storeaktualisiert werden.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping ab Version 1.7.0 (August 2023)
- Visibility Content ab Version 6.12.1 (August 2023)

Ausführliche Informationen zu den unterstützten Versionen von SQL Server finden Sie unter: Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Überprüfen Sie die Konfiguration der Anmeldeinformationen Windows .

Stellen Sie sicher, dass MID-Server mit dem Zielserver Windows verbunden ist. Weitere Informationen finden Sie unter Windows-Anmeldeinformationen

Überprüfen Sie bei Verwendung der SQL-Authentifizierung die Konfiguration der Applicative-Anmeldeinformationen .

Überprüfen Sie die Konfiguration von MID-Server

Stellen Sie sicher, dass MID-Server über die erforderlichen Berechtigungen zum Lesen der Windows -Registrierung im -Remote- - Modusverfügt. Die MSSQL-DB auf Windows verwendet Registrierungswerte, um SQL-Cluster-Details zu erkennen.

Überprüfen Sie die Berechtigungen zum Ausführen von WMI-Abfragen

Verifizieren Sie den schreibgeschützten Remote-Lesezugriff auf die folgenden WMI-Namespaces:

- `Stamm\CIMv2`
- `Stamm\Microsoft\SQLServer\ComputerManagement*`

Überprüfen Sie die SQL Server-Tabellenberechtigungen

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

Das Muster „MSSQL DB unter Windows“ erfordert schreibgeschützte Berechtigungen zum Lesen der folgenden Tabellen:

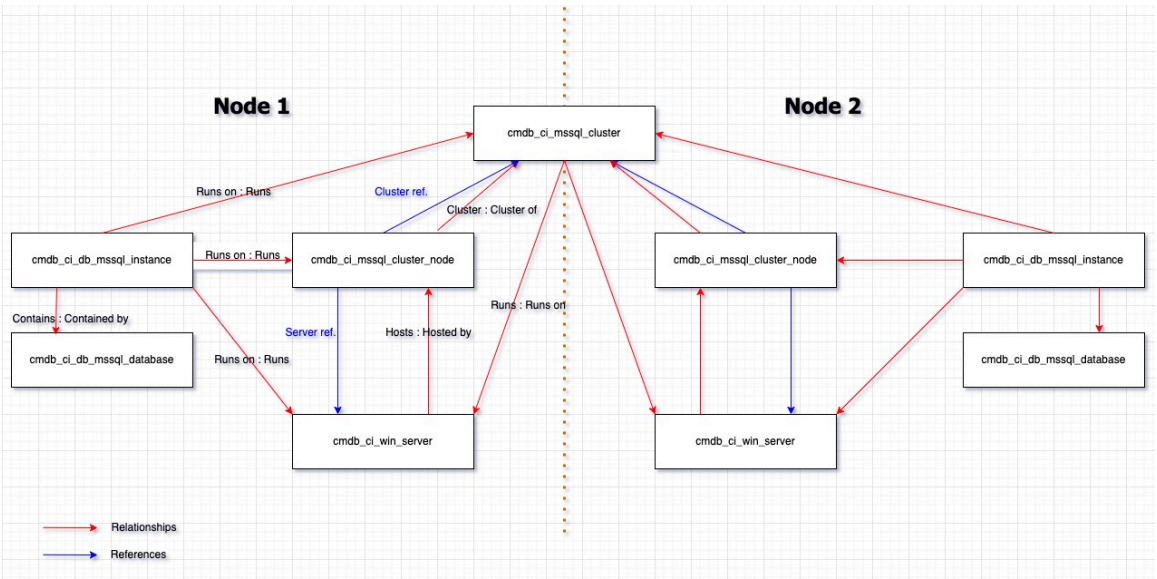
- `@@Version`
- `sys.configurations`
- `sys.dm_exec_sessions`
- `sys.dm_os_schedulers`
- `Servereigenschaft`

Überprüft die Konfiguration des Discovery-Berichts zum MSSQL-Setup

Das Muster führt die Discovery mithilfe eines Discovery-Berichts des MSSQL-Setups aus.

SQL-Failover-Clusterinstanz (FCI)

Die Aktualisierung des Mustersatzes Version 1.6.1, der ab August 2023 im ServiceNow® Store verfügbar ist, ermöglicht eine angemessene Erkennung der Details der Immer On-Verfügbarkeitsgruppe und der SQL-Failover-Cluster. Wenn das Failover-Szenario auftritt, erkennt das Muster „MSSQL DB unter Windows“ den Failover-Cluster (Knoten 2). Dann werden eine neue MSFT-SQL-Instanz und Datenbanken erstellt.



Das folgende Verfahren ermöglicht eine entsprechende Transparenz der SQL-Cluster.

1. Legen Sie die Eigenschaft *`sn_itom_pattern.discover_mssql_cluster.load_cluster_name_from_registry=true`* MID-Server auf **„true“** fest, um den Abschnitt **„MSSQL-Clusterinformationen sammeln – MSSQL-Clustererweiterung“** zu aktivieren.
2. Stellen Sie sicher, dass auf dem Server ein Prozess vom `Typ „sqlserver.exe“` zum Auslösen des Musters „MSSQL DB unter Windows“ ausgeführt wird.
3. Führen Sie eine CI-Discovery aus.

   Weitere Informationen finden Sie unter Erkennungen im Netzwerk ausführen.
4. Behalten Sie doppelte Instanzen und Datenbanken bei, oder löschen Sie sie.

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

- Um die doppelten Instanzen und Datenbanken beizubehalten, behalten Sie die Standardkonfiguration bei.
  - Der Installationsstatus der Knoten des passiven Clusters ändert sich in **Abwesend**.
  - Der Installationsstatus der Knoten des aktiven Clusters ändert sich in **Installiert**.
- Um die passiven Instanzen und Datenbanken zu löschen, setzen Sie die Systemeigenschaft *discovery.mssql.cluster.instance.postsensor.delete* auf den **Wert true**.

Während der horizontalen Erkennung erfasste Daten

MSFT SQL-Instanz [cmdb_ci_db_mssql_instance]

Die für die laufenden Prozesse der Datenbank (des eigentlichen SQL-Servers) gesammelten Daten werden als Datenbankinstanzbezeichnet

Feld	Beschreibung
Name [name]	Der Feldname. Beispiel: MSSQLSERVER@windows_server_name
Instanzname [instance_name]	Der Name der MSSQL-Instanz. Beispiel: MSSQLSERVER
Ist geclustert [is_clustered]	Gibt den Typ der Installation an: • Wenn dieser Wert auf **true**festgelegt ist, ist der SQL Server Teil eines Clusters, und der Failover-Mechanismus ist aktiviert. • Wenn dieser Wert auf **False**festgelegt ist, ist der SQL Server eine eigenständige Bereitstellung, und der Failover-Mechanismus ist deaktiviert.
Kommentare [comments]	Der Typ der Instanz: • standalone_instance • „failover_cluster“ • „always_on“
Version [version]	Die SQL Server-Versionsnummer. Beispiel: 16.0.1000.6
Versionsname [version_name]	Die SQL Server-Version nach Release-Daten. Beispiel: Der Wert **2022** steht für Version **16.0.1000.6**
Service Pack [service_pack]	Die Service Pack-Version. Beispiel: SP2.
Edition [edition]	Der Typ der Edition. Beispiel: Enterprise Edition.
TCP-Port [tcp_port]	Der TCP-Port, den die MSSQL-Instanz zum Akzeptieren von Verbindungen verwendet.
Installationsstatus [install_status]	Der Installationsstatus der Instanz:

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

Feld	Beschreibung
	Installiert: Die Instanz wird derzeit ausgeführt. **Abwesend**: Die Instanz wird nicht ausgeführt und ist die Sicherungsinstanz für ein Failover-Szenario.

MSSQL-Datenbank [cmdb_ci_db_mssql_database]

Feld	Beschreibung
Name [name]	Name der Datenbank Beispiel: msdb.
Installationsstatus [install_status]	Der Installationsstatus der Datenbank.
Instanzname [instance_name]	Der Name der Instanz.

MSSQL-Clusterknoten [cmdb_ci_mssql_cluster]

Feld	Beschreibung
Name [name]	Der Hostname des Servers
IP-Adresse [ip_address]	IP-Adresse des Hostservers Windows
Cluster [cluster]	Verweis auf den SQL-Clusterdatensatz.
Server [Server]	Verweis auf den Datensatz des Host-Servers Windows.

MSSQL-Cluster [cmdb_ci_mssql_cluster]

Feld	Beschreibung
Name [name]	Der Netzwerkname des SQL-Clusters
IP-Adresse [ip_address]	Die virtuelle IP-Adresse des SQL-Clusters [.

MSSQL-Serviceinformation [mssql_sqlservice_info]

Feld	Beschreibung
Beschreibung [description]	Beschreibt den MSSQL-Service. Beispiel: „Bietet die Speicherung, Verarbeitung und den kontrollierten Zugriff von Daten sowie schnelle Transaktionsverarbeitung.“
Servicename [service_name]	Der auf dem Server dargestellte MSSQL-Servicename. Beispiel: MSSQL$NAMEDMSSQL2016
Binärpfad [binary_path]	Der Dateipfad des Service. Beispiel: `C:\Programme \Microsoft SQL Server\MSSQL13.NAMEDMSSQL2016\MSSQL \Binn\sqlserver.exe`
CI [ci]	Verweis auf MSFT-SQL-Instanzdatensatz [cmdb_ci_db_mssql_instance]

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

Feld	Beschreibung
Installiert auf [installed_on]	Verweis auf den Datensatz des Servers Windows [cmdb_ci_win_server] **Hinweis:** Dieses Feld wird für eigenständige Bereitstellungen nicht ausgefüllt.

Info zu MSSQL-Komponenten [mssql_components_info]

Feld	Beschreibung
Installationspfad [install_path]	Der Installationspfad des Komponentenservice. Beispiel: `C:\Programme\Microsoft SQL Server \MSSQL16.SQLEXpress\MSSQL`
Servicename [service_name]	Der Komponentenservicetyp des Servers. Beispiel: **Datenbank-Engine-Services**
SKU-Name [sku_name]	Die MSSQL-Version des Komponentenservice. Beispiel: **Express Edition (64 Bit)**
Version [version]	Die MSSQL-Versionsnummer des Komponentenservice
CI [ci]	Verweis auf den Datensatz der MSFT-SQL-Instanz.
Installiert auf [installed_on]	Verweis auf den Serverdatensatz Windows [cmdb_ci_win_server]. **Hinweis:** Dieses Feld wird nur für SQL-Cluster und nicht für eigenständige Bereitstellungen ausgefüllt.

CI-Beziehungen

Das Muster „MSSQL DB On Windows “ erstellt CI-Beziehungen des Typs mithilfe des Erweiterungsabschnitts **„MSSQL-Komponenteninformationen sammeln“**, der in der folgenden Tabelle aufgeführt ist.

CI	Beziehung	CI
Windows-Server [cmdb_ci_win_server]	Wird ausgeführt:Wird ausgeführt auf	MSSQL-Cluster [cmdb_ci_mssql_cluster]
MSFT SQL-Instanz [cmdb_ci_db_mssql_instance]	Wird ausgeführt:Wird ausgeführt auf	MSSQL-Cluster [cmdb_ci_mssql_cluster]

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

CI	Beziehung	CI
MSSQL-Clusterknoten [cmdb_ci_mssql_cluster_node]	Cluster::Cluster von Referenz [Cluster]	MSSQL-Cluster [cmdb_ci_mssql_cluster]
Windows Server [cmdb_ci_win_server]	Hosts::Gehostet von Referenz [Server]	MSSQL-Clusterknoten [cmdb_ci_mssql_cluster_node]
MSFT SQL-Instanz [cmdb_ci_db_mssql_instance]	Wird ausgeführt auf::Wird ausgeführt	Windows Server [cmdb_ci_win_server]
MSFT SQL-Instanz [cmdb_ci_db_mssql_instance]	Enthält::Enthalten in	MS SQL-Datenbank [cmdb_ci_db_mssql_database]
[mssql_sqlservice_info] **Hinweis:** Diese Beziehung wird nur erstellt, wenn das Muster die WMI-Abfragen verwendet.	Referenz	[cmdb_ci_mssql_instance]

Zugehörige Informationen

Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen

Probe „Horizontal Pattern“

Discovery-Berichte von Database Administrator (DBA).

MySQL-Erkennung

Discovery kann eine unter UNIX oder Windows ausgeführte Instanz von MySQL erkennen.

Anforderungen

Discovery sucht für die folgenden Bereiche nach dem Speicherort der MySQL-Konfigurationsdatei:

- UNIX: Discovery sucht nach dem Speicherort der MySQL-Konfigurationsdatei im Prozess mysqld oder an Port 3306.
- Windows: Discovery sucht nach dem Speicherort der MySQL-Konfigurationsdatei im Prozess mysqld.exe oder an Port 3306.

Für jeden Prozess werden die folgenden Prozessparameter in der folgenden Reihenfolge untersucht:

```
--defaults-extra-file
```

```
--defaults-file
```


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

Wenn der Speicherort der MYSQL-Konfigurationsdatei bei dieser Suche nicht gefunden wird, geschieht Folgendes:

- UNIX: Für den Speicherort der Konfigurationsdatei wird standardmäßig `/etc/my.cnf` übernommen.
- Windows: Es ist kein Standardspeicherort für Konfigurationsdateien vorhanden, und die Probe zum Lesen des Speicherorts für Konfigurationsdateien wird übersprungen.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Berechtigungen

Konfigurieren Sie die folgenden Anmeldeinformationen:

- Windows-Anmeldeinformationen
- SSH-Anmeldeinformationen
- [optional] Applicative-Anmeldeinformationen

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Klassifizierer, Muster und Probes

Zur MySQL-Erkennung verwendet Discovery die folgenden Klassifizierer, Probes und Muster:

Klassifizierung	Auslöser-Probes	Muster
MySQL-Server	• Horizontal Pattern: Startet Muster • Windows - MySQL Configuration* • Windows - MySQL Version* • MySQL - Configuration* • MySQL - Version*	My SQL server On Windows and Linux - Muster

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Discovery füllt die folgenden Felder in der Tabelle „MySQL-Instanz“ [cmdb_ci_db_mysql_instance]:

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

Bezeichnung	Feldname	Quelle
MySQL-Konfiguration	myconf	my.cnf
TCP-Port(s)	tcp_port	running_process
Version	Version	mysqld

Zugehörige Informationen

Discovery-Berichte von Database Administrator (DBA).

MongoDB-Erkennung

Discovery erstellt oder aktualisiert einen CMDB-Datensatz, wenn eine ausgeführte Instanz von MongoDB erkannt wird.

Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen .

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Die folgenden Daten werden erfasst:

Von Discovery für MongoDB-Instanzen erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Version	cmdb_ci_db_mongodb_instance	Version	mongod (UNIX) oder mongod.exe (Windows)
Mongo-Konfiguration	cmdb_ci_db_mongodb_instance	mongodb_conf	mongod.conf
TCP-Port(s)	cmdb_ci_db_mongodb_instance	tcp_port	Prozessklassifizierung oder mongod.conf

PostgreSQL-Erkennung

Discovery kann Instanzen von PostgreSQL erkennen, die unter Windows und Linux ausgeführt werden.

Anmeldeinformationen und andere Voraussetzungen

Die folgenden Anmeldeinformationen sind erforderlich:

- SSH-Anmeldeinformationen
- [optional] Applicative-Anmeldeinformationen

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort

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

finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Der Benutzer muss Root-Zugriff auf die Datenbank haben, um auf die Datei `postgresql.conf` zugreifen zu können.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
PostgreSQL-Instanz	• Horizontal Pattern: Startet Muster • PostgreSQL - Configuration* (diesem Probe Parameter *must_sudo* hinzufügen) • PostgreSQL - Version*	PostgreSQL-DB

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Mit dem folgenden Verfahren werden die angegebenen Informationen vom Ziel erfasst. Wenn die Quelle nicht konfiguriert ist, werden Standardinformationen zurückgegeben. Beispiel: Für PostgreSQL Instance@hostname (Standardname) muss die Quelle geändert werden. Andernfalls werden für die Tabelle [cmdb_ci_db_postgresql_instance] alle „PostgreSQL Instance@hostname“-Namen der Quelle hinzugefügt.

Bezeichnung	Tabellenname	Feldname	Quelle
Name	cmdb_ci_db_postgresql_instance	Name	PostgreSQL Instance@*Hostname*
Datenverzeichnis	cmdb_ci_db_postgresql_instance	data_dir	Laufender Prozess
TCP-Port	cmdb_ci_db_postgresql_instance	tcp_port	Laufender Prozess
SQL-Konfiguration	cmdb_ci_db_postgresql_instance	postgres_conf	*Datenverzeichnis*/postgresql.conf
Version	cmdb_ci_db_postgresql_instance	Version	postmaster/postgres

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

Beziehungen

Übergeordnete Klasse	Beziehung	Untergeordnete Klasse
cmdb_ci_db_postgresql_instance	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_windows_server oder cmdb_ci_linux_server

Oracle Discovery von Datenbanken

Discovery kann eine Oracle -Datenbankinstanz identifizieren, die unter den Betriebssystemen UNIX oder Windows ausgeführt wird. Von Discovery kann auch Oracle-Clusterware erkannt werden, von der Real Application Clusters (RAC) ausgeführt werden.

Muster führen die Discovery von Oracle -Installationen durch. Diese Muster ersetzen mehrere Probes für neue Instanzen. Wenn Sie weiterhin Probes verwenden möchten, können Sie die Probe „Horizontal Discovery“ deaktivieren, die das Muster startet, und dann die erforderlichen Probes aktivieren.

Hinweis: Oracle DB on Unix und Oracle DB on Windows unterstützen keine RAC-Einzelknoten-Discovery.

Die Muster für Oracle DB unter Unix und Oracle DB unter Windows erkennen die Katalogobjekte Oracle über die Mustererweiterung „Kataloginformationen abrufen“. Weitere Informationen finden Sie unter Oracle Katalog-Discovery. Allgemeine Informationen zur Erkennung von Datenbankkatalogen finden Sie unter Datenbankkataloge.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Anmeldeinformationen

Konfigurieren Sie die folgenden Anmeldeinformationen:

Anmeldeinformationstyp	Zusätzliche Information
Applicative-Anmeldeinformationen	Applicative-Anmeldeinformationen sind für zwei Anwendungsfälle obligatorisch: • SQL-Abfragen für die Remote-Instanz von Oracle DB werden ausgeführt • Verbindungen zu Datenbanklinks erstellen • Software Asset Management aktiviert Sie müssen den Datenbankanwender hinzufügen, den Sie während der Installation der Datenbank Oracle konfiguriert haben. Geben Sie als CI-Typ `Oracle-Instanz [cmdb_ci_db_ora_instance]` an. Der Benutzer muss auch über Zugriff auf die Parameterdatei *`tnsnames.ora`* verfügen. Stellen Sie sicher, dass tnsnames.ora richtig konfiguriert ist und im Pfad Oracle auf dem Windows-Zielhost vorhanden ist. Stellen Sie außerdem sicher, dass die verwendeten Discovery-Anmeldeinformationen die Datei tnsnames.ora lesen können.

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

Anmeldeinformationstyp	Zusätzliche Information
	Der Benutzer benötigt Berechtigungen für das SQL*Plus-Befehlszeilentool und Berechtigungen zum Ausführen von SELECT-Abfragen für die folgenden Tabellen: • PRODUCT_COMPONENT_VERSION • V$VERSION • V$DATABASE • V$PARAMETER
Windows-Anmeldeinformationen SSH-Anmeldeinformationen	Neben Applicative-Anmeldeinformationen können Sie auch Windows- und SSH-Anmeldeinformationen verwenden. Für Windows-Anmeldeinformationen muss der Benutzer über Leseberechtigungen für die Datei `tnsnames.ora` verfügen. SSH-Anmeldeinformationen müssen Leseberechtigung für die Datei `oratab` und Leseberechtigung für das Serverparameterfile aufweisen. Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Zusätzliche Anforderungen

Discovery identifiziert eine laufende Instanz einer Datenbank Oracle auf UNIX anhand des Prozesses, der mit `ora_pmon_` beginnt. Stellen Sie sicher, dass dieser Prozess in dem IP-Bereich ausgeführt wird, den Sie für Discoveryfestlegen. Discovery identifiziert eine laufende Instanz einer Datenbank Oracle auf Windows anhand des Prozesses `oracle.exe`. Stellen Sie sicher, dass dieser Prozess in dem von Ihnen festgelegten IP-Bereich ausgeführt wird.

Für Oracle Clusterware benötigen Sie außerdem Berechtigungen zum Lesen der Datei `/etc/hosts/`, die Hostnamen IP-Adressen zuordnet.

Die folgenden Befehle werden für Oracle clusterware ausgeführt:

Befehl	Beschreibung
`ps -ef | grep 'crsd.bin' |grep -v grep`	Überprüft, ob der CRS-Prozess Oracle ausgeführt wird.
`ps -ef |grep Listener | grep -v $$ | -Kopf -1 | awk „{print $8}"`	Ruft die Startseite Oracle ab.
`/u01/app/12.1.0.2/grid/bin/olsnodes -c | egrep -v 'Fehler|Rückgabecode'`	Ruft den Oracle CRS-Clusternamen ab.
`/u01/app/12.1.0.2/grid/bin/crsctl Abfrage CRS Softwareversion| egrep -v 'Fehler|Rückgabecode'`	Ruft Oracle die CRS-Cluster-ID ab.

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

Befehl	Beschreibung
`/u01/app/12.1.0.2/grid/bin/crsctl Abfrage CRS Softwareversion| egrep -v 'Fehler|Rückgabecode'`	Ruft die CRS-Version Oracle ab.
`/u01/app/12.1.0.2/grid/bin/olsnodes | egrep -v 'Fehler|Rückgabecode'`	Ruft Oracle CRS-Knoten ab.
`/u01/app/12.1.0.2/grid/bin/crsctl Statusserver | egrep -v 'Fehler|Rückgabecode'`	Ruft den CRS-Knotenstatus Oracle ab.
`/u01/app/12.1.0.2/grid/bin/crsctl stat res -f | TR '\n' '#'`	Ruft Oracle CRS-Ressourcen ab.
`/u01/app/12.1.0.2/grid/bin/crsctl stat res -p | grep -v CHECK_R |grep -v error |grep -v failed`	Ruft Oracle CRS-VIP-Ressourcen ab.
/u01/app/12.1.0.2/grid/bin/srvctl config scan | tr '\n' ' '	Ruft Oracle RAC-Sscan-VIP-Konfigurationen ab.
/u01/app/12.1.0.2/grid/bin/srvctl config VIP -node ol7-121-rac1 | egrep „Name“ | awk „{print $3}“	Ruft den Oracle CRS-VIP-Namen ab.
/u01/app/12.1.0.2/grid/bin/srvctl config VIP -node ol7-121-rac1 | grep „IPv4-Adresse:“ | awk „{print $4}“	Rufen Sie Oracle CRS-VIPs ip_address ab.

Sudo-Berechtigung zur Ausführung: `sudo /u01/app/12.1.0.2/grid/bin/ocrcheck | egrep -v 'error|return code'`

Klassifizierer, Muster und Probes

Discovery verwendet diese Klassifizierer, Probes und Muster für die Datenbank-Discovery Oracle von :

Klassifizierung	Auslöser-Probes	Muster
Oracle-Instanz	• Probe „Horizontal Discovery“: Startet Muster • Powershell-Oracle - Instance PFile (für Windows)* • Powershell-Oracle - Instance Version (für Windows)*	Anwendungsmuster: • Oracle DB On Windows • Oracle DB on UNIX Das folgende Muster für gemeinsam genutzte Bibliotheken, das vom Muster Linux Server verwendet wird: UNIX Cluster - ORACLE Clusterware **Hinweis:** Dieses Muster für die gemeinsame Bibliothek wird ausgelöst, wenn der Prozess `„crsd.bin“` auf dem Datenbankserver Oracle ausgeführt wird.

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

Klassifizierung	Auslöser-Probes	Muster
	• SSHCommand-Oracle - Instance Details (für Linux)*	
Oracle-Listener	SSHCommand-Oracle - Listener Details	keine

*Probes inaktiv für neue Instanzen

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Erfasste Daten

Die folgenden Daten werden in der Tabelle „Oracle-Instanzen“ [cmdb_ci_db_ora_instance] für UNIX und Windowsgesammelt:

Daten, die auf UNIX -Computern erfasst wurden

Bezeichnung	Feldname	Zusätzliche Informationen
SID	sid	Abgeleitet aus dem Namen des Prozesses, der mit `ora_pmon_` beginnt
Installationsverzeichnis	install_directory	Abgeleitet aus dem Pfad von `ORA_HOME`
Version	Version	In der folgenden Reihenfolge abgerufen: • Aus der Ausgabe des Befehls `ORA_HOME/bin/sqlplus/NOLOG` • Aus der Ausgabe des Statusbefehls `ORA_HOME/bin/lsnrctl` • Aus dem Pfad von `ORA_HOME`
Parameterdatei	pfile	Die folgenden Speicherorte werden für den Speicherort des Systemparameterfile untersucht. Wenn diese Datei an keinem der untersuchten Speicherorte vorhanden ist, findet Discovery die Datei nicht, und es wird ein Fehler gemeldet. • *oracle_home*/dbs/spfile*SID*.ora • *oracle_home*/dbs/spfile.ora • *oracle_home*/dbs/init*SID*.ora
Oracle Home	oracle_home	Aus der Datei *ORATAB* abgerufen
Edition	Edition	Abgerufen aus der Datei `context.xml`
Name	Name	Kombination aus SID-Name und Hostname im Format *SID@HOST_NAME*

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

Daten, die auf UNIX -Computern erfasst wurden (Fortsetzung)

Bezeichnung	Feldname	Zusätzliche Informationen
TCP-Port(s)	tcp_port	Abgerufen aus der Datei `tnsnames.ora` oder mit dem Statusbefehl *`lsnrctl`*. Wenn keine gültigen Informationen abgerufen werden, wird der Standardport 1521 zugewiesen.

Hinweis: Unter Oracle Optionen finden Sie Informationen über Mustererweiterungen und zusätzlich erfasste Informationen.

Daten, die auf Windows -Computern erfasst wurden

Bezeichnung	Feldname	Zusätzliche Informationen
SID	sid	Abgeleitet aus dem Prozessparameter, der an den Prozess *`oracle.exe`* übergeben wird
Installationsverzeichnis	install_directory	
Version	Version	Abgerufen aus der Ausgabe des Befehls *`ORA_HOME/bin/sqlplus.exe -V`*
Parameterdatei	pfile	Die folgenden Speicherorte werden für den Speicherort des Systemparameterfile untersucht. Wenn diese Datei an keinem der untersuchten Speicherorte vorhanden ist, findet Discovery die Datei nicht, und es wird ein Fehler gemeldet. • *`oracle_home`*\database\spfile*`SID`*.ora • *`oracle_home`*\database\spfile.ora • *`oracle_home`*\database\init*`SID`*.ora
Oracle Home	oracle_home	Analysiert aus dem Pfad von *`oracle.exe`*
Edition	Edition	

Hinweis: Unter Oracle Optionen finden Sie Informationen über Mustererweiterungen und zusätzlich erfasste Informationen.

Oracle Optionen

Allgemeine Informationen zu Oracle -Optionen finden Sie unter https://docs.oracle.com/en/ .

Discovery kann auch die Optionen Oracle finden, die Sie in der Instanz mit der Legacy-Mustererweiterung Oracle-Optionserweiterung für Windows/Unix aktivieren. Beachten Sie, dass zum Erkennen von Oracle -Optionen das Plugin „Software Asset Management Professional for Oracle“ (com.snc.samp.oracle) erforderlich ist.

Oracle-Optionen [samp_oracle_options]

Bezeichnung	Feldname
Instanz	instance

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

Oracle-Optionen [samp_oracle_options] (Fortsetzung)

Bezeichnung	Feldname
Option	option
Lizenzierbar	lizenzierbar
Derzeit verwendet	currently_used
Datum der ersten Verwendung	first_usage
Datum der letzten Verwendung	last_usage
Datum des letzten Beispiels	last_sample
Erkannte Verwendung	detected_usage
Beispielintervall	sample_interval

Benötigte Tabellenberechtigungen	Zusätzliche Informationen
Auf die folgenden Tabellen wird als Teil der Oracle-Optionserweiterung für UNIX und Windows zugegriffen: • DBA_FEATURE_USAGE_STATISTICS • CDB_FEATURE_USAGE_STATISTICS • V$DATABASE • V$VERSION • GV$PARAMETER • V$CONTAINERS • V$INSTANCE	Die folgenden Mustererweiterungen verwenden das Skript Oracle :optionen_packs_usage_statistik.sql. Dieses SQL-Skript kann für DB Server Version 11.2 und höher verwendet werden. Um das Skript auszuführen, benötigen Sie die Berechtigung zur **Auswahl eines beliebigen Wörterbuchs**. Weitere Informationen zu Usage-Skripts finden Sie im Supportdokument ID13172651.1 auf https://support.oracle.com/portal/ . • Oracle-Optionserweiterungen für UNIX • Oracle-Optionserweiterungen für Windows

Auf Clusterware erfasste Daten

Tabelle	Bezeichnungen und Feldnamen
Unix-Cluster [cmdb_ci_unix_cluster]	Name [name] Clusterstatus [cluster_status] Clustertyp [cluster_type] IP-Adresse [ip_address] Kurzbeschreibung [short_description] Cluster-ID [cluster_id] Clusterversion [cluster_version]
cmdb_ci_unix_cluster_node	Name [name]

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

Auf Clusterware erfasste Daten (Fortsetzung)

Tabelle	Bezeichnungen und Feldnamen
	Knotenzustand [node_state] IP-Adresse [ip_address] Knotenstatus [node_status]
cmdb_ci_unix_cluster_resource	Name [name] Ressourcentyp [resource_type] Ressourcenstatus [resource_status] Eigenschaften [properties]
cmdb_ci_cluster_vip	Name [name] IP-Adresse [ip_address] Clustername [cluster_name] Cluster-ID [cluster_id]

In der Abhängigkeitsansicht bedeutet **+1** für einen Oracle -Datenbankserver, dass er Teil eines Clusters ist.

Erweiterung „Extend Oracle instance“

Hinweis: Discovery finden Sie auch zusätzliche Attribute für die Instanz mithilfe der Erweiterung „Oracle-Instanz erweitern“. Weitere Informationen zu Optionen finden Sie auf der Website Oracle: https://docs.oracle.com/en/ . Discovery speichert diese Attribute in der Tabelle „Oracle-Instanzen“ [cmdb_ci_db_ora_instance].

Bezeichnung	Feldname
Instanz	instance
Host-Name	host_name
IS_CDB	cdb_yn
DB – Eindeutiger Name	db_unique_name
DB-Name	database_name
Replikation aktiviert	replication_enabled

Benötigte Tabellenberechtigungen	Zusätzliche Informationen
Als Teil der Erweiterung „Extend Oracle Instance“ für UNIX und Windows wird auf die folgenden Tabellen zugegriffen:	Die Erweiterung „Extend Oracle Instance“ muss installiert sein. Diese Erweiterung ist in der Anwendung Discovery and Service Mapping Patterns, Version 1.0.72 oder höher,

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

Benötigte Tabellenberechtigungen	Zusätzliche Informationen
• V$DATABASE • V$INSTANCE	enthalten, die aus dem ServiceNow Store heruntergeladen werden kann.

Oracle Instanzen auf virtuellen Maschinen

Wenn Instanzen Oracle auf virtuellen Computern gehostet werden, erstellt das System Beziehungen zwischen CIs.

CI	Beziehung	CI
Oracle-Instanz	Gehostet auf	Computer [cmdb_ci_computer] oder Server [cmdb_ci_server] **Hinweis:** Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.
Computer [cmdb_ci_computer] oder Server [cmdb_ci_server] **Hinweis:** Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.	Virtualisiert von	Computer [cmdb_ci_computer] oder Server [cmdb_ci_server] **Hinweis:** Das ist kein virtueller Computer.

Oracle Instanzen auf virtuellen Maschinen, die in den Clouds AWS oder Azure gehostet werden

Basisklasse	Beziehung	Abhängige Klasse
Oracle-Instanz	Gehostet auf	Computer [cmdb_ci_computer] **Hinweis:** Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.
Computer [cmdb_ci_computer] **Hinweis:** Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.	Virtualisiert von	Computer [cmdb_ci_computer] **Hinweis:** Das ist kein virtueller Computer.
Computer [cmdb_ci_computer]	Virtualisiert von	VM-Instanz [cmdb_ci_vm_instance]

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

Basisklasse	Beziehung	Abhängige Klasse
Hinweis: Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.		**Hinweis:** Die vCPU-Anzahl wird in diese Tabelle gefüllt.
VM-Instanz [cmdb_ci_vm_instance]	Gehostet auf	AWS-Rechenzentrum [cmdb_ci_aws_datacenter] oder Azure-Rechenzentrum [cmdb_ci_azure_datacenter]

Beziehungen für Clusterware

CI	Beziehung	CI
Unix-Cluster [cmdb_ci_unix_cluster]	Virtualisiert::Virtualisiert von	Virtuelle Cluster-IP [cmdb_ci_cluster_vip]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	Verwendet::Verwendet von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Cluster von::Cluster	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Gehostet auf::Hostet	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Cluster [cmdb_ci_unix_cluster]	Hostet::Gehostet auf	Linux-Server [cmdb_ci_linux_server]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Gehostet auf::Hostet	Linux-Server [cmdb_ci_linux_server]

Zugehörige Informationen

Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen

Probe „Horizontal Pattern“

Discovery-Berichte von Database Administrator (DBA).

SAP Sybase ASE-Erkennung

Discovery und Service-Mapping verwenden das Sybase-Muster, um SAP Sybase Adaptive Server Enterprise (ASE)-Datenbanken und -Kataloge in Ihrer -Infrastruktur zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative

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

Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind.

Muster für Discovery und Service-Mapping

CMDB CI-Klassenmodelle

Visibility Content

Einzelheiten zum erkannten Produkt finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Hinweis: Discovery sucht Sybase-Katalog, der nur auf Linux ausgeführt wird.

Überprüfen Sie die Konfiguration der OS-Server-Anmeldeinformationen.

Überprüfen Sie die Konfiguration der Applicative-Anmeldeinformationen

Achten Sie beim Konfigurieren der Applicative-Anmeldeinformationen darauf, `Sybase -Instanz [cmdb_ci_db_syb_instance]` als CI-Typ anzugeben.

Weitere Informationen zu Applicative-Anmeldeinformationen finden Sie unter Applicative-Anmeldeinformationen

Vergewissern Sie sich, dass der -Benutzer berechtigt ist, die folgenden Befehle auszuführen

Führen Sie den *isql* -Befehl aus.

Lassen Sie die Sybase-Umgebung einen der folgenden Befehle ausführen:

- `"echo -ne 'nocount für ausgewählten Namen aus sysdatabases festlegen\ngo\n' | " + $isql_path + " -U $$username$$ -P '$$password$$' -S " + $instance + " -w 999 -b -y " + $process.environmentVariables.SYBASE.value`
- `"export SYBASE=" + $process.environmentVariables.SYBASE.value + " && . " + $process.environmentVariables.SYBASE.value + "/SYBASE.sh && reflektieren -ne 'set nocount on auswählen des Namens aus sysdatabases\ngo\n ' | " + $isql_path + " -U $$username$$ -P '$$password$$' -S " + $instance + " -w 999 -b -y " + $process.environmentVariables.SYBASE.value`

Überprüft die Konfiguration eines Discovery -Zeitplans

Ausführliche Informationen finden Sie unter Erkennungen im Netzwerk ausführen

Daten, die während der Horizontal-Discovery erfasst wurden

Discovery füllt die folgenden Daten in CMDB aus, wenn das Sybase-Muster ausgeführt wird.

Sybase-Instanz [cmdb_ci_db_syb_instance]	
Bezeichnung	**Feldname**
Name	Name

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

Sybase-Instanz [cmdb_ci_db_syb_instance]	
Bezeichnung	**Feldname**
Version	Version
Installationsverzeichnis	install_directory
Instanzname	Instanz
Konfigurationsdatei	config_file

Sybase-Katalog [cmdb_ci_db_syb_catalog]	
Bezeichnung	**Feldname**
Name	Name

CI-Beziehungen

Diese Beziehungen werden erstellt, um die Sybase ASE-Erkennung zu unterstützen.

CI	Beziehung	CI
[cmdb_ci_db_syb_instance]	Enthält::Enthalten in	[cmdb_ci_db_syb_catalog]

Erkennung von Netzwerkgeräten

Discovery erkennt verschiedene Netzwerkgeräte. Dazu gehören Lastenausgleichsmodule, Router, TCP-Verbindungen und IP-Netzwerke. Geräte können mit herkömmlichen Port-Probes, Identifizierungs- und Erkundungs-Probes oder Mustern erkannt werden. Discovery unterstützt auch die Erkennung durch die Identifizierung von HTTP- und TCP-Verbindungen.

Hinweis: Informationen zu model_id und Hersteller finden Sie im Wissensartikel KB0687582 .

Lastenausgleicherkennung

Discovery kann Daten über Netzwerkrouter, Switches und Anwendungen erfassen.

Discovery unterstützt die Datenerfassung aus der folgenden Software und Hardware:

- A10
- Apache mod_jk und Apache mod_proxy
- Big-IP F5 Traffic Manager
- Cisco
- Citrix NetScaler
- HAProxy
- NGINX
- Alteon
- ACE
- RadWare

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

Wichtig: In Discovery werden Lastenausgleichsmodule als lizenzierbare Entitäten behandelt. Es wird versucht, sie hauptsächlich mithilfe von SNMP zu ermitteln. Wenn ein Load Balancer in Ihrem System, der auf einem Linux-Host ausgeführt wird, SNMP- und SSH-Ports geöffnet hat, könnte Discovery ihn basierend auf dem SSH-Port klassifizieren. Diese Klassifizierung hat Vorrang vor SNMP. Um sicherzustellen, dass Discovery Ihre Hardware-Load Balancer richtig klassifiziert, erstellen Sie ein Discovery-Verhalten für Load Balancer, das SNMP, jedoch nicht SSH enthält. Software-Load Balancer werden als Anwendungen behandelt.

Lastenausgleichsmuster

Ab dem Jakarta-Release verwendet Discovery vordefinierte Muster, um einige Typen von Lastenausgleichsmodulen für neue Instanzen zu erkennen (siehe Tabelle).

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Load Balancer	Musternamen und -beschreibung	Gefüllte CI-Haupttabelle
A10	A10 LoadBalancer	A10 Load Balancer [cmdb_ci_lb_a10]
ACE	ACE Load Balancer by SSH (früher ACE Load Balancer)	ACE [cmdb_ci_lb_ace]
Alteon	Alteon Load Balancer	Alteon [cmdb_ci_lb_alteon]
F5 BIG-IP	F5 - HD, F5 Load Balancer	F5 BIG-IPs [cmdb_ci_lb_bigip]
NetScaler	Netscaler Load Balancer	Citrix NetScaler [cmdb_ci_lb_netscaler]
Radware - AppDirector	AppDirector Load Balancer	Radware-Load Balancer [cmdb_ci_lb_radware]
HAProxy Lastenausgleichsmodul-Discovery mit Mustern	HA-Proxy	HAProxy Load Balancer [cmdb_ci_lb_haproxy]

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Lastenausgleicherkennung, Service Mapping und benutzerdefinierte CI-Felder

Discovery erfasst Informationen über den Installations- und Betriebsstatus von Lastenausgleichsmodulen. Wenn Sie Discovery mit Service Mapping verwenden, wird davon abgeraten, die Felder [operational_status] und [install_status] anzupassen. Standardmäßig ignoriert Service Mapping alle Host-CIs, für die der Wert des Felds *[operational_status]* ungleich *1* (Funktionsfähig) oder der Wert des Statusfelds *[install_status]* gleich *100* (Abwesend) ist. Weitere Informationen zu diesem Verhalten finden Sie unter Preparing customized ServiceNow deployments to work with Service Mapping (Vorbereitung benutzerdefinierter ServiceNow-Bereitstellungen zur Verwendung mit Service Mapping) [KB0647574] in der HI Knowledge Base.

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

A10-Lastenausgleicherkennung

Discovery und Service-Mapping verwenden Muster, um Informationen über A10-Lastenausgleichsmodule zu sammeln.

Hinweis: Die Probe-zu-Muster-Migration wird ab dem New York-Release unterstützt. Weitere Informationen finden Sie in Artikel KB0694477 der Wissensdatenbank.

Die folgenden Muster unterstützen die A10-Lastenausgleicherkennung:

- A10 Lastenausgleich
- A10 Load Balancer SSH
- A10

Der A10 IP Source NAT (Network Address Translator) ist eine Erweiterung des A10 Load Balancer Pattern. Die Erweiterung „Muster für IP-Quell-NAT“ erkennt IP-Quell-NAT-Pools. Diese Erweiterung ist ab dem Release Februar 2023, Store-Version 1.0.98, im Store verfügbar.

Apps im Store anfordern

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

Voraussetzungen

Anmeldeinformationen

Konfigurieren Sie SNMP-Anmeldeinformationen oder (optional) SSH-Anmeldeinformationen .

Discovery and Service Mapping Patterns

Um Partitionen des A10-Lastenausgleichsmoduls zu erkennen, stellen Sie die Anwendung Muster für Discovery und Service-Mapping, Release 1.0.98, aus dem ServiceNow Storebereit.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
A10 Load Balancer [cmdb_ci_lb_a10]	
Seriennummer [serial_number]	Seriennummer des Lastenausgleichsmoduls im folgenden Format: ##Object_ID=<LB_ARN>
Betriebsstatus [operational_status]	Betriebsstatus des Lastenausgleichsmoduls
Load Balancer-Schnittstelle [cmdb_ci_lb_interface]	
Name [name]	Name der Lastenausgleichs-Schnittstelle
MAC-Adresse [mac_address]	MAC-Adresse der Lastenausgleichs-Schnittstelle im folgenden Format: 55:0d:f9:98:3i:ae
Betriebsstatus [operational_status]	Betriebsstatus der Lastenausgleichs-Schnittstelle
Load Balancer-Pool [cmdb_ci_lb_pool]	

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

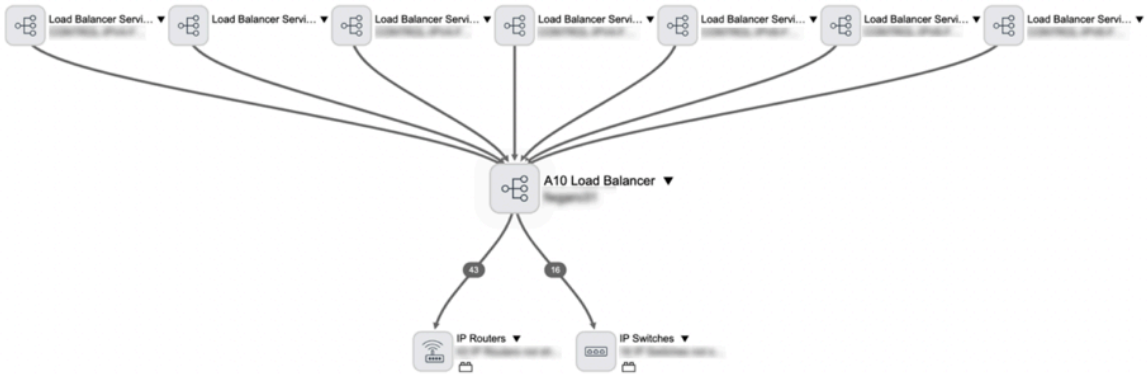
Tabelle und Feld	Beschreibung
Name [name]	Name des Pools von Lastenausgleichsmodulen
Lastenausgleichsmethode [load_balancing_method]	Die vom Lastenausgleichsmodul verwendete Methode
Betriebsstatus [operational_status]	Betriebsstatus des Pools von Lastenausgleichsmodulen
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	
Name [name]	Name des Poolmitglieds
IP-Adresse [ip_address]	IP-Adresse des Hosts des Poolmitglieds
Serviceport [service_port]	Vom Poolmitglied verwendeter Port
Betriebsstatus [operational_status]	Betriebsstatus der Mitglieder des Pools von Lastenausgleichsmodulen
Pool [pool]	Poolmitglied
Load Balancer-Services [cmdb_ci_lb_service]	
Name [name]	Name des Lastenausgleichsmoduls im folgenden Format: <LB-Name>:<LB-Port>
IP-Adresse [ip_address]	IP-Adresse des FQDN
Port [port]	Port des Lastenausgleichsmoduls
Betriebsstatus [operational_status]	Betriebsstatus des Lastenausgleichsservice
Installationsstatus [install_status]	Installationsstatus des Lastenausgleichsservice
Pool [pool]	Poolmitglied des Lastenausgleichsservice
DNS [cmdb_ci_dns_name]	
Name [name]	DNS-Name
IP-Adresse [ip_address]	DNS-IP-Adresse
Partition des A10-Lastenausgleichsmoduls [cmdb_ci_lb_a10_partition]	
Name [name]	Name der Partition
Index [index]	Partitions-ID. Ein Administrator weist diese ID beim Erstellen einer Partition zu.
Max. Aflex [Max_aflex]	Maximale Anzahl von aFleX-Skripts, die zur Partition gehören können
Administratoranzahl [admin_count]	Anzahl der der Partition zugewiesenen Administratoren
L3V [lev]	Wert, der angibt, ob die Layer 2/3-Virtualisierung für die Partition aktiviert ist
Netzwerkadapter [cmdb_ci_network_adapter]	
Betriebsstatus [operational_status]	Betriebsstatus des Netzwerkadapters
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
Alias [alias]	Aliasname des Netzwerkadapters

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

Tabelle und Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Name [name]	Name des Netzwerkadapters
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
Primäre IP [primaryIP]	Primäre IP-Adresse des Netzwerkadapters
IP-Adresse [cmdb_ci_ip_address]	
IP-Adresse [ip_address]	IP-Adresse
Netzmaske [netmask]	Netzmaske, zu der die IP-Adresse gehört
Version [version]	IP-Version
Betriebsstatus [operational_status]	Betriebsstatus der IP-Adresse
Seriennummer [cmdb_serial_number]	
Seriennummer [serial_number]	Attribute der Seriennummer des Lastenausgleichsmoduls
Seriennummerntyp [serial_number_type]	
Gültig [valid]	
Quell-NAT-IP-Pool [cmdb_ci_snat_ip_pool]	
NAT-Pool fehlgeschlagen [nat_pool_failed]	Die Gesamtzahl der Fehleingaben im Pool.
HA-Gruppe [ha_group]	
NET-Maske [net_mask]	
NAT-Pool insgesamt frei [nat_pool_total_free]	Die Gesamtzahl der freien Adressen im Pool.
Gesamtnutzung des NAT-Pools [nat_pool_total_usage]	Die Gesamtzahl der verwendeten Adressen im Pool.
Portnutzung des NAT-Pools [nat_pool_port_usage]	Gesamte Port-Auslastung im Pool.
Endadresse des NAT-Pools [nat_pool_end_address]	Die Endadresse des IP-NAT-Pools (IPv4 oder IPv6).
Startadresse des NAT-Pools [nat_pool_start_address]	Die Startadresse des IP-NAT-Pools (IPv4 oder IPv6).
Konfigurationselement [cmdb_ci]	

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

Abhängigkeitsansichten, in denen A10-Lastenausgleichsmodule und verbundene Komponenten und Anwendungen angezeigt werden



CI-Beziehungen

Um die A10-Lastenausgleicherkennung zu unterstützen, werden die folgenden Beziehungen erstellt:

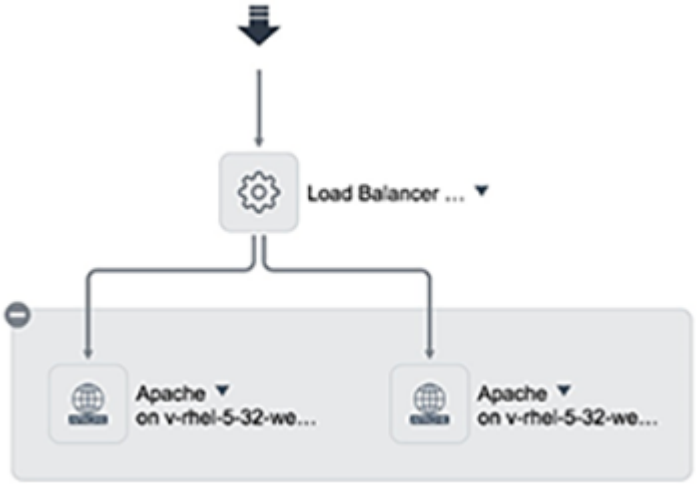
CI	Beziehung	CI
Routerschnittstelle [dscy_router_interface]	Verwendet::Verwendet von	Load Balancer-Pool [cmdb_ci_lb_a10]
Load Balancer-Schnittstelle [cmdb_ci_lb_interface]	Eigentümer von::Eigentum von	Load Balancer-Pool [cmdb_ci_lb_a10]
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	Eigentümer von::Eigentum von	Load Balancer-Pool [cmdb_ci_lb_pool]
Load Balancer-Services [cmdb_ci_lb_service]	Verwendet von::Verwendet	Load Balancer-Pool [cmdb_ci_lb_pool]
Load Balancer-Services [cmdb_ci_lb_service]	Wird ausgeführt auf::Wird ausgeführt	Load Balancer-Pool [cmdb_ci_lb_a10]
Load Balancer-Pool [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	Load Balancer-Pool [cmdb_ci_lb_a10]
DNS-Name [cmdb_ci_dns_name]	Verwendet von::Verwendet	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	Load Balancer-Pool [cmdb_ci_lb_a10]
Load Balancer-Pool [cmdb_ci_lb_a10]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Lastenausgleichsmodul A10 [cmdb_ci_lb_a10]	Besitzt: Im Besitz von	Quell-NAT-IP-Pool [cmdb_ci_snat_ip_pool]

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Service-Mapping erkennt die Verbindungen zwischen A10-Lastenausgleichsmodulen und Anwendungen in der Bereitstellung.

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

Servicezuordnung für A10-Lastenausgleichsanwendung



Cisco ACE-Lastenausgleicherkennung

Discovery identifiziert und klassifiziert Informationen über ACE-Lastenausgleichsmodule.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Anmeldeinformationen

Konfigurieren Sie SNMP- und SSH-Anmeldeinformationen .

Klassifizierer, Muster und Probe

Klassifizierung	Auslöser-Probes	Muster
ACE Load Balancer	Probe „Horizontal Discovery“: Startet Muster	ACE Load Balancer by SSH (früher ACE Load Balancer)

Erfasste Daten

In der Tabelle „ACE-Lastenausgleichsmodule“ `[cmdb_ci_lb_ace]` werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Seriennummer	serial_number
Betriebsstatus	operational_status

In der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Port	port

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

Bezeichnung	Feldname
Betriebsstatus	operational_status
Installationsstatus	install_status
Kurzbeschreibung	short_description

In der DNS-Tabelle [cmdb_ci_dns_name] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address

In der Tabelle „Load Balancer-Pool“ [cmdb_ci_lb_pool] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
Kontext	context
Lastenausgleichsmethode	load_balancing_method

In der Tabelle „Mitglieder von Load Balancer-Pools“ [cmdb_ci_lb_pool_member] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Serviceport	service_port
Pool	Pool
Kontext	context

In der Seriennummertabelle [cmdb_serial_number] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Seriennummer	serial_number
Seriennummerntyp	serial_number_type
Gültig	valid

In der Tabelle „Load Balancer-Schnittstelle“ [cmdb_ci_lb_interface] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	name
MAC-Adresse	mac_address

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

Bezeichnung	Feldname
Betriebsstatus	operational_status

Cisco GSS-Lastenausgleicherkennung

Die Erkennung von Cisco GSS-Lastenausgleichsmodulen wird sowohl von SNMP als auch von SSH durchgeführt.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Klassifizierungen

Um das Gerät zu klassifizieren, verwendet Discovery den Klassifizierer „Cisco GSS Load Balancer“, der die folgende Bedingung enthält: `sysdescr enthält Global Site Selector`.

Probes

Zur Identifizierung der Seriennummer des Geräts verwendet Discovery mehrere Probes, darunter eine SNMP-Probe zur Erkennung des spezifischen GSS-Geräts und eine Probe für die **Seriennummer**. In der Tabelle unten finden Sie eine Liste der zugehörigen Probes.

Warnung: Die SNMP- und SSH-Anmeldeinformationen müssen für die GSS-Lastenausgleichsmodule in Ihrem Netzwerk ordnungsgemäß konfiguriert sein.

Nach der Klassifizierung werden die folgenden Probes ausgelöst:

Probe	Beschreibung	Typ
Cisco GSS - Identity	Eine Multi-Probe, die das GSS-Gerät und die Seriennummer identifiziert	Mehrfachprobe
Cisco GSS - Network	In der Probe „Cisco GSS - Identify“ enthalten	Java-SNMP
Cisco GSS - Serial Number	In der Probe „Cisco GSS - Identify“ enthalten	JavaScript
Cisco GSS - Get Domains	Eine Probe, die globale Domänennamen erkennt, die dem Gerät entsprechen	JavaScript

Tabellen

Discovery erstellt einen Datensatz für jedes GSS-Gerät in der Tabelle „Cisco GSS“ [cmdb_ci_lb_cisco_gss]. Domänen werden in der Tabelle „DNS-Namen“ [cmdb_ci_dns_name] angegeben. Hostnamen und IP-Adressen werden in der Tabelle „IP-Adresse zu DNS-Name“ [cmdb_ip_address_dns_name] gespeichert. Diese Informationen werden von Service Mapping verwendet. Sie können die Informationen über DNS-Namen in der zugehörigen Liste **DNS-Namen für CIs** im Formular „Lastenausgleich“ anzeigen.

Hinweis: Das Muster „Cisco GSS“ ist standardmäßig zur Verwendung im Musterdesigner verfügbar.

Cisco CSS-Lastenausgleichsmodul

Die Erkennung von Cisco CSS-Lastenausgleichsmodulen erfolgt mithilfe von SNMP.

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

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Klassifizierungen

Discovery verwendet den Klassifizierer „Cisco CSS Load Balancer“, der die folgende OID-Klassifizierung enthält: 1.3.6.141.9.9.368.4.5.

Probes

Die folgenden Probes werden ausgelöst:

Probe	Beschreibung	Typ
SNMP - Load Balancer - Identity	Eine Multi-Probe, die Lastenausgleichsmodule erkennt	Java-SNMP
Cisco CSS - Get Services	Eine Java-Probe mit dem Cisco CSS-Sensor zum Erkennen von Services, die für das Lastenausgleichsmodul in der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service] definiert sind. Für jeden Service füllt Discovery **Name**, **ip_address**und **Port**aus.	Java-SNMP

Tabellen

Discovery erstellt einen Datensatz für jedes CSS-Gerät in der Tabelle „Cisco CSS“ [cmdb_ci_lb_cisco_css], die **Name**, **Modell**, **Seriennummer**, **Hersteller** und **NIC** (ip_address) des Geräts enthält. Außerdem wird für jeden Service in der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service] ein Datensatz erstellt.

.

Citrix NetScaler-Lastenausgleicherkennung

Discovery und Service-Mapping erkennen Citrix NetScaler-Lastenausgleichsmodule einschließlich Server Load Balancing (GSLB).

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Anforderungen und Support

Wichtig: In Discovery werden Lastenausgleichsmodule als lizenzierbare Entitäten behandelt. Es wird versucht, sie hauptsächlich mithilfe von SNMP zu ermitteln. Wenn ein Load Balancer in Ihrem System, der auf einem Linux-Host ausgeführt wird, SNMP- und SSH-Ports geöffnet hat, könnte Discovery ihn basierend auf dem SSH-Port klassifizieren. Diese Klassifizierung hat Vorrang vor SNMP. Um sicherzustellen, dass Discovery Ihre Hardware-Load Balancer richtig klassifiziert, erstellen Sie ein Discovery-Verhalten für Load Balancer, das SNMP, jedoch nicht SSH enthält. Software-Load Balancer werden als Anwendungen behandelt.

Virtuelle NetScaler-Lastenausgleichsmodule werden nicht vollständig unterstützt. Discovery unterstützt Lastenausgleichsmodule für lokale Server und GSLB.

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

Berechtigungen

- Konfigurieren Sie die SNMP-Anmeldeinformationen .

> **Hinweis:** Sie haben auch die Möglichkeit SSH-Anmeldeinformationen zu verwenden. Wenn jedoch die Nutzlast der an die Instanz zurückgegebenen Daten groß ist, kann der Discovery-Prozess fehlschlagen. Verwenden Sie in diesem Fall stattdessen SNMP-Anmeldeinformationen.

- (Optional) Gewähren Sie einem Benutzer den Lesezugriff auf die *NS.conf*-Konfigurationsdatei, wenn Sie keine SNMP- oder SSH-Anmeldeinformationen angeben möchten.
- Benutzen Sie die Anmeldeinformationen zur Standardauthentifizierung für die Discovery über REST.

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Klassifizierer, Muster und Probes

Klassifizierung	Auslöser-Probes	Muster
NetScaler Load Balancer	• Probe „Horizontal Discovery“: Startet Muster (siehe Spalte „Muster“) • NetScaler - Network Path Information (Multi-Probe) ◦ NetScaler - ARP Information ◦ NetScaler - Route Information • SNMP - NetScaler - Identity • SNMP - NetScaler - Identity - Serial • SNMP - NetScaler - Identity Info • SNMP - NetScaler - System	• NetScaler Load Balancer • NetScaler Load Balancer NS.CONF • NetScaler Load Balancer SSH • NITRO für Netscaler-Lastenausgleichsmodul

Um Probes für die horizontale Erkennung zu verwenden, stellen Sie sicher, dass die Multi-Probe *NetScaler - Network Path Information* in der zugehörigen Liste **Auslösertests** für den Klassifizierer *NetScaler Load Balancer* aktiv ist. Deaktivieren Sie dann die Probe *Horizontal discovery*, oder entfernen Sie sie aus der zugehörigen Liste **Auslösertests**.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

> **Hinweis:** Wenn Probes und Sensoren verwendet werden und die Systemeigenschaften *glide.discovery.hostname.snmp_trusted* und/oder *glide.discovery.hostname.dns_nbt_trusted* auf „false“ festgelegt sind, verwendet das System *dns_name* als Namen für das Lastenausgleichsmodul. Bei Verwendung des Musters „Netscaler Load Balancer“ erkennt das System diese Systemeigenschaften nicht, wenn sie auf „false“ festgelegt sind.

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

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping führt die Top Down-Discovery des NetScaler Global Server Load Balancer im Kontext von Anwendungsservices durch. Dadurch werden konfigurierte URLs des Lastenausgleichsmoduls NetScaler Global Server erkannt.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
DNS-Name [cmdb_ci_dns_name]	
Name [name]	Der Name oder der DNS-Namensalias des Lastenausgleichsmoduls NetScaler Global Server (GSLB)
IP-Adresse [ip_address]	Management-IP-Adresse des NetScaler Global Server-Lastenausgleichsmoduls (GSLB)
Port [port]	Der DNS-Port, den das Global Server-Lastenausgleichsmodul abhört
Citrix NetScaler `[cmdb_ci_lb_netscaler]`	
Seriennummer [serial_number]	Die Seriennummer des NetScaler-Geräts und dessen aktueller Betriebsstatus
Betriebsstatus [operational_status]	
Load Balancer-Pool `[cmdb_ci_lb_pool]`	
Name [name]	Der Name des Pools und die Methode für den Lastenausgleich, die der Pool aktiviert
Lastenausgleichsmethode [load_balancing_method]	
Load Balancer Pool-Mitglied `[cmdb_ci_lb_pool_member]`	
Name [name]	Name, IP-Adresse und Serviceport, die von jedem Poolmitglied verwendet werden
IP-Adresse [ip_address]	
Serviceport [service_port]	
VLAN des Lastenausgleichsmoduls `[cmdb_ci_lb_vlan]`	
Name [name]	Der Name des VLAN und das Tag, das diesem VLAN zur Identifizierung zugeordnet ist
Tag [tag]	
Load Balancer-Services `[cmdb_ci_lb_service]`	
Name [name]	Details zu dem Service, der im Lastenausgleichsmodul ausgeführt wird, zum Beispiel:
IP-Adresse [ip_address]	
Port [port]	
Betriebsstatus [operational_status]	
Installationsstatus [install_status]	
Trefferanzahl [hit_count]	
Weiterleitungsregeln für Exit-Schnittstellen `[dscy_route_interface]`	

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

Tabelle und Feld	Beschreibung
Routerschnittstelle [router_interface]	Details zu Weiterleitungsregeln für die Exit-Schnittstelle, einschließlich der Schnittstelle auf dem Router, ...
Konfigurationselement [cmdb_ci]	
Ziel-IP-Netzwerk [dest_ip_network]	
Weiterleitungsregeln für nächsten Hop `[dscy_route_next_hop]`	
IP-Adresse für nächsten Hop [router_interface]	Details zu den Weiterleitungsregeln im Lastenausgleichsmodul, einschließlich der IP-Adressen des nächsten Hop-Routers im Netzwerk. Das Feld „Konfigurationselement“ gibt den Router an, der das nächste Hop-Gerät ist.
Routerschnittstelle [router_interface]	
Konfigurationselement [cmdb_ci]	
Ziel-IP-Netzwerk [dest_ip_network]	

cmdb_ci_lb_netscaler

Spaltenname	Typ	Referenz
ip_address	IP-Adresse (validierte IPV4, IPV6)	
name	Zeichenfolge	
operational_status	Ganzzahl	
serial_number	Zeichenfolge	

Daten, die während des NITRO des Netscaler-Lastenausgleichsmoduls gesammelt wurden.

cmdb_serial_number

Spaltenbezeichnung	Spaltenname	Typ	Referenz
Konfigurationselement	cmdb_ci	Referenz	Konfigurationselement (Load Balancer)
Seriennummer	serial_number	Zeichenfolge	
Seriennummertyp	serial_number_type	Zeichenfolge	
Gültig	gültig	Wahr/Falsch	

cmdb_ci_lb_vlan

Spaltenbezeichnung	Spaltenname	Typ	Referenz
Lastenausgleichsmodul	load_balancer	Referenz	Konfigurationselement (Load Balancer)
Name	name	Zeichenfolge	
Tag	Tag	Ganzzahl	

cmdb_ci_lb_interface

Spaltenbezeichnung	Spaltenname	Typ	Referenz

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

cmdb_ci_lb_interface (Fortsetzung)

Lastenausgleichsmodul	load_balancer	Referenz	Konfigurationselement (Load Balancer)
Name	name	Zeichenfolge	
Betriebsstatus	operational_status	Ganzzahl	
MAC-Adresse	mac_address	Zeichenfolge	

cmdb_ci_lb_service

Spaltenbezeichnung	Spaltenname	Typ	Referenz
IP-Adresse	ip_address	IP-Adresse (validierte IPV4, IPV6)	
Lastenausgleichsmodul	load_balancer	Referenz	Konfigurationselement (Load Balancer)
Name	name	Zeichenfolge	
Port	port	Ganzzahl	

cmdb_ci_lb_pool

Spaltenbezeichnung	Spaltenname	Typ	Referenz
Lastenausgleichsmodul	load_balancer	Referenz	Konfigurationselement (Load Balancer)
Name	name	Zeichenfolge	

cmdb_ci_lb_pool_member

Spaltenbezeichnung	Spaltenname	Typ	Referenz
IP-Adresse	ip_address	IP-Adresse (validierte IPV4, IPV6)	
Lastenausgleichsmodul	load_balancer	Referenz	Konfigurationselement (Load Balancer)
Name	name	Zeichenfolge	
Pool	Pool	Referenz	Lastenausgleichsmodul-Pool
Serviceport	service_port	Ganzzahl	

Zum Anzeigen der DNS-Namen und -Aliasnamen für ein NetScaler-Lastenausgleichsmodul müssen Sie das Formular konfigurieren und die zugehörige Liste **DNS-Namen für CIs** hinzufügen. DNS-Namen beinhalten auch Aliasnamen.

Hinweis: Discovery fügt Informationen über die Lastenausgleichs-Schnittstelle ein, die zum Zuordnen des Netzwerkpfads in Service-Mapping erforderlich sind.

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

Beziehungen von Konfigurationselementen

Um die NetScaler Global Server-Lastenausgleicherkennung zu unterstützen, werden die folgenden Beziehungen erstellt:

CI	Beziehung	CI
DNS-Name [cmdb_ci_dns_name]	Verwendet::Verwendet von	IP-Adresse [cmdb_ci_ip_addresses]

Diese Beziehungen werden zur Unterstützung des NetScaler Load Balancer NITRO erstellt:

CI	Beziehung	CI
Netscaler [cmdb_ci_lb_netscaler]	Eigentümer von::Eigentum von	Schnittstellen [cmdb_ci_lb_interface]
Netscaler [cmdb_ci_lb_netscaler]	Eigentümer von::Eigentum von	vlan [cmdb_ci_lb_vlan]
Netscaler [cmdb_ci_lb_netscaler]	Eigentümer von::Eigentum von	Servicegruppen [cmdb_ci_lb_pool]
Servicegruppen [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	lbv-Server [cmdb_ci_lb_pool_member]
-Services [cmdb_ci_lb_service]	Wird ausgeführt auf::Wird ausgeführt	Netscaler [cmdb_ci_lb_netscaler]

sysName des NetScaler-Geräts

Um den sysName des NetScaler-Geräts zu verifizieren, überprüfen Sie die SNMP-MIB, und verifizieren Sie den sysName-Wert, indem Sie den Befehl *show snmp mib* ausführen.

Um den Wert von sysName zu ändern, führen Sie den folgenden Befehl aus: *set mib -name <DNS_NAME or NAME_OF_THE_NETSCALER_LB>*, um den Namen der SNMP-MIB festzulegen.

F5 BIG-IP-Lastenausgleicherkennung

Discovery und Service-Mapping erkennen F5 BIG-IP-Lastenausgleichsmodule über SNMP, SSH und die REST API.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

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

Voraussetzungen und wichtige Informationen

Wichtig: In Discovery werden Lastenausgleichsmodule als lizenzierbare Entitäten behandelt. Es wird versucht, sie hauptsächlich mithilfe von SNMP zu ermitteln. Wenn ein Load Balancer in Ihrem System, der auf einem Linux-Host ausgeführt wird, SNMP- und SSH-Ports geöffnet hat, könnte Discovery ihn basierend auf dem SSH-Port klassifizieren. Diese Klassifizierung hat Vorrang vor SNMP. Um sicherzustellen, dass Discovery Ihre Hardware-Load Balancer richtig klassifiziert, erstellen Sie ein Discovery-Verhalten für Load Balancer, das SNMP, jedoch nicht SSH enthält. Software-Load Balancer werden als Anwendungen behandelt.

Sie können VMware-Images von BIG-IP mit einer kostenlosen 90-Tage-Testversion von https://www.f5.com/trial herunterladen.

Für F5 Global Traffic Manager (GTM) BIG-IP Load Balancers kann Discovery den DNS-Namen der F5 GTM-Hardware sowie die DNS-Namen aller Server auflösen, die dem Load Balancer zugeordnet sind und verteilten Datenverkehr empfangen. Um diese Daten anzuzeigen, navigieren Sie zu **Alle** > **Konfiguration** > **Lastenausgleichsmodule** > **LB-Hardware** und öffnen Sie den Datensatz des F5-Lastenausgleichsmoduls, und wählen Sie dann die zugehörige Liste **DNS Names for CIs (DNS-Namen für CIs)** aus. Service-Mapping verwendet diese Informationen, um F5-Beziehungen zuzuordnen.

Hinweis: Wenn Ihr Gerät F5 BIG-IP Teil eines Failover-Clusters ist, kann es zwei Clusterknoten zugeordnet werden. In diesem Fall wird im Feld **Betriebsstatus** einer der Knoten als Funktionsfähig und der andere als Nicht funktionsfähig angezeigt.

Anmeldeinformationen

- Konfigurieren Sie die SNMP-Anmeldeinformationen .

  Hinweis: Wenn Sie keine SSH-Anmeldeinformationen verwenden möchten, können Sie mit der REST API eine Verbindung zu F5-BIG-IP-Geräten herstellen.

- (Optional) Wenn die Anmeldeinformationen für iRules oder SNMP-Community nicht ausreichen, um ausgehende Verbindungen zu ermitteln, konfigurieren Sie die SSH-Anmeldeinformationen auf Now Platform.

  Service-Mapping verwendet die SSH-Anmeldeinformationen zum Abrufen von Verbindungen, die nicht von CMDB stammen. Das Erkennen von Verbindungen mithilfe des SSH-Protokolls ist ein Failover-Mechanismus für die SNMP-basierte Discovery.

- Um die Mitglieder des Lastenausgleichsmodul-Pools erfolgreich zu erkennen, navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties] und legen die Systemeigenschaft *sys_db_bigpipe.displayservicenames* auf **false** fest.
- Benutzen Sie die Anmeldeinformationen zur Standardauthentifizierung für die Discovery über REST.

- Geben Sie für die Horizontal-Discovery mit Discovery Berechtigungen zum Ausführen der folgenden APIs an:
  - `https://" get_attr {"managementIP"}"/mgmt/tm/sys/global-settings`
  - `https://" get_attr {"managementIP"}"/mgmt/tm/sys/hardware`
  - `https://"get_attr {"managementIP"}"/mgmt/tm/sys/failover`
  - `https://"get_attr {"managementIP"}"/mgmt/tm/cloud/net/self`

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

- `https://"get_attr {"managementIP"}"/mgmt/tm/net/interface`
- `https://"get_attr {"managementIP"}"/mgmt/tm/net/self`
- `https://"get_attr {"managementIP"}"/mgmt/tm/net/vlan`
- `https://"get_attr {"managementIP"}"/mgmt/tm/ltm/pool`
- `https://"get_attr {"managementIP"}"/mgmt/tm/gtm/wideip`
- `https://"get_attr {"managementIP"}"/mgmt/tm/cm/traffic-group/`
- `https://"get_attr {"managementIP"}"/mgmt/tm/cm/device`

Geben Sie für die Top Down-Discovery mit Service-Mapping Berechtigungen zum Ausführen der folgenden APIs an:

- `https://" get_attr {"managementIP"}"/mgmt/tm/ltm/"get_attr {"irule"}`
- `https://" get_attr {"managementIP"}"/mgmt/tm/ltm/virtual/~Common~"get_attr {"vip_name"}`
- `https://" get_attr {"computer_system.managementIP"}"/mgmt/tm/ltm/pool/"get_attr {"pool_name"}"/members?`

- (Optional) Für die Top Down-Discovery mit Service-Mapping, konfigurieren Sie Applicative-Anmeldeinformationen .
- (Optional) Für die Top Down-Discovery mit Service-Mapping, stellen Sie einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle bereit:
  - Bigpipe-Befehle (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 9)
  - Bigpipe- und Traffic Management Shell-Befehle (TMSH) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 10)
  - TMSH-Befehle (Traffic Management Shell) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 11)
  - Erweiterte Befehle für die Traffic Management Shell (TMSH) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 10, 11 und 12)
  - Der *show cm traffic-group - get command* für die Erkennung von F5 BIG-IP Device Service Clustering
- (Optional) Für die Top Down-Discovery mit Service-Mapping , geben Sie dem Benutzer erhöhte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.

Erkennung von F5-Clustern

Der horizontale Erkennungsprozess kann F5-Cluster ermitteln. Zum Erkennen von Clustern müssen die Anmeldeinformationen über Leseberechtigungen für Datenverkehrgruppen verfügen. Für SNMP ist dies die reguläre Leseberechtigung. Für SSH muss **die Traffic Management Shell (TMSH-Shell)** aktiviert und zugänglich sein.

Hinweis: Da F5-Cluster dieselben virtuellen IPs und Adressen für alle Geräte gemeinsam nutzen, kann der horizontale Erkennungsprozess keine spezifischen IP-Adressen für jedes Gerät finden.

Klassifizierer, Muster und Probes

Zur F5-Erkennung verwendet Discovery die folgenden Klassifizierer, Probes und Muster:

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

Klassifizierungen	Auslöser-Probes	Muster
F5 BIG-IP-Lastenausgleichsmodul	Probe „Horizontal Discovery“: Startet Muster	Die folgenden Muster werden für die standardmäßige horizontale Erkennung verwendet, die die Erkennung von Clustern einschließt: • F5 Load Balancer • F5 Load Balancer SSH • F5REST • F5-REST-OAuth-2.0-Authentifizierung **Hinweis:** Die Muster „F5 Load Balancer“ und „F5 Load Balancer SSH“ enthalten den Erweiterungsabschnitt, der F5-Zertifikate erkennt.
F5 HTTP	Der Klassifizierer „F5 HTTP“ verwendet keine Auslöser-Probe. Er löst das Muster „F5 Load Balancer REST“ aus, um die Datensammlung über REST durchzuführen.	Diese Muster verwenden iRules, um Informationen über REST abzurufen. Service-Mapping verwendet die folgenden Muster für die Erkennung von oben nach unten: • F5 Load Balancer REST • F5 BIG-IP GTM • F5 BIG-IP LTM

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping führt die Top Down-Discovery des GTM BIG-IP-Lastenausgleichsmoduls im Kontext von Anwendungsservices durch. Es erkennt konfigurierte URLs der GTM BIG-IP-Load Balancer.

Von Discovery während der horizontalen Erkennung erfasste Daten

In der Tabelle „F5 Big-IP“ `[cmdb_ci_lb_bigip]` werden die folgenden Daten erfasst.

Tabelle und Feld	Beschreibung
F5 Big-IP [cmdb_ci_lb_bigip]	

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

Tabelle und Feld	Beschreibung
Name [name]	Details zum Lastenausgleichsmodul. Zeigen Sie einen Datensatz in dieser Tabelle an, um die vor- und nachgelagerten Beziehungen mit dem Lastenausgleichsmodul anzuzeigen.
Seriennummer [serial_number]	
Betriebsstatus [operational_status]	
Load Balancer-Schnittstelle [cmdb_ci_lb_interface]	
Name [name]	Details zu jeder Schnittstelle für das Lastenausgleichsmodul
MAC-Adresse [mac_address]	
Betriebsstatus [operational_status]	
Load Balancer-Pool [cmdb_ci_lb_pool]	
Name [name]	Der Name des Pools und die Methode für den Lastenausgleich, die der Pool aktiviert
Lastenausgleichsmethode [load_balancing_method]	
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	
Name [name]	Name, IP-Adresse und Serviceport, die von jedem Poolmitglied verwendet werden.
IP-Adresse [ip_address]	
Serviceport [service_port]	
Pool [pool]	
VLAN des Lastenausgleichsmoduls [cmdb_ci_lb_vlan]	
Name [name]	Der Name des VLAN und das Tag, das diesem VLAN zur Identifizierung zugeordnet ist
Tag [tag]	
MAC-Adresse [mac_address]	
Load Balancer-Services [cmdb_ci_lb_service]	
Name [name]	Details zum Lastenausgleichsservice, der die Arbeitslast auf andere Server (zum Beispiel Webserver) verteilt.
IP-Adresse [ip_address]	
Port [port]	
Betriebsstatus [operational_status]	
Trefferanzahl [hit_count]	
DNS [cmdb_ci_dns_name]	
Name [name]	Name und IP-Adresse des Domänennamenservers für die Netzwerkadapter
IP-Adresse [ip_address]	
Netzwerkadapter [cmdb_ci_network_adapter]	
Name [name]	Details über die Netzwerkadapter im Lastenausgleichsmodul
IP-Adresse [ip_address]	

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

Tabelle und Feld	Beschreibung
Netzmaske [netmask]	
MAC-Adresse [mac_address]	
Cluster [cmdb_ci_cluster]	
Name [name]	Details über das Cluster von Lastenausgleichsmodulen
Clusterstatus [cluster_status]	
Cluster-ID [cluster_id]	
IP-Adresse [ip_address]	
Clusterknoten [cmdb_ci_cluster_node]	
Name [name]	Details über alle Knoten in einem Cluster
Cluster-ID [cluster_id]	
Clusterstatus [cluster_status]	

Beziehungen von Konfigurationselementen für Cluster

Für Cluster werden die folgenden Beziehungen erstellt:

CI	Beziehung	CI
cmdb_ci_cluster	Hostet::Gehostet auf	cmdb_ci_lb_bigip
cmdb_ci_cluster_node	Gehostet auf::Hostet	cmdb_ci_lb_bigip
cmdb_ci_cluster_node	Cluster von::Cluster	cmdb_ci_cluster

HAProxy Lastenausgleichsmodul-Discovery mit Probes

Die Discovery von HAProxy Community Edition-Lastenausgleichsmodulen wird von SSH durchgeführt.

Hinweis: Ab Muster für Discovery und Service-Mapping Version 1.15.0 ist die musterbasierte Discovery die Standardmethode zur Erkennung von HAProxy -Lastenausgleichsmodulen.

- Informationen zum Aktivieren der probebasierten Discovery finden Sie unter Aktivieren Sie die Discovery des HAProxy-Lastenausgleichsmoduls mit Probes.
- Informationen zum HA-Proxy-Muster finden Sie unter HAProxy Lastenausgleichsmodul-Discovery mit Mustern.
- Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

HAProxy ist ein Open Source-Lastenausgleichsmodul, das jeden TCP-Service verwalten kann. Sie eignet sich besonders für den HTTP-Lastenausgleich, da sie die Sitzungspersistenz und die Layer-7-Verarbeitung unterstützt. Discovery unterstützt HAProxy für den HTTP-Lastenausgleich. Der TCP-Lastenausgleich wird nicht unterstützt.

Berücksichtigen Sie die folgenden Anforderungen für die Erkennung von HAProxy:

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

- Die Software HAProxy wird auf einem Linux-Server installiert und ausgeführt.
- MID-Server wird bereitgestellt, um den Server zu erkunden, und MID-Server hat Zugriff auf die Konfigurationsdatei des Servers HAProxy.
- Die Konfigurations-Probe sucht mit einer der folgenden Methoden nach der Datei `haproxy.cfg`:
  - Verwendung des Parameters *`-f`* für die Prozessausgabe HAProxy
  - Im Standardpfad `/etc/haproxy/haproxy.cfg`
- Die HAProxy -Proben erfordern Anmeldeinformationen und Ausführungsrechte, um Befehle auszuführen.

Discovery verwendet die Probe **„Unix – Aktive Prozesse“**, um ein HAProxy -Lastenausgleichsmodul zu identifizieren, wenn der Name des Prozesses *`haproxy`* ist. Wenn dieses Kriterium erfüllt ist, wird ein Datensatz in der Tabelle „HAProxy-Load Balancer“ [cmdb_ci_lb_haproxy] erstellt, falls für den ausgeführten Prozess noch kein Datensatz vorhanden ist.

Nach der Klassifizierung werden die folgenden Probes ausgelöst:

HAProxy-Probes

Probe	Beschreibung	Befehle
HAProxy - Version	Der Sensor dieser Probe füllt die Version HAProxy in der Tabelle „HAProxy-Lastenausgleichsmodule“ [cmdb_ci_lb_shaproxy] aus.	haproxy
HAProxy - Get Configuration	Der Sensor dieser Probe trägt zusätzliche Informationen in die Tabelle „HAProxy-Load Balancer“ [cmdb_ci_lb_haproxy] ein. Die Probe trägt auch Informationen in die Tabellen „Load Balancer-Service“ [cmdb_ci_lb_service], „Load Balancer-Pool“ [cmdb_ci_lb_pool], „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member], „Load Balancer-Schnittstelle“ [cmdb_ci_lb_interface] und „Load Balancer-Applikation“ [cmdb_ci_lb_appl] ein.	echo, sed, cut, grep, egrep (im Bourne-Shell-Skript)

Zusätzlich zur Datenauffüllung werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] die folgenden Beziehungsdatensätze erstellt:

- Die Datensätze in der Tabelle cmdb_ci_lb_appl werden in den Datensätzen der Tabelle cmdb_ci_web_server ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_pool werden von den Datensätzen der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_pool sind Mitglieder der Datensätze in der Tabelle cmdb_ci_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_pool_member sind Mitglieder der Datensätze in der Tabelle cmdb_ci_pool.

Aktivieren Sie die Discovery des HAProxy-Lastenausgleichsmoduls mit Probes

Wenn Sie nicht die standardmäßige musterbasierte HAProxy-Discovery verwenden möchten, aktivieren Sie die probebasierte HAProxy-Discovery, um stattdessen weiterhin zu verwenden.

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

Vorbereitungen
Erforderliche Rolle: discovery_admin

Prozedur
1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **Prozesse**.
2. Suchen Sie im Feld **Name** nach `HAProxy`.
3. Wählen Sie die HAProxy-Klassifizierung aus.
4. Wählen Sie in der zugehörigen Liste **Löst Probe ausBearbeiten**.
5. Entfernen Sie **das Horizontalmuster** aus der Liste der Auslösertests.
6. Fügen Sie in der Liste Sammlung **die Option HAProxy – Get-Konfiguration** und **HAProxy – Version** zur Liste der Auslösertests hinzu.
7. Wählen Sie **Speichern**.

Nächste Maßnahme
Planen Sie eine Horizontal-Discovery, um das HAProxy-Lastenausgleichsmodul mit Probes zu erkennen. Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Zugehörige Informationen

HAProxy Lastenausgleichsmodul-Discovery mit Probes

NGINX-Lastenausgleicherkennung

Die Erkennung von NGINX-Lastenausgleichsmodulen erfolgt mithilfe von SSH.

NGINX ist ein Open Source-Webserver mit einem Lastenausgleichsmodul. Discovery erkennt den Webserver und Informationen über das Lastenausgleichsmodul.

Beachten Sie die folgenden Anforderungen für die Erkennung von NGINX-Servern:

- NGINX ist auf dem Server installiert und wird ausgeführt.
- Der MID Server hat Zugriff auf die NGINX-Konfigurationsdatei, die standardmäßig `/etc/nginx/nginx.conf` lautet.
- Aktivieren Sie SSH-Befehle (Secure Shell).
- Zur Ausführung von Befehlen benötigen die NGINX-Probes Anmeldeinformationen und Ausführungsrechte.

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Der Prozessklassifizierer „Nginx“ erkennt einen laufenden Prozess, der während der Erkundung eines UNIX-Servers die folgenden Kriterien erfüllt:

- Der Name des Prozesses beginnt mit *`nginx`*.
- Der Name des Prozesses enthält *`master`*.

Die beiden folgenden Bedingungen müssen erfüllt sein:

- In der Tabelle „Webserver“ [cmdb_ci_web_server] wird ein Datensatz erstellt.
- In der Tabelle „CI-Beziehung“ [cmdb_rel_ci] wird für den Linux-Server (Linux-Server [cmdb_ci_linux_server]) und für den Webserver (Webserver [cmdb_ci_web_server]) eine Beziehung vom Typ **Wird ausgeführt auf** erstellt.

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

Nach der Klassifizierung werden die folgenden Probes ausgelöst:

NGINX-Probes

Probe	Beschreibung	Befehle
Nginx – Version	Diese Probe enthält ein Bourne-Shell-Skript. Er bestimmt die Version von NGINX und füllt die Tabelle „Webserver“ [cmdb_ci_web_server].	nginx
Nginx – Get Configuration	Diese Probe enthält ein Bourne-Shell-Skript und ein Argument, das den Pfad der NGINX-Konfigurationsdatei festlegt. Die Probe identifiziert Konfigurationsparameter basierend auf Schlüsselwörtern in der Konfigurationsdatei und gibt sie als einzelnes Nutzlastergebnis zurück.	echo, sed, cut, grep, egrep (im Bourne-Shell-Skript)

Zusätzlich zur Datenauffüllung werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] die folgenden Beziehungsdatensätze erstellt:

- Die Datensätze in der Tabelle „cmdb_ci_web_server“ werden für die Datensätze in der Tabelle „cmdb_ci_linux_server“ ausgeführt.
- Die Datensätze in der Tabelle cmdb_ci_lb_service verwenden die Datensätzen der Tabelle cmdb_ci_lb_pool.
- Die Datensätze in der Tabelle cmdb_ci_pool werden von den Datensätzen der Tabelle cmdb_ci_service verwendet.
- Die Datensätze in der Tabelle cmdb_ci_pool sind Mitglieder der Datensätze in der Tabelle cmdb_ci_pool_member.
- Die Datensätze in der Tabelle cmdb_ci_pool_member sind Mitglieder der Datensätze in der Tabelle cmdb_ci_pool.

Radware Alteon-Lastenausgleicherkennung

Discovery identifiziert und klassifiziert Informationen über Alteon-Lastenausgleichsmodule.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Anmeldeinformationen

Konfigurieren Sie die SNMP-Anmeldeinformationen .

Klassifizierer, Muster und Probe

Klassifizierung	Auslöser-Probe	Muster
Alteon Load Balancer	Horizontal pattern	Alteon Load Balancer by SNMP (früher Alteon Load Balancer)

Erfasste Daten

In der Alteon-Tabelle `[cmdb_ci_lb_alteon]` werden die folgenden Daten erfasst.

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

Bezeichnung	Feldname
Seriennummer	serial_number
Betriebsstatus	operational_status

In der Tabelle „Load Balancer-Schnittstelle“ [cmdb_ci_lb_interface] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
Name	nam
MAC-Adresse	mac_address
Betriebsstatus	operational_status
Index	index

In der Tabelle „Load Balancer-Pool“ [cmdb_ci_lb_pool] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
Index	index
Lastenausgleichsmethode	load_balancing_method

In der Tabelle „Load Balancer Pool-Mitglied“ [cmdb_ci_pool_member] werden die folgenden Daten erfasst:

Bezeichnung	Feldname
IP-Adresse	ip_address
Serviceport	service_port

In der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service] werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Port	port
Betriebsstatus	operational_status
Installationsstatus	install_status
Trefferanzahl	hit_count

In der DNS-Tabelle [cmdb_ci_dns_name] werden die folgenden Daten erfasst.

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

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address

Radware-appDirector-Lastenausgleicherkennung

Die Erkennung von Radware-Lastenausgleichsmodulen erfolgt mithilfe von SNMP.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Anforderungen

Wichtig: In Discovery werden Lastenausgleichsmodule als lizenzierbare Entitäten behandelt. Es wird versucht, sie hauptsächlich mithilfe von SNMP zu ermitteln. Wenn ein Load Balancer in Ihrem System, der auf einem Linux-Host ausgeführt wird, SNMP- und SSH-Ports geöffnet hat, könnte Discovery ihn basierend auf dem SSH-Port klassifizieren. Diese Klassifizierung hat Vorrang vor SNMP. Um sicherzustellen, dass Discovery Ihre Hardware-Load Balancer richtig klassifiziert, erstellen Sie ein Discovery-Verhalten für Load Balancer, das SNMP, jedoch nicht SSH enthält. Software-Load Balancer werden als Anwendungen behandelt.

Anmeldeinformationen

Konfigurieren Sie die SNMP-Anmeldeinformationen .

Klassifizierer, Muster und Probes

Klassifizierung	Probe	Muster
Radware - AppDirector - Load Balancer	Probe „Horizontal Discovery“: Startet Muster	AppDirector Load Balancer

Datenerkennung

In der Tabelle „Radware-Lastenausgleichsmodule“ `[cmdb_ci_lb_radware]` werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Seriennummer	serial_number

In der Tabelle „DNS-Name“ `[cmdb_ci_dns_name]` werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address

In der Tabelle „Load Balancer-Service“ `[cmdb_ci_lb_service]` werden die folgenden Daten erfasst.

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

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Port	port
Betriebsstatus	operational_status
Installationsstatus	install_status

Felder und Probes von Lastenausgleichsmodulen

Discovery speichert die Informationen der Lastenausgleichsmodule in mehreren Tabellen.

Die Informationen in diesem Thema beziehen sich nur auf die Erkennung mit Probes und Sensoren. Wenn Sie Muster verwenden, um zum Beispiel F5 Big-IP-Lastenausgleichsmodule zu erkennen, lesen Sie das entsprechende Thema für diesen Typ von Lastenausgleichsmodul.

Hinweis: Standardmäßig verwendet das System für den CI-Datensatz die erkannte IP-Adresse eines Lastenausgleichsmoduls. Das kann die Verwaltungs-IP sein, die für das Gerät erstellt wurde und die im Erkennungszeitplan verwendet wird. Anweisungen dazu, wie Discovery dazu gezwungen werden kann, anstelle einer Management-IP die IP-Adresse der NIC des Lastenausgleichsmoduls zu verwenden, finden Sie unter Eigenschaften der IP-Adressauswahl.

Felder in der Tabelle „Citrix NetScaler“ [cmdb_ci_lb_netscaler]

Feldbezeichnung und -name	Probes, die Daten erfassen
Seriennummer [serial_number]	SNMP - Netscaler - Identity - Serial
Asset-Tag [asset_tag]	SNMP - Netscaler - Identity
Modell-ID [model_id]	SNMP - Netscaler - Identity

Felder in der Tabelle „Cisco GSS“ [cmdb_ci_lb_cisco_gss]

Feldbezeichnung und -name	Probes, die Daten erfassen
Seriennummer [serial_number]	Cisco GSS - Serial Number
Modell-ID [model_id]	Cisco GSS - Identity
IP-Adresse [ip_address]	Cisco GSS - Network
Hersteller [manufacturer]	Cisco GSS - Identity

Felder in der Tabelle „Cisco CSS“ [cmdb_ci_lb_cisco_css]

Feldbezeichnung und -name	Probes, die Daten erfassen
Seriennummer [serial_number]	SNMP - Load Balancer – Identity
Modell-ID [model_id]	
IP-Adresse [ip_address]	
Hersteller [manufacturer]	

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

Felder in der Tabelle „F5 BIG-IP“ [cmdb_ci_lb_bigip]

Feldbezeichnung und -name	Probes, die Daten erfassen
Aktive Module [active_modules]*	SNMP - F5 BIG-IP - System
Asset-Tag [asset_tag]	
Modell-ID [model_id]	
Failover-Modus [failover_mode]*	
Failover-Peer [failover_peer]*	
Seriennummer [serial_number]	Cisco GSS - Serial Number

*Im Formular standardmäßig nicht sichtbar. Passen Sie das Formular an, indem Sie dieses Feld hinzufügen.

Felder in der Tabelle „Load Balancer“ [cmdb_ci_lb]

Feldbezeichnung und -name	Probes, die Daten erfassen
Betriebsstatus [operational_status]	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System • SNMP - Load Balancer - Identity
Name [name]	

Felder in der Tabelle „Load Balancer-Applikation“ [cmdb_ci_lb_appl]

Feldbezeichnung und -name	Probes, die Daten erfassen
Konfigurationsdatei [config_file]*	Nginx - Get Configuration
Name [name]	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • Nginx - Get Configuration
IP-Adresse [ip_address]*	
Letzter Discovery-Scan [last_discovered]*	
Version [version]	• Apache - Version • HAProxy - Version • Nginx - Version

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

Felder der Tabelle „Load Balancer-Schnittstelle“ [cmdb_ci_lb_interface]

Feldbezeichnung und -name	Probes, die Daten erfassen
Status [install_status]*	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Load Balancer [load_balancer]	
Name [name]	

*Im Formular standardmäßig nicht sichtbar. Passen Sie das Formular an, indem Sie dieses Feld hinzufügen.

Felder in der Tabelle „Load Balancer-Pool“ [cmdb_ci_lb_pool]

Feldbezeichnung und -name	Probes, die Daten erfassen
Lastenausgleichsmethode [load_balancing_method]	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Load Balancer [load_balancer]	
Letzter Discovery-Scan [last_discovered]*	
Name [name]	

*Im Formular standardmäßig nicht sichtbar. Passen Sie das Formular an, indem Sie dieses Feld hinzufügen.

Felder der Tabelle „Load Balancer Pool-Mitglied“ [cmdb_ci_lb_pool_member]

Feldbezeichnung und -name	Probes, die Daten erfassen
Vollqualifizierter Domänenname [fqdn]*	• HAProxy - Get Configuration • Nginx - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
IP-Adresse [ip_address]	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • Nginx- Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Load Balancer [load_balancer]	
Letzte Erkennung [last_discovery]*	
Name [name]	
Pool [pool]*	
Serviceport [service_port]	

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

*Im Formular standardmäßig nicht sichtbar. Passen Sie das Formular an, indem Sie dieses Feld hinzufügen.

Felder in der Tabelle „Load Balancer-Service“ [cmdb_ci_lb_service]

Feldbezeichnung und -name	Probes, die Daten erfassen
Eingabe-URL [input_url]	• Apache - Get JK Module • Apache - Get Proxy Module • Nginx - Get Configuration
IP-Adresse [ip_address]	• Apache - Get JK Module • Apache - Get Proxy Module • Cisco GSS - Identity • HAProxy - Get Configuration • Nginx - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Letzter Port [last_port]*	HAProxy - Get Configuration
Load Balancer [load_balancer]	• Apache - Get JK Module • Apache - Get Proxy Module • Cisco GSS - Identity • HAProxy - Get Configuration • Nginx - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Letzte Erkennung [last_discovery]*	
Serviceport [service_port]*	

*Im Formular standardmäßig nicht sichtbar. Passen Sie das Formular an, indem Sie dieses Feld hinzufügen.

Felder in der Tabelle „Load Balancer-VLAN“ [cmdb_ci_lb_vlan]

Feldbezeichnung und -name	Probes, die Daten erfassen
Load Balancer [load_balancer]	• Apache - Get JK Module • Apache - Get Proxy Module • HAProxy - Get Configuration • Nginx - Get Configuration • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System
Name [name]	

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

Felder in der Tabelle „Load Balancer-VLAN“ [cmdb_ci_lb_vlan] (Fortsetzung)

Feldbezeichnung und -name	Probes, die Daten erfassen
Tag [tag]	• SNMP - F5 BIG-IP - System • SNMP - Netscaler - System

Apache-Webserverdaten

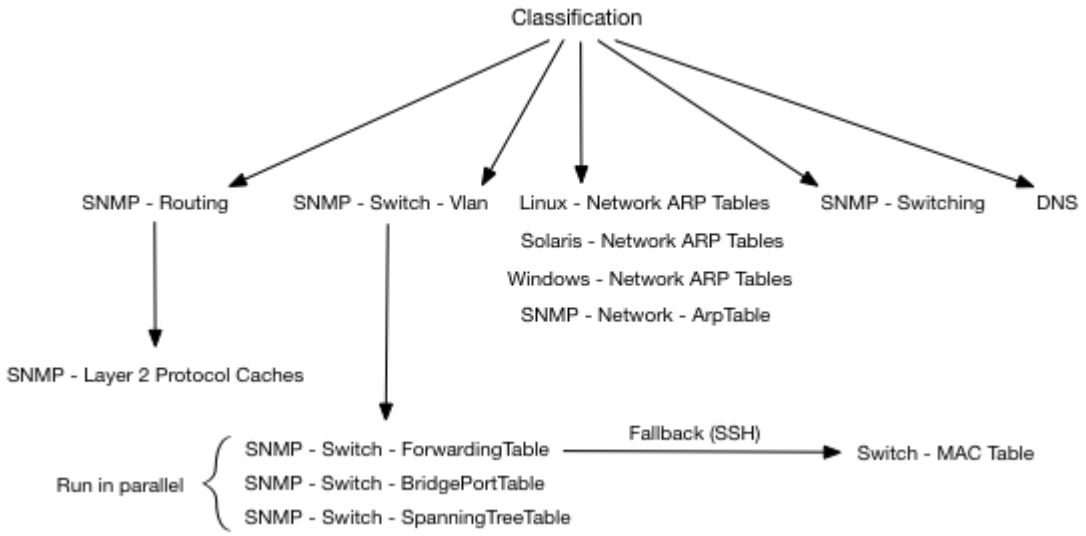
Discovery erfasst mithilfe von SSH auch Daten in Apache-Webserver-Lastenausgleichsmodulen. Unter Erkennung der Apache-Connectors mod_jk und mod_proxy finden Sie weitere Informationen zu Probes für Apache-Webserverdaten. Informationen zu den Tabellen, Feldern und Datenquellen, die Discovery für Apache-Webserver füllt, finden Sie unter Erkennung von Apache-Webservern.

Layer 2-Erkennung

Discovery kann die physischen Verbindungen (als Layer 2 bezeichnet) zwischen Netzwerkgeräten erkennen.

Layer 2-Erkennungsprozess

Discovery verwendet mehrere Probes, um Informationen über Netzwerkadapter und deren Layer 2-Verbindungen zu sammeln. Das folgende Diagramm zeigt die Probes, die Discovery für die Netzwerkerkennung startet, einschließlich der für die Layer 2-Erkennung verwendeten.



Wenn Discovery beispielsweise einen Switch in einem Netzwerk erkennt, werden die Probes *SNMP - Switch - Vlan* und *SNMP - Network - ARPTable* ausgelöst. Für jedes von Discovery erkannte VLAN werden verschiedene Switch-Probes ausgelöst. Wenn ein Switch über Weiterleitungsfunktionen verfügt, löst Discovery die Probe *SNMP - Routing* aus, um Informationen zu Netzwerkadaptern in der Tabelle „Netzwerkadapter“ [cmdb_ci_network_adapter] zu erfassen. Wenn Discovery einen Server erkennt, wird die entsprechende ARP-Probe (Address Resolution Protocol) für dieses Betriebssystem ausgelöst. Discovery unterstützt auch die Verwendung von Mustern wie *Network Switch* und *Network Router*, die in Discovery standardmäßig verfügbar sind. Weitere Informationen finden Sie unter Erkennung von Routern und Switches.

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

Während der Erkennung eines Netzwerkgeräts erstellt Discovery Datensätze in den Tabellen „Routerschnittstelle“ [dscy_router_interface] und „Switchport“ [dscy_switchport]. Diese Informationen beinhalten Informationen über die Netzwerkadapter für dieses Gerät. Für SNMP-fähige Geräte erfasst Discovery die Informationen während der Erkundungsphase von einer Weiterleitungs-Probe. Als Nächstes wird die Probe „Layer 2 Protocol Cache“ ausgeführt, um Nachbardaten von dem Gerät zu erfassen.

Nachbardaten abrufen

Während Discovery Netzwerkinformationen von den Probes auf einem Gerät erfasst, identifiziert die Probe „SNMP - Layer 2 Protocol Caches“ Nachbargeräte über CDP und LLDP. Diese Probe aktualisiert die Tabelle „Nachbargeräte“ [discovery_device_neighbors], die die Layer 2-Verbindungen zwischen Switches enthält. Manchmal sind der Instanz die Nachbarn dieses Geräts noch nicht bekannt. Die Schnittstelle des Nachbarn kann erst dann in einen Datensatz aufgelöst werden, wenn Discovery die Seite des Nachbarn in der Beziehung ermittelt hat. Wenn Discovery auf dem Nachbargerät ausgeführt wird, vervollständigt Discovery die Informationen für die Schnittstelle des Nachbarn für das ursprüngliche Meldegerät.

Aus den folgenden Caches kann Discovery Nachbardaten auf einem Netzwerkgerät abrufen:

- CDP (Cisco Discovery Protocol) : Cache auf Cisco-Geräten, der Informationen zu Nachbargeräten in Form einer protokollspezifischen Nachbar-ID enthält. CDP (Cisco Discovery Protocol).
- LLDP (Link Layer Discovery Protocol) : Generischer Cache, der Informationen zu Nachbargeräten in Form einer protokollspezifischen Nachbar-ID enthält
- ARP (Address Resolution Protocol) : Cache, der die IP- und MAC-Adressen aller verbundenen Geräte und Server enthält

Funktionsweise der Layer 2-Erkennung

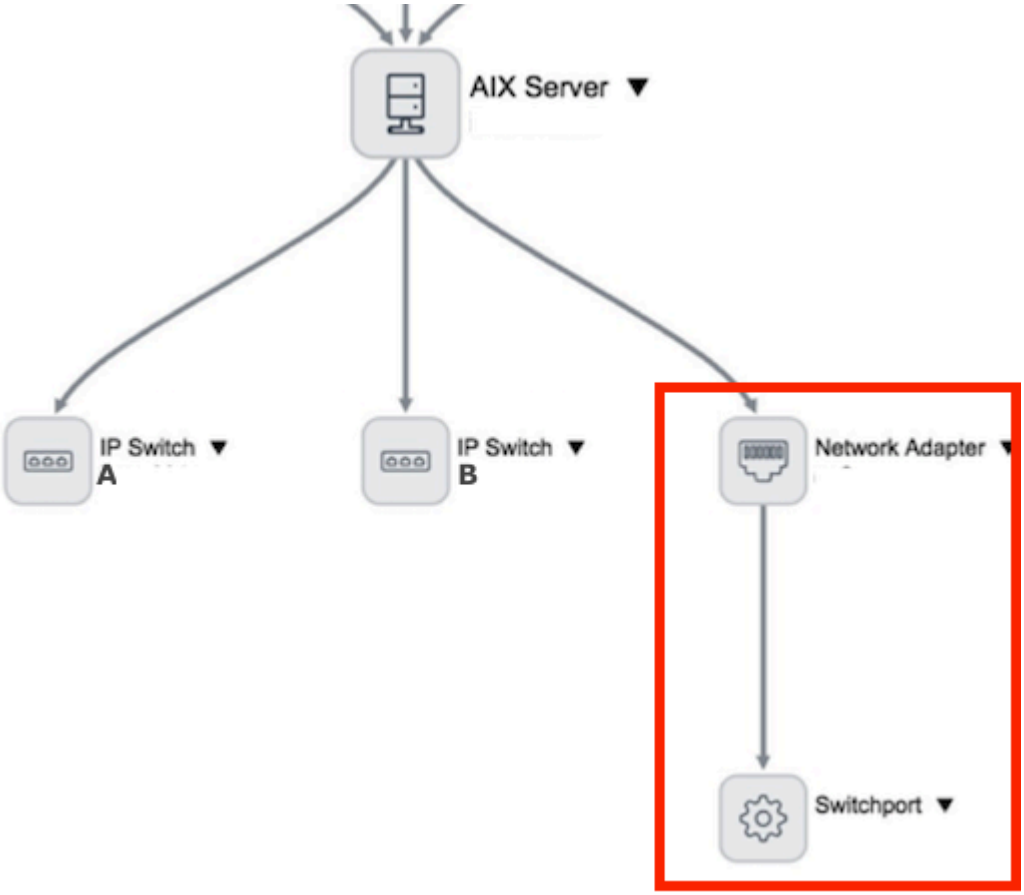
Nach der Geräteerkennung führt das System in der Gerätetabelle [discovery_device_history] die Geschäftsregel „Service Discovery - Device Complete (Service Discovery - Gerät abgeschlossen)“ aus. Diese Geschäftsregel verwendet mehrere Strategien zusammen mit Informationen aus verschiedenen Tabellen, um *Connects to:Connected by*-Beziehungen in der CMDB zu erstellen. Beziehungen können zwischen folgenden Komponenten erstellt werden:

- Einem Server und einem Switch
- Zwei Switches
- Einem Gerät und dem Port eines anderen Geräts
- Den Ports von zwei Geräten

Im folgenden Beispiel hat Discovery einen Server, auf dem AIX ausgeführt wird, und zwei IP-Switches im Netzwerk gefunden. Die folgenden Beziehungen wurden erstellt:

- Eine Beziehung vom Typ *Connects to* zwischen dem AIX-Server und den beiden IP-Switches A und B.
- Eine Referenz zwischen dem AIX-Server und seinem eigenen Netzwerkadapter.
- Eine Beziehung vom Typ *Connects to* zwischen den Adaptern auf den beiden IP-Switches (in der folgenden Abbildung nicht dargestellt).
- Eine Beziehung vom Typ *Connects to* zwischen dem Netzwerkadapter des AIX-Servers und dem Switchport von IP-Switch A (rot hervorgehoben). Diese Art von Beziehung wird standardmäßig erstellt.

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



Um diese Beziehungen anzuzeigen, öffnen Sie die Abhängigkeitsansicht für den Server. Um die Beziehung zwischen den beiden IP-Switches anzuzeigen, öffnen Sie die Abhängigkeitsansicht von einem der Switches aus, und wählen Sie in den Zuordnungseinstellungen als **Abhängigkeitstyp** die Option **Physische Netzwerkverbindungen** aus.

Layer 2-Verbindungsstrategien

Bei der Layer 2-Erkennung werden die folgenden Strategien verwendet, um Beziehungen zwischen Geräten in einem Netzwerk zu erstellen:

PhysicalHostConnectionStrategy

Diese Strategie erstellt eine Verbindung zwischen einem erkannten Server, der kein Netzwerkgerät ist, und einem Netzwerkgerät. Durch diese Strategie können Layer 2-Verbindungen nur erstellt werden, wenn in der Weiterleitungstabelle des Switch eine einzelne MAC-Adresse für den Port vorhanden ist. Wenn der Port über mehrere MAC-Adressen verfügt, erstellt Discovery keine Verbindung zwischen Server und Switch.

Wenn der Port des Switches identifiziert wird, erstellt Discovery eine Beziehung **Verbunden mit::Verbunden von** zwischen dem Serveradapter und dem Switch-Port. Andernfalls erstellt Discovery eine Beziehung **Verbunden mit::Verbunden von** zwischen dem Serveradapter und dem Switch selbst.

VMLayer2ConnectionStrategy

Diese Strategie erstellt eine Verbindung zwischen einer VM und einem Netzwerkgerät. Wenn die Anzahl der außergewöhnlichen MAC-Adressen sehr gering ist (weniger als 3 und weniger als 15 % aller MAC-Adressen des ESX-Servers und der zugehörigen VMs), erstellt Discovery eine Layer 2-Verbindung.

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

NetworkDeviceLayer2ConnnectionStrategy

Mit dieser Strategie wird eine Verbindung zwischen einem Netzwerkgerät und seinen Nachbarn erstellt. Discovery erstellt eine Layer 2-Verbindung, wenn ein einzelner Nachbar mit einer Nachbaradresse und/oder einer Nachbarschnittstelle ist. Wenn die Schnittstelle des Nachbarn vorhanden ist, erstellt Discovery eine Beziehung vom Typ **Verbunden mit::Verbunden von** zwischen der Ursprungsschnittstelle und der Schnittstelle des Nachbarn. Andernfalls erstellt Discovery eine Beziehung vom Typ **Verbunden mit::Verbunden von** zwischen der Ursprungsschnittstelle und dem Switch mit der Adresse des Nachbarn.

SpanningTreeLayer2ConnectionStrategy

Bei dieser Strategie wird eine Verbindung zwischen einem Netzwerkgerät und dem übergeordneten Element des Netzwerkgeräts in der Strukturansicht erstellt.

JavaScriptLayer2ConnectionStrategy

Diese Strategie ruft eine Javascript-Funktion mit leerer Implementierung auf. Dadurch wird die Erstellung einer zusätzlichen Strategie ermöglicht.

Address Resolution Protocol (ARP) bei der Layer 2-Erkennung

Die Probes für Address Resolution Protocol (ARP) ordnen die IP-Adresse eines Computers oder Netzwerkgeräts einer MAC-Adresse zu. Diese Probes rufen die IP-Adresse und MAC-Adresse für ein Konfigurationselement aus der Tabelle „Netzwerkinfrastrukturelement“ [dscy_net_base] ab. Geräte, die SNMP unterstützen, wie Linux-Computer und Netzwerkgeräte, speichern im Cache zwei Arten von Adressinformationen:

- **Statisch**: Manuell hinzugefügte Adressauflösungen
- **Dynamisch**: Paare aus Hardwarename und IP-Adresse, die dem Cache durch vorherige, erfolgreiche ARP-Auflösungen hinzugefügt wurden

Wenn Discovery mit der ARP-Tabelle fertig ist, erfasst das System alle statischen und dynamischen Tabelleneinträge von Geräten über SNMP. Wenn ein neuer ARP-Eintrag verfügbar ist, wird er der Netzwerk-ARP-Tabelle [discovery_net_arp_table] hinzugefügt. Wenn zuvor erkannte ARP-Einträge nicht mehr in der ARP-Tabelle des Geräts zwischengespeichert werden, löscht das System die entsprechenden Datensätze nach einem Abgleich aus der CMDB.

Hinweis: Wenn nach der Ausführung von Discovery neue ARP-Einträge erstellt werden, werden sie erst bei Ausführung des nächsten Discovery-Zeitplans erkannt. Wenn ARP-Einträge nach der Ausführung von Discovery vom Gerät gelöscht werden, wird die CMDB-ARP-Tabelle erst aktualisiert, wenn Discovery erneut ausgeführt wird.

Discovery stellt folgende Probes zum Extrahieren von Informationen zur Auflösung von IP- und MAC-Adressen bereit:

Probe	ECC-Warteschlangenthema	Befehl	Beschreibung
Linux - Network ARP Tables	SSHCommand	sh ${file:linux_arp.sh} Dadurch wird eine Skriptdatei ausgeführt, damit zuerst der Befehl net-tools (arp	Probe „SSH Command“, die Netzwerkinformationen aus der ARP-Tabelle auf einem Linux-Server abruft

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

Probe	ECC-Warteschlangenthema	Befehl	Beschreibung
		-n) ausgeführt wird. Wenn dies fehlschlägt, wird der Befehl iproute2 (ip neighbor) ausgeführt.	
Solaris - Network ARP Tables	SSHCommand	arp -an	Probe „SSH Command“, die Netzwerkinformationen aus der ARP-Tabelle auf einem Solaris-Server abruft
Windows - Network ARP Table	PowerShell	arp -a	Powershell-Probe, die Netzwerkinformationen aus der ARP-Tabelle auf einem Windows-Server abruft
SNMP - Network - ArpTable	SNMP	Tabelle Die SNMP-Probe verwendet zunächst folgende OID: `iso.org.dod.internet.mgmt.mib-2.ip.ipNetToMediaTa ipNetToMediaPhysAddress,ipNetToMediaNetAddress`. Wenn die Probe keine Ergebnisse zurückgibt, wird folgende OID verwendet: `iso.org.dod.internet.mgmt.mib-2.ip.ipNetToPhysica ipNetToPhysicalNetAddress,ipNetToPhysicalPhysAddr`	SNMP-Probe, die Informationen aus der ARP-Tabelle auf einem Switch oder Router sammelt

SNMP-Switch-Probes

Diese Probes geben Überbrückungsinformationen aus VLANs zurück, die über Netzwerk-Switches verbunden sind, einschließlich Portauswahl, Weiterleitungstabellen und die Nutzung des STP-Protokolls (Spanning Tree Protocol).

SNMP - Switch - BridgePortTable

Diese Probe gibt alle Ports eines Switch zurück, die zum Erstellen einer Bridge zwischen Netzwerksegmenten verwendet werden.

Zurückgegebene Überbrückungsdaten

Tabelle	Switch-Brückenporttabelle [discovery_switch_bridge_port_table] Diese Tabelle wird verwendet, um eine Portnummer in der Tabelle „discovery_switch_fwd_table“ einem Schnittstellenindex zuzuordnen.

Automatische Übersetzung

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

Zurückgegebene Überbrückungsdaten (Fortsetzung)

OID	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dBase.dot1dBasePortTable dot1dBasePort,dot1dBasePortIfIndex
Gefüllte Felder	• cmdb_ci • port • interface_index

SNMP - Switch - SpanningTreeTable

Diese Probe gibt den aktiven Pfad zwischen zwei beliebigen Netzwerkknoten zurück, die von einem Switch überbrückt werden.

Zurückgegebene Bereichsstrukturdaten

Tabelle	Switch-Bereichsstrukturtabelle [discovery_switch_spanning_tree_table]. Diese Tabelle wird für die Suche nach Layer 2-Verbindungen zwischen Switches verwendet.
OID	iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dStp.dot1dStpPortTable dot1dStpPort,dot1dStpPortState,dot1dStpPortEnable,dot1dStpPortDesignatedRoo
Gefüllte Felder	• cmdb_ci • port • port_state • port_enable • designated_root • designated_bridge_mac

SNMP - Switch - ForwardingTable

Diese Probe gibt Informationen aus der Weiterleitungstabelle eines Switch zurück.

Zurückgegebene Daten aus Weiterleitungstabellen

Tabelle	Switch-Weiterleitungstabelle [discovery_switch_fwd_table] Das ist die Weiterleitungstabelle für Switches.
OIDs	Diese OIDs werden nach Bedarf durch die Skripteinbindung *DiscoveryVlanSwitchProcessor* erstellt. • **Non-Cisco**: ◦ **Q-BRIDGE MIB**: `oid_spec_list = 'table iso.org.dod.internet.mgmt.mib-2.dot1dBridge.qBridgeMIB.qBridge dot1qTpFdbAddress.' + vlanIndex +`

Automatische Übersetzung

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

Zurückgegebene Daten aus Weiterleitungstabellen (Fortsetzung)

	',dot1qTpFdbPort.' + vlanIndex + ',dot1qTpFdbStatus.' + vlanIndex; ◦ **BRIDGE MIB**: oid_spec_list = 'table iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dTp.dot1dTpFdbTable dot1dTpFdbAddress,dot1dTpFdbPort,dot1dTpFdbStatus'; • **Cisco BRIDGE MIB**: `oid_spec_list = 'table iso.org.dod.internet.mgmt.mib-2.dot1dBridge.dot1dTp.dot1dTpFdbTa dot1dTpFdbAddress,dot1dTpFdbPort,dot1dTpFdbStatus';`
Zusätzliche aufgerufene Probe	Die SSH-Probe `Switch - MAC Table` kann durch die Skripteinbindung *`DiscoveryVlanSwitchProcessor`* ausgelöst werden, um zusätzliche Layer 2-Daten bereitzustellen. Wenn Layer 2-Daten fehlen, nachdem Sie die Erkennung in mehreren VLANs ausgeführt haben, sollten Sie das Auslösen der Probe `Switch - MAC Table` aktivieren und die Erkennung erneut ausführen. Fügen Sie dazu der Tabelle „Systemeigenschaft“ [sys_properties] die folgende Eigenschaft hinzu: `glide.discovery.sensors.forwardingtable.ssh`. Legen Sie den Wert der Eigenschaft auf **true** fest. Standardmäßig ist diese Eigenschaft auf „false“ eingestellt.
Befehl	show mac address-table
Gefüllte Felder	• cmdb_ci • vlan_id • port • Status • mac_address (aus dem Feld **cmdb_ci** in der Tabelle „Netzwerkinfrastrukturelement“ [discovery_net_base])

SNMP - Switch - Vlan

Diese Probe gibt VLAN-IDs von einem Netzwerk-Switch und die folgenden OIDs zurück:

```
iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoV
tpMIB.vtpMIBObjects.vlanInfo.vtpVlanTable vtpVlanState

iso.org.dod.internet.private.enterprises.cisco.ciscoMgmt.ciscoV
lanMembershipMIB.ciscoVlanMembershipMIBObjects.vmMembership.vmM
embershipSummaryTable vmMembershipSummaryVlanIndex,vmMembership
SummaryMemberPorts,vmMembershipSummaryMember2kPorts
```


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

```
iso.org.dod.internet.private.enterprises.juniperMIB.jnxMibs.jnx
ExMibRoot.jnxExSwitching.jnxExVlan.jnxVlanMIBObjects.jnxExVlanT
able jnxExVlanTag

iso.org.dod.internet.mgmt.mib-2.system.sysDescr
```

Andere Switch-Typen werden nicht unterstützt.

Porttabellen

Die folgenden Porttabellen werden während der horizontalen Erkennung eines Geräts gefüllt:

- Netzwerkadapter [cmdb_ci_network_adapter]
- Switchport [dscy_switchport]
- Routerschnittstelle [dscy_router_interface]
- Load Balancer-Schnittstelle [cmdb_ci_lb_interface]

Erkennung von TCP-Verbindungen

Discovery identifiziert und klassifiziert Informationen zu TCP-Verbindungen mithilfe der ADM- und ADME-Probes.

Discovery füllt die Tabelle „TCP-Verbindungen“ [cmdb_tcp] mit folgenden Daten.

Bezeichnung	Tabellenname	Feldname	Beschreibung
Abwesend	cmdb_tcp	absent	Wenn der Prozess auf diesem Gerät nicht mehr ausgeführt wird. Wenn der Prozess zum ersten Mal erkannt wird, wird der Wert nicht ausgewählt (sprich: der Prozess fehlt nicht). Wenn Discovery erneut ausgeführt wird und den Prozess nicht erkennt, wird er ausgewählt.
Computer	cmdb_tcp	Computer	Das Gerät, das mit dem TCP-Port verbunden ist oder diesen abhört
IP	cmdb_tcp	ip	Die IP-Adresse, die von diesem Gerät oder Prozess abgehört wird oder mit der eine Verbindung besteht. Wenn die IP-Adresse 127.0.0.1 lautet, handelt es sich um den Hostcomputer selbst.
PID	cmdb_tcp	pid	Die ID des Prozesses, zu dem eine Verbindung hergestellt wird oder der von diesem Gerät (IP-Adresse) abgehört wird
Port	cmdb_tcp	port	Die Portnummer, über die der TCP-Datenverkehr erkannt wurde
Vorgang	cmdb_tcp	process	Der Prozess, zu dem eine Verbindung hergestellt wird oder der von dem Port abgehört wird
Typ	cmdb_tcp	Typ	• **Lauschen auf**: Der Prozess hört das Gerät über TCP ab. • **Verbindung wird hergestellt**: Wenn der Prozess über TCP mit diesem Gerät verbunden ist

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

Bezeichnung	Tabellenname	Feldname	Beschreibung
count	cmdb_tcp	count	Die Häufigkeit, mit der Discovery eine bestimmte TCP-Verbindung erkennt. Dieses Feld wird von erweiterten ADM-Probes verwendet.

Discovery füllt die Tabelle „Laufender Prozess“ [cmdb_running_process] mit diesen Daten.

Bezeichnung	Feldname	Beschreibung
Name	Name	Der Name des laufenden Prozesses
Computer	Computer	Das Gerät, auf dem der Prozess ausgeführt wird
Übergeordnet	parent	Der übergeordnete Prozess dieses Prozesses, falls vorhanden
Lauschen auf	listening_on	Die Ports, die von den Prozessen abgehört werden
Verbunden mit	connected_to	Die Ports, mit denen die Prozesse verbunden sind
Befehl	command	Der Befehl für diesen Prozess, einschließlich Pfad
PID	pid	Die ID für den Prozess
PPID	ppid	Die ID für den übergeordneten Prozess
Abwesend	absent	Wenn der Prozess auf diesem Gerät nicht mehr ausgeführt wird. Wenn der Prozess zum ersten Mal erkannt wird, wird der Wert nicht ausgewählt (sprich: der Prozess fehlt nicht). Wenn Discovery erneut ausgeführt wird und den Prozess nicht erkennt, wird er ausgewählt.
Klassifizieren	classify	Gibt an, ob der laufende Prozess klassifiziert werden soll
Schlüsselparameter	key_parameters	Die Schlüsselparameter für den Befehl
Parameter	parameters	Die Parameter für den Befehl
Anzahl	count	Die Häufigkeit, mit der Discovery eine bestimmte TCP-Verbindung erkennt. Dieses Feld wird von erweiterten ADM-Probes verwendet.

Standardmäßige ADM-Probes

Mit der standardmäßigen ADM-Erkennung startet Discovery die folgenden Probes:

Name	Beschreibung	Eingeschlossene Sub-Probes
AIX - ADM	Fragt Informationen über aktive (laufende) AIX-Prozesse und aktive Verbindungen ab. Diese Informationen sind für die Zuordnung von Anwendungsabhängigkeiten erforderlich.	• AIX - Active Connections • AIX - Active Processes

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

Name	Beschreibung	Eingeschlossene Sub-Probes
HP-UX - ADM	Fragt Informationen über aktive (laufende) HP-UX-Prozesse und aktive Verbindungen ab. Diese Informationen sind für die Zuordnung von Anwendungsabhängigkeiten erforderlich. Diese Probe erfordert die Installation von lsof und die Aktivierung der Probe „UNIX - Active Connections“, der standardmäßig inaktiv ist.	• UNIX - Active Connections • HP-UX - Active Processes
Solaris - ADM	Fragt Informationen über aktive (laufende) Solaris-Prozesse und aktive Verbindungen ab. Diese Informationen sind für die Zuordnung von Anwendungsabhängigkeiten erforderlich. Diese Probe wird durch die Probe „Solaris Zones“ ausgelöst. Das System löst eine ADM-Probe für jede lokale Zone in einer globalen Zone aus. Diese Probe erfordert, dass lsof in der globalen Zone installiert wird.	• Solaris - Active Processes • Solaris - Active Connections
UNIX - ADM	Fragt Informationen über aktive (laufende) UNIX-Prozesse und aktive Verbindungen ab. Diese Informationen sind für die Zuordnung von Anwendungsabhängigkeiten erforderlich.	• UNIX - Active Connections • UNIX - Active Processes
Windows - ADM	Fragt Informationen über aktive (laufende) Windows-Prozesse und aktive Verbindungen ab. Diese Informationen sind für die Zuordnung von Anwendungsabhängigkeiten erforderlich.	• Windows - Active Connections • Windows - Active Processes
UNIX - ADM netstat	Führt dieselben Funktionen wie die Probe „UNIX ADM“ aus, ist dabei zur Unterstützung der kontinuierlichen TCP-basierten Erkennung auf Netstat angewiesen. Service Mapping verwendet diese Probe für die auf Datenverkehr basierende Erkennung.	• UNIX - Active Connections with Netstat. Diese Probe ruft TCP-Verbindungen ab, um die Tabellen cmdb_tcp und cmdb_tcp_connection zu füllen. • UNIX - Active Processes. Diese Probe ruft TCP-Prozesse ab und füllt die Tabelle cmdb_running_process.

Erweiterte ADM-Probes

Wenn erweitertes ADM aktiviert ist, startet Discovery die folgenden Probes:

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

Probe	Beschreibung
Windows - ADM Enhanced	Führt dieselben Funktionen wie die Probe „Windows ADM“ aus, jedoch mit zusätzlichen Parametern, um die kontinuierliche TCP-basierte Erkennung zu steuern. Diese Probe ist sowohl mit von WinRM unterstützten als auch mit nicht von WinRM unterstützten MID Servern kompatibel. Konfigurieren Sie Ihren MID Server mit dem Parameter `mid.windows.management_protocol`. Unter MID-Server-Parameter finden Sie die Werte, die Sie für diesen Parameter verwenden können.
UNIX - ADM Enhanced	Führt dieselben Funktionen wie die Probe „UNIX ADM“ aus, jedoch mit zusätzlichen Parametern, um die kontinuierliche TCP-basierte Erkennung zu steuern.

Verwenden Sie mit den erweiterten ADM-Probes die folgenden Probe-Parameter:

Parameter	Beschreibung
mid.adme.max_result_size	Steuert die Größe der TCP-Nachverfolgungsdatei
max.adme_result_payload_size	Steuert die Größe des Ergebnisses, einschließlich der Nutzlast **Hinweis:** Wenn dieser Wert größer als die MID-Server-Eigenschaften „mid.discovery.max_payload_size“ ist, kann ein Konfigurationsfehler auftreten.

Zugehörige Informationen

Application Dependency Mapping (ADM) für Discovery

Erkennung von IP-Adressen

Discovery identifiziert und klassifiziert Informationen über IP-Adressen.

Von Discovery über IP-Adressen erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
IP-Adresse	cmdb_ci_ip_address	ip_address	Verschiedene interne
IP-Version	cmdb_ci_ip_address	ip_version	Verschiedene interne
Netzmaske	cmdb_ci_ip_address	netmask	Verschiedene interne
Nic	cmdb_ci_ip_address	nic	Verschiedene interne

Erkennung von IP-Netzwerken

Discovery identifiziert und klassifiziert Informationen über IP-Netzwerke.

Von Discovery über IP-Netzwerke erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Erkennen	cmdb_ci_ip_network	discover	Verschiedene interne

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

Von Discovery über IP-Netzwerke erfasste Daten (Fortsetzung)

Bezeichnung	Tabellenname	Feldname	Quelle
Subnetz	cmdb_ci_ip_network	subnet	Verschiedene interne
Netzwerk-Discovery	cmdb_ci_ip_network	network_discovery	Verschiedene interne
Zuletzt erkannt	cmdb_ci_ip_network	last_discovered	Verschiedene interne
MID-Server	cmdb_ci_ip_network	mid_server	Verschiedene interne
Router	cmdb_ci_ip_network	router	Verschiedene interne
Status	cmdb_ci_ip_network	state	Verschiedene interne

Erkennung von Netzwerkdruckern

Discovery identifiziert und klassifiziert Informationen über Netzwerkdrucker.

Discovery kann Netzwerkdrucker identifizieren und klassifizieren.

Von Discovery über Netzwerkdrucker erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Seriennummer	cmdb_ci	serial_number	SNMP, verschiedene MIBs
Startdatum	cmdb_ci	start_date	SNMP, RFC1213 MIB
Hersteller	cmdb_ci	manufacturer	SNMP, RFC1213 MIB
Modell-ID	cmdb_ci	model_id	SNMP, RFC1213 MIB
IP-Adresse	cmdb_ci_network_adapter	ip_address	SNMP, IP MIB
MAC-Adresse	cmdb_ci_network_adapter	mac_address	SNMP, IF MIB
Druckertyp	cmdb_ci_printer	print_type	SNMP, PRINT MIB
Zähler verwenden	cmdb_ci_printer	use_count	SNMP, PRINT MIB
Einheiten für Nutzungszähler	cmdb_ci_printer	use_units	SNMP, PRINT MIB
Farben	cmdb_ci_printer	colors	SNMP, PRINT MIB
Horizontale Auflösung	cmdb_ci_printer	horizontal_resolution	SNMP, PRINT MIB
Vertikale Auflösung	cmdb_ci_printer	vertical_resolution	SNMP, PRINT MIB
Auflösungseinheiten	cmdb_ci_printer	resolution_units	SNMP, PRINT MIB
Beschreibung	discovery_printer_supplies	Beschreibung	SNMP, PRINT MIB
Versorgungstyp	discovery_printer_supplies	supply_type	SNMP, PRINT MIB
Versorgungsklasse	discovery_printer_supplies	supply_class	SNMP, PRINT MIB
Aktuelle Ebene	discovery_printer_supplies	current_level	SNMP, PRINT MIB
Max. Kapazität	discovery_printer_supplies	max_capacity	SNMP, PRINT MIB
Name	cmdb_ci	Name	Shazzam, SNMP, verschiedene MIBs

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

Erkennung von Routern und Switches

Discovery identifiziert und klassifiziert Informationen über Netzwerkrouter und Switches.

Netzwerkrouter und Switches besitzen oft sehr ähnliche Funktionen. Einige Switches, die als Layer 3-Switches bezeichnet werden, verfügen üblicherweise über IP-Weiterleitung. Größere Router mit optionalen Modulen können unter Umständen Switching-Module aufnehmen. Aufgrund dieser Überschneidungen und der sich daraus ergebenden Mehrdeutigkeit der Klassifizierung eines bestimmten Geräts erfasst Discovery für Router und Switches dieselben Daten, sofern diese auf einem bestimmten Gerät verfügbar sind. Weitere Informationen dazu, wie Discovery Daten über Verbindungen zwischen Netzwerkgeräten und anderen Komponenten erfasst, finden Sie unter Layer 2-Erkennung.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Voraussetzungen

- Der Router oder Switch muss über IP-Adressinformationen verfügen.
- Die Systemeigenschaft glide.discovery.L3_mapping wird auf „true“ festgelegt, damit Router und Switches erkannt werden.
- Der Router oder Layer 3-Switch, der die IP-Adresse bereitstellt, muss erfolgreich mit den vorhandenen Weiterleitungsregeln für Exit-Schnittstellen erkannt werden.
- Wenn Sie die Tabelle [discovery_device_neightors] während der horizontalen Layer-2-Discovery der BGP-fähigen Geräte ausfüllen müssen, legen Sie die Eigenschaft **Deaktivieren der BGP-Routererkundung** auf **Nein**fest. Beachten Sie, dass das Aktivieren dieser Eigenschaft zu Leistungsproblemen führen kann, einschließlich Problemen aufgrund von unzureichendem Arbeitsspeicher auf dem MID-Server.

Systemeigenschaften

Sie können viele Aspekte von Discovery so konfigurieren, dass sie Ihren persönlichen Präferenzen entsprechen. Die folgenden Eigenschaften gelten für Netzwerkrouter und -Switches. Um die Eigenschaften anzuzeigen, navigieren Sie zu **Discovery-Definition** > **Eigenschaften** sofern nicht anders angegeben.

Eigenschaft	Beschreibung
glide.discovery.L3_mapping	Dadurch wird eine Beziehung vom Typ IP-Verbindung::IP-Verbindung zwischen Servern und Netzwerkgeräten erstellt. • **Typ:** Zeichenfolge • **Standardwert:** Wahr • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
glide.discovery.max_concurrent_invocations_per_schedule	Legt die maximale Anzahl geplanter Aufrufe desselben Erkennungszeitplans fest. Dadurch wird verhindert, dass die geplanten Ausführungen in Rückstand geraten, wenn die Erkennung nicht vor

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

Eigenschaft	Beschreibung
	der geplanten Ausführung des nächsten Aufrufs abgeschlossen ist. Der Wert ist eine Ganzzahl, die der maximalen Anzahl automatisierter Aufrufe desselben Zeitplans entspricht, die gleichzeitig ablaufen können. Nach Erreichen des Limits werden nachfolgende geplante Aufrufe storniert. Diese Eigenschaft wird durch den Wert 0 oder eine negative Zahl deaktiviert. • **Typ:** Ganzzahl • **Standardwert:** 3 • **Standort: Discovery-Definition** > **Eigenschaften** **Hinweis:** Diese Eigenschaft gilt nicht für Zeitpläne, für die die Konfiguration „Ausführen nach“ auf „Auch bei Abbruch“ festgelegt ist.

Anmeldeinformationen

Discovery untersucht mit dem SNMP-Protokoll viele Arten von Geräten (Switches, Router, Drucker usw.). Anmeldeinformationen für SNMP-Communitys beinhalten keinen Benutzernamen, sondern nur ein Passwort, das als Community-Zeichenfolge bezeichnet wird. Die standardmäßige schreibgeschützte Community-Zeichenfolge für viele SNMP-Geräte ist öffentlich, und Discovery testet diese automatisch. SNMPv3-Anmeldeinformationen erfordern je nach ausgewähltem Protokoll einen Benutzernamen und einen Schlüssel. Geben Sie die entsprechenden SNMP-Anmeldeinformationen ein, wenn sie sich von der öffentlichen Community-Zeichenfolge unterscheiden.

Hinweis: SSH wird für Lastenausgleichsmodule unterstützt, für Router und Switches aber nicht.

Klassifizierer, Muster und Probes

Klassifizierungen	Auslöser-Probes	Muster
Standard Network Router Standard Network Switch	• Horizontal Pattern: Startet Muster • SNMP-Weiterleitung^ • DNS* • SNMP-Identität*	Network Router Network Switch

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

Klassifizierungen	Auslöser-Probes	Muster
	• SNMP-Switch-VLAN* • SNMP-Switching* • SNMP - Network - ArpTable* (nur Standard Network Switch)	

*Für neue Instanzen sind diese Probes für den Klassifizierer inaktiv. Discovery verwendet für die Erkennung Muster.

^Diese Probe bleibt für den Klassifizierer „Standard Network Router“ standardmäßig aktiv, selbst wenn Discovery die Mustererkennung verwendet.

Um Muster zu verwenden, vergewissern Sie sich, dass das richtige Muster in der horizontalen Mustersonde des Klassifizierers angegeben ist. Siehe Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen für Anweisungen.

Gestapelte Switches erkennen

Die gemeinsam genutzte Bibliothek „Network Switch“ bietet Unterstützung für gestapelte Cisco-Switches. Die CI-Tabelle hierfür ist „IP-Switch“ [cmdb_ci_ip_switch]. Mehrere Switches im Stapel werden anhand der primären IP-Adresse identifiziert. Jedes Mitglied des Stapels wird durch eine Kombination von Elementen identifiziert, darunter die primäre IP-Adresse, einen dem Switch zugeordneten Namen und den Stapelmodus. Die Beziehung wird zwischen einer primären und allen sekundären IP-Adressen erstellt. Der primäre Switch verfügt über alle in der folgenden Tabelle aufgeführten Felder. Der sekundäre Switch besitzt die Felder name, ip_address, serial_number, model_id, manufacturer, stack und stack_mode.

Hinweis: Wenn alle Ports auf einem Switch an Port 161 geöffnet sind, besitzt dieser Switch mehrere IP-Adressen (eine für jeden Port), während die Seriennummer für alle Ports identisch ist. Die CI-Identifizierung erfolgt basierend auf der Seriennummer. Daher wird jedes Mal derselbe Datensatz aktualisiert, anstatt einen neuen Datensatz zu erstellen.

Router- und Switch-Daten

Tabellenname	Bezeichnung/Feldname	Quelle
cmdb_ci	Seriennummer serial_number	SNMP, verschiedene MIBs
cmdb_ci	Startdatum (nur, wenn das Ziel ein Host ist) start_date	SNMP, RFC1213 MIB
cmdb_ci	Hersteller manufacturer	SNMP, RFC1213 MIB
cmdb_ci	Modell-ID	SNMP, RFC1213 MIB

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

Tabellenname	Bezeichnung/Feldname	Quelle
	model id	
cmdb_ci_ip_router	Name Name	
cmdb_ci_ip_router	Modell-ID model ID	SNMP, RFC1213 MIB
cmdb_ci_ip_router	Hersteller manufacturer	SNMP, RFC1213 MIB
cmdb_ci_ip_router	Seriennummer serial_number	SNMP, verschiedene MIBs
cmdb_ci_ip_router	IP-Adresse ip_address	SNMP, IP MIB
cmdb_ci_ip_router	Beschreibung short_description	
cmdb_ci_ip_router	IP-Routing möglich can_route	SNMP, IP MIB, BGP MIB
cmdb_ci_ip_router	IP-Switching möglich can_switch	SNMP, dot1dBridge MIB
cmdb_ci_ip_router	Port port	
cmdb_ci_ip_switch	Name Name	
cmdb_ci_ip_switch	Modell-ID model ID	SNMP, RFC1213 MIB
cmdb_ci_ip_switch	Hersteller	SNMP, RFC1213 MIB

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

Tabellenname	Bezeichnung/Feldname	Quelle
	manufacturer	
cmdb_ci_ip_switch	Seriennummer serial_number	SNMP, verschiedene MIBs
cmdb_ci_ip_switch	IP-Adresse ip_address	SNMP, IP MIB
cmdb_ci_ip_switch	Beschreibung short_description	
cmdb_ci_ip_switch	IP-Routing möglich can_route	SNMP, IP MIB, BGP MIB
cmdb_ci_ip_switch	Ports Ports	SNMP, dot1dBridge MIB
cmdb_ci_ip_switch	IP-Switching möglich can_switch	SNMP, dot1dBridge MIB
cmdb_ci_ip_switch	Kann VLANs partitionieren can_partitionvlans	SNMP, dot1dBridge MIB
cmdb_ci_ip_switch	Stapel stack	SNMP, entPhysicalTable
cmdb_ci_ip_switch	Stapelmodus stack_mode	SNMP, entPhysicalTable
cmdb_ci_netgear	IP-Routing möglich can_route	SNMP, IP MIB, BGP MIB
cmdb_ci_netgear	IP-Switching möglich can_switch	SNMP, dot1dBridge MIB
cmdb_ci_netgear	Kann VLANs partitionieren	SNMP, dot1dBridge MIB

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

Tabellenname	Bezeichnung/Feldname	Quelle
	cdscy_router_interface	
cmdb_ci_netgear	Hub möglich can_hub	SNMP, IP MIB
cmdb_ci_network_adapter	IP-Adresse ip_address	SNMP, IP MIB
cmdb_ci_network_adapter	MAC-Adresse mac_address	SNMP, IF MIB
discovery_device_neighbors	Nachbaradresse neighbor_address	ciscoCdpMIB
discovery_device_neighbors	Nachbar-ID neighbor_ID	ciscoCdpMIB, lldpMIB
discovery_device_neighbors	Nachbarschnittstelle neighbor_interface	ciscoCdpMIB, lldpMIB
discovery_device_neighbors	Nachbarquelle neighbor_source	ciscoCdpMIB, lldpMIB
discovery_device_neighbors	Ursprungsschnittstelle origin_interface	ciscoCdpMIB, lldpMIB
discovery_net_arp_table	IP-Adresse IP_address	SNMP, IP MIB
discovery_net_arp_table	MAC-Adresse mac_address	SNMP, IP MIB
discovery_switch_bridge_port_table	Schnittstellenindex interface_index	SNMP, dot1dBridge MIB
discovery_switch_bridge_port_table	Port	SNMP, dot1dBridge MIB

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

Tabellenname	Bezeichnung/Feldname	Quelle
	port	
discovery_switch_fwd_table	MAC-Adresse mac_address	SNMP, dot1dBridge MIB
discovery_switch_fwd_table	Port port	SNMP, dot1dBridge MIB
discovery_switch_fwd_table	Status Status	SNMP, dot1dBridge MIB
discovery_switch_fwd_table	VLAN-ID vlan_id	SNMP, dot1dBridge MIB
discovery_switch_spanning_tree_table	Festgelegter Brücken-MAC designated_bridge_mac	SNMP, dot1dBridge MIB
discovery_switch_spanning_tree_table	Festgelegter Root designated_root	SNMP, dot1dBridge MIB
discovery_switch_spanning_tree_table	Port port	SNMP, dot1dBridge MIB
discovery_switch_spanning_tree_table	Portaktivierung port_enable	SNMP, dot1dBridge MIB
discovery_switch_spanning_tree_table	Portstatus port_state	SNMP, dot1dBridge MIB
dscy_router_interface	Name Name	SNMP, IP MIB
dscy_router_interface	Typ Typ	SNMP, IP MIB
dscy_router_interface	Nummer	SNMP, IP MIB

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

Tabellenname	Bezeichnung/Feldname	Quelle
	Nummer	
dscy_router_interface	IP-Adresse ip_address	SNMP, IP MIB
dscy_router_interface	MAC-Adresse mac_address	SNMP, IP MIB
dscy_route_interface	Zielnetzwerk dest_ip_network	SNMP, IP MIB
dscy_route_interface	Typ Typ	SNMP, IP MIB
dscy_route_next_hop	Zielnetzwerk dest_ip_network	SNMP, IP MIB
dscy_route_next_hop	Typ Typ	SNMP, IP MIB
dscy_route_next_hop	Nächster Hop next_hop_ip_address	SNMP, IP MIB
dscy_switchport	Typ Typ	SNMP, dot1dBridge MIB
dscy_switchport	Status Status	SNMP, dot1dBridge MIB
dscy_switchport	MAC-Adresse mac_address	SNMP, dot1dBridge MIB
dscy_switchport	Portnummer port_number	SNMP, dot1dBridge MIB
dscy_switchport	Schnittstellenname	SNMP, dot1dBridge MIB

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

Tabellenname	Bezeichnung/Feldname	Quelle
	interface_name	
dscy_switchport	Schnittstellennummer interface_number	SNMP, dot1dBridge MIB
dscy_swtch_fwd_rule	MAC-Adresse mac_address	SNMP, dot1dBridge MIB
dscy_swtch_fwd_rule	MAC-Hersteller mac_mfr	SNMP, dot1dBridge MIB
dscy_swtch_fwd_rule	Status Status	SNMP, dot1dBridge MIB
dscy_swtch_fwd_rule	IP-Adresse ip_address	SNMP, dot1dBridge MIB
dscy_swtch_fwd_rule	Netzmaske netmask	SNMP, dot1dBridge MIB
dscy_swtch_partition	Basis-IP-Adresse base_ip_address	SNMP, dot1dBridge MIB
dscy_swtch_partition	Basis-MAC-Adresse base_mac_address	SNMP, dot1dBridge MIB
dscy_swtch_partition	Basis-Netzmaske base_netmask	SNMP, dot1dBridge MIB
dscy_swtch_partition	Typ Typ	SNMP, dot1dBridge MIB
dscy_swtch_partition	Transparent transparent	SNMP, dot1dBridge MIB
dscy_swtch_partition	Quellroute	SNMP, dot1dBridge MIB

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

Tabellenname	Bezeichnung/Feldname	Quelle
	sourceroute	
dscy_swtch_partition	Name Name	SNMP, dot1dBridge MIB
dscy_swtch_partition	Status Status	SNMP, dot1dBridge MIB
dscy_swtch_partition	Schnittstellennummer interface_number	SNMP, dot1dBridge MIB

Erfassung von Portdaten für SNMP-Netzwerkgeräte deaktivieren

In einigen Umgebungen möchten Sie die Portdaten für SNMP-Netzwerkgeräte möglicherweise nicht erfassen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Netzwerkgeräte eine sehr große Anzahl von Ports enthalten und die Informationen jedes einzelnen Ports für die Gesamtverwaltung der Geräte nicht kritisch sind, möchten Sie Portdaten für SNMP-Netzwerkgeräte möglicherweise nicht erfassen. Dies wirkt sich auf die Erstellung von Datensätzen in der Switchports-Tabelle (dscy_switchport) aus. Dieser Prozess wirkt sich nur auf die Probe-Erkennung aus.

Prozedur

1. Navigieren zu **Discovery-Definition** > **Probes**.
2. Wechseln Sie zur Probe **SNMP - Switching**.
3. Suchen Sie auf der Registerkarte **SNMP-Felder** nach dem Feld „ **ports“**, doppelklicken Sie auf den Wert in der Spalte **„Aktiv“**, und ändern Sie den Wert in **„false“**.
   Dadurch werden die Erfassung und Verarbeitung von Portinformationen für Switches deaktiviert. Das Feld **ports** für das Switch-CI muss die richtige Anzahl von Ports enthalten, auch wenn die zugehörige Liste **switchports** leer ist.
4. Klicken Sie auf das Häkchen, um die Änderung zu speichern.

Erkennung von IP-Services und Daemons

Discovery identifiziert und klassifiziert Informationen über Services und Daemons.

Von Discovery über Services und Daemons erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Name	`cmdb_ip_service`	Name	Verschiedene
Port	`cmdb_ip_service`	port	Verschiedene
Beschreibung	`cmdb_ip_service_ci`	Beschreibung	Verschiedene

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

Von Discovery über Services und Daemons erfasste Daten (Fortsetzung)

Bezeichnung	Tabellenname	Feldname	Quelle
CI	cmdb_ip_service_ci	ci	Interne Referenz
Service	cmdb_ip_service_ci	service	Interne Referenz

Erkennung unterbrechungsfreier Stromversorgungen (USV)

Discovery identifiziert und klassifiziert Informationen zu einer unterbrechungsfreien Stromversorgung (USV).

Discovery kann unterbrechungsfreie Stromversorgungen identifizieren und klassifizieren.

Von Discovery über unterbrechungsfreie Stromversorgungen erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Seriennummer	cmdb_ci	serial_number	SNMP, verschiedene MIBs
Startdatum	cmdb_ci	start_date	SNMP, RFC1213 MIB
Hersteller	cmdb_ci	manufacturer	SNMP, RFC1213 MIB
Modell-ID	cmdb_ci	model_id	SNMP, RFC1213 MIB
IP-Adresse	cmdb_ci_network_adapter	ip_address	SNMP, IP MIB
MAC-Adresse	cmdb_ci_network_adapter	mac_address	SNMP, IF MIB
Version der USV-Software	cmdb_ci_ups	ups_software_version	SNMP, UPS MIB
Version der Agent-Software	cmdb_ci_ups	agent_software_version	SNMP, UPS MIB
Angeschlossene Geräte	cmdb_ci_ups	attached_devices	SNMP, UPS MIB
Batteriestatus	cmdb_ci_ups	battery_status	SNMP, UPS MIB
Sekunden Restbatterieleistung	cmdb_ci_ups	seconds_on_battery	SNMP, UPS MIB
Geschätzte Minuten Restbatterieleistung	cmdb_ci_ups	est_mins_remaining	SNMP, UPS MIB
Geschätzte verbleibende Ladung (%)	cmdb_ci_ups	est_charge_remaining	SNMP, UPS MIB
Batteriespannung	cmdb_ci_ups	battery_voltage	SNMP, UPS MIB
Batteriestromstärke	cmdb_ci_ups	battery_current	SNMP, UPS MIB

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

Von Discovery über unterbrechungsfreie Stromversorgungen erfasste Daten (Fortsetzung)

Bezeichnung	Tabellenname	Feldname	Quelle
Batterietemperatur (C)	cmdb_ci_ups	battery_temperature	SNMP, UPS MIB
Eingangsleitungsfehler	cmdb_ci_ups	input_line_bads	SNMP, UPS MIB
Ausgangsquelle	cmdb_ci_ups	output_source	SNMP, UPS MIB
Ausgangsfrequenz	cmdb_ci_ups	output_freq	SNMP, UPS MIB
Umgehungs-Frequenz	cmdb_ci_ups	bypass_freq	SNMP, UPS MIB
Nenn-Eingangsspannung	cmdb_ci_ups	nom_input_volt	SNMP, UPS MIB
Nenn-Eingangsfrequenz	cmdb_ci_ups	nom_input_freq	SNMP, UPS MIB
Nenn-Ausgangsspannung	cmdb_ci_ups	nom_output_volt	SNMP, UPS MIB
Nenn-Ausgangsfrequenz	cmdb_ci_ups	nom_output_freq	SNMP, UPS MIB
Nenn-Ausgangs-VA	cmdb_ci_ups	rated_output_va	SNMP, UPS MIB
Nenn-Ausgangsleistung	cmdb_ci_ups	rated_output_power	SNMP, UPS MIB
Schwellenwert niedriger Batteriestand (Minuten)	cmdb_ci_ups	low_battery_threshold_mins	SNMP, UPS MIB
Akustischer Alarmstatus	cmdb_ci_ups	audible_alarm_status	SNMP, UPS MIB
Niederstrom-Transferpunkt	cmdb_ci_ups	low_voltage_transfer_point	SNMP, UPS MIB
Starkstrom-Transferpunkt	cmdb_ci_ups	high_voltage_transfer_point	SNMP, UPS MIB
Eingabeverzeichnis	cmdb_ci_ups_input	input_index	SNMP, UPS MIB
Eingangsfrequenz (Hz)	cmdb_ci_ups_input	input_freq	SNMP, UPS MIB
Eingangsspannung (RMS VAC)	cmdb_ci_ups_input	input_volt	SNMP, UPS MIB
Eingangsstrom (RMS AAC)	cmdb_ci_ups_input	input_current	SNMP, UPS MIB
Eingangsleistung (Watt)	cmdb_ci_ups_input	input_power	SNMP, UPS MIB

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

Von Discovery über unterbrechungsfreie Stromversorgungen erfasste Daten (Fortsetzung)

Bezeichnung	Tabellenname	Feldname	Quelle
Ausgangsverzeichnis	cmdb_ci_ups_output	output_index	SNMP, UPS MIB
Ausgangslast (%)	cmdb_ci_ups_output	output_load	SNMP, UPS MIB
Ausgangsspannung (RMS VAC)	cmdb_ci_ups_output	output_volt	SNMP, UPS MIB
Ausgangsstrom (RMS AAC)	cmdb_ci_ups_output	output_current	SNMP, UPS MIB
Ausgangsleistung (Watt)	cmdb_ci_ups_output	output_power	SNMP, UPS MIB
Verzeichnis umgehen	cmdb_ci_ups_bypass	bypass_index	SNMP, UPS MIB
Spannung umgehen (RMS VAC)	cmdb_ci_ups_bypass	bypass_volt	SNMP, UPS MIB
Stromstärke umgehen (RMS AAC)	cmdb_ci_ups_bypass	bypass_current	SNMP, UPS MIB
Leistung umgehen (Watt)	cmdb_ci_ups_bypass	bypass_power	SNMP, UPS MIB
Alarmverzeichnis	cmdb_ci_ups_alarm	alarm_index	SNMP, UPS MIB
Alarmtyp	cmdb_ci_ups_alarm	alarm_type	SNMP, UPS MIB
Alarmzeit	cmdb_ci_ups_alarm	alarm_time	SNMP, UPS MIB

IBM WebSphere DataPower-Discovery

ITOM-Transparenz erkennt IBM WebSphere DataPower. Discovery verwendet das Muster „DataPower Server“ für die horizontale Erkennung. Service-Mapping verwendet das Muster „DataPower“ für die Erkennung von oben nach unten.

Voraussetzungen

Konfigurieren Sie vor der Erkennung von IBM WebSphere DataPower-Geräten die folgenden Anmeldeinformationen:

SNMP-Anmeldeinformationen

SNMP-Anmeldeinformationen sind für die Verwendung der folgenden SNMP-Abfragen erforderlich:

- Für die Horizontal-Discovery des Hostservers von DataPower [cmdb_ci_datapower_server]:
  - 1.3.6.1.2.1.1.1
  - 1.3.6.1.2.1.1.5
  - 1.3.6.1.2.1.4.20.1
  - 1.3.6.1.2.1.2.2.1

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

- 1.3.6.1.4.1.14685.3.1.196.1
- 1.3.6.1.4.1.14685.3.1.11.1
- 1.3.6.1.4.1.14685.3.1.112.1

- Für die Top Down-Discovery des Hostservers für DataPower [cmdb_ci_datapower_server]:
  - 1.3.6.1.2.1.1.1
  - 1.3.6.1.2.1.1.5
  - 1.3.6.1.4.1.14685.3.1.11.1

Applicative-Anmeldeinformationen

Neben SNMP-Anmeldeinformationen sind zum Erkennen von DataPower-Anwendungsdomänen auch Applicative-Anmeldeinformationen erforderlich, auch als logische CIs bekannt.

Darüber hinaus werden SNMP- und Applicative-Anmeldeinformationen für die Top Down-Discovery von Anwendungsbeziehungen (entsprechende DataPower-Anwendungsdomäne) verwendet.

Benutzer mit Berechtigungen zum Ausführen von SOAP

Damit eine Top Down-Discovery für den DataPower-Webservice und die MQ-Verbindung ausgeführt werden kann, sind Berechtigungen zum Ausführen von SOAP-Abfragen erforderlich.

Von Discovery während der horizontalen Erkennung erfasste Daten

Standardmäßig verwendet Discovery zur Erkennung das Muster „DataPower Server“.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Tabelle und Feld	Beschreibung
DataPower-Hosting-Server [cmdb_ci_datapower_server]	
Modellnummer [model_number]	Das Modell des Servers, auf dem WebSphere DataPower gehostet wird
Hostname [host_name]	Der Hostname des Servers, auf dem WebSphere DataPower gehostet wird
Seriennummer [serial_number]	Die Seriennummer des Servers, auf dem WebSphere DataPower gehostet wird
IP-Adresse [cmdb_ci_ip_address]	
IP-Adresse [ip_address]	Die IP-Adresse des Servers, auf dem WebSphere DataPower gehostet wird
Netzmaske [netmask]	Die Netzmaske des Servers, auf dem WebSphere DataPower gehostet wird
Netzwerkadapter [cmdb_ci_network_adapter]	
MAC-Adresse [mac_address]	Die MAC-Adresse des Netzwerkadapters
Name [name]	Der Name des Netzwerkadapters

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

CI-Beziehungen

CI	Beziehung/Referenz	CI
DataPower-Hosting-Server [cmdb_ci_datapower_server]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	DataPower-Hosting-Server [cmdb_ci_datapower_server]

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Tabelle und Feld	Beschreibung
DataPower [cmdb_ci_app_server_datapower]	
Hostname [host_name]	Die Attribute der Anwendung DataPower
SOAP-URL [soap_url]	
Version [version]	
IP-Adresse [ip_address]	
Name [name]	
Domäne [domain]	

Erkennung von Cisco UCS-HD-Geräten (Unified Computing System)

Discovery identifiziert und klassifiziert Informationen über Cisco UCS-Geräte, einschließlich Gehäuse und Blades.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Apps im Store anfordern

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

Voraussetzungen

Anmeldeinformationen

Konfigurieren Sie sowohl SNMP-Anmeldeinformationen als auch Applicative-Anmeldeinformationen .

Klassifizierer, Muster und OIDs

Der Klassifizierer UCS verwendet HorzontalDiscoveryProbe, um das Muster UCS - HD zu starten. Der Klassifizierer verwendet auch die folgenden SNMP-OIDs, die die Tabelle „Cisco-UCS-Zubehör“ `[cmdb_ci_ucs_equipment]` angeben:

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

OID	Hersteller	Modell	Tabelle
1.3.6.1.4.1.9.12.3.1.3.847	Unified Computing Cisco UCS 6120XP 20-Port Fabric Interconnect	1.4(3u)(NX-OS) 5.0 Aggregation Switch	Cisco-UCS-Zubehör
1.3.6.1.4.1.9.12.3.1.3.899	Unified Computing Cisco UCS 6140XP 40-Port Fabric Interconnect	1.4(3u)(NX-OS) 5.0 Aggregation Switch	Cisco-UCS-Zubehör
1.3.6.1.4.1.9.12.3.1.3.1062	Unified Computing Cisco UCS 6248UP 48-Port Fabric Interconnect	2.0(1t)(NX-OS) 5.0.2 Aggregation Switch	Cisco-UCS-Zubehör
1.3.6.1.4.1.9.12.3.1.3.1063	Unified Computing Cisco UCS 6296UP 96-Port Fabric Interconnect	2.0(1t)(NX-OS) 5.0.2 Aggregation Switch	Cisco-UCS-Zubehör

Erfasste Daten

Es werden nur Geräte der B-Serie erkannt. Mit dem Muster „UCS - HD“ werden keine Geräte der C-, S- oder E-Serie erkannt. In der Tabelle „Cisco-UCS-Zubehör“ `[cmdb_ci_ucs_equipment]` werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
IP-Adresse	ip_address
Modell	model_id
Distinguished Name (DN)	dn
UCS-Manager-Version	version

In der Tabelle „Cisco-UCS-Gehäuse“ `[cmdb_ci_ucs_chassis]` werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
Modellnummer	model_number
Seriennummer	serial_number
Gehäuse-ID	chassis_id
Betriebsstatus	operational_status
Distinguished Name (DN)	dn

In der Tabelle „Cisco-UCS-Blade“ `[cmdb_ci_ucs_blade]` werden die folgenden Daten erfasst.

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

Bezeichnung	Feldname
Name	Name
Modellnummer	model_number
Seriennummer	serial_number
CPU-Anzahl	cpu_count
Anzahl CPU-Kerne	cpu_core_count
RAM	ram
Anzahl der Adapter	number_of_adapters
Gehäuse-ID	chassis_id
Steckplatz-ID	slot_id
Beschreibung	short_description
Distinguished Name (DN)	dn
Blatt-Seriennummer	Blade_serial_number
Betriebsstatus	operational_status

In der Tabelle „Cisco-UCS-Rackmount-Einheiten“ `[cmdb_ci_ucs_rack_unit]` werden die folgenden Daten erfasst.

Bezeichnung	Feldname
Name	Name
Lieferant	Lieferant
Server-ID	server_id
Verfügbarkeitsdiagramm	availability
UUID	uuid
Rack-Seriennummer	rack_serial
Anzahl an CPUs	num_of_cpus
Anzahl der Kerne	num_of_cores
Modell-ID	model_id
Speicher gesamt	total_memory
Distinguished Name (DN)	dn
Status	state

Beziehungen

Diese Beziehungen werden zur Unterstützung der UCS-HD-Discovery erstellt:

CI	Beziehung	CI
cmdb_ci_ucs_chassis	Enthält::Enthalten in	cmdb_ci_ucs_blade

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

CI	Beziehung	CI
cmdb_ci_ucs_equipment	Enthält::Enthalten in	cmdb_ci_ucs_rack_unit
cmdb_ci_ucs_equipment	Enthält::Enthalten in	cmdb_ci_ucs_chassis
cmdb_ci_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_ucs_blade

Erkennung von Dell Remote Assistant Cards

Die Dell™ Remote Assistant Card (DRAC) und die Integrated Remote Assistance Card (iDRAC) bieten Benutzern Tools und Funktionen zur Überwachung, Fehlerbehebung und Reparatur von Servern. Sie können DNS-URLs für den Zugriff auf Out-of-Band-Geräte generieren, wenn der Zugriff von IP-Adressen aus Sicherheitsgründen verhindert wird.

Zur Identifizierung von DRACs verwendet Discovery die Probe **SNMP - DRAC**. Diese Probe verwendet SNMPv1 und SMNPv2c. Für Out-of-Band-Geräte gibt es einen dedizierten Verwaltungskanal zur Gerätewartung. Systemadministratoren können Geräte mit dem dedizierten Managementkanal remote überwachen und verwalten. Dies schließt die Überwachung von Hardwaresensoren, den Zugriff auf lokale Medienlaufwerke und die Anpassung der BIOS-Einstellungen ein. Für Out-of-Band-Geräte können DNS-URLs generiert werden, um auf die Seite des Out-of-Band-Geräts zuzugreifen, wenn das SSL-Zertifikat die Navigation zur IP-Adresse verbietet.

Erfasste Daten

Von Discovery über Dell DRAC erfasste Daten

Bezeichnung	Tabelle	Name	Befehl
Firmware-Version	cmdb_ci_outofband_device	firmware_version	SNMP-Walk: drsFirmwareVersion (racFirmwareVersion für iDRAC7)
Host *	cmdb_ci_outofband_device	host	SNMP-Walk: drsSystemServiceTag (systemServiceTag für iDRAC7)
IP-Adresse	cmdb_ci_outofband_device	ip_address	DNS probe
Name	cmdb_ci_outofband_device	Name	SNMP Identity probe
Produktversion	cmdb_ci_outofband_device	product_version	SNMP-Walk: drsProductVersion (racVersion für iDRAC7)
Typ	cmdb_ci_outofband_device	Typ	SNMP-Walk: drsProductType (racType für iDRAC7)
URL	cmdb_ci_outofband_device	url	SNMP-Walk: drsProductURL (racURL für iDRAC7)

* **Host** verweist über die Seriennummer auf die Tabelle cmdb_ci_computer. Damit das Feld cmdb_ci_outofband_device.host ordnungsgemäß gefüllt wird, muss der Hostcomputer erkennbar oder in der CMDB mit der entsprechenden Seriennummer vorhanden sein.

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

Out-of-Band-Geräte

Eine **DNS-URL** wird für Konfigurationselemente in der Liste **Out-Of-Band-Gerät** generiert, wenn das Konfigurationselement einen **Namen** und eine **DNS-Domäne** besitzt. **DNS-URLs** können für Out-of-Band-Geräte generiert werden, um auf die Out-of-Band-Geräteseite zuzugreifen, wenn das SSL-Zertifikat die Navigation zur **IP-URL** verbietet. Die **DNS-URL** weist das Format `https://Name.DNS_Domain` auf. Wenn das Feld **Name** oder **DNS-Domäne** leer ist, enthält die **DNS-URL** den Wert im Feld **URL**.

Erkennung von HTTP-Geräten

Discovery kann Geräte erkennen, die das HTTP-Protokoll verwenden.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Klassifizierer, Probes und Muster

Die HTTP-Erkennung basiert auf der Port-Probe *HTTP*, den Discovery nach dem Versuch ausführt, Probes für SSH- und SNMP-Ports auszuführen. Diese Port-Probe startet die Probe *HTTP - Classify*, der eine HTTP GET-Anforderung für jeden Eintrag in der HTTP-Klassifizierungstabelle ausführt. Sie sollten Ihre eigenen Klassifizierungen konfigurieren, auf die die Probe *HTTP - Classify* zugreifen kann.

Die Port-Probe „HTTP“ verwendet Zuordnungen zwischen einem Protokoll und einer Portnummer in der Tabelle „IP-Service“ [cmdb_ip_service]. In dieser Tabelle können Sie zusätzliche Port-zu-Protokoll-Definitionen hinzufügen oder das für einen bestimmten HTTP-Klassifizierer verwendete Protokoll überschreiben.

Klassifizierung	Probes	Muster
	HTTP (Port-Probe): Diese Probe startet die Probe „HTTP - Classify“, die eine HTTP GET-Anforderung für jeden Eintrag in der HTTP-Klassifizierungstabelle ausführt.	

Erkennung über einen HTTP- oder HTTPS REST-Aufruf ausführen

Discovery kann Geräte klassifizieren, die das HTTP(S)-Protokoll nutzen. Anstatt SNMP- oder SSH-Anmeldeinformationen zu verwenden, können Sie Ihren eigenen HTTP-Klassifizierer erstellen, um Geräte zu erkennen und mit Anmeldeinformationen der Standardauthentifizierung darauf zuzugreifen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

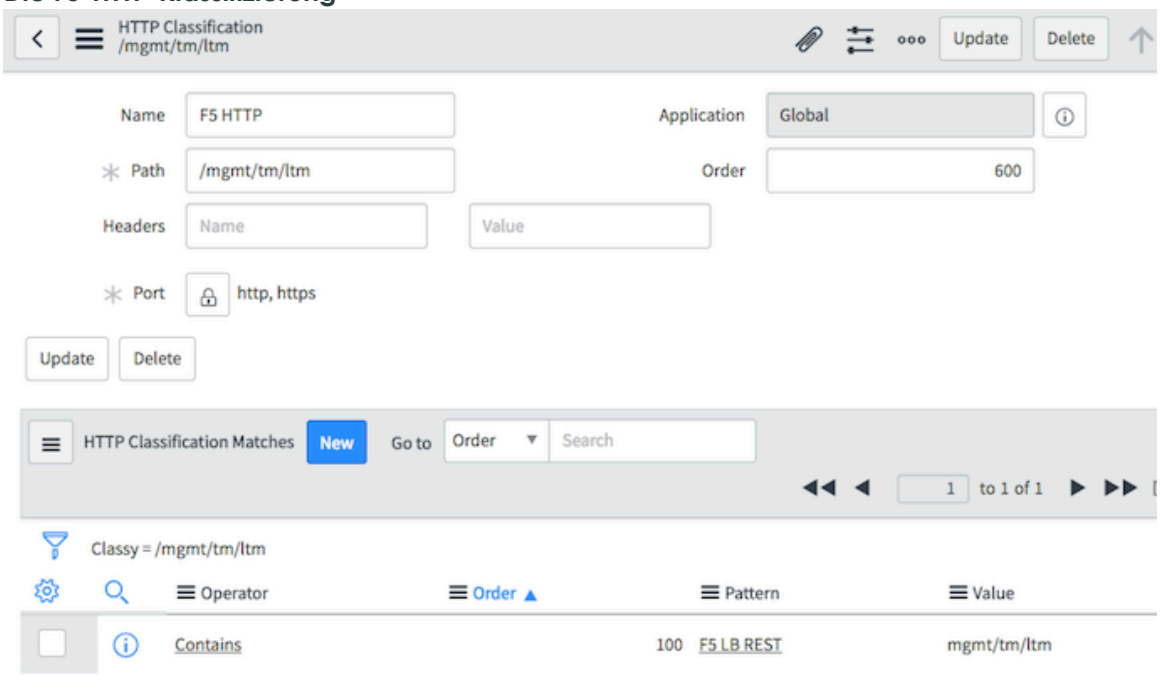
Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **Basisanmeldedaten**.
   In den meisten Fällen können Sie über einen HTTP- oder HTTPS REST-Aufruf mit Standardauthentifizierungsinformationen auf ein Gerät zugreifen.
4. Fügen Sie den Benutzernamen und das Passwort hinzu, die Sie für den Zugriff auf das Gerät benötigen.
5. Klicken Sie auf **Absenden**.

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

6. Richten Sie eine HTTP-Klassifizierung ein, indem Sie zu navigieren **Discovery-Definition** > **CI-Klassifizierung** > **HTTP**.
7. Klicken Sie auf **Neu**.
8. Füllen Sie die Formularfelder aus (siehe Tabelle):

Die F5-HTTP-Klassifizierung



Feld	Beschreibung
Name	Geben Sie einen Namen für den Klassifizierer ein.
Pfad	Geben Sie den Pfad für die HTTP-GET-Anforderung ein.
Header	Fügen Sie einen Optionsheader mit einem Wert hinzu. Sie können eine Variable im Format `${variable}` anstatt eines statischen Wertes verwenden. Die unterstützten Header hängen vom REST-Webservice-Provider ab, zu dem Sie eine Verbindung herstellen möchten. In der Dokumentation Ihres Web Service Providers erfahren Sie, welche Header gültig oder erforderlich sind.
Port (IP-Dienst)	Wenn Sie möchten, dass dieser Klassifizierer einen benutzerdefinierten Port verwendet, der nicht bereits ein Standardwert in der Tabelle IP-Dienst [cmdb_ip_service] ist, führen Sie folgende Schritte aus: **a.** Wählen Sie das Suchsymbol, um die Liste der IP-Services anzuzeigen. **b.** Wählen Sie **Neu** aus und erstellen Sie eine Port-zu-Protokoll-Zuordnung. **c.** Wählen Sie diese Port-zu-Protokoll-Zuordnung dafür im Feld **Port**.

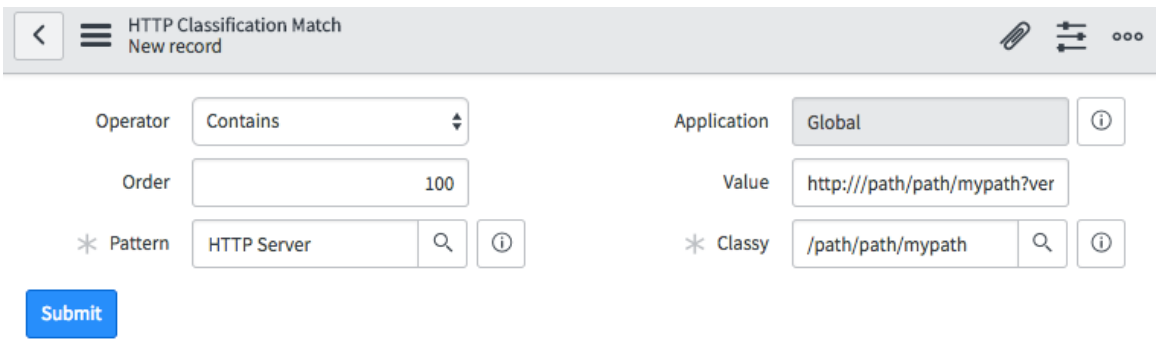
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Feld	Beschreibung
	Viele häufig verwendete Protokolle sind standardmäßig bereits Ports zugeordnet, z. B. `http` zu Port 80 und `https` zu Port 443. Wenn Sie eine dieser standardmäßigen Port-zu-Protokoll-Zuordnungen verwenden möchten, geben Sie keine Werte in das Feld **Port** ein. Die HTTP-Port-Sonde verwendet standardmäßig den richtigen Port.
Reihenfolge	Geben Sie eine Zahl ein, die die Priorität dieses Klassifizierers darstellt. Wenn Discovery mehr als einen zutreffenden Klassifizierer verwendet, wird der Klassifizierer mit niedriger **Rang-**Nummer verwendet.
Protokoll [optional] Dieses Feld ist standardmäßig nicht sichtbar. Sie müssen das Formular konfigurieren, um es hinzuzufügen.	Wenn Sie eine eindeutige Port-zu-Protokoll-Zuordnung für das Fel **Port** konfigurieren, geben Sie in das Feld eine optionale Protokollüberschreibung ein, die Discovery mit diesem Klassifizierer verwendet. Wenn Sie beispielsweise Port 5000 und das HTTP-Protokoll verwenden möchten, fügen Sie die 5000/HTTP-Port-zu-Protokoll-Zuordnung zum Feld **Port** hinzu, und wählen Sie dann **http** im Feld **Protokoll**.

9. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**. Die zugehörige Liste „Übereinstimmung der HTTP-Klassifizierung“ wird angezeigt. Diese zugehörige Liste enthält Kriterien, die Sie für den Abgleich mit dem Hauptteil der Antwort auf die von Discovery gesendete GET-Anforderung konfigurieren können.
10. Definieren Sie in der zugehörigen Liste „Übereinstimmung der HTTP-Klassifizierung“ die Abgleichskriterien, und geben Sie das für diesen Klassifizierer zu startende Muster an:

    a. Klicken Sie auf **Neu**.

    b. Füllen Sie die Felder des Formulars „Übereinstimmung der HTTP-Klassifizierung“ aus (siehe Tabelle).



Feld	Beschreibung
Operator	Wählen Sie den Operator aus, mit dem das System die Bedingung bewertet:

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

Feld	Beschreibung
	▪ **Enthält** ▪ **Ist gleich** ▪ **Regulärer Ausdruck**
Reihenfolge	Geben Sie eine Zahl ein, die die Priorität dieser Bedingung darstellt. Wenn Discovery mehr als eine zutreffende Bedingung findet, wird die Bedingung mit niedriger Rang-Nummer verwendet.
Muster	Geben Sie das Muster an, das nach einer korrekten Übereinstimmung gestartet werden soll. Dieses Muster muss HTTP verwenden, um das Gerät zu ermitteln.
Wert	Geben Sie den Wert ein, den der Rumpf der zurückgegebenen REST-Methode haben muss.

c. Klicken Sie auf **Absenden**.

d. Definieren Sie so viele Übereinstimmungen der HTTP-Klassifizierung wie erforderlich. Das ist hilfreich, wenn für die verschiedenen Versionen des zu erkennenden Geräts verschiedene Muster vorhanden sind.

Example:
In diesem Beispiel ist die HTTP-Klassifizierung für die Verwendung der API des F5-Lastenausgleichsmoduls konfiguriert:

Nächste Maßnahme
Wenn Sie keine andere Arten von Anmeldeinformationen haben, die Geräte erkennen können, zum Beispiel Linux-Anmeldeinformationen oder SNMP-Anmeldeinformationen, können Sie sehen, wie die Discovery-Anwendung die HTTP-Erkennung verarbeitet:

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne** und führen Sie eine Discovery aus.
2. Überprüfen Sie nach Abschluss des Discovery-Prozesses die ECC-Warteschlange, um die Ergebnisse der HTTP-Erkennung anzuzeigen.

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

Sie sollten sehen, dass die Klassifizierungs-Probes „Unix“ und „SNMP“ fehlgeschlagen sind, nachdem die Shazzam-Probe gestartet wurde. Es sollte sowohl die Probe „HTTP - Classify“ als auch das Muster gestartet werden, die Sie im HTTP-Klassifizierungsdatensatz angeben.

Topic	Name	Source	Queue
Multiprobe	Unix - Classify	10.196.39.128	input
Multiprobe	Unix - Classify	10.196.39.128	output
SNMP	SNMP - Classify	10.196.39.128	output
SNMP	SNMP - Classify 108 OIDs	10.196.39.128	input
HTTPClassyProbe	HTTPClassyProbe	10.196.39.128	input
HTTPClassyProbe	HTTPClassyProbe	10.196.39.128	output
Shazzam	wmi,snmp,ssh,wins,dns,slp,wbem,vmapp,win..	See Payload	input
Shazzam	wmi,snmp,ssh,wins,dns,slp,wbem,vmapp,win..	See Payload	output

Erkennung von Speicher

Discovery sammelt Informationen zu Direct Attached Storage (DAS), Storage Area Networks (SAN) und Network Attached Storage (NAS).

Speicher kann auf speziellen Geräten wie Speicher-Arrays, Fibre Channel-Switches, iSCSI-Datenträgern oder auf Host-Betriebssystemen wie Windows, Linuxund Solarisliegen.

Discovery erkennt Abhängigkeiten für die folgenden Speichertypen und ordnet sie zu:

- Direct Attached Storage (DAS), Network Attached Storage (NAS), Storage Area Network (SAN)
- NAS- oder SAN-Speicher, der über Storage Management Initiative Specification (SMI-S) und ein Common Information Model (CIM) erkannt wird
- Virtueller Speicher für VMware ESX-Server und Linux Kernel-basierte virtuelle Maschinen (KVM). Discovery ordnet diesen Speicher dem zugrunde liegenden physischen Speicher zu.

Durch die Erkennung von Speicher über einen Host werden Daten abgeglichen und Beziehungen zwischen den Dateisystemen des Hosts und zugehörigen lokalen Speichergeräten erstellt. Die lokalen Speichergeräte stellen den für den Host verfügbaren Speicher dar, und zwar unabhängig davon, ob er direkt angeschlossen ist oder über Fibre Channel oder iSCSI bereitgestellt wird. Bei diesem Abgleich wird davon ausgegangen, dass der Speicherserver bereits erkannt wurde.

Hinweis: Treiber für Bandspeicher werden nicht erkannt.

Discovery sammelt und erstellt CIs in CMDB für die folgenden Informationen:

- Dateisysteme (lokal und NAS)
- Datenträger (sowohl SAN-Datenträger als auch DAS-Laufwerke)
- FC-HBAs und -Ports (Fibre Channel)

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

- Linux Volume Manager-Volumes (LVM). LVM-Volumedaten befinden sich in der Tabelle „Speicherpool“ [cmdb_ci_storage_pool].
- Veritas Volume Manager-Datenträger, -Teildatenträger, -Datenträgergruppen, -Plexe und -Volumes

Hinweis: Weitere Informationen zur Erkennung von auf einem Linux-Host bereitgestelltem Direct Attached Storage oder Multipath Block Storage finden Sie unter KB0622583 .

Probes, Sensoren und Muster

- KVM - Storage Pools: Identifiziert Speicher, der an virtuelle KVM-Computer angeschlossen ist
- Linux – Speicher: Identifiziert Speicher, der an Systeme angehängt ist, auf denen das Betriebssystem Linux ausgeführt wird.
- Solaris – Speicher: Identifiziert Speicher, der an Systeme angehängt ist, auf denen das Betriebssystem Solaris ausgeführt wird.
- Windows – Speicher 2008: Identifiziert Speicher, der an Systeme mit Windows 2008 angehängt ist.
  - Windows – Speicher 2008 – PS: identifiziert Speicher, der an Systeme mit Windows 2008 angehängt ist, mithilfe von PowerShell.
  - Windows – Speicher 2008 – WMI: identifiziert Speicher, der an Systeme mit Windows 2008 angehängt ist, mithilfe von WMI Runner.
- Windows – Speicher 2012: Identifiziert Speicher, der an Systeme mit Windows 2012 und höher angehängt ist.
  - Windows – Speicher 2012 – PS: identifiziert Speicher, der an Windows -Systeme angehängt ist, mithilfe von PowerShell.
  - Windows – Speicher 2012 – WMI: Identifiziert Speicher, der an Windows -Systeme angehängt ist, mithilfe von WMI Runner.
- VMWare - vCenter ESX Hosts Storage: Erfasst Informationen über ESX-Server und erstellt Beziehungen von Datenspeichern zu zugrunde liegenden Datenträgern
- Muster zur Erkennung von NetApp-Speicher:
  - NetApp 7-Modus: Erkennt NetApp-Server über REST mit zwei Knoten
  - NetApp-Cluster-Modus: Erkennt NetApp Server über REST, wenn mehr als zwei Knoten über einen Cluster Interconnect Switch verbunden sind

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Anforderungen

Windows

- Unterstützt die folgenden Konfigurationen:
  - Windows Server 2012, DAS oder NAS mit Fibre Channel (FC) oder Internet Small Computer System Interface (iSCSI).
  - Windows Server 2008, DAS oder NAS mit FC oder iSCSI.
- Installieren Sie das Tool „`fcinfo.exe`“ auf Servern Windows 2008 und 2012, die über FC an den Speicher angehängt sind.
- Installieren Sie Windows Management Instrumentation (WMI).

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

- Aktivieren Sie PowerShell auf dem Hostserver MID-Server.
- Stellen Sie der Instanz die erforderlichen Anmeldeinformationen für den Hostserver bereit.
- Platzieren Sie den Computer MID-Server und den Zielcomputer in derselben Domäne, oder fügen Sie den Zielcomputer der Liste der vertrauenswürdigen Hosts auf dem Computer MID-Server hinzu.
- Installieren Sie auf dem Hostserver optional Windows Remote Management (WinRM) , um Fibre Channel-Informationen zu erkennen. WinRM ist für Windows 2012- und Windows 2016-Computer standardmäßig aktiviert, nicht jedoch für Windows 2008-Computer.

Linux

- Unterstützt die folgenden Konfigurationen:
  - Solaris, DAS, NAS oder SAN mit iSCSI
  - CentOS, DAS, NAS oder SAN mit FC oder iSCSI
  - Ubuntu Server, DAS, NAS oder SAN mit iSCSI
- Stellen Sie dem Gerät SSH-Anmeldeinformationen mit Root- oder Sudo-Zugriff bereit.
- Stellen Sie MID-Server die erforderlichen Anmeldeinformationen für den Hostserver zur Verfügung.

Beziehungen

Discovery erstellt für Speicher-CIs die folgenden Beziehungen:

Übergeordnete Komponente	Beziehung	Untergeordnete Komponente
Speicherexport [cmdb_ci_storage_export]	Exportieren nach::Importieren von	Speichergerät [cmdb_ci_storage_device]
Fibre Channel-Datenträger [cmdb_ci_fc_disk]	Stellt bereit::Bereitgestellt von	Dateisystem [cmdb_ci_file_system]
iSCSI-Datenträger [cmdb_ci_iscsi_disk]	Stellt bereit::Bereitgestellt von	Dateisystem [cmdb_ci_file_system]

Erkennung von Hosts mit angeschlossenem Speicher konfigurieren

Discovery kann Informationen über UNIX-, Linux- und Windows-Hosts mit angeschlossenem Speicher erkennen.

Discovery für die Erkennung von UNIX- oder Linux-Hosts mit angeschlossenem Speicher konfigurieren

Discovery kann Informationen über einen UNIX- oder Linux-Host und angeschlossenen Speicher erkennen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

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

Prozedur

1. Wahlweise: Weisen Sie dem Konto, das von Discovery verwendet wird, auf dem Host erweiterte Berechtigungen zu.
2. Fügen Sie in der Instanz ServiceNowdie Anmeldeinformationen der Tabelle Discovery Anmeldeinformationen hinzu.
3. Erstellen Sie einen Discovery-Zeitplan für jede Host-IP-Adresse.
4. Wahlweise: Erstellen Sie ein Verhalten, das eine Funktionalitätsdefinition mit einer wbem-Port-Probe verwendet, um die anfängliche Port-Scanphase (Shazzam) effizienter zu gestalten.
5. Führen Sie eine Netzwerkerkennung aus.

> **Hinweis:** Wenn der Host auch eine Verbindung zu einem NAS- oder SAN-Speicher-Array herstellt, richten Sie den SMI-S-Provider und CIM-Anmeldeinformationen ein.

Discovery für die Erkennung von Windows-Hosts mit angeschlossenem Speicher konfigurieren

Discovery kann Informationen über einen Windows-Hosts und angeschlossenen Speicher erkennen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Führen Sie die folgenden Schritte aus, wenn Sie die Windows 2008-Server verwenden, die an einen Speicher angehängt sind:
   a. Laden Sie das Microsoft Fibre Channel-Informationstool von http://www.microsoft.com herunter, installieren Sie es, und suchen Sie auf der Website nach dem Microsoft Fibre Channel-Informationstool.
   b. Legen Sie den Umgebungspfad für die ausführbare Datei `fcinfo.exe` fest, und führen Sie sie aus.

   > **Hinweis:** Bei Servern mit neueren Betriebssystemen ist eine ähnliche Funktionalität für das Betriebssystem vorhanden. Dieser Schritt ist nicht erforderlich.

2. Für alle Windows-Hosts einschließlich Windows 2008 fügen Sie der Tabelle DiscoveryAnmeldeinformationen Windows- Anmeldeinformationen hinzu.
3. Erstellen Sie in der ServiceNow-Instanz einen Discovery-Zeitplan für jede Host-IP-Adresse.
4. Wahlweise: Erstellen Sie ein Verhalten, das eine Funktionalitätsdefinition mit einer wbem-Port-Probe verwendet, um die anfängliche Port-Scanphase (Shazzam) effizienter zu gestalten.
5. Führen Sie eine Netzwerkerkennung aus.

> **Hinweis:** Wenn der Host auch eine Verbindung zu einem NAS- oder SAN-Speicher-Array herstellt, richten Sie den SMI-S-Provider und CIM-Anmeldeinformationen ein.

Für Speicher über einen Host erfasste Erkennungsdaten

Discovery erfasst Informationen über Speichereinheiten, die über einen lokalen E/A-Port oder Hostbusadapter (HBA) mit Linux-, Solaris- und Windows-Hosts verbunden sind.

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

Probes, die zum Erkennen von Speicher von einem Host aus verwendet werden

Tabelle	Probes
Datenträger [cmdb_ci_disk]	• KVM • Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Datenträgerpartition [cmdb_ci_disk_partition]	• KVM • Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Fibre Channel-Datenträger [cmdb_ci_fc_disk]	• Linux - Storage • Solaris - Storage • Windows - Storage 2008
Fibre-Channel-Port [cmdb_ci_fc_port]	• Linux - Storage • Solaris - Storage • Windows - Storage 2008
Dateisystem [cmdb_ci_file_system]	• KVM • Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
iSCSI-Datenträger [cmdb_ci_iscsi_disk]	• KVM • Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
NAS-Dateisystem [cmdb_ci_nas_file_system]	• KVM • Linux - Storage • Solaris - Storage

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

Tabelle	Probes
	• Windows - Storage 2008 • Windows - Storage 2012
Speicher-HBA [cmdb_ci_storage_hba]	• Linux - Storage • Solaris - Storage • Windows - Storage 2008
Speicherpool [cmdb_ci_storage_pool]	Linux - Storage
Speicherpoolmitglied [cmdb_ci_storage_pool_member]	Linux - Storage
VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	VMware - vCenter Datastores

Erkannte Speicherreferenzen

Discovery ordnet diese Referenzen für Speichereinheiten zu, die über einen lokalen E/A-Port oder Hostbusadapter (HBA) mit einem Host verbunden sind.

Tabelle und Spalte	Referenz	Zieldatenelement
cmdb_ci_storage_device.computer	referenziert	cmdb_ci_computer
cmdb_ci_storage_device.provided_by	referenziert	cmdb_ci_fc_port (nur für FC)
cmdb_ci_disk_partition.disk	ist eine Partition von	cmdb_ci_disk
cmdb_ci_storage_hba.computer	ist	cmdb_ci_computer
cmdb_ci_fc_port.controller	enthält	cmdb_ci_storage_hba
cmdb_ci_fc_port.computer	ist identisch mit	cmdb_ci_computer wie cmdb_ci_storage_hba.computer
cmdb_ci_storage_volume.computer	ist	cmdb_ci_computer
cmdb_ci_storage_volume.provided_by	ist	cmdb_ci_storage_pool oder cmdb_ci_storage_pool oder cmdb_ci_storage_device (bereitstellender Speicher)
cmdb_ci_storage_pool.hosted_by	ist	cmdb_ci_computer
cmdb_ci_computer	Pool befindet sich in	cmdb_ci_storage_pool.container
cmdb_ci_storage_pool.container	ist	cmdb_ci_storage_pool oder cmdb_ci_storage_pool_member, die Pool enthalten (wenn Pool vorhanden)
cmdb_ci_storage_pool_member.pool	ist	cmdb_ci_storage_pool

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

Tabelle und Spalte	Referenz	Zieldatenelement
cmdb_ci_storge_pool_member.storage	ist	cmdb_ci_storage_pool, cmdb_ci_disk_partition oder cmdb_ci_storage_device (bereitstellender Speicher)

Für HBAs auf Linux- und ESX-Servern erfasste Daten

Discovery erfasst Informationen über Hostbusadapter (HBA) für Fibre Channel-fähige Geräte, die mit Linux- und ESX-Servern verbunden sind.

HBA-Tabellen und -Felder

Bezeichnung	Tabelle	Feldname	Quelle
Name	Speicher-HBA [cmdb_ci_storage_hba]	Name	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
WWNN	Speicher-HBA [cmdb_ci_storage_hba]	wwnn	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Modell-ID	Speicher-HBA [cmdb_ci_storage_hba]	model_id	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Computer	Speicher-HBA [cmdb_ci_storage_hba]	Computer	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage

Fibre Channel-Ports

Bezeichnung	Tabelle	Feldname	Quelle
WWPN	Fibre-Channel-Port [cmdb_ci_fc_port]	wwpn	VMWare - vCenter ESX Hosts Storage • probe • Linux - Storage
WWNN	Fibre-Channel-Port [cmdb_ci_fc_port]	wwnn	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage

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

Fibre Channel-Ports (Fortsetzung)

Bezeichnung	Tabelle	Feldname	Quelle
Porttyp	Fibre-Channel-Port [cmdb_ci_fc_port]	port_type	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Geschwindigkeit	Fibre-Channel-Port [cmdb_ci_fc_port]	speed	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Controller	Fibre-Channel-Port [cmdb_ci_fc_port]	controller	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage
Computer	Fibre-Channel-Port [cmdb_ci_fc_port]	Computer	• Probe „VMWare - vCenter ESX Hosts Storage“ • Linux - Storage

Fibre Channel-Ziele

Bezeichnung	Tabelle	Feldname	Quelle
FC-Datenträger	Fibre Channel-Ziele [cmdb_fc_target]	fc_disk	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Erstellt von	Fibre Channel-Ziele [cmdb_fc_target]	sys_created_by	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Erstellt	Fibre Channel-Ziele [cmdb_fc_target]	sys_created_on	• Linux - Storage • Solaris - Storage

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

Fibre Channel-Ziele (Fortsetzung)

Bezeichnung	Tabelle	Feldname	Quelle
			• Windows - Storage 2008 • Windows - Storage 2012
SysID	Fibre Channel-Ziele [cmdb_fc_target]	sys_id	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Updates	Fibre Channel-Ziele [cmdb_fc_target]	sys_mod_count	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Aktualisiert von	Fibre Channel-Ziele [cmdb_fc_target]	sys_updated_by	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
Aktualisiert	Fibre Channel-Ziele [cmdb_fc_target]	sys_updated_on	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012
WWNN	Fibre Channel-Ziele [cmdb_fc_target]	wwnn	• Linux - Storage • Solaris - Storage

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

Fibre Channel-Ziele (Fortsetzung)

Bezeichnung	Tabelle	Feldname	Quelle
			• Windows - Storage 2008 • Windows - Storage 2012
WWPN	Fibre Channel-Ziele [cmdb_fc_target]	wwpn	• Linux - Storage • Solaris - Storage • Windows - Storage 2008 • Windows - Storage 2012

Für HBAs auf Solaris-Servern erfasste Daten

Discovery unter Solaris unterstützt HBAs von:

- Emulex
- QLogic

In der Tabelle „Speicher-HBA“ [cmdb_ci_storage_hba] füllt Discovery mithilfe der Probe „Solaris - Storage“ und des zugehörigen Sensors die folgenden Felder.

Bezeichnung	Feldname
Name	Name
Computer	Computer
Geräte-ID	device_id
Hersteller	manufacturer
Modell-ID	model_id
Seriennummer	serial_number

In der Tabelle „Fibre Channel-Port“ [cmdb_ci_fc_port] füllt Discovery die folgenden Felder.

Bezeichnung	Feldname
Name	Name
Computer	Computer
Controller	controller
WWPN	wwpn
WWNN	wwnn
Porttyp	port_type

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

Bezeichnung	Feldname
Geschwindigkeit	speed
Betriebsstatus	operational_status

In der Tabelle „Fibre Channel-Datenträger“ [cmdb_ci_fc_disk] füllt Discovery die folgenden Felder.

Bezeichnung	Name
Name	Name
Speichertyp	storage_type
Geräteschnittstelle	device_interface
Geräte-LUN	device_lun

In der Tabelle „Fibre Channel-Ziele“ [cmdb_ci_fc_port] füllt Discovery die folgenden Felder.

Bezeichnung	Name
FC-Datenträger	fc_disk
WWNN	wwnn
WWPN	wwpn

Für HBAs auf Windows-Servern erfasste Daten

Unter Windows unterstützt Discovery unter beliebigen Betriebssystemen ausgeführte HBAs.

HBA-Tabellen und -Felder

Bezeichnung	Tabelle	Feldname	Quelle
Name	Speicher-HBA [cmdb_ci_storage_hba]	Name	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
WWNN	Speicher-HBA [cmdb_ci_storage_hba]	wwnn	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
Modell-ID	Speicher-HBA [cmdb_ci_storage_hba]	model_id	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012

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

HBA-Tabellen und -Felder (Fortsetzung)

Bezeichnung	Tabelle	Feldname	Quelle
Computer	Speicher-HBA [cmdb_ci_storage_hba]	Computer	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012

Fibre Channel-Ports

Bezeichnung	Tabelle	Feldname	Quelle
WWPN	Fibre-Channel-Port [cmdb_ci_fc_port]	wwpn	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
WWNN	Fibre-Channel-Port [cmdb_ci_fc_port]	wwnn	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
Porttyp	Fibre-Channel-Port [cmdb_ci_fc_port]	port_type	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
Geschwindigkeit	Fibre-Channel-Port [cmdb_ci_fc_port]	speed	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012
Controller	Fibre-Channel-Port [cmdb_ci_fc_port]	controller	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012

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

Fibre Channel-Ports (Fortsetzung)

Bezeichnung	Tabelle	Feldname	Quelle
Computer	Fibre-Channel-Port [cmdb_ci_fc_port]	Computer	• Probe „VMWare - vCenter ESX Hosts Storage“ • Windows - Storage 2008 • Windows - Storage 2012

Speichererkennung über SMI-S und CIM

Discovery kann Speichergeräte untersuchen, die einen SMI-S Provider (Storage Management Initiative Specification), einen speziellen CIM-Server (Common Information Model), enthalten.

Die aktuelle Liste der Lieferanten und Produkte, die von SNIA auf SMI-S-Konformität getestet wurden, finden Sie auf der SNIA-Website .

Für andere Speichertypen, zum Beispiel über einen Host angeschlossenen Speicher, auf VMware ESX-Servern verfügbaren VM-Speicher und Speicher für Kernel-VM (KVM), werden separate Probes und Sensoren verwendet.

Discovery erfasst Informationen über SAN (Storage Area Network) und NAS (Network Attached Storage) von spezialisierten Geräten wie Speicher-Arrays und FC-Switches (Fibre Channel). Discovery erfasst und erstellt CIs in der CMDB für die folgenden Informationen:

- Array-Datenträger, Pools und Volumes
- Fibre Channel-HBAs, -Ports und -Controller
- FC-Exporte
- Fabrics, einschließlich Endpunkte, Zoning und Switches
- Abhängigkeiten zwischen untergeordneten Speicherkomponenten

Hinweis: Weitere Informationen zur Speichererkennung und zur Verwendung des Abfragetools CIM zur Problembehandlung können Sie Wissensartikel KB0782305 entnehmen.

Anforderungen

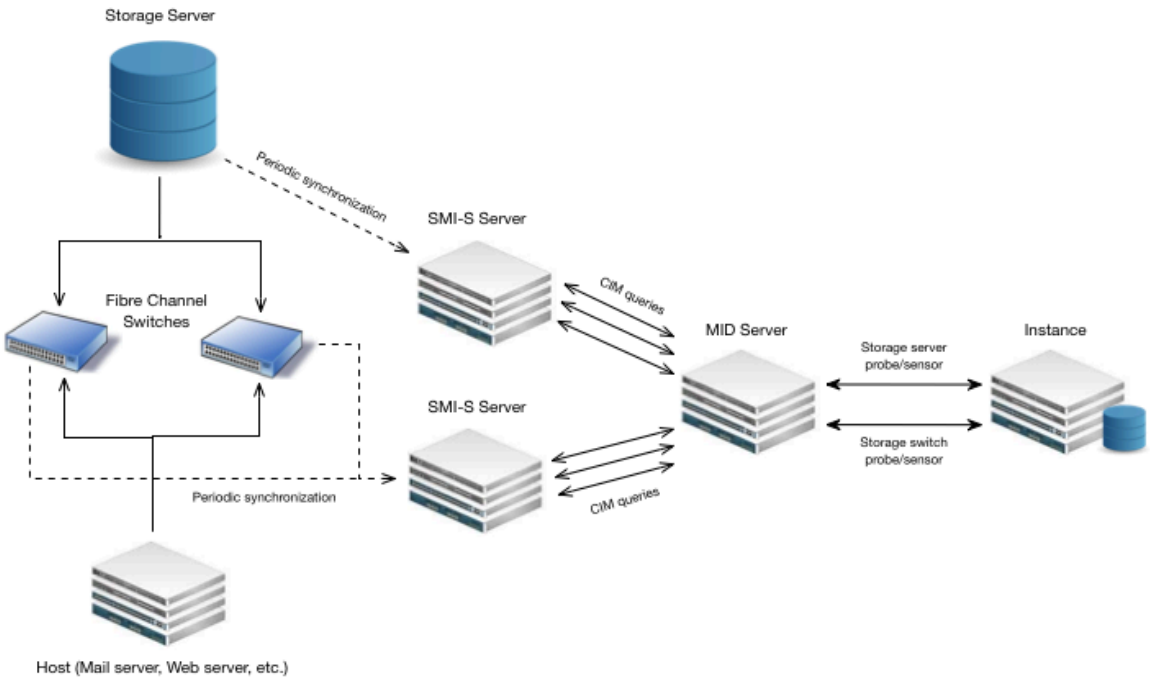
- Ein CIM-Server mit SMI-S 1.4 oder höher
- Mindestens ein CIM-Server pro Speicheranbieter
- NAS- und SAN-Systeme großer Anbieter wie EMC, Hitachi, HP und NetApp. SAN-Speichergeräte müssen FC verwenden.
- FC-Switches großer Anbieter wie Brocade und Cisco
- Die CIM-Anmeldeinformationen müssen für die SMI-S-Konfiguration verfügbar sein. Die CIM-Anmeldeinformationen können sich von den Anmeldeinformationen für das System unterscheiden, auf dem der CIM-Server gehostet wird.
- Stellen Sie sicher, dass SMI-S für Ihr Speicherprodukt aktiviert ist.

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

- Stellen Sie sicher, dass eine Verbindung zwischen dem MID Server und dem CIM-Server besteht.
- Neue CIM-Anmeldeinformationen müssen in der Instanz konfiguriert werden. Die Anmeldeinformationen für den CIM-Server können von denen für das System abweichen, auf dem der erforderliche CIM-Server gehostet wird.

Hinweis: Da der SMI-S Provider Informationen über Speichergeräte zwischenspeichert, hat die Discovery-Abfrage an den Provider keine Auswirkungen auf die Leistung der Speichergeräte.

SMI-S Discovery-Architektur



CIM-Architektur

CIM-Probes können jedes Gerät basierend auf dem Common Information Model (CIM) erkennen, indem sie einen CIM-Server abfragen, der auch als CIMOM (Common Information Model Object Manager) bezeichnet wird. Standardmäßig verwendet Discovery CIM-Probes zum Untersuchen von Speichersystemen sowie zum Abrufen der Seriennummern von ESX-Servern.

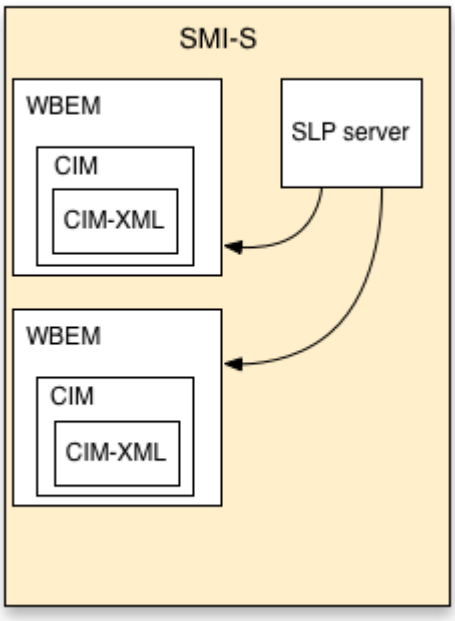
Discovery fragt SMI-S-konforme Speichergeräte mithilfe von CIMIQL-Abfragen ab.

Die folgenden Komponenten sind Teil von CIM:

- Common Information Model (CIM): Mit CIM können mehrere Parteien Informationen über verwaltete Elemente austauschen. CIM stellt diese verwalteten Elemente und die Verwaltungsinformationen dar und stellt gleichzeitig den Mechanismus zur aktiven Steuerung und Verwaltung der Elemente bereit.
- Storage Management Initiative Specification (SMI-S): SMI-S ist ein Nutzungsstandard, der Methoden für die Speichererkennung auf Anbieterseite beschreibt. ServiceNow verwendet SMI-S, um zu bestimmen, wie CIM erkannt wird. SMI-S basiert auf den Standards Common Information Model (CIM) und Web-Based Enterprise Management (WBEM), die Verwaltungsfunktionen über HTTP definieren. Das Hauptziel von SMI-S besteht darin, die Verwaltung unterschiedlicher Speicherprodukte zu ermöglichen. ServiceNow unterstützt SMI-S Version 1.4 oder höher.

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

CIM SMI-S-Standard – Diagramm



- Web-Based Enterprise Management (WBEM): WBEM definiert eine bestimmte Implementierung von CIM, einschließlich Protokollen zum Erkennen und Zugreifen auf CIM-Implementierungen.
- Service Location Protocol (SLP): SLP ist ein Ad-hoc-Protokoll zum Abrufen und Zuordnen von Konfigurationsinformationen über CIM-Server, zum Beispiel Standardpfade, Fähigkeiten und der genaue Interop-Namespace. Discovery ruft den Interop-Namespace von CIM-Servern über SLP ab und übergibt diese Informationen an die Probe „CIM Classify“. SLP, hier als SLP-Server bezeichnet, verwendet Service Agents (SA), um Informationen zu einem CIM-Server in einem Subnetz zu sammeln und zu verbreiten. Ein Subnetz kann über mehrere Service Agents verfügen.

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

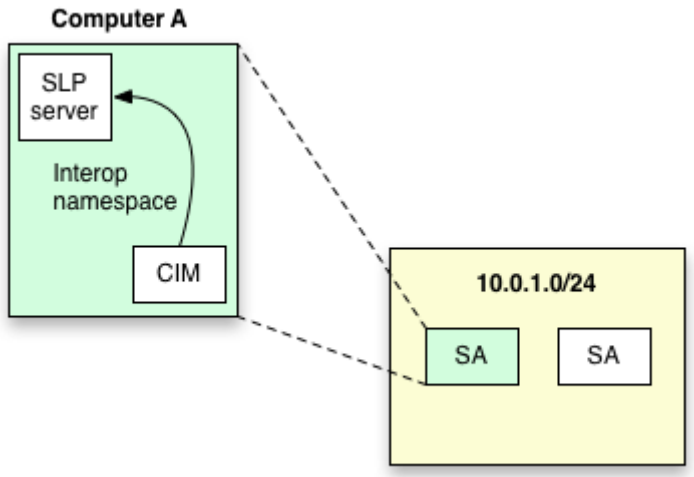
Hinweis:

Die Systemeigenschaft *mid.cim.interop.namespace* vier Standardspeicher-Namespaces:

- interop
- root/interop
- root/pg_interop
- pg_interop

Wenn Sie mehrere Speicheranbieter verwenden, für die anwenderdefinierte Namespaces nicht als Standard angegeben sind, fügen Sie die neuen Namespaces der durch Kommas getrennten Liste in dieser Eigenschaft hinzu. Wenn Sie einen der Standard-Namespaces weiterhin verwenden möchten, müssen Sie diese in die Eigenschaft aufnehmen.

CIM-Agent – Diagramm



SLP- und WBEM-Unterstützung

SLP ist für CIM Discovery erforderlich, da es Teil des SMI-S-Stapels (Storage Management Initiative Specification) ist. Einige Speichergeräte unterstützen womöglich das WBEM-Protokoll, aber SLP nicht.

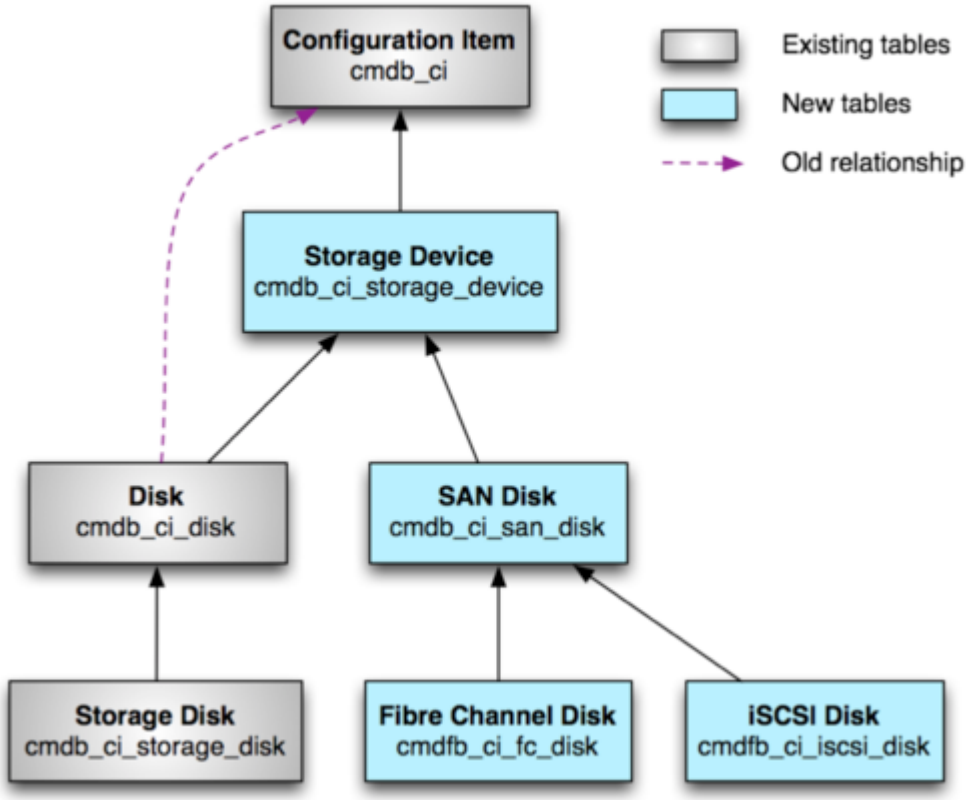
Sie können die WBEM-Services mit einem gängigen Linux-Tool wie *slptool* manuell für SLP registrieren. Dieses Tool stellt eine Befehlszeilenschnittstelle bereit, mit der Sie SLPv2-UA-Anforderungen (User Agent) erstellen können, die normalerweise zum Lieferumfang des SLP-Daemon-Pakets gehören. Zum Registrieren eines Service geben Sie eine URL und eine Liste von Attributen an. Beispiele können mit demselben Tool von einem funktionierenden SLP-Server extrahiert werden.

Tabellenschema für Speichererkennung

In folgendem Diagramm ist das hierarchische Datenträgerschema für die Speichererkennung dargestellt.

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

Hierarchisches Datenträgerschema



Tabellen und Probes zur Speichererkennung

Discovery verwendet die folgenden Tabellen und Probes, um Informationen über Speichergeräte zu erfassen, die von einem SMI-S Provider verwaltet werden.

Erfasste Daten

Tabelle	Probe
Datenträger [cmdb_ci_disk]	SMI 1.5 - Storage Server
Fibre Channel-Export [cmdb_ci_fc_export]	SMI 1.5 - Storage Server
Fibre-Channel-Port [cmdb_ci_fc_port]	SMI 1.5 - Storage Server
SAN-Export [cmdb_ci_san_export]	SMI 1.5 - Storage Server
Speichercontroller [cmdb_ci_storage_controller]	SMI 1.5 - Storage Server
Speicherexport [cmdb_ci_storage_export]	SMI 1.5 - Storage Server
Speicherdateifreigabe [cmdb_ci_storage_fileshare]	SMI - Array - File Shares
Speicherpool [cmdb_ci_storage_pool]	SMI 1.5 - Storage Server
Speicherserver [cmdb_ci_storage_server]	CIM - Identity
Speicher-Switch [cmdb_ci_storage_switch]	CIM - Identity
Speichervolume [cmdb_ci_storage_volume]	SMI 1.5 - Storage Server
Speichergerät [cmdb_ci_storage_device]	SMI 1.5 - Storage Server
Storage Area Network [cmdb_ci_san]	SMI - Fabric

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

Erfasste Daten (Fortsetzung)

Tabelle	Probe
SAN-Verbindung [cmdb_ci_san_connection]	SMI - Fabric
SAN-Endpunkt [cmdb_ci_san_endpoint]	SMI - Fabric
SAN-Fabric [cmdb_ci_san_fabric]	SMI - Fabric
SAN-Zone [cmdb_ci_san_zone]	SMI - Fabric
SAN-Zonenalias [cmdb_ci_san_zone_alias]	SMI - Fabric
SAN-Zonenaliasmitglied [cmdb_ci_san_zone_alias_member]	SMI - Fabric
SAN-Zonenmitglied [cmdb_ci_san_zone_member]	SMI - Fabric
SAN-Zonensatz [cmdb_ci_san_zone_set]	SMI - Fabric

Die folgenden Probes sind verfügbar, werden aber derzeit nicht verwendet:

- SMI - Storage Server
- SMI - Array - Controllers
- SMI - Array - Disks
- SMI - Array - Pools
- SMI - Array - Ports
- SMI - Array - Volumes

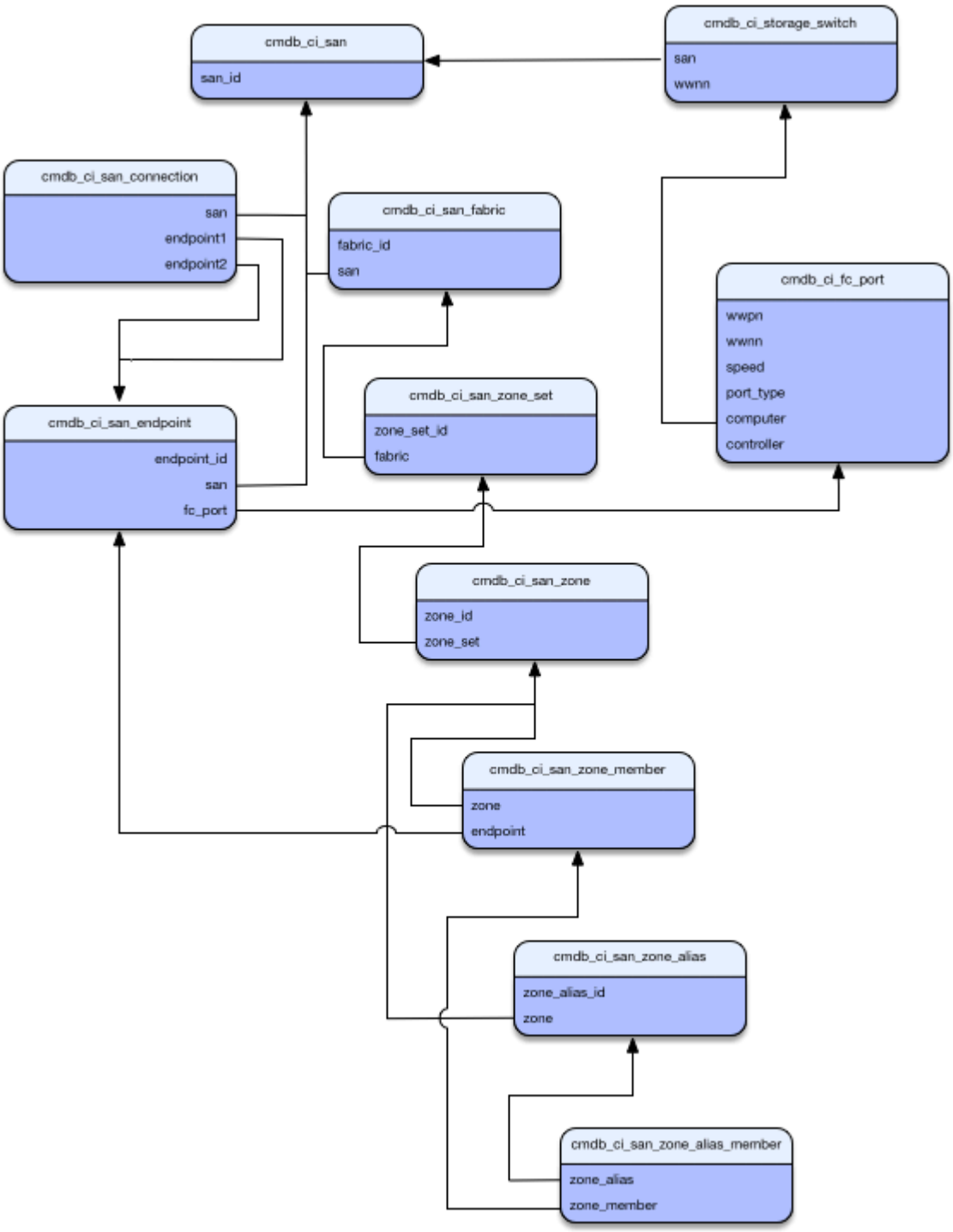
Erkennung von Storage Area Networks (SAN)

Discovery erfasst Informationen über Speichernetzwerke von spezialisierten Geräten wie Speicher-Arrays und Fibre Channel Switches (FC-Switches) und erzeugt bestimmte Referenzen zwischen den Tabellen im SAN-Schema.

SAN-Schema von ServiceNow

Im folgenden Diagramm sind die Tabellen im SAN-Schema und die zwischen ihnen definierten Standardreferenzen dargestellt.

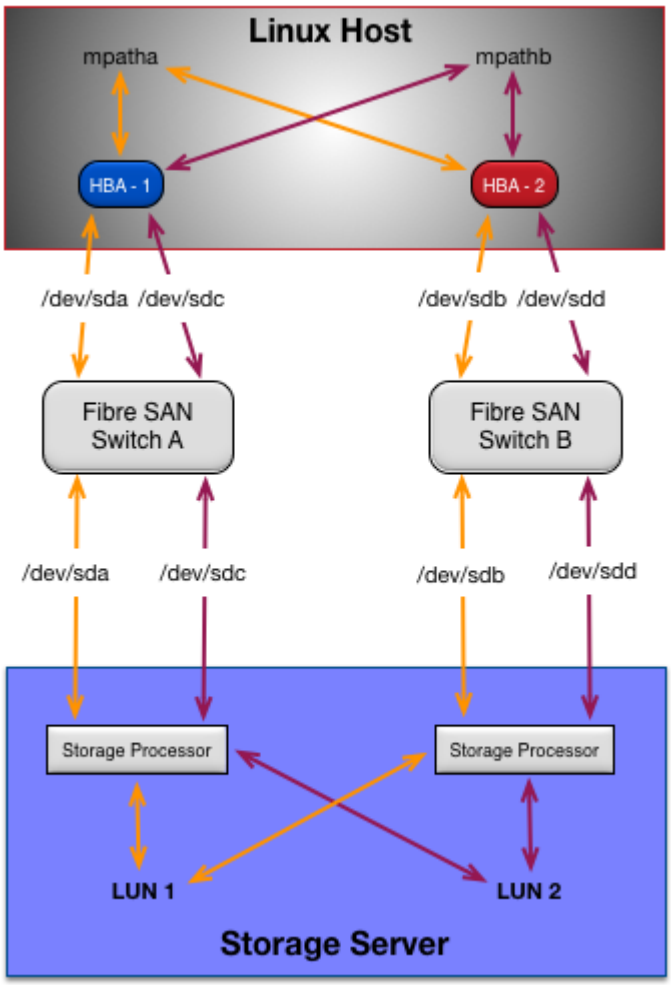
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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



Beispiel für Multipfad-SAN-Speicher

In diesem Diagramm ist die Beziehung von SAN-Speichervolumes zu einem Hostcomputer dargestellt. Der Speicher, auf den der Linux-Host zugreifen kann, besteht aus zwei physischen Fibre Channel-Datenträgern (mpatha und mpathb), die über ein Multipfad-FC-SAN mit dem Host verbunden sind. Die beiden HBAs auf der Hostschnittstelle sind mit jeweils zwei Glasfaserkabeln verbunden, um FC-Switches für die Failover-Funktionalität zu trennen. Die FC-Fabric Switches sind mit zwei FC-Speicherprozessoren auf dem Speicherserver verbunden. In folgendem Beispiel sind alle Speicherprozessoren mit den Speichervolumes **LUN 1** und **LUN 2** verbunden.

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



Funktionsweise der CIM-Erkennung

Im folgenden ist der Verarbeitungsablauf für die Klassifizierung von CIM-Speichersystemen (Common Information Model) dargestellt.

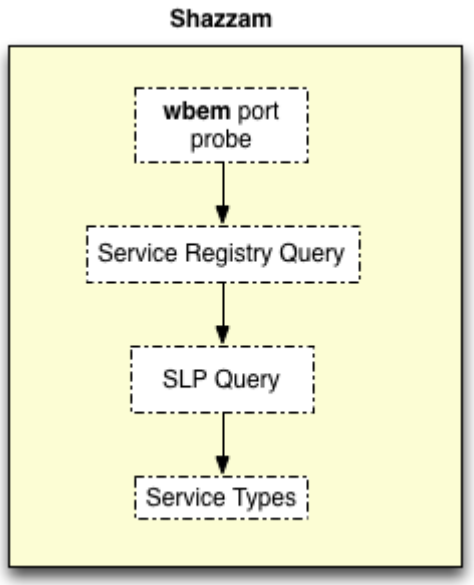
Verarbeitungsablauf

1. Die Shazzam-Probe startet die Port-Probe „wbem“ als Teil der Netzwerkerkennung.
2. Die Wbem-Port-Probe erkennt Aktivitäten an den Zielports SLP 427, CIM 5989 und 5988 und untersucht dann die zugehörige Liste **Service-Registry-Abfragen** unter **Discovery-Definition** > **Anschlussprobes**, für die SLP-Abfrage. Das Basissystem stellt diese Abfrage zur Erkennung des Servicetyps „service:wbem“ bereit, der das Vorhandensein eines SLP-Servers anzeigt.
3. Die Shazzam-Probe startet einen Scanner für den WBEM-Servicetyp. Der Scanner ruft Folgendes ab:
   - Die Attribute des Service vom SLP-Server
   - Die interop-Namespaces der CIM-Server im Netzwerk
4. Der Scanner hängt die gefundenen Namespace-Werte an die Ergebnisse der Port-Probe an.
5. Die Port-Probe „wbem“ hängt die enthaltenen SLP-Daten an die Probes vom Typ „CIM - Classify“ an.

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

6. Die Probe „CIM Classify“ verwendet diese Informationen, um die CIM-Server zu untersuchen.

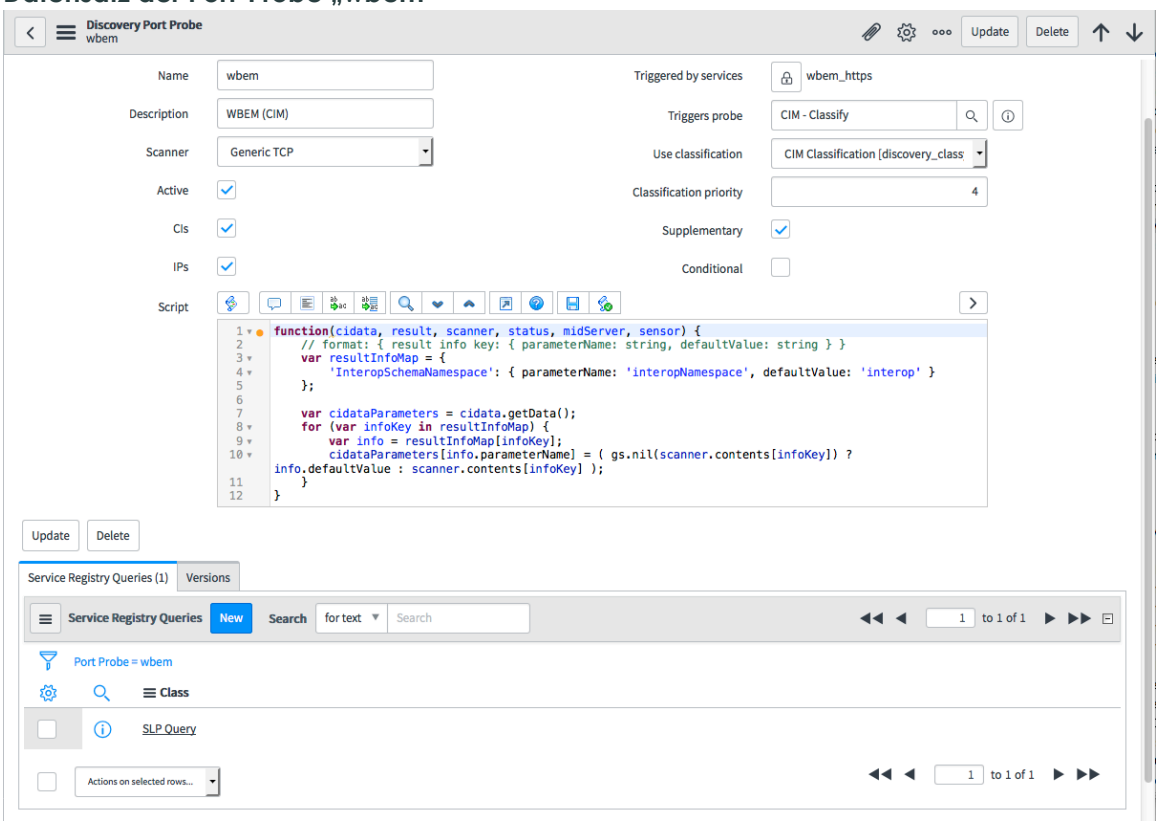
CIM-Shazzam-Verarbeitungsdiagramm



Port-Probe „wbem“

Die Probe **wbem** speichert die abgerufenen Daten in der Tabelle „CIM-Klassifizierung“ `[discovery_classy_cim]`. Um die Wbem-Port-Probe anzuzeigen, navigieren Sie zu **Discovery-Definition** > **Anschlussprobes**.

Datensatz der Port-Probe „wbem“

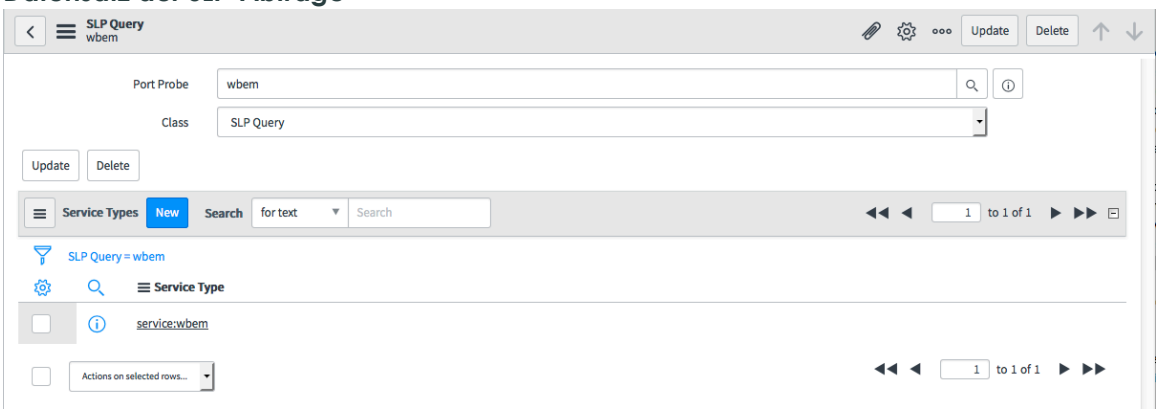


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

SLP-Abfrage

Die SLP-Abfrage erkennt den Service wbem (service:wbem) auf einem SLP-Server und erfasst seine Attribute. Öffnen Sie zum Anzeigen des SLP-Abfragedatensatzes den Datensatz der Port-Probe „wbem“, und wählen Sie **SLP-Abfrage** in der zugehörigen Liste **Service- Registry-Abfragen** aus.

Datensatz der SLP-Abfrage



Probe „CIM - Classify“

Die Port-Probe „wbem“ hängt die enthaltenen SLP-Daten einschließlich Namespaces an der Probe „CIM - Classify“ an, bevor er diesen startet. Die CIM-Klassifizierungs-Probe extrahiert VMware ESX-Seriennummern und Connector-Beziehungen zwischen den SAN- und NAS-Komponenten von CIM-Servern im Netzwerk.

Um auf die CIM-Klassifizierungsprobe zuzugreifen, navigieren Sie zu **Discovery-Definition** > **Probes** und wählen Sie in der Liste der Probes **CIM – Klassifizieren aus**.

Hinweis:

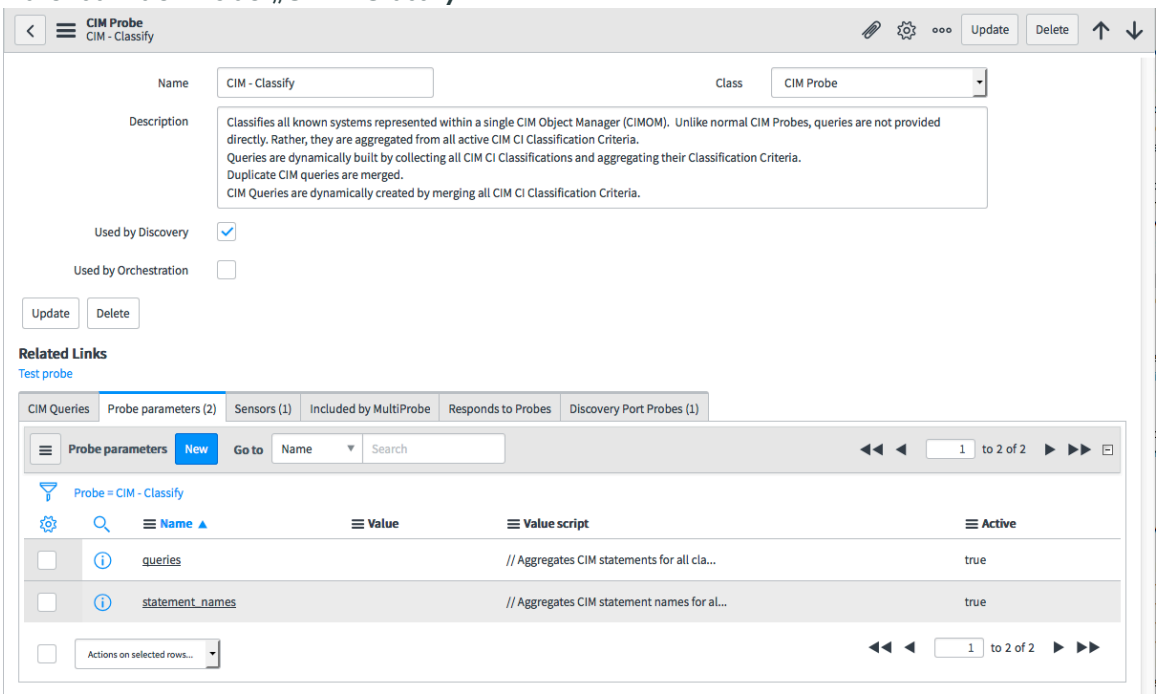
Die Systemeigenschaft *`mid.cim.interop.namespace`* vier Standardspeicher-Namespaces:

- interop
- root/interop
- root/pg_interop
- pg_interop

Wenn Sie mehrere Speicheranbieter verwenden, für die anwenderdefinierte Namespaces nicht als Standard angegeben sind, fügen Sie die neuen Namespaces der durch Kommas getrennten Liste in dieser Eigenschaft hinzu. Wenn Sie einen der Standard-Namespaces weiterhin verwenden möchten, müssen Sie diese in die Eigenschaft aufnehmen.

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

Datensatz der Probe „CIM - Classify“



SMI-S- und CIM-Probes und -Sensoren

SMI-S- und CIM-Probes und -Sensoren

Probe/Sensor	Beschreibung
CIM - Identity	Identifiziert ein System über CIM mithilfe von SMI-S
SMI - Array - Controllers	Ruft Controller-Informationen ab
SMI - Array - Disks	Ruft Informationen zum Speicherdatenträger ab
SMI - Array - File Shares	Listet NAS-Dateifreigaben von einem Speicherserver auf
SMI - Array - Pools	Ruft Speicherpools ab
SMI - Array - Ports	Ruft Speicherports ab
SMI - Array - Volumes	Ruft Speichervolumes ab
SMI - Fabric	Ruft SANs, Fabrics, Zonensätze, Zonen, Zonenaliase, Endpunkte und Verbindungen ab
SMI - Fibre Channel Switch	Ruft FC-Switches ab
SMI - NAS Head - Component Systems	Ruft alle virtuellen Dateiserver in einem NAS-Head-Profil ab
SMI - NAS Head - File Server IPs	Ruft IP-Adressen für jeden NAS-Dateiserver ab
SMI - NAS Head - File Servers	Ruft NAS-Dateiserver wie Common Internet File System (CIFS) und Network File System (NFS) ab

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

SMI-S- und CIM-Probes und -Sensoren (Fortsetzung)

Probe/Sensor	Beschreibung
SMI - NAS Head - File Shares	Ruft Dateifreigaben für jeden NAS-Dateiserver ab
SMI - Storage Server	Ruft SAN- und NAS-Arrays und -Server ab
SMI - WBEM Service	Ruft Informationen zum WBEM-Service wie Profile und die SMI-S-Version ab

SMI-S Provider zur Speichererkennung konfigurieren

Verwenden Sie dieses Verfahren zum Konfigurieren eines eigenständigen Speichergeräts mit dem erforderlichen SMI-S Provider für Discovery.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

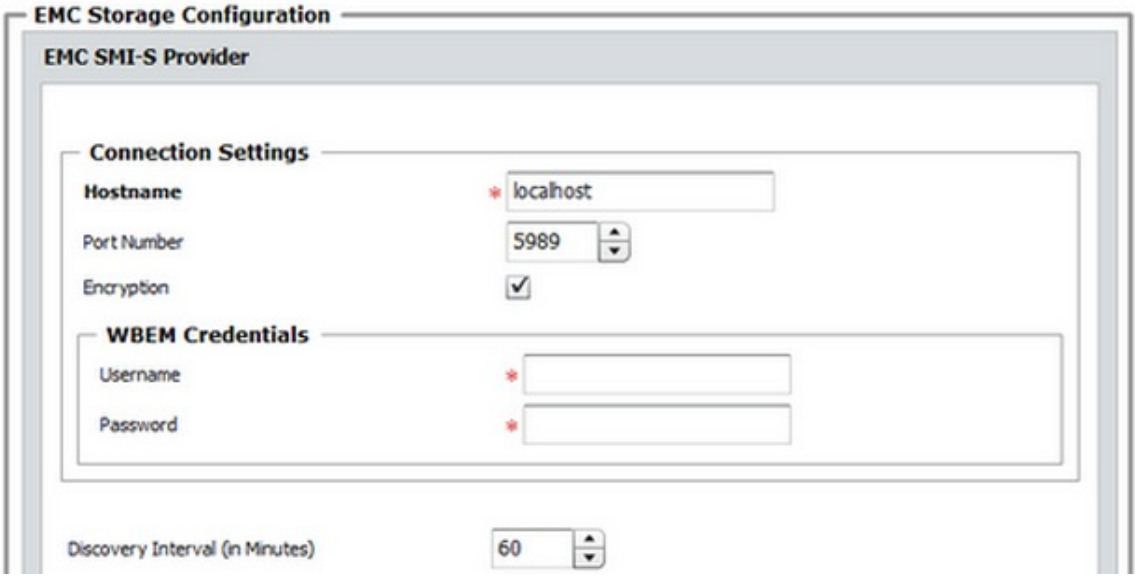
1. Wenn der SMI-S Provider auf dem Speichergerät nicht vorhanden ist, installieren Sie die SMI-S Provider-Software.
   Die SMI-S Provider-Software ist häufig Teil der Geräteverwaltungssoftware. Um weitere Informationen zu erhalten, laden Sie sich für die Anweisungen zum SMI-S Provider von der Website des Speicheranbieters herunter.
2. Installieren Sie für NetApp-Speichergeräte den SMI-S-Agent auf dem Speichergeräthost.

   Hinweis: Mit Discovery können NetApp-Server auch nativ erkannt werden, ohne auf den SMI-S-Server zuzugreifen. Weitere Informationen finden Sie unter Discovery für NetApp Server und Cluster.

3. Starten Sie den SMI-S Provider-Service.
4. Konfigurieren Sie im SMI-S Provider oder Agent das **Discovery-Intervall** mit einer Synchronisierungsrate, die es der Probe „wbem“ ermöglicht, während der Erkennung die aktuellen Informationen zu empfangen.
   Legen Sie beispielsweise das **Discovery-Intervall** für Speicher von EMC fest.

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

Beispiel für den Anbieter EMC



5. Richten Sie in der ServiceNow-Instanz die CIM-Anmeldeinformationen ein.
6. Erstellen Sie einen Erkennungszeitplan mit den IP-Adressen der einzelnen SMI-S Provider.
7. Wahlweise: Erstellen Sie ein Discovery-Verhalten, das eine Funktionalitätsdefinition mit einem *wbem*-Port-Probe verwendet, um die anfängliche Port-Scan-Phase (Shazzam) effizienter zu gestalten.
8. Führen Sie eine einfache Discovery für IP-Adressen aus.

Von Discovery auf Speichergeräten erfasste Daten

Discovery identifiziert und klassifiziert Informationen über Speichergeräte.

Von Discovery über Speichergeräte erfasste Daten

Bezeichnung	Tabellenname	Feldname	Quelle
Sys ID	Speicherdatenträger [cmdb_ci_storage_disk]	sys_id	N/V
Dateifreigabe-ID	Speicherdateifreigabe [cmdb_ci_storage_fileshare]	fileshare_id	Die CIM-Probe
Pfad	Speicherdateifreigabe [cmdb_ci_storage_fileshare]	Pfad	Die CIM-Probe
Festplattenspeicher (GB)	Speicherpool [cmdb_ci_storage_pool]	disk_space	Die CIM-Probe
Pool-ID	Speicherpool [cmdb_ci_storage_pool]	pool_id	Die CIM-Probe
Geschwindigkeit (GFC)	Speicheranschluss [cmdb_ci_storage_port]	speed	Die CIM-Probe
WWPN	Speicheranschluss [cmdb_ci_storage_port]	wwpn	Die CIM-Probe
Geräte-ID	Speicher-HBA [cmdb_ci_storage_hba]	device_id	Die CIM-Probe

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

Von Discovery über Speichergeräte erfasste Daten (Fortsetzung)

Bezeichnung	Tabellenname	Feldname	Quelle
Firmware-Version	Speicherserver [cmdb_ci_storage_server]	firmware_version	Die CIM-Probe
Festplattenspeicher (GB)	Speichervolume [cmdb_ci_storage_volume]	disk_space	Die CIM-Probe
LUN	Speichervolume [cmdb_ci_storage_volume]	lun	Die CIM-Probe
Größe (vdisk)	Speichervolume [cmdb_ci_storage_volume]	size	Die CIM-Probe
Name (vdisk)	Speichervolume [cmdb_ci_storage_volume]	Name	Die CIM-Probe
Objekt-ID (vdisk)	Speichervolume [cmdb_ci_storage_volume]	object_id	Die CIM-Probe

Speicherbeziehungen

Discovery stellt die richtigen Beziehungen zwischen NAS-Speichergeräten (Network Attached Storage) und remote bereitgestellten Client-Servern her, die den Speicher verbrauchen. Discovery ordnet NAS-Dateifreigaben zu. Die Zuordnung erfolgt anhand der IP oder des Hostnamens eines remote bereitgestellten Datenträgers auf dem Clientcomputer. Anschließend wird sie mit der IP oder dem Hostnamen des Speicherservers abgeglichen, der das exportierte Dateisystem bereitstellt.

Discovery erstellt die folgenden Beziehungen für Speicher-CIs, die in Speicherbereichsnetzwerken ausgeführt werden.

SAN-CI-Beziehungen

Übergeordnete Komponente	Beziehung	Untergeordnete Komponente
Speichervolume [cmdb_ci_storage_volume]	Exportieren nach::Importieren von	Fibre Channel-Datenträger [cmdb_ci_fc_disk]
Speichervolume [cmdb_ci_storage_volume]	Exportieren nach::Importieren von	iSCSI [cmdb_ci_iscsi_disk]

Discovery ordnet NAS-Dateifreigaben zu. Die Zuordnung zu einer IP-Adresse erfolgt durch Auflösung des Hostnamens eines remote bereitgestellten Datenträgers auf dem Clientcomputer. Anschließend wird sie mit der IP-Adresse des Speicherservers abgeglichen, der das exportierte Dateisystem bereitstellt. Discovery extrahiert den Hostnamen oder die IP-Adresse aus dem NAS-Pfad, um die Identität des Speicherservers zu bestimmen. Wenn der Hostname ein tatsächlicher Hostname ist, löst das System diesen Wert sofort in eine IP-Adresse auf. Außerdem wird sie im Feld **nas_ip_address** der Tabelle „NAS-Dateisystem“ [cmdb_ci_nas_file_system] gespeichert.

Discovery erstellt die folgenden Beziehungen für Speicher-CIs, die in Network Attached Storage (NAS) ausgeführt werden. Diese Beziehungen sind für Linux- und Windows-Betriebssystemhosts identisch.

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

NAS-CI-Beziehungen

Übergeordnete Komponente	Beziehung	Untergeordnete Komponente
NAS-Dateisystem [cmdb_ci_nas_file_system]	Zugeordnet von::Zugeordnet zu	Speicherdateifreigabe [cmdb_ci_storage_fileshare]

Für Veritas Volume Manager unter Linux erfasste Daten

Discovery erfasst Informationen über Datenträger und Volumes für Veritas Volume Manager (VxVM) auf Linux-Hosts und ordnet auf Veritas-Volumes bereitgestellte Dateisysteme dem vorgelagerten Speicheranbieter zu.

Hinweis: Stellen Sie sicher, dass VxVM ordnungsgemäß installiert und konfiguriert ist. Wenn Sie Treiber von Drittanbietern verwenden, müssen Sie die sudo-Berechtigung für *vxdmpadm* konfigurieren.

Tabellenschema

VxVM-Tabellen

Tabelle	Erweitert Tabelle
Veritas-Datenträger [cmdb_ci_veritas_disk]	Speicherpool [cmdb_ci_storage_pool]
Veritas-Datenträgergruppe [cmdb_ci_veritas_disk_group]	Konfigurationselement [cmdb_ci]
Veritas-Plex [cmdb_ci_veritas_plex]	Speicherpool [cmdb_ci_storage_pool]
Veritas-Teildatenträger [cmdb_ci_veritas_subdisk]	Speicherpoolmitglied [cmdb_ci_storage_pool_member]
Veritas-Laufwerk [cmdb_ci_veritas_volume]	Speicherpool [cmdb_ci_storage_pool]

Erfasste Daten

Erfasste VxVM-Daten

Tabelle	Felder	Beziehung
Veritas-Datenträger [cmdb_ci_veritas_disk]	• Name • size_bytes • disk_group	Beziehung vom Typ „Bereitgestellt von::Stellt bereit“ zum physischen Datenträger
Veritas-Datenträgergruppe [cmdb_ci_veritas_disk_group]	Name	Beziehung vom Typ „Enthält::Enthalten in“ zu Veritas-Datenträgern in der Gruppe
Veritas-Plex [cmdb_ci_veritas_plex]	• Name • size_bytes • layout (CONCAT, STRIPE, RAID)	

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

Erfasste VxVM-Daten (Fortsetzung)

Tabelle	Felder	Beziehung
Veritas-Teildatenträger [cmdb_ci_veritas_subdisk]	• partition_number • source_start_offset: Offset auf dem Datenträger, von dem dieser Teildatenträger partitioniert ist • source_end_offset: Offset auf dem Datenträger, von dem dieser Teildatenträger partitioniert ist • start_offset: Offset dieses Teildatenträgers im Plex, der ihn verwendet • end_offset: Offset dieses Teildatenträgers im Plex, der ihn verwendet • size_bytes	
Veritas-Laufwerk [cmdb_ci_veritas_volume]	Name	Beziehung vom Typ „Gespeichert auf::Stellt Speicher bereit für“ zu Veritas-Datenträgern, auf denen das Volume gespeichert ist

Daten anzeigen

VxVM Discovery ordnet Dateisysteme den Datenträgern zu, die Speicher bereitstellen. Standardmäßig handelt es sich dabei um die einzigen Informationen, die in der Benutzeroberfläche angezeigt werden. Die Beziehung zwischen Dateisystem und Datenträger wird im Formular „Dateisystem“ als vorgelagerte Beziehung vom Typ **Gespeichert auf** angezeigt. Zum Anzeigen der restlichen Informationen, die Discovery für VxVM erfasst, müssen Sie dem Formular „Linux-Server“ die entsprechende zugehörige Liste hinzufügen. Folgende Listen sind verfügbar:

- Veritas Disk Group
- Veritas-Laufwerk
- Veritas-Plex
- Veritas Subdisk (Computer)
- Veritas Subdisk (Speicher)
- Veritas-Laufwerk

Discovery für NetApp Server und Cluster

Discovery und Service-Mapping finden NetApp-Server und -Cluster entweder mithilfe von CIM-Proben oder -Mustern. Um einige dieser Ressourcen zu erkennen, müssen

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

Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Informationen zu den Komponenten und Versionen von NetApp-Servern und -Clustern, die erkannt werden können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Discovery-Methoden für NetApp Server und Cluster

Methode	Unterstützte Modi	Upgrades
Erkennung mit Mustern mithilfe der ONTAP-API. Diese Muster unterstützen die native Erkennung von NetApp-Servern, ohne dass der SMI-S-Server erkannt werden muss.	• NetApp 7-Modus • NetApp-Clustermodus	Standardmäßig aktiviert.
Discovery mit Mustern mithilfe der HTTP-REST-API.	NetApp-Clustermodus	Verfügbar im Muster für Discovery und Service-Mapping Store Anwendung ab August 2023.
Erkennung mit Probes und Sensoren mit SMI-S	• NetApp 7-Modus • NetApp-Clustermodus	Legacy

Eigenschaften der NetApp-Erkennung

Um Discovery mit Mustern zu verwenden, navigieren Sie zu **Discovery-Definition** > **Eigenschaften** und aktivieren Sie diese Eigenschaften:

Eigenschaftsbezeichnung	Name
Verwenden Sie für 7-Mode NetApp Storage Server die native Erkennung anstelle von SMI-S.	glide.discovery.sensors.netapp_native_7mode
Für den Cluster-Modus verwenden NetApp Storage Server die native Erkennung anstelle von SMI-S.	glide.discovery.sensors.netapp_native_cluster_mode

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

Hinweis: Wenn Sie bereits eine NetApp-Discovery mit Probes durchgeführt haben und dann diese Eigenschaften aktivieren, wird bei der nächsten NetApp-Discovery ein Migrationsskript ausgeführt. Dieses Skript kann CIs für Elemente wie Speicherpools löschen, die von Probes, aber nicht von Mustern erkannt werden. Außerdem werden Beziehungen erstellt.

Voraussetzungen

Allgemeine Voraussetzungen

Stellen Sie sicher, dass die Anwendungen auf dem neuesten Stand sind:

- Muster für Discovery und Service-Mapping
- Visibility Content

SSLv3 deaktivieren und TLS für den NetApp-Zielserver aktivieren, da die von MID-Server verwendete Java-Ausführung SSLv3 nicht standardmäßig aktiviert. Der Schlüssel zum Verschlüsseln des Zertifikats muss mindestens 1024 Bit aufweisen.

Voraussetzungen für die SNMP-basierte Discovery

Konfigurieren Sie die Anmeldeinformationen für die SNMP-Community, um den NetApp-Server zu klassifizieren. Weitere Informationen finden Sie unter SNMP-Community-Anmeldeinformationen .

Aktivieren Sie den **schreibgeschützten** Zugriff auf die ONTAP-API auf dem NetApp-Server.

- Clustermodus: Der Benutzer kann eine schreibgeschützte Rolle mit Standardzugriff haben.
- 7-Modus: Der -Benutzer muss über eine anwenderdefinierte Rolle mit den folgenden Fähigkeiten verfügen:
  - `login-snmp, login-ndmp, login-sp, and login-http-admin`
  - `Api-*`

Konfigurieren Sie Anmeldeinformationen für die Standardauthentifizierung für den schreibgeschützten Benutzer. Weitere Informationen finden Sie unter Virtual Server Interface .

Voraussetzungen für REST-basierte Discovery:

Deaktivieren Sie die SNMP-basierte Discovery. Weitere Informationen finden Sie unter SNMP-basierte NetApp-Speicher-Cluster-Discovery deaktivieren.

Stellen Sie sicher, dass der Anwendungsbenutzer über eine **schreibgeschützte** Rolle verfügt.

Konfigurieren Sie Anmeldeinformationen für die Standardauthentifizierung für den schreibgeschützten Benutzer. Weitere Informationen finden Sie unter Virtual Server Interface .

Wird ausgeführt Discovery

Zum Ausführen einer Discovery mit Mustern erstellen Sie einen Discovery-Zeitplan, der auf die Verwaltungs-IP-Adresse des NetApp-Servers abzielt.

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

Hinweis: NetApp erstellt unterschiedliche Speichervolume-Bezeichner, wenn es mit unterschiedlichen Protokollen ausgeführt wird. Wenn Sie eine Discovery mit HTTP nach einer Discovery mit SNMP ausführen, werden für dasselbe Speichervolume doppelte CIs erstellt. Ein CI wird für den eindeutigen Bezeichner (UUID) erstellt, den die NetApp ONTAP API bereitstellt, und ein CI wird für den eindeutigen Bezeichner (UUID) erstellt, der die NetApp HTTP REST API bereitstellt.

Vom SNMP-Muster des NetApp-Clusters gesammelte Daten

In den folgenden Tabellen sind die Daten aufgeführt, die Discovery bei der Ausführung der NetApp-Erkennungsmuster finden kann.

Tabelle	Felder
cmdb_ci_storage_server	Name firmware_version serial_number manufacturermode model_id cim_object_path short_description ip_address
cmdb_ci_storage_cluster	short_description ip_address manufacturer
cmdb_ci_storage_cluster_node	Name operational_status
cmdb_ci_storage_node_element	Cluster short_description manufacturer serial_number model_id ram cpu_type cpu_manufaturer

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

Tabelle	Felder
	cpu_core_count
cmdb_ci_network_adapter	Name ip_address netmask cmdb_ci
cmdb_serial_number	serial_number serial_number_type
cmdb_ci_ip_address	ip_address netmask nic ip_version (Storage-7 mode) Name
cmdb_ci_disk	Name device_id serial_number manufacturer model_id storage_type device_interface size_bytes Computer
cmdb_ci_storage_fileshare	Pfad Name
cmdb_ci_storage_pool	Name short_description free_space_bytes pool_id

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

Tabelle	Felder
	size_bytes
cmdb_ci_storage_volume	Name lun volume_id
cmdb_ci_iscsi_export	Name lun initiator_iqn iqn export_id
cmdb_ci_storage_controller	Name device_id
cmdb_ci_fc_export	initiator_wwpn export_id Name lun
cmdb_ci_fc_port	speed Name wwnn wwpn

Hinweis: Weitere Informationen zur NetApp-Erkennung mit CIM finden Sie unter Speichererkennung über SMI-S und CIM.

Vom NetApp-Cluster-HTTP-Muster gesammelte Daten

Die folgenden Daten werden erkannt, wenn das **SNMP-Muster für NetApp-Cluster** deaktiviert wird.

Tabelle	Felder
cmdb_ci_storage_server	ip_address cluster_version

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

Tabelle	Felder
	serial_number
cmdb_ci_storage_node_element	Cluster ip_address_range
cmdb_ci_storage_cluster_node	Name operational_status Cluster
cmdb_ci_storage_server	firmware_version description ip_address_range
cmdb_serial_number	serial_number serial_number_type
cmdb_ci_ip_address	name netmask nic
cmdb_ci_disk	Computer Schnittstelle size_bytes
cmdb_ci_storage_pool	name size_bytes free_space_bytes
cmdb_ci_fc_port	speed
cmdb_ci_storage_fileshare	path
cmdb_ci_storage_volume	name volume_id size_bytes free_space_bytes

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

Tabelle	Felder
cmdb_ci_iscsi_export	Name lun export_id initiator_iqn iqn
cmdb_ci_storage_controller	Name device_id
cmdb_ci_fc_export	name lun export_id initiator_wwpn

CI-Beziehungen

CI	Beziehungstyp	CI
cmdb_ci_storage_node_element	Verwaltet von::Verwaltet	cmdb_ci_storage_cluster
cmdb_ci_storage_cluster_node	Gehostet auf::Hostet	cmdb_ci_storage_node_element
cmdb_ci_storage_cluster_node	Cluster von:Clustern	cmdb_ci_storage_cluster
cmdb_ci_storage_server	Wird ausgeführt auf: Wird ausgeführt	cmdb_ci_storage_cluster
cmdb_ci_storage_server	Zugeordnet an:Zugeordnet von	cmdb_ci_storage_node_element
cmdb_ci_storage_node_element	Besitzer: Im Besitz von	cmdb_ci_network_adapter
cmdb_ci_storage_server	Besitzer: Im Besitz von	cmdb_ci_network_adapter
cmdb_ci_storage_node_element	Besitzer: Im Besitz von	cmdb_ci_ip_address
cmdb_ci_storage_server	Besitzer: Im Besitz von	cmdb_ci_ip_address
cmdb_ci_storage_node_element	Enthält::Enthalten in	cmdb_ci_disk
cmdb_ci_storage_node_element	Enthält::Enthalten in	cmdb_ci_storage_pool
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_storage_pool
cmdb_ci_storage_server	Besitzer: Im Besitz von	cmdb_ci_fc_port
cmdb_ci_storage_fileshare	Bereitgestellt von: Stellt bereit	cmdb_ci_storage_server
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_storage_volume
cmdb_ci_storage_controller	Controller für:gesteuert von	cmdb_ci_fc_port

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

CI	Beziehungstyp	CI
cmdb_ci_iscsi_export	Gehostet auf::Hostet	cmdb_ci_storage_server
cmdb_ci_fc_export	Gehostet auf::Hostet	cmdb_ci_storage_server

SNMP-basierte NetApp-Speicher-Cluster-Discovery deaktivieren

Deaktivieren Sie die standardmäßige SNMP-basierte NetApp-Speichercluster-Discovery, und verwenden Sie stattdessen die REST-basierte Discovery, um die Sicherheit zu erhöhen.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **SNMP**.
2. Suchen Sie im Feld **Name** nach `NetApp Storage Server Cluster-Mode`.
3. Wählen Sie den Datensatz „NetApp Storage Server-Clustermodus“.
4. Deaktivieren Sie das Kontrollkästchen **Aktiv**.
5. Wählen Sie **Aktualisieren**.

Nächste Maßnahme
Konfigurieren Sie Anmeldeinformationen für die Standardauthentifizierung für einen Benutzer mit einer schreibgeschützten Rolle. Weitere Informationen finden Sie unter Virtual Server Interface .

Zugehörige Informationen

Discovery für NetApp Server und Cluster

Große Speichernutzlasten in Linux und Solaris verwalten

Hohe Nutzlasten für direkt angeschlossenen Linux- und Solaris-Speicher können zu Fehlern aufgrund von Speichermangel führen, wenn sie nicht für die Serialisierung der Verarbeitung der Nutzlast konfiguriert sind.

Vorbereitungen
Erforderliche Rolle: admin oder discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Linux- oder Solaris-Speichersensoren Nutzlasten großer Datenträger-Arrays verarbeiten, werden Worker-Threads gleichzeitig ausgeführt, was dazu führen kann, dass einem Instanzknoten der Arbeitsspeicher ausgeht und er neu gestartet werden muss. Um das zu verhindern, steuert die Tabelle [discovery_sensor_yield] das Verhalten von Worker-Threads, die zur Verarbeitung großer Nutzlasten verwendet werden. Wenn Discovery einen Sensor verarbeitet, wird die Tabelle [discovery_sensor_yield] für diesen Sensor überprüft. Wenn der Sensor in der Tabelle aufgeführt ist und die Nutzlastgröße den in der Tabelle konfigurierten Grenzwert überschreitet, versucht der Worker vor der Verarbeitung der Nutzlast, eine Sperre zu setzen. Wenn die Sperre nicht verfügbar ist, da ein anderer Worker bereits eine große Nutzlast verarbeitet, plant der wartende Worker die Neuausführung des Auftrags in 30 Sekunden und fährt mit anderen Aufgaben fort. Der Auftrag wartet dann in der Tabelle „Zeitplanelement“ [sys_trigger] darauf, dass ein inaktiver Worker ihn abholt. Diese Serialisierung erfolgt knotenweise, sodass mehrere Knoten gleichzeitig hohe Nutzlasten verarbeiten können. Das Verarbeitungsintervall von 30 Sekunden ist nicht konfigurierbar.

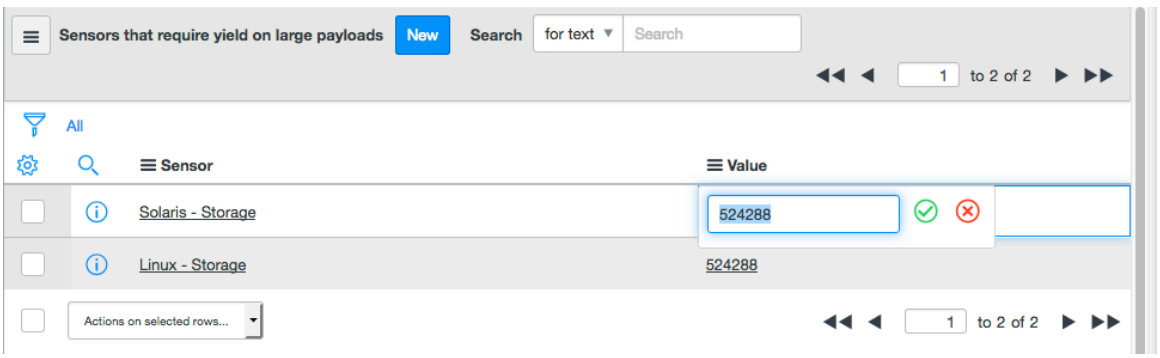
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Wichtig: Diese Schwellenwerte wurden nur für Linux- und Solaris-Speichersensoren erstellt und sollten in den meisten Fällen nicht geändert werden. Wenn Ihrer Instanz nicht genügend Arbeitsspeicher zur Verfügung steht, während gleichzeitig mehrere große Speichernutzlasten verarbeitet werden, sollten Sie die Erkennung dieser Systeme zu Zeiten geringerer Aktivität planen. Wenn dies nicht möglich ist, überprüfen Sie die ECC-Warteschlange, um zu bestimmen, welcher Speichersensor möglicherweise das Problem verursacht, und notieren Sie sich die Größe der Nutzlast. Wenn die Nutzlastgröße unter dem Schwellenwert in der Tabelle [discovery_sensor_yield] liegt, senken Sie den Schwellenwert weit genug, damit die Nutzlast serialisiert wird. Wenn ein anderer Sensor als der Linux- oder Solaris-Speichersensor verantwortlich ist, können Sie diesen Sensor der Tabelle [discovery_sensor_yield] hinzufügen. Stellen Sie sicher, dass der Schwellenwert für die Nutzlastgröße richtig festgelegt ist. Die Serialisierung der Sensorverarbeitung kann Discovery verlangsamen.

Prozedur

1. Geben Sie im Anwendungsnavigatorfilter **discovery_sensor_yield.list** ein.
   Das Discovery-Basissystem serialisiert die folgenden Sensoren, wenn ihre Nutzlasten 512 KB überschreiten:
   - **Solaris - Storage**
   - **Linux - Storage**
2. Um den Schwellenwert zu ändern, doppelklicken Sie in der Liste in die Spalte **Wert**, und bearbeiten Sie die Größe.

Schwellenwert für Sensorlast bearbeiten



3. Um einen weiteren Sensor hinzuzufügen und für die Nutzlastserialisierung zu konfigurieren, klicken Sie auf **Neu**, und füllen Sie die Felder im Formular aus.
   - **Sensor**: Zu konfigurierender Speichersensor
   - **Wert**: Schwellenwertgröße für den Sensor
4. Klicken Sie auf **Absenden**.

Beispiele für die Speichererkennung

Discovery erstellt Konfigurationselemente (CI) und CI-Beziehungen für physische und logische Speicherkomponenten, die direkt an Anwendungs- und Datenbankserver oder über Fibre Channel Switched Fabric in einer Multipfadkonfiguration angeschlossen sind.

Direct Attached Storage

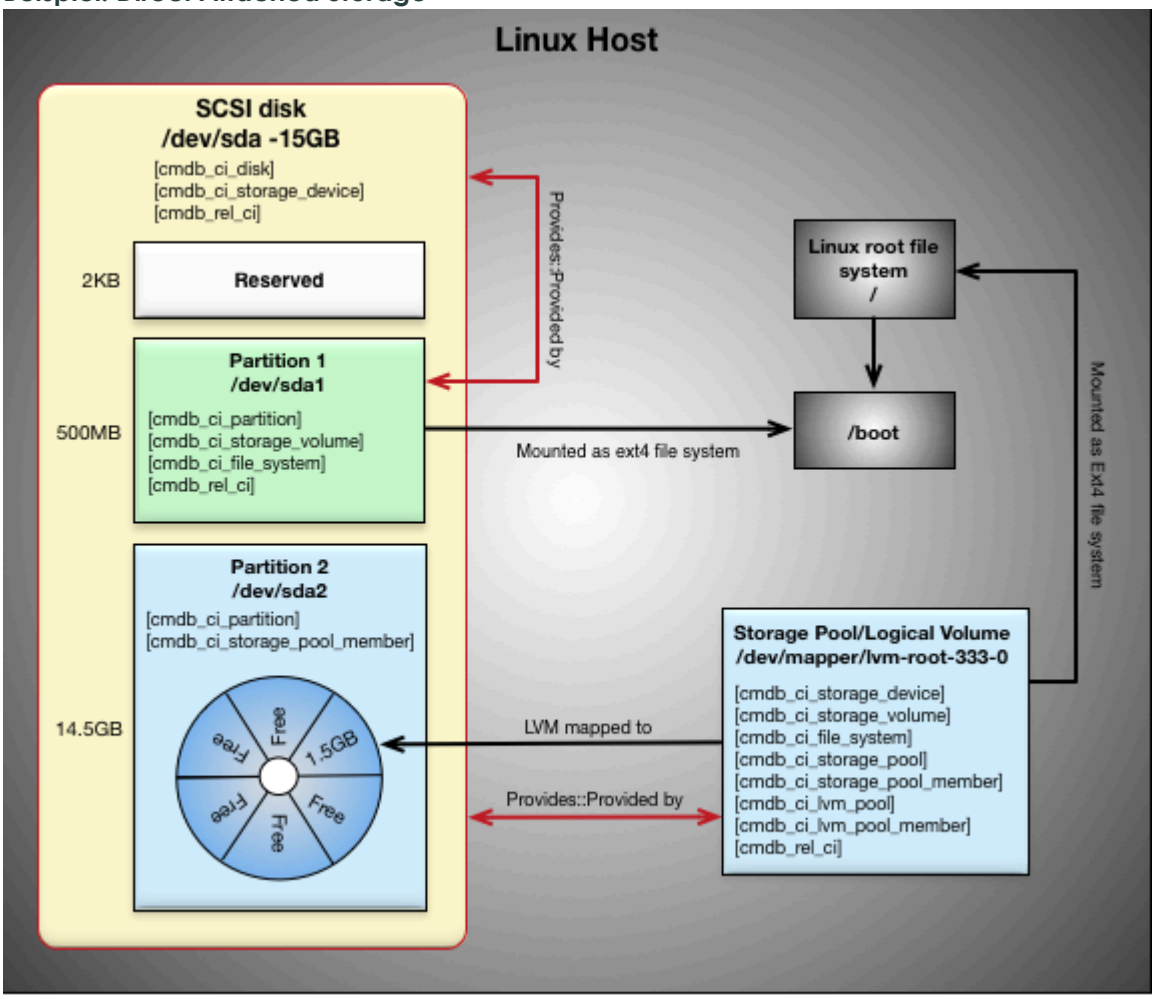
In diesem Beispiel für Direct Attached Storage (DAS) wird ein SCSI-Laufwerk mit den beiden Partitionen `/dev/sda1` und `/dev/sda2` an einen Linux-Host angeschlossen. Die Partition `/dev/sda1` ist startfähig und unterstützt die Systemsoftware. Die Partition `/dev/sda2` enthält ein logisches Volume, das als Speicherpool konfiguriert und von Logical Volume

Automatische Übersetzung

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

Management (LVM) in das Linux-Stammdateisystem geladen wurde. Der Speicherpool verwendet nur 1,5 GB der Partition, sodass 13 GB Speicherplatz für weitere logische Volumes zur Verfügung stehen.

Beispiel: Direct Attached Storage



Für Direct Attached Storage (DAS) erstellte Konfigurationselemente und Beziehungen

Konfigurationselement	Beschreibung	Tabellen	Schlüsselreferenz und Beziehungen
/dev/sda	Physisches SCSI-Speichergerät	• [cmdb_ci_disk] • [cmdb_ci_storage_device] • [cmdb_rel_ci]	[cmdb_rel_ci] • **Stellt bereit**: /dev/sda • **Bereitgestellt von**: /dev/sda1
			[cmdb_rel_ci]

Automatische Übersetzung

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

Für Direct Attached Storage (DAS) erstellte Konfigurationselemente und Beziehungen (Fortsetzung)

Konfigurationselement	Beschreibung	Tabellen	Schlüsselreferenz und Beziehungen
			• **Stellt bereit**: /dev/sda • **Bereitgestellt von**: /dev/mapper/lvm-root-333-0
/dev/sda1	Partition 1 auf SCSI-Speichergerät	• [cmdb_ci_partition] • [cmdb_ci_storage_volume] • [cmdb_ci_file_system] • [cmdb_rel_ci]	[cmdb_ci_file_system] • **Bereitstellungspunkt**: /boot • **Dateisystem**: Ext4
			[cmdb_rel_ci] • **Stellt bereit**: /dev/sda • **Bereitgestellt von**: /dev/sda1
/dev/sda2	Partition 2 auf SCSI-Speichergerät	• [cmdb_ci_partition] • [cmdb_ci_storage_pool_member]	[cmdb_ci_storage_pool_member] • **Pool**: /dev/mapper/lvm-root-333-0 • **Speicher**: /dev/sda2
/dev/mapper/lvm-root-333-0	Logisches Linux-Volume, das mit LVM einer physischen Plattenspeicherpartition zugeordnet ist	• [cmdb_ci_storage_device] • [cmdb_ci_storage_volume] • [cmdb_ci_file_system] • [cmdb_ci_storage_pool] • [cmdb_ci_storage_pool_member] • [cmdb_ci_lvm_pool] • [cmdb_ci_lvm_pool_member] [cmdb_rel_ci]	[cmdb_ci_file_system] • **Bereitstellungspunkt**: / • **Dateisystem**: Ext4
			[cmdb_rel_ci] • **Stellt bereit**: /dev/sda • **Bereitgestellt von**: /dev/mapper/lvm-root-333-0
			[cmdb_ci_storage_pool_member]

Automatische Übersetzung

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

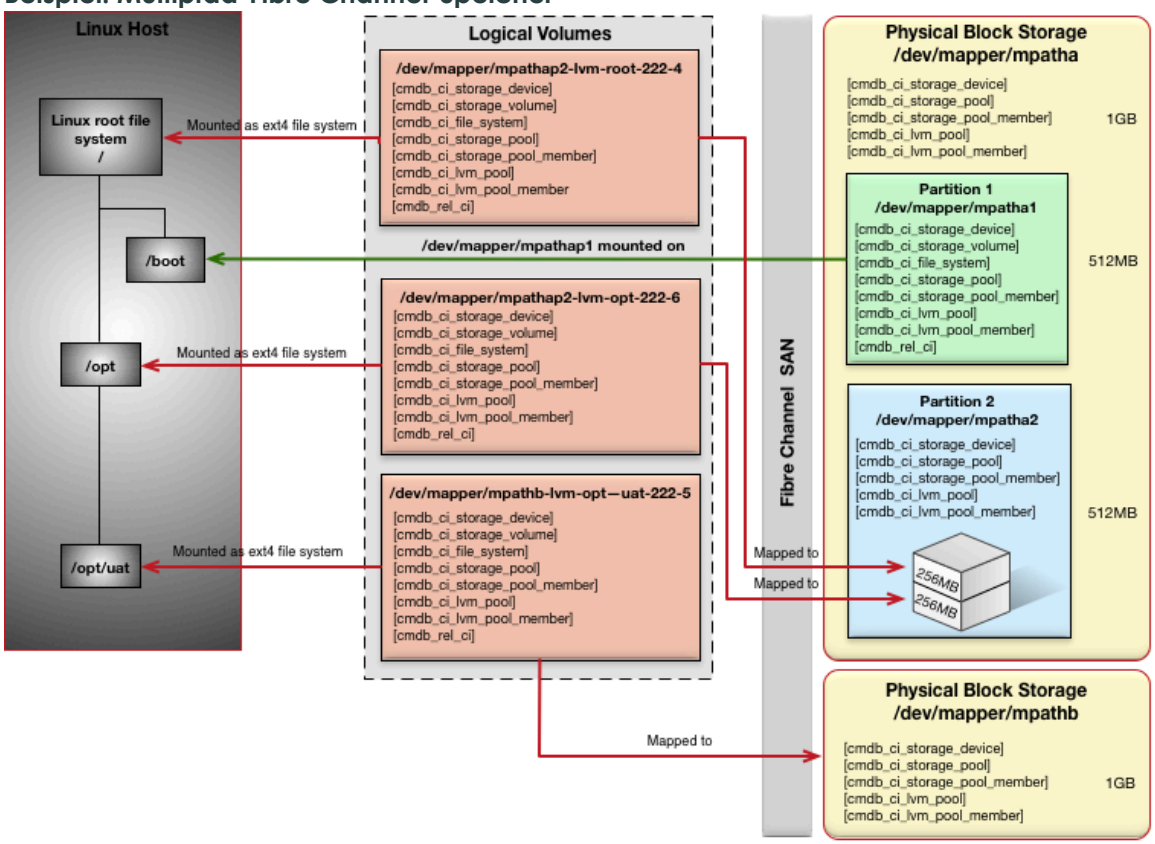
Für Direct Attached Storage (DAS) erstellte Konfigurationselemente und Beziehungen (Fortsetzung)

Konfigurationselement	Beschreibung	Tabellen	Schlüsselreferenz und Beziehungen
			• **Pool**: /dev/mapper/lvm-root-333-0 • **Speicher**: /dev/sda2

Multipfad-Fibre Channel-Speicher

In diesem Beispiel eines Fibre Channel-SAN (Storage Area Network) werden die beiden physischen Speichergeräte `mpatha` und `mpathb` über Fibre Channel Switches mit einem Linux-Host verbunden, die Failover-Funktionen bereitstellen. Das Laufwerk `mpatha` enthält die beiden Partitionen `mpatha1` und `mpatha2`. Die erste Partition wird in `/boot` direkt auf dem Linux-Host bereitgestellt. Drei logische Volumes werden der Partition `mpatha2` und dem physischen Gerät `mpathb` zugeordnet. Die logischen Volumes werden als Ext4-Dateisysteme in Ordnern in der Linux-Stammstruktur bereitgestellt. Das folgende Beispiel zeigt die CIs, die Discovery für jede Komponente verwaltet, und die Bereitstellungspunkte für die logischen Volumes auf dem Linux-Host.

Beispiel: Multipfad-Fibre Channel-Speicher



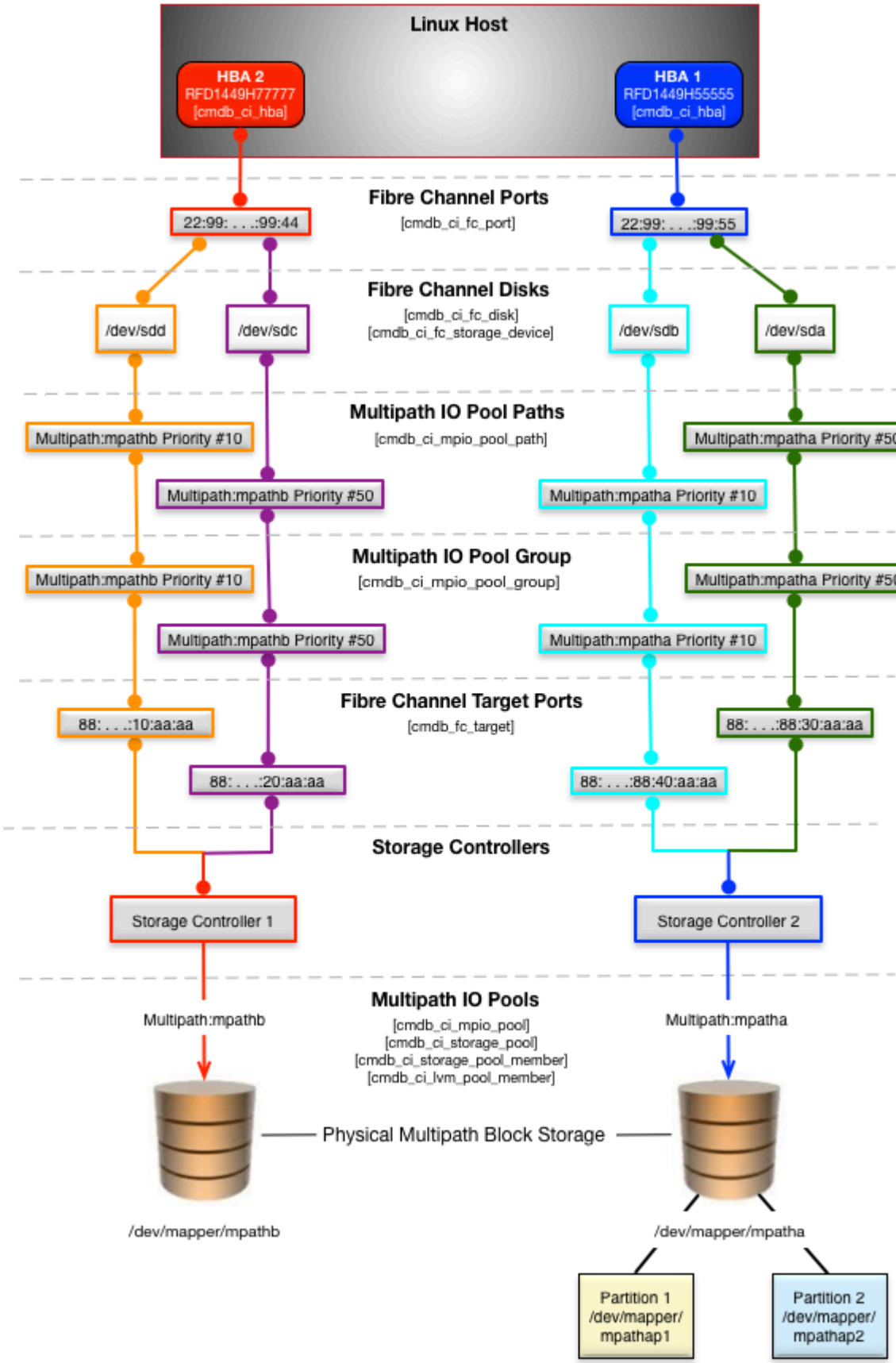
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Details zu Switched Fibre Fabrics

Discovery erstellt CIs für die logischen Unterkomponenten in NAS- und SAN-Umgebungen, zum Beispiel Fibre Channel-Datenträger und Poolkomponenten sowie für Hostbusadapter (HBA) und physischen Blockspeicher. In Multipfadumgebungen erstellt Discovery CI-Beziehungen innerhalb der Switched Fibre Fabrics, die den Linux-Host mit den physischen Speichergeräten verbinden. In diesem Diagramm verfügen die Fibre Fabrics über redundante Pfade, die in der SAN-Umgebung beim Ausfall von Verbindungen für Failover verwendet werden können.

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

Redundante Fibre Fabric-Pfade



Automatische Übersetzung

Cloud-Ressourcen-Erkennung

ITOM-Transparenz erkennt Ressourcen auf Cloud-Plattformen.

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

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Für Amazon gesammelte Daten AWS Cloud-Discovery

Discovery erfasst Informationen über Cloud-Ressourcen in AWS-Rechenzentren. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

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

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping.
- CMDB CI-Klassenmodelle.
- Visibility Content.

Konfigurieren Sie einen Discovery-Zeitplan

Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Bei der Erkennung von AWS Cloud erfasste Daten

AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Bezeichnung	Feldname
Name	Name
Region	region
Objekt-ID	object_id

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

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Bezeichnung	Feldname
Name	Name

VM-Instanz [cmdb_ci_vm_instance]

Bezeichnung	Feldname
Name	Name
Status	Status
Objekt-ID	object_id
CPUs	CPUs
Datenträger	disks
Arbeitsspeicher	memory
Netzwerkadapter	nics
ID der VM-Instanz	vm_inst_id

Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	Status

Images [cmdb_ci_os_template]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Gast-BS	guest_os
Stammgerätetyp	root_device_type
Image-Quelle	image_source
Bildtyp	image_type

Hardwaretyp [cmdb_ci_compute_template]

Bezeichnung	Feldname
Name	Name
vCPUs	vcpus
Arbeitsspeicher – MB	memory_mb
Lokaler Speicher – GB	local_storage_gb

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

Speichervolume [cmdb_ci_storage_volume]

Bezeichnung	Feldname
Name	Name
Status	Status
Objekt-ID	object_id
Speichertyp	storage_type
Größe	size

Cloud-Netzwerke [cmdb_ci_network] und VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]

Bezeichnung	Feldname
Name	Name
Status*	Status
CIDR*	cidr

*In VMware vCenter-Netzwerken nicht erkannt

Cloud-Subnetze [cmdb_ci_cloud_subnet]

Bezeichnung	Feldname
Name	Name
Status	Status
CIDR	cidr

Cloud Management-Netzwerkschnittstellen [cmdb_ci_nic]

Bezeichnung	Feldname
Name	Name
Netzmaske	netmask
MAC-Hersteller	mac_manufacturer
Status	install_status

Cloud-Lastenausgleichsmodule [cmdb_ci_cloud_load_balancer]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	Status

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

Ressourcengruppen [cmdb_ci_resource_group]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	Status

Öffentliche IP-Adressen [cmdb_ci_cloud_public_ipaddress]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Öffentliche IP-Adresse	public_ip_address
Öffentlicher DNS	public_dns

Speicherkonten [cmdb_ci_cloud_storage_account]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
SKU-Name	sku_name
Status	Status

DNS-Alias [cmdb_ci_dns_alias] und DNS-Name [cmdb_ci_dns_name]

Bezeichnung	Feldname
DNS-Alias [cmdb_ci_dns_alias]	
Name	Name
Kategorie	Kategorie
Status	Status
DNS-Name [cmdb_ci_dns_name]	
Name	Name
IP-Adresse	ip_address

Cloud-Datenbanken [cmdb_ci_cloud_database]

Bezeichnung	Feldname	Beschreibung
Name	Name	Der Name der Datenbank, die Sie in AWS erstellt haben
Objekt-ID	object_id	Dies ist auch der Name der Datenbank.
Typ	Typ	Der Typ der von Ihnen erstellten Datenbank.

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

Cloud-Datenbanken [cmdb_ci_cloud_database] (Fortsetzung)

Bezeichnung	Feldname	Beschreibung
Vollqualifizierter Domänenname	fqdn	Der FQDN, den AWS Ihrer Datenbank zugewiesen hat. Ein Beispielformat für AWS lautet wie folgt: `database-name.{random-number}.{datacenter}.rds.amazonaws.com`
Status	Status	Der Status der Datenbank: Verfügbar oder Beendet.
TCP-Port(s)	tcp_port	Der TCP-Port, über den die Datenbank kommuniziert.
Kategorie	Kategorie	Die Instanzklasse der Datenbank, zum Beispiel: db.t2.micro.

Cloud-Webserver [cmdb_ci_cloud_webserver]

Bezeichnung	Feldname
Name	Name
Installationsstatus	install_status
Lieferant	Lieferant
Vollqualifizierter Domänenname	fqdn
Betriebsstatus	operational_status
Status	state

Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]

Bezeichnung	Feldname	Beschreibung
Name	Name	Der Name des kube-Controller-Manager-Leader
Port	port	Der Bezeichner für den Kubernetes-Apiserver-Port.
Kubernetes-UID	k8s_uid	Eindeutiger Bezeichner für den Kubernetes-Cluster.
Lieferant	Lieferant	Anbieter des Kubernetes-Clusters.
Vollqualifizierter Domänenname	fqdn	Vollständig qualifizierter Domänenname des Kubernetes-API-Servers.

Für Microsoft Azure Cloud-Discovery erfasste Daten

Von Discovery werden Informationen über Cloud-Ressourcen in Microsoft Azure-Rechenzentren erfasst. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

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

Apps im Store anfordern

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

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle
- Visibility Content

Erstellen Sie Cloud-Anmeldeinformationen für Azure .

Erstellen Sie Microsoft Azure-Anmeldeinformationen für den Zugriff auf das Microsoft Azure-Konto. Weitere Informationen finden Sie unter Azure Cloud-Anmeldeinformationen erstellen.

Konfigurieren Sie einen Discovery-Zeitplan

Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Vorgehensweise von Discovery zur Erkennung von Microsoft Azure-Ressourcen

Discovery verwendet die API Cloud Provisioning and Governance und Muster für Discovery und Service-Mapping, um Cloud-Ressourcen zu finden.

Standardmuster

Muster	Beschreibung
Azure Datenbank (LP)	Erkennt folgende Datenbanktypen: • Microsoft.sql/server • Microsoft.sql/managedInstances • Microsoft.dbformysql • Microsoft.documentdb/databaseaccounts • Microsoft.cache/redis • Microsoft.dbfürpostgresql/servers • Microsoft.dbformysql/server • Microsoft.dbformysql/flexibleservers • Microsoft.dbfürpostgresql/flexibleservers

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

Standardmuster (Fortsetzung)

Muster	Beschreibung
	Füllt die Tabelle [cmdb_ci_cloud_database] aus.
Azure LoadBalancer TD	Ruft Microsoft Azure-Lastenausgleichsmodule ab und füllt die Tabelle cmdb_ci_lb_service. Dieses Muster wird nicht von Discovery für die horizontale Erkennung verwendet, sondern nur von Service-Mapping für die Erkennung von oben nach unten.
Azure Website (LP)	Ruft Microsoft Azure-Webserver ab und füllt die Tabellen „Cloud-Webserver“ [cmdb_ci_cloud_webserver] und „IP-Adresse“ [cmdb_ci_ip_address].

Von Discovery während der horizontalen Erkennung erfasste Daten

Azure-Rechenzentrum [cmdb_ci_azure_datacenter]

Bezeichnung	Feldname
Name	Name
Region	region
Objekt-ID	object_id

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Bezeichnung	Feldname
Name	Name

VM-Instanz [cmdb_ci_vm_instance]

Bezeichnung	Feldname
Name	Name
Status	Status
Objekt-ID	object_id
CPUs	CPUs
Datenträger	disks
Datenträgergröße (GB)	disks_size
Arbeitsspeicher	memory
Netzwerkadapter	nics
ID der VM-Instanz	vm_inst_id

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

Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	Status

Images [cmdb_ci_os_template]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Gast-BS	guest_os
Image-Quelle	image_source

Speichervolume [cmdb_ci_storage_volume]

Bezeichnung	Feldname
Name	Name
Status	Status
Objekt-ID	object_id
Speichertyp	storage_type
Größe	size

Cloud-Netzwerke [cmdb_ci_network] und VMware vCenter-Netzwerk [cmdb_ci_vcenter_network]

Bezeichnung	Feldname
Name	Name
Status*	Status
CIDR*	cidr

*In VMware vCenter-Netzwerken nicht erkannt.

Cloud-Subnetze [cmdb_ci_cloud_subnet]

Bezeichnung	Feldname
Name	Name
Status	Status
CIDR	cidr

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

Cloud Provisioning and Governance Netzwerkschnittstellen [cmdb_ci_nic]

Bezeichnung	Feldname
Name	Name
Netzmaske	netmask
MAC-Adresse	mac_address
MAC-Hersteller	mac_manufacturer
Status	install_status

Cloud-Lastenausgleichsmodule [cmdb_ci_cloud_load_balancer]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	state

Azure-Bereitstellungen [cmdb_ci_azure_deployment]

Bezeichnung	Feldname
Name	Name
Bereitstellungsstatus	provisioning_state

Hinweis: Diese Tabelle ist nur für Discovery verfügbar, wenn das Plugin Cloud Provisioning and Governance aktiviert ist.

Ressourcengruppen [cmdb_ci_resource_group]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Status	Status
Betriebsstatus	operational_status
Installationsstatus	install_status

Hinweis:

- Wenn eine Ressourcengruppe zum ersten Mal erkannt wird, wird das Feld **„Status“** auf **„Verfügbar“**festgelegt, **operational_status=Operativ**und **Status=Installiert**; basierend auf der Antwortzuordnung.
- Wenn eine Ressourcengruppe am Microsoft Azurebeendet wird, setzen die CMPReconciler-Skripts das Feld **Status** auf **Beendet**und **operational_status=Nicht funktionsfähig** und **Status=Abwesend**.

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

Öffentliche IP-Adressen [cmdb_ci_cloud_public_ipaddress]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Öffentliche IP-Adresse	public_ip_address
Öffentlicher DNS	public_dns

Speicherkonten [cmdb_ci_cloud_storage_account]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
SKU-Name	sku_name
Status	state

Cloud-Datenbanken [cmdb_ci_cloud_database]

Bezeichnung	Feldname
Vollqualifizierter Domänenname	fqdn
Name	Name
Objekt-ID	object_id
Betriebsstatus	operational_status
Typ	Typ
Status	state
Lieferant	Lieferant
Version	Version
Kategorie	Kategorie

Cloud-Webserver [cmdb_ci_cloud_webserver]

Bezeichnung	Feldname
Name	Name
Installationsstatus	install_status
Lieferant	Lieferant
Vollqualifizierter Domänenname	fqdn
Betriebsstatus	operational_status
Status	state

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

IP-Adresse [cmdb_ci_ip_address]

Bezeichnung	Feldname
Vollqualifizierter Domänenname	fqdn
Installationsstatus	install_status
IP-Adresse	ip_address
Name	Name
Netzmaske	netmask
Betriebsstatus	operational_status
Lieferant	Lieferant

Datenbank [cmdb_ci_database]

Bezeichnung	Feldname
Status der Lebenszyklusphase	life_cycle_stage_status
Name	Name
Status	status
Seriennummer	serial_number
Typ	Typ

Berechnungsvorlage [cmdb_ci_compute_template]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
VCPUS	vcpus

Hardwaretyp [cmdb_ci_hardware_type]

Bezeichnung	Feldname
Name	Name
Objekt-ID	object_id
Anbieter	Anbieter
vCPUs	vcpus

Zugehörige Informationen

Erkennung von Microsoft Azure-Cloud-Komponenten mithilfe von Mustern

Für GCP Cloud-Discovery erfasste Daten

Discovery sammelt Informationen zu Cloud-Ressourcen in Google Cloud Platform (GCP). Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

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

Apps im Store anfordern

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

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping.
- CMDB CI-Klassenmodelle.
- Visibility Content.

Konfigurieren Sie einen Discovery-Zeitplan

Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

GCP Daten gesammelt

Tabelle	ServiceNow-Feld	GCP-Feld
Region [cmdb_ci_google_datacenter]	object_id	items.id
	Name	Name
	short_description	Beschreibung
	Status	Status
	region	items.name
Virtueller Server [cmdb_ci_vm_instance]	object_id	id
	Name	Name
	state	Status
	CPUs	Nicht zugeordnet
	memory	Nicht zugeordnet
	disks	Datenträger (Array-Größe)
	disks_size	Nicht zugeordnet
	nics	networkInterfaces (Array-Größe)
	termination_protection	deletionProtection
	Nicht zugeordnet	canIpForward

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

Tabelle	ServiceNow-Feld	GCP-Feld
	Nicht zugeordnet	selfLink
	sys_created_on	creationTimestamp
Speichervolume (cmdb_ci_storage_volume)	object_id	items.id
	Name	Name
	short_description	Beschreibung
	Status	Status
	status	Status
	size	sizeGb
	storage_type	storage_type
Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]	object_id	items.id
	Name	Name
	public_ip_address	address
	Status	Status
Verfügbarkeitszone [cmdb_ci_availability_zone]	object_id	items.id
	Name	Name
	short_description	Beschreibung
	Status	Status
	status	Status
Hardwarevorlage [cmdb_ci_compute_template]	object_id	items.id
	Name	Name
	short_description	Beschreibung
	vcpus	guestCpus
	memory_mb	memoryMb
	local_storage_gb	imageSpaceGb
Instanzvorlage [cmdb_ci_instance_template]	object_id	items.id
	Name	Name
	short_description	Beschreibung
Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]	object_id	items.id
	Name	Name
	state	Status
	volume_name	sourceDisk
	Kapazität	storageBytes
	Keine Zuordnung	storageBytesStatus
	Keine Zuordnung	selfLink
	Keine Zuordnung	labelFingerprint

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

Tabelle	ServiceNow-Feld	GCP-Feld
	Keine Zuordnung	diskSizeGb
Datenträgertyp [cmdb_ci_disk_type]	object_id	zone:name
	Name	name@zone
	short_description	Beschreibung
	valid_disk_size	validDiskSize
	default_disk_size_gb	defaultDiskSizeGb
Subnetz [cmdb_ci_cloud_subnet]	object_id	id
	Name	Name
	cidr	ipCidrRange
	gateway	gatewayAddress
Image [cmdb_ci_os_template]	object_id	items.id
	Name	Name
	image_type	sourceType
	Keine Zuordnung	Status
	Keine Zuordnung	archiveSizeBytes
	Keine Zuordnung	diskSizeGb
	image_source	• sourceDisk • sourceDiskId
Lastenausgleichsmodul [cmdb_ci_cloud_load_balancer]	object_id	id
	Name	Name
	Keine Zuordnung	defaultService
Lastenausgleichsservice (cmdb_ci_lb_service)	object_id	id
	Name	Name
	Pool	backends
	port	port
	listener_protocol	protocol
	Keine Zuordnung	portName
	Keine Zuordnung	loadBalancingScheme
	Keine Zuordnung	sessionAffinity
	Keine Zuordnung	enableCDN
	service_type	Back-End/Front-End
Lastenausgleichsmodul-Integritätsservice [cmdb_ci_lb_health_service]	object_id	id
	Name	Name
	monitor_type	type (tcp/http/https)

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

Tabelle	ServiceNow-Feld	GCP-Feld
	request_path	requestPath
	port	port
	unhealthy_threshold	unhealthyThreshold
	healthy_threshold	healthyThreshold
	timeout_sec	timeoutSec
	check_interval_sec	checkIntervalSec
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	object_id	Instanz-ID von GCP
	Name	instance.substring nach dem letzten „/“
	Betriebsstatus	Status
Load Balancer-Pool [cmdb_ci_lb_pool]	object_id	id
	Name	Name
Netzwerk [cmdb_ci_network]	Status	Keine Zuordnung
	cidr	IPv4Range
	is_external	Keine Zuordnung
	Name	Name
	object_id	items_id
	Beschreibung	Beschreibung
Netzwerk-ACL [cmdb_ci_network_acl]	object_id	id
	Name	Name
	short_description	Beschreibung
Regel für Netzwerk-Zugriffssteuerungsliste [cmdb_ci_network_acl_rule]	is_outbound (True/False)	ac
	dest_from_port	Keine Zuordnung
	dest_to_port	Keine Zuordnung
	src_from_port	Keine Zuordnung
	src_to_port	Keine Zuordnung
	source_ranges	sourceRanges
	destination_ranges	destinationRanges
	target_tags	targetTags
	allowed_traffic	allowed
Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]	IP-Adresse	ip_address
	Name	Name
	Port	port
	Kubernetes-UID	k8s_uid
	Lieferant	Lieferant

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

Für IBM Cloud-Discovery erfasste Daten

Discovery sammelt Informationen zu Cloud-Ressourcen in IBM Cloud Platform und erstellt Beziehungen zwischen den gefundenen CIs. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

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

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping.
- CMDB CI-Klassenmodelle.
- Visibility Content.

Konfigurieren Sie einen Discovery-Zeitplan

Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Lastenausgleichsmodule

Für Lastenausgleichsmodule erfasste Daten

Tabelle	Feldname/-beschreibung
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	**object_id**: Eindeutiger Bezeichner des Lastenausgleichsmoduls
	name: Name des Lastenausgleichsmoduls
	fqdn: Adresse (Hostname) des Lastenausgleichsmoduls. Das ist der vollqualifizierte Domänenname des Lastenausgleichsmoduls.
	dns_name: Adresse (Hostname) des Lastenausgleichsmoduls
	short_description: Beschreibung des Lastenausgleichsmoduls
	operational_status: Betriebsstatus des Lastenausgleichsmoduls, entweder **ONLINE** oder **OFFLINE**

Automatische Übersetzung

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

Für Lastenausgleichsmodule erfasste Daten (Fortsetzung)

Tabelle	Feldname/-beschreibung
	location: Verweist auf den Standort des Lastenausgleichsmoduls mit dem Typ
	state: Bereitstellungsstatus des Lastenausgleichsmoduls, entweder **Verfügbar** oder **Beendet**
Load Balancer-Service [cmdb_ci_lb_service]	**object_id**: Eindeutiger Bezeichner des Lastenausgleichsservice
	name: Name, der durch das Muster erstellt wurde und Folgendes enthält: • Name des Lastenausgleichmoduls • Protokoll • Port • Ressourcentyp: **-listener**
	Port: Portnummer des Listener-Protokolls
	front_end_port: Portnummer des Listener-Protokolls
	listener_protokoll: Listener-Protokoll, entweder **TCP**, **HTTP** oder **HTTPS**
	operational_status: Bereitstellungsstatus des Listener.
Load Balancer-Pool [cmdb_ci_lb_pool]	**object_id**: Eindeutiger Bezeichner des Pools von Lastenausgleichsmodulen
	name: Name, der durch das Muster erstellt wurde und Folgendes enthält: • Name des Lastenausgleichmoduls • Protokoll • Port • Ressourcentyp: **-pool**
	port: Protokollport am Back-End
	pool_status: Bereitstellungsstatus eines Lastenausgleichsmodul-Pools
	load_balancing_method: Methode, die für den Lastenausgleich des Pools verwendet wird
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	**object-id**: Eindeutiger Bezeichner des Poolmitglieds, zusammengesetzt aus der ID des Mitglieds und der Listener-ID
	name: Name, der durch das Muster erstellt wurde und Folgendes enthält: • Name des Lastenausgleichmoduls • Protokoll

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

Für Lastenausgleichsmodule erfasste Daten (Fortsetzung)

Tabelle	Feldname/-beschreibung
	• Port • Ressourcentyp: **-member** • IP-Adresse des Poolmitglieds
	ip_address: IP-Adresse eines Lastenausgleichsmodulmitglieds
	server_id: ID des Mitglieds in der IBM-Cloud
	load_balancer: Name des zugehörigen Lastenausgleichsmoduls
Lastenausgleichsmodul-Integritätsservice [cmdb_ci_lb_health_service]	**object_id**: Eindeutiger Bezeichner der Integritätsserviceprüfung
	name: Name, der durch das Muster erstellt wurde und Folgendes enthält: • Name des Lastenausgleichmoduls • Protokoll • Ressourcentyp: **Integritätsprüfung** • Ressourcen-ID
	monitor_type: Typ der Integritätsprüfung. Gültige Werte: **TCP**, **HTTP** und **HTTPS**
	timeout_sec: Dauer in Sekunden, die auf die Antwort der Integritätsprüfung gewartet wird, bis eine Zeitüberschreitung auftritt
	check_interval_sec: Intervall in Sekunden zur Durchführung der Integritätsprüfung

Für Lastenausgleichsmodule erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_load_balancer	Enthält::Enthalten in	cmdb_ci_lb_health_service
cmdb_ci_cloud_load_balancer	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_service	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_lb_service
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_service	Enthält::Enthalten in	cmdb_ci_lb_pool

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

Für Lastenausgleichsmodule erstellte Beziehungen (Fortsetzung)

CI	Beziehung	CI
cmdb_ci_lb_pool	Eigentümer von::Eigentum von	cmdb_ci_lb_pool_member

Organisationen und Bereiche

Für Organisationen und Bereiche erfasste Daten

Tabelle	Felder
IBM Cloud-Organisationen [cmdb_ci_cloud_org]	• **guid**: Der eindeutige Bezeichner der Organisation • **URL**: Die eindeutige URL der Organisation • **billing_enabled**: Gibt an, ob die Abrechnungsmethode der Organisation aktiviert oder deaktiviert ist • **name**: Eindeutiger Name der Cloud-Organisation • **quota_definition_url**: Ressourcen, die für die Organisation verfügbar sind • **spaces_url**: Eindeutige URL des Bereichs, der der Organisation zugewiesen ist • **operational_status**: Betriebsstatus der Organisation
IBM-Cloudbereich [cmdb_ci_cloud_space]	• **object_id**: Eindeutiger Bezeichner (GUID) des Bereichs • **name**: Eindeutiger Name des Bereichs • **url**: Eindeutige URL des Bereichs • **allow_ssh**: Die IP-Adresse einer Speicherressource

Für Organisationen und Bereiche erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_org	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_space	Gehostet auf::Hostet	cmdb_ci_cloud_org
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_cloud_space

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

SSH-Schlüssel

Für SSH-Schlüssel erfasste Daten

Tabelle	Felder
Cloud-Schlüsselpaare [cmdb_ci_cloud_key_pair]	• **object_id**: ID des SSH-Schlüsseldatensatzes • **Name**: Beschreibender Name, der zur Identifizierung des SSH-Schlüssels verwendet wird • **key**: SSH-Schlüssel • **finger_print**: Kurze Bytefolge, die zur Authentifizierung oder Suche nach einem längeren SSH-Schlüssel verwendet wird. Diese wird beim Hinzufügen oder Ändern des SSH-Schlüssels automatisch generiert. Diese Eigenschaft ist schreibgeschützt. Vorgenommene Änderungen werden ignoriert. • **created_date**: Datum, an dem der SSH-Schlüssel hinzugefügt wurde. Diese Eigenschaft ist schreibgeschützt. Vorgenommene Änderungen werden ignoriert. • **modify_date**: Datum, an dem der SSH-Schlüssel zuletzt geändert wurde. Diese Eigenschaft ist schreibgeschützt. Vorgenommene Änderungen werden ignoriert. • **short_description**: Kurze Notiz zum SSH-Schlüssel.

Für SSH-Schlüssel erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_ibm_datacenter	Enthalten in::Enthält	cmdb_ci_availability_zone
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_cloud_service_account

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

IBM Cloud-Speicher

Für IBM Cloud-Speicher erfasste Daten

Tabelle	Felder
Speichervolume [cmdb_ci_storage_volume]	• **object_id**: Eindeutiger Bezeichner des Speicherkontos • **size**: Kapazität des Speicherkontos in Gigabyte • **size_bytes**: Kapazität des Speicherkontos in Byte • **name**: Benutzername, der für den Zugriff auf ein Nicht-EVault-Speichervolume verwendet wird. Dieser Benutzername wird verwendet, um den EVault-Server-Agent beim Vault-Sicherungssystem zu registrieren. • **label**: Name der Netzwerkressource für den Speicher • **storage_type**: Beschreibung des Speicherobjekts • **fqdn**: IP-Adresse einer Speicherressource • **device**: Eindeutige Identifikationsnummer des Gasts, der dem Speichervolume zugeordnet ist
Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]	• **object_id**: Eindeutiger Bezeichner des Speicherkontos • **name**: Name der Netzwerkressource des Speichers • **capacity**: Konfigurierte Snapshot-Speichergröße des Volume • **fqdn**: IP-Adresse einer Speicherressource • **location**: Eindeutige Verfügbarkeitszone, in der sich das Speichervolume befindet

Für IBM Cloud-Speicher erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_storage_volume	Bereitgestellt::Bereitgestellt von	cmdb_ci_storage_vol_snapshot
cmdb_ci_storage_vol_snapshot	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter

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

Für IBM Cloud-Speicher erstellte Beziehungen (Fortsetzung)

CI	Beziehung	CI
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_vol_snapshot	Positioniert in Zone::Zone beinhaltet	cmdb_ci_availability_zone
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_storage_volume

IBM Virtuelle Cloud-Server

Daten, die für virtuelle Cloud-Server IBM erfasst wurden

Tabelle	Felder
VM-Instanz [cmdb_ci_vm_instance]	• **name**: Name des virtuellen Computers • **object_id**: ID des virtuellen Computers • **dns_domain**: Domäne des virtuellen Computers • **fqdn**: IP-Adresse des virtuellen Computers • **short_description**: Hinweise, die dem virtuellen Computer auf der IBM-Konsole hinzugefügt sind • **cpus**: Anzahl der CPUs des virtuellen Computers • **memory**: Größe des Arbeitsspeichers des virtuellen Computers • **disks**: Anzahl der vom virtuellen Computer verwendeten Datenträger • **state**: Ausführungsstatus des virtuellen Computers Die Auswahlmöglichkeiten sind: ◦ **Wird ausgeführt** ◦ **Angehalten** • **placement_group_id**: Name der IBM-Platzierungsgruppe, die den virtuellen Computer enthält • **nics**: Anzahl der Netzwerkschnittstellen auf dem virtuellen Computer
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	• **name**: Name und Port der NIC im Format **<Name><Port>** • **ip_address**: Auf der NIC konfigurierte IP-Adresse • **mac_address**: MAC-Adresse der NIC • **netmask**: Netzmaske der NIC • **object_id**: ID der NIC • **status**: Status der NIC – VERFÜGBAR

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

Daten, die für virtuelle Cloud-Server IBM erfasst wurden (Fortsetzung)

Tabelle	Felder
Image [cmdb_ci_os_template]	• **name**: Lange Beschreibung der Vorlage. Beispiel: **CentOS 7.0-64 Minimal für VSI**. • **version**: Version des Betriebssystems. Beispiel: **7.0-64 Minimal für VSI** • **object_id**: ID des Image • **guest_os**: Betriebssystem des virtuellen Computers, zum Beispiel Windows, Ubuntu und CentOS
Cloud-Schlüsselpaar [cmdb_ci_cloud_key_pair]	• **name**: Schlüsselbezeichnung • **object_id**: ID des Schlüssels
Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]	• **name**: Name der Sicherheitsgruppe • **object_id**: ID der Sicherheitsgruppe • **short_description**: Hinweise zur Sicherheitsgruppe
Speichervolume [cmdb_ci_storage_volume]	**object_id**: ID des Speichervolume

Für IBM Virtuelle Cloud-Server erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_vm_instance	Positioniert in::Anordnen	cmdb_ci_availability_zone
cmdb_ci_nic	Enthalten in::Enthält	cmdb_ci_vm_instance
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_os_template	Bereitgestellt von::Stellt bereit	cmdb_ci_vm_instance
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_key_pair	Verwendet von::Verwendet	cmdb_ci_vm_instance
cmdb_ci_compute_security_group	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_compute_security_group	Endpunkt implementieren von::Endpunkt implementieren in	cmdb_ci_vm_instance
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_volume	Endpunkt implementieren von::Endpunkt implementieren in	cmdb_ci_vm_instance

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

IBM Cloud-Servicekonto

Daten, die für das Cloud-Servicekonto IBM erfasst wurden

Tabelle	Feld
Cloud-Servicekonto [cmdb_ci_cloud_service_account]	• **name**: Anzeigename des Cloud-Servicekontos • **account_id**: Servicekonto-ID • **object_id**: Cloud-ID des Servicekontos. Diese ist mit der account_id identisch. • **datacenter_type**: Dies ist **cmdb_ci_ibm_datacenter**. • **discovery_credentials**: Die sys_id der Anmeldeinformationen
IBM-Rechenzentrum [cmdb_ci_ibm_datacenter]	• **name**: Anzeigename des Cloud-Servicekontos • **account_id**: Servicekonto-ID • **object_id**: Cloud-ID des Servicekontos. Diese ist mit der account_id identisch. • **datacenter_type**: Dies ist **cmdb_ci_ibm_datacenter**.

Beziehungen erstellt für IBM Cloud-Service-Accounts

CI	Beziehung	CI
cmdb_ci_cloud_service_account	Enthalten in::Enthält	cmdb_ci_availability_zone
cmdb_ci_cloud_service_account	Enthalten in::Enthält	cmdb_ci_ibm_datacenter
cmdb_ci_cloud_service_account	Hostet::Gehostet auf	cmdb_ci_cloud_key_pair
cmdb_ci_cloud_service_account	Hostet::Gehostet auf	cmdb_ci_vm_instance
cmdb_ci_cloud_service_account	Hostet::Gehostet auf	cmdb_ci_lb_service
cmdb_ci_ibm_datacenter	Enthalten in::Enthält	cmdb_ci_availability_zone
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Hostet::Gehostet auf	cmdb_ci_network

Daten gesammelt für Oracle Cloud-Discovery

ServiceNow Discovery nutzt das Discovery-Muster Oracle Cloud Infrastructure (OCI), um Echtzeitelastizität für Unternehmensanwendungen bereitzustellen, indem die autonomen Services von Oracle, die integrierte Sicherheit und das Cloud-Computing kombiniert werden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

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

Apps im Store anfordern

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

Voraussetzungen

Store-App Visibility Content

Stellen Sie sicher, dass die neueste Version der App Visibility Content installiert ist.

Store-App „CMDB CI Class Models“

Stellen Sie sicher, dass die neueste Version der Store-App CMDB CI-Klassenmodelle installiert ist.

Store-App Muster für Discovery und Service-Mapping

Stellen Sie sicher, dass die neueste Version der Store-App Muster für Discovery und Service-Mapping installiert ist.

OCI-Anmeldeinformationen

Stellen Sie sicher, dass Ihre OCI-Anmeldeinformationen konfiguriert sind und dass Ihre privaten und öffentlichen Schlüssel in das RSA-Format konvertiert werden. Weitere Informationen finden Sie unter Generieren Sie Ihre Oracle Cloud Infrastructure(OCI)-Anmeldeinformationen.

Erstellen Sie einen Cloud-Discovery-Zeitplan

Informationen zum Ausführen einer bedarfsgerechten Cloud-Discovery finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Erstellen Sie einen Erkennungszeitplan für die Ausführung in LRZs.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
2. Klicken Sie auf die Schaltfläche **Cloud Discovery**.
3. Wählen Sie im Feld **Provider** die Option **OCI** aus. Füllen Sie das Formular aus, um ein neues Konto zu erstellen, oder wählen Sie ein vorhandenes Konto aus.

Formular „Account hinzufügen“

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für das OCI-Servicekonto ein.
Account-ID	Geben Sie die **Compartment-ID** für OCI ein.
Discovery-Anmeldeinformationen	Wählen Sie die **OCD-Anmeldeinformationen** aus.
Rechenzentrums-URL	Geben Sie einen Wert für das Rechenzentrum ein, z. B. `https://$service.ap-mumbai-1.oraclecloud.com`.
Datencenter-Typ	Wählen Sie das OCI-Rechenzentrum [cmdb_ci_oci_datacenter].

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

4. Filtern Sie auf der Seite **Rechenzentren auswählen**, für welche LZRs Sie die Erkennung ausführen möchten.
5. Wählen Sie auf der Seite **Virtuelle Computer erkennen (optional)** aus, ob Sie die Erkennung von Betriebssystemen für virtuelle Computer ausführen möchten.
6. Wenn Sie fertig sind, navigieren Sie zur Seite **Zeitplan erstellen**, und klicken Sie auf die Schaltfläche **Beenden und ausführen.**

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Oracle-Konfigurationsdaten umfassen die folgenden Tabellen und Felder.

Feld	Beschreibung
Cloud-Datenbank (cmdb_ci_cloud_database)	
name	Name der Datenbank
object_id	Eindeutiger Bezeichner der Datenbank
operational_status	Betriebsstatus der Datenbank
Lieferant	Der Anbieter: **Oracle**.
Typ	Typ der Oracle-Datenbank
Version	Version der Datenbank
state	Status der Datenbank
Anmerkungen	Das Attribut wird für die Löschstrategie ausgegeben.
install_status	Status der Installation
Image (cmdb_ci_os_template)	
name	Image-Name
object_id	Eindeutiger Bezeichner des Images
Version	Version des Gastbetriebssystems
guest_os	Name des Gastbetriebssystems
Servicekonto (cmdb_ci_cloud_service_account)	
name	Name des Kontos
datacenter_type	Datencenter-Typ.
account_id	Eindeutiger Bezeichner des Kontos
object_id	Eindeutiger Bezeichner des Kontos (gleicher Wert wie die Konto-ID)

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

Feld	Beschreibung
discovery_credentials	Anmeldeinformationen im Zusammenhang mit dem Servicekonto
is_master_account	**true**, wenn es sich um das Stamm-Compartment handelt. **false**, wenn es sich nicht um das Stamm-Compartment handelt.
Netzwerk (cmdb_ci_network)	
name	Name des Netzwerks
object_id	Eindeutiger Bezeichner des Netzwerks
cidr	CIDR des Netzwerks
domain_name	Name der Domäne
state	Status des Netzwerks
NIC (cmdb_ci_nic)	
name	NIC-Name
object_id	Eindeutiger Bezeichner der NIC
public_ip	Öffentliche IP-Adresse
mac_address	MAC-Adresse
Primär	Legen Sie entsprechend der Konfiguration **true**/**false** fest.
private_ip	Private IP-Adresse
state	Status der NIC
Speichervolume (cmdb_ci_storage_volume)	
name	Name des Speichervolume.
object_id	Eindeutiger Bezeichner des Speichervolume
state	Status des Speichervolume
volume_id	Eindeutiger Bezeichner des Speichervolume (gleicher Wert wie Konto-ID)
size	Größe des Speichervolume
size_bytes	Größe des Speichervolume in Byte
Subnetz (cmdb_ci_cloud_subnet)	
name	Name des Subnetzes
object_id	Eindeutiger Bezeichner des Subnetzes
cidr	CIDR des Subnetzes
domain_name	Name der Domäne
state	Status des Subnetzes
Virtuelle Maschine (cmdb_ci_vm_instance)	
name	Name der VM
object_id	Eindeutiger Bezeichner der VM
state	Status der VM
memory	Größe des Arbeitsspeichers

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

Feld	Beschreibung
CPUs	Anzahl an CPUs

Tags werden in die Tabelle **cmdb_key_value** eingetragen und beziehen sich auf die relevante CMDB-CI-Ressource. Um dies zu unterstützen, wurden Erweiterungsabschnitte für die folgenden Ressourcen erstellt:

- Autonomous DB
- Exadata-DB
- Bild
- Netzwerk
- NIC
- Speicher-Laufwerk
- Account
- Subnetz
- Virtueller Computer

CI-Beziehungen

Beziehungen, die mithilfe des Musters „Oracle OCI - Availability Domain (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_oci_datacenter	Enthält::Enthalten in	cmdb_ci_availablity_zone

Beziehungen, die mithilfe des Musters „Oracle OCI - Block (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_vm_instance	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_block
cmdb_ci_endpoint_block	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_storage_volume

Beziehungen, die mithilfe des Musters „Oracle OCI - Fault Domain (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_oci_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone

Hinweis: Wenn Sie für einen Teil der LZRs einen Cloud Discovery-Zeitplaner konfigurieren, wird das Muster „Oracle OCI - Fault Domain (LP)“ nicht ausgelöst.

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

Beziehungen, die mithilfe des Musters „Oracle OCI - Image (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_oci_datacenter

Beziehungen, die mithilfe des Musters „Oracle OCI - LDC (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_oci_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account

Beziehungen, die mithilfe des Musters „Oracle OCI - Network (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_network	Gehostet auf::Hostet	cmdb_ci_oci_datacenter

Beziehungen, die mithilfe des Musters „Oracle OCI - NIC Attachment (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_vm_instance	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_subnet
cmdb_ci_vm_instance	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_vnic
cmdb_ci_endpoint_vnic	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_nic
cmdb_ci_cloud_subnet	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_endpoint_subnet

Beziehungen, die mithilfe des Musters „Oracle OCI - NIC (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_nic	Gehostet auf::Hostet	cmdb_ci_oci_datacenter

Beziehungen, die mithilfe des Musters „Oracle OCI - Storage Volume (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_availablity_zone	Enthält::Enthalten in	cmdb_ci_storage_volume
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_oci_datacenter

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

Beziehungen, die mithilfe des Musters „Oracle OCI - Subnet (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_network	Enthält::Enthalten in	cmdb_ci_cloud_subnet

Beziehungen, die mithilfe des Musters „Oracle OCI - Virtual machine (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_oci_datacenter
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_os_template
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_compute_template
cmdb_ci_vm_instance	DR bereitgestellt von::Stellt DR bereit für	cmdb_ci_avaliability_zone
cmdb_ci_avaliability_zone	Enthält::Enthalten in	cmdb_ci_vm_instance

Für VMware Cloud Discovery erfasste Daten

Discovery erfasst Informationen über VMware-Ressourcen in Ihren Cloud-Servicekonten.

Erkennung von Distributed Resource Scheduler (DRS)

VMware Discovery erfasst diese DRS-Einstellungen und speichert sie in der Tabelle „DRS-VM-Konfig.“ [cmdb_ci_drs_vm_config]:

- DRS-Einstellungen von vCenter-Clustern
- DRS-Einstellungen von VMs, die so konfiguriert sind, dass sie das Clusterverhalten überschreiben

DRS-VM-Konfiguration [cmdb_ci_drs_vm_config]

Feldbezeichnung	Spaltenname
Cluster	Cluster
DRS-Verhalten	drs_behavior
DRS-fähig	drs_enabled
Virtueller Computer	virtual_machine

VMware-Tags

VMware Cloud-Discovery erfasst VMware-Tags aus vCenter und speichert sie in der Tabelle „Schlüsselwert“ [cmdb_key_value].

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

Schlüsselwerte [cmdb_key_value]

Feldbezeichnung und -name	Beschreibung
Konfigurationselement [configuration_item]	Referenzierte VM mit angehängtem Tag in vCenter
Schlüssel [key]	Kategoriename des Tag, das auf die Ressource in vCenter angewendet wird
Tag [tag]	Quelle in vCenter, aus der Tags abgerufen werden. In diesem Fall lautet der Wert immer **Tags**.
Wert [value]	Name des Tag, das in vCenter auf die Ressource angewendet wird

Discovery

ServiceNow Discovery ist ein automatisierter Prozess, der alle Komponenten innerhalb der IT-Infrastruktur kontinuierlich scannt und identifiziert. Spielt eine entscheidende Rolle dabei, einen Multisource-CMDB mit den gefundenen Informationen korrekt und aktuell zu halten.

Discovery ist als separates Abonnement vom Rest von Now Platformverfügbar. Details siehe Discovery anfordern.

Discovery unterstützt Datenbankverschlüsselung und Festplattenverschlüsselung. Details siehe Datenbankverschlüsselung .

Erste Schritte

Einführung

- Yokohama
- Discovery erkunden
- Durch ITOM-Transparenz erfasste Daten

Einrichten

- Discovery anfordern
- Discovery einrichten
- MID Server-Installation
- Anmeldeinformationen erstellen und testen
- Migrieren Sie von CAPI zu Mustern

konfigurieren

- Discovery konfigurieren
- Discovery-Eigenschaften
- Discovery-Verhalten erstellen
- Discovery-CI-Klassifizierung erstellen
- Discovery-Prozessklassifizierung erstellen

Verwenden

- Horizontale Erkennung planen
- Schnell-Discovery ausführen
- Discovery-Status

Integrieren und entwickeln

- Aktivieren Sie geplante SCCM-Asset-Intelligence-Importe
- Discovery-APIs im ServiceNow® Developer Site

Problembehandlung und Hilfe

- Monitoring von Erkennungen und Problemlösung
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen

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

- Erkennungsergebnisse validieren
- Cloud-Discovery erkunden
- Zertifikatsbestand-Management
- Fragen im ITOM-Forum stellen oder beantworten
- Kontakt Kundenservice und Support

Discovery Lizenzierung

Bei der für Now Platform® verwendeten Lizenzierungsmethode zahlt Ihre Organisation für die Nutzung von Discovery, das als separate Lizenz von ITOM-Transparenzverfügbar ist. Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung und -Abonnements.

Discovery erkunden

Discovery findet Computer, Server, Drucker, verschiedene IP-fähige Geräte und die Anwendungen, die darauf ausgeführt werden. Es kann dann die CIs in Ihrer CMDB mit den gesammelten Daten aktualisieren.

Horizontale Erkennung und Erkennung von oben nach unten

Es gibt zwei Arten von Erkennung:

Horizontale Erkennung

Die horizontale Erkennung ist eine Technik, die Discovery verwendet, um Ihr Netzwerk zu scannen, Computer und Geräte zu erkennen und dann die CMDB mit den gefundenen CIs zu füllen. Bei der horizontalen Erkennung werden direkte Beziehungen zwischen CIs erstellt, zum Beispiel eine Beziehung vom Typ `Wird ausgeführt auf` zwischen dem CI einer Anwendung und dem CI des tatsächlichen Computers, auf dem die Anwendung ausgeführt wird. Die horizontale Erkennung erkennt keine Business Services und erstellt keine Beziehungen zwischen CIs basierend auf dem Business Service, in dem sie sich befinden.

Erkennung von oben nach unten

Die Erkennung von oben nach unten ist eine Technik, die von Service Mapping verwendet wird, um CIs zu finden und zuzuordnen, die Teil von Business Services wie einem E-Mail-Service sind. Beispielsweise kann die Erkennung von oben nach unten einen Business Service für Websites zuordnen, indem die Beziehungen zwischen einem Apache Tomcat-Webserverdienst, einem Windows-Server und der MSSQL-Datenbank angezeigt werden, in der die Daten für den Business Service gespeichert werden.

Normalerweise arbeiten Service-Mapping und Discovery zusammen und führen zuerst die horizontale Erkennung durch, um CIs zu finden, und anschließend die Erkennung von oben nach unten, um die Beziehungen zwischen Business Services herzustellen, die Sie kennen müssen.

Probes, Sensoren und Muster

Discovery verwendet die folgenden Komponenten für die Suche nach CIs:

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

Sonden und Sensoren

Probes und Sensoren sind Skripts, die Daten auf einem Host erfassen und verarbeiten und anschließend die CMDB aktualisieren. Genauer gesagt: Probes untersuchen die CIs in Ihrem Netzwerk, und Sensoren analysieren die Daten, die von den Probes zurückgegeben werden. Standardmäßig werden mehrere Probes und Sensoren bereitgestellt, die von Ihnen angepasst werden können, um nach anderen Informationen zu suchen. Sie können Probes und Sensoren aber auch selbst erstellen. Sie können auch mehrere Parameter konfigurieren, um das Verhalten einer bestimmten Probe bei jeder Auslösung zu steuern.

Muster

Muster entsprechen wie Probes und Sensoren einer Reihe von Vorgängen, die Daten auf einem Host erfassen, verarbeiten und die CMDB aktualisieren. Muster unterscheiden sich von Probes und Sensoren dadurch, dass sie in NDL (Neebula Discovery Language) anstatt in JavaScript geschrieben sind und in den späteren Phasen des horizontalen Erkennungsprozesses in Aktion treten. Es werden Standardmuster bereitgestellt, Sie können Muster jedoch auch mit dem Musterdesigner anpassen oder erstellen.

Phasen der horizontalen Erkennung

Die Phasen der horizontalen Erkennung lauten:

Discovery folgt diesen Phasen:

Scanvorgang

Discovery sendet eine Probe namens „Shazzam“ an das Netzwerk, um zu sehen, ob häufig verwendete Ports geöffnet sind und ob diese Ports auf Abfragen antworten können. Wenn Shazzam beispielsweise ein Gerät findet, das an Port 135 antwortet, weiß Discovery, dass es sich um einen Windows-Server handelt.

Klassifizierung

Wenn Discovery Geräte oder Computer findet, werden zusätzliche Probes gesendet, um den Gerätetyp oder das Betriebssystem auf dem Gerät zu ermitteln. Beispiel: Discovery sendet die WMI-Probe an einen Windows-Computer, um das Windows 2012-Betriebssystem zu erkennen. Dann verwendet Discovery Datensätze, die als Klassifiziererbezeichnet werden und die Auslöserprobes angeben, die während der nächsten beiden Phasen ausgeführt werden. Wenn Sie Muster verwenden, gibt der Klassifizierer eine Auslöserprobe an, die wiederum ein Muster startet.

Identifizierung

Discovery versucht, weitere Informationen über das Gerät zu sammeln, und versucht dann festzustellen, ob in der CMDB ein CI für das Gerät vorhanden ist. Discovery verwendet dann zusätzliche Probes, Sensoren und Identifier, um vorhandene CIs in der CMDB zu aktualisieren oder neue zu erstellen. Kennungen, auch als Identifikationsregeln bezeichnet, geben die Attribute an, die die Sonden beim Abgleichen von Daten mit den CIs in der CMDB betrachten. Wenn Sie Muster verwenden, verwendet Discovery die entsprechende Identifizierungsregel für den im Muster angegebenen CI-Typ.

Durchsuchen

Der Bezeichner startet zusätzliche im Klassifizierer konfigurierte Sonden. Diese Proben sind speziell als Erkundungsproben konzipiert, um zusätzliche Informationen über das Gerät zu sammeln, z. B. die Anwendungen, die es ausführen, und zusätzliche Attribute wie Arbeitsspeicher, Netzwerkkarten und Treiber. Discovery stellt dann Beziehungen zwischen Anwendungen und Geräten

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

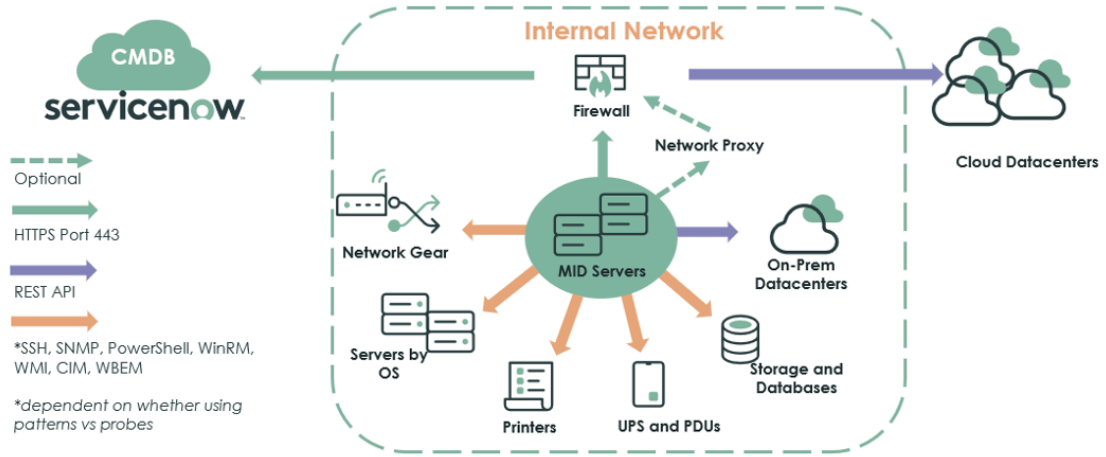
sowie zwischen Anwendungen her. Wenn Sie Muster verwenden, führen die Vorgänge im Muster die Exploration des CI durch.

Kommunikation während der Erkennung über MID Server

Ein MID Server , der eine Instanz ständig nach auszuführenden Probes abfragt, führt die Anweisungen in der Probe oder in dem von der Probe angegebenen Muster aus. Der MID Server gibt dann die Ergebnisse an die Instanz zurück, wo sie von Sensoren verarbeitet werden. Der MID Server speichert keine Erkennungsinformationen.

Der MID Server startet die gesamte Kommunikation über SOAP auf HTTPS. Dies bedeutet, dass die gesamte Kommunikation sicher ist und alle Kommunikationen innerhalb der Firewall des Unternehmens initiiert werden. Es sind keine speziellen Firewall-Regeln oder VPNs erforderlich.

Discovery wird ohne Agents ausgeführt. Das bedeutet, dass zur Erkennung keine permanente Software auf einem Computer oder Gerät installiert werden muss. Daher nutzt der MID Server verschiedene Methoden, um Geräte ohne Agents zu erkennen. Beispielsweise stellt der MID Server mithilfe von SSH eine Verbindung zu einem Unix- oder Linux-Computer her und kann dann den in der Probe angegebenen Standardbefehl ausführen, um Informationen zu erfassen. Ebenso wird SNMP (Simple Network Management Protocol) verwendet, um Informationen von einem Netzwerk-Switch oder Netzwerkdrucker zu erfassen.



Arten der Erkennung

Die folgende Tabelle enthält die Arten der horizontalen Erkennung, die Discovery ausführen kann:

Typ	Beschreibung
Netzwerk-Discovery	Führen Sie diese Art der Erkennung aus, um die internen IP-Netzwerke in Ihrem Unternehmen zu erkennen. Wenn Sie die IP-Adressbereiche in Ihrem Netzwerk bereits kennen, ist die Netzwerkerkennung nicht erforderlich.
CI-Erkennung	Führen Sie diese Art der Erkennung aus, um die Geräte, Computer und Anwendungen in Ihrem Netzwerk zu ermitteln. Das ist im Prinzip der Standardtyp der Erkennung, die am häufigsten ausgeführt wird.
Cloud Discovery	Führen Sie diese Art der Erkennung aus, um AWS- und Azure-Ressourcen in der Cloud Ihres Unternehmens zu ermitteln.

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

Typ	Beschreibung
Serverlose Erkennung	Führen Sie diese Art der Erkennung aus, um Anwendungen auf Hostcomputern zu ermitteln, ohne den Host zuerst erkennen zu müssen. Die serverlose Erkennung basiert auf Mustern zum Untersuchen von CIs auf einem Host.

IP-Serviceaffinität

IP-Serviceaffinität bedeutet, dass die IP-Serviceinformationen, die zur erfolgreichen Erkennung eines Geräts benötigt werden, gespeichert und der IP-Adresse des Geräts zugeordnet werden. Mit diesen Informationen kann Discovery in nachfolgenden Ausführungen anhand des genauen Protokolls das Gerät anvisieren. Discovery zeichnet den IP-Service zusammen mit der IP-Adresse auf. Discovery kann die erfolgreichen IP-Serviceinformationen in der Tabelle „IP-Serviceaffinität“ [ip_service_affinity] speichern.

Beispiel: Auf einem Netzwerkgerät sind sowohl ein SSH-Port als auch ein SNMP-Port geöffnet. Aufgrund des Agent-losen Designs versucht Discovery es zuerst mit SSH. Netzwerkgeräte müssen jedoch über SNMP erkannt werden. Daher schlägt die von Discovery zuerst versuchte SSH-Probe fehl. Dadurch wird die SNMP-Probe ausgelöst, der erfolgreich ist. Durch die Zuordnung von IP-Adressen zu IP-Services verwenden nachfolgende Erkennungsläufe, die auf diese IP-Adresse abzielen, zuerst SNMP, da dies die erfolgreiche Probe war.

Zugehörige Informationen

Discovery einrichten

Monitoring von Erkennungen und Problemlösung

Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren

Der horizontale Erkennungsprozess durchläuft die vier Erkennungsphasen mit Probes, die Informationen auf dem Zielcomputer erfassen, und dann mit Sensoren, mit deren Hilfe Discovery ermittelt, was mit diesen Informationen geschehen soll.

Discovery starten

Ein Benutzer löst die horizontale Erkennung aus, indem er einen Discovery-Zeitplan konfiguriert oder eine On-Demand-Discovery mit Discover now oder Quick Discovery startet. Der Zeitplan gibt eine oder mehrere IP-Adressen oder einen Bereich von IP-Adressen an.

Scanphase

1. Discovery nimmt zuerst die Shazzam-Sonde (und dann die Port-Sonden) und platziert sie in einer Anforderung in der Queue des externen Kommunikationskanals (ECC).
2. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab, führt die Tests im Abgleich mit dem Host aus und erkennt offene Ports.
3. Die Port-Tests prüfen gängige Ports mit verschiedenen Protokollen wie WMI, HTTP, SSH und SNMP.
4. Wenn ein oder mehrere Ports antworten, sendet die Shazzam-Sonde Informationen zum Port über den MID Server zurück an die ECC-Warteschlange.
5. Discovery überprüft die ECC-Warteschlange, um herauszufinden, welche Ports geantwortet haben, wodurch der Maschinentyp identifiziert wird. Wenn beispielsweise Shazzam feststellt, dass der Computer an Port 22 empfangsbereit ist, behandelt Discovery den Computer als UNIX- oder Linux-Computer.

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

Klassifizierungsphase

1. Die Discovery-Anwendung bestimmt, welche Klassifizierungsprüfung an das neu erkannte Gerät gesendet werden soll, indem sie die Informationen im Datensatz der Portprüfung verwendet, die erfolgreich geantwortet haben.
2. Discovery versetzt die Klassifizierungsprüfung in die ECC-Warteschlange.
3. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab und führt die Klassifizierungsprüfung aus.
4. Die Klassifizierungsprüfung ruft zusätzliche Informationen ab, z. B. welche Version des Betriebssystems auf einem Computer ausgeführt wird. Diese Informationen bestimmen die Klasse des von der Discovery gefundenen CIs. Pro erkanntem Gerät gibt es nur eine Klassifizierungssonde.
5. Die Klassifizierungsprüfung sendet Informationen über den MID Server an die Instanz-ECC-Warteschlange zurück.

Identifizierungsphase

1. Discovery bestimmt basierend auf der Klasse des CI und den in allen CI-Klassifiziererdatensätzen angegebenen Kriterien, welcher Klassifizierer zu verwenden ist. Der Klassifizierer gibt an, welche Probes für die nächsten beiden Phasen zu verwenden sind.
2. Discovery setzt die Auslöser-Probe für die Identifizierung für den CI-Klassifizierer in die ECC-Warteschlange. Beispiel: Für einen unter HP-UX ausgeführten Unix-Computer ist der Klassifizierer „HP-UX“ erforderlich, der angibt, dass die Probe „Multi Probe-HP-UX Identity“ die Identifizierung auslöst. Diese Probes verwenden Identifizierungsregeln, um zu bestimmen, ob ein CI in die CMDB eingefügt oder darin aktualisiert werden muss.

   Hinweis: Bei der Auslöser-Probe kann es sich auch um die Probe „Horizontal Pattern“ handeln, der Discovery anweist, die Vorgänge im angegebenen Muster zu verfolgen, anstatt zusätzliche Probes zu versenden. Die Vorgänge im Muster decken sowohl die Identifizierungs- als auch die Erkundungsphase ab. Discovery erkennt anhand des CI-Typs, welche Identifizierungsregeln zu verwenden sind, und führt basierend auf diesen Regeln Einfügungen oder Aktualisierungen in der CMDB durch. Probes und Sensoren werden nicht verwendet.

3. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab und führt die Auslöser-Probe für die Identifizierung aus.
4. Die Identifizierungs-Probe erfasst Identifizierungsdaten für jedes Gerät und sendet diese Daten über den MID Server an die Instanz zurück.
5. Discovery verwendet Sensoren für die Identifizierungs-Probe, um die Informationen zu verarbeiten.
6. Discovery führt die Analyse der CMDB mithilfe von CI-Bezeichnern durch. Discovery kann vorhandene CIs in der CMDB aktualisieren oder neue erstellen.

Erkundungsphase

1. Discovery durchsucht die zugehörige Liste „Auslösertests“ (Auslöser-Probes) im Klassifizierer, um die auszuführende Erkundungs-Probes zu ermitteln.
2. Discovery setzt die Auslöser-Probe für die Erkundung in die ECC-Warteschlange.

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

3. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab und führt die Auslöser-Probe für die Erkundung aus.
4. Die Probes senden Daten über den MID Server an die Instanz zurück, und die Sensoren aktualisieren genau wie in der Identifizierungsphase die CMDB.

Zugehörige Informationen

Muster und horizontale Erkennung

Prozess-Flow der horizontalen Erkennung mit Mustern

Die horizontale Erkennung mit Mustern weist ebenso wie die horizontale Erkennung mit Probes vier Phasen auf. Für die letzten beiden Phasen löst Discovery jedoch keine zusätzlichen Probes-Sätze aus, sondern Vorgänge aus einem Muster.

Scanphase

1. Discovery nimmt zuerst die Shazzam-Sonde (und dann die Port-Sonden) und platziert sie in einer Anforderung in der Queue des externen Kommunikationskanals (ECC).
2. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab, führt die Tests im Abgleich mit dem Host aus und erkennt offene Ports.
3. Die Port-Tests prüfen gängige Ports mit verschiedenen Protokollen wie WMI, HTTP, SSH und SNMP.
4. Wenn ein oder mehrere Ports antworten, sendet die Shazzam-Sonde Informationen zum Port über den MID Server zurück an die ECC-Warteschlange.
5. Discovery überprüft die ECC-Warteschlange, um herauszufinden, welche Ports geantwortet haben, wodurch der Maschinentyp identifiziert wird. Wenn beispielsweise Shazzam feststellt, dass der Computer an Port 22 empfangsbereit ist, behandelt Discovery den Computer als UNIX- oder Linux-Computer.

Klassifizierungsphase

1. Die Discovery-Anwendung bestimmt, welche Klassifizierungsprüfung an das neu erkannte Gerät gesendet werden soll, indem sie die Informationen im Datensatz der Portprüfung verwendet, die erfolgreich geantwortet haben.
2. Discovery versetzt die Klassifizierungsprüfung in die ECC-Warteschlange.
3. Der MID Server prüft die ECC-Warteschlange, ruft die Erkennungsanforderung ab und führt die Klassifizierungsprüfung aus.
4. Die Klassifizierungsprüfung ruft zusätzliche Informationen ab, z. B. welche Version des Betriebssystems auf einem Computer ausgeführt wird. Diese Informationen bestimmen die Klasse des von der Discovery gefundenen CIs. Pro erkanntem Gerät gibt es nur eine Klassifizierungssonde.
5. Die Klassifizierungsprüfung sendet Informationen über den MID Server an die Instanz-ECC-Warteschlange zurück.

Identifizierungs- und Erkundungsphase

Muster vereinheitlichen die Identifizierungs- und Erkundungsphase der Erkennung.

1. Discovery bestimmt basierend auf der Klasse des CI und den in allen CI-Klassifiziererdatensätzen angegebenen Kriterien, welcher Klassifizierer zu verwenden ist. Der Klassifizierer gibt die Probe Horizontal Pattern an, der wiederum das zu startende Muster

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

angibt. Die Probe „Horizontal Pattern“ enthält auch einen Sensor, der die tatsächliche Aktualisierung der CMDB ausführt.

Hinweis: Muster benötigen Applicative-Anmeldeinformationen, um auf Hostcomputern ausgeführte Anwendungen zu finden. Stellen Sie sicher, dass Sie Applicative-Anmeldeinformationen zusammen mit den für den Zugriff auf den Hostcomputer erforderlichen Anmeldeinformationen konfiguriert haben.

2. Die Vorgänge im Muster geben die Aktionen an, die Discovery für die Identifizierungs- als auch die Erkundungsphase ausführen muss. Discovery weiß, welche Identifizierungsregeln je nach CI-Typ im Muster zu verwenden sind, und anhand dieser Regeln fügt Discovery Einfügungen in die CMDB ein oder aktualisiert sie. Nur der Sensor für die horizontale Erkennung wird verwendet. Andere Probes und Sensoren werden nicht verwendet.

Discovery-Administratorarbeitsbereich

Discovery-Administratorarbeitsbereich dient als zentraler Ort für die Überwachung, Nachverfolgung und Durchführung von Discovery-bezogenen Aufgaben. Profitieren Sie von einem optimierten Discovery-Prozess und höherer Effizienz durch die Integration von Zeitplänen, Diagnosen, Optimierungen und mehr in diesem Arbeitsbereich.

Homepage von Discovery-Administratorarbeitsbereich

Auf der Homepage Discovery-Administratorarbeitsbereich finden Sie Tools, mit denen Sie die wichtigsten Discovery-Aufgaben identifizieren und beheben können. Greifen Sie auf kritische Informationen und Anwendungen zu, um Discovery zu bewerten, den Discovery-Prozess zu verwalten und zugehörige Fehler zu beheben.

Um auf Discovery-Administratorarbeitsbereich zuzugreifen, navigieren Sie zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich**.

Schneller Überblick

Zeigen Sie den Discovery-Status mithilfe Datenanzahl und Visualisierungen an, und identifizieren Sie Unregelmäßigkeiten, die sich auf die Discovery auswirken könnten. Die angezeigte Anzahl stellt Daten aus den letzten 24 Stunden dar, und die Trendlinie zeigt Aktivitätsmuster aus den letzten 7 Tagen oder länger. Um detaillierte Informationen zu erhalten, wählen Sie die entsprechende Kachel aus.

Wählen Sie das Symbol **Weitere Optionen** (⋮) und dann **Aktualisieren**, um die Daten für jede Visualisierung in diesem Abschnitt zu aktualisieren.

Hinweis: Updates werden erst angezeigt, wenn die tägliche Aufgabe Performance Analytics abgeschlossen ist. Weitere Einzelheiten finden Sie unter Sammeln Sie Daten für Platform Analytics and Reporting-LösungenPlatform Analytics-Lösungen .

Abgebrochene Erkennungen

Führen Sie einen Drilldown durch, um abgebrochene Erkennungen anhand der angezeigten Daten zu analysieren. Flache Abschnitte der Trendlinie zeigen keine Abbrüche an, während Spitzen abgebrochene Erkennungen darstellen. Wenn Sie diese Visualisierung auswählen, werden Sie zu einer der Registerkarten für die Seite **„Discovery-Zeitpläne“** weitergeleitet. Um zugehörige abgebrochene Discovery-Status anzuzeigen, wählen Sie die Registerkarte **Discovery-Status**.

Last der ECC-Warteschlange

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

Beheben Sie potenzielle Discovery-Probleme mithilfe einer Datenvisualisierung von MID-Server Aufgaben, die sich derzeit in der ECC-Warteschlange (External Communications Channel) befinden. Ungewöhnliche Spitzen in der Trendlinie können auf Aktivitäten hinweisen, die den Discovery-Prozess stören könnten. Wenn Sie diese Visualisierung auswählen, werden Sie zum ECC-Warteschlangenprotokoll weitergeleitet. Weitere Informationen finden Sie unter ECC-Warteschlange für Discovery.

Fehleraufgaben

Die angezeigte Anzahl stellt die Discovery-Fehleraufgaben dar, die in den letzten 24 Stunden geöffnet wurden, während die Visualisierung die Fehleraufgaben zeigt, die in den letzten 7 Tagen oder länger geöffnet wurden. Wenn Sie diese Visualisierung auswählen, werden Sie zur Seite **„Fallverwaltung“** weitergeleitet, auf der Sie alle Discovery-Fehleraufgaben anzeigen können.

Discovery -Administratoraufgaben

Überprüfen Sie die drei kritischsten Discovery-Fehleraufgaben. Wählen Sie die Schaltfläche **Aufgabe bearbeiten** aus, um auf die Detailseite zuzugreifen, auf der Sie die Fehleraufgabe zuweisen oder aktualisieren oder Arbeitsnotizen hinzufügen können. Um alle Aufgaben für Discovery-Fehler anzuzeigen und zu verwalten, wählen Sie **Alle anzeigen** aus, um auf die Seite **„Fallverwaltung“** zuzugreifen.

Hinweis: Dieser Abschnitt konzentriert sich ausschließlich auf Discovery-Fehler, denen Aufgaben zugeordnet sind, und nicht auf alle Discovery-Fehler.

Discovery-Optimierungsempfehlung

Optimieren Sie die Einstellungen für Discovery und MID-Server mit automatisierten Vorschlägen, die aus Scans Ihrer -Instanz abgeleitet werden. Diese Ergebnisse identifizieren potenzielle Probleme und sind in der Reihenfolge ihrer Relevanz angeordnet. Wenn Sie ein Ergebnis auswählen, gelangen Sie zur Seite **„Abstimmungsprüfung“**, auf der Sie weitere Details finden.

Schnell-Discovery

Erkennen Sie Geräte in Ihrem Netzwerk außerhalb einer geplanten Discovery. Geben Sie eine einzelne IP-Adresse, mehrere durch Kommas getrennte IP-Adressen oder ein IP-Netzwerk ein, wie im folgenden Beispiel:

- IP-Netzwerkadresse: 10.0.1.0/24
- IP-Adressbereich – 10.0.2.1–10.0.2.15
- IP-Adressliste – 10.0.3.176,10.0.3.222,2001::100,2600:1bdc::fffe

Wählen Sie ein MID-Serveroder ein MID-Cluster aus, oder aktivieren Sie Discovery, um MID-Server automatisch auszuwählen.

ITOM-Transparenz Apps

Erweitern Sie die Funktionalität von Discovery-Administratorarbeitsbereich durch die Integration zusätzlicher ITOM-Transparenz -Anwendungen. Wenn Sie **Alle anzeigen**auswählen, können Sie sowohl die in Ihrer Instanz installierten Anwendungen als auch andere, die für die Installation verfügbar sind, anzeigen. Weitere Informationen finden Sie unter ITOM-Transparenz -Apps mit Discovery-Administratorarbeitsbereich anzeigen und filtern.

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

Erkenntnisse

Erhalten Sie Anleitungen zur Verwaltung des Discovery-Prozesses und zur Behebung von Discovery-Fehlern mit ITOM-Transparenz Knowledge Base. Greifen Sie auf relevante Artikel aus dem ServiceNow Knowledge Basezu, erkunden Sie Blog-Posts, oder sehen Sie sich Video-Tutorials mit Anleitungen an, um weitere Informationen zu erhalten.

Hinweis: Um die Ressourcen in diesem Abschnitt anzuzeigen, vergewissern Sie sich, dass Sie ITOM Content Service Version 1.2.8 installiert haben.

Voraussetzungen

Plugins und Anwendungen ServiceNow Store :

- Discovery
- Visibility Content
- CMDB-Arbeitsbereich
- Discovery-Administratorarbeitsbereich

Rollen

Die folgenden Rollen haben Zugriff auf Discovery-Administratorarbeitsbereich :

admin oder discovery_admin.

Abhängigkeiten

Eine Liste der Discovery-Administratorarbeitsbereich Anwendungsabhängigkeiten finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Transparenz.

Discovery-Administratorarbeitsbereich Zeitpläne

Die Seite Discovery-Administratorarbeitsbereich Zeitpläne bietet einen einheitlichen Arbeitsbereich, um Einblicke in die Leistung aller Ihrer Erkennungen zu erhalten. Der -Arbeitsbereich bietet schnellen Zugriff auf die Verwaltung von Discovery -Zeitplänen und Discovery -Status.

Über die Seite Discovery-Administratorarbeitsbereich Zeitpläne können Discovery -Administratoren sofort auf alle täglichen Discovery -Aktivitäten zugreifen.

Um auf die Seite Discovery-Administratorarbeitsbereich Zeitpläne zuzugreifen, navigieren Sie zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Zeitpläne**.

Schlüsselfunktionen

Übersicht

Auf der Übersichtsseite Discovery-Administratorarbeitsbereich können Sie mithilfe leistungsstarker Visualisierungen datengesteuerte Entscheidungen treffen.

Datenvisualisierungen

Berichtstitel	Typ	Beschreibung
Zeitpläne nach Ort	Karte	In diesem Bericht werden Discovery -Zeitpläne nach Ort angezeigt.

Automatische Übersetzung

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

Datenvisualisierungen (Fortsetzung)

Berichtstitel	Typ	Beschreibung
		Wählen Sie einen Bereich der Karte aus, um Discovery -Zeitpläne in der ausgewählten Region anzuzeigen.
Zeitpläne insgesamt	Liniendiagramm	In diesem Bericht wird die Gesamtzahl der in den letzten 24 Stunden ausgeführten Zeitpläne Discovery angezeigt. Wählen Sie das Diagramm aus, um Discovery -Zeitpläne anzuzeigen.
Fehler nach Kategorie	Ringdiagramm	In diesem Bericht wird die Anzahl aller Discovery -Fehler nach Kategorie angezeigt. Wählen Sie eine Kategorie aus, um sie dem Diagramm hinzuzufügen oder daraus zu entfernen.
Discovery-Versuche insgesamt	Linien- und Flächendiagramm	In diesem Bericht wird die Anzahl aller Discovery abgeschlossenen und stornierten Versuche angezeigt.

Discovery-Zeitpläne

Über die Registerkarte Discovery-Administratorarbeitsbereich Discovery Zeitpläne haben Sie schnellen Zugriff auf alle Ihre Discovery -Zeitpläne. Sie können einen Discovery -Zeitplan auswählen, um ausführliche Details anzuzeigen und Zeitplanfeldparameter zu aktualisieren. Weitere Einzelheiten finden Sie unter Horizontale Erkennung planen.

Discovery-Status

Die Statusseite Discovery-Administratorarbeitsbereich Discovery zeigt den aktuellen Status der geplanten Erkennungen an. Sie können eine Discovery Statusnummer auswählen, um detaillierte Informationen anzuzeigen. Weitere Einzelheiten finden Sie unter Discovery-Status.

Voraussetzungen

Bestätigen Sie, dass Sie die neueste Version von CMDB-Arbeitsbereichinstalliert haben.

Rollen

Die folgenden Rollen haben Zugriff auf Discovery-Administratorarbeitsbereich :

- Administrator
- discovery_admin

Erstellen Sie einen neuen IP-basierten Discovery-Zeitplan

Verwenden Sie das Dashboard „Discovery-Administratorarbeitsbereich“, um IP-basierte Discovery-Zeitpläne aus der Tabelle „Zeitpläne“ zu erstellen.

Voraussetzungen: Store-App-Version 1.5.0

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

Erstellen Sie auf der Registerkarte **Discovery-Zeitpläne** einen neuen Zeitplan, indem Sie in der Tabelle Discovery-Zeitpläne **Neu** auswählen. Dieser Zeitplan gilt nur für IP-basierte Discovery. Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Discovery-Details

Name: Geben Sie einen Namen für den Discovery-Zeitplan ein

Standort: Wählen Sie einen der verfügbaren Discovery-Standorte aus. Dieses Feld ist nicht erforderlich.

IP-Bereiche auswählen:

- **Vorhandenen IP-Bereichssatz verwenden:** Wählen Sie aus vorhandenen IP-Bereichssätzen aus. Weitere Informationen zu IP-Bereichsgruppen finden Sie unter Konfiguration der Discovery-IP-Adresse.

- **Neue IP-Bereiche eingeben:** Geben Sie eine kommagetrennte Liste mit IPv4-Adressbereichen, IPv4-Netzwerken oder einzelnen IP-Adressen ein, die die hinzuzufügenden Bereiche beschreiben. Sie können einen Namen eingeben, um den IP-Bereichssatz zu speichern.

Wählen Sie Ihren MID-Server aus

MID-Server automatisch auswählen: Ein verfügbarer MID-Server wird automatisch ausgewählt, wenn der Discovery-Zeitplan ausgeführt wird. Weitere Informationen finden Sie unter Automatische MID-Server-Auswahl.

Cluster von MID-Servern: Wählen Sie einen vorhandenen MID-Server-Cluster aus, oder erstellen Sie einen neuen. Cluster bieten Failover-Schutz und Lastenausgleich zwischen MID Servern. Weitere Informationen finden Sie unter Ein MID-Server-Cluster konfigurieren .

MID-Server: Wählen Sie einen bestimmten MID-Server für die Ausführung des Discovery-Zeitplans. Alle MID-Server werden angezeigt, aber nur die aktiven und validierten können einen Discovery-Zeitplan erfolgreich ausführen.

Zeitplandetails

Zu geplanter Zeit ausführen: Verwenden Sie die Felder, um zu definieren, wann der Zeitplan ausgeführt wird.

Nach Serie ausführen: Wählen Sie diese Option, um den Zeitplan nach einem anderen vorhandenen Discovery-Zeitplan auszuführen. Wenn Sie einen vorhandenen Zeitplan auswählen, wird eine Beziehungszuordnung aller anderen zugeordneten Zeitpläne angezeigt.

Bei Bedarf ausführen: Der Zeitplan wird nur ausgeführt, wenn er manuell ausgelöst wird. Der Zeitplan kann ausgelöst werden, indem Sie am Ende dieses Setups **Beenden und ausführen** auswählen oder in der Tabelle „Zeitpläne“ zum Zeitplan navigieren und **Jetzt erkennen**auswählen.

Maximale Laufzeit: Legt ein Limit für die Ausführungsdauer eines Zeitplans fest, nach der der Zeitplan abgebrochen wird. Grenzwerte können die Leistung des MID-Servers verbessern und Probleme verhindern.

Fertigstellen: Nach der Auswahl werden alle bereitgestellten Informationen validiert. Ein Discovery-Zeitplan wird erstellt, und Sie werden zu seinem Eintrag in der Tabelle „Zeitpläne“

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

weitergeleitet. Sie können die Informationen des Zeitplans bearbeiten oder ihn ausführen, indem Sie **Jetzt erkennen**auswählen.

Beenden und ausführen: Nach der Auswahl werden alle angegebenen Informationen validiert. Dann wird im Hintergrund ein Discovery-Zeitplan erstellt, und ein Discovery-Status wird erstellt, und der Zeitplan wird ausgeführt.

Discovery-Administratorarbeitsbereich Diagnose

Die Diagnose ermöglicht Ihnen das Priorisieren und Behandeln von Discovery Zeitplanfehlern. Erstellen und verwalten Sie Fehleraufgaben, um den Fortschritt bei der Behebung von Fehlern nachzuverfolgen.

Diagnose

Auf der Seite **„Diagnose“** werden alle Fehler aus allen Erkennungen angezeigt. Für jeden Eintrag in der Tabelle **„Discovery-Fehler“** können Sie eine neue Fehleraufgabe erstellen oder den Fehler mit den Schaltflächen **Aufgabe erstellen** und **Ignorieren** ignorieren. Einträge, denen bereits eine Fehleraufgabe zugeordnet ist, haben stattdessen eine Schaltfläche **Aufgabe bearbeiten** und geben den Namen und die Priorität der Aufgabe an.

Verwenden Sie die Filteroptionen, um Fehler zu priorisieren und zu beheben. Sie können mit dem Dropdown-Menü **Zeitplan** nach Discovery-Zeitplan filtern oder mit der **Suchleiste** nach dem Namen des Fehlers suchen. Die Ergebnisse können auch mit dem Dropdown-Menü **Sortieren** nach in aufsteigender oder absteigender Reihenfolge mit den folgenden Optionen organisiert werden: Code, Priorität und Gesamtfehler.

Die Fehlerdatensätze können auch mit den Dropdown-Menüs **Filter** und **Hat Aufgabe** gefiltert werden. Im Menü **„Filter“** können Sie auswählen, ob nur Fehler im Zusammenhang mit CMDB, Konfiguration, Anmeldeinformationen, Intern oder Netzwerk angezeigt werden sollen. Es können mehrere Kategorien gleichzeitig ausgewählt werden. Im Menü **Hat Aufgabe** werden entweder alle Fehlerdatensätze, diejenigen, die eine Aufgabe haben, oder die, die keine Aufgabe haben, angezeigt.

Für jeden Eintrag in der Tabelle **„Discovery-Fehler“** kann die Zahl **„Fehler insgesamt“** ausgewählt werden, um zur **Seite „Fehlerstatistiken“**zu navigieren. Die Seite enthält Informationen zum Fehler und empfiehlt **Anweisungen**sowie einen zugehörigen Knowledge Base-Artikel. Wenn dem Fehler eine Fehleraufgabe zugeordnet ist, wird deren Aufgabennummer angezeigt, und es kann über die zugehörige Schaltfläche darauf zugegriffen werden.

Das Dropdown-Menü **Aktion** enthält vorgeschlagene Aktionen basierend auf der Art des Fehlers und wird mit der Seite Fehleraufgabe geteilt. In der Tabelle **„Fehler“** kann das Dropdown-Menü **Aktion für ausgewählte** IP-Adressen die Fehler einzelner IP-Adressen ignorieren, ihre Discovery wiederholen, sie der globalen Ausschlussliste hinzufügen oder ihren Shazzam-Portstatus überprüfen.

Fallmanagement

Die Seite **„Fallverwaltung“** bietet eine Übersicht über die Status von Fehleraufgaben. Alle Fehleraufgaben können ausgewählt werden, um zu ihrem Fehleraufgaben-Datensatz zu navigieren. Neue Aufgaben können erstellt und über die Schaltfläche **Aufgabe erstellen** mit vorhandenen Fehlern verknüpft werden. Der Anzeigestil kann mit den Schaltflächen **Kanban-Tafelansicht** und **Listenansicht** geändert werden.

Support-Tools

Auf der Seite **„Supporttools“** finden Sie Tools zur Untersuchung und Fehlerbehebung Ihrer Instanz. Das Tool **„CAPI zu Mustern“** hilft Ihnen, Ihre Cloud-Discovery von der Verwendung

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

von Cloud-API-REST-Aufrufen zur Verwendung von Mustern zu migrieren. Das Tool **für die Migration von Probes zu Muster** migriert ältere Probes zu neuen, flexibleren und effizienteren Mustern. Mit dem Tool **Häufig erkannte CIs erkennen** wird ermittelt, welche CIs häufiger erkannt werden als andere.

Protokolle

Auf der Seite **„Protokolle“** können Sie auf die Protokolle der **ECC-Warteschlange**, **Discovery-Protokolle**und **Discovery-Musterprotokolle**zugreifen. Diese Protokolle können gefiltert werden, und jeder Eintrag kann ausgewählt werden, um weitere Details anzuzeigen. Das Überprüfen der Protokolle kann bei der Diagnose und Behebung von Fehlern hilfreich sein.

Ignorierte Fehler

Auf der Seite **„Ignorierte Fehler“** werden alle in den letzten 30 Tagen ignorierten Fehler aufgezeichnet. Fehler, die älter als 30 Tage sind, werden gelöscht. Sie können einen Fehler mithilfe der Schaltfläche **„Ignorieren rückgängig machen“** wieder der Tabelle **„Discovery-Fehler“** hinzufügen.

Discovery-Administratorarbeitsbereich Inhalt 360

Mit Discovery-Administratorarbeitsbereich Content 360 können Sie Anwendungen erkennen und Anwendungsvorschläge basierend auf maschinellem Lernen oder Crowdsourcing-Ressourcen bewerten. Erstellen Sie dann mit einem einzigen Klick Konfigurationselemente.

Discovery-Administratorarbeitsbereich Content 360 verwendet Datenvisualisierungen, um eine umfassende Transparenz der Anwendungen Ihrer Infrastruktur und der verfügbaren Ressourcen für die Erstellung von Anwendungskonfigurationselementen (CIs) zu bieten. Sie bietet Zugriff auf eine Liste von Klassifizierern, die der Discovery hinzugefügt werden sollen.

Um auf die Seite Discovery-Administratorarbeitsbereich Inhalt 360 zuzugreifen, navigieren Sie zu **Arbeitsbereiche** > *Discovery-Administratorarbeitsbereich* > **Content 360**.

Schlüsselfunktionen

Von KI vorgeschlagene Fingerabdrücke für Anwendungen

Zeigen Sie eine Liste der vorgeschlagenen Anwendungen mit Fingerabdrücken an, die Sie dem Discovery-Prozess über die von KI vorgeschlagene Fingerabdruckfunktion hinzufügen können. Sie können dann einen Gruppennamen wählen, um ausführliche Details zu einer Anwendung anzuzeigen.

- Ändern Sie bestimmte Details, z. B. den Namen des Discovery-Musters oder die vorgeschlagene Klasse CMDB.
- Zeigen Sie zusätzliche Informationen zu Prozessbeispielen und zugehörigen Servern an.
- Wählen Sie diese Option aus, um angezeigte Vorschläge bei der nächsten Ausführung von Discovery zu ignorieren.
- Fügen Sie bei der nächsten Ausführung von Discovery Vorschläge zu Configuration Management Database (CMDB) hinzu.

Weitere Informationen zur Discovery auf Grundlage von Anwendungsfingerabdrücken finden Sie unter Anwendungen basierend auf Fingerabdrücken erkennen.

Anwendungs-CIs erkannt

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

Überwachen Sie Informationen zu Anwendungs-CIs, die basierend auf Anwendungsfingerabdrücken oder Vorschlägen ITOM Content Service von über Discovery-Administratorarbeitsbereich erkannt wurden. Ein Kreisbericht veranschaulicht die Gesamtzahl der erkannten anwenderdefinierten Anwendungs-CIs, während ein Balkenbericht die fünf häufigsten erkannten Anwendungs-CIs, die innerhalb der letzten zwei Tage erstellt und nach Klasse gruppiert dargestellt werden.

ITOM Content Service

ITOM Content Service sammelt Fingerabdrücke von unbekannten Anwendungen aus verschiedenen Umgebungen. KI-Bibliothekare analysieren diese Fingerabdrücke und erstellen dedizierte Klassifizierer, die wöchentlich aktualisiert und an Sie gesendet werden. Da neue IT-Produkte schnell auf den Markt kommen, ermöglicht Ihnen diese Funktion die Aktualisierung der Transparenz und bietet folgende Vorteile:

- Es überprüft jede Woche die Produkte, die Sie derzeit verwenden, und liefert neue Anwendungsfingerabdrücke.
- Es identifiziert irrelevante Prozesse, die keine geeigneten Kandidaten für CIs sind.
- Basierend auf KI hilft es Ihnen, Fingerabdrücke laufender Prozesse und SNMP-Objektbezeichner (Simple Network Management Protocol) (OIDs) zu identifizieren und die CIs zu erstellen, die Sie für die Überwachung Ihrer Infrastruktur benötigen.
- Erkennt eine höhere Anzahl von Produkten mithilfe von KI-Fähigkeiten, die laufende Anwendungsprozesse gruppieren und klassifizieren.

Weitere Informationen zu ITOM Content Service finden Sie unter ITOM Content Service .

Datenfreigabe für *ITOM Content Service*

Das Continuance Delivery System (CDS), eine ServiceNow® -Technologie, synchronisiert Daten zwischen der Instanz der Datenservices, die Daten speichert und verteilt, und den Kundeninstanzen, indem nur die Prozesse und SNMP-OIDS-Daten verwendet werden. Mit der Funktion ITOM Content Service über das CDS können Sie die Freigabe von Anwendungsfingerabdruck-Prozessdaten aktivieren. Diese Daten können von KI-Bibliothekaren getaggt und klassifiziert werden, sodass ITOM Content Service jede Woche neue CIs liefern kann. Ihre Daten werden für die Instanz ServiceNow® in einer sicheren Umgebung freigegeben. Sie haben die Gewissheit, dass keine personenbezogenen Daten preisgegeben werden und alle Informationen anonym bleiben. Die Teilnahme ist optional und Sie können die Teilnahme jederzeit abwählen. Weitere Informationen finden Sie unter Daten freigeben für ITOM Content Service.

Voraussetzungen

Erforderliche Plugins für ITOM Content Service:

- Discovery
- Normalisierungsdatenservices

Rollen

Die folgenden Rollen haben Zugriff auf Discovery-Administratorarbeitsbereich Content 360:

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

- Administrator
- discovery_admin

Erkennen Sie Anwendungen mithilfe von Anwendungsfingerabdrücken oder ITOM Content Service

Erkennen Sie Anwendungen anhand von Vorschlägen basierend auf ServiceNow Predictive Intelligence oder ServiceNow ITOM Content Service, um Konfigurationselemente zu erstellen.

Vorbereitungen

Erforderliche Rolle: admin oder discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Überprüfen Sie Anwendungsvorschläge basierend auf Anwendungsfingerabdrücken oder ITOM Content Service, und fügen Sie sie der Discovery hinzu.

- Die auf Fingerabdrücken basierte Erkennung nutzt Algorithmen, um laufende Prozesse zu identifizieren und in Gruppen zu organisieren. Diese Prozessgruppen werden zu vorgeschlagenen Anwendungen oder Kandidaten. Sie überprüfen vorgeschlagene Anwendungen und wählen aus, welche erkannt werden sollen. Die Liste der vorgeschlagenen Anwendungen wird stündlich aktualisiert. Weitere Informationen finden Sie unter Anwendungen basierend auf Fingerabdrücken erkennen.
- ITOM Content Service identifiziert die Produkte, die Sie derzeit verwenden, und liefert jede Woche neue Produktvorschläge. Weitere Informationen finden Sie unter ITOM Content Service.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Content 360**.
2. Wählen Sie einen Anwendungsvorschlag aus, der der Discovery basierend auf Anwendungsfingerabdrücken oder ITOM Content Servicehinzugefügt werden soll.

Vorschlagsquelle	Aktionen
Fingerabdrücke der Anwendung	**a.** Wählen Sie das Widget **für vorgeschlagene KI-Anwendungsfingerabdrücke** aus. **b.** Wählen Sie den Vorschlag unter **Suggested Group Name (Vorgeschlagener Gruppenname)**aus. **c.** Überprüfen Sie im angezeigten Formular mit den Fingerabdruckfingerabdrücken die Informationen. Informationen zu den Formularfeldern finden Sie unter Vorschlagsformular für Fingerabdrücke der Anwendung. **d.** Bestimmt, ob der Vorschlag der Discovery hinzugefügt werden soll. ▪ Wenn der Vorschlag nicht relevant ist und Sie ihn nicht hinzufügen möchten, wählen Sie **Ignorieren**aus. ▪ Wenn Sie ihn hinzufügen möchten, wählen Sie **Zu Discovery hinzufügen**.

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

Vorschlagsquelle	Aktionen
ITOM Content Service	**a.** Bestätigen Sie, dass Sie ITOM Content Serviceaktiviert haben. **Hinweis:** Wenn die **Option Aktivieren** angezeigt wird, haben Sie die Teilnahme noch nicht aktiviert. Weitere Informationen finden Sie unter Daten freigeben für ITOM Content Service. **b.** Wählen Sie das Widget **Inhaltsservicevorschläge** aus. **c.** Überprüfen Sie die Liste, und wählen Sie den Namen des entsprechenden Vorschlags aus, um detailliertere Informationen anzuzeigen. **Hinweis:** Sie können mehrere Vorschläge auswählen, um sie der Discovery gleichzeitig hinzuzufügen. Aktivieren Sie das Kontrollkästchen neben jedem Vorschlag, und wählen Sie dann **Aktivieren**aus. **d.** Bestimmt, ob der Vorschlag der Discovery hinzugefügt werden soll. ▪ Wenn der Vorschlag nicht relevant ist und Sie ihn nicht hinzufügen möchten, kehren Sie zur Liste der vorgeschlagenen Anwendungen zurück. ▪ Wenn Sie Änderungen am Vorschlag vorgenommen haben, ihn der Discovery jedoch nicht hinzufügen möchten, wählen Sie **Speichern**aus. ▪ Um den Vorschlag zur Discovery hinzuzufügen, wählen Sie **Aktivieren aus**.

Discovery-Administratorarbeitsbereich Einblicke

Die Registerkarte Discovery-Administratorarbeitsbereich Einblicke bietet Zugriff auf spezielle Widgets, Dashboards und Berichte, um das IT Operations Management und die Infrastrukturüberwachung Ihrer Organisation zu nutzen. Dabei werden die Fähigkeiten von Discovery zur Verbesserung der betrieblichen Transparenz und der Integrität der Infrastruktur genutzt.

Voraussetzungen

Um auf die Registerkarte „Einblicke“ zuzugreifen, stellen Sie sicher, dass das Plugin Discovery installiert und aktiv ist.

Sie müssen auch über die aktuelle Version ServiceNow® Store der folgenden Anwendungen verfügen:

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

- Visibility Content
- CMDB-Arbeitsbereich
- Discovery-Administratorarbeitsbereich
- (optional) Muster für Discovery und Service-Mapping

Sie müssen über die Rolle admin oder discovery_admin verfügen, um auf Discovery-Administratorarbeitsbereich zuzugreifen.

Informationen, auf die über die Registerkarte „Einblicke“ zugegriffen wird

Über die Registerkarte „Einblicke“ können Sie auf die folgenden Informationen zugreifen:

- Oracle Globale GLAS-Datensammlung (Global License Advisory Services)
- Kubernetes Explorer
- Nutanix-Dashboard
- MID-Server-Dashboard
- Agent Health-Dashboard
- Erkennen Sie fehlende Rechenressourcen
- Shazzam-Einblicke
- VM-Explorer

Erkennen Sie fehlende Rechenressourcen

Verwenden Sie Discovery-Administratorarbeitsbereich , um Compute-Ressourcen zu identifizieren, die in letzter Zeit nicht erkannt wurden. Führen Sie eine Schnell-Discovery aus, um die Daten der Ressource zu aktualisieren. Wenn eine Ressource nicht erkennbar ist, ignorieren Sie sie, und schließen Sie sie aus dem Bericht aus. Dieses Verfahren hilft Ihnen, Ihre Ressourcen optimal zu nutzen.

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig enthält der Bericht die folgenden Informationen:

- Von der Plattform ServiceNow® und ServiceWatch-Suiteerkannte Ressourcen.
- Ressourcen, die seit der Ausführung der vorherigen Discovery vor 14 Tagen nicht erkannt wurden oder die im Feld **Neueste Erkennung** kein Discovery-Datum aufweisen.
- Ressourcen, die kein Tag zum **Ignorieren von Berichten** aufweisen.

Vorbereitungen

Erforderliche Rolle: admin oder discovery_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** > **Fehlende Rechenressourcen aus Discovery**.
2. Führen Sie eine Schnell-Discovery für eine Ressource aus.
   a. Wählen Sie in der Liste die Ressource aus.
   b. Wählen Sie **Schnell-Discovery**aus.
   c. Wählen Sie MID-Server aus, um eine Discovery auszuführen.

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

Die **Liste „IP eingeben“** wird automatisch ausgefüllt.

d. Wählen Sie in den Feldern **MID-Auswahlmethode** und **MID-Server** die gewünschten Optionen aus.
Weitere Informationen finden Sie unter MID-Server-Auswahl .

e. Wählen Sie **Discovery ausführen**aus.

3. Wenn die Discovery der Ressource fehlgeschlagen ist, ignorieren Sie die Ressource, und schließen Sie sie aus dem Bericht aus.

   Wenn Sie eine Ressource erfolgreich ignorieren, wird ein grünes Banner angezeigt, um anzuzeigen, dass die Ressource im Bericht ignoriert wird. Wenn die Ressource ignoriert wird, wird sie aus dem Bericht **„Fehlende Rechenressourcen“** entfernt.

   a. Wählen Sie in der Liste die Ressource aus.

   b. Wählen Sie **In Bericht ignorieren aus**.

4. Wahlweise: Wenn Sie die Discovery für eine zuvor ignorierte Ressource aktivieren möchten, entfernen Sie das **Ignorieren aus dem Berichts** -Tag.

   a. Navigieren Sie zu **Alle**, und geben Sie den Filter `cmdb_ci_server.list`ein.

   b. Personalisieren Sie die Liste so, dass sie die Spalte **„Tags“** enthält, indem Sie die Schaltfläche „Einstellungen“ verwenden.

   c. Suchen Sie nach dem Ressourcennamen.

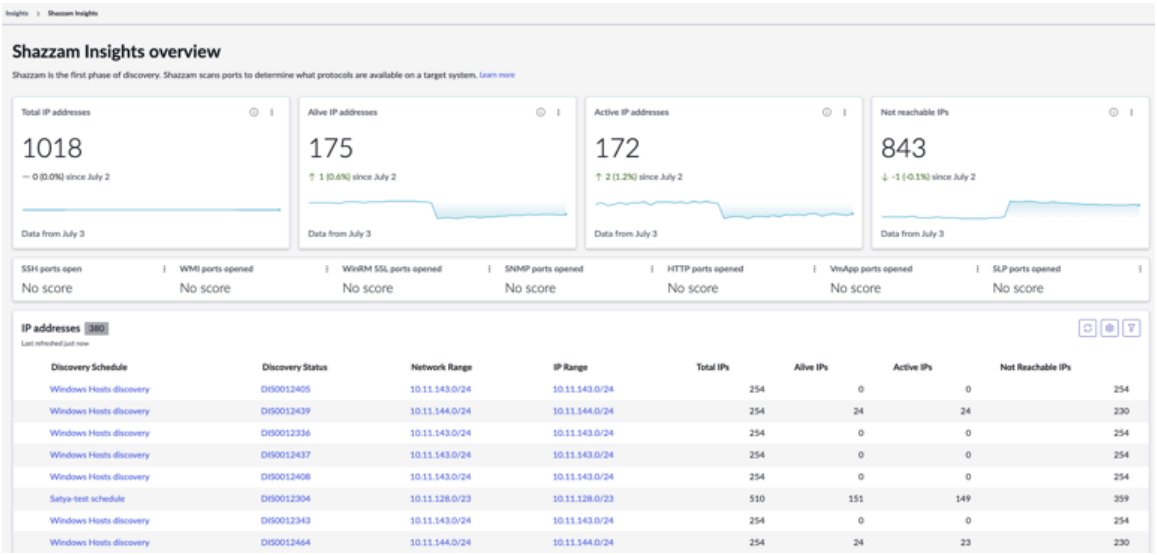
   d. Wählen Sie im Feld **Tags** die Option zum Entfernen aus.

Ergebnisse

Wenn die Schnell-Discovery erfolgreich war, wird die Instanz zum **Discovery-Status** -Dashboard umgeleitet. Wenn die Ressource erkannt wird, wird sie aus dem Bericht **„Fehlende Rechenressourcen“** entfernt und in der Tabelle „Server“ [cmdb_ci_server] aufgeführt.

Shazzam-Einblicke-Dashboard

Discovery-Administratorarbeitsbereich zeigt Ihre Informationen zu Port-Scans, die IP-Adressnutzung und die Zeitpläne Discovery an.



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

Erforderliche Now Platform-Rollen

- discovery_admin
- Administrator

Voraussetzungen

Vergewissern Sie sich, dasseingerichtet ist

- Discovery.
- Discovery-Administratorarbeitsbereich 1.3.1. (Store-Release August 2024).
- CMDB-Arbeitsbereich
- Visibility Content

Aktivieren Sie die -Datenerfassung

Erforderliche Rolle: system_administrator.

Legen Sie die Eigenschaft *glide.discovery.shazzaminsights* auf **true**fest.

Führen Sie einen Discovery -Zeitplan aus. Weitere Informationen finden Sie unter: Erkennungen im Netzwerk ausführen.

Greifen Sie auf das Dashboard „Shazzam-Einblicke“ zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** > **Shazzam-Einblicke**.

Indikatoren

Gesamtzahl der IP-Adressen

Die Gesamtzahl und der Trend der IP-Adressdaten, die Shazzam seit einem bestimmten Datum gescannt hat. Die Daten werden aus der Tabelle Shazzam-Zusammenfassung [shazzam_summary] extrahiert.

Aktive IP-Adressen

Anzahl und Trend der reaktionsfähigen und pingbaren IP-Adresseund, die von Shazzam seit einem bestimmten Datum gescannt wurden. Die Daten werden aus der Tabelle Shazzam-Status [shazzam_status] extrahiert.

Aktive IP-Adressen

Anzahl und Trend der verbundenen IP-Adressenund, die Shazzam seit einem bestimmten Datum gescannt hat. Die Daten werden aus der Tabelle Shazzam-Status [shazzam_status] extrahiert.

Nicht erreichbare IPs

Anzahl und Trend der nicht reagierenden IP-Adressenes, die Shazzam seit einem bestimmten Datum gescannt hat. Die Daten werden aus der Tabelle Shazzam-Zusammenfassung [shazzam_summary] extrahiert.

Offene Ports

- Punktzahl der offenen SSH-Ports
- Punktzahl der offenen WMI-Ports
- Punktzahl der offenen WinRM-SSL-Ports

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

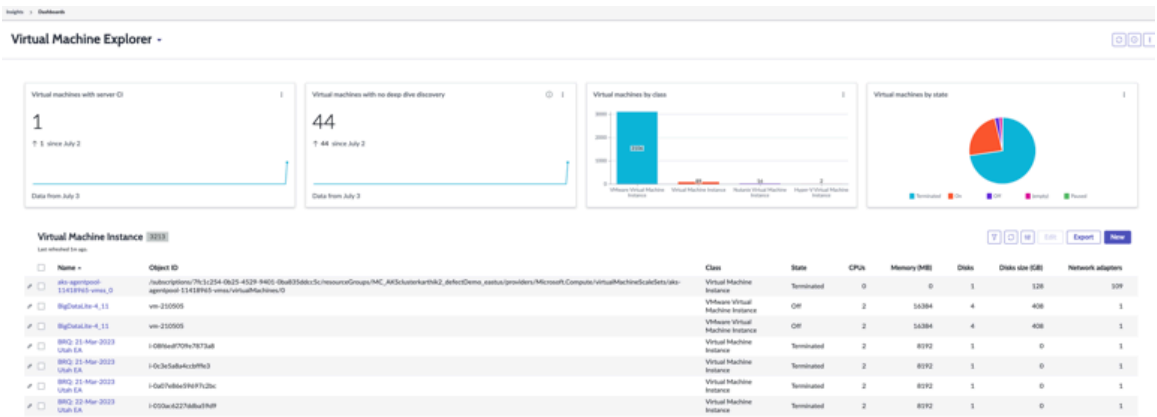
- Punktzahl der offenen SNMP-Ports
- Punktzahl der offenen HTTP-Ports
- Punktzahl der offenen VmApp-SSL-Ports
- Punktzahl der offenen SLP-Ports

Filter

Name	Typ	Beschreibung
IP-Adressen	Boolean	Mit dem Filter können Sie alle Discovery Zeitpläne, die Sie überprüfen möchten, nach Kategorie auswählen. Die verfügbaren Kategorien sind: • IP-Bereich • Aktiv • Aktiv

VM-Explorer-Dashboard

Discovery-Administratorarbeitsbereich zeigt Informationen zur Aktivität und Kapazität Ihrer VM-Instanzen an, wie durch die Discovery ermittelt.



Erforderliche Now Platform-Rollen

- discovery_admin
- Administrator

Greifen Sie auf das Dashboard des VM-Explorers zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** > **VM-Explorer**.

Indikatoren

Virtuelle Maschinen mit Server-CI

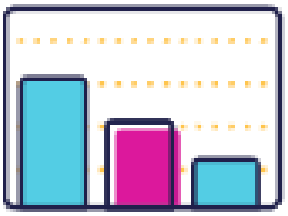
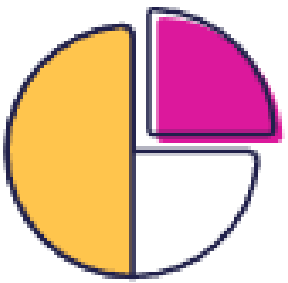
Gesamtanzahl und Trend der virtuellen Computer, für die seit einem bestimmten Datum ein Server-CI erkannt wurde.

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

Virtuelle Computer ohne Deep Dive-Erkennung

Die Gesamtanzahl und der Trend der erkannten virtuellen Computer, für die keine CI-Beziehungen erstellt wurden.

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Virtuelle Maschinen nach Klasse		[cmdb_ci_vm_instance]	Die Anzahl der VMs in Ihrer Infrastruktur, sortiert nach Klasse.
Virtuelle Maschinen nach Status		[cmdb_ci_vm_instance]	Der Prozentsatz der VMs, gruppiert nach Status: ein, aus oder andere.

Filter

Name	Beschreibung
VM-Instanz	Mit dem Filter können Sie alle zu exportierenden Instanzen nach Kategorien wie **Status** und **Datenträgergröße**auswählen.

Discovery-Administratorarbeitsbereich Optimierung

Die Optimierung validiert Ihre vorhandenen Konfigurationen und hilft Ihnen, Konfigurationsprobleme zu beheben.

Discovery-Administratorarbeitsbereich Homepage für Optimierung

Die Optimierungs-Homepage Discovery-Administratorarbeitsbereich bietet Tools zum Bewerten der Instanzintegrität durch konfigurierte Prüfungen und zeigt fehlgeschlagene Prüfungen nach Priorität, Kategorie und Suite an.

Ergebnisse der Optimierungsprüfung

Verwenden Sie die Optimierungstools, um Ihre Instanz nach Konfigurationen abzufragen, die auf Integritätsprobleme hinweisen und Möglichkeiten zur Lösung von Best Practices identifizieren. Die Optimierung überprüft Ihre vorhandenen Konfigurationen und hilft Ihnen, Probleme zu beheben. Weitere Informationen zum Ausführen von Prüfungen finden Sie unter Führen Sie Optimierungsprüfungen aus.

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

Rollen

Die folgenden Rollen haben Zugriff auf die Optimierung Discovery-Administratorarbeitsbereich :

- Administrator
- discovery_admin

Führen Sie Optimierungsprüfungen aus

Optimierungsprüfungen sind Scans, die auf die Optimierung von Konfigurationen abzielen und in Suiten gruppiert sind, wobei die einzelnen Prüfungen im Folgenden beschrieben werden.

Vorbereitungen

Erforderliche Rolle: admin oder discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Die konfigurierten Prüfungen sind unter den folgenden Registerkarten aufgeführt:

- Discovery-Suite
- MID-Suite
- Suite zur Selbstüberwachung

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Optimierung**.
2. Wählen Sie **Prüfungen**aus.
3. Um manuell eine Prüfung für Discovery-Suite, MID-Suite oder Selbstüberwachungs-Suite auszuführen, wählen Sie **Jetzt ausführen**aus.

   Hinweis:

   Es kann jeweils nur ein Instanzscan ausgeführt werden. Warten Sie daher, bis der laufende Scan abgeschlossen ist, bevor Sie die Suite erneut ausführen.

4. Um auf weitere Informationen zu einem Problem zuzugreifen, wählen Sie den Schecknamen aus.

   Hinweis:

   - Um das Problem zu verstehen, wählen Sie den Link Prüfungsbeschreibung anzeigen.
   - Um weitere Details zu dem Problem zu erfahren, wählen Sie Dokumentation über den Prüflink aus.
   - Um die Definitionsseite anzuzeigen, wählen Sie den Link Prüfungsdefinitionsseite aus. Informationen zum Bearbeiten eines Schecks finden Sie unter Bearbeiten Sie einen vorhandenen Scheck.

Bearbeiten Sie einen vorhandenen Scheck

Durch Bearbeiten der Definitionsprüfung können Sie die Beschreibung und das Skript ändern.

Vorbereitungen

Erforderliche Rolle: Administrator

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

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Optimierung**.
2. Wählen Sie **Überprüfen aus**.
3. Wählen Sie den Link Prüfungsdefinitionsseite aus.
4. Um den Scheck zu bearbeiten, wählen Sie **Bereich wechseln**.
5. Aktualisieren Sie alle erforderlichen Details, und wählen Sie **Speichern**aus.

Hinweis: Wenn die Option Aktiv aktiviert ist:

- Die Discovery-Suite wird einmal wöchentlich am Sonntag um 8:00 Uhr ausgeführt.
- Die MID-Suite wird einmal wöchentlich am Sonntag um 10:00 Uhr ausgeführt.
- Die Selbstüberwachungs-Suite wird alle 15 Minuten ausgeführt.

ITOM-Transparenz -Apps mit Discovery-Administratorarbeitsbereich anzeigen und filtern

Greifen Sie von einem zentralen Ort aus auf alle Discovery-Administratorarbeitsbereich *ITOM-Transparenz* -Apps zu. Zeigen Sie sowohl die bereits in Ihrer Instanz installierten als auch die für die Installation verfügbaren Anwendungen an, und filtern Sie sie. Verwenden Sie diese Funktion, um Anwendungen zu integrieren und die Experience Discovery von zu verbessern.

Warum und wann dieser Vorgang ausgeführt wird

Sie können zwar auf Details zu den in Ihrer Instanz installierten Apps zugreifen, Informationen zu Preisen und Paketen werden jedoch nicht bereitgestellt, da diese je nach Vertrag variieren. Eine allgemeine Übersicht über Lizenzierungs- und Abonnementdetails finden Sie unter ITOM/OT SU-Lizenzierung und -Abonnements.

Vorbereitungen

Erforderliche Rolle: admin oder discovery_admin

Auf dieser Seite können Sie neue Anwendungen installieren und vorhandene aktualisieren. Zum Aktualisieren von Anwendungen benötigen Sie die Administratorrolle.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich**.
2. Wählen Sie im Abschnitt ITOM-Transparenz -Apps-Apps **die Option Alle anzeigen** aus. Die Seite **„Transparenz-Anwendungen“** wird geöffnet und zeigt alle Anwendungen in zwei Kategorien an: **Installierte Anwendungen** und **Nicht installierte Anwendungen**.
3. Verwenden Sie die Dropdown-Liste für Filter, um das gewünschte Abonnement zum Anzeigen auszuwählen.

Discovery anfordern

Discovery ist als vom Rest von Now Platform getrenntes Abonnement verfügbar und erfordert das Plugin Discovery (com.snc.discovery).

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

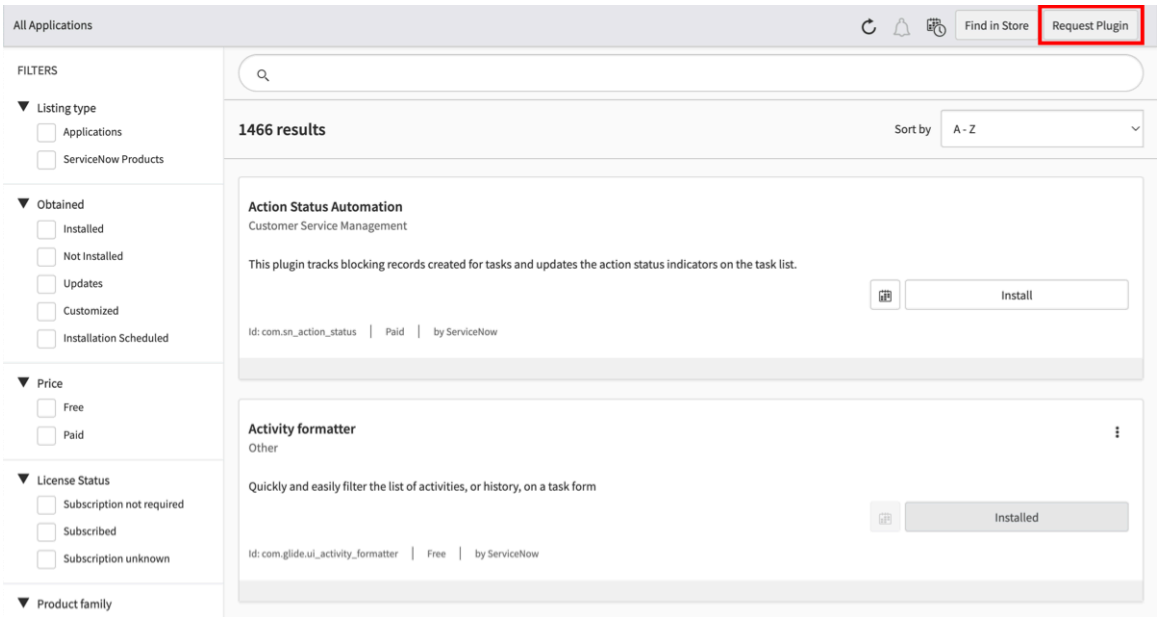
Wenden Sie sich zum Erwerben eines Discovery -Abonnements an Ihren Account Manager oder Vertriebsmitarbeiter ServiceNow von . Wenn das Plugin Discovery aktiviert ist, werden

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

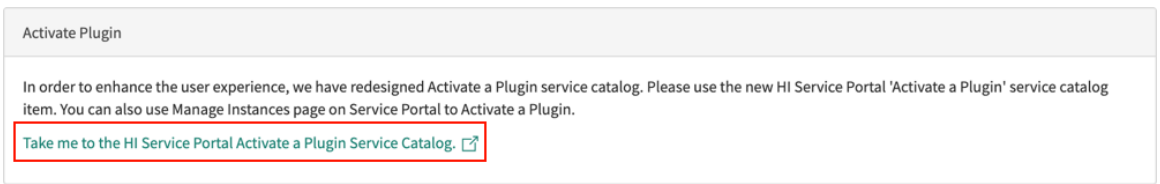
mehrere Plugins und Anwendungen installiert. Weitere Informationen finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Transparenz.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins

Automatische Übersetzung

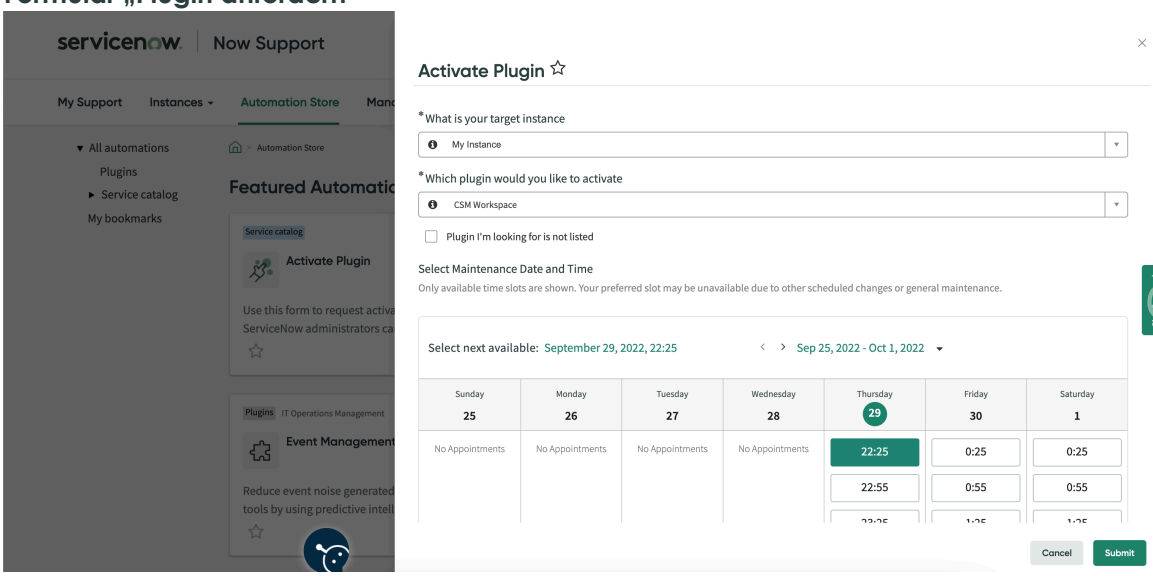
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Feld	Beschreibung
	Hinweis: Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-Artikel [KB0751715] in Now Support Knowledge Base.

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

Zugehörige Informationen

Discovery einrichten

Monitoring von Erkennungen und Problemlösung

Discovery einrichten

Um nach der Aktivierung von Discovery loszulegen, haben Sie verschiedene Möglichkeiten.

Hinweis: Wenn sowohl das Plugin „Discovery“ (com.snc.discovery) in der Instanz als auch ein Sprach-Plugin (z. B. Spanisch) aktiviert ist, stellen Sie sicher, dass die Sprache für den MID-Server im Benutzerdatensatz ebenfalls auf „English/None“ (Englisch/Keine) festgelegt ist.

Wählen Sie die Setupmethode aus:

Setupmethode	Beschreibung
Guided Setup	Verwenden Sie diese Methode, wenn Sie alles für die Verwendung von Discovery einrichten möchten, einschließlich eines MID Servers. Das Guided Setup für Discovery stellt eine Reihe von Aufgaben bereit, die Sie beim Konfigurieren von Discovery in Ihrer ServiceNow-Instanz unterstützen. Um das geführte Setup für Discovery zu öffnen, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .
Ohne Guided Setup	Verwenden Sie diese Methode, wenn Sie die Komponenten jeweils einzeln einrichten möchten. Sie können MID Server, Anmeldeinformationen und Rollen getrennt konfigurieren und dann einen der Erkennungstypen aus dem Erkennungszeitplan konfigurieren.
Discovery Schnellstart	Verwenden Sie diesen Assistenten, um alles zu konfigurieren, was Sie für die Subnetz- und CI-Erkennung in Ihrer Umgebung benötigen. Bevor Sie Schnellstart verwenden können, müssen Sie Ihre MID Server installieren und validieren und die erforderlichen Anmeldeinformationen erstellen.

Zugehörige Informationen

Discovery einrichten

Monitoring von Erkennungen und Problemlösung

Discovery ohne Guided Setup einrichten

Wenn Sie das Guided Setup nicht verwenden, müssen Sie mehrere Konfigurationsschritte manuell ausführen, um die Anwendung zu aktivieren und um den MID Server und Discovery einzurichten.

Vorbereitungen

- Discovery-Rolle gewähren: Stellen Sie sicher, dass Benutzer, die in Ihrem Netzwerk Discovery konfigurieren und ausführen sollen, über die Rolle discovery_admin verfügen. Diese Rolle gewährt Zugriff auf die Tabellen in Discovery.
- Bestimmen Sie einen Computer als Host für den MID Server.

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

- Sammeln Sie die Anmeldeinformationen, die der MID Server für den Zugriff auf die zu erkennenden Geräte benötigt.
- Bestimmen Sie, welche IP-Adressen von Discovery gescannt werden müssen. Gruppieren Sie in einem sehr komplexen Netzwerk IP-Bereiche in Range Sets, die für verschiedene Zeitpläne wiederverwendbar sind. Discovery scannt nicht außerhalb dieser Bereiche.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Installieren Sie einen oder mehrere MID-Server auf physischen oder virtuellen Servern, die die Systemanforderungen für MID-Server erfüllen, und konfigurieren Sie sie für die Kommunikation mit der entsprechenden ServiceNow -Instanz.
   Installieren Sie zuerst mindestens zwei MID Server, und weisen Sie sie verschiedenen Zeitplänen und IP-Bereichen zu, um Erkennungen schneller abzuschließen. Seit dem Istanbul-Release müssen Sie sicherstellen, dass dem MID Server die Anwendung Discovery oder die Anwendung **ALLE** zugewiesen ist.
2. Stellen Sie die Konnektivität des MID-Servers sicher, indem Sie zu navigieren **Discovery** > **MID-Server**.
   Wenn die MID Server ordnungsgemäß konfiguriert sind, werden sie in der Liste der MID Server angezeigt.
3. Wenn ein MID Server in der Instanz nicht als Auswahl angezeigt wird, führen Sie die folgenden Prüfungen durch:
   - Stellen Sie sicher, dass die URL in der bereitgestellten zugehörigen Liste „Konfigurationsparameter“ korrekt ist.
   - Wenn der MID Server unter Windows installiert ist, stellen Sie sicher, dass der ServiceNow MID Server-Service ordnungsgemäß mit den richtigen Anmeldeinformationen konfiguriert ist und ausgeführt wird.
   - Überprüfen Sie das MID Server-Protokoll auf Fehler.
     - Navigieren Sie in der Instanz zu **Discovery** > **MID-Server** > **[MID-Server]** > **Protokolle**.
     - Navigieren Sie auf dem MID Server-Host zum Verzeichnis `agent\logs\agent0.log0`.
   - Wenn die Standardauthentifizierung aktiviert ist, müssen ein Benutzername und ein Passwort angegeben werden.
   - Der MID Server hat möglicherweise keinen ausgehenden Zugriff an Port 443 (SSL), oder ein Proxy-Server verhindert möglicherweise die TCP-Kommunikation mit der Instanz.
   - Stellen Sie sicher, dass keine Firewalls die Kommunikation zwischen dem MID Server und der Instanz blockieren.
4. Legen Sie in der Instanz die Anmeldeinformationen für alle Computer, Drucker und Netzwerkgeräte in Ihrer Umgebung fest.
   Anmeldeinformationen für Windows-Geräte (mithilfe des WMI-Protokolls) werden von der für den MID Server-Service auf dem Windows-Serverhost konfigurierten Anmeldung bereitgestellt. Anmeldeinformationen für UNIX, vCenter und SNMP müssen für die Instanz konfiguriert werden. Discovery ermittelt automatisch, welche Anmeldeinformationen für einen bestimmten Computer oder ein bestimmtes Gerät funktionieren.
5. Definieren Sie Erkennungszeitpläne, und führen Sie sie aus.

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

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

Adressen. Erstellen Sie so viele Zeitpläne wie erforderlich, verwenden Sie verschiedene Arten von Erkennungen, und konfigurieren Sie sie so, dass sie jederzeit ausgeführt werden können. Lassen Sie Discovery gemäß dem konfigurierten Zeitplan ausführen, oder führen Sie Discovery zum gewünschten Zeitpunkt manuell aus. Sie können einen einzelnen Zeitplan für das gesamte Netzwerk oder separate Zeitpläne für jeden Standort oder jedes VLAN einrichten. Wenn Sie die zu scannende IP-Adresse in Ihrem Netzwerk nicht kennen, führen Sie zuerst eine Discovery im Netzwerk aus, um die IP-Netzwerke zu erkennen. Nach der Erkennung können Sie diese Netzwerke in Range Sets von IP-Adressen konvertieren, die Sie in einem Discovery-Zeitplan verwenden.

Hinweis: Verwenden Sie für erweiterte Erkennungen Discovery Verhaltenweisen, etwa für Erkennungen, die einen Lastenausgleich oder das Scannen über mehrere Domänen hinweg erfordern.

6. Validieren Sie die Discovery-Ergebnisse.
   Öffnen Sie die ECC-Warteschlange, analysieren Sie die XML-Nutzlast, und überprüfen Sie dann das Discovery-Protokoll. Weitere Informationen finden Sie im Abschnitt zur Validierung von Ergebnissen in Horizontale Erkennung planen.

Discovery Schnellstart

Discovery Schnellstart ist ein Assistent, der Sie bei der schnellen Inbetriebnahme von Discovery unterstützt. Verwenden Sie Discovery Schnellstart-Aufgaben, um IP-Bereiche oder Subnetze in Ihrer Umgebung zu erkennen und anschließend die Konfigurationselemente (CI) in diesen Subnetzen zu identifizieren.

Installieren und validieren Sie MID Server noch vor der Verwendung von Discovery Schnellstart. Weitere Informationen finden Sie unter Installation des MID-Servers .

Subnetzerkennung konfigurieren und planen

Bei der Subnetzerkennung werden alle Subnetze in Ihrer Umgebung erkannt, um verfügbare IP-Bereiche zu bestimmen und sicherzustellen, dass MID Server für den Zugriff auf diese Bereiche verfügbar sind.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

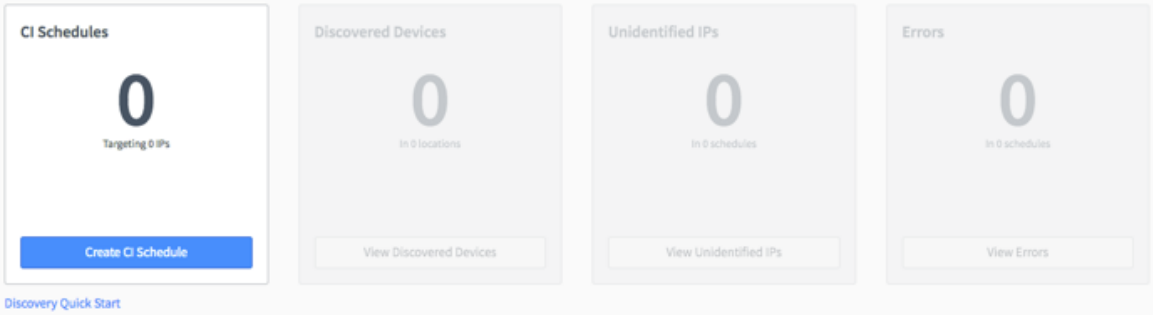
Das Ziel dieser Phase besteht in der Erkennung aller Subnetze in Ihrem Netzwerk. Dazu muss Discovery über die richtigen SNMP-Anmeldeinformationen verfügen, um die ermittelten Router zu identifizieren. Mit den von Ihnen bereitgestellten Anmeldeinformationen liest Discovery zunächst die Routertabellen des Routers, der mit dem MID Server verbunden ist, um verbundene Router zu identifizieren. Discovery geht dann von innen nach außen durch das Netzwerk von Router zu Router, bis alle lokalen Subnetze erkannt wurden.

Nachdem Discovery die Subnetze identifiziert hat, werden in Vorbereitung auf die CI-Erkennungsphase die IP-Bereiche dieser Subnetze automatisch qualifizierten MID Servern zugewiesen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**.
   Beim ersten Zugriff auf die Startseite von Discovery wird ein Willkommensbildschirm angezeigt. Nachdem Sie die Subnetzerkennung konfiguriert und den Zeitplan ausgeführt haben, zeigt Schnellstart die Subnetzergebnisse an.
2. Klicken Sie auf **Discovery-Schnellstart**, um mit der Konfiguration zu beginnen.

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



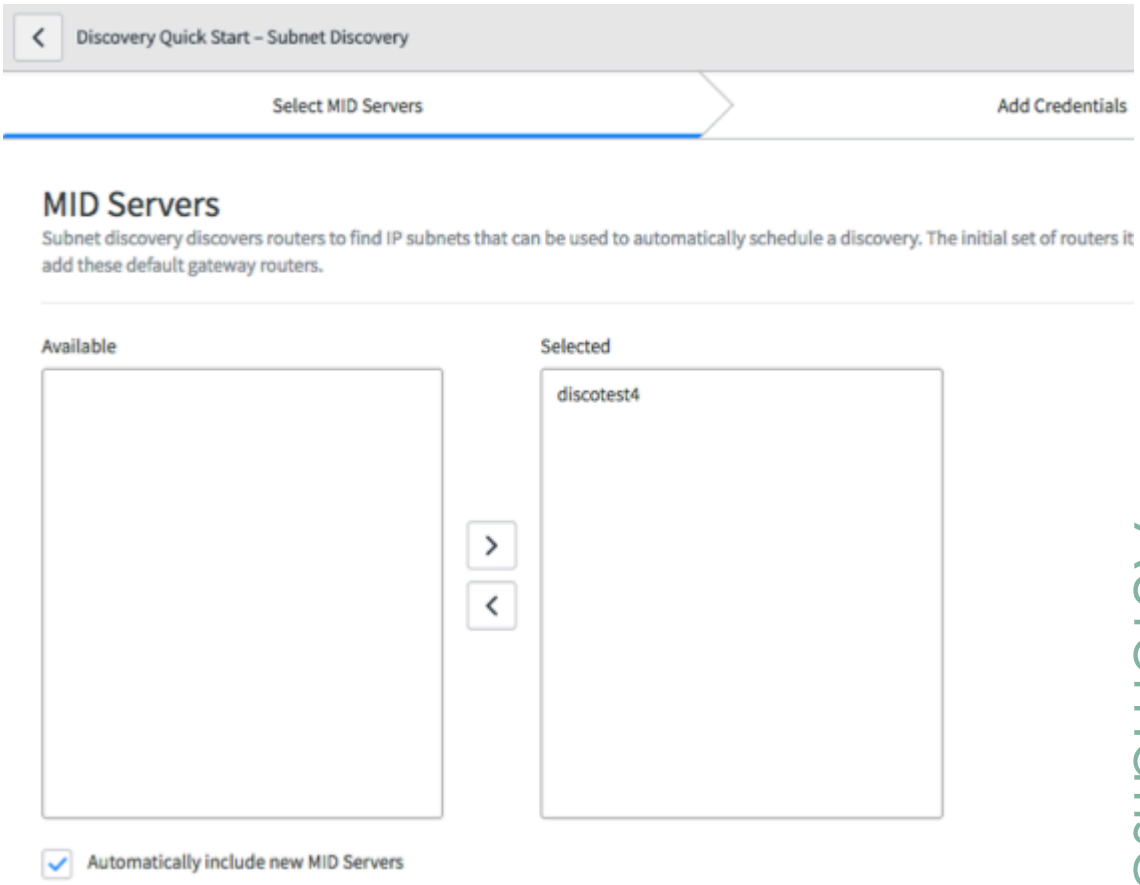
Hinweis: Fall Sie noch keinen MID Server eingerichtet haben, klicken Sie, wenn Sie aufgefordert werden, den MID Server-Benutzer zu erstellen, den MID Server herunterzuladen und zu installieren sowie ihn zu validieren, auf **MID Server-Einrichtung mit Anleitung**. Über Links im Guided Setup gelangen Sie zu Discovery Schnellstart, um mit der Konfiguration der Subnetzerkennung fortzufahren. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

3. Wählen Sie auf der Registerkarte **MID Server auswählen** qualifizierte MID Server für die Subnetzerkennung aus.

   a. Verschieben Sie die MID Server, die Sie für die Subnetzerkennung verwenden möchten, aus der Spalte **Verfügbar** in die Spalte **Ausgewählt**.
   Verfügbare MID Server müssen die folgenden Anforderungen erfüllen:

   - Sie müssen konfiguriert sein und den Status **In Betrieb** aufweisen.
   - Sie müssen validiert sein.
   - Ihnen müssen die Anwendung Discovery oder **ALLE** Anwendungen angefügt sein.

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



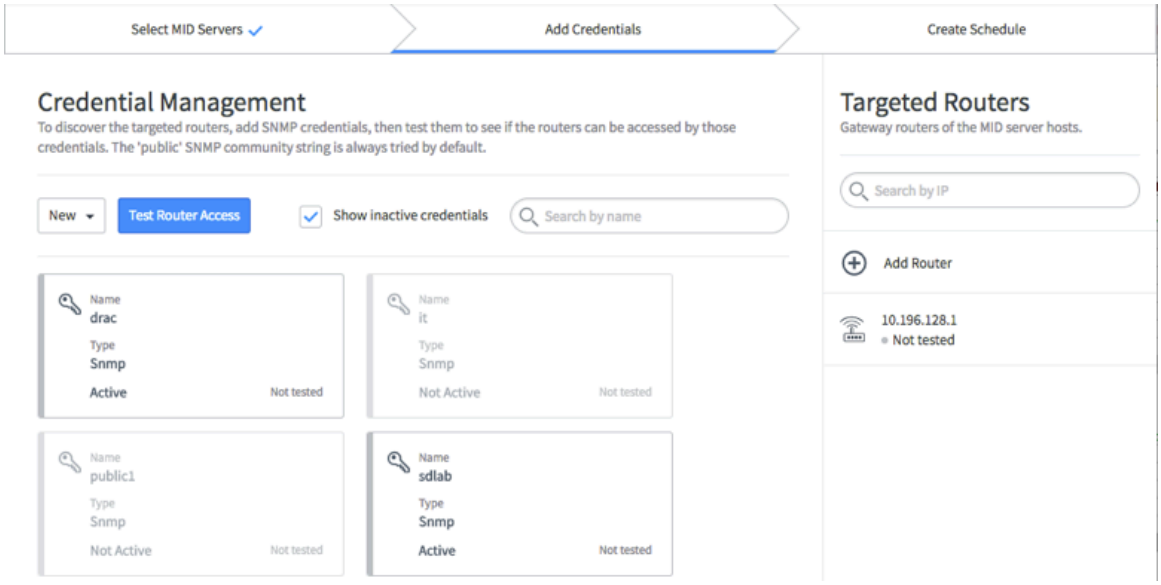
b. Wenn Sie möchten, dass Discovery alle neuen MID Server verwendet, die die Setupkriterien erfüllen, aktivieren Sie das Kontrollkästchen **Neue MID Server automatisch einschließen** aus.

c. Klicken Sie auf **Next (Weiter)**.

4. Fügen Sie auf der Registerkarte **Anmeldeinformationen hinzufügen** Anmeldeinformationen für die zu erkennenden Router hinzu.
Diese Registerkarte zeigt alle SNMP-Anmeldeinformationen, die bereits konfiguriert sind. Router, die in der Liste **Zielrouter** angezeigt werden, sind Standard-Gateway-Router, mit denen der MID Server-Host verbunden ist.

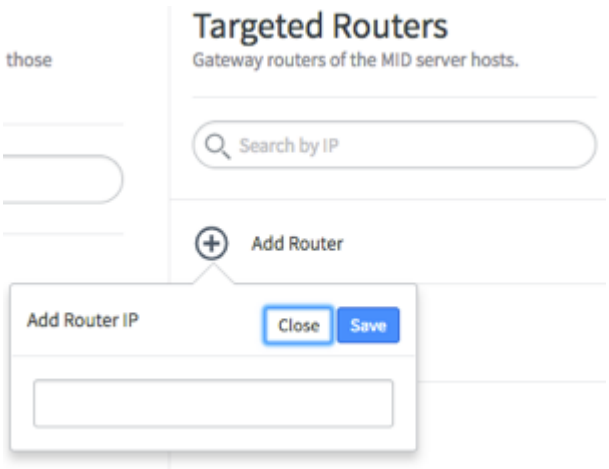
Hinweis: Sie können nach dem Erstellen eines Zeitplans zum Hinzufügen von Anmeldeinformationen zu dieser Phase zurückkehren.

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



a. Klicken Sie auf **Neu**, um gegebenenfalls SNMP-Community- oder SNMP V3-Anmeldeinformationen hinzuzufügen.

b. Wenn die Liste der Zielrouter nicht alle erwarteten Router enthält, klicken Sie auf das Pluszeichen, und fügen Sie den Router anhand der IP-Adresse hinzu.



c. Nachdem Sie alle erforderlichen Anmeldeinformationen konfiguriert haben, klicken Sie auf **Routerzugriff testen**, um zu prüfen, ob Discovery Ihre Anmeldeinformationen für den Zugriff auf Router verwenden kann.
Die Gateway-Router werden in der Spalte **Router** angezeigt, und zwar unabhängig davon, ob die Anmeldeinformationen auf den Router zugreifen können. Diese Router, auf die mit den Anmeldeinformationen erfolgreich zugegriffen werden kann, werden mit dem Indikator **Erfolg** angezeigt. Die Router, die nicht erreichbar sind, werden mit dem Indikator **Fehlgeschlagen** angezeigt.

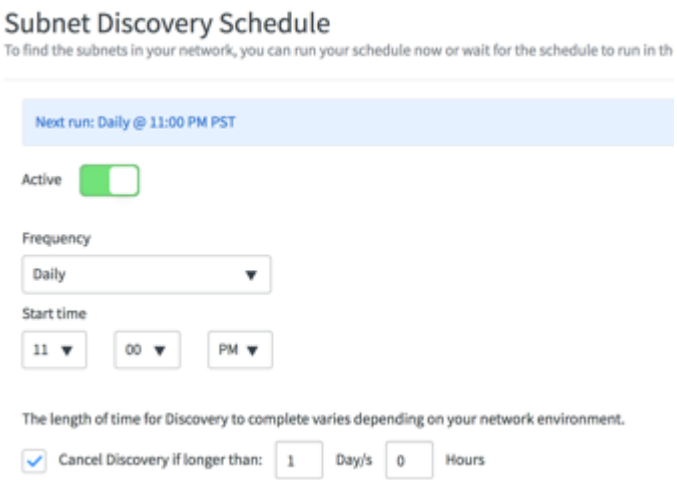
Sie können die Liste mithilfe des Felds **Nach IP durchsuchen** oder mithilfe der Optionen **Erreichte Router** oder **Nicht erreichte Router** in der Auswahlliste **Ansicht** filtern.

d. Klicken Sie auf **Next (Weiter)**.

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

5. Erstellen Sie auf der Registerkarte **Zeitplan erstellen** einen Zeitplan zur regelmäßigen Ausführung der Subnetzerkennung.
   Bei der Ausführung dieses Zeitplans findet die Subnetzerkennung statt, und die automatische Zuweisung des IP-Subnetzes wird ausgelöst, durch die die erkannten Subnetze qualifizierten MID Servern zugewiesen werden.

   a. Schließen Sie den Zeitplan mithilfe der Felder in der Liste ab.



   - **Akti** : Aktiviert oder deaktiviert diesen Zeitplan.
   - **Frequenz**: Legen Sie fest, wie oft der Zeitplan ausgeführt werden soll:
     - **Täglich**: Discovery zu einem bestimmten Zeitpunkt jeden Tag ausführen.
     - **Wöchentlich**: Discovery an einem bestimmten Tag jeder Woche ausführen.
     - **Monatlich**: Discovery an einem bestimmten Tag des Monats ausführen. Wenn der angegebene Tag nicht in dem Monat vorkommt, wird der Zeitplan in diesem Monat nicht ausgeführt. Wenn Sie beispielsweise Tag 30 festlegen, wird der Zeitplan im Februar nicht ausgeführt.
     - **Einmal**: Discovery einmal am angegebenen Datum und zur gewünschten Uhrzeit ausführen.
     - **Regelmäßig**: Jedes angegebene Mal Discovery ausführen. Verwenden Sie das Feld **Wiederholungsintervall**, um die Zeit in Tagen, Stunden, Minuten und Sekunden zu definieren. Die erste Erkennung wird zu dem Zeitpunkt ausgeführt, der im Feld **Start** festgelegt ist. Die nachfolgenden Enrkennungen werden nach Ablauf jedes **Wiederholungsintervall**-Zeitraums ausgeführt.
   - **Discovery abbrechen, wenn länger als**: Beenden Sie den Discovery-Prozess, wenn er die angegebene Dauer überschreitet. Discovery kann aufgrund einer Vielzahl von Faktoren, einschließlich der Größe Ihres Netzwerks, übermäßig lange dauern.

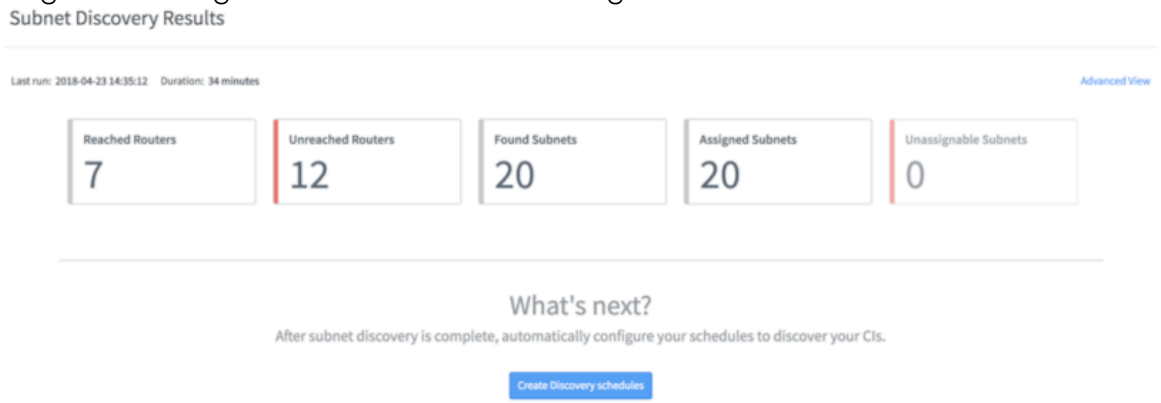
     Hinweis: Eine MID-Server-Verarbeitung findet statt, wenn Discovery abgebrochen wird/abschließen darf. Alle Ausgabedatensätze, die MID-Server nicht erfasst haben, werden jedoch abgebrochen.

   b. Klicken Sie auf eine der folgenden Optionen:

   - **Beenden und ausführen** speichert den Zeitplan und führt die Erkennung sofort aus.
   - **Fertigstellen** speichert den Zeitplan. Discovery wird dann in dem im Zeitplan angegebenen Intervall ausgeführt.

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

6. Zeigen Sie die Ergebnisse der Subnetzerkennung an.



   a. Klicken Sie auf die einzelnen Kacheln, um Details anzuzeigen.
   Wenn die Subnetzerkennung noch nicht ausgeführt wurde, wird für jede Kachel der Wert **0** angezeigt.
      - **Erreichte Router**: Die Anzahl der Router, auf die Discovery zugreifen konnte und die erkannt wurden
      - **Unerreichte Router**: Die Anzahl der Router, auf die Discovery nicht zugreifen konnte
      - **Subnetze gefunden**: Die Anzahl der durch Discovery gefundenen Subnetze
      - **Zugewiesene Subnetze**: Die IP-Subnetze, die mindestens einem MID Server zugewiesen wurden
      - **Unzuweisbare Subnetze**: IP-Subnetze, die keinem MID Server zugewiesen wurden

   b. Klicken Sie auf **Zeitplan bearbeiten**, um zur Registerkarte **MID Server auswählen** zurückzukehren.
   Beheben Sie Probleme mit der Subnetzerkennung, indem Sie zur Seite für den Routerzugriff zurückkehren und sicherstellen, dass alle Anmeldeinformationen ordnungsgemäß konfiguriert sind. Testen Sie auch den Routerzugriff für alle Anmeldeinformationen.

   c. Klicken Sie auf **Erweiterte Ansicht**, um das Formular „Automatisierungstatussatz“ anzuzeigen.
   Dieses Formular zeigt detaillierte Ergebnisse sowohl für die Subnetzerkennung als auch für die automatische Zuweisung von IP-Bereichen an.

CI-Erkennung konfigurieren und planen

Mit den von Ihnen angegebenen Anmeldeinformationen findet der Schnellstart-Assistent alle Konfigurationselemente (CI) für die während der Subnetzerkennung identifizierten IP-Bereiche.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Sie sollten dieses Verfahren nach Abschluss von Subnetzerkennung konfigurieren und planen in Discovery Schnellstart ausführen.

Warum und wann dieser Vorgang ausgeführt wird

Das Ziel dieser Phase besteht in der Erstellung der Zeitpläne, die zum Erkennen der CIs in jedem Subnetz erforderlich sind. Discovery Schnellstart erledigt dies automatisch und führt diese Zeitpläne dann mit den von Ihnen angegebenen Anmeldeinformationen aus. Sie können jederzeit zusätzliche Anmeldeinformationen hinzufügen. Optional können Sie

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

Standorte für jeden der Subnetzrouter definieren. Discovery erstellt dann separate Zeitpläne für jeden Standort.

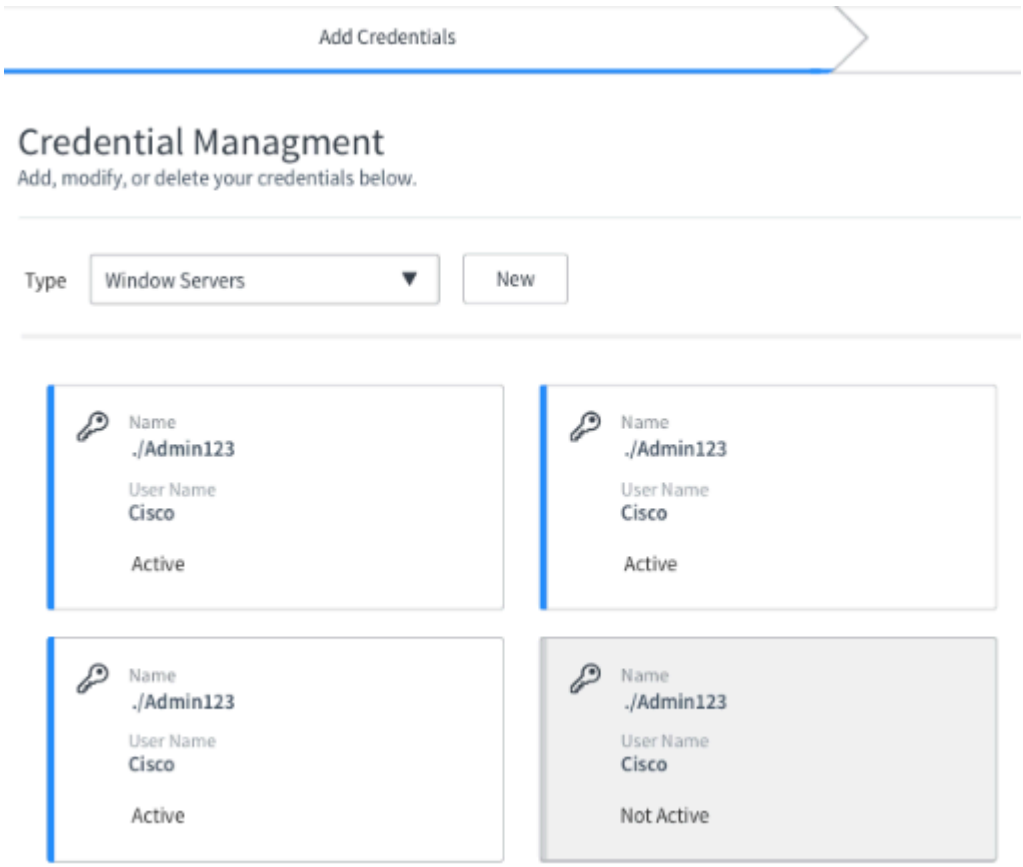
Sie müssen mit den Typen der Anmeldeinformationen vertraut sein, die Sie für die CIs in Ihrem Netzwerk benötigen. Jeder CI-Typ erfordert andere Anmeldeinformationen. Wenn Discovery beispielsweise Muster anstelle von Proben verwendet, sind für die Muster möglicherweise Applicative-Anmeldeinformationen erforderlich.

Überprüfen Sie die Anforderungen für die zu erkennenden CI-Typen. Konsultieren Sie Durch ITOM-Transparenz erfasste Daten, und suchen Sie dann den spezifischen Geräte-, Computer oder Anwendungstyp.

Prozedur

1. Erstellen Sie auf der Registerkarte **Anmeldeinformationen hinzufügen** in Discovery Schnellstart die für die Erkennung von CIs in Ihrem Netzwerk erforderlichen Anmeldeinformationen.

   a. Wählen Sie im Feld **Typ** den Anmeldeinformationstyp aus, den Sie verwalten möchten. Alle derzeit für diesen CI-Typ konfigurierten Anmeldeinformationen werden in Kachelzeilen



   angezeigt.

   b. Klicken Sie auf **Neu**, um Anmeldeinformationen hinzuzufügen. Das Formular „Anmeldeinformationen hinzufügen“, in dem Sie neue Anmeldeinformationen angeben können, wird angezeigt.

   c. Klicken Sie auf **Weiter**, um zur Phase **Routerstandort** zu wechseln.

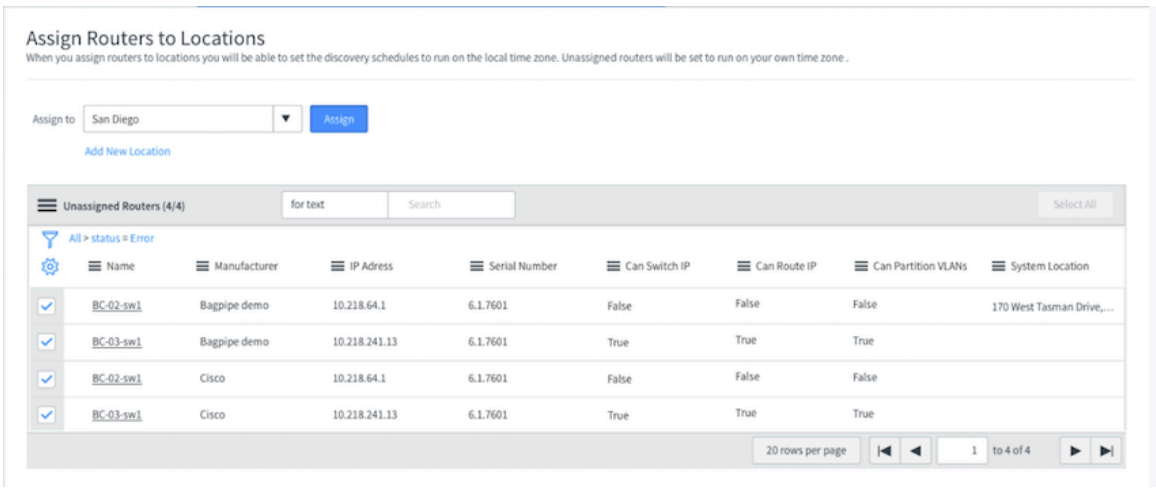
2. **Optional:** Weisen Sie auf der Registerkarte **Routerstandort zuweisen** allen Routern, die durch die Subnetzerkennung gefunden wurden, einen Standort zu.

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

Bei der Konfiguration von Routerstandorten haben Sie die Möglichkeit, für jeden Standort einen Zeitplan zu erstellen. Wenn Sie keine Standorte zuweisen, wird für alle Ihre Subnetze ein einziger Discovery-Zeitplan erstellt. Wenn Sie einem Standort eine Zeitzone zuweisen, erstellt Discovery einen Zeitplan, der in der Zeitzone dieses Standorts ausgeführt wird. Wenn Sie einem Standort keine Zeitzone zuweisen, wird der Zeitplan dieses Standorts in der lokalen Zeitzone des Benutzers ausgeführt.

Hinweis: Ein Subnetz kann mehreren Routern angehören. Wenn Zeitpläne nach Standort erstellt werden, erkennt Discovery Subnetze, die von mehreren Routern mit mehreren Zeitplänen verwaltet werden.

Die Liste der Gateway-Router zeigt die Geräte an, die derzeit keinem Standort zugewiesen sind.



a. Aktivieren Sie die Kontrollkästchen für die Router, denen Sie einen Standort zuweisen möchten.
Nutzen Sie die Spalte **Systemstandort** in der Tabelle als Hilfsmittel zur einfacheren Zuordnung eines Standorts zu einem Router.

b. Wählen Sie den Standort in der Auswahlliste **Zuweisen zu** aus.

c. Wenn sich der Standort noch nicht in der Liste befindet, klicken Sie auf **Neuen Standort hinzufügen**, und fügen Sie den Standort hinzu.

d. Stellen Sie sicher, dass für den Standort eine Zeitzone definiert ist.
Mit Zeitzonen können Sie einen Zeitplan für jeden Standort basierend auf der Zeitzone erstellen.

e. Klicken Sie auf **Zuweisen**.

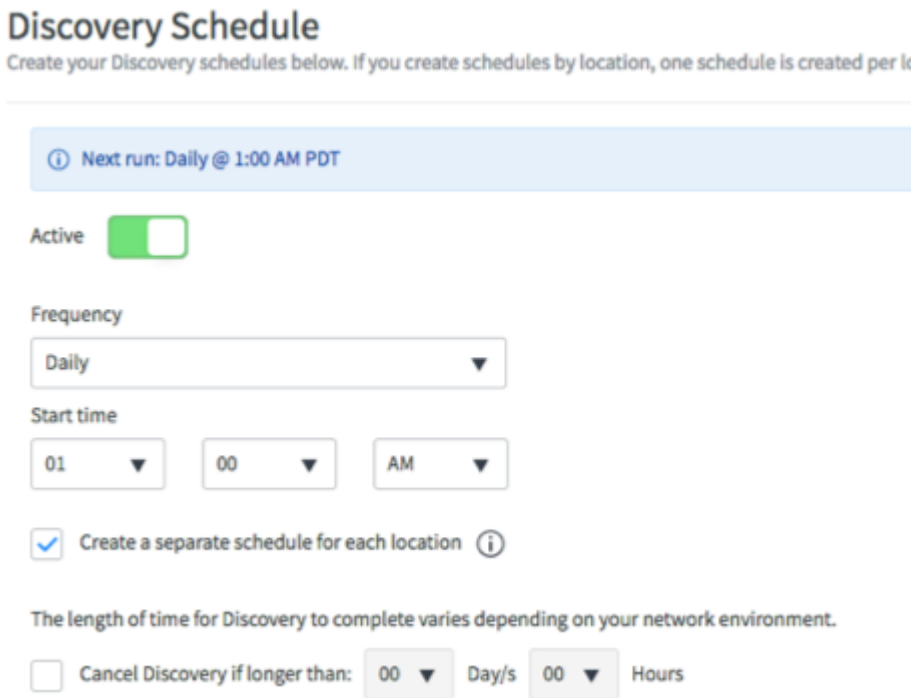
Hinweis: Nicht zugewiesene Router können standortbasierten Zeitplänen nicht hinzugefügt werden.

f. Klicken Sie auf **Next (Weiter)**.

3. Erstellen Sie einen Discovery-Zeitplan für CIs.

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

a. Schließen Sie den Zeitplan mithilfe der Felder in der Liste ab.



- **Akti** : Aktiviert oder deaktiviert diesen Zeitplan.
- **Frequenz**: Legen Sie fest, wie oft der Zeitplan ausgeführt werden soll:
  - **Täglich**: Discovery zu einem bestimmten Zeitpunkt jeden Tag ausführen.
  - **Wöchentlich**: Discovery an einem bestimmten Tag jeder Woche ausführen.
  - **Monatlich**: Discovery an einem bestimmten Tag des Monats ausführen. Wenn der angegebene Tag nicht in dem Monat vorkommt, wird der Zeitplan in diesem Monat nicht ausgeführt. Wenn Sie beispielsweise Tag 30 festlegen, wird der Zeitplan im Februar nicht ausgeführt.
  - **Einmal**: Discovery einmal am angegebenen Datum und zur gewünschten Uhrzeit ausführen.
  - **Regelmäßig**: Jedes angegebene Mal Discovery ausführen. Verwenden Sie das Feld **Wiederholungsintervall**, um die Zeit in Tagen, Stunden, Minuten und Sekunden zu definieren. Die erste Erkennung wird zu dem Zeitpunkt ausgeführt, der im Feld **Start** festgelegt ist. Die nachfolgenden Enrkennungen werden nach Ablauf jedes **Wiederholungsintervall**-Zeitraums ausgeführt.
- **Separaten Zeitplan für jeden Standort erstellen**: Es werden automatisch Zeitpläne für alle von Ihnen konfigurierten Routerstandorte erstellt. Diese Zeitpläne werden an dem von Ihnen angegebenen Tag und zu der von Ihnen angegebenen Uhrzeit ausgeführt, jedoch in ihrer eigenen Zeitzone. Deaktivieren Sie das Kontrollkästchen, um einen einzigen Zeitplan für alle Ihre Standorte zu erstellen, der in der Zeitzone des Anwenders ausgeführt wird. Diese Option ist nur verfügbar, wenn Sie die Router-Standorte konfiguriert haben.

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

- **Discovery abbrechen, wenn länger als**: Beenden Sie den Discovery-Prozess, wenn er die angegebene Dauer überschreitet. Discovery kann aufgrund einer Vielzahl von Faktoren, einschließlich der Größe Ihres Netzwerks, übermäßig lange dauern.

  Hinweis: Eine MID-Server-Verarbeitung findet statt, wenn Discovery abgebrochen wird/abschließen darf. Alle Ausgabedatensätze, die MID-Server nicht erfasst haben, werden jedoch abgebrochen.

b. Klicken Sie auf eine der folgenden Optionen, um den Schnellstart abzuschließen:

- **Beenden und ausführen** speichert den Zeitplan und führt die Erkennung sofort aus.
- **Fertigstellen** speichert den Zeitplan. Discovery wird dann in dem im Zeitplan angegebenen Intervall ausgeführt.

Migrieren Sie von CAPI zu Mustern

Migrieren Sie von Cloud API (CAPI)-basiert Cloud-Discovery zu musterbasiert Cloud-Discovery. Die Aufgabe erfordert eine unterstützte Instanz und einige Plugins. Die Migration funktioniert für Amazon Web Services (AWS) und Microsoft Azure. Der Administrator kann diese Aufgabe ausführen, nachdem die erste Instanz eingerichtet wurde.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Stellen Sie sicher, dass Ihre Now Platform über Folgendes verfügt:

- Die Release-Version ist Paris oder höher.
- Das Plugin „Muster für Discovery und Service-Mapping“ (sn_itom_pattern).

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Migration ausgelöst wird, deaktiviert das Skript die entsprechenden CAPI-Erkennungsschritte für die Cloud-Umgebung, um zu verhindern, dass sie während der Cloud-Discovery ausgelöst werden. Außerdem aktiviert das Skript die entsprechenden Cloud-Muster für die Umgebung, die zur Ausführung der zukünftigen Cloud-Discovery verwendet wird. Nach der Migration verwendet die Discovery die neuesten Muster anstelle der veralteten Discovery-Methode CAPI.

Hinweis:

Die CAPI-basierte Discovery-Methode wird in Zukunft eingestellt.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Migrieren Sie CPG zu Muster**.
2. Lesen Sie auf der Seite „CAPI-zu-Muster-Migration“ die Anweisungen, und wählen Sie **Prüfung der Voraussetzungen ausführen**aus.
3. Nachdem die Voraussetzungsprüfung bestanden wurde, können Sie wie folgt auswählen:
   - Alle migrieren: Migrieren Sie AWS und Azure gleichzeitig.
   - AWS migrieren oder Azure migrieren: Migrieren Sie jede Instanz einzeln.

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

4. Wählen Sie Migrieren und bestätigen Sie, um mit der Migration fortzufahren.

Hinweis:

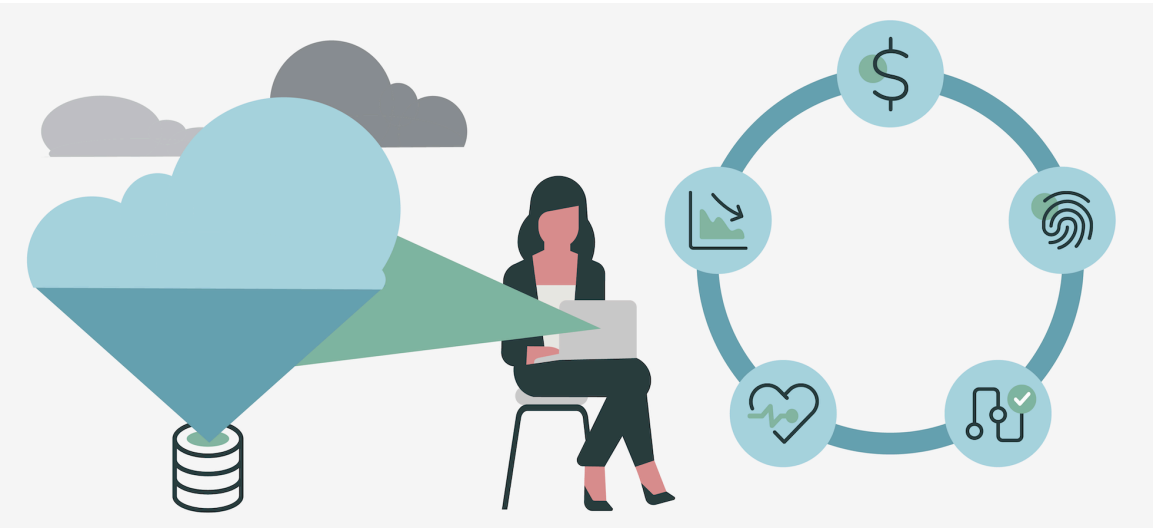
Bei Problemen bei der Migration lesen Sie die Schritte zur Fehlerbehebung, die im Artikel CAPI-zu-Muster-Migration: Verfahren für den Wechsel von CAPI-basierter Cloud-Discovery zu musterbasierter Cloud-Discovery [KB0827153] in der Now Support Knowledge Basedokumentiert sind.

Cloud-Discovery erkunden

Cloud-Discovery ermöglicht IT-Abteilungen von Unternehmen, detaillierte Informationen über ihre cloudbasierte Infrastruktur zu sammeln. Cloud-Discovery findet Ressourcen bei wichtigen Cloud Service Providern.

Einführungsvideo zu Cloud-Discovery

Cloud-Discovery findet Ressourcen bei den folgenden Cloud-Anbietern: Amazon AWS Cloud, Microsoft Azure Cloud, Google Cloud Platform (GCP), IBM Cloud Platformund Oracle Cloud Infrastructure (OCI). Cloud-Discovery sammelt die dem Account zugeordneten logischen Rechenzentren sowie alle Unterkonten. Das Sammeln von Informationen über Ressourcen in der Cloud ist relevant für Unternehmen, Organisationen und Cloud-Unternehmen, die Platform-as-a-Service-Lösungen bereitstellen.



Servicekontobasierte Erkennung

Bei der servicekontobasierten Erkennung werden alle Ressourcen in einem Servicekonto erkannt. Diese Art der Erkennung erfasst Metadaten mithilfe der APIs des Cloud Providers und füllt dann die CMDB-Tabelle der Geräteinstanz mit Basisattributen. Die Service-Account-Discovery bietet Einblick in Tags, was die Datenberichterstellung und Workflow-Automatisierung unterstützt. Beispielsweise können Cloud-Events verwendet werden, um die Erkennung bei Bedarf für Zielservices auszulösen. Dadurch kann Cloud-Discovery Änderungen erkennen und automatisch die CMDB aktualisieren.

IP-basierte Erkennung

Beim anderen Cloud-Discovery-Typ, der IP-basierten Erkennung, werden die Metadaten verwendet, die bei der servicekontobasierten Erkennung gesammelt wurden, um detailliertere Informationen zu erfassen. Dieser Typ stellt Daten über installierte Software, Prozessinformationen, TCP/IP-Verbindungen usw. bereit.

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

Cloudbasierte Erkennungsmethoden

Cloud-Discovery verwendet Erkennungsmuster, um Geräte und Anwendungen abzufragen und Informationen darüber zu sammeln. Ein Muster ist eine Folge von Befehlen, deren Zweck darin besteht, Attribute eines CI und seiner ausgehenden Verbindungen zu ermitteln. In Cloud-Discovery sind viele vorkonfigurierte Muster verfügbar. Darüber hinaus werden im ServiceNow Store regelmäßig neue Muster verfügbar.

Ihre Instanz kann auch Benachrichtigungen und Warnungen aus der Cloud-Umgebung erkennen. Diese Events werden über eine REST-Verbindung an Ihre Instanz gesendet. Ihre Instanz kann diese Events dann verarbeiten und CIs in CMDB entsprechend aktualisieren.

Hinweis: Für die eventgestützte Erkennung für Amazon AWS Cloud, Microsoft Azure Cloud und Google Cloud Platform ist Cloud Provisioning and Governance nicht erforderlich.

Cloud-Ressourcen verwalten

Die Instanz zeigt alle Ergebnisse von Cloud-Discovery auf der Discovery-Homepage an. Sie können Drilldowns zu bestimmten Zeitplänen, erkannten Geräten, Cloud-Ressourcen und Fehlern durchführen. Sortieren Sie diese Ergebnisse, um sie genauer zu betrachten, und zeigen Sie Erkennungstrends für die erkannten Geräte an. Anhand von Fehlermeldungen erhalten Sie konkrete Empfehlungen zur Behebung von Problemen.

Cloud-Discovery auf Now Platform

Cloud-Discovery verwendet MID-Server für den Zugriff auf externe Geräte und Anwendungen im lokalen Netzwerk eines Unternehmens. Weitere Informationen zu den Fähigkeiten des MID-Servers in Bezug auf Cloud-Discovery finden Sie unter MID-Server .

Cloud Provisioning and Governance hängt von den von Cloud-Discovery gefundenen Informationen ab. Cloud Provisioning and Governance bietet eine einzige Oberfläche, über die Sie auf Cloud-Ressourcen zugreifen, Cloud-Angebote in einem Katalog veröffentlichen und die Nutzung dieser Ressourcen verwalten können.

Darüber hinaus verwenden die folgenden Geschäftsbereiche und Produkte von Now Platform die Informationen, die Cloud-Discovery liefert: IT Service Management, Security Incident Response, Hardware Asset Management, Software Asset Management, Governance, Risk und Compliance und Anwendungs-Portfoliomanagement.

Cloud-Discovery Setup mit klassisch Cloud-Discovery

Sie beginnen mit Cloud-Discovery, indem Sie Anmeldeinformationen, Servicekonten, Zeitpläne und MID-Server konfigurieren.

Das Einrichten von Cloud-Discovery ist die erste Stufe der Cloud-Erkennung und der Verwendung von Cloud Provisioning and Governance zur Verwaltung erkannter Cloud-Ressourcen.

Cloud-Discovery ist Teil von Now Platform und stellt einige der auf der gesamten Plattform genutzten Mechanismen und Funktionen bereit. Es gibt allerdings auch einige Konfigurationen, die nur für Cloud-Discovery gelten.

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster

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

sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Führen Sie die folgenden Aufgaben exakt in der Reihenfolge aus, in der sie unten aufgeführt sind:

1. Bewerten Sie Ihre Cloud-Bereitstellung, und planen Sie, wie Sie darin eine Erkennung durchführen möchten.
2. Discovery anfordern.
3. Installieren und konfigurieren Sie die MID Server.
4. Richten Sie Servicekonten ein, und konfigurieren Sie den Zugriff darauf.
   - AWS-Servicekonten einrichten
   - Servicekonten für Azure erstellen
   - Servicekonten für GCP erstellen
   - Servicekonten für VMware erstellen
5. Konfigurieren Sie für Amazon AWS Cloud und Microsoft Azure CloudBenachrichtigungen und Warnungen von Amazon AWS Cloud und Microsoft Azure Cloud, um die erforderlichen Aktualisierungen ohne zusätzliches Scannen an Ihrem CMDB vorzunehmen.
   - Konfigurieren Sie den Konfigurationsservice AWS, um Ereignisbenachrichtigungen an die Instanz ServiceNow zu senden
   - Konfigurieren Sie den Warnungsservice Microsoft Azure so, dass er automatisch aktualisiert wird CMDB
   - Konfigurieren Sie den Service Google Stackdriver Logging für die automatische Aktualisierung von CMDB
   - Konfigurieren Sie den Service VMware-Events für die automatische Aktualisierung von CMDB

   Hinweis: Für die eventgestützte Erkennung ist Cloud Provisioning and Governance nicht erforderlich.
6. Stellen Sie sicher, dass Ihre ServiceNow-Instanz über die relevanten Muster und CI-Klassen (Typen) für Cloud-Ressourcen verfügt. Möglicherweise müssen Sie die neueste Version der folgenden Anwendungen aus dem ServiceNow Store bereitstellen.
   - Discovery and Service Mapping Patterns
   - CMDB CI Class Models
7. Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen.

Cloud-Discovery Setup mit Arbeitsbereich für Cloud-Vorgänge

Führen Sie die erforderlichen Verfahren aus, um sich auf die Erkennung von Ressourcen-CIs in der Cloud vorzubereiten.

Das Einrichten von Cloud-Discovery ist die erste Stufe der Cloud-Erkennung und der Verwendung von Cloud Provisioning and Governance zur Verwaltung erkannter Cloud-Ressourcen.

Cloud-Discovery ist Teil von Now Platform und stellt einige der auf der gesamten Plattform genutzten Mechanismen und Funktionen bereit. Es gibt allerdings auch einige Konfigurationen, die nur für Cloud-Discovery gelten.

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

Arbeitsbereich für Cloud-Vorgänge stellt eine erweiterte Möglichkeit zum Erstellen von Discovery-Zeitplänen bereit. Sie können auch die für die Erkennung von Cloud-Ressourcen erforderlichen Voraussetzungen überprüfen, z. B. Anmeldeinformationen und Servicekonten.

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Führen Sie die folgenden Aufgaben exakt in der Reihenfolge aus, in der sie unten aufgeführt sind:

1. Bewerten Sie Ihre Cloud-Bereitstellung, und planen Sie, wie Sie darin eine Erkennung durchführen möchten.
2. Discovery anfordern.
3. Installieren Sie Cloud Discovery Workspace.
4. Installieren und konfigurieren Sie die MID Server.
5. (Für Amazon AWS Cloud und Microsoft Azure Cloud) Konfigurieren Sie Benachrichtigungen und Warnungen von Amazon AWS Cloud und Microsoft Azure Cloud, um die erforderlichen Aktualisierungen an Ihrer CMDB ohne zusätzliches Scannen vorzunehmen.
   - Konfigurieren Sie den Konfigurationsservice AWS, um Ereignisbenachrichtigungen an die Instanz ServiceNow zu senden
   - Konfigurieren Sie den Warnungsservice Microsoft Azure so, dass er automatisch aktualisiert wird CMDB
   - Konfigurieren Sie den Service Google Stackdriver Logging für die automatische Aktualisierung von CMDB
   - Konfigurieren Sie den Service VMware-Events für die automatische Aktualisierung von CMDB

   Hinweis: Für die eventgestützte Erkennung ist Cloud Provisioning and Governance nicht erforderlich.
6. Stellen Sie sicher, dass Ihre ServiceNow-Instanz über die relevanten Muster und CI-Klassen (Typen) für Cloud-Ressourcen verfügt. Möglicherweise müssen Sie die neueste Version der folgenden Anwendungen aus dem ServiceNow Store bereitstellen.
   - Muster für Discovery und Service-Mapping
   - CMDB CI Class Models
7. Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge.

Zugehörige Informationen

Arbeitsbereich für Cloud-Vorgänge

Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen

Erstellen Sie abhängig von der von Ihnen gewählten Cloud Discovery-Methode (Servicekonten oder IP-Bereiche) Zeitpläne für die Erkennung von Cloud-Ressourcen.

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

Discovery-Manager-Schnittstelle

Verwenden Sie die Schnittstelle zur Cloud-Discovery-Zeitplankonfiguration, um die Informationen einzugeben, die Sie für den Zugriff auf Ihre Servicekonten und Unterkonten benötigen. Sie können die Anmeldeinformationen angeben, um ausgewählte Konten zu validieren. Testen Sie die Verbindungen zu Ihren Konten, und erstellen Sie dann Zeitpläne, um die Cloud-Ressourcen in den ausgewählten Rechenzentren zu erkennen.

Fortschrittsanzeige

Während Sie die einzelnen Konfigurationsphasen abschließen, können Sie den Fortschritt auf den Registerkarten oben im Discovery-Manager nachverfolgen. Abgeschlossene Phasen werden durch ein Häkchen gekennzeichnet. Ein dunkler Unterstrich markiert die aktuelle Phase. Die Registerkarten sind interaktiv, sodass Sie zu einer Phase wechseln können, indem Sie auf die entsprechende Registerkarte klicken.

Discovery-Manager-Bezeichnungen anpassen

Die Tabelle „Feldoptionen für Servicekonten“ [service_account_field_options] enthält Felder zum Ändern der Bezeichnungen im Discovery-Manager. Über diese Felder können Sie den Discovery-Manager für die Verarbeitung neuer Service Provider anpassen oder vorhandene Bezeichnungen ändern, um interne Richtlinien zu erfüllen. Beispiel: Die Bezeichnung der Account-ID Microsoft Azure lautet standardmäßig Microsoft Azure Abonnement-GUID. Sie können sie je nach Bedarf in „Abonnement-ID“, „Konto-ID“ oder in eine beliebige andere Einstellung ändern.

Servicekonto auswählen und Anmeldeinformationen testen

Geben Sie Ihren Cloud-Provider an, und wählen Sie das zu erkennende Servicekonto aus. Sie können ein oder alle verfügbaren Unterkonten in einen Zeitplan aufnehmen. Wählen Sie die Anmeldeinformationen für das Cloud-Servicekonto aus, und testen Sie die Verbindung.

Vorbereitungen
Bevor Sie versuchen, Cloud-Discovery zu konfigurieren, benötigen Sie mindestens einen validierten MID-Server mit dem Status **In Betrieb**. Der MID-Server muss die IP-Bereiche erreichen, auf die sich die Erkennung beziehen soll. Sie können den MID-Server mithilfe des geführten Setups MID-Server verwenden oder durch manuelles Herunterladen und Ausführen des Installationsprogramms installieren. Weitere Informationen können Sie den MID-Server-Installationsanweisungen für Linux und Windows entnehmen. Stellen Sie sicher, dass Sie den für Cloud-Discovery verwendeten MID-Server mit Cloud-Management-Funktionalität konfigurieren.

Erforderliche Rolle: discovery_admin oder admin

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

Warum und wann dieser Vorgang ausgeführt wird

Der ServiceNow® Cloud-Discovery-Assistent beginnt mit der Kontoauswahl und der Testphase. Verwenden Sie zur Vermeidung langer Wartezeiten oder unerwarteter Zeitüberschreitungen die Systemeigenschaft *cdu.record.watcher.timeout*, um die maximale Wartezeit für diese Cloud-Discovery-Konfigurationsprozesse zu definieren:

- Servicekonto validieren
- Mitgliedskonto-Discovery
- Discovery für logische Rechenzentren

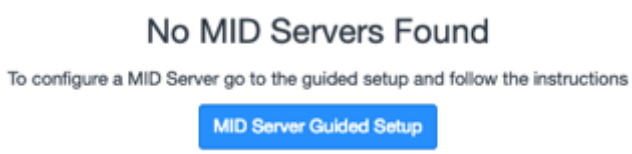
Der Standardwert für die Zeitüberschreitung beträgt 300.000 Millisekunden bzw. 5 Minuten.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**, und klicken Sie dann im Willkommensbildschirm **auf Cloud-Ressourcen erkennen**.

   Hinweis: Der Willkommensbildschirm enthält einen Link zu Discovery Schnellstart. Dieser Assistent wurde entwickelt, um schnell eine grundlegende Discovery einzurichten. Sie können Schnellstart verwenden, um Discovery auszuwerten oder um neue Netzwerkgeräte zu erkunden. Die Anleitung ist jedoch nicht für die Erkennung von Cloud-Ressourcen konzipiert.

   Wenn das System keinen geeigneten MID-Servererkennen kann, werden Sie aufgefordert, einen MID-Server mithilfe des geführten Setups für MID-Server zu installieren und zu konfigurieren. Diese Benachrichtigung wird auch angezeigt, wenn ein vorhandener MID-Server aufgrund eines Upgrades nicht verfügbar ist.

2. Wählen Sie im Bereich „Grundlegende Informationen“ des Discovery-Managers im Feld **Provider** den Namen Ihres Cloud-Providers aus, zum Beispiel **AWS** oder **Azure**.
   Im Bereich „MID Servers“ des Assistenten wird die Anzahl der validierten und verfügbaren MID Servers angezeigt.
3. Wenn Sie AWS, Azureoder GCPverwenden, können Sie den Auswahltyp MID-Server im Feld **MID-Auswahltyp** angeben.

   Hinweis: Die AuswahlAWS und Azure ist erst nach der Migration zum musterbasierten Discoveryverfügbar. Weitere Informationen finden Sie unter Migrieren Sie von CAPI zu Mustern.

   Die folgenden Optionen sind verfügbar:

   - **MID-Server automatisch auswählen**: Der Assistent verwendet automatisch einen geeigneten MID-Server.
   - **Spezifischer MID-Server**: Der Assistent verwendet den im Feld **MID-Server** angegebenen MID-Server. Um MID Servers zu filtern und anzuzeigen, die für die Übernahme einer IAM-Rolle zur Erkennung von Cloud-Ressourcen konfiguriert sind, aktivieren Sie die Option **Discovery ohne Anmeldeinformationen**.

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

4. Wenn kein MID-Server über die Cloud-Management-Fähigkeit verfügt, klicken Sie **auf MID-Server konfigurieren**, und konfigurieren Sie einen entsprechend.

   a. Navigieren zu **MID-Server** > **Fähigkeiten**.

   b. Wählen Sie aus der Liste der MID-Server-Fähigkeiten **Cloud Management** aus.
   Sie können auch **ALLE** auswählen, wodurch Cloud Management standardmäßig eingeschlossen ist.

   c. Klicken Sie in der zugehörigen Liste MID Servers auf **Bearbeiten**, und fügen Sie dann Ihr MID Servers zur Fähigkeit hinzu.

   d. Klicken Sie auf **Speichern**.
   Ihre MID Servers sind für die Kommunikation mit Ihren Cloud-Servicekonten bereit.

5. Geben Sie im Feld **Zeitplanname** einen eindeutigen und beschreibenden Namen für den Zeitplan ein.
6. Wählen Sie im Bereich „Servicekonten“ ein vorhandenes Konto für den neu benannten Zeitplan aus.
   Wenn Sie ein vorhandenes Konto auswählen, füllt das System das Formular automatisch mit den verfügbaren Informationen. Wenn Sie ein Konto hinzufügen, müssen Sie die Konto-ID, Anmeldeinformationen und gegebenenfalls die URL angeben. Für VMware müssen Sie die URL angeben.
   - Die AWS-Konto-ID entspricht der Konto-ID.
   - Die Azure-Konto-ID entspricht der Azure-Abonnement-GUID.
   - Die GCP-Konto-ID entspricht der Projekt-ID.
   - Die VMware-Konto-ID entspricht der UUID der VM-Instanz.

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

Hinweis: Die VMware-Erkennung kann ohne Servicekonto ausgeführt werden. Um VMware-Ressourcen zu erkennen, konfigurieren Sie den Zeitplan zur Ausführung für die IP-Adresse des vCenter-Servers .

7. Wählen Sie die Anmeldeinformationen für dieses Cloud-Servicekonto aus, oder fügen Sie neue Anmeldeinformationen hinzu.

   a. Um Anmeldeinformationen hinzuzufügen, klicken Sie auf das Pluszeichen (**+**).

   b. Wählen Sie den entsprechenden Typ der Cloud-Anmeldeinformationen in der Liste aus.

   c. Füllen Sie das Formular aus, und klicken Sie auf **Speichern**.

   Hinweis: Sie können AWS so konfigurieren, dass temporäre Anmeldeinformationen für Servicekonten generiert werden. Mit dieser Funktionalität müssen keine Anmeldeinformationen für die Instanz definiert werden. Dadurch erhöht sich die Sicherheit Ihrer Mitgliedskonten (Unterkonten). Details finden Sie unter Zugriff für AWS-Servicekonten einrichten.

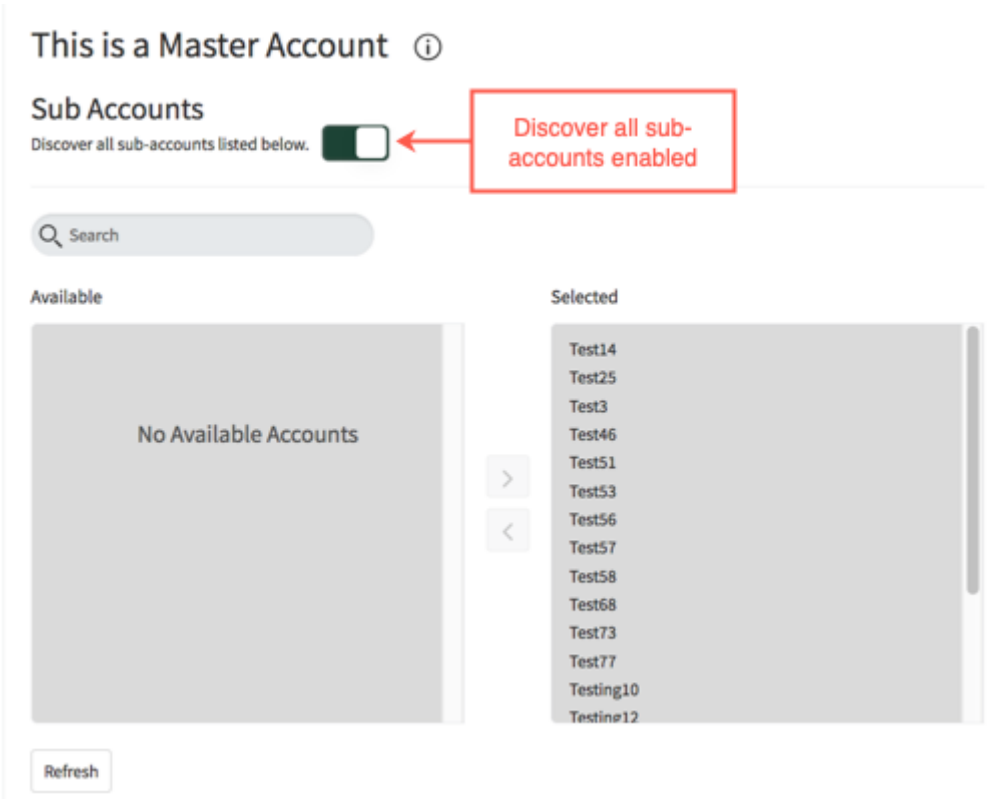
8. Klicken Sie auf **Testaccount**, um das Konto mit den angegebenen Details zu validieren.

   Nachrichten in der Headerleiste benachrichtigen Sie über die Validierungsergebnisse. Wenn Sie ein Verwaltungskonto angegeben haben und der Verbindungstest erfolgreich war, zeigt der Assistent einen Auswahlbildschirm für alle Mitgliedskonten an, die dem Verwaltungskonto zugeordnet sind. Standardmäßig sind alle aktuellen Mitgliedskonten für den Zeitplan ausgewählt und können nicht in die Liste „Verfügbar“ verschoben werden.

   Hinweis:

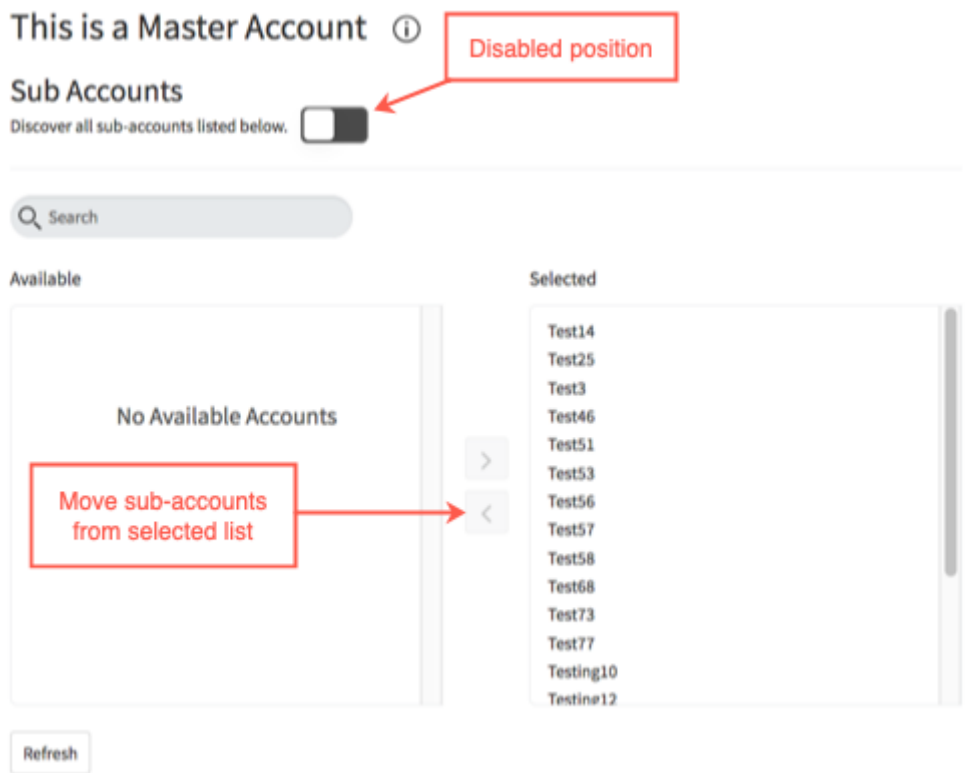
   Wenn der Validierungsprozess keine oder kürzlich hinzugefügte Unterkonten zurückgibt, klicken Sie auf **Mitglieder aktualisieren**, oder führen Sie den Validierungsprozess erneut aus. Wenn bei der Validierung wiederholt Zeitüberschreitungen auftreten, erhöhen Sie das Zeitüberschreitungsintervall in der MID Server-Eigenschaft `cdu.record.watcher.timeout`.

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



9. Um bestimmte Unterkonten für den Zeitplan auszuwählen, deaktivieren Sie die automatische Auswahlfunktion.

Standardmäßig sind alle Unterkonten ausgewählt. Um die Funktion zu deaktivieren und die Auswahl bestimmter zu erkennender Rechenzentren zuzulassen, schieben Sie den Umschalter nach links.



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

10. Um ein Unterkonto auszuschließen, ziehen Sie das Unterkonto aus der Liste „Ausgewählt“ in die Liste „Verfügbar“.
11. Klicken Sie auf **Weiter**.

Zu erkennendes Cloud Provider-Rechenzentrum auswählen

Cloud-Discovery zeigt die Liste der verfügbaren Rechenzentren an, wenn Sie den Serviceaccount validieren. Geben Sie an, welche Rechenzentren mit diesem Zeitplan erkannt werden sollen.

Vorbereitungen
Erforderliche Rolle: discovery_admin, admin

Prozedur

1. Um die zu erkennenden Rechenzentren auszuwählen, klicken Sie in der Registerkartenleiste des Discovery-Managers auf die Phase **Rechenzentren auswählen**.
   Standardmäßig werden alle dem Servicekonto zugeordneten Rechenzentren für den Cloud-Discovery -Zeitplan ausgewählt.

   Hinweis:

   - Wenn keine Rechenzentren angezeigt werden, wählen Sie **Rechenzentren aktualisieren** aus, oder führen Sie die Kontovalidierung erneut aus. Wenn bei der Validierung wiederholt Zeitüberschreitungen auftreten, erhöhen Sie das Zeitüberschreitungsintervall in der Eigenschaft *cdu.record.watcher.timeout* MID-Server.
   - Sie können Cloud-Discovery so konfigurieren, dass die Liste der Unterkonten und Rechenzentren vor jeder geplanten Erkennung automatisch aktualisiert wird. Weitere Informationen finden Sie unter Automatische Aktualisierung von Unterkonten und Rechenzentren aktivieren.

2. Um bestimmte Rechenzentren für den Zeitplan auszuwählen, deaktivieren Sie die automatische Auswahlfunktion, indem Sie den **Umschalter Alle unten aufgeführten Rechenzentren** erkennen nach links schieben.
3. Verschieben Sie die Rechenzentren, die Sie erkennen möchten, aus der Liste **Verfügbar** in die Liste **Ausgewählt**.
4. Wählen Sie in der Registerkartenleiste die nächste Phase aus.
   Bei Bedarf können Sie IP-Bereiche konfigurieren, um virtuelle Maschinen (VM) zu erkennen, oder zur Phase „Zeitplan“ wechseln und das Setup Cloud-Discovery abschließen.

Erkennung von virtuellen Maschinen aktivieren

Während der Erkennung der Cloud-Ressourcen können Sie virtuelle Maschinen (VMs) erkennen. Cloud-Discovery führt eine umfassende Erkennung der durch den Cloud-Zeitplan identifizierten virtuellen Maschinen (VMs) anhand ihrer IP-Adressen aus.

Vorbereitungen
Alle MID Servers, die Sie für Cloud-Discovery verwenden möchten, müssen validiert sein, den Status **In Betrieb** aufweisen und auf die IP-Bereiche im Cloud Provider-Konto zugreifen können.

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

Wichtig: Durch den Upgrade-Prozess von Madrid auf New York werden die vorhandenen Cloud-Discovery -Zeitplänedeaktiviert. Stellen Sie sicher, dass alle Zeitpläne im Discovery-Manager reaktiviert, die möglicherweise während eines Upgrades von Madrid deaktiviert wurden. Diese Zeitpläne weisen in der Tabelle „Discovery-Zeitplan“ [discovery_schedule] den **Ausführen**-Status **Nicht definiert** auf.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Für die mit Cloud-Discovery verwendeten MID Servers müssen Sie keine IP-Bereiche konfigurieren. Cloud-Discovery wählt die IP-Adressen der virtuellen Maschinen automatisch in den Rechenzentren aus, die Sie im Assistenten ausgewählt haben.

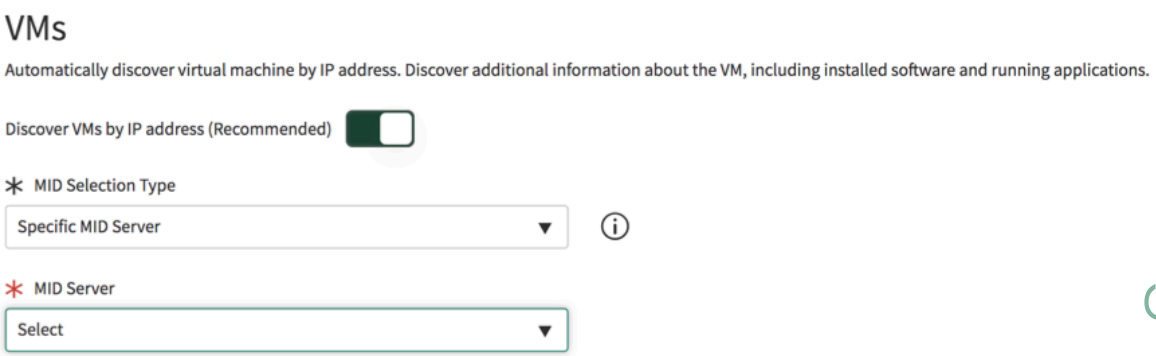
Prozedur

1. Zur Erkennung der VMs, die Teil des aktuellen Zeitplans sind, klicken Sie in der Registerkartenleiste des Discovery-Managers auf die Phase **Virtuelle Computer erkennen (optional)**.

   Die Erkennung von virtuellen Maschinen (VMs) ist standardmäßig aktiv.

   Hinweis: Weitere Informationen zur Funktionsweise von **Virtuelle Maschinen erkennen (optional)** in Cloud-Discovery finden Sie im KB-Artikel Funktionsweise von „Virtuellen Computer erkennen“ (optional) in Cloud-Discovery .

2. Wählen Sie den zu verwendenden MID-Server aus.
   Die folgenden Optionen sind verfügbar:
   - **Automatische Auswahl**: Discovery wählt automatisch einen geeigneten MID-Server aus.
   - **Spezifischer MID Server-Cluster**: Discovery verwendet das genannte MID-Server-Cluster.
   - **Spezifischer MID Server**: Discovery verwendet den genannten MID-Server.



3. Um die VM-Erkennung zu deaktivieren, schieben Sie den Schalter **VMs anhand IP-Adresse erkennen** nach links.
   Das Feld **MID-Auswahltyp** wird ausgeblendet.
4. Wählen Sie in der Registerkartenleiste die Phase **Zeitplan erstellen** aus.

Laufzeit für einen Cloud-Discovery-Zeitplan festlegen

In der letzten Phase des Assistenten für Discovery-Manager wird der Zeitplan erstellt, der die Erkennung der Cloud-Ressourcen auslöst.

Vorbereitungen

Erforderliche Rolle: admin, discovery_admin

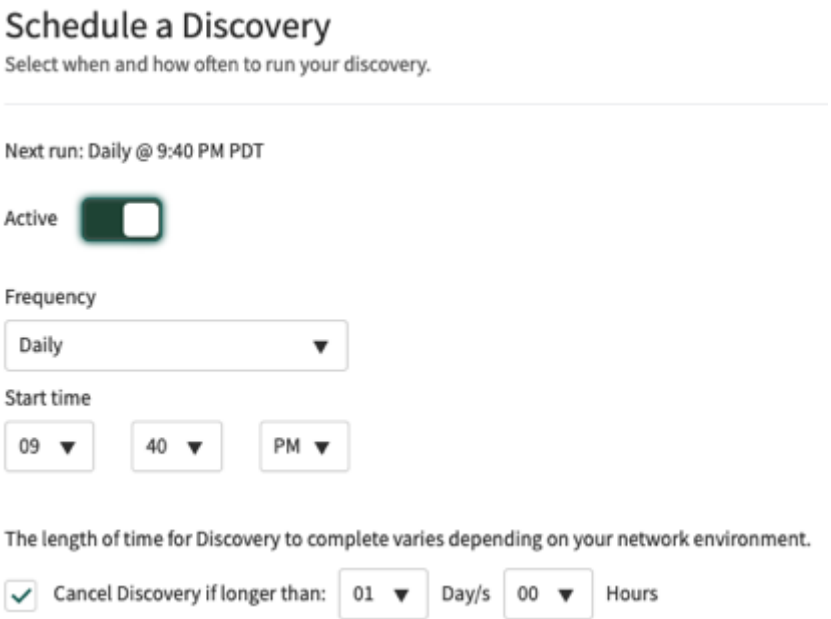
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch über das Formular „Discovery-Zeitplan“ auf die Zeitplanphase des Discovery-Managers zugreifen. Navigieren zu **Discovery** > **Discovery-Zeitpläne** und klicken Sie in der Liste der Zeitpläne **auf Cloud-Discovery**.

Prozedur

1. Um den Cloud Discovery-Zeitplan zu konfigurieren, wählen Sie in der Registerkartenleiste des Discovery-Managers die Option **Zeitplan erstellen** aus.
   Der Zeitplan ist standardmäßig aktiv.
2. Konfigurieren Sie, wann und wie oft der Zeitplan ausgeführt werden soll, und definieren Sie einen Timeout-Schwellenwert, wenn Sie Cloud-Discovery auf eine bestimmte Dauer beschränken möchten.



3. Zum Deaktivieren des Zeitplans verschieben Sie den Schalter **Aktiv** nach links.
4. Schließen Sie den Prozess Cloud-Discovery für die Planung von ab, indem Sie eine der folgenden Optionen auswählen:
   - **Beenden und ausführen**: wird Discovery sofort unter Verwendung der aktuellen Konfiguration ausgeführt. Alle nachfolgenden Cloud-Erkennungen werden gemäß dem von Ihnen angegebenen Zeitplan ausgeführt.
   - **Fertigstellen**: Beendet den Assistenten und führt Cloud-Discovery gemäß dem von Ihnen angegebenen Zeitplan aus.

Nächste Maßnahme

Öffnen Sie die Discovery-Homepage, und zeigen Sie die Ergebnisse Ihres Discoveryan.

Automatische Aktualisierung von Unterkonten und Rechenzentren aktivieren

Konfigurieren Sie die Cloud-Discovery, um die Liste der Unterkonten und Rechenzentren vor jeder geplanten Erkennung automatisch zu aktualisieren. Wenn von Cloud-Discovery neue Unterkonten oder Rechenzentren identifiziert werden, werden sie der Configuration Management Database (CMDB) hinzugefügt und in den Discovery-Zeitplan aufgenommen.

Vorbereitungen

Erforderliche Rolle: admin

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

Warum und wann dieser Vorgang ausgeführt wird

Von Cloud-Discovery kann die Liste der Unterkonten und Rechenzentren, die von einem Discovery-Zeitplan abgedeckt werden, automatisch aktualisiert werden, sofern die folgenden Kriterien erfüllt sind:

- Der Cloud-Provider ist Amazon Web Services (AWS), Microsoft Azure oder Google Cloud Platform (GCP).
- Die Eigenschaft *glide.discovery.cdu.auto_refresh_sub_accounts_and_ldcs* ist auf `true` festgelegt.
- Der Zeitplan Cloud-Discovery wird für ein Verwaltungskonto erstellt.
- Der Zeitplan Cloud-Discovery wird so konfiguriert, dass die Ressourcen aller Unterkonten und Rechenzentren des Verwaltungskontos erkannt werden.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen Sie nach dem folgenden Systemeigenschaftsdatensatz, und öffnen Sie den Datensatz.

   glide.discovery.cdu.auto_refresh_sub_accounts_and_ldcs

3. Ändern Sie im Formular das Feld „Wert“ in `true`.
4. Wählen Sie **Aktualisieren**.

Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Erstellen Sie abhängig von der von Ihnen gewählten Discovery-Methode (Servicekonten oder IP-Bereiche) Zeitpläne für die Discovery von Cloud-Ressourcen. Im Discovery-Zeitplan werden die verschiedenen Einstellungen für die Cloud-Discovery definiert.

Vorbereitungen

- Stellen Sie sicher, dass die Anwendung Arbeitsbereich für Cloud-Vorgänge auf Now Platforminstalliert ist. Weitere Informationen finden Sie unter Arbeitsbereich für Cloud-Vorgänge installieren.
- Bevor Sie versuchen, Cloud-Discovery zu konfigurieren, benötigen Sie mindestens einen validierten MID-Server mit dem Status **In Betrieb**. Der MID-Server muss die IP-Bereiche erreichen, auf die sich die Erkennung beziehen soll. Sie können den MID-Server mithilfe des geführten Setups MID-Server verwenden oder durch manuelles Herunterladen und Ausführen des Installationsprogramms installieren. Weitere Informationen können Sie den MID-Server-Installationsanweisungen für Linux und Windows entnehmen. Stellen Sie sicher, dass Sie den für Cloud-Discovery verwendeten MID-Server mit Cloud-Management-Funktionalität konfigurieren.
- Vergewissern Sie sich, dass auf der Now Platform geeignete Anmeldeinformationen verfügbar sind, damit eine Verbindung mit den Servicekonten hergestellt werden kann, für die Sie die Discovery durchführen möchten.
- Standardmäßig wird die musterbasierte Discovery ausgeführt. In Szenarien, in denen die neueste Musteranwendung nicht installiert ist, schlägt die Erkennung fehl, und Sie werden aufgefordert, die CAPI-basierte Erkennung zu installieren oder zu migrieren. Weitere Informationen finden Sie unter Migrieren Sie von CAPI zu Mustern.

Erforderliche Rolle: discovery_admin

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

Warum und wann dieser Vorgang ausgeführt wird

Der ServiceNow® Cloud-Discovery-Assistent beginnt mit der Kontoauswahl und der Testphase. Verwenden Sie zur Vermeidung langer Wartezeiten oder unerwarteter Zeitüberschreitungen die Systemeigenschaft *cdu.record.watcher.timeout*, um die maximale Wartezeit für diese Cloud-Discovery-Konfigurationsprozesse zu definieren:

- Servicekonto validieren
- Mitgliedskonto-Discovery
- Discovery für logische Rechenzentren

Der Standardwert für die Zeitüberschreitung beträgt 300.000 Millisekunden bzw. 5 Minuten.

Sie können Cloud-Discovery so konfigurieren, dass die Liste der Unterkonten und Rechenzentren vor jeder geplanten Discovery automatisch aktualisiert wird. Weitere Informationen finden Sie unter Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen.

Prozedur

1. Navigieren zu *Arbeitsbereich für Cloud-Vorgänge* > *Cloud-Discovery* > **Dashboard**.
2. Wählen Sie **Neuer Discovery-Zeitplan**.
3. Wählen Sie den Cloud Provider aus.

   a. Füllen Sie die Werte im Formular „Choose the provider (Anbieter auswählen)“ aus. Eine Beschreibung der Formularfelder finden Sie unter Erstellen Sie eine neue Formularreferenz für den Discovery-Zeitplan.

   b. Wählen Sie **Weiter**.

4. Wählen Sie einen Serviceaccount für den Cloud-Discovery-Zeitplan aus, oder erstellen Sie einen Serviceaccount.

   Beschreibungen der Felder für den Serviceaccount finden Sie unter Cloud-Discovery Formularreferenz für Service-Account. Wenn Sie ein vorhandenes Konto auswählen, füllt das System das Formular automatisch mit den verfügbaren Informationen.

   Hinweis: Die Discovery für VMware kann ohne Servicekonto ausgeführt werden. Um VMware-Ressourcen zu erkennen, konfigurieren Sie den Zeitplan zur Ausführung für die IP-Adresse des vCenter-Servers.

   a. Wahlweise: Um die Verbindung mit dem Servicekonto zu überprüfen, wählen Sie **Testaccount** aus.

   b. Wahlweise: Wenn Sie den Discovery-Zeitplan für einen Verwaltungsaccount erstellen, geben Sie an, ob alle Mitgliedsaccounts oder nur bestimmte Mitgliedsaccounts erkannt werden sollen.
   Standardmäßig werden alle vorhandenen Mitgliedsaccounts für den Discovery-Zeitplan ausgewählt.

   c. Wahlweise: Wenn Sie den Discovery-Zeitplan für einen Verwaltungsaccount erstellen und der Validierungsprozess die Unteraccounts nicht zurückgibt, wählen Sie **Aktualisieren**, oder wiederholen Sie die Accountvalidierung.

   d. Wählen Sie **Weiter**.

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

5. Rechenzentren für Discovery-Zeitplan auswählen.
   Sie können entweder alle mit dem Servicekonto verbundenen Rechenzentren oder bestimmte Rechenzentren auswählen.
   a. Wahlweise: Wenn Sie bestimmte Rechenzentren erkennen möchten, wählen Sie die **Rechenzentren** in der Dropdown-Liste „Rechenzentren auswählen“ aus.
   b. Wahlweise: Wenn keine Rechenzentren angezeigt werden, wählen Sie **Rechenzentren aktualisieren**, oder wiederholen Sie die Accountvalidierung.
   c. Wählen Sie **Weiter**.
6. Wahlweise: Geben Sie an, ob Sie virtuelle Computer (VM) und ihre Attribute erkennen möchten.
   a. Wählen Sie einen MID-Server oder ein MID-Cluster aus, von dem die VMs erkannt werden können.
   Wenn Sie sich bei der MID-Auswahl nicht sicher sind, wählen Sie **Automatische Auswahl***MID-Server*.
   b. Wählen Sie **Weiter**.
7. Erstellen Sie einen Zeitplan für die Ausführung der Cloud-Discovery.
   a. Wählen Sie eine Ausführungshäufigkeit für den Cloud-Discovery-Zeitplan aus.
   b. Geben Sie eine Startzeit für die Ausführung der Discovery an.
   c. Wahlweise: Geben Sie Kriterien zum Abbrechen der Discovery an.
   d. Aktivieren Sie den Discovery-Zeitplan.
8. Führen Sie eine der folgenden Aktionen aus.

Option	Beschreibung
Beenden und ausführen	Von Cloud-Discovery wird der Zeitplan gespeichert und ausgeführt.
Fertigstellen	Cloud-Discovery speichert den Zeitplan und führt ihn gemäß der definierten Häufigkeit aus.

Amazon AWS Cloud Discovery

Verwenden Sie Cloud-Discovery, um virtuelle Ressourcen in Ihren AWS-Organisationen zu erkennen: Management und Mitgliederkonten.

Stellen Sie sicher, dass Sie Cloud-Discovery einrichten und alle erforderlichen Berechtigungen und Anmeldeinformationen für die Erkennung von AWS-Ressourcen bereitstellen. Weitere Informationen finden Sie unter AWS-Servicekonten einrichten.

Erkannte Beziehungen zwischen virtuellen Computern, Rechenzentren und anderen CIs

Klasse	Beziehung	Klasse
VM-Instanz [cmdb_ci_vm_instance]	Gehostet auf	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

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

Klasse	Beziehung	Klasse
		vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter] **Hinweis:** Diese Tabellen erweitern die Tabelle „Logisches Rechenzentrum“ [cmdb_ci_logical_datacenter]. Die Beziehung zwischen der VM und dem spezifischen Typ des Rechenzentrums ergibt sich aus der Tabelle „Logisches Rechenzentrum“.
	Virtualisiert	Computer [cmdb_ci_computer] **Hinweis:** Das ist ein virtueller Computer. Das Feld **Ist virtuell** enthält den Wert **true**.
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Enthält	Ressourcengruppe [cmdb_ci_resource_group]
	Hosts	Öffentliche IP-Adresse [cmdb_ci_cloud_public_ip_address]
	Gehostet auf	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
	Hosts	Speicherkonto [cmdb_ci_cloud_storage_account]
	Enthält	Verfügbarkeitszone [cmdb_ci_av availability_zone]
	Enthält	Hostcluster [cmdb_ci_host_cluster]
	Hosts	BS-Vorlage [cmdb_ci_os_template]
	Hosts	Berechnungsvorlage [cmdb_ci_compute_template]
	Gehostet auf	Cloud Management-Netzwerkschnittstellen [cmdb_ci_nic]
Cloud-Datenbank [cmdb_ci_cloud_database]	Eigentümer von	IP-Adresse [cmdb_ci_ip_address]
	Gehostet auf	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
	Gehostet auf	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Um erkannte Komponenten in Serviceinstanzen aufzunehmen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von Service-Mappingverwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Konfiguration der Tag-basierten Discovery.

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

Service-Mapping verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

AWS-Konfigurationsservice

Wenn Sie den AWS Config-Service konfiguriert haben, kann die Instanz Benachrichtigungen erhalten, wenn Änderungen an Cloud-Ressourcen auftreten. Discovery kann reagieren und Updates vornehmen.

Die Instanz kann eine AWS-Konfigurationsbenachrichtigung vom Nachrichtentyp `ConfigurationItemChangeNotification` für die folgenden Ressourcentypen erkennen:

- AWS::DynamoDB::Table
- AWS::EC2::Instance
- AWS::EC2::SecurityGroup
- AWS::EC2::Subnet
- AWS::EC2::Volume
- AWS::EC2::VPC
- AWS::ElasticLoadBalancing::LoadBalancer
- AWS::ElasticLoadBalancingV2::LoadBalancer
- AWS::RDS::DBInstance
- AWS::S3::Bucket

Discovery kann dann Aktualisierungen an Datensätzen in der Tabelle „Antwortzuordnungen“ [sn_cmp_response_mapping] vornehmen, die im Feld **Datenquelle** den Wert „Cloud-Event“ aufweisen.

API-Liste für Amazon Connect Discovery

AWS Rechenzentrum (cmdb_ci_aws_datacenter)

CI-Attribute	Attribute von **AWS**
object_id	DescribeRegionsResponse.regionInfo.item.regionName
Name	DescribeRegionsResponse.regionInfo.item.regionName
region	DescribeRegionsResponse.regionInfo.item.regionName
status	Installiert/Deaktiviert

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

Verfügbarkeitszone (cmdb_ci_av availability_zone)

CI-Attribute	Attribute von **AWS**
object_id	DescribeAvailabilityZonesResponse.availabilityZoneInfo.item.zoneName
Name	DescribeAvailabilityZonesResponse.availabilityZoneInfo.item.zoneName
Status	DescribeAvailabilityZonesResponse.availabilityZoneInfo.item.zoneState
status	Installiert/Deaktiviert

Öffentliche IP-Adresse (cmdb_ci_cloud_public_ipaddress)

CI-Attribute	Attribute von **AWS**
object_id	DescribeAddressesResponse.addressesSet.item.allocationid
name	DescribeAddressesResponse.addressesSet.item.elastic_name
public_ip_address	DescribeAddressesResponse.addressesSet.item.eip
region	DescribeAddressesResponse.addressesSet.item.region
Domäne	DescribeAddressesResponse.addressesSet.item.domain
status	Installiert/Deaktiviert

Virtueller Server (cmdb_ci_vm_instance)

CI-Attribute	Attribute von **AWS**
memory	DescribeInstancesResponse.reservationSet.item.instancesSet.item.instanceType - Hardwaretypen aufrufen
Status	DescribeInstancesResponse.reservationSet.item.instancesSet.item.instanceState.name
object_id	DescribeInstancesResponse.reservationSet.item.instancesSet.item.instanceId
CPUs	DescribeInstancesResponse.reservationSet.item.instancesSet.item.instanceType - Hardwaretypen aufrufen
disks	DescribeVolumesResponse.volumeSet.item.attachmentSet.item.blockDeviceMapping[].size
nics	DescribeInstancesResponse.reservationSet.item.instancesSet.item.networkInterfaceSet[].size
vm_inst_id	DescribeInstancesResponse.reservationSet.item.instancesSet.item.instanceId
Name	"DescribeInstancesResponse.reservationSet.item.instancesSet.item.tagSet.item.value==Name OR DescribeInstancesResponse.reservationSet.item.instancesSet.item.instanceId"
Status	Installiert/Deaktiviert

Speichervolume (cmdb_ci_storage_volume)

CI-Attribute	Attribute von **AWS**
state	DescribeVolumesResponse.volumeSet.item.status
storage_type	block

Automatische Übersetzung

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

Speichervolume (cmdb_ci_storage_volume) (Fortsetzung)

volume_id	DescribeVolumesResponse.volumeSet.item.volumeId
Name	"DescribeVolumesResponse.volumeSet.item.volumeId OR DescribeVolumesResponse.volumeSet.item.tagSet.value==Name"
size_bytes	DescribeVolumesResponse.volumeSet.item.size * 1024 * 1024 * 1024
object_id	DescribeVolumesResponse.volumeSet.item.volumeId
size	DescribeVolumesResponse.volumeSet.item.size + "GB"
Status	Installiert/Deaktiviert

Image (cmdb_ci_os_template)

CI-Attribute	Attribute von **AWS**
Name	DescribeImagesResponseimagesSet.item.name
object_id	DescribeImagesResponseimagesSet.item.imageId
guest_os	DescribeImagesResponseimagesSet.item.platform
image_type	DescribeImagesResponseimagesSet.item.imageType
root_device_type	DescribeImagesResponseimagesSet.item.rootDeviceType
image_source	DescribeImagesResponseimagesSet.item.imageLocation
Status	Installiert/Deaktiviert

Netzwerk (cmdb_ci_network)

CI-Attribute	Attribute von **AWS**
is_shared	FALSCH
object_id	DescribeVpcsResponse.vpcSet.item.vpcId
Status	DescribeVpcsResponse.vpcSet.item.state
netmask	Nicht zutreffend
Name	"DescribeVpcsResponse.vpcSet.item.tagSet.item.value <key=""name""> OR DescribeVpcsResponse.vpcSet.item.cidrBlock+ '"'["+DescribeVpcsResponse.vpcSet.item.tagSet.item.vpcId+"]'""
is_external	FALSCH
cidr	DescribeVpcsResponse.vpcSet.item.cidrBlock + DescribeVpcsResponse.vpcSet.item.cidrBlockAssociationSet.item.ipv6CidrBlock
default_gateway	DescribeInternetGatewaysResponse.internetGatewaySet.item.internetGatewayId
status	Installiert/Deaktiviert

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

Cloud-Schlüsselpaar (cmdb_ci_cloud_key_pair)

CI-Attribute	Attribute von **AWS**
Name	aws-service_account_name + region_name + DescribeKeyPairsResponse.keySet.item.keyName
finger_print	DescribeKeyPairsResponse.keySet.item.keyFingerprint
object_id	DescribeKeyPairsResponse.keySet.item.keyName
Status	Installiert/Deaktiviert

Cloud-Lastenausgleichsmodul (cmdb_ci_cloud_load_balancer)

CI-Attribute	Attribute von **AWS**
object_id	DescribeLoadBalancersResponse.DescribeLoadBalancersResult.LoadBalanc
Name	DescribeLoadBalancersResponse.DescribeLoadBalancersResult.LoadBalanc
Status	Verfügbar/Beendet
dns_name	DescribeLoadBalancersResponse.DescribeLoadBalancersResult.LoadBalanc
fqdn	DescribeLoadBalancersResponse.DescribeLoadBalancersResult.LoadBalanc
canonical_hosted_zone_name	DescribeLoadBalancersResponse.DescribeLoadBalancersResult.LoadBalanc
canonical_hosted_zone_id	DescribeLoadBalancersResponse.DescribeLoadBalancersResult.LoadBalanc
Status	Installiert/Deaktiviert

AWS RDS (cmdb_ci_cloud_database)

CI-Attribute	Attribute von **AWS**
category – DB-Klasse („Vorlagen“ für CPU und Arbeitsspeicher)	https://rds.us-east-1.amazonaws.com/?Action=DescribeDBInstances
object_id – DB-Name (eindeutig für jedes LRZ)	https://rds.us-east-1.amazonaws.com/?Action=DescribeDBInstances&DBInstanceIdentifi
fqdn – DB-Endpunktadresse (DNS-Name)	https://tagging.us-east-1.amazonaws.com/ (Tags-Erkennung)
tcp_port – DB-Endpunktport	DescribeDBInstancesResponse.DescribeDBInstancesResult.DBInstances.Endpoint.Port Oder DescribeDBClustersResponse.DescribeDBClustersResult.DBClusters.Port
name – DB-Name	DescribeDBInstancesResponse.DescribeDBInstancesResult.DBInstances.DBName

Automatische Übersetzung

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

AWS RDS (cmdb_ci_cloud_database) (Fortsetzung)

	Oder DescribeDBClustersResponse.DescribeDBClustersResult.DBClusters.DBClusterIdentifier
version – DB-Version	DescribeDBInstancesResponse.DescribeDBInstancesResult.DBInstances.EngineVersion Oder DescribeDBClustersResponse.DescribeDBClustersResult.DBClusters.EngineVersion
type – Datenbanktyp (Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle Database, and SQL Server)	DescribeDBInstancesResponse.DescribeDBInstancesResult.DBInstances.Engine Oder DescribeDBClustersResponse.DescribeDBClustersResult.DBClusters.Engine
operational_status – Status der Datenbank	Funktionsfähig/Nicht funktionsfähig/Deaktiviert
ip_address – IP-Adresse des FQDN	com.snc.sw.util.DNSUtils.resolveHostName(DescribeDBInstancesResponse.DescribeDBIns
vendor – „Amazon“	Amazon
fqdn – DB-Endpunktadresse (DNS-Name)	DescribeDBInstancesResponse.DescribeDBInstancesResult.DBInstances.Endpoint.Address Oder DescribeDBClustersResponse.DescribeDBClustersResult.DBClusters.Endpoint

Cloud-Subnetz (cmdb_ci_cloud_subnet)

CI-Attribute	Attribute von **AWS**
Name	"DescribeSubnetsResponse.subnetSet.item.cidrBlock OR DescribeSubnetsResponse.subnetSet.item.tagSet.item.value <key=""name"">"
object_id	DescribeSubnetsResponse.subnetSet.item.subnetId
cidr	DescribeSubnetsResponse/subnetSet/item/cidrBlock + /DescribeSubnetsResponse/subnetSet/item/ ipv6CidrBlockAssociationSet/item/ipv6CidrBlock/
status	Installiert/Deaktiviert
state	DescribeSubnetsResponse.subnetSet.item.state
available_ip_count	DescribeSubnetsResponse.subnetSet.item.availableIpAddressCount

Automatische Übersetzung

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

Cloud-Netzwerk (Interfaces cmdb_ci_nic)

CI-Attribute	Attribute von **AWS**
Name	DescribeNetworkInterfacesResponse.networkInterfaceSet.item.networkInterfaceId
private_ip	DescribeNetworkInterfacesResponse.networkInterfaceSet.item.privateIpAddress
object_id	DescribeNetworkInterfacesResponse.networkInterfaceSet.item.networkInterfaceId
public_ip	DescribeNetworkInterfacesResponse.networkInterfaceSet.item.asscoiation.publicIp
gateway	Nicht zutreffend
private_dns	DescribeNetworkInterfacesResponse.networkInterfaceSet.item.privateDnsName
state	In Gebrauch/Beendet
owner	Nicht zutreffend
netmask	255.255.255.0
is_source_dest_check	DescribeNetworkInterfacesResponse.networkInterfaceSet.item.sourceDestCheck
public_dns	DescribeNetworkInterfacesResponse.networkInterfaceSet.item.asscoiation.publicDns
status	Installiert/Deaktiviert

Speicherzuordnung (cmdb_ci_storage_mapping)

CI-Attribute	Attribute von **AWS**
Name	DescribeVolumesResponse.volumeSet.item.attachmentSet.item.blockDeviceMapping.ebs.v
object_id	DescribeVolumesResponse.volumeSet.item.attachmentSet.item.blockDeviceMapping.ebs.v
mapping_type	DescribeVolumesResponse.volumeSet.item.attachmentSet.item.blockDeviceMapping.rootD
host	DescribeVolumesResponse.volumeSet.item.attachmentSet.item.blockDeviceMapping.publi
mount_point	DescribeVolumesResponse.volumeSet.item.attachmentSet.item.blockDeviceMapping.rootD

Sicherheitsgruppen (cmdb_ci_compute_security_group)

CI-Attribute	Attribute von **AWS**
object_id	DescribeSecurityGroupsResponse.securityGroupInfo.item.groupId
Name	DescribeSecurityGroupsResponse.securityGroupInfo.item.groupName
state	Verfügbar/Beendet
status	Installiert/Deaktiviert

Hardwaretypen (cmdb_ci_compute_template)

CI-Attribute	Attribute von **AWS**
object_id	Keine AWS-Antwort
Name	DescribeInstanceTypesResponse.instanceTypeSet.item.instanceType
vcpus	DescribeInstanceTypesResponse.instanceTypeSet.item.vCpuInfo.defaultVCpus

Automatische Übersetzung

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

Hardwaretypen (cmdb_ci_compute_template) (Fortsetzung)

memory_mb	DescribeInstanceTypesResponse.instanceTypeSet.item.memoryInfo.sizeInMiB
local_storage_gb	DescribeInstanceTypesResponse.instanceTypeSet.item.instanceStorageInfo.totalSizeInGB
cores	DescribeInstanceTypesResponse.instanceTypeSet.item.vCpuInfo.defaultCores
status	Installiert/Deaktiviert

Öffentliche IP-Adresse der Cloud (cmdb_ci_cloud_lb_ipaddress)

CI-Attribute	Attribute von **AWS**
object_id	<aufgelöster DNS-Name>
Name	<aufgelöster DNS-Name>
ipaddress_type	<wird nicht von CMP gefüllt>
status	Installiert/Deaktiviert

Lastenausgleichsservice der Cloud (cmdb_ci_lb_service)

CI-Attribute	Attribute von **AWS**
Name	DescribeLoadBalancersResponse.DescribeLoadBalancersResult.LoadBalancers.DNSName
object_id	DescribeLoadBalancersResponse.DescribeLoadBalancersResult.LoadBalancers.DNSName
port	DescribeListenersResponse.DescribeListenersResult.Listeners.Port
server_port	DescribeListenersResponse.DescribeListenersResult.Listeners.Port
server_protocol	DescribeListenersResponse.DescribeListenersResult.Listeners.Protocol
listener_protocol	DescribeListenersResponse.DescribeListenersResult.Listeners.Protocol
status	Installiert/Deaktiviert
ssl_certificate_id	Nicht zutreffend

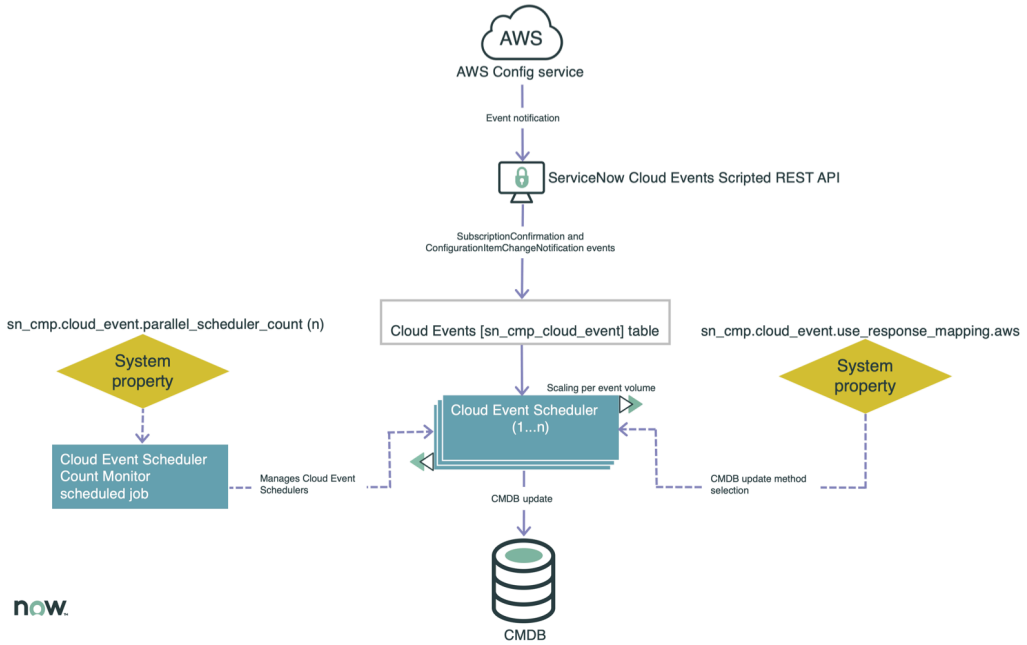
AWS ereignisgesteuerte Discovery

Der Konfigurationsservice Amazon Web Services (AWS) kann Ereignisse für alle Änderungen des Lebenszyklusstatus oder der Konfiguration einer Cloud-Ressource auslösen. Die ServiceNow® ereignisgesteuerte Discovery verwendet die -Ereignisse, um die neuesten Ressourceninformationen in Configuration Management Database (CMDB)automatisch zu aktualisieren.

Automatische Übersetzung

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

Übersicht über die ereignisgesteuerte Discovery AWS von [].



Konfigurieren Sie den Konfigurationsservice AWS, um SNS-Benachrichtigungen (Simple Notification Service) an die Instanz ServiceNow zu senden. Weitere Informationen finden Sie unter Konfigurieren Sie den Konfigurationsservice AWS, um Ereignisbenachrichtigungen an die Instanz ServiceNow zu senden. Nachdem Sie den Service konfiguriert haben, beginnt er mit dem Senden von Ereignisbenachrichtigungen an die ServiceNow Cloud Events-REST API. Wenn ein Ereignis eines der folgenden Kriterien erfüllt, schreibt die API es in die Tabelle „Cloud-Ereignisse“ [sn_cmp_cloud_event]:

- Der *Type* des Ereignisses ist *SubscriptionConfirmation*.
- *Type* des Ereignisses ist *Notification*, und *messageType* ist *ConfigurationItemChangeNotification*.
- Amazon CloudWatch hat das Ereignis für eine Änderung des Tags ausgelöst, das dem Configuration Item (CI) zugeordnet ist.

Der Cloud Event Scheduler wählt dann die Ereignisse im Status Bereit für die Batch-Verarbeitung aus. Während der Ereignisverarbeitung verwendet die ereignisgesteuerte Discovery Antwortzuordnungen oder -muster, um die Details der betroffenen Ressource in CMDBzu aktualisieren. Die Eigenschaft *sn_cmp.cloud_event.use_response_mapping_aws* bestimmt die Aktualisierungsmethode CMDB. Um den Status eines Ereignisses zu verstehen, überprüfen Sie den Status in der Tabelle „Cloud-Ereignisse“ [sn_cmp_cloud_event].

Ab Release Yokohama ist die Eigenschaft *sn_cmp.cloud_event.use_response_mapping_aws* standardmäßig auf true festgelegt. Wenn diese Eigenschaft auf true festgelegt ist und geeignete Antwortzuordnungen verfügbar sind, verwendet die ereignisgesteuerte Discovery die Antwortzuordnungen, um das CI in CMDBzu erstellen oder zu aktualisieren. Andernfalls löst die eventgesteuerte Discovery die entsprechenden Muster aus, um die betroffene Ressource zu erkennen und das CI in CMDBzu erstellen oder zu aktualisieren.

Ab Release Yokohama verwenden Sie die Eigenschaft *sn_cmp.cloud_event.parallel_scheduler_count*, um den Cloud Event Scheduler anhand der Ereignis-Zuflussrate zu skalieren. Die parallele Ausführung mehrerer Cloud-Ereignisplaner trägt zur Verbesserung der Ereignisverarbeitungsrate der Instanz bei. Weitere Informationen zur Skalierung der Cloud Event Scheduler finden Sie unter Skalieren Sie die Cloud-Ereignisplaner AWS ..

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

Während der Eventverarbeitung identifiziert der Cloud Event Scheduler die Domäne des Serviceaccounts und weist sie dem Event zu. Wenn beim Identifizieren der Domäne vor der Verarbeitung ein Fehler auftritt, kann das Event manchmal nicht zugewiesen werden und wird für alle Domänen sichtbar. Um zu verhindern, dass die fehlgeschlagenen Events für alle Domänen sichtbar sind, können Sie die Eigenschaft *sn_cmp.error_events.default_domain* auf die sys_id der Service Provider-Domäne festlegen, sodass die fehlgeschlagenen Events nur dem Domänenadministrator des Service Providers angezeigt werden.

Konfigurieren Sie den Konfigurationsservice AWS, um Ereignisbenachrichtigungen an die Instanz ServiceNow zu senden

Konfigurieren Sie den Konfigurationsservice Amazon Web Services (AWS), um Ereignisbenachrichtigungen an die Instanz ServiceNow zu senden, wenn sich der Lebenszyklusstatus einer Ressource ändert.

Vorbereitungen

- Stellen Sie sicher, dass das Plugin Discovery (com.snc.discovery) in der Instanz installiert und aktiviert ist.
- Stellen Sie sicher, dass Sie gültige AWS -Abonnements (Servicekonten) haben und die zugehörigen logischen Rechenzentren erkannt werden.
- Stellen Sie sicher, dass das Passwort des Anwenderkontos, das zum Abonnieren der Instanz beim Simple Notification Service (SNS) verwendet wird, kein @- oder #-Zeichen enthält.

Erforderliche Rollen:

- Stellen Sie sicher, dass die Rolle AWS verfügbar ist, die auf die folgenden Services und Ressourcen zugreifen kann:
  - SNS
  - AWS-Konfigurationsservice
  - Ressourcentypen, für die Sie die Konfigurationsänderung nachverfolgen möchten
- ServiceNow-Rollen:
  - discovery_admin
  - sn_cmp.cloud_event_integration: Die Zugriffsanmeldeinformationen eines Anwenders mit der Rolle „sn_cmp.cloud_event_integration“ sind erforderlich, um die Instanz für die SNS-Benachrichtigungen zu abonnieren. Weitere Informationen finden Sie unter Benutzer erstellen und Einem Benutzer eine Rolle zuweisen .

Warum und wann dieser Vorgang ausgeführt wird

Die eventgesteuerte Discovery ServiceNow® von verwendet die -Ereignisse, um die neuesten Ressourceninformationen in der Configuration Management Database (CMDB) zu aktualisieren. Weitere Informationen finden Sie unter AWS ereignisgesteuerte Discovery.

Viele der Schritte im Thema werden im AWS-Portal ausgeführt. Weitere Informationen finden Sie in der folgenden AWS-Dokumenten.

- Einrichten von Amazon SNS-Benachrichtigungen
- Das AWS Config-Dashboard anzeigen

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

Hinweis:

Wenn Sie Domänentrennung für Cloud-Discovery verwenden, sind auch die Ereignisse nach Domänen getrennt. Daher können Sie die Details eines verarbeiteten Events nur anzeigen, wenn es zu Ihrer Domäne gehört. Wenn ein Ereignis keinem Servicekonto zugeordnet ist, wird es der globalen Domäne zugeordnet.

Während der Eventverarbeitung identifiziert der Cloud Event Scheduler die Domäne des Serviceaccounts und weist sie dem Event zu. Wenn beim Identifizieren der Domäne vor der Verarbeitung ein Fehler auftritt, kann das Event manchmal nicht zugewiesen werden und wird für alle Domänen sichtbar. Um zu verhindern, dass die fehlgeschlagenen Events für alle Domänen sichtbar sind, können Sie die Eigenschaft *sn_cmp.error_events.default_domain* auf die sys_id der Service Provider-Domäne festlegen, sodass die fehlgeschlagenen Events nur dem Domänenadministrator des Service Providers angezeigt werden.

Prozedur

1. Melden Sie sich beim Account AWS an.
2. Navigieren Sie auf der Seite „Services“ zu **AWS-Services** > **Services suchen** > **Einfacher Benachrichtigungsservice**.
3. Erstellen Sie ein Amazon SNS-Thema.
   Der Konfigurationsservice AWS verwendet das SNS-Thema, um die Ereignisbenachrichtigungen zu veröffentlichen.

   a. Navigieren Sie im SNS-Dashboard zu **Themen** > **Thema „Erstellen“.**.

   b. Füllen Sie die Felder des Formulars aus.

   Formular „Thema erstellen“.

Feld	Beschreibung
Typ	Thementyp der Benachrichtigung. Wählen Sie den Thementyp **Standard** aus.
Name	Name des SNS-Themas.
Anzeigename: optional	Anzeigename des SNS-Themas.

   c. Wählen Sie **Thema erstellen**.

4. Abonnieren Sie das SNS-Thema für die Instanz.
   Nach dem Abonnieren des SNS-Themas kann die -Instanz die Ereignisbenachrichtigungen von der Cloud AWS empfangen.

   a. Wählen Sie auf der Seite „Themendetails“ **Abonnement erstellen aus**.

   b. Füllen Sie die Felder des Formulars aus.

   Formular zum Erstellen von Abonnements

Feld	Beschreibung
Protokoll	Zu verwendende Kommunikationsprotokolle.

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

Feld	Beschreibung
	Wählen Sie HTTPS für das Abonnement aus, das CMDBautomatisch aktualisiert. **Hinweis:** Nach dem Erstellen des HTTPS-Abonnements können Sie ein separates Abonnement erstellen, das E-Mails an eine angegebene Person sendet.
Endpunkt	URL der ServiceNow Cloud-Ereignisse-REST API. Stellen Sie sicher, dass die URL der folgenden Syntax entspricht: `https://<username>:<user_password>@<instance_URL>/api/now/cloud_event`

c. Wählen Sie **Abonnement erstellen aus**.

5. Aktivieren Sie **die AWS-** Ereignisaufzeichnung.

a. Navigieren zu **Konfiguration** > **Einstellungen**.

b. Wählen Sie auf der Seite Einstellungen **die Option Bearbeiten**aus.

c. Aktivieren Sie das Kontrollkästchen **Aktivieren**.

d. Wählen Sie im Dialogfeld „Aufzeichnung starten“ **die Option Bestätigen aus**.

e. Füllen Sie die Werte im Formular Einstellungen bearbeiten aus.

Eine Beschreibung der Formularfelder finden Sie unter Referenz des Formulars „Einstellungen bearbeiten“..

f. Wählen Sie **Speichern**.

Nächste Maßnahme
Nachdem einige Events generiert wurden, navigieren Sie zum Cloud-Benutzerportal, um sich die Events anzusehen.

Skalieren Sie die Cloud-Ereignisplaner AWS .

Skalieren Sie die Cloud-Ereignisplaner, um die Ereignisverarbeitungsrate für Amazon Web Services (AWS) in der Instanz ServiceNow zu verbessern.

Vorbereitungen
Erforderliche Rolle: cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn die Instanz eine große Anzahl von Ereignissen empfängt und diese nicht innerhalb angemessener Zeit verarbeitet, erstellen Sie zusätzliche Cloud-Ereignisplanungen.
Die parallele Ausführung mehrerer Cloud-Ereignisplaner trägt zur Verbesserung der Ereignisverarbeitungsrate der Instanz bei. Wenn die Rate des Ereignis-Zuflusses abnimmt, können Sie einige der Cloud Event Scheduler deaktivieren. Weitere Informationen finden Sie unter AWS ereignisgesteuerte Discovery.

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

Prozedur

1. Konfigurieren Sie die Anzahl der Cloud-Ereignisplaner, die Sie verwenden möchten.

   a. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.

   b. Suchen Sie in der Spalte Name nach *sn_cmp.cloud_event.parallel_scheduler_count*.

   c. Legen Sie im Eigenschaftsformular *sn_cmp.cloud_event.parallel_scheduler_count* das Feld **Wert** auf einen geeigneten Wert fest.

   Wichtig:

   - Stellen Sie sicher, dass der Wert der Eigenschaft *sn_cmp.cloud_event.parallel_scheduler_count* die Anzahl der verfügbaren Worker-Knoten nicht überschreitet.
   - Wenn Sie mehrere Domänen haben, in denen Cloud-Ereignisse konfiguriert sind, verwenden Sie die Eigenschaft *sn_cmp.cloud_event.parallel_scheduler_count* mit Vorsicht, da jeder Cloud-Ereignisplaner mehrere Iterationen für jede Domäne hat, in der Cloud-Ereignisse aktiv sind.

   d. Wählen Sie **Aktualisieren**.

2. Führen Sie die geplante Aufgabe zur Überwachung der Anzahl von Cloud-Event-Zeitplanern aus.
   Die geplante Aufgabe „Cloud Event Scheduler-Anzahlüberwachung“ verwaltet die Anzahl der Cloud Event Scheduler gemäß dem in der Eigenschaft *sn_cmp.cloud_event.parallel_scheduler_count* angegebenen Wert.

   a. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.

   b. Öffnen Sie die geplante Aufgabe „Cloud Event Scheduler Count Monitor“.

   c. Wählen Sie **Jetzt ausführen**.

Erstellen Sie einen Datenbankindex für die Tabelle „Cloud-Ereignisse“.

Erstellen Sie einen Datenbankindex aus den angegebenen Spalten der Tabelle „Cloud-Ereignisse“ [sn_cmp_cloud_event], um die Leistung der Cloud-Ereignisverarbeitung AWS zu verbessern.

Vorbereitungen

Stellen Sie sicher, dass der Bereich auf Cloud Provisioning and Governancefestgelegt ist.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie nach dem Upgrade von Cloud Provisioning and Governance auf Release Utah einen Datenbankindex aus den angegebenen Spalten der Tabelle „Cloud-Events“ [sn_cmp_cloud_event]. Der Datenbankindex hilft, die Leistung der Verarbeitung von AWS-Events (Amazon Web Services) durch die Instanz zu verbessern. Wenn Sie Cloud Provisioning and Governance mit Release Utah verwenden, wird der Datenbankindex bei der Installation der Anwendung automatisch erstellt.

Anstatt den Datenbankindex manuell zu erstellen, können Sie ihn mit einer regelmäßigen Aufgabe erstellen. Weitere Informationen finden Sie unter ServiceNow®

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

ereignisgesteuerte Discovery: Erstellen Sie einen Datenbankindex für die Tabelle „Cloud-Ereignisse“ (KB1207069).

Sie können auch die Cloud-Ereignisplaner skalieren, um die Verarbeitungsrate von Amazon Web Services (AWS) in der Instanz ServiceNow zu verbessern. Weitere Informationen finden Sie unter Skalieren Sie die Cloud-Ereignisplaner AWS ..

Prozedur

1. Zu `https://`navigieren<instance name> .service-now.com/sn_cmp_cloud_event_list.do
2. Auswahlvorgang **Spaltenoptionen** > **Konfigurieren** > **Tabelle**.
3. Wählen Sie die zugehörige Liste **Datenbankindizes** aus.
4. Wählen Sie **Neu**.
5. Wählen Sie in der Liste der verfügbaren Spalten die folgenden Spalten in der angegebenen Reihenfolge aus.
   a. **Status**
   b. **Prozess-ID**
   c. **Ressourcen-ID**
6. Wählen Sie **Index erstellen aus**.
7. Wahlweise: Wählen Sie eine Option aus, um anzugeben, ob Sie bei der Indexerstellung eine Benachrichtigung erhalten möchten.
8. Wählen Sie **OK**.
9. Benennen Sie den neuen Index um, um die Identifizierung zu erleichtern.

Erkennung von Azure-Clouds

Wenn sich Ihre Cloud-Ressourcen in einer Azure-Cloud befinden, müssen Sie eine Benutzeridentität erstellen, die als Service-Prinzipal bezeichnet wird und MID-Server Berechtigungen für den Zugriff auf ausgewählte Ressourcen gewährt.

Azure-Verwaltungsgruppen und -Abonnements

Eine Azure-Verwaltungsgruppe enthält andere Verwaltungsgruppen und Abonnements. Die Verwaltungsgruppen in einer Azure-Cloud-Umgebung bilden eine Hierarchie, enthält jedoch keine und enthält keine Volumes oder virtuellen Computer. Abonnements enthalten Cloud-Ressourcen, zum Beispiel virtuelle Computer. Die Abonnements, die zu Verwaltungsgruppen gehören, werden als Unterkonten bezeichnet.

Die Verwendung von Verwaltungsgruppen hat folgende Vorteile:

Einfaches Füllen von Unterkonten

Nachdem Sie die Verwaltungsgruppe konfiguriert und die erforderlichen Anmeldeinformationen angegeben haben, können Sie das Konto testen. Wenn der Test erfolgreich ist, gibt Discovery eine Liste von Abonnements in dieser Verwaltungsgruppe zurück. Aus dieser Liste können Sie mindestens ein Abonnement-Unterkonto auswählen, das mithilfe der Verwaltungsgruppe in den Erkennungszeitplan aufgenommen wird. Weitere Informationen zur Hierarchie von Verwaltungsgruppen und Abonnements finden Sie unter Ressourcen mit Azure-Verwaltungsgruppen organisieren

Erkennung von Unterkontoressourcen mithilfe dynamisch bezogener Anmeldeinformationen

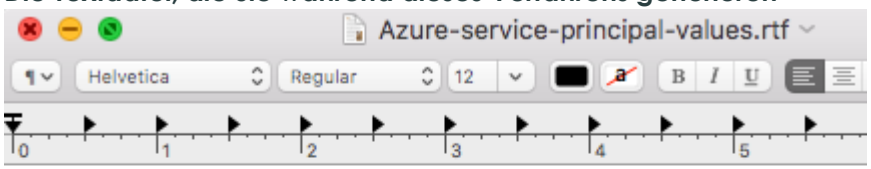
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie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

Wenn Sie Discovery für Ihre Abonnements ausführen, benötigen Sie keine separaten Anmeldeinformationen für jedes Unterkonto. Discovery erkennt die Anmeldeinformationen für die Verwaltungsgruppe und ordnet sie allen Unterkontos des Abonnements zu. Der Cloud Discovery-Prozess verarbeitet Anmeldeinformationen automatisch, indem temporäre Anmeldeinformationen für jedes Unterkonto über eine Azure-API abgerufen werden. Sie können die Standardkonfiguration verwenden oder den MID Server anpassen, um andere Rollen für zusätzliche Steuerungen und Sicherheitseinstellungen zu übernehmen. Darüber hinaus kann Discovery die Liste der in einem Discovery-Zeitplan enthaltenen Unterkonten und Rechenzentren automatisch aktualisieren. Weitere Informationen finden Sie im KB-Artikel Neuere Accounts/Unteraccounts automatisch über Cloud-Discovery abrufen.

Ein Dienstprinzipal für Azure-Cloud-Services ähnelt einem Microsoft Windows-Servicekonto, über das Windows-Prozesse in einer Active Directory-Domäne miteinander kommunizieren können.

Kopieren Sie zum Erstellen des Azure-Dienstprinzipals in Ihrer ServiceNow-Instanz die Anmeldeinformationen des Dienstprinzipals aus dem Azure-Portal in einen Texteditor und übertragen Sie diese Werte dann in die Instanz.

Die Textdatei, die Sie während dieses Verfahrens generieren



Directory ID: 8bcdd120-9979-491e-8683-d9a4550bdd

Application ID: e6821ea9-e5c5-428a-b50c-7ea62993b2d

Application key: d348050-f893ccb7-hg84yg8-rg200hd

Subscription ID: 4803be48c3ee89-96d2-4fed-bedb-22e49013ee89

Diese Tabelle zeigt den Wert des Azure-Dienstprinzipals und den Ort in Azure, an dem Sie die für die Anmeldeinformationen benötigten Werte finden können.

Einstellung für Cloud Provisioning and Governance	**Wert „Azure-Dienstprinzipal“**	**Speicherort des Azure-Werts**
Mandanten-ID	Wert der Azure-**Verzeichnis-ID** aus der Textdatei	**Azure Active Directory** > **Eigenschaften** > **Verzeichnis-ID**
Client-ID	Wert der Azure-**Anwendungs-ID** aus der Textdatei	**Azure Active Directory** > **App-Registrierungen** > **Registrierte App.Anwendungs-ID**
Geheimer Schlüssel	Wert des Azure-**Anwendungsschlüssels** aus der Textdatei	**Azure Active Directory** > **App-Registrierungen** > **Registrierte App** > **Einstellungen** > **Schlüssel (ausgeblendet)**

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

Einstellung für Cloud Provisioning and Governance	**Wert „Azure-Dienstprinzipal“**	**Speicherort des Azure-Werts**
Account-ID	Azure **-Abonnement-ID, die** der Mandanten-ID zugeordnet ist.	**Azure Active Directory** > **Abonnements** > **Abonnement-ID**

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Um erkannte Komponenten in Serviceinstanzen aufzunehmen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von Service-Mappingverwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Konfiguration der Tag-basierten Discovery.

Service-Mapping verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	**Beziehung**	**CI**
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

API-Liste für Azure Cloud Discovery

Logisches Rechenzentrum (cmdb_ci_logical_datacenter)

CI-Attribute	**Azure-Attribute**
object_id	response.name
Name	response.name
region	response.displayName
Status	Installiert

Verfügbarkeitszone (cmdb_ci_av availability_zone)

CI-Attribute	**Azure-Attribute**
object_id	response.id
Name	response.name
Status	Installiert/Deaktiviert
Status	

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

Ressourcengruppe (cmdb_ci_resource_group)

CI-Attribute	Azure-Attribute
object_id	id
Name	Name
Status	available
Status	Installiert/Deaktiviert

Netzwerk (cmdb_ci_network)

CI-Attribute	Azure-Attribute
object_id	id
Status	
Name	Name
cidr	properties.addressSpace.addressPrefixes

Subnetz (cmdb_ci_cloud_subnet)

CI-Attribute	Azure-Attribute
subnetName	response.name
subnetId	response.id
resourceGroup	response.properties.resourceGuid
networkId	response.id.split('/subnets/')
networkName	getNetwork(networkId)
cidrBlock	response.properties.addressSpace.addressPrefixes

Speichervolume (cmdb_ci_storage_volume)

CI-Attribute	Azure-Attribute
Status	properties.provisioningState
storage_type	properties.BlobType
volume_id	id
Name	Name
size_bytes	properties.diskSizeGB * 1024 * 1024 * 1024
object_id	id
size	response.properties.diskSizeGB
"volume_container"	containerName
Status	Installiert/Deaktiviert

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

Sicherheitsgruppen (cmdb_ci_compute_security_group)

CI-Attribute	Azure-Attribute
object_id	id
Name	Name
Status	properties.provisioningState

Virtueller Server (cmdb_ci_vm_instance)

CI-Attribute	Azure-Attribute
memory	properties.hardwareProfile.vmSize
state	Die Instanzstatus: • erfolgreich: auf • wird ausgeführt: erfolgreich/wird beendet • Zuordnung aufheben: wird gestoppt/gestoppt • freigegeben: aus • beendet: Fehler
object_id	id
CPUs	properties.hardwareProfile.vmSize
disks	properties.storageProfile.dataDisks
nics	properties.networkProfile.networkInterfaces[].size
vm_inst_id	properties.vmId
Name	Name
Status	Installiert/Deaktiviert

Hardwarevorlage (cmdb_ci_compute_template)

CI-Attribute	Azure-Attribute
Name	Name
object_id	Name
vcpus	numberOfCores
memory_mb	memoryInMB
local_storage_gb	resourceDiskSizeInMB
cores	numberOfCores

Öffentliche IP-Adresse der Cloud (cmdb_ci_cloud_public_ipaddress)

CI-Attribute	Azure-Attribute

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

Öffentliche IP-Adresse der Cloud (cmdb_ci_cloud_public_ipaddress) (Fortsetzung)

object_id	response.id
Name	response.name
public_dns	properties.dnsSettings.fqdn
public_ip_address	properties.ipAddress

Cloud LB IP-Adresse (cmdb_ci_cloud_lb_ipaddress)

CI-Attribute	Azure-Attribute
object_id	"properties.frontendIPConfigurations.properties.privateIPAddress ODER properties.frontendIPConfigurations.properties.publicIPAddress, dann API für öffentliche IP-Adresse aufrufen"
Name	"properties.frontendIPConfigurations.properties.privateIPAddress ODER properties.frontendIPConfigurations.properties.publicIPAddress, dann API für öffentliche IP-Adresse aufrufen"
ipaddress_type	"properties.frontendIPConfigurations.properties.privateIPAddress ==> Private IP-Adresse ODER properties.frontendIPConfigurations.properties.publicIPAddress ==> Öffentliche IP-Adresse"
Status	Installiert

„Cloud-Netzwerkschnittstellen (cmdb_ci_nic)“

CI-Attribute	Azure-Attribute
object_id	id
Name	Name
private_ip	properties.ipConfigurations
public_dns	API für öffentliche IP-Adresse aufrufen – properties.dnsSettings.fqdn
Status	properties.provisioningState
is_static	properties.ipConfigurations
mac_address	properties.macAddress
public_ip	API für öffentliche IP-Adresse aufrufen –

Image (cmdb_ci_os_template)

CI-Attribute	Azure-Attribute
Name	response.id
object_id	response.name
guest_os	properties.storageProfile.osDisk.osType
image_source	id

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

Image (cmdb_ci_os_template) (Fortsetzung)

Status	Installiert/Deaktiviert

Cloud-Speicherkonto (cmdb_ci_cloud_storage_account)

CI-Attribute	Azure-Attribute
Name	Name
object_id	id
sku_name	sku.name
Status	properties.provisioningState

Lastenausgleichsmodul [cmdb_ci_cloud_load_balancer]

CI-Attribute	Azure-Attribute
object_id	response.id
Name	response.name
Status	
dns_name	.
fqdn	
canonical_hosted_zone_name	

Anmeldeinformationen für Azure-Cloud erstellen

Wenn sich Ihre Cloud-Ressourcen in einer Azure-Cloud befinden, erstellen Sie Anmeldeinformationen, die auf das Azure-Konto zugreifen können. Dieses Verfahren erfordert die Konfiguration Ihres Azure-Kontos.

Vorbereitungen

Erforderliche Rollen:

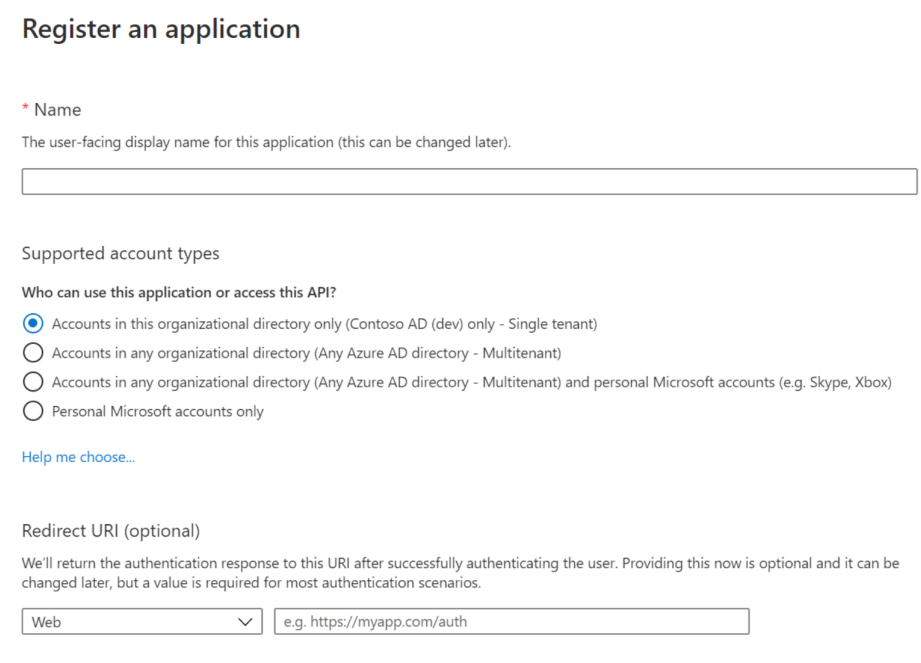
- Rollen discovery_admin, service_mapping_admin, sn_cmp.cloud_admin in Cloud Provisioning and Governance oder Rolle sn_cloud_ops_ws.cloud_ops_admin in Arbeitsbereich für Cloud-Vorgänge.
- Vorgänge im Microsoft Azure-Portal erfordern eine der folgenden Rollen:
  - Administrator für Azure oder Azure AD (Active Directory)
  - Applikationsadministrator
  - Anwendungsentwickler
  - Cloud-Anwendungsadministrator

  und die Rolle „Mitwirkender bei Ressourcenrichtlinien“ zum Erstellen oder Ändern von Ressourcenrichtlinien.
- Aktivieren Sie die interne Netzwerkverbindung zwischen den MID-Servern und den Azure-Cloud-API-Endpunkten: `Management.Azure.com`

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

Prozedur

1. Melden Sie sich beim Azure-Portal an, und navigieren Sie zu **Azure Active Directory**.
2. Navigieren Sie zum Abschnitt **App registrations** (Appregistrierungen), und klicken Sie auf **New application registration** (Neue Anwendungsregistrierung).
   Geben Sie für Ihre Anwendung folgende Informationen ein:



Feld	Beschreibung
Name	Eindeutiger Name für die Anwendung und ihre Integrationsanmeldeinformationen. Beispiel: `ServiceNow Integration`.
Unterstützte Account-Typen	Geben Sie an, wer die Anwendung verwenden kann.
Redirect URI (optional, Umleitungs-URI)	URL, die auf Azure zugreift. Normalerweise die URL der ServiceNow-Instanz

3. Wählen Sie **Register** aus, um die Registrierung der App abzuschließen.
4. Wenn die Registrierung abgeschlossen ist, kopieren Sie die Werte für Anwendungs-ID (Client) und Verzeichnis-ID (Mandant), und fügen Sie sie in den Texteditor ein.
5. Beschriften Sie die Werte **Anwendungs-ID** bzw. **Verzeichnis-ID**.
6. Navigieren Sie im Azure-Portal zum Abschnitt **Certificates & secrets** (Zertifikate und geheime Schlüssel), und geben Sie dann unter **New client secret** (Neuer Client-Geheimschlüssel) die folgenden Werte an:

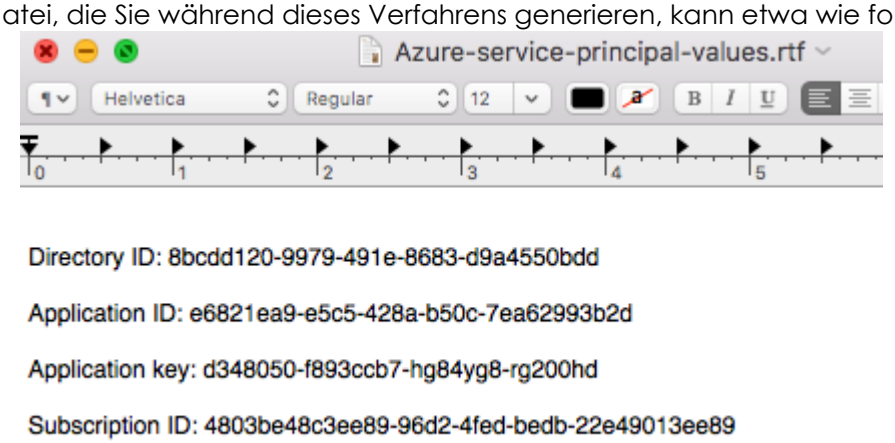
Feld	Beschreibung
Schlüsselbeschreibung	Beschreibung für den Schlüssel
Dauer	Ablauf für den Schlüssel.

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

Feld	Beschreibung
	Hinweis: Ihre Organisation kann Richtlinien anwenden, um die Gültigkeitsdauer des Schlüssels einzuschränken. Wählen Sie die entsprechende Dauer aus.

7. Klicken Sie auf **Hinzufügen**.
8. Kopieren Sie den Schlüsselwert, fügen Sie ihn in den Texteditor ein, und beschriften Sie den Wert als **Anwendungsschlüssel**.
9. Damit der Dienstprinzipal mit verschiedenen Azure-Abonnements arbeiten kann, navigieren Sie zu **Abonnements**.
   Zum Verwalten mehrerer Abonnements müssen Sie das folgende Verfahren für jedes Abonnement ausführen:

   a. Fügen Sie die Abonnements-ID in den Texteditor ein, und beschriften Sie sie als **Abonnements-ID**.
   Die Textdatei, die Sie während dieses Verfahrens generieren, kann etwa wie folgt



   aussehen:

   b. Navigieren Sie zum Abonnement, und wählen Sie im Menü die Option **Zugriffssteuerung (IAM)** aus.

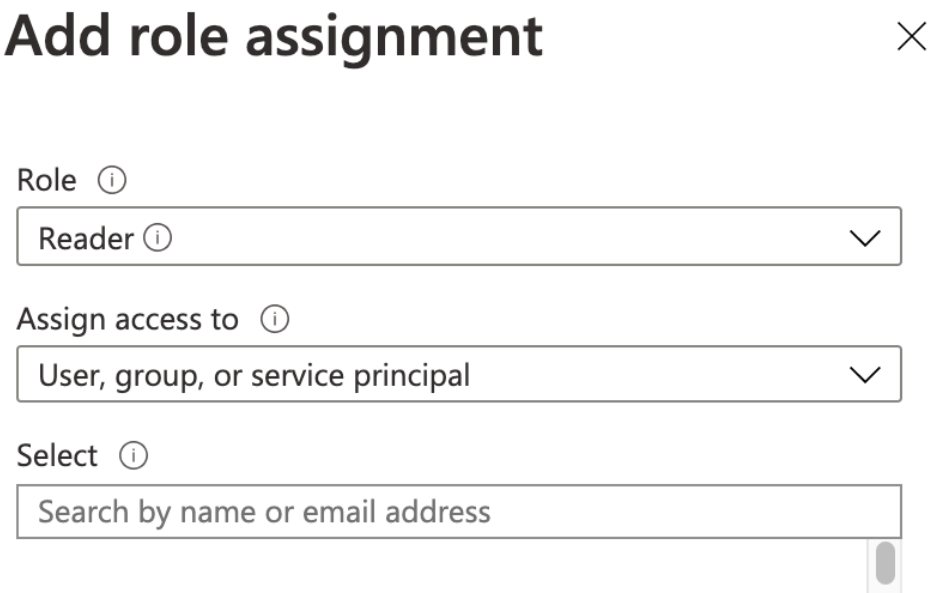
   c. Klicken Sie oben im Bildschirm auf **+ Hinzufügen** und dann auf **Add role assignment** (Rollenzuweisung hinzufügen).

   d. Wählen Sie im Feld **Rolle** den Wert **Leser** aus.
   Lassen Sie den Standardwert für **User, group, or service principal** (Benutzer, Gruppe oder Service-Prinzipal) für das Feld **Assign Access to** (Zugriff zuweisen an) unverändert.

   Hinweis: Die Rolle **Mitwirkender bei Ressourcenrichtlinien** ist nur für die Bereitstellung erforderlich.

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

e. Wählen Sie im Feld **Auswählen** den Namen aus, den Sie in Schritt 2 erstellt haben, und klicken Sie auf **Speichern**.



10. Führen Sie die entsprechende Aktion aus.

- Wenn Sie Cloud-Discovery nicht über Arbeitsbereich für Cloud-Vorgänge verwenden, gehen Sie wie folgt vor:

  Klicken Sie im Discovery Manager auf das Plus-Symbol (**+**), und wählen Sie in der Liste **Azure-Dienstprinzipal** aus.

- Wenn Sie Cloud-Discovery über Arbeitsbereich für Cloud-Vorgänge verwenden, gehen Sie wie folgt vor:

  a. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.

  b. Wählen Sie **Neu**.

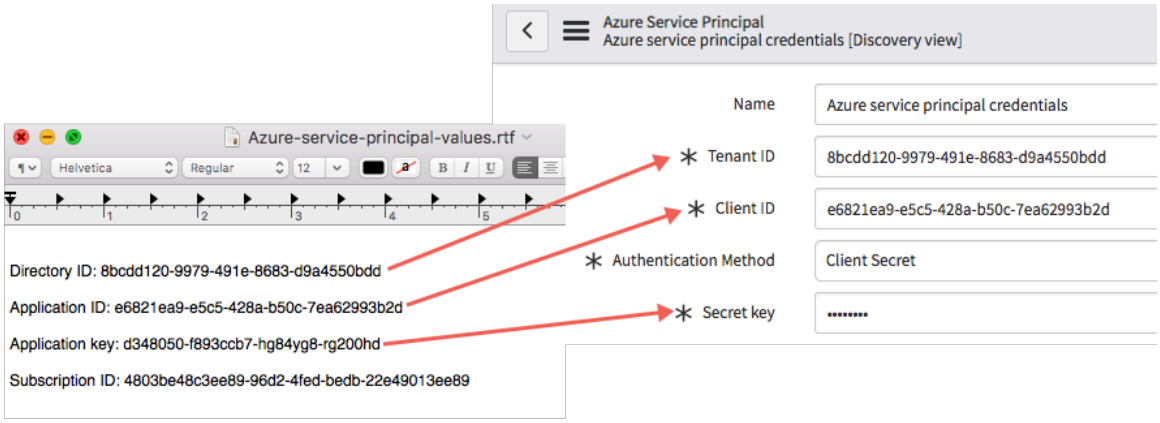
  c. Wählen Sie **Azure-Service-Prinzipal** aus.

11. Geben Sie die folgenden Werte im Azure-Service-Principal-Formular an:

Feld	Wert
Name	Name des Dienstprinzipals, der bei der Instanz registriert werden soll. Beispiel: `Azure service principal credentials`.
Authentifizierungsmethode	Wählen Sie **Client-Geheimnis**. Das Feld **Geheimer Schlüssel** wird angezeigt, wenn Sie **Geheimer Clientschlüssel** auswählen. **Hinweis:** **Client-Zusicherung** wird nicht unterstützt.

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

12. Kopieren Sie die Werte aus der temporären Textdatei, und fügen Sie sie in die verbleibenden Felder ein.



Formularfeld „Anmeldeinformationen“	Wert „Azure-Dienstprinzipal“
Mandanten-ID	Wert der Azure-**Verzeichnis-ID** aus der Textdatei
Client-ID	Wert der Azure-**Anwendungs-ID** aus der Textdatei
Geheimer Key	Wert des Azure-**Anwendungsschlüssels** aus der Textdatei

13. Klicken Sie auf **Speichern**, um den Azure-Dienstprinzipal zu erstellen.
14. Klicken Sie auf den zugehörigen Link **Abonnements erkennen**, um alle Abonnements für den Azure-Dienstprinzipal zu suchen.
    Die Instanz erstellt ein Servicekonto für jedes erkannte Abonnement. In der zugehörigen Liste **Azure-Abonnements** sind alle Abonnements aufgeführt, die mit dem Azure-Dienstprinzipal verknüpft sind.
15. Klicken Sie auf ein Abonnement, um das für das Abonnement erstellte Servicekonto anzuzeigen.
16. Klicken Sie auf einen Discovery-Statuseintrag in der Liste **Berechtigung Discovery-Status**, um das Discovery-Protokoll anzuzeigen.
    Bei jedem Klicken auf **Discovery-Abonnement** generiert die Instanz einen neuen Discovery-Status und zeigt ihn in der Liste **Berechtigung Discovery-Status** an.

Azure-Cloud-Discovery unter Verwendung eines Dienstprinzipals mit SSH-Zertifikaten

Erkennen Sie virtuelle Linux-Maschinen in Azure mithilfe eines Serviceprinzipals (SP) mit kurzgültigen SSH-Zertifikaten. Die Verwendung dieser Zertifikate erspart Passwörter oder Schlüsselpaare aus öffentlichen und privaten Schlüsseln.

Vorbereitungen

Erforderliche Rolle: Administrator

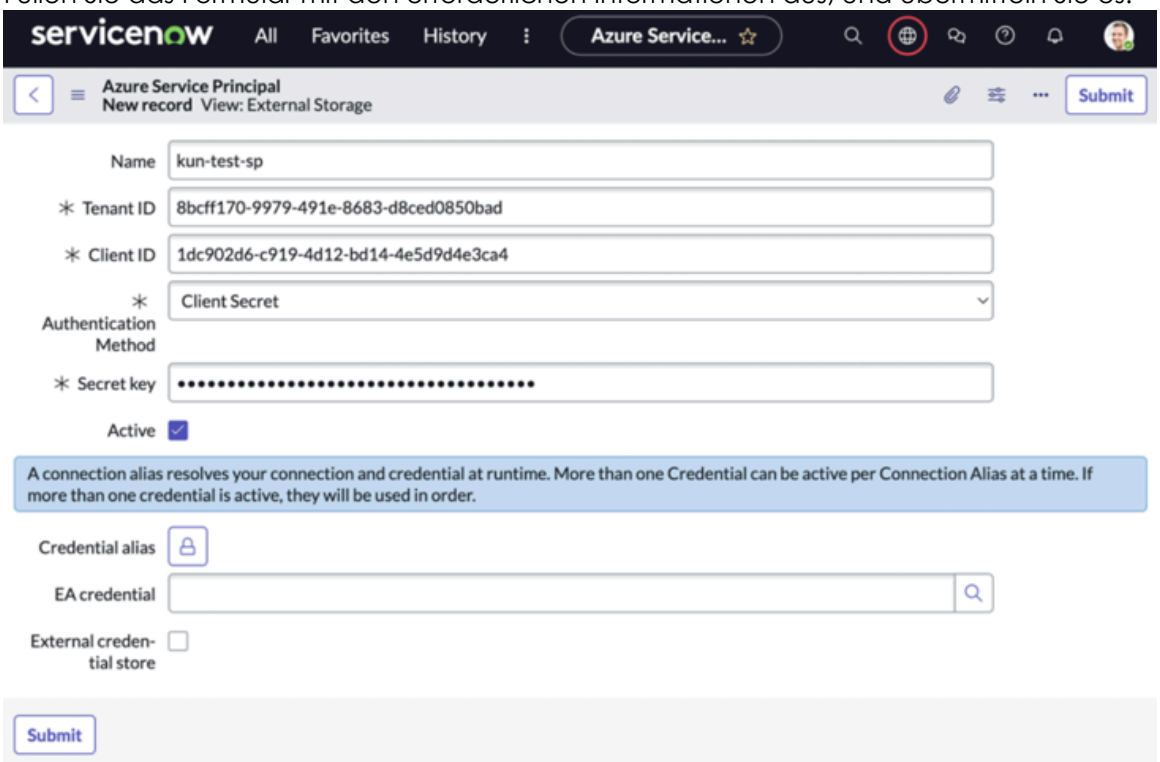
Vor dem Erstellen von Cloud-Discovery-Anmeldeinformationen müssen Serviceprinzipien im Azure-Portal eingerichtet werden. Weitere Informationen finden Sie auf der Microsoft Azure- Dokumentationswebsite. Nach dem Erstellen einer Linux-VM mit aktivierter Azure AD-Anmeldung müssen Sie die Anforderungen für die Anmeldung bei Azure AD mithilfe der zertifikatsbasierten OpenSSH-Authentifizierung für Linux-VMs überprüfen. Konfigurieren Sie geeignete Rollenzuweisungen für das Serviceprinzipal und die Ressourcengruppe.

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

Vor dem Erstellen von Anmeldeinformationen ist das Plugin **„Externer Anmeldeinformationsspeicher“** erforderlich, um eine Verbindung zur Azure-VM über OpenSSH-Zertifikate herzustellen.

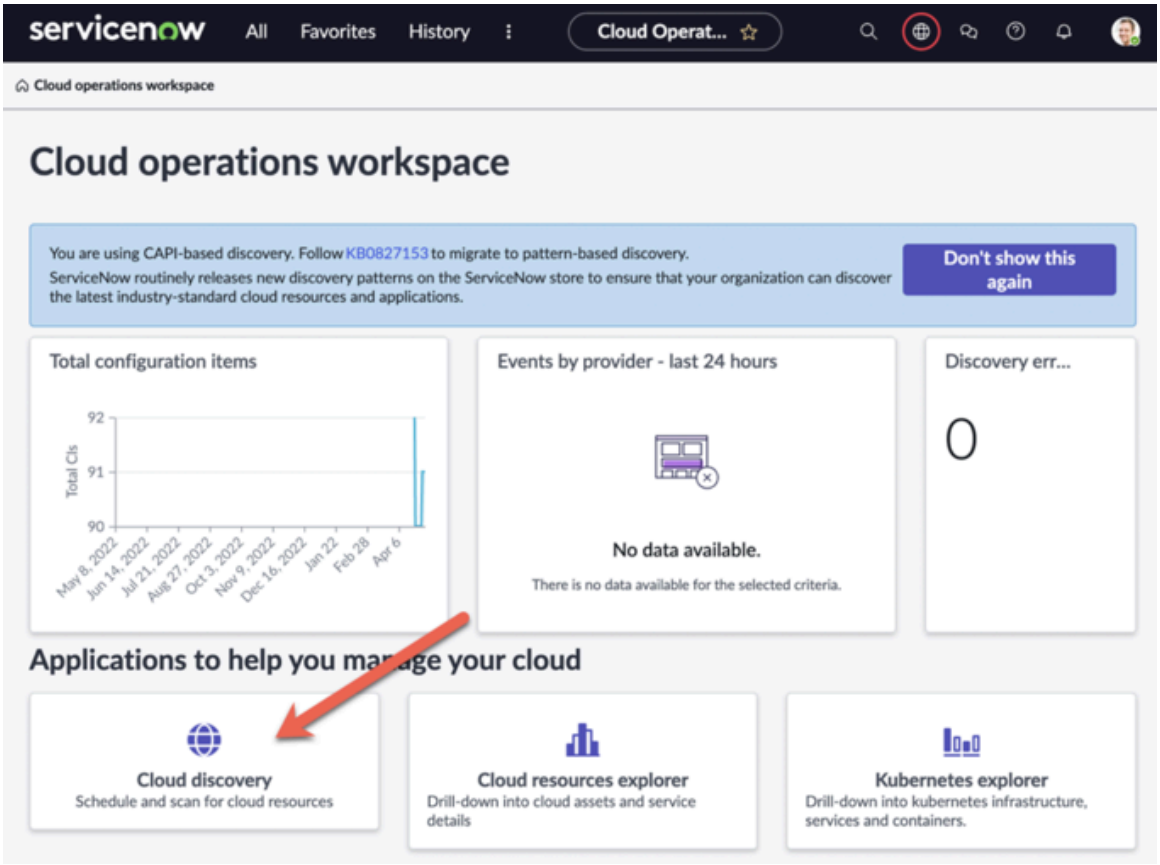
Prozedur

1. Navigieren Sie in der Instanz zu **Discovery** > **Anmeldeinformationen** und wählen Sie **Neu**aus.
2. Wählen Sie als Typ der Anmeldeinformationen **Azure-Dienstprinzipal**aus.
3. Füllen Sie das Formular mit den erforderlichen Informationen aus, und übermitteln Sie es.



4. Navigieren zu **Discovery** > **Anmeldeinformationen** und wählen Sie **Neu**aus.
5. Wählen Sie für diesen Anmeldeinformationstyp **Azure SSH-Zertifikat-Anmeldeinformationen**aus.
6. Füllen Sie das Formular mit den erforderlichen Informationen aus, einschließlich der Verknüpfung der in Schritt 3 erstellten Anmeldeinformationen für das Serviceprinzip. Die Anmeldeinformationen für den Azure-Service Provider und das SSH-Zertifikat wurden erstellt und verknüpft. Setzen Sie das Verfahren zum Erstellen des Cloud-Discovery-Zeitplans fort.
7. Navigieren Sie zur Startseite des Cloud-Discovery-Arbeitsbereichs, und wählen Sie **Cloud-Discovery**aus.

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



8. Wählen Sie **Neuer Discovery-Zeitplan**.
9. Geben Sie einen Namen für den Zeitplan an, und wählen Sie **Azure** als Cloud-Anbieter aus.
10. Erstellen Sie ein neues Abonnement mit den in Schritt 3 erstellten Anmeldeinformationen **des Azure-Dienstprinzipals**.
11. Wählen Sie Rechenzentren aus.
12. Aktivieren Sie die Option zum Erkennen virtueller Computer.
13. Schließen Sie die Zeitplanerstellung ab, indem Sie **Beenden und ausführen**auswählen.

Ergebnisse

Der Discovery-Zeitplan sollte gestartet werden, und auf der Homepage für Cloud-Vorgänge sollte der Ausführungsstatus für den neu erstellten Zeitplan angezeigt werden. Nach einiger Zeit sollte die geplante Erkennung abgeschlossen werden. Anschließend wird ein neuer Zeitplan für die VM-Erkennung erstellt und ausgeführt. Der neue VM-Discovery-Zeitplan verwendet den SP, den wir für die Generierung von SSH-Zertifikaten erstellt haben, um sich bei den VMs zu authentifizieren. Sie können dies im Abschnitt „Discovery IP Affinity“ für die Anmeldeinformationen beobachten.

Über Microsoft Azure-Warnungen gesteuerte Erkennung

Der Microsoft Azure-Warnungsservice kann Warnungen für Änderungen am Lebenszyklusstatus oder an der Konfiguration einer Cloud-Ressource auslösen. Sie können den Service so konfigurieren, dass die neuesten Ressourceninformationen in der Configuration Management Database (CMDB) automatisch aktualisiert werden, ohne auf die Ausführung der nächsten geplanten Cloud-Discovery zu warten.

Automatische Übersetzung

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

Wichtig: Die Change-Verarbeitung Azure bietet im Vergleich zur warnungsgesteuerten Discovery Microsoft Azure, die eine veraltete Form der Authentifizierung verwendet, eine optimale Leistung und sollte nicht mehr verwendet werden. Ab Version 1.1.0 der App Muster für Discovery und Service-Mapping hat die Change-Verarbeitung Azure für die warnungsgesteuerte Discovery Microsoft Azure für ersetzt. Verwenden Sie den neuen sicheren Webhook, oder migrieren Sie zu Azure Verarbeitung von Changes, um die Leistung zusätzlich zu steigern. Weitere Informationen zum sicheren Webhook finden Sie im Knowledge Base-Artikel Azure-Warnungsservice zur automatischen Aktualisierung der CMDB über eine Webhook-URL ohne Anmeldeinformationen im Azure-Portal .

Während der Eventverarbeitung identifiziert der Cloud Event Scheduler die Domäne des Serviceaccounts und weist sie dem Event zu. Wenn beim Identifizieren der Domäne vor der Verarbeitung ein Fehler auftritt, kann das Event manchmal nicht zugewiesen werden und wird für alle Domänen sichtbar. Um zu verhindern, dass die fehlgeschlagenen Events für alle Domänen sichtbar sind, können Sie die Eigenschaft *sn_cmp.error_events.default_domain* auf die sys_id der Service Provider-Domäne festlegen, sodass die fehlgeschlagenen Events nur dem Domänenadministrator des Service Providers angezeigt werden.

Sie können die Cloud Event Scripted REST API so konfigurieren, dass Warnungen vom Microsoft Azure-Warnungsservice empfangen werden. Für jede Warnung – auch Event genannt – erstellt die API einen Datensatz in der Tabelle „Cloud-Events“ [sn_cmp_cloud_event]. Der Cloud Event Scheduler liest die Events aus der Tabelle [sn_cmp_cloud_event] für die Batch-Verarbeitung. Der Scheduler ruft das Muster auf, um die Events zu verarbeiten, die sich im Status „Bereit“ befinden. Die Muster erkennen die betroffene Ressource und fügen ihre Details in der CMDB hinzu oder aktualisieren sie. Mit dieser Methode können Sie die Daten des Configuration Item (CI) CMDB aktualisieren und die neuesten Daten im Cloud-Benutzerportal anzeigen.

Wichtig: Wenn Sie Domänentrennung für Cloud-Discovery verwenden, sind auch die Ereignisse nach Domänen getrennt. Daher können Sie die Details eines verarbeiteten Events nur anzeigen, wenn es zu Ihrer Domäne gehört. Wenn ein Ereignis keinem Servicekonto zugeordnet ist, wird es der globalen Domäne zugeordnet.

Für jedes Event speichert die Cloud Event Scripted REST API die folgende Informationen in der Tabelle [sn_cmp_cloud_event]:

- **Quelle**: Dieses Feld ist immer auf `azure activity log` (Azure-Aktivitätsprotokoll) festgelegt.
- **Eventname**: Name des von der Microsoft Azure-Konsole empfangenen Events.
- **Ressourcen-ID**: ID der betroffenen Ressource. Wenn VM-Events vorhanden sind, verwendet Cloud-Discovery diese Informationen, um die VM zu identifizieren.
- **Ressourcentyp**: Ressourcentyp der betroffenen Ressource.

Konfigurieren Sie den Warnungsservice Microsoft Azure so, dass er automatisch aktualisiert wird CMDB

Konfigurieren Sie den Microsoft Azure-Warnungsservice so, dass die Configuration Management Database (CMDB) automatisch aktualisiert wird, ohne auf die Ausführung der nächsten geplanten Cloud-Discovery zu warten.

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

Vorbereitungen

- Vergewissern Sie sich, dass entweder Discovery oder Cloud Provisioning and Governance in der Instanz aktiviert ist.
- ◦ Ein aktiver MID-Server mit Microsoft Azure-Discovery-Funktionalität ist verfügbar.

Hinweis: Die Warnungskonfiguration pingt weiterhin Warnungen, auch wenn der MID-Server nicht verfügbar ist. Dies führt wiederum zu einer hohen Anzahl von Fehlern in der ECC-Warteschlange. Wenn kein MID-Server verfügbar ist, müssen Sie die Microsoft Azure-Warnungsregel manuell deaktivieren. Die Tabelle „Azure-Warnungsregeln“ [azure_alert_rule] enthält alle Microsoft Azure-Warnungsregeln.

Erforderliche Rolle:

- ServiceNow-Rolle: sn_cmp.cloud_event_integration
- Microsoft Azure-Rollen:
  - ◦ Microsoft Azure-Anmeldeinformationen mit der Leser-Rolle
  - ◦ Benutzerdefinierte Microsoft Azure-Rolle mit den folgenden Berechtigungen:

```
"permissions": [
            {
                "actions": [
                    "Microsoft.Insights/ActionGroups/Write",
                    "Microsoft.Insights/ActionGroups/Delete",
                    "Microsoft.Insights/ActionGroups/Read",
                    "Microsoft.Insights/ActivityLogAlerts/Write",
                    "Microsoft.Insights/ActivityLogAlerts/Delete",
                    "Microsoft.Insights/ActivityLogAlerts/Read",

 "Microsoft.Insights/ActivityLogAlerts/Activated/Action",
                    "Microsoft.Insights/AlertRules/Write",
                    "Microsoft.Insights/AlertRules/Delete",
                    "Microsoft.Insights/AlertRules/Read",
                    "Microsoft.Resources/deployments/write",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Resources/deployments/read"
                ],
```

Hinweis: Zum Einrichten der warnungsbasierten Erkennung können Sie einen Microsoft Azure-Dienstprinzipal nur mit der Leserrolle verwenden. Weitere Informationen finden Sie im Community-Artikel Azure alert driven discovery with reader privileges (Auf Azure-Warnungen basierte Erkennung mit Leseberechtigungen).

Warum und wann dieser Vorgang ausgeführt wird

Nachdem Sie den Warnungsservice konfiguriert haben, erleichtert er die Nachverfolgung des Lebenszyklusstatus und der Konfiguration der Cloud-Ressourcen Microsoft Azure.

Wichtig: Sie können einen sicheren Webhook verwenden, um die Warnungen Microsoft Azure an Now Platformweiterzuleiten. Weitere Informationen finden Sie unter Verwenden Sie einen sicheren Webhook, um den weiterzuleiten Microsoft Azure Warnungen für Now Platform [KB1208357] .

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

Prozedur

1. Deaktivieren Sie die Authentifizierung für die Cloud Event Scripted REST API, da die Microsoft Azure-Warnung die Standardauthentifizierung nicht unterstützt.

   a. Navigieren Sie als Administrator zu **Scripted Web Services** > **Scripted REST APIs**.

   b. Öffnen Sie den Cloud Event-Datensatz.

   c. Öffnen Sie auf der Registerkarte **Ressourcen** den Datensatz zur Option Cloud Config Event Post (Veröffentlichung zu Cloud-Konfigurations-Event).

   d. Setzen Sie den Anwendungsbereich auf **Global**.

   e. Deaktivieren Sie auf der Registerkarte **Sicherheit** das Kontrollkästchen **Erfordert Authentifizierung**.

   > **Wichtig:** In der ServiceNow-Instanz wird eine Webhook-URL für die warnungsbasierte Erkennung verwendet. Die Microsoft Azure-Warnungskonfiguration der ServiceNow-Instanz unterstützt jedoch keine Authentifizierung zum Erstellen des Webhooks. Sie können die Authentifizierung aktivieren, indem Sie den Benutzernamen und das Passwort in der Webhook-URL angeben. Weitere Informationen finden Sie im KB-Artikel KB0963526 .

2. Navigieren zu **Discovery** > **Cloud-Warnungen** > **Azure-Warnmeldungskonfigurationen**.

   > **Hinweis:** Wenn Sie Discovery in der Instanz aktiviert haben, können Sie mit der Instanz-URL direkt zu **Warnungskonfigurationen** navigieren. Beispiel:
   >
   > ```
   > https://{instancename}.service-now.com/sn_cmp_azure_alert_configuration_list.do
   > ```

3. Wählen Sie auf der Registerkarte **Azure** die Option **Neu** aus.
4. Füllen Sie die Felder des Formulars aus.

Azure-Warnungskonfiguration – Formular

Feld	Beschreibung
Servicekonto	Microsoft Azure-Servicekonto, für das Sie die Azure-Warnungskonfiguration erstellen möchten. Stellen Sie sicher, dass Cloud-Discovery alle dem Cloud-Konto zugeordneten logischen Rechenzentren (LRZ) erkannt hat.
Ressourcengruppe	Ressourcengruppe, die die Warnungsregeln enthält. Wählen Sie das Microsoft Azure-Servicekonto aus. Weitere Informationen zum Hinzufügen eines Microsoft Azure-Servicekontos finden Sie unter Fügen Sie eine hinzu Azure Servicekonto. Die Warnungsregeln werden von der Instanz für alle innerhalb des Servicekontos verfügbaren Ressourcen erstellt.
Aktivieren	Option zum Angeben des Status der Warnungskonfiguration.

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

Feld	Beschreibung
	Diese Option ist standardmäßig ausgewählt.
Anwender	Benutzername eines ServiceNow-Benutzers mit der Rolle sn_cmp.cloud_event_integration.
Passwort	Passwort des ServiceNow-Benutzerkontos.

5. Wählen Sie **Absenden** aus.
   Bei erfolgreicher Konfiguration des Microsoft Azure-Warnungsservice ändert sich der Status der Warnungskonfiguration von **Keine** in **Aktiviert**.

Microsoft Azure-Warnungsregel hinzufügen

Aktivieren Sie die warnungsbasierte Erkennung für einen neuen Microsoft Azure-Warnungstyp, indem Sie ihn der Tabelle „Azure-Warnungsregeln“ [azure_alert_rule] hinzufügen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Die Tabelle „Azure-Warnungsregeln“ [azure_alert_rule] enthält alle unterstützten Warnungstypen. Weitere Informationen finden Sie unter Unterstützte Microsoft Azure-Warnungstypen. Vom Microsoft Azure-Warnungsservice werden diese Warnungsregeln, die in der Tabelle „Azure-Warnungsregeln“ [azure_alert_rule] gespeichert sind, dazu verwendet, die Warnungen auszulösen. Cloud-Discovery unterstützt auch alle Warnungen, die für die Mitglieder der in der Microsoft Azure-Warnungskonfiguration angegebenen Ressourcengruppe generiert wurden.

Prozedur

1. Navigieren Sie zur Tabelle „Azure-Warnungsregeln“ [azure_alert_rule], indem Sie in die Navigationsleiste des Browsers die folgende URL eingeben:
   `https://<instance name>.service-now.com/azure_alert_rule_list.do`
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Azure-Warnungsregel – Formular

Feld	Beschreibung
Regelname	Name des Microsoft Azure-Warnungstyps.
Aktion	Microsoft Azure-API-Pfad für Ressourcenvorgänge. Weitere Informationen zu den Microsoft Azure -Ressourcen, für die Sie Warnungen auslösen können, finden Sie unter Microsoft Azure Dokumentation und lesen Sie den Abschnitt „Vorgänge des Azure-Ressourcenanbieters“.
Aktiv	Option zum Angeben des Status des Microsoft Azure-Warnungstyps. Diese Option ist standardmäßig ausgewählt.

4. Wählen Sie **Absenden** aus.

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

Unterstützte Microsoft Azure-Warnungstypen

Von der Cloud-Discovery des Basissystems wird die warnungsbasierte Erkennung für mehrere Microsoft Azure-Warnungstypen unterstützt. Die Tabelle „Azure-Warnungsregeln“ [azure_alert_rule] enthält die unterstützten Warnungstypen.

Von der Cloud-Discovery des Basissystems werden folgende Microsoft Azure-Warnungstypen unterstützt:

```
Microsoft.Compute/virtualMachines/deallocate/action
Microsoft.Network/privateDnsZones/delete
Microsoft.Compute/availabilitySets/write
Microsoft.Network/loadBalancers/write
Microsoft.Network/connections/delete
Microsoft.Network/publicIPAddresses/delete
Microsoft.Storage/storageAccounts/write
Microsoft.Network/virtualNetworks/delete
Microsoft.Sql/servers/databases/delete
Microsoft.Network/expressRouteCircuits/write
Microsoft.Network/localnetworkgateways/delete
Microsoft.Network/networkInterfaces/delete
Microsoft.Compute/virtualmachines/write
Microsoft.Network/expressRouteCircuits/delete
Microsoft.Network/natGateways/write
Microsoft.Network/loadBalancers/delete
Microsoft.Compute/virtualMachineScaleSets/delete
Microsoft.Network/virtualNetworks/virtualNetworkPeerings/delete
Microsoft.Storage/storageAccounts/delete
Microsoft.Compute/availabilitySets/delete
Microsoft.Network/connections/write
Microsoft.Compute/virtualMachines/start/action
Microsoft.Compute/virtualMachines/restart/action
Microsoft.Sql/servers/databases/write
Microsoft.Compute/virtualMachines/delete
Microsoft.Network/networkInterfaces/write
Microsoft.Network/privateDnsZones/write
Microsoft.Network/localnetworkgateways/write
Microsoft.Network/natGateways/delete
Microsoft.Compute/virtualMachines/stop/action
Microsoft.Network/publicIPAddresses/write
Microsoft.Compute/virtualMachineScaleSets/write
Microsoft.Network/virtualNetworks/virtualNetworkPeerings/write
Microsoft.Network/virtualNetworks/write
Microsoft.Sql/servers/delete
Microsoft.Sql/servers/write
```

Azure Verarbeitung von Changes

Das Change-Verarbeitungsfunktion Azure sammelt nahezu in Echtzeit Informationen über Microsoft Azure -Ressourcen, die eine Lebenszyklus-Statusänderung oder Konfigurationsänderungerfahren haben. Anschließend verwendet es die gesammelten Informationen, um Configuration Management Database (CMDB)zu aktualisieren.

Die geplanten Aufgaben zur Verarbeitung von Azure Changes fragen die Azure API ab und sammeln die Informationen zu Ressourcen-Changes. Während jedes Ausführungszyklus sammelt die regelmäßige Aufgabe Informationen über alle Ressourcen, die nach dem letzten Verarbeitungszyklus von Azure Change geändert haben. Nach dem Sammeln der Change-Informationen verwendet die Azure Change-Verarbeitung Antwortzuordnungen, um die Change-Informationen in CMDBzu aktualisieren. Während der nächsten Discovery

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

löst Cloud-Discovery entsprechende Muster aus, falls verfügbar, und trägt detaillierte Ressourceninformationen in CMDBein.

Standardmäßig werden die Azure geplanten Change-Verarbeitungsaufgaben alle 5 Minuten in ausgeführt. Passen Sie bei Bedarf die Ausführungshäufigkeit des Zeitplans an Ihre Bedürfnisse an. Legen Sie die Ausführungshäufigkeit innerhalb des Mindestwerts von einer Minute fest.

Wenn Sie die Verarbeitung des Change Azure zum ersten Mal ausführen, kann sie aufgrund von Änderungen an der Verarbeitungsressource, die in den letzten vier Stunden aufgetreten sind, einige Stundenausgeführt werden. Wenn Sie den Standardausführungszeitraum erhöhen möchten, stellen Sie sicher, dass genügend Worker-Knoten für die Ausführung des Zeitplans verfügbar sind.

Während der Eventverarbeitung identifiziert der Cloud Event Scheduler die Domäne des Serviceaccounts und weist sie dem Event zu. Wenn beim Identifizieren der Domäne vor der Verarbeitung ein Fehler auftritt, kann das Event manchmal nicht zugewiesen werden und wird für alle Domänen sichtbar. Um zu verhindern, dass die fehlgeschlagenen Events für alle Domänen sichtbar sind, können Sie die Eigenschaft *sn_cmp.error_events.default_domain* auf die sys_id der Service Provider-Domäne festlegen, sodass die fehlgeschlagenen Events nur dem Domänenadministrator des Service Providers angezeigt werden.

Hinweis:

Azure Die Verarbeitung von -Changes kann Ressourcen-Changes-Informationen nur aus den Service-Accounts abrufen, die mit „discovery_admin“ oder „sn_cmp.cloud_admin“ erstellt wurden.

Aktualisieren Sie Ihr Plugin Muster für Discovery und Service-Mapping auf ServiceNow Store auf mindestens Version 1.21.0 von Azure Change-Verarbeitung. Siehe Upgrade-Szenario in KB1705862

Ab Version Muster für Discovery und Service-Mapping 1.21.0 wurden die geplanten Aufgaben erweitert und umbenannt:

- Die geplante Aufgabe *Azure Process Changes* wurde in *ACP Pull Changes*umbenannt.
- Die geplante Aufgabe *CPG Build Azure Changes IRE Payload*wurde in *ACP Process Changes*umbenannt.

ACP-Tabellen

Ab Version Muster für Discovery und Service-Mapping 1.21.0 führt die Erweiterung Azure Change Processing vier Tabellen ein.

ACP-Ressourcentyp [sn_itom_pattern_acp_supported_resource_types]

Sie können diese Tabelle verwenden, um alle unterstützten Ressourcentypen zu überprüfen, einen Ressourcentyp für die Change-Verarbeitung hinzuzufügen und die Verarbeitung für eine bestimmte Ressource zu deaktivieren oder zu aktivieren.

Weitere Informationen zum Hinzufügen von Unterstützung für den Ressourcentyp Azure finden Sie unter Fügen Sie Unterstützung für die Change-Verarbeitung für einen Ressourcentyp Azure hinzu.

Schlüsselfelder:

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

- Ressourcentyp
- Abfrage: Die Ressourcendiagramm-Abfrage, die Changes von Azureabruft.
- Aktiv: Gibt an, ob der Ressourcentyp aktiv abgefragt wird.

ACP-Auftragsstatus [sn_itom_pattern_acp_order_status]

Diese Tabelle verfolgt den Status der Azure Resource Graph-Abfrage für jeden Ressourcentyp basierend auf den zugehörigen Anmeldeinformationen, die für die Abfrage Azurevon verwendet werden. Sie können diese Tabelle verwenden, um den Verarbeitungsstatus zu überprüfen. Weitere Informationen zur Abfrage finden Sie unter KB1705862 .

Schlüsselfelder:

- Ressourcentyp
- Anmeldeinformationen: Die spezifischen Anmeldeinformationen, die zum Abrufen von Changes verwendet werden.
- Letzte Verarbeitungszeit.
- Status: Verfolgt den Erfolg oder Fehler des Ereignis-Abrufprozesses. Nach der nächsten geplanten Aufgabe wird dieser Status basierend auf dem CMP-Auftragsstatus aktualisiert.
- CMP-Auftrag: Verweis auf das Feld „CMP-Auftrag“ [sn_cmp_order], das Details zum aktuellen Auftragsfortschritt und -ergebnis enthält.

ACP-Ressourcenänderung [sn_itom_pattern_acp_resource_change]

In dieser Tabelle werden die in den Ressourcen Azure erkannten Änderungen aufgezeichnet. Die Tabelle [sn_cmp_resource_changes_payload_info], in der diese Informationen vor Version 1.21.0 gespeichert wurden, ist nicht mehr verfügbar.

Schlüsselfelder:

- Ressourcen-ID: der eindeutige Bezeichner für die geänderte Ressource in Azure.
- Payload ändern: Ein Snapshot der Attribute, die für die Ressource relevant sind.
- Reihenfolge: Ein Verweis auf das Feld „CMP-Reihenfolge“ [sn_cmp_order], das den Change abgerufen hat.
- Ressourcenstatus: Ein Verweis auf die Tabelle „ACP-Ressourcenstatus“, um den Verarbeitungsstatus des Change nachzuverfolgen.
- Status: Der aktuelle Verarbeitungsstatus des Change. Wenn der Status als „Fehler“ markiert ist, überprüfen Sie den zugehörigen Ressourcenstatus-Datensatz auf weitere Details.

ACP-Ressourcenstatus [sn_itom_pattern_acp_resource_status]

Diese Tabelle verfolgt den Gesamtstatus der Ressourcenverarbeitung.

Schlüsselfelder:

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

- Ressourcen-ID: Der Bezeichner für die verarbeitete Ressource.
- Status: der Verarbeitungsstatus. Die Status sind: Bereit, In Bearbeitung, Fehler und Erfolg.
- Fehlermeldung: Wenn die Verarbeitung fehlgeschlagen ist, enthält dieses Feld Details zum Fehler.

Unterstützte Azure Ressourcentypen und Changes

Azure Die Change-Verarbeitung verfolgt eine Reihe von Ressourceneigenschaften für jeden unterstützten Ressourcentyp. Wenn in einer dieser Eigenschaften eine Änderung erkannt wird, ruft die Change-Verarbeitung Azure einen aktualisierten Snapshot der Ressource von Azureab und verarbeitet ihn in CMDB entsprechend der Änderung.

Ressourcentyp	Ressourceneigenschaft
MicrosoftMicrosoft Azure Event Hubs.Compute/ virtualMachine	• *CreateOrDeleteVm : properties.changeType in ('Create','Delete')* • *ChangeStatus: (properties.extended.instanceView.powerState.code) in ('PowerState/running', 'PowerState/stopped', 'PowerState/deallocated'))* • *ChangeDisk: properties.storageProfile* • *ChangeTag: tags.** • *ChangeNetworkInterface : properties.networkProfile.networkInterfaces*
MicrosoftMicrosoft Azure Event Hubs.Compute/ Datenträger	• *CreateOrDeleteDisk : properties.changeType in ('Create','Delete')* • *ChangeState : properties.diskState* • *ChangeSize : properties.storageProfile* • *ChangeTag : tags.**
MicrosoftMicrosoft Azure Event Hubs.Netzwerk/ networkSecurityGroups	• *CreateOrDeleteNsg : properties.changeType in ('Create','Delete')* • *ChangeTag : tags.**
MicrosoftMicrosoft Azure Event Hubs.Netzwerk/ Netzwerkschnittstellen	• *CreateOrDeleteNic : properties.changeType in ('Create','Delete'),* • *changePrimary : properties. properties.primary* • *ChangeIp : properties.ipConfigurations[0]'* • *ChangeTag : tags.**

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

Ressourcentyp	Ressourceneigenschaft
MicrosoftMicrosoft Azure Event Hubs.Netzwerk/ publicIPAddresses	• *CreateOrDeleteIp : properties.changeType in ('Create','Delete'),* • *ChangeIpAddress : 'properties.ipaddress',* • *ChangeFqdn : properties.dnsSettings.fqdn* • *ChangeIpConfig : properties.ipConfiguration* • *ChangeTag : tags.**

Vorteile der Verarbeitung von Changes Azure .

Die Verarbeitung von Changes Azure für bietet gegenüber der durch Warnungen gesteuerten Erkennung Microsoft Azure von folgende Vorteile:

- Verbesserte Leistung und geringere Wahrscheinlichkeit der Azure -API-Drosselung
- Einfaches Setup

Verbesserte Leistung und geringere Wahrscheinlichkeit der Azure -API-Drosselung

Die warnungsgesteuerte Discovery Microsoft Azure von löst eine gezielte Discovery für jede betroffene Ressource aus. Wenn Now Platform eine große Anzahl von Warnungen erhält, kann die gezielte Discovery daher zu einer Drosselung der Azure -APIs führen. Dies kann dazu führen, dass sich die Leistung bei der Warnungsverarbeitung von Now Platform verringert. Im Gegensatz dazu löst die Verarbeitung des Change Azure keine gezielte Discovery für jede betroffene Ressource aus. Stattdessen werden Antwortzuordnungen verwendet, um die CMDB gemäß den verfügbaren Change-Informationen zu aktualisieren. Während der nächsten Discovery löst Cloud-Discovery entsprechende Muster aus, falls verfügbar, und trägt detaillierte Ressourceninformationen in CMDBein. Daher verbessert die Change-Verarbeitung Azure die Change-Verarbeitungsleistung von Now Platform und verringert die Wahrscheinlichkeit einer Azure -API-Drosselung.

Einfaches Setup

Die durch -Warnungen gesteuerte Discovery Microsoft Azure von verwendet einen Webhook, um Warnungen an Now Platformzu senden. Da die Cloud Azure Warnungen auf Abonnementebene generiert, benötigt die warnungsgesteuerte Discovery Microsoft Azure von einen Webhook für jedes Abonnement, das Sie überwachen möchten. Im Gegensatz dazu verwendet die Change-Verarbeitung Azure CAPI und MID-Server, um mit der Ressourcen-Changes-API Azure zu interagieren. Die API kann Change-Informationen auf Verwaltungsgruppenebene bereitstellen. Daher macht die Change-Verarbeitung Azure Webhooks überflüssig und vereinfacht das Setup.

Sie können die Azure-Change-Verarbeitung konfigurieren, um Informationen zu Ressourcen-Changes aus der Cloud Microsoft Azure abzurufen und zum Aktualisieren von CMDBzu verwenden.

Wenn Sie die warnungsgesteuerte Discovery Microsoft Azure von verwenden, können Sie zur Azure-Change-Verarbeitung migrieren, um die Leistung bei der Change-Verarbeitung von Now Platform zu verbessern und das vereinfachte Setup zu nutzen.

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

Zugehörige Informationen

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1705862

Erkennung von Microsoft Azure-Cloud-Komponenten mithilfe von Mustern

Konfigurieren Sie die Verarbeitung von Changes Azure .

Konfigurieren Sie die Change-Verarbeitung für Azure, um Informationen über Ressourcen-Changes aus der Cloud Microsoft Azure abzurufen und zum Aktualisieren von Configuration Management Database (CMDB)zu verwenden.

Vorbereitungen

- Stellen Sie sicher, dass die neueste Version der Store-App Muster für Discovery und Service-Mapping auf Now Platforminstalliert ist.
- Stellen Sie sicher, dass die warnungsgesteuerte Discovery Microsoft Azure nicht für Now Platformkonfiguriert ist.

Erforderliche Rolle: discovery_admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zur Verarbeitung von Azure-Changes finden Sie unter Azure Verarbeitung von Changes.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Konfigurieren Sie die Verarbeitung von** *Azure* **-Changes**.
2. Wählen Sie die Accounts aus, für die Sie die Verarbeitung von Azure -Changes konfigurieren möchten.

   a. Wählen Sie in der Liste **Serviceaccounts ohne „Pull-basierte“ Change-Verarbeitung** die Accounts aus, für die Sie die Azure-Change-Verarbeitung konfigurieren möchten.

   b. Fügen Sie die ausgewählten Accounts der Liste **„Service-Accounts mit Pull-basierter“ Change-Verarbeitung** hinzu.

   Hinweis: Wenn Sie die Verarbeitung von Azure -Changes für eine Azure -Verwaltungsgruppe aktivieren, wird sie auch für alle Abonnements in der Verwaltungsgruppe aktiviert.

3. Wählen Sie **OK**.

Zugehörige Informationen

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1705862

Change-Verarbeitung für Migration zu Azure .

Migrieren Sie zu Change-Verarbeitung Azure, um die Leistung bei der Change-Verarbeitung von Now Platform zu verbessern und das vereinfachte Setup zu nutzen.

Vorbereitungen

- Stellen Sie sicher, dass die neueste Version der Store-App Muster für Discovery und Service-Mapping auf Now Platforminstalliert ist.
- Stellen Sie sicher, dass die warnungsgesteuerte Discovery Microsoft Azure unter Now Platformkonfiguriert ist.

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

- Stellen Sie sicher, dass die Tabelle „Cloud-Ereignisse“ [sn_cmp_cloud_event] kein Ereignis im Status „Bereit“ enthält.
- Stellen Sie sicher, dass der Bereich auf Global festgelegt ist.
- Stellen Sie sicher, dass mindestens ein aktiver MID-Server verfügbar ist.

Erforderliche Rolle: discovery_admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die warnungsgesteuerte Erkennung Microsoft Azure von verwenden und der Now Platform eine große Anzahl von Warnungen aus der Cloud Azure erhält, kann die Verarbeitung der Warnungen und die Aktualisierung des Configuration Management Database (CMDB)sehr viel Zeit in Anspruch nehmen. Migrieren Sie zur Change-Verarbeitung Azure, um die Leistungsprobleme zu beheben. Weitere Informationen zur Verarbeitung von -Changes Azure finden Sie unter Azure Verarbeitung von Changes.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Konfigurieren Sie die Verarbeitung von** *Azure* **-Changes**.
2. Wählen Sie Warnungskonfigurationen Azure abrufen aus, um die Liste aller aktiven Warnungskonfigurationen Azure abzurufen.
3. Wählen Sie *Azure*– **Warnungskonfigurationen deaktivieren aus**.
   Now Platform deaktiviert die Warnungskonfigurationen Azure und entfernts Webhooks aus dem Portal Azure.
4. Wählen Sie die Accounts aus, für die Sie die Verarbeitung von Azure -Changes konfigurieren möchten.

   a. Wählen Sie in der Liste **Serviceaccounts ohne „Pull-basierte“ Change-Verarbeitung** die Accounts aus, für die Sie die Change-Verarbeitung Azure konfigurieren möchten.

   b. Fügen Sie die ausgewählten Accounts der Liste **„Service-Accounts mit Pull-basierter“ Change-Verarbeitung** hinzu.

   > **Hinweis:** Wenn Sie die Verarbeitung von Azure -Changes für eine Azure -Verwaltungsgruppe aktivieren, wird sie auch für alle Abonnements in der Verwaltungsgruppe aktiviert.

5. Wählen Sie **OK**.

Ergebnisse

Das Migrationsskript markiert das Konfigurationsmodul Azure als veraltet. In der Cloud-Discovery. Die Seite Azure Warnungskonfigurationen wird in Arbeitsbereich für Cloud-Vorgängeausgeblendet.

Zugehörige Informationen

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1705862

Fügen Sie Unterstützung für die Change-Verarbeitung für einen Ressourcentyp Azure hinzu

Fügen Sie Unterstützung für die Change-Verarbeitung Azure für einen Ressourcentyp Azure gemäß den Anforderungen Ihrer Organisation hinzu.

Vorbereitungen

Erforderliche Rolle: discovery_admin oder cloud_root_admin

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

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren gilt nur für Store-Versionen Muster für Discovery und Service-Mapping, die älter als 1.21.0 sind. Ab Version 1.21.0 werden alle unterstützten Ressourcentypen in der Tabelle [sn_itom_pattern_acp_supported_resource_types] aufgeführt. Alle Ressourcentypen sind standardmäßig aktiviert. Die MID-Server -Eigenschaft *mid.cmp.azure.event.supported_resource_types* ist nicht mehr verfügbar. In der Tabelle [sn_itom_pattern_acp_supported_resource_types] können Sie einen Eintrag für einen Ressourcentyp und eine Abfrage hinzufügen. Informationen zum Hinzufügen einer Abfrage finden Sie im Abschnitt „VM-Beispielabfrage“ in KB1705862 .

Um Unterstützung für die Change-Verarbeitung für einen Azure -Ressourcentyp in Legacy-Versionenhinzuzufügen, fügen Sie die Ressourcentypen der Eigenschaft *mid.cmp.azure.event.supported_resource_types* hinzu. Als durch Kommas getrennten Wert Erstellen Sie dann Antwortzuordnungen zwischen den Change-Feldern und den Configuration Item (CI)-Feldern. Antwortzuordnungen definieren eine 1:1-Zuordnung zwischen den Quelldatenfeldern und den CI-Feldern. Bei der Change-Verarbeitung Azure werden anhand der Zuordnungsinformationen die Change-Daten der Ressourcen in den entsprechenden CI-Klassenfeldern aktualisiert.

Prozedur

1. Navigieren zu **Alle** > *MID-Server* > **Eigenschaften**.
2. Öffnen Sie die Eigenschaft *mid.cmp.azure.event.supported_resource_types*.
3. Fügen Sie im Feld **Wert** den Ressourcentyp *Azure* als kommagetrennten Wert hinzu.
4. Wählen Sie **Aktualisieren**.
5. Erstellen Sie Antwortzuordnungen für die Change-Felder, die Sie in Configuration Management Database (CMDB)aktualisieren möchten.

   a. Navigieren Sie zur Tabelle „Antwortzuordnung“ [sn_cmp_response_mapping].
   ```
   https://<instance name> .service-now.com/
   sn_cmp_response_mapping_list.do
   ```

   b. Wählen Sie **Neu**.

   c. Füllen Sie die Felder des Formulars aus.

Formular „Antwortzuordnung“.

Feld	Beschreibung
CI-Klasse	Name der CI-Klasse, die die Azure-Ressource in CMDBdarstellt.
Datenquelle	Name der Eingabedatenquelle. Setzen Sie das Feld Datenquelle auf Azure Ressourcenänderungen.
CI-Klassenfelder	Name des CI-Klassenfelds, das dem Quellfeld logisch entspricht.
Quellenfeld	Name des Quellfelds, das Sie im angegebenen CI-Klassenfeld aktualisieren möchten.

Weitere Informationen zur Antwortzuordnung finden Sie unter Thema „Antwortzuordnung verwenden“ in der ServiceNow Community.

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

d. Wählen Sie **Absenden**.

e. Wiederholen Sie die Schritte 5.b bis 5.d für alle Change-Felder, die Sie in CMDBaktualisieren möchten.

Erkennung von Google Cloud Platform

Discovery erkennt Google Cloud Platform und die zugehörigen Komponenten. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Für die Google Cloud Platform-Komponenten erkannten Daten bieten Sichtbarkeit für mehrere ServiceNow-Produkte, einschließlich Cloud Provisioning and Governance.

Discovery verwendet mehrere Muster, um GCP-Komponenten zu erkennen.

Sie können globale und regionale Ressourcen erkennen.

Erkennbare globale und regionale GCP-Ressourcen

Global	Regional
Globale statische externe IP-Adressen	Regionale statische externe IP-Adressen
Globale Lastenausgleichsmodule (Globale HTTP-Lastenausgleichsmodule)	Regionale Lastenausgleichsmodule (regionale HTTP-Lastenausgleichsmodule, TCP/UDP-Lastenausgleichsmodule)
Bilder	Subnetze
Snapshots	Regionale verwaltete Instanzgruppen
Instanzvorlagen	Regionale persistente Festplatten
VPC-Netzwerk	
Firewalls	

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping ab Version 1.8.0 (September 2023)
- CMDB CI-Klassenmodelle ab Version 1.49.0 (September 2023)
- Visibility Content ab Version 6.13.0 (September 2023)

MID-Server-Anforderungen

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

- Verwenden Sie zur Cloud-Erkennung einen dedizierten MID-Server. Der MID-Server muss über 16 Kerne und 8 GB mit 4 GB Java Memory Model (JVM)-Speicherzuweisung verfügen.
- Stellen Sie den dedizierten MID-Server mit Internetzugang bereit und stellen Sie die Verbindung her.
- Weitere Informationen zu den MID-Server -Konfigurationen finden Sie unter Installieren und konfigurieren Sie MID Servers für den Zugriff auf Cloud-Umgebungen.

Google Cloud BigQuery und Google Cloud Bigtable

Um Google Cloud BigQuery und Google Cloud Bigtable zu erkennen, stellen Sie sicher, dass die Eigenschaft *sn_itom_pattern.google_dbservice_table_collection* auf **True**festgelegt ist.

Benutzerrolleneinstellungen

Legen Sie die Benutzerberechtigung für das Google Cloud Platform-Mitglied auf **Betrachter** fest:

1. Navigieren Sie in der Google Cloud Platform-Konsole zu **IAM**.
2. Wählen Sie das entsprechende Mitglied aus der Liste aus, und klicken Sie auf das Symbol **Bearbeiten**.
3. Wählen Sie im Fenster „Bearbeitungsberechtigungen“ in der Liste **Rolle** `Betrachter` aus.
4. Klicken Sie auf **Speichern**.

Überprüfen Sie die Konfiguration der Google API-Anmeldeinformationen

Weitere Informationen finden Sie unter Konfigurieren Sie die Google API-Anmeldeinformationen für Cloud-Discovery

(Optional) Google Cloud Platform-Servicekonto erstellen

Erstellen Sie ein GCP-Servicekonto, um die Ergebnisse dieser Erkennung in Cloud Provisioning and Governance zu verwenden. Verwenden Sie für das Servicekonto die Anmeldeinformationen, die Sie zuvor im Anmeldeinformationsverfahren definiert haben.

1. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**.
2. Klicken Sie auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**. Weitere Informationen finden Sie unter Cloud-Anmeldeinformationen .

Formular „Servicekonto“

Feld	Beschreibung
Name	Name dieses Servicekontos. Beispiel: `gcp-snow`.
Konto-ID	GCP-Projektname

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

Feld	Beschreibung
Discovery Anmeldeinformationen	Discovery-Anmeldeinformationen, die Sie zuvor definiert haben
Datencenter-Typ	Datencenter-Typ. Wählen Sie `Google-Rechenzentrum [cmdb_ci_google_datacenter]`.

Sammeln von Cloud-Protokollierungs-Events aktivieren

Die Google Cloud Platform-Muster können Cloud-Protokollierungs-Events sammeln, die von den nativen Google Cloud-APIs generiert werden. Konfigurieren Sie den Service Google Stackdriver Logging für die automatische Aktualisierung von CMDB.

Cloudbezogenen CI-Beziehungen aktivieren

Um erkannte Komponenten in Serviceinstanzen aufzunehmen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von Service-Mappingverwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Konfiguration der Tag-basierten Discovery.

Stellen Sie sicher, dass ein Zeitplan Discovery konfiguriert ist

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Ressourcen, die von allen zur Erkennung von GCP-Produkte entwickelten Mustern erkannt werden

Feld	Beschreibung
Haupt-CI: Cloud-Servicekonto [cmdb_ci_cloud_service_account]	
account_id	Name des Projekts, das für die Erkennung verwendet wird
object_id	Feld mit demselben Wert wie account_id. Von den IRE-Identifizierungsregeln verwendet.
datacenter_type	Name des CI, das die Rechenzentren für Google Cloud Platform cmdb_ci_google_datacenter enthält
Zugehörige CI: Google-Rechenzentrum [cmdb_ci_google_datacenter]	
Name	Name des Rechenzentrums oder der Region
region	Feld mit demselben Wert wie das Namensfeld
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.

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

Feld	Beschreibung
short_description	Beschreibung des Rechenzentrums oder der Region, die Sie zur einfachen Identifizierung angeben
Status	Status des Rechenzentrums oder der Region Eine der folgenden Möglichkeiten: • In Betrieb • Ausgeschaltet
state	Feld mit demselben Wert wie das Statusfeld
Zugehörige CI: Verfügbarkeitszone [cmdb_ci_av availability_zone]	
Name	Name der Verfügbarkeitszone (AZ)
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
short_description	Verfügbarkeitszonenbeschreibung, die Sie angeben

Ressourcen, die von der Säule Google Cloud Platform Discovery Computer erkannt wurden

Feld	Beschreibung
Zugehörige CI: Virtuelle Maschine [cmdb_ci_vm_instance]	
Name	Name des virtuellen Computers (VM)
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
state	VM-Status. Eine der folgenden Möglichkeiten: • An • Wird ausgeführt • Aus • Beendet • Angehalten
Datenträger und NICs	Anzahl der dieser VM zugewiesenen Datenträger und Netzwerkschnittstellen-Controller (NICs)
CPUs und Arbeitsspeicher	Anzahl der CPU-Kerne und Arbeitsspeichergröße, die dieser VM zugewiesen sind
Zugehörige CI: Instanzvorlage [cmdb_ci_instance_template]	
Name	Name der Instanzvorlage
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
short_description	Beschreibung der Instanzvorlage
source_image	Quell-Image der Instanzvorlage
Zugehörige CI: NIC [cmdb_ci_nic]	

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

Feld	Beschreibung
Name	Name des NIC
object_id	Eindeutiger Bezeichner, der aus einer Verkettung von vm_id + „:“ + nic_name besteht.
ip_address	Primäre interne IP-Adresse des NIC
state	Feld mit demselben Wert wie das GCP-Statusfeld
Zugehörige CI: Speicher-Laufwerk [cmdb_ci_storage_volume]	
Name	Name des Datenträgers
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
size	Datenträgergröße in GB
short_description	Beschreibung, die Sie zur einfachen Identifizierung angeben
state	Status des Datenträgers. Der Status ist immer „verfügbar“, da er bei der Erkennung zurückgegeben wurde.
Status	Installiert
storage_type	Datenträgertyp. Beispielsweise „pd-standard“ oder „lokale SSD“.
Zugehörige CI: Image [cmdb_ci_os_template]	
Name	Name des Image.
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
image_type	Image-Typ
image_source	Image-Quelle, z. B. Quelldatenträger / Snapshot + „/“ + Quelldatenträger-/Snapshot-ID
Zugehörige CI: Hardwaretyp [cmdb_ci_compute_template]	
Name	Name des Image.
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
vCPUs	Anzahl der dieser Vorlage zugewiesenen CPU-Kerne
memory_mb	Speichergröße, die dieser Vorlage zugewiesen ist
local_storage_gb	Speicher, der dieser Vorlage zugewiesen ist

Hinweis: Unter bestimmten Umständen stellen Sie möglicherweise eine ungewöhnlich große Anzahl von Datensätzen in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] fest. In solchen Fällen können Sie die erkannten Hardwaretypen in der Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type] speichern. Weitere Informationen finden Sie unter Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren.

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

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktiviert die Discovery von Cloud-BS-Images.

Ressourcen, die von der Säule Google Cloud Platform Discovery External IP erkannt wurden

Feld	Beschreibung
Zugehörige CI: Öffentliche IP-Adresse [cmdb_ci_cloud_public_ip_address]	
Name	Name der externen IP
public_ip_address	Adresse der öffentlichen IP
state	Status der externen IP-Adresse. Eine der folgenden Möglichkeiten: • In Gebrauch • Verfügbar Verwenden Sie „In Gebrauch“, wenn die externe IP verwendet wird, oder „Verfügbar“, wenn sie für eine spätere Verwendung reserviert ist.

Ressourcen entdeckt durch das Google Cloud Platform Discovery-Lastenausgleichsmodul

Feld	Beschreibung
Zugehörige CI: Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	
Name	Name des load_balancer
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
Zugehörige CI: Load Balancer-Services [cmdb_ci_lb_service]	
Name	Name des Lastenausgleichsmodul-Services
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
service_type	Servicetyp. Einer der folgenden: • Benutzeroberfläche (HTTP/TCP/UDP LB) • Back-End (nur HTTP-LB)
port	Listener-Protokoll-Portnummer (Back-End)
front_end_port	Listener-Protokoll-Portnummer (Front-End)
listener_protocol	Listener-Protokoll Einer von

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

Feld	Beschreibung
	• TCP • HTTP • HTTPS
Pool	Pool, der vom LB-Service verwendet wird
Zugehöriges CI: Load Balancer-Pool [cmdb_ci_lb_pool]	
Name	Poolname. Für TCP-/UDP-LBs ohne Pools der Name, der den LB-Namen **-Pool** enthält.
object_id	Der eindeutige Bezeichner des LB-Pools Für TCP-/UDP-LBs ohne Pools der Name, der den LB-Namen **-Pool** enthält.
Zugehöriges CI: Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	
Name	Name des Poolmitglieds
object_id	Eindeutiger Bezeichner des Poolmitglieds, erstellt aus der ID der Instanz object_id
Zugehöriges CI: Load Balancer Pool-Mitglied [cmdb_ci_lb_health_service]	
Name	Name des Integritätsservice
object_id	Eindeutiger Bezeichner der Integritätsdienstprüfung
monitor_type	Typ der Integritätsprüfung. Einer der folgenden: • TCP • HTTP • HTTPS
timeout_sec	Zeit in Sekunden, die auf die Antwort der Integritätsprüfung gewartet wird
check_interval_sec	Intervall in Sekunden zum Ausführen der Integritätsprüfung
healthy_threshold	Anzahl der sequenziellen erfolgreichen Probe-Ergebnisse, damit eine VM-Instanz als fehlerfrei gilt
unhealthy_threshold	Anzahl der sequenziellen fehlerhaften Probe-Ergebnisse, damit eine VM-Instanz als fehlerhaft gilt
request_path	URL-Pfad, an den GCP Integritätsprüfungs-Probe-Anforderungen sendet. Wenn keine Angabe erfolgt, sendet GCP Probe-Anforderungen an den Stammpfad.
port	Protokoll und Port, um zu bestimmen, wie GCP-Integritätsprüfsysteme mit den VMs in Kontakt treten

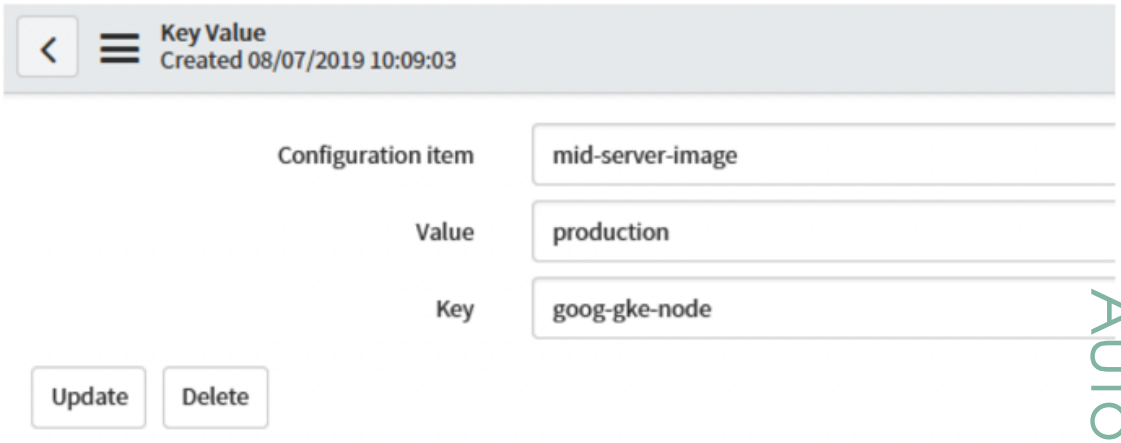
Ressourcen, die von Google Cloud Platform Discovery anhand von Bezeichnungen erkannt wurden

Wenn Google Cloud Platform Discovery während der Erkennung Bezeichnungen verwendet, werden die folgenden Daten aus dem Schlüsselwertformular gesammelt:

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

- Schlüssel
- Wert
- Konfigurationselement

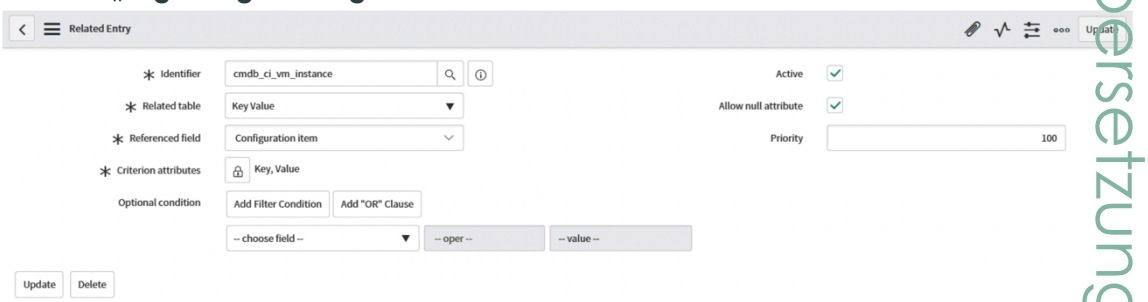
Schlüsselwertformular



Diese Daten werden im Formular „Zugehöriger Eintrag“ für die folgenden CMDB-Tabellen identifiziert:

- Virtuelle Maschine [cmdb_ci_vm_instance]
- Image [cmdb_ci_os_template]
- Speichervolume [cmdb_ci_storage_volume]
- Speicher-Snapshot [cmdb_ci_storage_vol_snapshot], wie vom übergeordneten Element übernommen

Formular „Zugehörige Einträge“



Ressourcen, die von der Säule Google Cloud Platform Discovery Network erkannt wurden

Feld	Beschreibung
Netzwerk [cmdb_ci_network]	
name	Name des VPC-Netzwerks (Virtual Private Cloud)
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
default_gateway	Gateway-Adresse für Standardweiterleitung aus dem Netzwerk

Automatische Übersetzung

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

Feld	Beschreibung
state	Status des Netzwerks Der Status ist immer „verfügbar“, da er bei der Erkennung zurückgegeben wurde.
Cloud-Subnetz [cmdb_ci_cloud_subnet]	
name	Name der Instanzvorlage
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
cidr	Kombination aus Subnetz-CIDR, sekundärem CIDR und IPv6-CIDR. Beispiel: 10.0.0.0/16,10.2.0.0/16,fd20:957:65cb:bc00:0:0:0:0/64,10.1.0.0/16,fd20:957:65cb:bc00:0:0 :0:0/64
subnet_mask	Darstellung der Subnetzmaske mit Punkten. Beispiel: 255.255.255.0
gateway	Gateway-Adresse für Standardweiterleitung aus dem Netzwerk
broadcast_address	Broadcast-Adresse des Subnetzes
available_ip_count	Anzahl der IPs, die im Subnetz verfügbar sind. Dieser Wert enthält keine Netzwerk- und Broadcast-Adressen.
Netzwerk-ACL [cmdb_ci_network_acl]	
name	Name der Zugriffssteuerungsliste (ACL)
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
short_description	ACL-Beschreibung, die Sie angeben
Regel für Netzwerk-Zugriffssteuerungsliste [cmdb_ci_network_acl_rule]	
name	ACL-Regelname. Dieser Name ist mit dem Namen von cmdb_ci_network_acl identisch.
allow_deny	ACL-Regelverhalten Einer der folgenden: • Zugelassen • Abgelehnt
is_outbound	Regel für ausgehenden Datenverkehr. Verwenden Sie eine der folgenden Optionen: • „True“, wenn die Regel für ausgehenden Datenverkehr ist • „False“, wenn die Regel für eingehenden Datenverkehr ist
source_ranges	JSON-Blobservice, der Quellen enthält, die CIDR-Darstellungen (Classless Inter-Domain Routing) sind, für die die Regel den Datenverkehr vom Service zulässt oder blockiert

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

Feld	Beschreibung
destination_ranges	JSON-Blobservice, der Ziele enthält, die CIDR-Darstellungen sind, für die die Regel den Datenverkehr vom Service zulässt oder blockiert
target_tags	JSON-Blobservice, der die Liste der Tags darstellt, die steuern, für welche Instanzen die Firewall-Regel gilt
allowed_deny_traffic	JSON-Blobservice, der die Regeln enthält, die von dieser ACL-Regel entweder zugelassen oder verweigert werden
Image [cmdb_ci_os_template]	
name	Name des Image.
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
image_type	Image-Typ
image_source	Image-Quelle, z. B. Quelldatenträger / Snapshot + „/“ + Quelldatenträger-/Snapshot-ID
Hardwaretyp [cmdb_ci_compute_template]	
name	Name des Image.
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
vCPUs	Anzahl der dieser Vorlage zugewiesenen CPU-Kerne
memory_mb	Speichergröße, die dieser Vorlage zugewiesen ist
local_storage_gb	Speicher, der dieser Vorlage zugewiesen ist

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktiviert die Discovery von Cloud-BS-Images.

Ressourcen, die von der Säule Google Cloud Platform Discovery Storage erkannt wurden

Feld	Beschreibung
Speichervolume [cmdb_ci_storage_volume]	
name	Name des Speicherdatenträgers
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
size	Datenträgergröße in GB
state	Status des Netzwerks Der Status ist immer „verfügbar“, da er bei der Erkennung zurückgegeben wurde.
Status	Datenträgerstatus: Installiert

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

Feld	Beschreibung
storage_type	Datenträgertyp. Beispielsweise „pd-standard“ oder „local-ssd“.
Datenträgertyp [cmdb_ci_disk_type]	
name	Name des Datenträgers im Format: <Datenträgertyp-Name>@<Zonenname>
object_id	Datenträgertyp ist pro Zone eindeutig. Verwendetes Format: <Zone>:<Datenträgertyp-Name>
short_description	Beschreibung des Datenträgertyps. Beispielsweise „lokale SSD“.
valid_disk_size	Datenträgergrößen, die für diesen Datenträgertyp gültig sind
default_disk_size_gb	Standard-Datenträgergröße (in GB) für diesen Datenträgertyp
Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]	
name	Name des Snapshots
object_id	Eindeutiger Bezeichner, der von Google Cloud für diese Ressource zugewiesen wird.
short_description	ACL-Beschreibung, die Sie angeben
state	Feld mit demselben Wert wie das GCP-Statusfeld
volume_name	Name des Quelldatenträgers: Speichervolume [cmdb_ci_storage_volume]
Kapazität	Anzahl der im Snapshot gespeicherten Bytes

Für Google Cloud Memorystore, Google Cloud BigQuery, Google Cloud Bigtable, Google Cloud Spanner und Google Cloud SQL erkannte Ressourcen

Feld	Beschreibung
Cloud-Datenbank [cmdb_ci_cloud_database]	
name	Eigenschaften der Cloud-Datenbank.
object_id	
install_status	
operational_status	
state	
Typ	
processing_units (nur für Cloud Spanner)	
Datenbank [cmdb_ci_database]	
name	Eigenschaften der Datenbank.
Typ	

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

Feld	Beschreibung
install_status	

Für Google Cloud Firebase erkannte Ressourcen

Feld	Beschreibung
Cloud-Datenbank [cmdb_ci_cloud_database]	
name	Eigenschaften der Cloud-Datenbank.
object_id	
install_status	
operational_status	
state	
Typ	

Für Google Cloud Firebase Datastore erkannte Ressourcen

Feld	Beschreibung
Datenbank [cmdb_ci_database]	
name	Eigenschaften der Datenbank.
Typ	
install_status	

Von den Mustern „Virtual Google Cloud Platform (GCP) – VM-Lizenz“ und Google Cloud Platform (GCP) „ – Virtual Server“ erkannte Ressourcen

In diesen Mustererweiterungsabschnitten wird die Bring Your Own License (BYOL) oder die enthaltenen Lizenzen für Windows-VMs und RHEL-VMs erkannt.

Feld	Beschreibung
Schlüsselwert [cmdb_key_value]	
Schlüssel [key]	Der Schlüssel ist eine der Optionen: • Windows_OS_License_Type_automatic • RHEL_OS_License_Type_automatic • SQL_Server_Lizenz_Typ_automatisch
Wert [value]	Der Wert ist eine der Optionen: • BYOL • Lizenz enthalten
CI [ci]	Verweis auf den Datensatz der VM-Instanz.
Klasse	Die Klasse ist *Virtual Machine Instance*.

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

CI-Beziehungen

Diese Beziehungen sollen die Google Cloud Platform-Erkennung unterstützen.

Beziehungen für Ressourcen, die von der Säule Google Cloud PlatformComputer erkannt werden

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]		
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Verfügbarkeitszone [cmdb_ci_av availability_zone]		
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Virtuelle Maschine [cmdb_ci_vm_instance]		
Virtuelle Maschine [cmdb_ci_vm_instance]	Gehostet auf::Host	Google-Rechenzentrum [cmdb_ci_google_datacenter]
	Enthält::Enthalten in	cmdb_ci_availability_zone
Instanzvorlage [cmdb_ci_instance_template]		
Instanzvorlage [cmdb_ci_instance_template]	Host::Gehostet auf	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
	Verwendet::Verwendet von	Hardwaretyp [cmdb_ci_compute_template]
		Image [cmdb_ci_os_template]
NIC [cmdb_ci_nic]		
NIC [cmdb_ci_nic]	Gehostet auf::Host	Google-Rechenzentrum [cmdb_ci_google_datacenter]
	Endpunkt implementieren auf	cmdb_ci_endpoint_vnic
	Endpunkt implementieren von	Virtuelle Maschine [cmdb_ci_vm_instance]
Zugehörige CI: Speicher-Laufwerk [cmdb_ci_storage_volume]		
Speichervolume [cmdb_ci_storage_volume]	Enthält::Enthalten in	cmdb_ci_availability_zone
	Endpunkt implementieren auf:	cmdb_ci_endpoint_block
	Endpunkt implementieren von:	Virtuelle Maschine [cmdb_ci_vm_instance]
Image [cmdb_ci_os_template]		
Image [cmdb_ci_os_template]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Zugehöriges CI: Cloud-Image [cmdb_ci_cloud_os_image]		
Hardwaretyp [cmdb_ci_compute_template]		

Automatische Übersetzung

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

CI	Beziehung	CI
Hardwaretyp [cmdb_ci_compute_template]	Gehostet auf::Host	cmdb_ci_ google_datacenter
	Bereitgestellt von:	Hardwaretyp [cmdb_ci_compute_template]

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktiviert die Discovery von Cloud-BS-Images.

Beziehungen für Ressourcen, die von der Säule Google Cloud Platform IP erkannt werden

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]		
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Host	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Verfügbarkeitszone [cmdb_ci_av availability_zone]		
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Öffentliche IP-Adressen [cmdb_ci_cloud_public_ipaddress]		
Öffentliche IP-Adressen [cmdb_ci_cloud_public_ipaddress]	Gehostet auf::Host	Google-Rechenzentrum [cmdb_ci_google_datacenter] Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Beziehungen für Ressourcen, die vom Google Cloud Platform-Lastenausgleichsmodul erkannt werden

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]		
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
	Enthält::Enthalten in	cmdb_ci_availability_zone
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]		
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter] Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Load Balancer-Pool [cmdb_ci_lb_pool]		
Load Balancer-Pool [cmdb_ci_lb_pool]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]

Automatische Übersetzung

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

CI	Beziehung	CI
	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Load Balancer-Services [cmdb_ci_lb_service]		
Load Balancer-Services [cmdb_ci_lb_service]	Gehostet auf::Host	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Lastenausgleichsmodul-Services [cmdb_ci_lb_service] (Für HTTP LB)		
Load Balancer-Services [cmdb_ci_lb_service]	Verwendet::Verwendet von	Load Balancer-Pool [cmdb_ci_lb_pool]
Zugehörige CI: Cloud-Load Balancer [cmdb_ci_cloud_load_balancer] für TCP/UDP LB		
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Verwendet::Verwendet von	Load Balancer-Pool [cmdb_ci_lb_pool]
Integritätsservice [cmdb_ci_lb_health_service] (Für HTTP LB)		
Integritätsservice [cmdb_ci_lb_health_service]	Verwendet::Verwendet von	Load Balancer-Services [cmdb_ci_lb_service]
Integritätsservice [cmdb_ci_lb_health_service] (Für HTTP LB)		
Integritätsservice [cmdb_ci_lb_health_service]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter] Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Integritätsservice [cmdb_ci_lb_health_service] (Für TCP/UDP LB)		
Integritätsservice [cmdb_ci_lb_health_service]	Verwendet::Verwendet von	Load Balancer-Pool [cmdb_ci_lb_pool]

Beziehungen für Ressourcen, die von der Säule Google Cloud PlatformNetwork erkannt werden

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]		
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Host	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Verfügbarkeitszone [cmdb_ci_av availability_zone]		
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Netzwerk [cmdb_ci_network]		
cmdb_ci_network	Gehostet auf::Host	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Cloud-Subnetz [cmdb_ci_cloud_subnet]		
cmdb_ci_cloud_subnet	Enthält::Enthalten	cmdb_ci_network
		Google-Rechenzentrum [cmdb_ci_google_datacenter]

Automatische Übersetzung

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

CI	Beziehung	CI
Netzwerk-ACL [cmdb_ci_network_acl]		
cmdb_ci_network_acl	Enthält::Enthalten	cmdb_ci_network
Netzwerk-ACL-Regel [cmdb_ci_network_acl_rule]		
cmdb_ci_network_acl_rule	Enthält::Enthalten	cmdb_ci_network_acl

Beziehungen für Ressourcen, die von der Säule Google Cloud Platform Storage erkannt werden

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]		
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Host	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
cmdb_ci_availability_zone		
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Speichervolume [cmdb_ci_storage_volume]		
Speichervolume [cmdb_ci_storage_volume]	Enthält::Enthalten	Verfügbarkeitszone [cmdb_ci_av availability_zone]
	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Datenträgertyp [cmdb_ci_disk_type]		
Datenträgertyp [cmdb_ci_disk_type]	Host::Gehostet auf	Verfügbarkeitszone [cmdb_ci_av availability_zone]
		Google-Rechenzentrum [cmdb_ci_google_datacenter]
Snapshot des Speichervolumes [cmdb_ci_storage_vol_snapshot]		
Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
	Bereitgestellt von::Bereitgestellt mit	Speichervolume [cmdb_ci_storage_volume] Diese Beziehung bedeutet, dass dieser Datenträger von diesem Snapshot erstellt wurde.
	Repliziert zu::Repliziert von	Speichervolume [cmdb_ci_storage_volume] Diese Beziehung bedeutet, dass dieser Snapshot von diesem Datenträger erstellt wurde.

Für die VM-Instanz erkannte Beziehungen

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

CI	Beziehung	CI
Server [cmdb_ci_server]	Virtualisiert von::Virtualisiert	VM-Instanz [cmdb_ci_instance]

Für Google Cloud BigQuery, Google Cloud SQL, Google Cloud Spanner und Google Cloud Bigtable erkannte Ressourcen

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Repliziert zu::Repliziert von	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Enthält::Enthalten in	Datenbank [cmdb_ci_database]
Schlüsselwert [cmdb_key_value]	Nur Referenz	Cloud-Datenbank [cmdb_ci_cloud_database]

Für Google Cloud Platform Firebase erkannte Beziehungen

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Repliziert zu::Repliziert von	Google-Rechenzentrum [cmdb_ci_google_datacenter]

Beziehungen für Google Cloud Platform Firestore

CI	Beziehung	Ci
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]

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

CI	Beziehung	Ci
Cloud-Datenbank [cmdb_ci_cloud_database]	Repliziert zu::Repliziert von	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Beziehungen für Google Cloud Platform Memorystore

CI	Beziehung	CI
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Google-Rechenzentrum [cmdb_ci_google_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Cloud-Datenbank [cmdb_ci_cloud_database]	Gehostet auf::Hostet	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Cloud-Datenbank [cmdb_ci_cloud_database]	Repliziert zu::Repliziert von	Verfügbarkeitszone [cmdb_ci_av availability_zone]
Schlüsselwert [cmdb_key_value]	Nur Referenz	Cloud-Datenbank [cmdb_ci_cloud_database]

Daten, die von Service-Mapping während der tagbasierten Erkennung erfasst wurden

Service-Mapping verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Konfigurieren Sie den Service Google Stackdriver Logging für die automatische Aktualisierung von CMDB

Sie können den Google Stackdriver Logging-Service aktivieren, um CMDB CI-Daten automatisch zu aktualisieren, wenn Google Cloud Connector oder Ihr Google-Konto bei einer Google Cloud Platform-Ressource eine Änderung des Lebenszyklusstatus oder der Konfiguration durchführt. Die CI-Daten werden dann in der CMDB aktualisiert, ohne dass auf die Ausführung von Discovery gewartet werden muss.

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

Vorbereitungen

- Aktivieren Sie Discovery and Service Mapping-Muster. Weitere Informationen finden Sie unter Google Cloud Platform Discovery.
- Discovery hat die logischen Rechenzentren des Google-Projekts erfolgreich erkannt. Weitere Informationen finden Sie unter Richten Sie Cloud-Konto und Servicekonto für ein Google Cloud Platform.

> **Hinweis:** Vergewissern Sie sich, dass Sie auf der Seite „Google-Servicekonto“ das Kontrollkästchen **Sollte Events abrufen** aktiviert haben, bevor Sie Discovery für das Rechenzentrum ausführen.

Erforderliche Rolle:

- discovery_admin für Cloud-Discovery und `sn_cmp.cloud_event_integration`, wenn eine Authentifizierung beim Cloud-Event-Endpunkt erforderlich ist. Diese Rolle ist erforderlich, um eine Warnungsregel in der Instanz einzurichten.
- Google Cloud Platform-Administrator für Konfigurationsschritte in der GCP-Konsole.
- Protokollierungsrolle für den Google Cloud Platform (GCP)-Integrationsbenutzer, die OAuth-Bereiche für Folgendes zulässt:
  - `https://www.googleapis.com/auth/logging.admin`
  - `https://www.googleapis.com/auth/cloud-platform.read-only`
  - `https://www.googleapis.com/auth/cloud-platform`
  - `https://www.googleapis.com/auth/logging.read`

Warum und wann dieser Vorgang ausgeführt wird

Discovery unterstützt Warnungen der Monitoring API-Warnungen der Operations Suite von Google Cloud aus einem bestimmten Projekt im Google Cloud Platform. Wenn eine Warnung/ein Event für die Ressourcen in einem Projekt generiert wurde, erfasst Discovery die Warnungsdaten.

Erstellen und verwalten Sie Warnungsrichtlinien mit der Überwachungskonsole der Operations Suite von Google Cloud, der Überwachungs-API der Operations Suite und dem Cloud SDK. Jede Richtlinie legt Folgendes fest:

- Bedingungen, die angeben, dass sich eine Ressource oder eine Gruppe von Ressourcen in einem fehlerhaften Zustand befindet.
- Benachrichtigungen, die über E-Mail, SMS oder andere Kanäle gesendet werden, um darauf hinzuweisen, dass ein Ressourcenstatus fehlerhaft ist.
- Dokumentation oder Informationen, die in einige Benachrichtigungstypen aufgenommen werden können, um Ihr Supportteam bei der Lösung des Problems zu unterstützen.

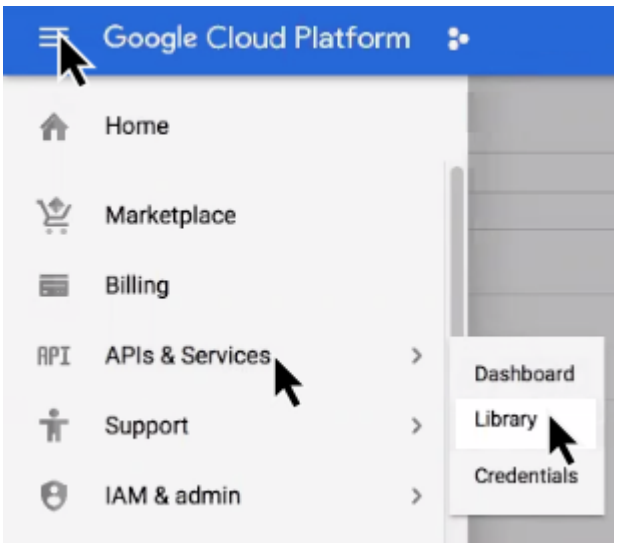
Wenn Ereignisse Bedingungen in einer Ihrer Warnungsrichtlinien auslösen, erstellt die Überwachung der Operations Suite von Google Cloud einen Incident und zeigt ihn in der Überwachungskonsole der Operations Suite von Google Cloud an.

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

Hinweis: Wenn Sie sich in einer domänengetrennten Instanz befinden, sind nur die Events sichtbar, die in der CMDB aktualisiert wurden und zu Ihrer Domäne gehören. Events erstellen Configuration Items (CIs) in der gleichen Domäne wie das Cloud-Servicekonto, dem sie zugeordnet sind. Events, die keinem Servicekonto zugeordnet sind, sind für alle Domänen sichtbar.

Prozedur

1. Melden Sie sich bei Ihrem Google Cloud Platform-Konto an.
   Navigieren Sie für Ihr Projekt zu **APIs und Services** > **Bibliothek**.

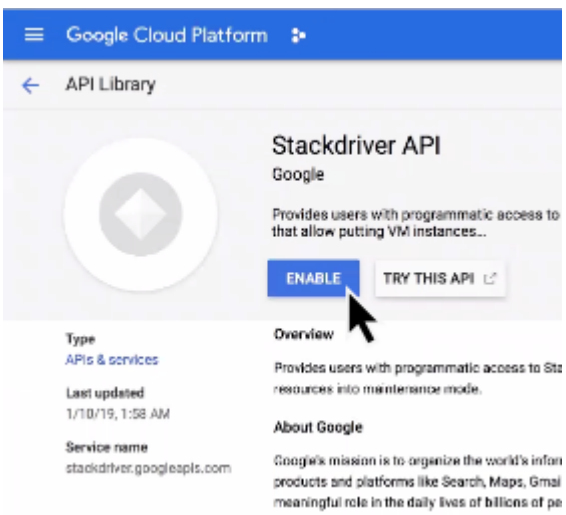


2. Aktivieren Sie sowohl die **Stackdriver API** als auch die **Cloud Logging API**.

   a. Suchen Sie in der Bibliothek nach `Stackdriver`.

   b. Klicken Sie auf die Karte **Stackdriver API**.

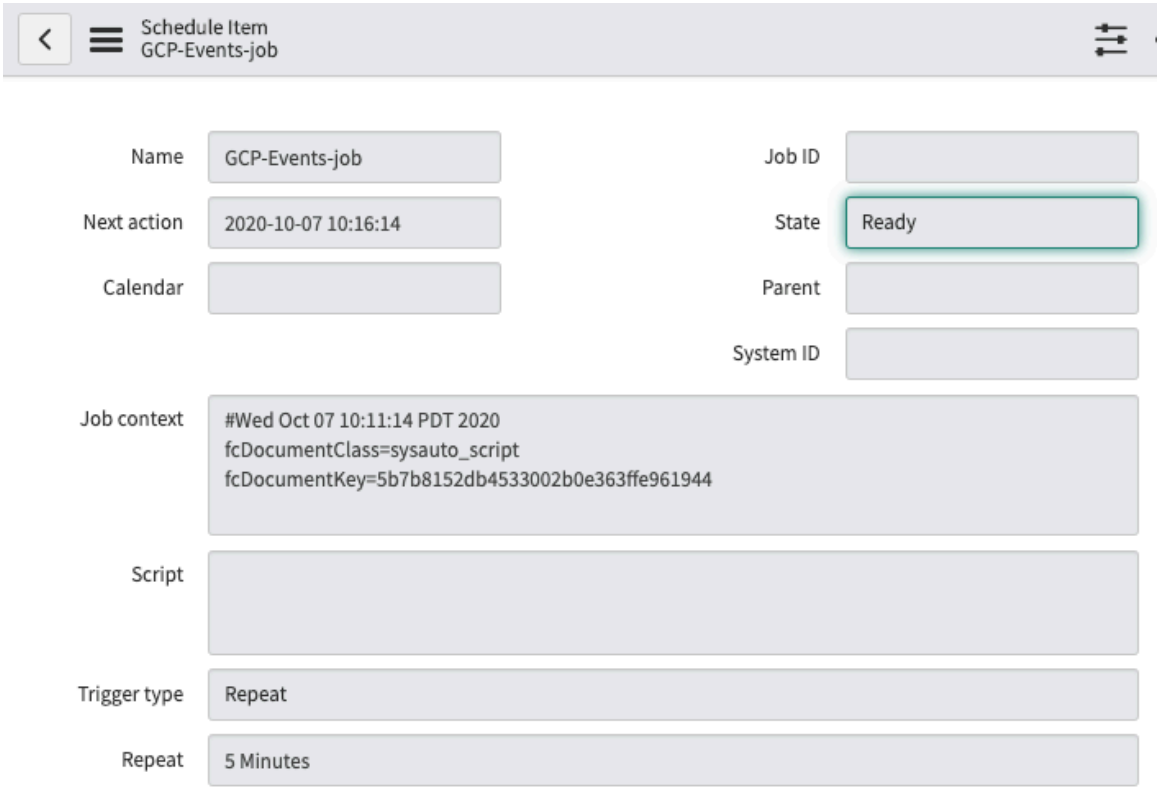
   c. Klicken Sie auf der Seite der Stackdriver API auf **Aktivieren**.



3. Wiederholen Sie den vorherigen Schritt für die **Cloud Logging API**.
   Standardmäßig ruft eine regelmäßigen Aufgabe für Ihre Instanz (GCP-Events-job) alle 5 Minuten Aktualisierungen vom Google Stackdriver Logging-Service ab.

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

4. Um den Zeitplan zu ändern, navigieren Sie zu **Systemzeitplaner** > **Geplante Aufgaben** Klicken Sie dann auf **GCP-Events-job**, und aktualisieren Sie anschließend die Einstellung **Wiederholen** nach Bedarf.



5. Klicken Sie auf **Aktualisieren**.

Ergebnisse

- Sobald die Google Cloud Platform ein Event generiert und Discovery die Eventinformationen empfängt, werden die regelmäßigen Aufgaben „GCP-Events-job“ im Hintergrund ausgeführt.

- Durch den geplanten Auftrag wird die Eventnutzlast an das Modul für Identifizierung und Abgleich (Identification and Reconciliation Engine, IRE) übergeben. Die IRE ergreift dann die erforderlichen Aktionen, um den Status der Ressourcen basierend auf dem Event zu ändern.

Erkennung von IBM-Clouds

Wenn sich Ihre Cloud-Ressourcen in einer IBM-Cloud befinden, erstellen Sie Anmeldeinformationen, die auf das IBM-Konto zugreifen können.

Formular für IBM-Anmeldeinformationen

Feld	Wert
Name	Eindeutiger Name der IBM-Anmeldeinformationen, die bei der Instanz registriert werden sollen

Automatische Übersetzung

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

Formular für IBM-Anmeldeinformationen (Fortsetzung)

Feld	Wert
Reihenfolge	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
SoftLayer-API-Benutzer	Benutzername der Softlayer-Cloud
SoftLayer-API-Schlüssel	Schlüssel der SoftLayer-API
Bluemix-API-Schlüssel	Schlüssel der Bluemix-API

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Um erkannte Komponenten in Serviceinstanzen aufzunehmen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von Service-Mappingverwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Konfiguration der Tag-basierten Discovery.

Service-Mapping verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

API-Liste für IBM Cloud Discovery

Region

CI-Attribute	IBM-Einschränkungen
object_id	Name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Region (Fortsetzung)

dns_domain	domain
Name	alias
short_description	display_name
region	Name

cmdb_ci_availability_zone

CI-Attribute	IBM-Einschränkungen
object_id	id
short_description	longName
Name	Name
install_status	statusId

Standortgruppe (cmdb_ci_cloud_location_group)

CI-Attribute	IBM-Einschränkungen
object_id	id
short_description	Beschreibung
location_group_type_id	locationGroupTypeId
Name	Name
location_group_type	locationGroupType.name

Virtueller Server (cmdb_ci_vm_instance)

CI-Attribute	IBM-Einschränkungen
object_id	id
CPUs	maxCpu/startCpus
memory	maxMemory
disks	<nicht zugeordnet>
disks_size	<nicht zugeordnet>
nics	<nicht zugeordnet>
terminated_on	<nicht zugeordnet>
Status	statusId
termination_protection	<nicht zugeordnet>
short_description	notes
Name	hostname
dns_domain	domain

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Virtueller Server (cmdb_ci_vm_instance) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
fqdn	fullyQualifiedDomainName

Image (cmdb_ci_os_template)

CI-Attribute	IBM-Einschränkungen
cmdb_ci_os_template	
image_type	
guest_os	
Version	
offer	
OS Status	
root_device_type	
image_source	
Anmeldeinformationen	
infuse_key	
update_host_name	
Name	Name
object_id	id
short_description	Beschreibung

Öffentlichen Schlüssel hinzufügen (cmdb_ci_cloud_key_pair)

CI-Attribute	IBM-Einschränkungen
object_id	id
finger_print	fingerprint
created_date	createDate
key	key
Name	Bezeichnung
modify_date	modifyDate
short_description	notes

Speichervolume (cmdb_ci_storage_volume)

CI-Attribute	IBM-Einschränkungen
volume_id	id
size	capacityGb
size_bytes	capacityGb

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichervolume (cmdb_ci_storage_volume) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
free_space	<nicht zugeordnet>
free_space_bytes	<nicht zugeordnet>
media_type	<nicht zugeordnet>
file_system	<nicht zugeordnet>
Bezeichnung	serviceResourceName
lun (Logische Einheitsnummer)	<nicht zugeordnet>
volume_container	<nicht zugeordnet>
Status	?
storage_type	storageTypeId
protected_by	<nicht zugeordnet>
share_count	<nicht zugeordnet>
sharable	FALSCH
Gerät	guestId
delete_on_termination	<nicht zugeordnet>
mapping_type	<nicht zugeordnet>
object_id	id
vdisk_id	<nicht zugeordnet>
storage_type	nasType
Name	serviceResourceName

Snapshot des Speichervolume (cmdb_ci_storage_vol_snapshot)

CI-Attribute	IBM-Einschränkungen
object_id	id
Kapazität	capacityGb
is_encrypted	
volume_name	serviceResourceName
storage_server	
start_time	
Status	
snapshotSizeBytes	snapshotSizeBytes

Netzwerk (cmdb_ci_network)

CI-Attribute	IBM-Einschränkungen
Status	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerk (cmdb_ci_network) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
cidr	<nicht zugeordnet>
is_external	Wahr/Falsch
netmask	<nicht zugeordnet>
broadcast_address	<nicht zugeordnet>
default_gateway	<nicht zugeordnet>
is_shared	<nicht zugeordnet>
is_dhcp_enabled	<nicht zugeordnet>
scope	<nicht zugeordnet>
max_ports	<nicht zugeordnet>
terminated_on	<nicht zugeordnet>
provided_contracts	<nicht zugeordnet>
object_id	id
access_port_vlan	vlanNumber
<nicht zugeordnet>	primarySubnetId
Name	vlanNumber
<nicht zugeordnet>	accountId

Subnetz (cmdb_ci_cloud_subnet)

CI-Attribute	IBM-Einschränkungen
subnet_mask	netmask
cidr	networkIdentifier +'/' + cidr
available_ip_count	usableIpAddressCount
broadcast_address	broadcastAddress
primary_dns	<nicht zugeordnet>
secondary_dns	<nicht zugeordnet>
tertiary_dns	<nicht zugeordnet>
is_dhcp_enabled	<nicht zugeordnet>
ipam_provider	<nicht zugeordnet>
domain_name	<nicht zugeordnet>
parent_domain_name	<nicht zugeordnet>
gateway	gateway
route_table_association_id	<nicht zugeordnet>
Status	<nicht zugeordnet>
<nicht zugeordnet>	modifyDate

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subnetz (cmdb_ci_cloud_subnet) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
<nicht zugeordnet>	Version
<nicht zugeordnet>	networkVlanId
<nicht zugeordnet>	isCustomerRoutable
object_id	id
<nicht zugeordnet>	broadcastAddress
<nicht zugeordnet>	isCustomerOwned
<nicht zugeordnet>	sortOrder
<nicht zugeordnet>	networkIdentifier
<nicht zugeordnet>	totalIpAddresses
<nicht zugeordnet>	addressSpace
category	subnetType
Name	networkIdentifier +'/' + cidr

Compute-Sicherheitsgruppe (cmdb_ci_compute_security_group)

CI-Attribute	IBM-Einschränkungen
region	<nicht zugeordnet>
object_id	id
intId	<nicht zugeordnet>
tenant_name	<nicht zugeordnet>
Status	<nicht zugeordnet>
<nicht zugeordnet>	port
<nicht zugeordnet>	Beschreibung
<nicht zugeordnet>	createDate
<nicht zugeordnet>	modifyDate
Name	Name
short_description	Beschreibung

Neues CI (cmdb_ci_compute_security_group_rule)

CI-Attribute	IBM-Einschränkungen
erstellt	createDate
direction	direction
ethertype	ethertype
object_id	id
aktualisiert	modifyDate

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neues CI (cmdb_ci_compute_security_group_rule) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
portRangeMax	portRangeMax
portRangeMin	portRangeMin
protocol	protocol
remoteGroupId	remoteGroupId
securityGroupId	securityGroupId

Lastenausgleichsmodul [cmdb_ci_cloud_load_balancer]

CI-Attribute	IBM-Einschränkungen
Status	"operatingStatus"
canonical_hosted_zone_id	
canonical_hosted_zone_name	
dns_name	address
snat_ip_address	
vlan	
app_code	
component_code	
env_code	
ip_address_pool	
	"accountId"
	"address"
	"createDate"
	"description"
object_id	"id"
	isPublic
	"locationId"
	"modifyDate"
Name	"name"
	"provisioningStatus"
	"useSystemPublicIpPool"
	"uuid"

Lastenausgleichsservice (cmdb_ci_lb_service)

CI-Attribute	IBM-Einschränkungen
cmdb_ci_lb_service	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lastenausgleichsservice (cmdb_ci_lb_service) (Fortsetzung)

CI-Attribute	IBM-Einschränkungen
Pool	
port	protocolPort
last_port	
input_url	
host_name	
back_end_port	
front_end_port	protocolPort
listener_protocol	protocol
server_port	
server_protocol	
traffic_domain	
ssl_certificate_id	
object_id	id
hit_count	

LB-Integritätsservice (cmdb_ci_lb_health_service erweitert cmdb_ci_vm_object)

CI-Attribute	IBM-Einschränkungen
check_interval_sec	interval
max_retries	maxRetries
monitor_type	monitorType
provisioning_status	provisioningStatus
timeout_sec	timeout
object_id	id

LB Pool (cmdb_ci_lb_pool)

CI-Attribute	IBM-Einschränkungen
	createDate
load_balancing_method	loadBalancingAlgorithm
	modifyDate
	protocol
	protocolPort
pool_status	provisioningStatus
object_id	uuid

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LB-Poolmitglied (cmdb_ci_lb_pool_member)

CI-Attribute	IBM-Einschränkungen
server_id	address
object_id	id
	createDate
	modifyDate
	provisioningStatus
	uuid
	weight

Ressourcengruppe (cmdb_ci_resource_group)

CI-Attribute	IBM-Einschränkungen
Name	Name
Nachschauen, was das ist?	quota_id
	tags
object_id	id

Organisation (cmdb_ci_cloud_org)

CI-Attribute	IBM-Einschränkungen
Name	Name
url	url
billing_enabled	billing_enabled
quota_definition_url	quota_definition_url
spaces_url	spaces_url
guid	guid
Status	Status
object_id	metadata.guid

Organisation (cmdb_ci_cloud_space)

CI-Attribute	IBM-Einschränkungen
Name	Name
url	url
object_id	metadata.guid
allow_ssh	allow_ssh
guid	metadata.guid

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennung von VMware-Clouds

Anwendungen, mit denen auf VMware-Cloud-Ressourcen zugegriffen wird, benötigen Zugriff auf VMware-Anmeldeinformationen.

Beispielsweise ermöglicht der Anmeldeinformationstyp „VMware“ Discovery, das auf einem Windows-Computer ausgeführte vCenter von VMware zu untersuchen, um ESX-Maschinen, virtuelle Maschinen und Ressourcenpools zu erkennen. VMware Discovery und die Automatisierungs-API (vCenter-API) stellen jetzt die global eindeutige Seriennummer für Computer-CIs bereit. CIM-Anmeldeinformationen sind nicht erforderlich, um den Zugriff auf jeden VMware-Host zu aktivieren.

Hinweis: Windows-Anmeldeinformationen sind für vCenter Discoverynicht erforderlich, wenn gültige VMware-Anmeldeinformationen verwendet werden.

Formular für VMWare-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für die VMware-Anmeldeinformationen ein.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Anwendername	Geben Sie den Anwendernamen ein, den Sie für Ihr VMware-Konto verwenden. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt. Die VMware-Anmeldeinformationen müssen in vCenter über die Rolle mit Lesezugriff verfügen.
Passwort	Geben Sie das Passwort für das VMware-Konto ein.
Betrifft	Wählen Sie einen oder mehrere MID Servers aus der Liste der verfügbaren MID Serversaus. Die in diesem Datensatz konfigurierten Anmeldeinformationen sind für MID Servers in dieser Liste verfügbar. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Reihenfolge	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.

Konfigurieren Sie den Service VMware-Events für die automatische Aktualisierung von CMDB

Konfigurieren Sie Events der Cloud-Umgebung so, dass die CMDB ohne zusätzlichen Scanvorgang aktualisiert wird. Der VMware-Events-Service kann CI-Daten in der CMDB automatisch aktualisieren, wenn Cloud Provisioning and Governance bei einer VMware-Ressource eine Änderung des Lebenszyklusstatus oder der Konfiguration durchführt. Die CI-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten werden dann in der CMDB aktualisiert, ohne dass Discovery vorher ausgeführt werden muss.

Vorbereitungen

Wichtig: Sie können den Service für VMware-Events so konfigurieren, dass die CMDB für eventbasierte Erkennungs- oder Konfigurationsänderungen automatisch aktualisiert wird, auch wenn Sie die Cloud Provisioning and Governance-Plugins nicht abonniert und aktiviert haben.

- Sie müssen über ein Cloud-Konto mit VMware, Servicekonten und zugehörigen logischen Rechenzentren verfügen.
- Die folgenden Cloud Provisioning and Governance-Plugins müssen aktiviert sein (nicht obligatorisch für Cloud Discovery):
  - Cloud Provisioning and Governance (com.snc.cloud.mgmt)
  - Cloud Provisioning and Governance Core (com.snc.cloud.core)
  - Cloud API (com.snc.cloud.api)
  - Verwaltung der Cloud-Konfiguration (com.snc.config.mgmt)
- Ein MID-Server muss mit den Fähigkeiten **„Alle“** oder **„VMware“** verfügbar sein.
- Die vCenter-Rechenzentren werden erfolgreich erkannt, und die zugehörigen Daten werden ausgefüllt.

Erforderliche Rolle: sn_cmp.cloud_event_integration

Warum und wann dieser Vorgang ausgeführt wird

Wenn VMware-Events ein Update sendet, verarbeitet die Instanz das Event und erstellt oder aktualisiert den CI-Eintrag in der CMDB und die CI-Informationen im Cloud-Anwenderportal. Jedes Event wird als Datensatz in der Tabelle „Events“ auf Ihrer Instanz gespeichert. Konfigurieren Sie alle Event-/Warnungsregeln im vCenter.

So stellen Sie eine Verbindung mit einem anderen MID-Server oder mit vCenter her: Aktualisieren Sie die Einstellungen, und klicken Sie dann auf den zugehörigen Link **Starten**. Der Wert für **Status** ändert sich in **Aktualisierung läuft** und dann in **Gestartet**.

Wichtig:

Wenn Sie sich in einer domänengetrennten Instanz befinden, sind nur die Events sichtbar, die zur CMDB aktualisiert wurden und zu Ihrer Domäne gehören. Events erstellen Configuration Items (CIs) in der gleichen Domäne wie das Cloud-Servicekonto, dem sie zugeordnet sind. Events, die keinem Servicekonto zugeordnet sind, sind für alle Domänen sichtbar.

Während der Eventverarbeitung identifiziert der Cloud Event Scheduler die Domäne des Serviceaccounts und weist sie dem Event zu. Wenn beim Identifizieren der Domäne vor der Verarbeitung ein Fehler auftritt, kann das Event manchmal nicht zugewiesen werden und wird für alle Domänen sichtbar. Um zu verhindern, dass die fehlgeschlagenen Events für alle Domänen sichtbar sind, können Sie die Eigenschaft *sn_cmp.error_events.default_domain* auf die sys_id der Service Provider-Domäne festlegen, sodass die fehlgeschlagenen Events nur dem Domänenadministrator des Service Providers angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie auf eine der folgenden Arten zur VMware-Warnungskonfiguration:
   - Verwenden Sie `https://baseURL/ecc_agent_ext_context_vcenter` zur direkten Navigation über die URL.
   - Navigieren Sie im **Cloud-Adminportal zu Verwalten** > **Warnmeldungskonfigurationen**.
2. Klicken Sie auf der Registerkarte **VMware** auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

vCenter-Ereignissammlungskontext

Feld	Beschreibung
Name	Ein eindeutiger Name für den Datensatz der Event-Sammlung
Kurzbeschreibung	Kurzbeschreibung des Datensatzes
Ausführen auf	Wählen Sie **Spezifischer MID Server** aus.
MID-Server	Wählen Sie einen MID-Server.
vCenter	Wählen Sie das zu überwachende vCenter aus.
Erweiterung [schreibgeschützt]	Die MID-Server-Erweiterung dieses Kontexts. Aktualisiert, wenn die Datenerfassung beginnt.
Status [schreibgeschützt]	Der Status des Datenerfassungsprozesses, z. B. „Wird gestartet“, „Gestartet“ usw.
Ausführung auf [schreibgeschützt]	Der MID-Server, auf dem der Eventsammler ausgeführt wird.

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.
5. Testen Sie die Verbindung zwischen dem vCenter und dem MID-Server: Klicken Sie auf **Testparameter**.
   In einem Popup-Fenster wird bei Erfolg **Parameter verifiziert** angezeigt. Das Feld **Status** ändert sich nicht. Zum Aktualisieren eines Parameters (z. B. zum Ändern von MID-Server oder vCenter) ändern Sie die Einstellung und klicken Sie dann auf **Parameter aktualisieren**.
6. Klicken Sie auf den zugehörigen Link **Starten**, um mit dem Sammeln von Events für vCenter zu beginnen.
   - Um zu bestätigen, dass die Instanz Events empfängt, stellen Sie sicher, dass im Feld **Status** der Wert **Gestartet** angezeigt wird.
   - Klicken Sie auf **Stoppen**, um die Erfassung von Events für ein bestimmtes vCenter zu beenden.
   - Klicken Sie auf **Neu starten**, um die Sammlung von Events neu zu starten.

   vCenter-Events werden in Tabelle *sn_cmp_cloud_event* ausgefüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

- Wenn das vCenter Events im Event-Manager aufweist und dieselben Events konfiguriert sind, erfasst Cloud Provisioning and Governance die Events und ergreift entsprechende Maßnahmen für die CIs.
- Die Engine für Identifizierung und Abgleich (Identification and Reconciliation Engine, IRE) ändert den CI-Status basierend auf der empfangenen Eventnutzlast, und die IRE kann nicht angepasst werden.

Cloud-Discovery Berichterstellung

Cloud-Discovery Die Berichterstellung bietet eine anwenderfreundliche Oberfläche zum Navigieren und Analysieren Ihres Cloud-Ressourcenbestands. Sie bietet Optionen wie Drilldown- und Segment-and-Dice-Ansichten, um granulare Einblicke in Ihre Cloud-Ressourcenbestände mit Details aus der Discovery zu erhalten. Es bietet eine einfache Möglichkeit, den Status und den Standort Ihrer Cloud-Ressourcen schnell zu ermitteln und zu identifizieren, wodurch Ihre Verwaltungsaufgaben optimiert werden.

Erfahren Sie mehr über die Berichterstellung für Cloud-Discovery :

- Analytics und Berichte für Cloud Resources
- Dashboard Cloud-Ressourcen
- Cloud-Ressourcenbestand

Hinweis: Um bessere Ergebnisse zu erzielen, verwenden Sie den Cloud-Ressourcen-Explorer anstelle der Platform Analytics-Lösungen, die im Cloud-Ressourcen-Dashboard angezeigt werden.

Analytics und Berichte für Cloud Resources

Platform Analytics and Reporting-Lösungen enthalten vorverpackte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen Now Platform-Produkten.

Übersicht über das Performance Analytics-Inhaltspaket für Cloud-Ressourcen

Das Performance Analytics Content Pack for Cloud Resources zeigt die zusammengefasste Ansicht all Ihrer Cloud-Ressourcen an. Sie können nach bestimmten Informationen filtern, um weitere Details anzuzeigen. Es gibt auch Analytics-Tabellen und -Ansichten, in denen Tags mit Ressourcen verknüpft werden, sodass Sie eigene benutzerdefinierte Dashboards und Berichte erstellen können.

Das Performance Analytics Content Pack for Cloud Resources funktioniert mit Discovery und Cloud Provisioning and Governance und bietet Unterstützung für die folgenden Cloud-Provider:

- Amazon Web Services
- Microsoft Azure Public Clouds
- VMware vCenter
- Google Cloud Platform (GCP) (Unterstützt mit Performance Analytics Content Pack for Cloud Resources, Version 1.2.1 und höher).

Die Gesamtanzahl der einzelnen Cloud-Ressourcen und die neuesten Cloud-Discovery-Fehlerprotokolle werden im Dashboard angezeigt. Sie können die Cloud-Ressourcen nach Servicekonten, Rechenzentren oder Ressourcengruppen (nur für Microsoft Azure) unter einem bestimmten Anbieter filtern und die Ressourcenanzahl sowie die Ressourcen entsprechend anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Performance Analytics Content Pack for Cloud Resources-Dashboard des Basissystems enthält kein Widget für die GCP-Ressourcen. Sie können die Berichte und Widgets erstellen, indem Sie Daten aus den entsprechenden Tabellen verwenden. Weitere Informationen zu den Tabellen, die die GCP-Ressourcendaten enthalten, finden Sie unter Dashboard Cloud-Ressourcen. Alternativ dazu können Sie die Anwendung Arbeitsbereich für Cloud-Vorgänge installieren, um die GCP-Berichte und -Widgets anzuzeigen. Weitere Informationen finden Sie unter Arbeitsbereich für Cloud-Vorgänge.

Für jeden Cloud-Anbieter wird alle 30 Minuten eine separate regelmäßige Aufgabe ausgelöst. Die aktuellen CI-Daten werden in den Analytics-Tabellen für Cloud-Ressourcen aktualisiert, damit das Dashboard realistischer ist und die aktualisierte Anzahl ausweist. Die Informationen zu den einzelnen regelmäßigen Aufgaben sind in der Tabelle für den Cloud-Dashboard-Aufgabenstatus [sn_disco_cd_cloud_dashboard_job_status] verfügbar. In dieser Tabelle werden die Aufgabendetails einschließlich Anbietertyp, Status, Startzeit, Endzeit und Dauer gespeichert.

Die Berichte für die Cloud-Dashboard-Widgets werden aus den Analytics-Tabellen für Cloud-Ressourcen generiert. Die Analytics-Tabellen werden durch die regelmäßige Aufgabe gefüllt. Die regelmäßige Aufgabe fragt die neuen Datenbankansichten ab. Anschließend werden die Datensätze in die Analytics-Tabellen eingefügt und aktualisiert.

Die maximale Ausführungsdauer der regelmäßigen Aufgabe beträgt 360 Minuten. die maximale Zeitüberschreitung für Aufgaben wird mithilfe der Systemeigenschaft (sn_disco_cd.scheduled_job_time_out_in_mins) festgelegt. Wenn die regelmäßige Aufgabe 360 Minuten oder die in dieser Eigenschaft festgelegte Dauer überschreitet, wird sie abgebrochen.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- Now Platform-Administrator (admin): Installiert und aktiviert diese Analytics- und Reporting-Lösung und kann alle erforderlichen Änderungen an den Systemeigenschaften vornehmen
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datensammlung ein und startet diese. Gibt die Dashboards für die entsprechenden Stakeholder frei
- Cloud-Dashboard-Benutzer (sn_disco_cd.user): Stellt die Cloud-Ressourcen-Widgets im Cloud-Dashboard zusammen und verfügt über Lesezugriff auf die Analytics-Tabellen für Cloud-Ressourcen und die Dashboard-Berichte
- Cloud-Dashboard-Administrator (sn_disco_cd.admin): Kann Dashboard-Widgets und -Berichte anzeigen, hinzufügen oder bearbeiten und verfügt über Lesezugriff auf die Analytics-Tabellen für Cloud-Ressourcen. Standardmäßig enthält (sn_disco_cd.admin) die Rolle (sn_disco_cd.user), und (discovery_admin) enthält die Rolle (sn_disco_cd.admin).

Zugehörige Informationen

Analytics- und Reporting-Lösungen

Analytics und Berichte für Cloud Resources aktivieren

Aktivieren Sie das Performance Analytics Content Pack für die ServiceNow Store-Anwendung Cloud Resources für die Analytics- und Reporting-Lösung.

Vorbereitungen

Vergewissern Sie sich, dass das Plugin „Cloud Provisioning and Governance“ (com.snc.cloud.core) installiert und aktiviert ist und dass Sie auf Release Orlando oder höher aktualisiert haben. Cloud Provisioning and Governance Core ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sowohl mit Discovery als auch mit dem Plugin „Cloud Provisioning and Governance Core“ verfügbar.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

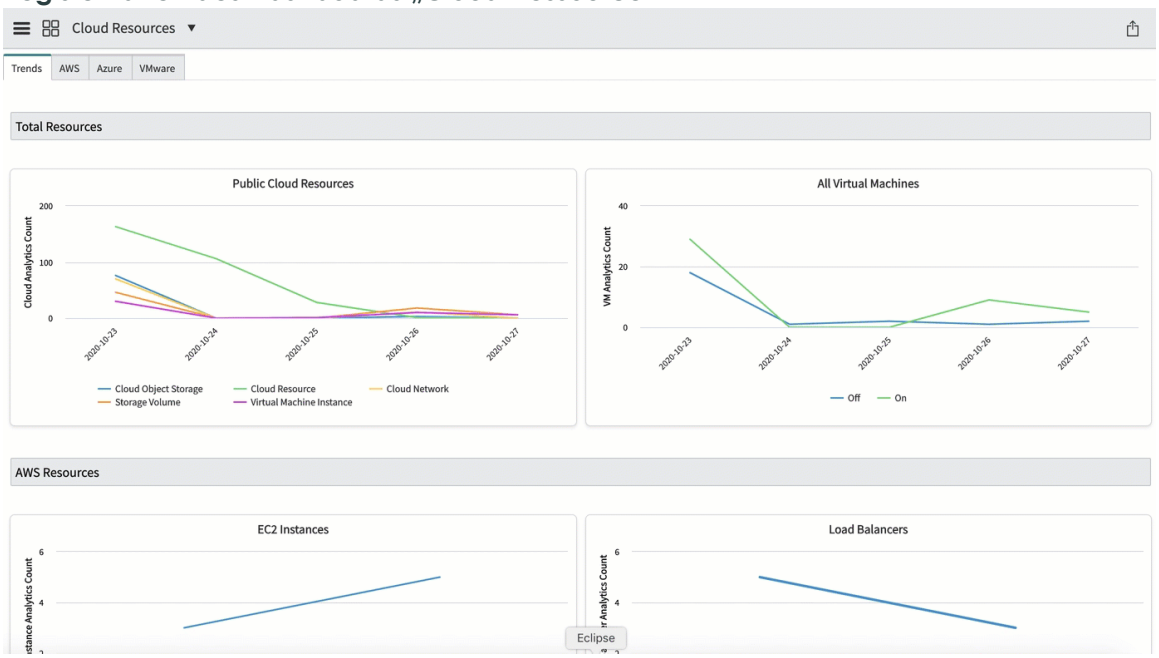
1. Navigieren zu **Systemanwendungen** > **Alle Anwendungen** > **ServiceNow Store**.
2. Suchen Sie nach Performance Analytics Content Pack for Cloud Resources, und vergewissern Sie sich, dass Sie über die erforderlichen gültigen Berechtigungen verfügen.

   Sie benötigen ein HI-Konto und die Berechtigung zum Anfordern von Anwendungen für die betreffenden Instanzen. HI-Konto und Instanz müssen zum selben Unternehmen gehören. Weitere Informationen finden Sie unter Install a ServiceNow Product (ServiceNow-Produkte installieren) im ServiceNow Store.
3. Installieren Sie die Anwendung `Performance Analytics Content Pack for Cloud Resources`.

Dashboard Cloud-Ressourcen

Im Dashboard „Cloud-Ressourcen“ werden neben der zusammengefassten Ansicht all Ihrer Cloud-Ressourcen kombinierte Analyseansichten, eine visuelle Zusammenfassung und Details aller Cloud-Ressourcen angezeigt.

Registerkarten des Dashboards „Cloud-Ressourcen“



Anwendungsfälle

Die Anwendungsfälle bieten Beispiele dafür, wie Benutzer in Ihrem Unternehmen dieses Dashboard verwenden könnten.

Anwender	Dashboard-Verwendung
Cloud-Benutzer	Discovery-Kunden haben mit Cloud-Discovery eine enorme Anzahl von CIs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender	Dashboard-Verwendung
	erkannt, die an einem zentralen Ort angezeigt werden können.
Cloud-Benutzer mit der Rolle sn_disco_cd.admin	Verwenden Sie die verfügbaren Analytics-Tabellen, um benutzerdefinierte Dashboards zu erstellen. Diese Tabellen sind spezifische Baseline-Datenbankansichten mit Ressourcen-Tags. Weitere Informationen finden Sie unter Dashboard „Cloud-Ressourcen“ anpassen.

Datenvisualisierungen

Titel	Typ	Quelltabelle
Cloud-Netzwerke	Liniendiagramm	VMware-Netzwerk-Analytics [sn_disco_cd_vmware_network_analytics]
Cloud-Netzwerke	Einzelne Punktzahl	VMware-Netzwerk-Analytics [sn_disco_cd_vmware_network_analytics]
Public Cloud-Ressourcen	Liniendiagramm	Cloud-Analytics [sn_disco_cd_analytics]
Cluster	Einzelne Punktzahl	Analytics für VMware-Cluster [sn_disco_cd_vmware_cluster_analytics]
Cluster	Liniendiagramm	Analytics für VMware-Cluster [sn_disco_cd_vmware_cluster_analytics]
Compute-Sicherheitsgruppen	Einzelne Punktzahl	Analytics für AWS-Sicherheitsgruppen [sn_disco_cd_aws_sec_group_analytics]
Datenbanken	Einzelne Punktzahl	Azure-Datenbank-Analytics [sn_disco_cd_azure_database_analytics]
Datenbanken	Liniendiagramm	Azure-Datenbank-Analytics [sn_disco_cd_azure_database_analytics]
Datenspeicher-Datenträger	Einzelne Punktzahl	Analytics für VMware-Datenspeicher-Datenträger [sn_disco_cd_vmware_ds_disk_analytics]
Datenspeicher	Einzelne Punktzahl	Analytics für VMware-Datenspeicher [sn_disco_cd_vmware_datastore_analytics]
Datenträger	Liniendiagramm	Analytics für Azure-Datenträger [sn_disco_cd_azure_disk_analytics]
Datenträger	Einzelne Punktzahl	Analytics für Azure-Datenträger [sn_disco_cd_azure_disk_analytics]
Verteilte virtuelle Portpruppen	Einzelne Punktzahl	Analytics für verteilte virtuelle VMware-Portgruppen [sn_disco_cd_vmware_dv_port_grp_analytics]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle
Verteilte virtuelle Switches	Einzelne Punktzahl	Analytics für verteilte virtuelle VMware-Switches [sn_disco_cd_vmware_dvs_analytics]
EC2-Instanzen	Einzelne Punktzahl	Analytics für AWS EC2-Instanzen [sn_disco_cd_aws_ec2_instance_analytics]
EC2-Instanzen	Liniendiagramm	Analytics für AWS EC2-Instanzen [sn_disco_cd_aws_ec2_instance_analytics]
EC2-Instanzen	Tortendiagramm	Analytics für AWS EC2-Instanzen [sn_disco_cd_aws_ec2_instance_analytics]
ESX-Server	Einzelne Punktzahl	ESX-Server-Analytics [sn_disco_cd_vmware_esx_analytics]
ESX-Server	Liniendiagramm	ESX-Server-Analytics [sn_disco_cd_vmware_esx_analytics]
Ordner	Einzelne Punktzahl	Analytics für vCenter-Ordner [sn_disco_cd_vmware_folder_analytics]
Funktionen	Einzelne Punktzahl	Analytics für Azure-Funktionen [sn_disco_cd_azure_function_analytics]
Generische Cloud-Ressourcen	Einzelne Punktzahl	Analytics für generische AWS-Cloud-Ressourcen [sn_disco_cd_aws_gen_resource_analytics]
Generische Cloud-Ressourcen	Liniendiagramm	Analytics für generische AWS-Cloud-Ressourcen [sn_disco_cd_aws_gen_resource_analytics]
Generische Cloud-Ressourcen	Einzelne Punktzahl	Analytics für generische Azure-Cloud-Ressourcen [sn_disco_cd_azure_gen_resource_analytics]
Bilder	Einzelne Punktzahl	Analytics für AWS-Images [sn_disco_cd_aws_image_analytics]
Bilder	Einzelne Punktzahl	Analytics für Azure-Images [sn_disco_cd_azure_image_analytics]
Lambdas	Einzelne Punktzahl	Analytics für AWS Lamda [sn_disco_cd_aws_lambda_analytics]
Lastenausgleichsmodule	Liniendiagramm	Analytics für AWS-Lastenausgleichsmodule [sn_disco_cd_aws_loadbalancer_analytics]
Lastenausgleichsmodule	Einzelne Punktzahl	Analytics für AWS-Lastenausgleichsmodule [sn_disco_cd_aws_loadbalancer_analytics]
Lastenausgleichsmodule	Einzelne Punktzahl	Analytics für Azure-Lastenausgleichsmodule [sn_disco_cd_azure_loadbalancer_analytics]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle
Lastenausgleichsmodule	Liniendiagramm	Analytics für Azure-Lastenausgleichsmodule [sn_disco_cd_azure_loadbalancer_analytics]
Netzwerkschnittstellen	Einzelne Punktzahl	Analytics für AWS-Netzwerkschnittstellen [sn_disco_cd_aws_nw_interface_analytics]
Netzwerkschnittstellen	Einzelne Punktzahl	Analytics für Azure-Netzwerkschnittstellen [sn_disco_cd_azure_nw_interface_analytics]
Netzwerksicherheitsgruppen	Einzelne Punktzahl	Analytics für Azure-Netzwerksicherheitsgruppen [sn_disco_cd_azure_nw_sec_group_analytics]
Relational Database Services (RDS)	Liniendiagramm	AWS RDS-Analytics [sn_disco_cd_aws_rds_analytics]
Relational Database Services (RDS)	Einzelne Punktzahl	AWS RDS-Analytics [sn_disco_cd_aws_rds_analytics]
S3-Buckets	Einzelne Punktzahl	Analytics für AWS S3-Buckets [sn_disco_cd_aws_s3_bucket_analytics]
Speicher-Laufwerke	Einzelne Punktzahl	Analytics für AWS-Speichervolumes [sn_disco_cd_aws_storage_volume_analytics]
Speicher-Laufwerke	Liniendiagramm	Analytics für AWS-Speichervolumes [sn_disco_cd_aws_storage_volume_analytics]
Virtuelle Maschinen	Liniendiagramm	Azure-VM-Analytics [sn_disco_cd_azure_vm_analytics]
Virtuelle Maschinen	Einzelne Punktzahl	Azure-VM-Analytics [sn_disco_cd_azure_vm_analytics]
Virtuelle Maschinen	Tortendiagramm	Azure-VM-Analytics [sn_disco_cd_azure_vm_analytics]
Virtuelle Maschinen	Liniendiagramm	VMware-VM-Analytics [sn_disco_cd_vmware_vm_analytics]
Virtuelle Maschinen	Tortendiagramm	VMware-VM-Analytics [sn_disco_cd_vmware_vm_analytics]
Virtuelle Maschinen	Einzelne Punktzahl	VMware-VM-Analytics [sn_disco_cd_vmware_vm_analytics]
Alle virtuellen Computer	Liniendiagramm	VM-Analytics [sn_disco_cd_vm_analytics]
Virtuelle Netzwerke	Einzelne Punktzahl	Analytics für virtuelle Azure-Netzwerke [sn_disco_cd_azure_virtual_nw_analytics]
Virtual Private Clouds (VPC)	Liniendiagramm	AWS-VPC-Analytics [sn_disco_cd_aws_vpc_analytics]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle
Virtual Private Clouds (VPC)	Einzelne Punktzahl	AWS-VPC-Analytics [sn_disco_cd_aws_vpc_analytics]
VM-Vorlagen	Einzelne Punktzahl	Analytics für VMware-VM-Vorlagen [sn_disco_cd_vmware_vm_template_analytic

Dashboard „Cloud-Ressourcen“ aufrufen

Um auf das Dashboard „Cloud-Ressourcen“ zuzugreifen, navigieren Sie zu **Discovery** > **Cloud-Ressourcen-Dashboard** oder **Cloud Provisioning and Governance** > **Cloud-Ressourcen-Dashboard**.

Dashboard „Cloud-Ressourcen“ anpassen

Passen Sie das Dashboard auf jeder Cloud-Anbieter-Registerkarte an, indem Sie nach folgenden Attributen filtern:

- Servicekonto: Es werden alle Servicekonten aufgelistet, die für die ausgewählte Cloud-Anbieter-Registerkarte spezifisch sind.
- Rechenzentren: Die Rechenzentren werden basierend auf dem Cloud-Anbieter gefüllt.
- Ressourcengruppe: Mit diesem nur für Microsoft Azure gültigen Filter werden Objekte und Ressourcen auf die ausgewählte Ressourcengruppe beschränkt.

Verwenden Sie diese Datenbankansichten mit Ressourcen-Tags, um Ihr eigenes Dashboard zu erstellen.

AWS-Datenbankansichten mit Ressourcen-Tags

Name der Datenbank-Ansichtstabelle	Bezeichnung
sn_disco_cd_aws_api_gateway_analytics_tags_db_view	Analytics für AWS API-Gateways mit Tags
sn_disco_cd_aws_ec2_instance_analytics_tags_db_view	Analytics für AWS EC2-Instanzen mit Tags
sn_disco_cd_aws_gen_resource_analytics_tags_db_view	Analytics für AWS Cloud-Ressourcen mit Tags
sn_disco_cd_aws_image_analytics_tags_db_view	Analytics für AWS-Images mit Tags
sn_disco_cd_aws_lambda_analytics_tags_db_view	AWS Lamda-Analytics mit Tags
sn_disco_cd_aws_loadbalancer_analytics_tags_db_view	Analytics für AWS-Lastenausgleichsmodule mit Tags
sn_disco_cd_aws_nw_interface_analytics_tags_db_view	Analytics für AWS NW-Schnittstellen mit Tags
sn_disco_cd_aws_rds_analytics_tags_db_view	AWS RDS-Analytics mit Tags
sn_disco_cd_aws_s3_bucket_analytics_tags_db_view	Analytics für AWS S3-Bucket mit Tags

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Datenbankansichten mit Ressourcen-Tags (Fortsetzung)

Name der Datenbank-Ansichtstabelle	Bezeichnung
sn_disco_cd_aws_sec_group_analytics_tags_db_view	Analytics für AWS-Sicherheitsgruppen mit Tags
sn_disco_cd_aws_storage_volume_analytics_tags_db_view	Analytics für AWS-Speichervolumes mit Tags
sn_disco_cd_aws_vpc_analytics_tags_db_view	AWS VPC-Analytics mit Tags
sn_disco_cd_aws_zone_analytics_tags_db_view	Analytics für AWS-Zonen mit Tags

Microsoft Azure-Datenbankansichten mit Ressourcen-Tags

Name der Datenbank-Ansichtstabelle	Bezeichnung
sn_disco_cd_azure_database_analytics_tags_db_view	Analytics für Azure-Datenbanken mit Tags
sn_disco_cd_azure_disk_analytics_tags_db_view	Analytics für Azure-Datenträger mit Tags
sn_disco_cd_azure_function_analytics_tags_db_view	Analytics für Azure-Funktionen mit Tags
sn_disco_cd_azure_gen_resource_analytics_tags_db_view	Analytics für Azure-Cloud-Ressourcen mit Tags
sn_disco_cd_azure_image_analytics_tags_db_view	Analytics für Azure-Images mit Tags
sn_disco_cd_azure_loadbalancer_analytics_tags_db_view	Analytics für Azure-Lastenausgleichsmodule mit Tags
sn_disco_cd_azure_nw_interface_analytics_tags_db_view	Analytics für Azure NW-Schnittstellen mit Tags
sn_disco_cd_azure_nw_sec_group_analytics_tags_db_view	Analytics für Azure-Sicherheitsgruppen mit Tags
sn_disco_cd_azure_virtual_nw_analytics_tags_db_view	Analytics für Azure Virtual NW mit Tags
sn_disco_cd_azure_vm_analytics_tags_db_view	Analytics für Azure-VMs mit Tags
sn_disco_cd_azure_zone_analytics_tags_db_view	Analytics für Azure-Zonen mit Tags

VMware-Datenbankansichten mit Ressourcen-Tags

Name der Datenbank-Ansichtstabelle	Bezeichnung
sn_disco_cd_vmware_cluster_analytics_tags_db_view	Analytics für VMware-Cluster mit Tags
sn_disco_cd_vmware_datastore_analytics_tags_db_view	Analytics für VMware-Datenspeicher mit Tags

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VMware-Datenbankansichten mit Ressourcen-Tags (Fortsetzung)

Name der Datenbank-Ansichtstabelle	Bezeichnung
sn_disco_cd_vmware_ds_disk_analytics_tags_db_view	Analytics für VMware-Datenspeicher-Datenträger mit Tags
sn_disco_cd_vmware_dvs_analytics_tags_db_view	Analytics für VMware DVS mit Tags
sn_disco_cd_vmware_dv_port_grp_analytics_tags_db_view	Analytics für VMware DV-Portgruppen mit Tags
sn_disco_cd_vmware_esx_analytics_tags_db_view	VMware ESX-Analytics mit Tags
sn_disco_cd_vmware_folder_analytics_tags_db_view	Analytics für VMware-Ordner mit Tags
sn_disco_cd_vmware_network_analytics_tags_db_view	Analytics für VMware-Netzwerke mit Tags
sn_disco_cd_vmware_vm_analytics_tags_db_view	Analytics für VMware-VMs mit Tags
sn_disco_cd_vmware_vm_template_analytics_tags_db_view	Analytics für VMware-VM-Vorlagen mit Tags

Die folgenden Ressourcen, die für GCP unterstützt werden, werden von GCPResourcePopulateScheduledJob gefüllt.

Google Cloud Platform (GCP)-Analytics-Tabellen und ihre entsprechenden CI-Ressourcentabellen (Configuration Item) in der Configuration Management Database (CMDB)

Analytics-Tabelle	CMDB-CI-Ressourcen
Analytics für GCP-VMs [sn_disco_cd_gcp_database_analytics]	VM-Instanz [cmdb_ci_vm_instance]
Analytics für GCP-Speichervolumes [sn_disco_cd_gcp_storage_volume_analytics]	Speichervolume [cmdb_ci_storage_volume]
Analytics für GCP-Datenbanken [sn_disco_cd_gcp_database_analytics]	Cloud-Datenbank [cmdb_ci_cloud_database]
Analytics für virtuelle GCP-Netzwerke [sn_disco_cd_gcp_virtual_nw_analytics]	Cloud-Netzwerk [cmdb_ci_network]
Analytics für GCP-Lastenausgleichsmodule [sn_disco_cd_gcp_loadbalancer_analytics]	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Analytics für GCP-Images [sn_disco_cd_gcp_image_analytics]	Cloud-Betriebssystem-Images [cmdb_ci_cloud_os_images]
Analytics für generische GCP-Cloud-Ressourcen [sn_disco_cd_gcp_gen_resource_analytics]	Cloud-Ressource [cmdb_ci_cmp_resource]
Analytics für GCP-Netzwerkschnittstellen [sn_disco_cd_gcp_nw_interface_analytics]	Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgaben

Regelmäßige Aufgaben installiert

Auftrag	Beschreibung
GCPResourcePopulateScheduledJob	Regelmäßige Aufgabe, mit der die GCP-CI-Daten in der Analytics-Tabelle abgerufen und gefüllt werden.
AWSResourcePopulateScheduledJob	Regelmäßige Aufgabe, mit der die AWS-CI-Daten in der Analytics-Tabelle abgerufen und gefüllt werden.
AzureResourcePopulateScheduledJob	Regelmäßige Aufgabe, mit der die Microsoft Azure-CI-Daten in der Analytics-Tabelle abgerufen und gefüllt werden.
VMwareResourcePopulateScheduledJob	Regelmäßige Aufgabe, mit der die VMware-CI-Daten in der Analytics-Tabelle abgerufen und gefüllt werden.

Da für jeden Cloud-Provider alle 30 Minuten eine separate regelmäßige Aufgabe ausgelöst wird, können Sie überprüfen, ob die letzte Aufgabe erfolgreich war. Wenn die geplante Aufgabe nicht erfolgreich ist, können Sie sie manuell auslösen, indem Sie zu wechseln **Systemdefinition** > **Geplante Aufgaben**. Wählen Sie die Aufgabe für den betreffenden Cloud-Anbieter aus, und klicken Sie auf **Jetzt ausführen**.

Im Rahmen der alle 30 Minuten stattfindenden Aktualisierungsaufgaben werden Analytics-Tabellen mit Daten gefüllt, und das Datum wird aktualisiert. Sie können diese Häufigkeit steigern, um häufiger aktualisierte Daten zu erhalten.

In folgenden Fällen ist eine Synchronisierung erforderlich:

- Der Ressourcenstatus wurde von **Installiert** auf einen anderen Status (z. B. „Deaktiviert“ oder „Abgebrochen“) aktualisiert.
- Vor Kurzem wurden neue Ressourcen erkannt.

In folgenden Fällen ist keine Synchronisierung erforderlich:

- Es wurden keine Ressourcen aktualisiert.
- Es sind neue Ressourcen vorhanden, die noch nicht erkannt wurden.

Wichtiger Hinweis:

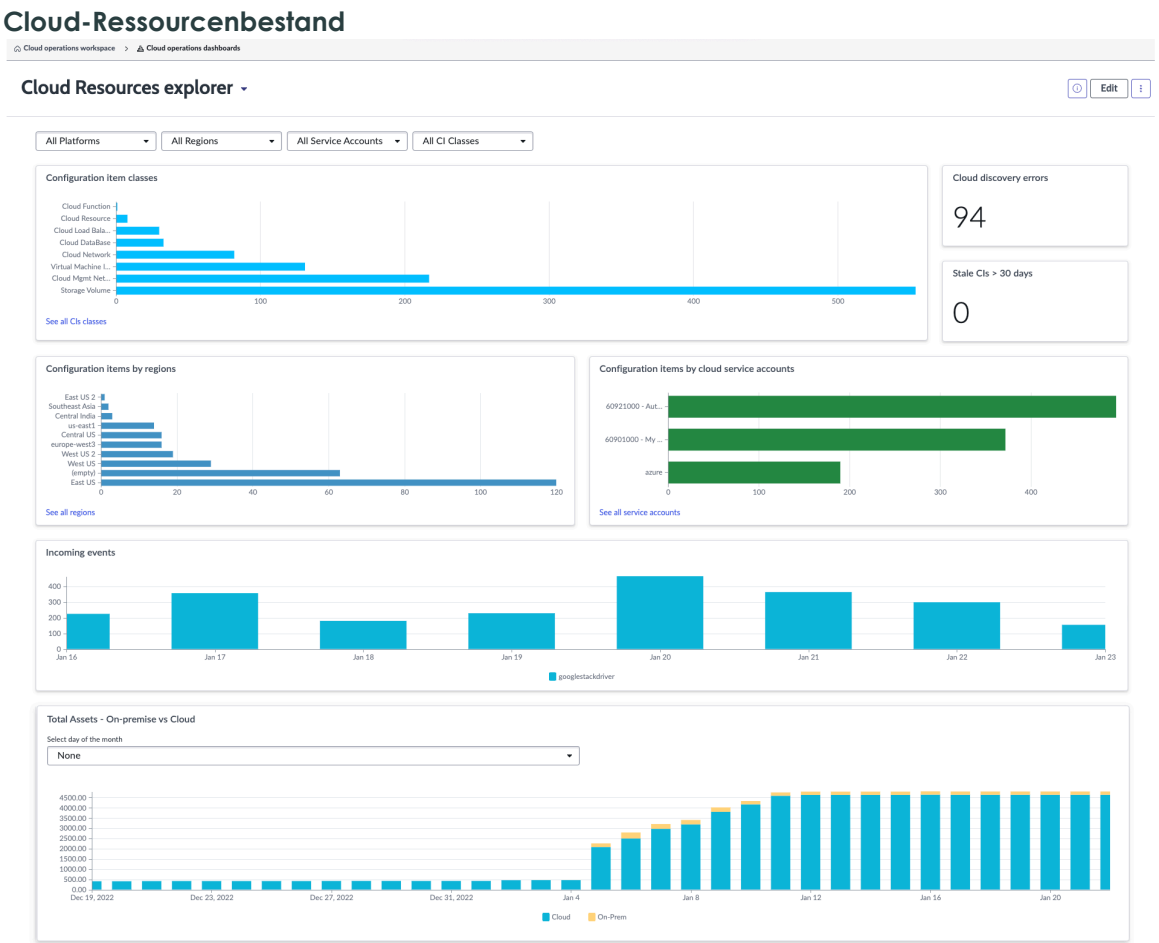
- Es kann jeweils nur eine Aufgabe ausgeführt werden. Wenn beispielsweise bei der Aufgabenausführung bereits eine AWS-Aufgabe ausgeführt wird, können Sie keine weitere AWS-Aufgabe auslösen.
- Wenn die Felder „LRZ“ (logisches Rechenzentrum) und „Servicekonto“ einer CI-Ressource leer sind, kann die Ressource in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] keinem LRZ zugeordnet werden, oder die Ressource ist eine generische Cloud-Ressource vom Typ IAM, und die Felder sind leer.
- Nur die Ressourcen, deren Installationsstatus auf „Installiert“ festgelegt ist, werden gezählt und in den Widgets des Dashboards „Cloudressourcen“ dargestellt.
- Wenn nach Ausführung der regelmäßigen Aufgabe eine neue Ressource erkannt wird, werden von der nächsten regelmäßigen Aufgabe die Ressourcendetails in den Analytics-Tabellen hinzugefügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn eine Aufgabe in der Tabelle „Cloud-Dashboard-Aufgabenstatus“ [sn_disco_cd_cloud_dashboard_job_status] als fehlgeschlagen markiert wird, ist der Grund des Fehlers in den Systemprotokollen verzeichnet. Filtern Sie die Systemprotokolltabelle nach der sys_id der Aufgabe, um die Fehlermeldung abzurufen.
- Wenn IP-basierte Discovery zur vCenter-Erkennung verwendet wird, bleibt das Feld „Servicekonto“ der VMware-Ressource leer.
- Systemadministrator dürfen die Datensätze nicht aus der Analytics-Tabelle löschen, da Datensätze, die aus der Analytics-Tabelle gelöscht wurden, von der regelmäßigen Aufgabe nicht erneut gefüllt werden. Das Löschen von Datensätzen führt zu Dateninkonsistenzen in der Analytics-Tabelle.
- Um eine vollständige Aktualisierung der VMware-Datensätze (einschließlich der Servicekonten) nach Änderung des Mechanismus zur Erkennung von VMware-Ressourcen sicherzustellen, löschen Sie die VMware-Datensätze aus der Tabelle „Cloud-Dashboard-Auftragsstatus“ [sn_disco_cd_cloud_dashboard_job_status], und führen Sie die regelmäßige Aufgabe aus. In der Tabelle „Cloud-Dashboard-Auftragsstatus“ ist das Provider-Feld aller VMware-Ressourcen auf *vmware* festgelegt. Sie können entweder die IP-basierte vCenter-Erkennung oder die vCenter-Servicekonto-Erkennung verwenden, um die VMware-Ressourcen zu erkennen.

Cloud-Ressourcenbestand

Verwenden Sie ServiceNow® Cloud-Ressourcenbestand, um die Verteilung der Ressourcen in Ihrer Multi-Cloud-Umgebung zu filtern und zu visualisieren. Erhalten Sie Einblicke in Betriebsinformationen wie veraltete Ressourcen und Zuflussraten von Cloud-Ereignissen.



Der Cloud-Ressourcenbestand bietet Unterstützung für folgende Cloud-Anbieter:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Amazon Web Services.
- Microsoft Azure Public Clouds.
- VMware vCenter.
- Google Cloud Platform (GCP) (Unterstützt mit Performance Analytics Content Pack for Cloud Resources, Version 1.2.1 und höher).

Erforderliche Now Platform-Rollen

Zum Anzeigen von Cloud-Ressourcenbestandist die Rolle sn_cloud_ops_ws.cloud_ops_admin erforderlich.

Auf Cloud-Ressourcenbestand zugreifen

Um Cloud-Ressourcenbestandzu öffnen, navigieren Sie zu **Alle** > **Cloud-Discovery-Arbeitsbereich** > **Cloud-Ressourcen-Explorer**.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
sn_cloud_ops_ws.cloud_ops_admin	• Erhalten Sie Einblicke in die Anzahl der Bestände von Cloud-Ressourcen und die aktuelle Größe der Configuration Management Database (CMDB) und darüber, wie viele Objekte sich im Geltungsbereich befinden. • Erhalten Sie Einblicke in fehlerbezogene Informationen wie Cloud-Discovery-Fehler. • Erhalten Sie Einblicke in Betriebsinformationen wie die Zufluss- und die Verarbeitungsrate des Ereignisses. • Erhalten Sie Einblicke in die Integrität der CMDB. • Erhalten Sie Einblicke in die Verteilung von Ressourcen in der lokalen Cloud und in Public Clouds.

Indikatoren

Cloud-Discovery-Fehler

Cloud-Discovery-Fehler insgesamt, die im Laufe der Zeit aufgetreten sind.

Veraltete CIs > 30 Tage

Wenn ein CI in den letzten 30 Tagen nicht aktualisiert wurde, gilt es als veraltetes CI.

Ein veraltetes CI gibt an, dass das CI in der Configuration Management Database (CMDB), aber möglicherweise nicht im Rechenzentrum vorhanden

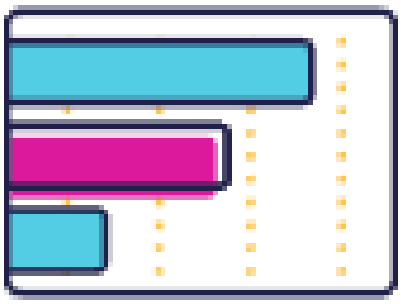
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ist. Das Identifizieren der veralteten CIs ist wichtig für die Aufrechterhaltung der Integrität der CMDB.

Hier sind einige der Szenarien aufgeführt, die dazu führen, dass veraltete CIs entstehen:

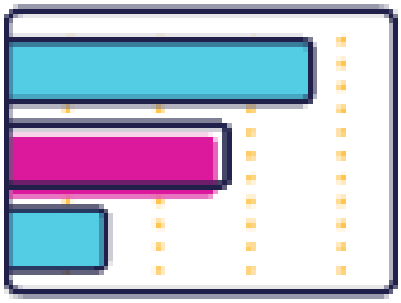
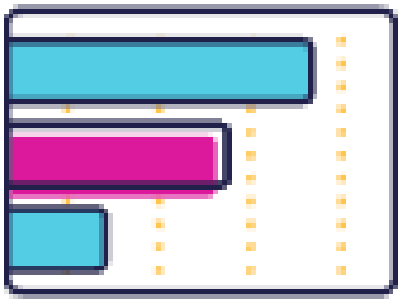
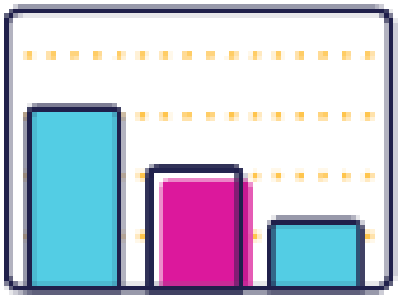
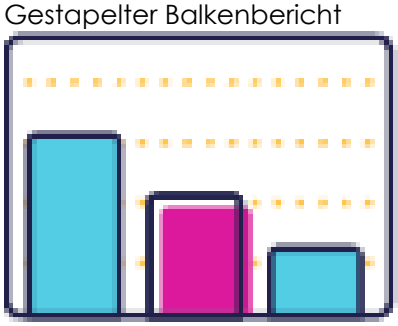
- Die Cloud-Ressource ist nicht vorhanden, ihre Löschung wird jedoch nicht in der CMDB aktualisiert.
- Das Gerät befindet sich möglicherweise noch im Netzwerk, aber im Rahmen der automatisierten Erkennung kann keine Verbindung zum Gerät hergestellt werden, damit es erneut erkannt werden kann.
- Das Gerät ist im Netzwerk vorhanden, und es kann darauf zugegriffen werden, aber es wird im Identifizierungsprozess nicht eindeutig erkannt. Daher wurde von Cloud-Discovery ein doppeltes CI in der CMDB erstellt.

Datenvisualisierungen

Titel	Typ	Quelltabelle
Konfigurationselementsklassen	Bericht mit horizontalen Balken 	Cloud-Analytics [sn_disco_cd_analytics]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle
Konfigurationselemente nach Regionen	Bericht mit horizontalen Balken 	Cloud-Analytics [sn_disco_cd_analytics]
Konfigurationselemente nach Cloud-Servicekonten	Bericht mit horizontalen Balken 	Cloud-Analytics [sn_disco_cd_analytics]
Eingehende Events	Balkenbericht 	Cloud-Ereignis [sn_cmp_cloud_event]
Lokale Cloud-Ressourcen im Vergleich zu öffentlichen Cloud-Ressourcen insgesamt	Gestapelter Balkenbericht 	Tägliche Ressourcenanzahl nach Anbietern [sn_disco_cd_daily_resource_cnt_by_provid

Automatische Übersetzung

Zum Füllen der Tabelle „Cloud Analytics“ [sn_disco_cd_analytics] verwendet Cloud-Ressourcenbestand denselben Satz geplanter Aufgaben wie das Inhaltspaket für Cloud-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen Performance Analytics. Weitere Informationen zu den geplanten Aufgaben finden Sie unter Dashboard für Cloud-Ressourcen.

Zum Anzeigen der Details der Betriebssystem-Images, die in den AWS-, Microsoft Azure- und GCP-Clouds erkannt werden, muss die Store-App Discovery and Service-Mapping Patterns, Version 1.0.87 oder höher, in der Instanz installiert sein. Außerdem muss die Eigenschaft *sn_cmdb_ci_class.use_single_cloud_os_image* auf `true` festgelegt werden.

Filter

Name	Typ	Beschreibung
Cloud-Ressourcenfilter	Auswahlbasierter Filter	Verwenden Sie den Cloud-Ressourcenfilter, um die gewünschten Cloud-Ressourcendaten auszuwählen und zu visualisieren. Standardmäßig werden im Cloud-Ressourcenbestand Daten für alle Cloud-Ressourcen der Cloud-Anbieter Ihrer Organisation angezeigt. Allerdings werden im Cloud-Ressourcenfilter nur die Cloud-Anbieter angezeigt, die Sie auf der Auswahlseite für Cloud-Anbieter der App Arbeitsbereich für Cloud-Vorgänge ausgewählt haben. Sie haben die Wahl zwischen den folgenden überlappenden Filtern: • Plattform: Wählen Sie den Cloud-Anbieter mit den Ressourcendaten aus, die Sie visualisieren möchten. • Region: Wählen Sie die Region oder das Rechenzentrum mit den Ressourcendaten aus, die Sie visualisieren möchten. • Service-Account: Wählen Sie den Serviceaccount mit den Ressourcendaten aus, die Sie visualisieren möchten. • CI-Klasse: Wählen Sie die CI-Klasse mit den Ressourcendaten aus, die Sie visualisieren möchten. • Ressourcengruppe: Wählen Sie die Ressourcengruppe mit den Ressourcendaten aus, die Sie visualisieren möchten. Dieses Feld ist nur verfügbar, wenn in der Dropdown-Liste „Plattform“ `Azure` ausgewählt ist. Sie können den Bericht „Eingehende Ereignisse“ nur basierend auf dem Plattformfilter filtern. Die im Cloud-Discovery-Fehlerindikator angezeigten Daten sind nicht von den im Cloud-Ressourcenfilter ausgewählten Kriterien betroffen.
Tagesnavigator	Auswahlbasierter Filter	Verwenden Sie den Tagesnavigator, um den Bericht „Lokale Cloud-Ressourcen im Vergleich zu öffentlichen Cloud-Ressourcen insgesamt“ in die folgenden Dimensionen zu segmentieren:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
		• Keine: Der Bericht zeigt die im letzten Jahr gesammelten Daten an, falls verfügbar. • Erster Tag des Monats: Der Bericht zeigt die Verlaufsdaten an, die für den ersten Tag des Monats im letzten Jahr gesammelt wurden, falls verfügbar. • Mitte des Monats: Der Bericht zeigt die Verlaufsdaten an, die für die Monatsmitte des letzten Jahres gesammelt wurden, falls verfügbar. • Letzter Tag des Monats: Der Bericht zeigt die Verlaufsdaten an, die für den letzten Tag des Monats im letzten Jahr gesammelt wurden, falls verfügbar. • Datum des Monats auswählen: Der Bericht zeigt die Verlaufsdaten an, die für den ausgewählten Tag des Monats im letzten Jahr gesammelt wurden, falls verfügbar.

Container-Discovery

Container-Discovery ermöglicht IT-Abteilungen von Unternehmen, detaillierte Informationen über ihre Containerverwaltungstools in der Infrastruktur zu sammeln. Discovery sucht nach Ressourcen bei wichtigen Container-Verwaltungsservices.

Erkennung von Kubernetes

Discovery von Amazon-ECS-Ressourcen

Erkennung von Pivotal Cloud Foundry

Erkennung von Kubernetes

ServiceNow ITOM-Transparenz sucht nach den Komponenten Kubernetes und OpenShift und erstellt Anwendungsservices, die diese enthalten. Discovery sucht auch nach Ereignissen Kubernetes vom Typ und aktualisiert regelmäßig das Ereignis CMDB entsprechend der dynamischen Umgebung Kubernetes.

Discovery verwendet das Muster Kubernetes und die zugehörigen Erweiterungsabschnitte, um Kubernetes -Komponenten für Kubernetes Version 1.21 zu erkennen:

- Der Erweiterungsabschnitt *Collect OpenShift info* des Musters Kubernetes erkennt die OpenShift -Komponenten der Bereitstellung Kubernetes. Der Abschnitt zur Erweiterung OpenShift Build Config ist ab Store-Version 1.0.53 verfügbar.
- Von der *Service Mesh*-Erweiterung werden Servicenetz-Details erkannt. Diese Informationen ermöglichen es dem Muster, Service-zu-Service-Beziehungen zu erstellen, die als Verbunden zu::Verbunden angezeigt werden. Service Mesh-Discovery erfordert die Bereitstellung von Istio in Ihrem K8s-Cluster (Kubernetes). Der Abschnitt „Service Mesh-Erweiterung“ ist in den Kubernetes-Erweiterungsklassen verfügbar. Es wird auf Now Platform mit Release Madrid oder höher unterstützt.
- Von *Collect Container Repository* und Erweiterungsabschnitt wird nach Container-Registrierungen und Images in diesen Registrierungen gesucht.

Darüber hinaus verwendet Discovery das Muster Kubernetes Event, um Ereignisse für Kubernetes -Komponenten für die Versionen Kubernetes Version 1.21 zu erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab Release 1.0.68 auf ServiceNow Storekann Service-Mapping CI-Beziehungen verwenden, um die Komponenten Kubernetes während der Tag-basierten Erkennung Anwendungsservices hinzuzufügen.

Discovery verwendet die folgenden Muster, um die gesamte Kubernetes -Infrastruktur zu erkennen, die auf GCP, AWS und Azure bereitgestellt wird:

- Google Cloud Platform (GCP) – Kubernetes Clustersabrufen.
- Amazon Web Services (AWS) – Abrufen von Kubernetes Clustern.
- Microsoft Azure Cloud Computing Services – Kubernetes Clustersabrufen.

Mit diesen Mustern werden Cloud-Abfragen durchgeführt, Daten zu allen Kubernetes-Clustern gesammelt und Zeitpläne für die serverlose Erkennung für die einzelnen Cluster erstellt. Wenn der Cluster gelöscht wird, wird der Zeitplan als inaktiv markiert. Mithilfe dieser Funktion wird der Mehraufwand für die Erstellung und Verwaltung mehrerer Anmeldeinformationen und Zeitpläne für serverlose Erkennung pro Cluster eliminiert. Die Cloud-Infrastrukturmuster werden durch die standardmäßige Cloud-Erkennung ausgelöst.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Hinweis: Informationen zu den Voraussetzungen für die Discovery der Cloud-Infrastruktur Kubernetes finden Sie unten.

Hinweis: Das Ausführen automatischer serverloser Zeitpläne Kubernetes ruft das Bearer-Token ab. Das Hinzufügen von Anmeldeinformationen ist nicht erforderlich.

Führen Sie die folgenden Schritte aus, um sicherzustellen, dass Discovery das Muster verwenden kann, um Kuberneteserfolgreich zu finden.

1. Stellen Sie die aktuelle Anwendung Discovery and Service Mapping Patterns aus dem ServiceNow Store bereit.
2. Suchen Sie auf der Plattform Kubernetes nach den Parametern zum Einrichten der Discovery für Kubernetes :
   - Suchen Sie nach der URL des kubeapi-Servers:
     a. Führen Sie auf der Plattform Kubernetes den folgenden Befehl aus:

     ```
     kubectl cluster-info
     ```

     b. Suchen Sie in der Ausgabe nach der Zeile, die die URL des kubeapi-Servers angibt. Beispiel: Die Steuerungsebene Kubernetes wird um ausgeführt

     ```
     https://10.154.144.146:443
     ```

   - Suchen Sie den Namespace des Kubeapi-Servers:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Führen Sie auf der Plattform Kubernetes diesen Befehl aus:

```
kubectl get namespaces
```

b. Suchen Sie in der Ausgabe die Zeile, die die Namespaces angibt. Beispiel: `kube-system`.

◦ Suchen Sie den Anwendernamen und das Passwort Kubernetes :

a. Führen Sie auf der Plattform Kubernetes diesen Befehl aus:

```
kubectl config view
```

b. Suchen Sie in der Ausgabe den Benutzernamen und das Passwort.

> **Hinweis:** Wenn in einer bestimmten Umgebung der Befehl „`kubectl config view`“ nicht die erwarteten Details anzeigt, verwenden Sie den `unterstützten` Befehl des Administrators Kubernetes, um den Anwendernamen und die Passwortdetails abzurufen.

◦ Suchen Sie das gültige Bearer-Token mit den richtigen Berechtigungen:

a. Wenn Sie nicht über den Standard-Token-Namen verfügen, verwenden Sie den folgenden Befehl: `kubectl beschreiben geheimnis`.

b. Tie Ausgabe zeigt alle Accounts und alle Token an. Suchen Sie das gültige Token:

Wobei „`kubectl`“ für den generischen Account Kubernetes und „`describe`“ für die generische Kubectl-Methode steht.

Der Parameter „`secret`“ gibt an, dass in Ihrem Cluster Kubernetes das Standardtoken geschützt wird, indem es im Objekt vom Typ „geheimnis“ enthalten ist.

Die Ausgabe des Befehls„`kubectl-describe-secret`“ liegt im BASE64-codierten Format vor.

c. Wenn Sie den Namen des Standardtokens kennen, verwenden Sie den folgenden Befehl: `kubectl beschreiben geheimes Standard-Token-g6pwc`

`default-token-g6pwc` spiegelt den Parameterwert des Standardtokens für g6pwc wider.

d. Die Ausgabe zeigt alle vorhandenen Token für diesen Kubernetes -Account.

Wählen Sie ein Token aus, das zum Konfigurieren Kubernetes der -Anmeldeinformationen auf der Plattform ServiceNow verwendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Stellen Sie sicher, dass der API-Server vom MID-Server für eine erfolgreiche Kubernetes -Discovery erreichbar ist.
4. Stellen Sie sicher, dass der auf der Plattform Kubernetes konfigurierte Benutzer über die Berechtigungen zum Ausführen der folgenden /api/v1-Elemente verfügt:
   - https://<URL>/api/v1/namespaces/
   - https://<URL>/api/v1/namespaces/<Namespace>
   - https://<URL>/api/v1/namespaces/kube-system/endpoints/kube-controller-manager
   - https://<URL>/api/v1/services
   - https://<URL>/api/v1/pods
   - https://<URL>/api/v1/nodes
   - https://<url> /api/v1/replicationcontrollers
   - https://<url> /apis/network.k8s.io/v1/ingdresses
   - https://<url> /apis/apps/v1/deployments
   - https://<url> /apis/apps/v1/statefulsets
   - https://<url> /apis/apps/v1/daemonsets
   - https://<url> /apis/apps/v1/replicasets
   - https://<url> /apis/batch/v1/cronjobs
   - https://<url> /apis/batch/v1/jobs
5. Um die OpenShift -Komponenten der Bereitstellung Kubernetes zu erkennen, vergewissern Sie sich, dass der auf der Plattform Kubernetes konfigurierte Benutzer über die Berechtigungen zum Ausführen der folgenden /api/v1-Elemente verfügt:
   - /apis/apps.openshift.io/v1/deploymentconfigs
   - /apis/build.openshift.io/v1/buildconfigs
   - /apis/route.openshift.io/v1/routes
   - /apis/user.openshift.io/v1/groups
   - /apis/user.openshift.io/v1/users
   - /apis/project.openshift.io/v1/projects
   - /apis/image.openshift.io/v1/images
   - /apis/image.openshift.io/v1/imagestreams

   So erkennen Sie Service-Mesh-Informationen:
   - Stellen Sie Istio auf Ihrem K8s-Cluster bereit.
   - Geben Sie die Prometheus-URL an.
   - Konfigurieren Sie Prometheus, um Metriken aus Istio zu entfernen.
6. Aktivieren Sie die Erweiterung **„Kubernetes Config Files abrufen“** für:
   - Konfigurationsdateien erkennen.
   - Erstellen Sie nachverfolgte Konfigurationsdateien.
   - Ordnen Sie die Arbeitsauslastungen und Services der Konfigurationsdateien mit einer Beziehung zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Der Inhalt von nachverfolgten Dateien liegt ab Version 1.0.92 im JSON-Format vor. Der Inhalt von nachverfolgten Dateien liegt in Version 1.0.91 und früher im YAML-Format vor.

7. Erstellen Sie die Kubernetes -Anmeldeinformationen auf der Plattform ServiceNow :
   a. Navigieren Sie auf der Plattform ServiceNow zu **Alle** > **Discovery** > **Anmeldeinformationen**.
   b. Wählen Sie **Neu**.
   c. Wählen Sie **die Kubernetes-Anmeldeinformationen**aus.
   d. Füllen Sie die Formularfelder aus (siehe Tabelle):

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Benutzername	Geben Sie den zu erstellenden Benutzernamen in die Tabelle „Berechtigungsnachweise“ ein. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachgestellte Leerzeichen im Benutzernamen erkennt.
Passwort	Geben Sie das Passwort für diese Anmeldeinformationen ein.
Bearertoken	Geben Sie für die erweiterte Authentifizierung mit einem Bearer-Token das Bearer-Token ein, das Discovery für die Authentifizierung beim Zugriff auf Kubernetesverwendet. Verwenden Sie die Zeichenfolge als Token, z. B. 31ada4fd-adec-460c-809a-9e56ceb75269. **Hinweis:** Das Bearer-Token muss im BASE64-codierten Format vorliegen.
Bearertoken-Authentifizierung	Aktivieren Sie dieses Kontrollkästchen für die erweiterte Authentifizierung mit einem Bearer-Token.
Anmeldeinformationsalias	Konfigurieren Sie den Alias für die Verwendung der Anmeldeinformationen Kubernetes für andere Geräte und Anwendungen als Kubernetes. Sie verwenden diesen Alias auch zum Definieren eines serverlosen Discovery-Zeitplans zum Erkennen der Bereitstellung Kubernetes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	i. Wählen Sie das Schlosssymbol und dann das Suchsymbol. **ii.** Wählen Sie im Formular „Aliasse für Verbindungen und Anmeldeinformationen“ **Neu**. **iii.** Geben Sie einen Namen für den Aliasdatensatz für Anmeldeinformationen an. **iv.** Definieren Sie Attribute für den Alias. Legen Sie den *Type* auf `Berechtigung` fest. **v.** Klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie **Speichern**und dann **Aktualisieren**aus. **vi.** Wählen Sie im Formular „Aliasse für Verbindungen und Anmeldeinformationen“ den neu hinzugefügten Alias aus. Der Alias wird im Feld „Anmeldeinformationsalias“ angezeigt.

e. Wählen Sie im Anmeldeinformationsformular Kubernetes**die Option Aktualisieren aus**.

8. Erstellen Sie einen serverlosen Discovery-Zeitplan für das Muster Kubernetes.

Erstellen und definieren Sie das Ausführungsmuster ohne Server wie in der Produktdokumentation beschrieben. Konfigurieren Sie die für das Muster Kubernetes erforderlichen Parameter wie folgt:

Attribute für Ausführungsmuster konfigurieren

Feld	Beschreibung
URL	Der Bezeichner für den Hostnamen, die IP oder der FQDN und der Port des Kubernetes -API-Servers. Verwenden Sie das folgende Format: beispiel_hostname:beispiel_port oder beispiel_ip:beispiel_port. Geben Sie das richtige Protokoll (HTTP oder HTTPS) in der URL an.
namespace	Die Namespaces, die das System in der Discovery-Konfiguration Kubernetes übergibt. Geben Sie einen der folgenden Werte ein: ◦ Individueller Namespace: Geben Sie den Namespace und dann „kube-system“ ein. Beispiel: `dev,kube-system` ◦ Der Standardwert: Geben Sie `Standard, Kube-System`ein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Namespaces für mehrere Stapel: Geben Sie die Namespaces ein, trennen Sie die Werte durch Kommas (,), und geben Sie dann „kube-system“ ein. Beispiel: `Automation,Application,Test,Kube-System` ◦ Alle Namespaces: Verwenden Sie ein Sternchen (*), um alle Namespaces einzugeben
Alias für Anmeldeinformationen	Der Alias, der den zuvor erstellten Kubernetes -Anmeldeinformationen zugeordnet ist.
Clustername	Der Name des Clusters Kubernetes im folgenden Format:<serviceaccountid><space><clustername>
Anbieter	Der Cloud-Anbieter: GCP oder AWS oder Azure.
cluster_resource_id	Beispiel für eine Clusterressourcen-ID: ◦ Azure Kubernetes -Cluster: Ressourcen-ID. ◦ AWS-Cluster-ARN. ◦ GCP – globaler Name des Clusters.

9. Erstellen Sie einen Zeitplan für die serverlose Discovery für das Muster Kubernetes Event. Konfigurieren Sie den Zeitplan so, dass er alle 5 oder 10 Minuten ausgeführt wird.

   Hinweis: Wenn das Muster zum ersten Mal ausgeführt wird, wird ein event_timestamp gespeichert. Später werden nur die Delta-Events basierend auf dem Zeitstempel erfasst. Je häufiger das Muster ausgeführt wird, desto weniger Updates für die CMDB-IRE sind erforderlich.

   Erstellen Sie ein Ausführungsmuster ohne Server für den Discovery-Zeitplan, und weisen Sie es dem Muster Kubernetes Events zu. Konfigurieren Sie die für das Muster Kubernetes erforderlichen Parameter wie in Attribute für Ausführungsmuster konfigurierenbeschrieben.

10. Um erkannte Komponenten in Serviceinstanzen aufzunehmen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von Service-Mappingverwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Konfiguration der Tag-basierten Discovery.

Voraussetzungen für die Erkennung von Kubernetes-Cloud-Infrastrukturen

Führen Sie für das Muster Google Cloud Platform (GCP) – Get Kubernetes Clusters Folgendes aus:

1. Richten Sie in der ServiceNow-Instanz ein Servicekonto für Google Cloud Platform (GCP) mit gültigen Anmeldeinformationen und Berechtigungen ein.
2. Richten Sie in der Infrastruktur GCPMID-Server mit vollständigem Zugriff auf alle Cloud-APIs ein: Legen Sie für Cloud-API-Zugriffsbereiche „Vollständigen Zugriff auf alle Cloud-APIs zulassen“ fest. Die MID-Serverinstanz kann nur auf die für das Projekt spezifischen Cluster zugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Navigieren Sie zu `sys_properties.list`, und konfigurieren Sie die folgenden Eigenschaften:

   - *`sn_itom_pattern.k8s_midserver`*: Geben Sie einen gültigen MID-Server -Namen an.
   - *`sn_itom_pattern.k8s_create_schedule_enabled`*: Legen Sie den Wert auf **true** fest.

   Hinweis: Durch Aktivieren der Eigenschaft *`sn_itom_pattern.k8s_create_schedule_enabled`* wird automatisch ein Zeitplan ohne Server für Ihre Cloud-Cluster erstellt, sodass keine manuelle Planung erforderlich ist. Wenn ein manueller Zeitplan vorhanden ist und Sie ihn in einen automatischen Zeitplan konvertieren möchten, aktivieren Sie die Eigenschaft. Ihr manueller Zeitplan wird aktualisiert. wird kein zusätzlicher Zeitplan erstellt.

4. Erstellen und ausführen Google Cloud Discovery

   Hinweis:

   Um das Bearer-Token abzurufen, während der GKE-Zeitplan Kubernetes ausgeführt wird, verwenden Sie den gcloud-Befehl:

   ```
   gcloud config config-helper --format =
   „value(credential.access_token)“
   ```

   Durch die Konfiguration von gcloud in der MID-Server-Instanz wird dem GKE-Cluster Zugriff gewährt, um das Token abzurufen.

Führen Sie für die Discovery des Clusters Amazon Elastic Kubernetes Service (EKS) Folgendes aus:

1. Richten Sie in der ServiceNow-Instanz ein Servicekonto für AWS mit gültigen Anmeldeinformationen für das Verwaltungskonto sowie mit gültigen Berechtigungen ein.

   a. Stellen Sie sicher, dass der Cluster Amazon Elastic Kubernetes Service (EKS) über eine Clusterrolle mit Lesezugriff auf alle Ressourcen verfügt.
   b. Erstellen Sie eine Clusterrollenbindung zwischen der Clusterrolle und einem Kubernetes-Benutzer. Beispiel: schreibgeschützter Benutzer.
   c. Erstellen Sie eine AWS-IAM-Rolle mit der Richtlinie EKSReadOnly.
   d. Ordnen Sie die IAM-Rolle dem Kubernetes-Benutzer auf eine der folgenden Arten zu:

      - Bearbeiten Sie im Cluster die aws-auth ConfigMap.
      - Führen Sie den folgenden Befehl aus:

      ```
      eksctl create iamidentitymapping --cluster yourClusterName --
      arnarn:aws:iam::yourAccountID:role/yourIAMRoleName --username read-
      only-user
      ```

2. Führen Sie die Cluster-Discovery für Amazon Elastic Kubernetes Service (EKS) auf eine von zwei Arten aus: mit der Befehlszeilenschnittstelle (CLI) AWS von oder ohne Verwendung der AWS -CLI. Legen Sie zuerst die Systemeigenschaft *`sn_itom_pattern.k8s_aws_cli_to_generate_token`* fest, um das von Ihnen gewählte Modell zu verwenden. Diese Systemeigenschaft ist standardmäßig auf **true** festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie diese Systemeigenschaft auf **„true“** fest, um AWS die CLI zum Generieren eines Tokens zu verwenden.

- Legen Sie diese Systemeigenschaft auf **„false“** fest, um „Rollen übernehmen“ zum Generieren eines Tokens zu verwenden.

a. Führen Sie die Cluster-Discovery Amazon Elastic Kubernetes Service (EKS) mit AWS der -CLI aus:

i. Richten Sie MID-Server mit konfigurierter AWS -CLI ein. Die Konfiguration AWS der CLI-Anmeldeinformationen gewährt Zugriff auf den Cluster Amazon Elastic Kubernetes Service (EKS).

Hinweis: Der beim System angemeldete Benutzer muss mit dem Benutzer MID-Server identisch sein.

ii. Um das Bearer-Token zu generieren, verwenden Sie während der Ausführung des Zeitplans Amazon Elastic Kubernetes Service (EKS) den CLI-Befehl AWS :`aws eks get-token --cluster-name`<cluster_name> .

Durch die Konfiguration des AWS -CLI-Anwenders/der Rolle in der MID-Server -Instanz wird der Zugriff auf den Amazon Elastic Kubernetes Service (EKS) -Cluster gewährt, um das Token zu generieren.

b. Führen Sie die Cluster-Discovery Amazon Elastic Kubernetes Service (EKS) aus, ohne AWS die -CLI zu verwenden:

Hinweis:

Diese Funktion wird ab Muster für Discovery und Service-Mapping Version 1.0.96 – Dezember 2022 unterstützt.

Ausführliche Anweisungen finden Sie im folgenden KB-Artikel: KB1182188: EKS-Cluster-Discovery mit STS AssumeRoles (Ohne AWS-CLI)

3. Navigieren Sie zu `sys_properties.list`, und konfigurieren Sie die folgenden Eigenschaften:

- *`sn_itom_pattern.k8s_midserver`*: Geben Sie einen gültigen MID-Server -Namen an.
- *`sn_itom_pattern.k8s_create_schedule_enabled`*: Legen Sie den Wert auf **true** fest.

Hinweis: Durch Aktivieren der Eigenschaft *`sn_itom_pattern.k8s_create_schedule_enabled`* wird automatisch ein Zeitplan ohne Server für Ihre Cloud-Cluster erstellt, sodass keine manuelle Planung erforderlich ist. Wenn ein manueller Zeitplan vorhanden ist und Sie ihn in einen automatischen Zeitplan konvertieren möchten, aktivieren Sie die Eigenschaft. Ihr manueller Zeitplan wird aktualisiert. wird kein zusätzlicher Zeitplan erstellt.

4. Erstellen Sie den AWS Cloud Discovery-Zeitplan, und führen Sie diesen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Führen Sie für die Cluster-Discovery von Microsoft Azure Kubernetes Services (AKS)–Kubernetes Folgendes aus:

Hinweis: Das Muster Kubernetes unterstützt die Discovery von AKS-Clusterversionen vor Version 1.30.

1. Führen Sie eine Aktualisierung auf die neueste Version Muster für Discovery und Service-Mapping durch.
2. Konfigurieren Sie in der Instanz ServiceNow den Serviceaccount Azure mit gültigen Anmeldeinformationen und Berechtigungen Azure für .
3. Navigieren Sie zu `sys_properties.list`, und konfigurieren Sie die folgenden Eigenschaften:
   - *sn_itom_pattern.k8s_midserver*: Geben Sie einen gültigen MID-Server -Namen an.
   - *sn_itom_pattern.k8s_create_schedule_enabled*: Legen Sie den Wert auf **true** fest.

     Hinweis: Durch Aktivieren der Eigenschaft *sn_itom_pattern.k8s_create_schedule_enabled*wird automatisch ein Zeitplan ohne Server für Ihre Cloud-Cluster erstellt, sodass keine manuelle Planung erforderlich ist. Wenn ein manueller Zeitplan vorhanden ist und Sie ihn in einen automatischen Zeitplan konvertieren möchten, aktivieren Sie die Eigenschaft. Ihr manueller Zeitplan wird aktualisiert. wird kein zusätzlicher Zeitplan erstellt.

   .
4. Wenn Sie keine lokalen Accounts mit Kubernetes RBAC haben und die Mustereffizienz verbessern möchten, navigieren Sie zu **MID-Server** > **Eigenschaften** und legen Sie die Eigenschaft *sn_itom_pattern.aks_fetch_local_ad_token* auf **false**fest.
5. Führen Sie einen Cloud-Discovery-Zeitplan Azure aus.
6. Konfigurieren Sie MID-Server in den Zeitplänen Discovery entsprechend dem Cluster-Account-Typ. Wenn Sie keine lokalen Accounts bei RBAC haben, können Sie diesen Schritt ignorieren.

Clusterkontotyp	Discovery **Zeitplan** MID-Server
MS Entra ID-Authentifizierung mit Kubernetes RBAC.	Beliebiger MID-Server.
MS Entra ID-Authentifizierung mit Azure RBAC.	Beliebiger MID-Server.
Lokale Konten mit Kubernetes RBAC.	Wählen Sie MID-Server mit konfigurierter Befehlszeilenschnittstelle (CLI) Azure aus. Durch die Konfiguration der Azure CLI-Anmeldeinformationen wird der Zugriff auf den AKS-Cluster gewährt. Um das Bearer-Token während der Ausführung des AKS-Zeitplans Kubernetes abzurufen, verwenden Sie den CLI-Befehl Azure : `az aks get-credentials --name`<cluster_name> --overwrite-existing --

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Clusterkontotyp	Discovery **Zeitplan** MID-Server
	resource-group<resourceGroup_name> -- Datei - .

Hinweis:

- Der beim System angemeldete Benutzer muss mit dem Benutzer MID-Server identisch sein.
- Ausführliche Informationen zur Konfiguration von AKS-Cluster-Discovery finden Sie im Artikel AKS-Cluster-Discovery-Konfigurationsdetails [KB1220553] in der Now Support Knowledge Base.

Andere unterstützte Systemkonfiguration

	Eigenschaftsname	Eigenschaftsbeschre	Typ	Standardwert
	sn_itom_pattern.manifest_digest_image_id		Boolean	falsch **Hinweis:** Bevor Sie diese Eigenschaft auf **„wahr“** festlegen und Discovery ausführen: Verhindern Sie die Erstellung von doppelten Datensätzen, indem Sie alle Docker Bilddatensätze löschen.
	sn_itom_pattern.k8s_create_schedule_enabled	Funktionskennzeichnung, die unter den Systemeigenschaften aktiviert/ deaktiviert werden kann und für die Steuerung der Musterausführung verantwortlich ist. Wenn diese Option aktiviert ist, werden Discovery-Zeitpläne	Boolean	falsch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere unterstützte Systemkonfiguration (Fortsetzung)

	Eigenschaftsname	Eigenschaftsbeschre	Typ	Standardwert
		unabhängig vom neuen Eigenschaftswert erstellt.		
	sn_itom_k8s_run_cloud_discove	Wenn diese Eigenschaft aktiviert ist, führt sie Cloud-K8s-Muster aus und erkennt K8s-Cluster, ohne automatische Zeitpläne zu erstellen.	Boolean	falsch
MID-Server	sn_itom_pattern.k8s_midserver	[String] Beispiel: Gültiger MID-Server-Name	Zeichenfolge	
	sn_itom_pattern.k8s_<service_account_id>_midserver	[String auf der Service-Account-Ebene] Beispiel: Gültiger MID-Server-Name	Zeichenfolge	
	sn_itom_pattern.k8s_<service_account_id>_<clustername>_midserver	[String auf Clustername] Beispiel: Gültiger MID-Server-Name	Zeichenfolge	
	sn_itom_pattern.kubernetes_collekt_volume	Wenn diese Eigenschaft auf **true** festgelegt ist, werden die Daten für das Kubernetes-Volume [cmdb_ci_kubernetes_volume] ausgefüllt.	Zeichenfolge	falsch
Anmeldeinformationsalias	sn_itom_pattern.k8s_cred_alias	[String	Zeichenfolge	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere unterstützte Systemkonfiguration (Fortsetzung)

	Eigenschaftsname	Eigenschaftsbeschre	Typ	Standardwert
		Beispiel: Name des Alias für Anmeldeinformationen		
	sn_itom_pattern.k8s_<service_account_id>_alias	[Benennen auf der Service-Account-Ebene] Beispiel: Gültiger Aliasname für Anmeldeinformationen.	Zeichenfolge	
	sn_itom_pattern.k8s_<service_account_id>_<clustername>_alias	[Benennen auf Clustername] Beispiel: Gültiger Aliasname für Anmeldeinformationen.	Zeichenfolge	
Prometheus-URL	sn_itom_pattern.k8s_<service_account_id>_prometheusUrl	[Standardmäßig] Beispiel: Gültige Prometheus-URL	Zeichenfolge	
	sn_itom_pattern.k8s_<service_account_id>_prometheusUrl	[Benennen auf der Service-Account-Ebene] Beispiel: Gültige Prometheus-URL	Zeichenfolge	
	sn_itom_pattern.k8s_<service_account_id>_<clustername>_prometheusUrl	[Benennen auf Clustername] Beispiel: Gültige Prometheus-URL	Zeichenfolge	
	sn_itom_pattern.k8s_Ausführung	[Unterstützte Ausführung des Discovery-Zeitplans – Täglich, Bei Bedarf, Wochentage, Wochenenden, Monatsletzter Tag, Ende des Kalenderquartals]	Zeichenfolge	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Andere unterstützte Systemkonfiguration (Fortsetzung)

	Eigenschaftsname	Eigenschaftsbeschre	Typ	Standardwert
		Beispiel: Täglich		
	sn_itom_pattern.k8s_batch_event	[Gibt an, wie viele Zeitpläne im Batch ausgeführt werden sollen – Standardwert ist 5] Beispiel: 5 (Anzahl der Zeitpläne, die im Batch ausgeführt werden sollen)	Ganzzahl	5
	sn_itom_pattern.k8s_batch_delay	[Legt die Zeitdifferenz zwischen zwei Batches, deren Wert in Sekunden angegeben ist] Beispiel: 300 (in Sekunden)	Ganzzahl	
	sn_itom_pattern.k8s_run_time	[Verfolgt die aktuelle Zeit für einen Batch] Wenn diese Eigenschaft festgelegt ist, können Sie dieselbe oder unsere dynamische Zeiteinstellung verwenden, die 5 Minuten nach der aktuellen Systemzeit liegt. Werte enthalten im Format HH:MM:SS Beispiel: 10:11:12 (HH:MM:SS)	Zeichenfolge	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: <service_account_id>ist der Account-ID-Name unter Cloud-Servicekonten. Weitere Informationen finden Sie unter: Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen

Kubernetes Discovery ohne Anmeldeinformationen oder MID-in-Cluster-Discovery

Voraussetzungen für Kubernetes Discovery ohne Anmeldeinformationen:

Stellen Sie den containerisierten MID-Server im Cluster Kubernetes bereit. Das Konfigurieren der Anmeldeinformationen für Kubernetes ist nicht erforderlich, da das Cluster MID-Server in Kubernetes den API-Server automatisch erkennt und authentifiziert.

Ausführungsmusterattribute für Discovery ohne Anmeldeinformationen konfigurieren

Feld	Beschreibung
URL	Geben Sie einen der folgenden Werte in das URL-Feld ein: https://Cluster Oder https://kubernetes.default.svc
namespace	Die Namespaces, die das System in der Discovery-Konfiguration Kubernetes übergibt. Geben Sie einen der folgenden Werte ein: • Individueller Namespace: Geben Sie den Namespace und dann „kube-system“ ein. Beispiel: `dev,kube-system` • Der Standardwert. Geben Sie Folgendes ein:`default,kube-system` • Namespaces für mehrere Stapel: Geben Sie die Namespaces ein, trennen Sie die Werte durch Kommas (,), und geben Sie dann „kube-system“ ein. Beispiel: `Automation,Application,Test,Kube-System` • Alle Namespaces: Verwenden Sie ein Sternchen (*), um alle Namespaces einzugeben.
cluster_name	Geben Sie einen eindeutigen Namen ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Kubernetes Cluster [cmdb_ci_kubernetes_cluster]	
Name	Der Name des kube-Controller-Manager-Leader
K8s_uid	Die UID des kube-system-Namespace [unterstützte Versionen: 1.0.92 und höher]
ip_address	Der Bezeichner für die host_ip des API-Servers Kubernetes.
port	Der Bezeichner für den Apiserver-Port Kubernetes.
namespace	Dieser Wert zeigt die Namespaces, die das System in der Discovery-Konfiguration Kubernetes übergeben hat.
event_timestamp	Der Zeitstempel des letzten Ereignisses, das in diesem Kubernetes -Cluster zum Zeitpunkt der Discovery erstellt wurde.
Kubernetes Knoten [cmdb_ci_kubernetes_node]	Der virtuelle Aspekt des Kubernetes -Knotens. Daten, die sich auf den physischen Aspekt des Knotens Kubernetes beziehen, werden unter dem Server Linux gespeichert.
name	Der Name des Kubernetes -Knotens. Das Format kann nur der Name des Computers oder der vollständige Name sein, der aus dem Namen und dem Hostnamen besteht: `<name>.<hostname>`.
k8s_uid	Der Bezeichner für die Knoten-UUID Kubernetes
Cluster	Der Name des Clusters, der diese Ressource enthält.
operational_status	Der Betriebsstatus des Knotens Kubernetes
Kubernetes Service [cmdb_ci_kubernetes_service]	
name	Der Name des Kubernetes -Services.
Auswahl	Kommagetrennte Liste der in der Konfiguration Kubernetes angegebenen Bezeichnungsauswahlen, die zur Auswahl von Ziel-Pods verwendet werden.
namespace	Der Namespace Kubernetes, zu dem der Service Kubernetes gehört.
k8s_uid	Die Kubernetes -Service-UUID.
Cluster	Der Name des Clusters, der diese Ressource enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Kubernetes -Pod [cmdb_ci_kubernetes_pod]	
name	Der Name des Kubernetes -Pods.
k8s_uid	Die Kubernetes -Pod-UUID.
resourceVersion	Die Ressourcenversion des Kubernetes -Pods.
namespace	Der Kubernetes -Namespace, zu dem dieser Kubernetes -Pod gehört.
Cluster	Der Name des Clusters, der diese Ressource enthält.
state	Der Status des Pods Kubernetes : Ausstehend, Wird ausgeführt, Erfolgreich, Fehlgeschlagen und Unbekannt.
Kubernetes Cron-Job [cmdb_ci_kubernetes_cronjob]	
name	Der Name des Kubernetes -Cronjobs
namespace	Der Kubernetes -Namespace, zu dem dieser Kubernetes -Pod gehört.
k8s_uid	Die Cron-Job-UUID Kubernetes.
Cluster	Der Name des Clusters, der diese Ressource enthält.
Kubernetes Auftrag [cmdb_ci_kubernetes_job]	
name	Der Name des Auftrags Kubernetes .
namespace	Der Namespace Kubernetes, zu dem der Auftrag Kubernetes gehört.
k8s_uid	Die Kubernetes -Auftrags-UUID
Cluster	Der Name des Clusters, das den Auftrag Kubernetes enthält.
Kubernetes Daemonset [cmdb_ci_kubernetes_daemonset]	
name	Der Name des Kubernetes -DaemonSets.
namespace	Der Namespace Kubernetes, zu dem dieses Kubernetes -Daemonset gehört.
k8s_uid	Die Kubernetes -DaemonSet-UUID.
Cluster	Der Name des Clusters, der diese Ressource enthält.
pods_avail	Die Anzahl der verfügbaren Pods.
pods_failed	Die Anzahl der Pods in der fehlgeschlagenen Phase.
pods_running	Die Anzahl der Pods in der Phase „Ausgeführt“.
pods_succeeded	Die Anzahl der Pods in der Phase „Erfolgreich“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
pods_waiting	Die Anzahl der Pods in der Wartephase.
Kubernetes Eingehend [cmdb_ci_kubernetes_ingdress]	
name	Der Name des Eingangs Kubernetes
namespace	Der Namespace Kubernetes, zu dem dieser Kubernetes -Eingang gehört.
k8s_uid	Die Kubernetes Eingangs-UID
Cluster	Der Name des Clusters, der diese Ressource enthält.
Kubernetes Bereitstellung [cmdb_ci_kubernetes_deployment] Kubernetes Replikatsatz [cmdb_ci_kubernetes_replicaset] Kubernetes Replikationscontroller [cmdb_ci_kubernetes_replicationcontroller] Kubernetes Statefulset [cmdb_ci_kubernetes_statefulset]	
name	Der Name dieser Ressource
namespace	Der Namespace Kubernetes, zu dem diese Ressource gehört.
K8s_uid	Die Kubernetes -UID dieser Ressource
Cluster	Der Name des Clusters, der diese Ressource enthält.
total_replicas	Anzahl der Replikate in dieser Ressource
desired_replicas	Die Anzahl der Replikate in der gewünschten Phase
available_replicas	Anzahl der verfügbaren Replikate
unavailable_replicas	Anzahl der Replikate in der nicht verfügbaren Phase
updated_replicas	Anzahl der aktualisierten Replikate
Docker-Container [cmdb_ci_docker_container]	Die Komponente, die das Docker-Image ausführt
container_id	Der eindeutige Bezeichner für den Docker-Container Kubernetes . In Fällen, in denen doppelte Datensätze erstellt werden, werden Deduplizierungsaufgaben angezeigt, sobald Discovery ausgeführt wird. Informationen zur Lösung dieser Aufgaben finden Sie im Artikel Docker-Container-Bezeichner unabhängig machen [KB1443042] in der ServiceNow® Knowledge Base.
namespace	Der Namespace Kubernetes, zu dem der Docker-Container Kubernetes gehört

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Docker-Image [cmdb_ci_docker_image]	Ein ausführbares Paket einer Anwendung und der zugehörigen Software, das von einem Docker-Container instanziiert werden kann
image_id	Der Bezeichner für das Docker-Image Kubernetes .
name	Der Name des Docker-Images Kubernetes.
image_url	Die URL für das Herunterladen des Docker-Image.
namespace	Der Namespace Kubernetes, zu dem dieses Docker-Image Kubernetes gehört.
Linux-Server [cmdb_ci_linux_server]	Der Server, der den Knoten Kubernetes hostet.
name	Der Name des Linux-Servers, der den Kubernetes -Knoten antreibt.
hostname	Der Hostname des Linux-Servers
os	Das auf diesem Linux-Server bereitgestellte Betriebssystem
kernel_release	Die Version des auf diesem Linux-Server bereitgestellten Linux-Kernel-Betriebssystems.
ram	Die Größe des auf diesem Linux-Server installierte RAM.
ip_address	Die IP-Adresse des Linux-Servers
Schlüsselwert [cmdb_key_value]	Dieses Configuration Item enthält Kubernetes Bezeichnungen. Bezeichnungen sind Schlüssel/Wert-Paare, die an Objekte wie Pods angehängt werden.
Schlüssel	Der Schlüssel des Parameters Kubernetes „ Pod oder Kubernetes Service *Key Value*.
Wert	Der Wert des Parameters Kubernetes „ Pod oder Kubernetes Service *Key Value*.
Kubernetes Volumen [cmdb_ci_kubernetes_volume]	
k8s_uid	Die UUID des Kubernetes -Volumes.
mount_path	Der Pfad für den Zugriff auf dieses Kubernetes -Volume.
name	Der Name des Volumes Kubernetes.
namespace	Der Namespace Kubernetes, zu dem dieses Volume Kubernetes gehört.
Cluster	Der Name des Clusters, der diese Ressource enthält.
volume_id	Die ID des Kubernetes -Volumes.
OpenShift Bereitgestellte Konfiguration [cmdb_ci_openshift_dep_conf]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
name	Der Name der Bereitstellungskonfiguration OpenShift.
namespace	Der Name des Namespace, der die Bereitstellungskonfiguration enthält
k8s_uid	Die UUID des Kubernetes -Volumes.
URL	Die URL der bereitgestellten Konfiguration OpenShift.
OpenShift Buildkonfiguration [cmdb_ci_openshift_build_conf]	
name	Der Name der Build-Konfiguration OpenShift.
namespace	Der Name des Namespace OpenShift, der die Build-Konfiguration enthält.
k8s	Die UUID des Kubernetes -Volumes.
URL	Die URL der Build-Konfiguration OpenShift.
OpenShift Quelle2Bild [cmdb_ci_openshift_source_2_image]	
name	Der Name des OpenShift-Quell-Image
bis	Zugehöriges Image
parent_id	Die ID des Quell-Image OpenShift
OpenShift Weiterleitung [cmdb_ci_openshift_route]	
name	Der Name der Route OpenShift.
namespace	Der Name des Namespace, der die Route OpenShift enthält.
k8s_uid	Die UUID des Kubernetes -Volumes.
URL	Die URL der Route OpenShift.
host	Der Zielhost der Route OpenShift.
port	Der Zielport der Route OpenShift.
OpenShift Gruppe [cmdb_ci_openshift_group]	
name	Der Name der Gruppe OpenShift
k8s_uid	Die UUID des Kubernetes -Volumes.
URL	Die URL der Gruppe OpenShift
OpenShift Benutzer [cmdb_ci_openshift_user]	
name	Der Name des Anwenders OpenShift.
k8s_uid	Die UUID des Kubernetes -Volumes.
URL	Die URL des Anwenders OpenShift.
full_name	Der vollständige Name des Anwenders OpenShift.
OpenShift Projekt [cmdb_ci_openshift_project]	
name	Der Name des OpenShift -Projekts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
k8s_uid	Die UUID des Kubernetes -Volumes.
URL	Die URL des Projekts OpenShift
OpenShift Bild [cmdb_ci_openshift_images]	
name	Der Name des OpenShift Image.
k8s_uid	Die UUID des Kubernetes -Volumes.
URL	Die URL des Bildes OpenShift
docker_image_metadata_id	Die ID des Docker-Image
docker_image_metadata_parent_id	Die ID der übergeordneten ID des Image
arch	Architektur des Image
size	Die Image-Größe
hostname	Der dem Image zugeordnete Host-Name
OpenShift Bilderstrom [cmdb_ci_openshift_images_stream]	
name	Der Name des OpenShift Image-Streams.
k8s_uid	Die UUID des Kubernetes -Volumes.
URL	Die URL des OpenShift Image-Streams.
namespace	Der Name des Namespace, der den Image-Stream OpenShift enthält.
OpenShift Docker-Image-Repository [cmdb_ci_openshift_docker_images_repository]	
name	Der Name des Docker-Image-Repositorys OpenShift.
parent_ID	Die ID des übergeordneten Systems
-Namespace [cmdb_ci_kubernetes_namespace]	
name	Der Name des Kubernetes -Namespace.
state	Die Namespacephasen Kubernetes : „Aktiv“ oder „Wird beendet“.

Diese Daten werden vom Erweiterungsabschnitt *Collect Container Repository* erfasst.

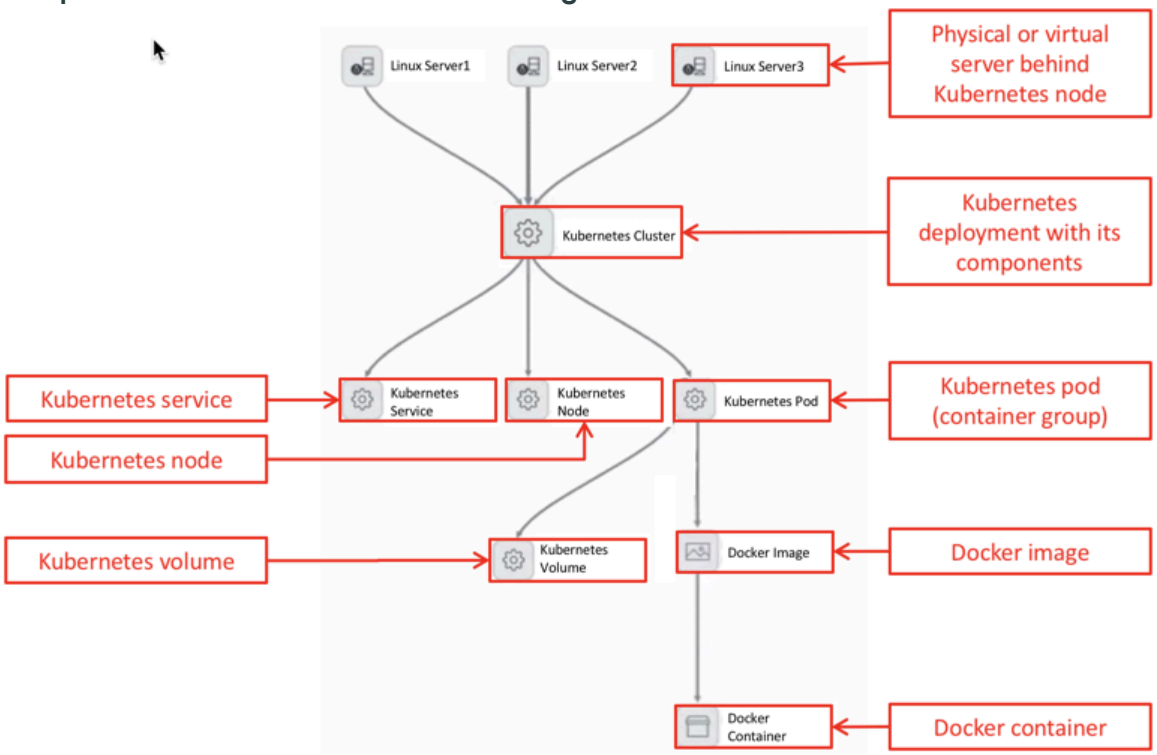
Tabelle und Feld	Beschreibung
Container-Repository [cmdb_ci_container_repository]	
Name [name]	Der Name des Container-Repositorys.
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]	
Name [name]	Der Name des Container-Repository-Eintrags.
Kategorie [category]	Die Kategorie des Container-Repository-Eintrags.

Die Grafik veranschaulicht CIs, die Teil der Discovery von Kubernetes sind.

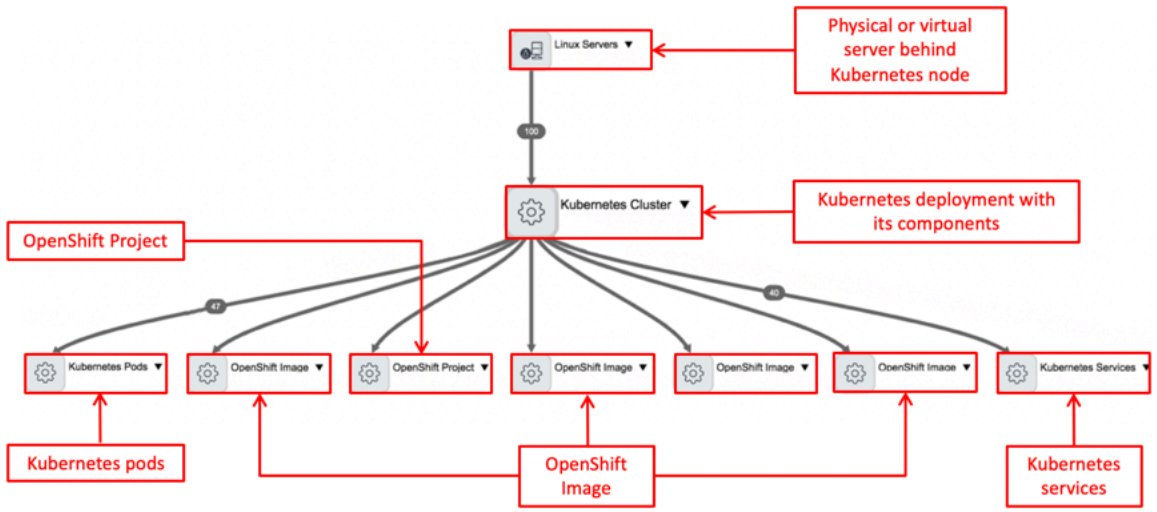
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Diese Abhängigkeitsansichten-Zuordnung wurde der Übersichtlichkeit halber vereinfacht. Ihre Kubernetes -Bereitstellungen können viel mehr CIs enthalten.

Komponenten der Kubernetes -Bereitstellung



Komponenten der Kubernetes -Bereitstellung, einschließlich OpenShift



Vom Muster „Kubernetes“ erfasste CI-Beziehungen

Diese Beziehungen werden mit Kubernetes dem Mustererstellt:

CI	Beziehung	CI
Kubernetes Cluster [cmdb_ci_kubernetes_cluster]	Enthält::Enthalten in	Kubernetes Service [cmdb_ci_kubernetes_service]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
	Enthält::Enthalten in	Kubernetes -Pod [cmdb_ci_kubernetes_pod]
	Enthält::Enthalten in	Kubernetes Eingehend [cmdb_ci_kubernetes_ingdress]
	Enthält::Enthalten in	Kubernetes -Namespace [cmdb_ci_kubernetes_namespace]
	Enthält::Enthalten in	[cmdb_ci_openshift_source_2_image]
	Enthält::Enthalten in	OpenShift Gruppe [cmdb_ci_openshift_group]
	Enthält::Enthalten in	OpenShift Benutzer [cmdb_ci_openshift_user]
	Enthält::Enthalten in	OpenShift Projekt [cmdb_ci_openshift_project]
	Enthält::Enthalten in	OpenShift Bild [cmdb_ci_openshift_images]
	Enthält::Enthalten in	OpenShift Docker-Image-Repository [cmdb_ci_openshift_docker_images_reposito
	Cluster von::Cluster	Kubernetes Knoten [cmdb_ci_kubernetes_node]
	Verwaltet::Verwaltet von	Linux-Server [cmdb_ci_linux_server]
	Enthalten in::Enthält	Ressourcengruppe [cmdb_ci_resource_group]
Kubernetes -Pod [cmdb_ci_kubernetes_pod]	Enthält::Enthalten in	Docker-Container [cmdb_ci_docker_container]
	Enthält::Enthalten in	Docker-Image [cmdb_ci_docker_image]
	Enthält::Enthalten in	Kubernetes Volumen [cmdb_ci_kubernetes_volume]
Kubernetes Arbeitsauslastung [cmdb_ci_kubernetes_workload]	Gehostet auf::Hostet	Kubernetes Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes-Service [cmdb_ci_kubernetes_service]	Stellt Folgendes bereit::Bereitgestellt von	Kubernetes Arbeitsauslastung [cmdb_ci_kubernetes_workload]
Kubernetes-Bereitstellung [cmdb_ci_kubernetes_deployment]	Besitzt::Eigentum von	Kubernetes Replikatsatz [cmdb_ci_kubernetes_replicaset]
Kubernetes Replikatsatz [cmdb_ci_kubernetes_replicaset]	iInstantiates:: Instanziiert von	Kubernetes -Pod [cmdb_ci_kubernetes_pod]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Kubernetes Arbeitsauslastung [cmdb_ci_kubernetes_workload]	Bereitgestellt von::Stellt bereit für	Kubernetes Service [cmdb_ci_kubernetes_service]
Kubernetes Bereitstellung [cmdb_ci_kubernetes_deployment]	Gehostet auf::Hostet	Kubernetes Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes Daemonset [cmdb_ci_kubernetes_daemonset]	Gehostet auf::Hostet	Kubernetes Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes Statefulset [cmdb_ci_kubernetes_statefulset]	Gehostet auf::Hostet	Kubernetes Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift Bereitgestellte Konfiguration [cmdb_ci_openshift_dep_conf]
	Enthält::Enthalten in	OpenShift Buildkonfiguration [cmdb_ci_openshift_build_conf]
	Enthält::Enthalten in	OpenShift Weiterleitung [cmdb_ci_openshift_route]
	Enthält::Enthalten in	OpenShift Bilderstrom [cmdb_ci_openshift_images_stream]
Docker-Image [cmdb_ci_docker_image]	Instanziiert::Instanziiert von	Docker-Container [cmdb_ci_docker_container]
Linux-Server [cmdb_ci_linux_server]	Enthält::Enthalten in	Kubernetes -Pod [cmdb_ci_kubernetes_pod]
	Wird ausgeführt:Wird ausgeführt auf	Docker-Container [cmdb_ci_docker_container]
	Hostet::Gehostet auf	Kubernetes Knoten [cmdb_ci_kubernetes_node]
OpenShift Bereitstellungskonfiguration [cmdb_ci_openshift_dep_conf]	Enthält::Enthalten in	[cmdb_ci_config_file_tracked]

Der Erweiterungsabschnitt *`Collect Container Repository`* des Kubernetes-Musters identifiziert diese Beziehungen.

CI	Beziehung	CI
Docker-Image [cmdb_ci_docker_image]	Bereitgestellt von::Bereitgestellt	Container-Repository-Eintrag [cmdb_ci_container_repository_entry]
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]	Gehostet auf::Hostet	Container-Repository [cmdb_ci_container_repository]

Von der Erweiterung „Istio Service Mesh“ erfasste CI-Beziehungen

Voraussetzungen für die Erweiterung „Istio Service Mesh“:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass die Istio Service Mesh- und Prometheus-Komponenten im Cluster Kubernetes konfiguriert sind.
- Stellen Sie sicher, dass Prometheus die Serviceverbindungsinformationen mit dem Befehl `„queryistio_requests_total"` erkennt.
- Stellen Sie sicher, dass die Anwendungsservices verbunden sind, und überprüfen Sie den Datenverkehrs-Flow von Service zu Service im Katalog von „Kiali Graph".

Weitere Informationen zur Anwendung „Bookinfo" finden Sie unter: https://istio.io/latest/docs/examples/bookinfo/

CI	Beziehung	CI
Kubernetes Service [cmdb_ci_kubernetes_service]	Verbindet mit::Verbunden mit	Kubernetes Service [cmdb_ci_kubernetes_service]

Vom Ereignismuster Kubernetes erfasste CI-Beziehungen

Diese Beziehungen werden erstellt, um die Erkennung des Ereignisses Kubernetes zu unterstützen:

CI	Beziehung	CI
Kubernetes Cluster [cmdb_ci_kubernetes_cluster]	Enthält::Enthalten in	Kubernetes Service [cmdb_ci_kubernetes_service]
	Enthält::Enthalten in	Kubernetes -Pod [cmdb_ci_kubernetes_pod]
	Cluster von::Cluster	Kubernetes Knoten [cmdb_ci_kubernetes_node]
	Verwaltet::Verwaltet von	[cmdb_ci_linux_server]
Kubernetes -Pod [cmdb_ci_kubernetes_pod]	Enthält::Enthalten in	Docker-Container [cmdb_ci_docker_container]
	Enthält::Enthalten in	Docker-Image [cmdb_ci_docker_image]
	Enthält::Enthalten in	Kubernetes Volumen [cmdb_ci_kubernetes_volume]
Docker-Image [cmdb_ci_docker_image]	Instanziiert::Instanziiert von	Docker-Container [cmdb_ci_docker_container]
Linux-Server [cmdb_ci_linux_server]	Enthält::Enthalten in	Kubernetes -Pod [cmdb_ci_kubernetes_pod]
	Wird ausgeführt:Wird ausgeführt auf	Docker-Container [cmdb_ci_docker_container]
	Hostet::Gehostet auf	Kubernetes Knoten [cmdb_ci_kubernetes_node]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten, die von Service-Mapping während der tagbasierten Erkennung erfasst wurden

Service-Mapping verwendet die Tag-basierte Discovery, um Anwendungsservice-Zuordnungen einschließlich der Kubernetes -Komponenten zu erstellen. Service-Mapping enthält die folgenden vorkonfigurierten CI-Beziehungen, die für die Tag-basierte Erkennung verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Kubernetes-Service [cmdb_ci_kubernetes_service]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
OpenShift-Projekt [cmdb_ci_openshift_project]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes-Pod [cmdb_ci_kubernetes_pod]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes-Pod [cmdb_ci_kubernetes_pod]	Cluster::Cluster von	Kubernetes-Service [cmdb_ci_kubernetes_service]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	Bereitgestellte OpenShift-Konfiguration [cmdb_ci_openshift_dep_conf]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Buildkonfiguration [cmdb_ci_openshift_build_conf]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Route [cmdb_ci_openshift_route]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Image-Stream [cmdb_ci_openshift_images_stream]

Kubernetes-Dashboard

Nachdem Discovery die Discovery von Komponenten der Bereitstellung Kubernetes abgeschlossen hat, können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** und verwenden Sie das Dashboard Kubernetes Explorer, um die Umgebungen und Ressourcen Ihrer Organisation Kubernetes anzuzeigen. Um das erweiterte Dashboard Kubernetes zu verwenden, vergewissern Sie sich, dass Sie über Discovery-Administratorarbeitsbereich ab Version Version 1.3.1 (Store August 2024) verfügen. Weitere Informationen zu Kubernetes Explorer finden Sie unter Kubernetes Explorer.

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

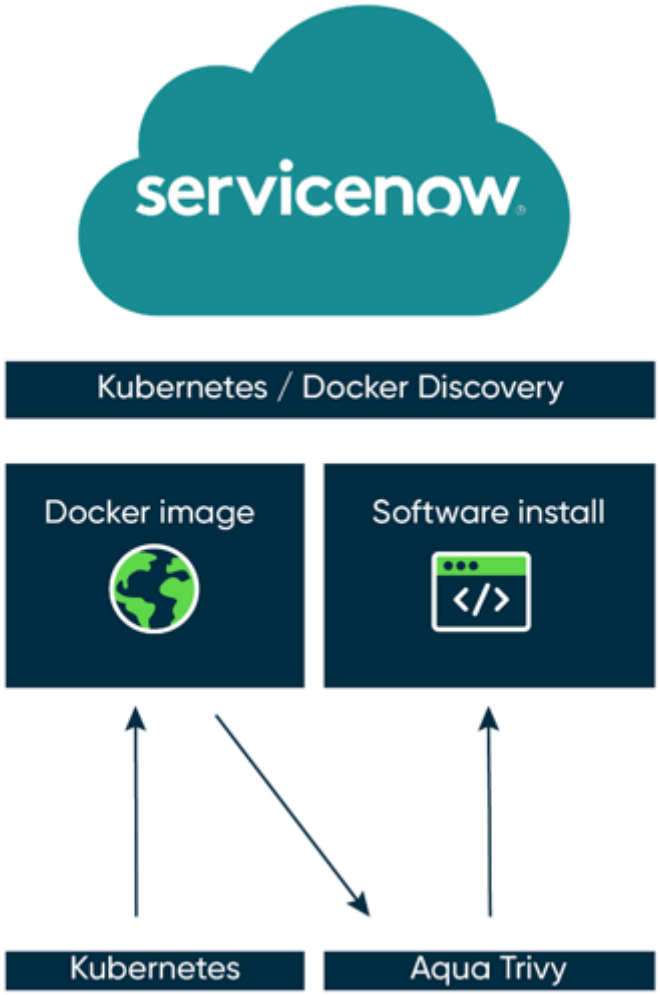
Symptom	Ursache	Lösung
die REST-Zeitüberschreitung verursacht wurde.	nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter *sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Betriebsinformationen zum Ausführen des Musters Kubernetes im Debug-Modus finden Sie unter KB0832567 .

Container-Image-Scans für Softwarezerlegung

Die Apps ITOM-Transparenz, Muster für Discovery und Service-Mapping und Kubernetes Visibility Agent sind in Aqua Trivy integriert, um Daten zu Container-Images und Betriebssystempaketen zu sammeln. Sie können Ihre Kontrolle über die Containerbereitstellung erhöhen, indem Sie Einblick in die Containerkomponenten erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Vorteile des Scannens von Bildern

Durch das Scannen Ihrer Container erhalten Sie Einblick in die Inhalte von Kubernetes - oder Docker -Containern oder Betriebssystempaketen. Das Scannen von Bildern kann Sie auf verschiedene Arten unterstützen.

- Es hilft Ihnen, in Containern installierte Software für regulatorische und Compliance-Anwendungsfälle zu identifizieren.
- Es hilft Ihnen, Unternehmensrichtlinien einzuhalten, z. B. die Verwendung von Golden Images, veraltete Software, obligatorische Bezeichnungen oder Konfigurationsrichtlinien.
- Es hilft Ihnen auch bei der Verwaltung von lizenzierter Software, die in Containern ausgeführt wird.
- Sie können den Servicekontext auch mithilfe von Tags und Service Mesh abrufen, um deren Auswirkungen auf Ihre Organisation zu verstehen.

Anwendungsfälle für das Scannen von Bildern mit ITOM-Transparenz

Sie können zwei Apps ITOM-Transparenz verwenden, um Container-Images zu scannen: Muster für Discovery und Service-Mapping und Kubernetes Transparenz-Agent. Muster sind ein Funktionssatz, der von Discovery, Cloud-Discoveryund Service-Mappingverwendet wird. Kubernetes Transparenz-Agent ist eine Funktion von Agent Client Collector. Während Kubernetes Visibility Agent (früher bekannt als CNO-V) besser für Kubernetes und dynamische

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

containerisierte Arbeitsauslastungen geeignet ist, eignet sich die musterbasierte Discovery besser für Nicht-Kubernetes-Container Docker.

Anwendungsfall Nr. 1

Sobald eine Anwendung in Container-Images paketiert wurde, kann ein Sicherheitsexperte das Basis-Image sowie das endgültige Image auf Schwachstellen scannen und Betriebssystempakete, Softwareabhängigkeiten und Anwendungsdatensätze identifizieren. Dies gilt speziell für den containerisierten MSSQL-Server.

Transparenzmethoden für Anwendungsfall Nr. 1

Transparenzmethoden	Methodeneigenschaften	Was erkannt wird
Muster für Discovery und Service-Mapping und Aqua Trivy: • Am besten geeignet für selbst gehostete oder Cloud-Bereitstellungen Kubernetes mit Zugriff auf Bearer-Token und Anmeldeinformationen. • Unterstützt das Scannen von öffentlichen und selbstgehosteten Repository-Images.	• Musterbasierte Discovery ohne Cloud-Discovery: ◦ Verwendet ein Bearer-Token. ◦ Manuell erstellter Discovery-Zeitplan Kubernetes pro Cluster. • Musterbasierte Discovery mit Cloud-Discovery: ◦ Kein Bearer-Token erforderlich. ◦ Verwendet Cloud-Anmeldeinformationen. ◦ Automatische Erstellung des Discovery-Zeitplans Kubernetes. • Weitere Informationen zum Scannen von Bildern mit Aqua Trivyfinden Sie unter Container-Images scannen.	Erkannt mit Muster für Discovery und Service-Mapping: • Kubernetes Cluster • Kubernetes Services • Kubernetes Topologie • Docker Container und Bilder • Kubernetes einschließlich OpenShift • Namespace • Bezeichnungen und Tags • Software in Containern • Details zur Account-Region können nur von erkannt werden Cloud-Discovery • Docker-Muster sammelt Daten zu bestimmten Objekten in einer Docker-Engine, die auf einem Linux-Host ausgeführt wird Weitere Informationen finden Sie unter: • Container-Image-Discovery • Erkennung von Kubernetes • Docker-Virtualisierung
Kubernetes Transparenz-Agent und Aqua Trivy:	Für die aufKubernetes dem Transparenz-Agent basierende	Erkannt mit Kubernetes Visibility Agent

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transparenzmethoden für Anwendungsfall Nr. 1 (Fortsetzung)

Transparenzmethoden	Methodeneigenschaften	Was erkannt wird
• Am besten geeignet für die Bereitstellung durch native Cloud-App-Teams. • Optionale Möglichkeit zur Überwachung von Kubernetes mit AIOps. • Für Cloud-Umgebungen wird nur AWS ECR (öffentlich und privat) unterstützt.	Discovery müssen keine Anmeldeinformationen eingerichtet werden, und auch MID-Serverist nicht erforderlich. Der Zugriff erfolgt über ServiceAccount/ ClusterRole. Die Installation erfolgt über die YAML-Datei „Helm Chart“ oder Kubernetes. Die Discovery wird nahezu in Echtzeit ausgeführt. Verwenden Sie den Kubernetes Explorer, um SBOMherunterzuladen.	• Kubernetes Namespaces • Knoten und Pods • Bereitstellungen • Statefulsets • Daemonsets • Replikatesätze • Aufträge • Cron-Jobs • Services • Docker Container • Docker-Bild • Container-Repository • Details zur Account-Region können nur von erkannt werden Cloud-Discovery

Anwendungsfall Nr. 2

Ein Compliance-Beauftragter kann einen SBOMgenerieren, um eine detaillierte Liste der Abhängigkeiten des Containerimages zu erhalten und um sicherzustellen, dass die Software die Branchenvorschriften erfüllt.

Transparenzmethoden für Anwendungsfall Nr. 2

Transparenzmethode	Methodeneigenschaften
Kubernetes -Muster oder Docker -Muster	SBOM Die Erstellung von ist Teil des Container-Scans.
Kubernetes Transparenz-Agent	Die ErstellungSBOM von ist auch Teil des Container-Scans, , aber die Verwendung von ACC eignet sich am besten für Organisationen, die Flexibilität benötigen, um sowohl eine vollständige als auch eine kontinuierliche Discovery durchzuführen.

Anwendungsfall Nr. 3

Ein Techniker hat einen Fehler in einem anwenderdefinierten Image gefunden und muss alle Kubernetes -Pods finden, die mit diesem Image ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transparenzmethoden für Anwendungsfall Nr. 3

Transparenzmethode	Methodeneigenschaften	Was erkannt wird
Kubernetespattern	Aqua Trivy Containerscans sind nicht erforderlich. Sie können die Pods anhand von Mustern identifizieren.	• Kubernetes Cluster • Kubernetes Container • Kubernetes Services • Bezeichnungen • Pods • Bilder • Tags
Kubernetes -Muster mit Cloud-Discovery	Aqua Trivy Containerscans sind nicht erforderlich. Sie können die Pods anhand von Mustern identifizieren.	Alle oben genannten sowie Account- oder Regionsdetails

Anwendungsfall Nr. 4

Ein -Entwickler findet einen Fehler in einem anwenderdefinierten Image und muss alle Docker -Container (nicht Kubernetes) finden, die mit diesem Image ausgeführt werden.

Transparenzmethode	Methodeneigenschaften	Was erkannt wurde
Horizontal-Discovery von VM mit Docker (MusterDocker)	Aqua Trivy Containerscans sind nicht erforderlich. Sie können die Pods anhand von Mustern identifizieren.	Siehe: Docker-Virtualisierung

Bilderscans mit Muster für Discovery und Service-Mapping

Die MusterKubernetes und Docker sind in das Tool Aqua Trivy integriert und führen regelmäßige Aufgaben aus, um Container-Images und Betriebssystempakete in festen Intervallen von 10 Images pro Minute zu erkennen. Während des Scanvorgangs zeigt das Muster den Scanstatus an. Das -Muster erkennt BS-Pakete, die zu einem Image gehören. Dann werden die Image-Befehlsattribute wie die CI-Klasse gesucht. Basierend auf den Befehlsattributen erstellt das Muster Anwendungsdatensätze. Darüber hinaus verwendet das Muster angereicherte Skripts, um den Anwendungsdatensätzen Details hinzuzufügen. Danach ordnet das Muster die Beziehungen zwischen den BS-Paketen und den Containern zu.

Ein Teil der Daten wird in Tabellen CMDB und ein Teil in Transformationstabellen (temporäre Nicht-CMDB-Tabellen) gefüllt. Die Transformationstabellen werden mit dem Muster installiert. Die Informationen, die Sie durch das Scannen erhalten, umfassen beispielsweise die Ursprungsregistrierung, den Softwarenamen und die Version.

Zugehörige Informationen

Cloud Native Operations für Transparenz

Container-Images scannen

Aktivieren Sie das Scannen von Containerbildern mit dem Tool Aqua Trivy.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Hinweis: Das Muster unterstützt nur das Linux-Betriebssystem und wird unter Linux MID-Serverausgeführt.

Überprüfen Sie das folgende Setup:

- Muster für Discovery und Service-Mapping, ab 1.7.0 (Store-Release vom August 2023).
- CMDB CI-Klassenmodelle, ab 1.43.0.
- Visibility Content, ab 6.7.2.
- Damit der Scanvorgang für Container-Images erfolgreich ausgeführt werden kann, stellen Sie sicher, dass alle MID Servers in Ihrer Umgebung für bestimmte Fähigkeiten konfiguriert und nicht auf **Alle**festgelegt sind. Weitere Informationen zum Konfigurieren von Fähigkeiten finden Sie unter MID-Server-Fähigkeiten .
- MID-Server Anforderungen:
  - 8 GB RAM mit 4 GB JVM
  - MID-Server **Fähigkeit,** die zum **Scannen von Container-Images**konfiguriert ist
  - Kann auf das Image-Repository zugreifen
- Aqua Trivy ab 0.44.0 ist auf MID-Serverinstalliert. Die letzte validierte Version ist 0.51.0. Weitere Informationen zur Installation Aqua Trivyvon finden Sie im Artikel Übersicht über die Scan-Funktion für Container-Images [KB1218504] in Now Support Knowledge Base.
- Zum Sammeln von Datensätzen für das Container-Image Docker oder Kubernetes müssen Sie zuerst die Discovery Docker oder Kubernetes ausführen, bevor Sie die Funktion zum Scannen von Container-Images aktivieren. Weitere Informationen finden Sie unter Erkennung von Kubernetes und Docker-Virtualisierung.
- Ab Muster für Discovery und Service-Mapping Version 1.18.0 unterstützt die Funktion Container-Image-Scan außerdem Folgendes:
  - Verwenden eines Proxy-Servers MID-Server zum Scannen der Containerbilder in den folgenden Repositorys: öffentliche, selbstgehostete private und Amazon Elastic Container Registry-Repositorys (Amazon ECR). Um einen Proxy MID-Serverzu verwenden, stellen Sie sicher, dass die Proxy-Parameter MID-Server richtig konfiguriert sind. Weitere Informationen finden Sie unter MID-Server-Parameter .
  - Container-Images in selbst gehosteten privaten Repositorys werden gescannt. Um diese Repositorys zu scannen, müssen Sie Anmeldeinformationen für das Container-Image-Repository erstellen. Weitere Informationen finden Sie unter Anmeldeinformationen erstellen und testen und Anmeldeinformationen für das Container-Image-Repository .
  - Bilddatensätze aus Amazon ECR werden in öffentlichen und privaten Repositorys gesammelt. Um diese Amazon ECR-Bilddatensätze zu sammeln, müssen Sie zuerst die ECS-Ressourcen-Discovery Amazon ausführen, bevor Sie den Container-Image-Scan aktivieren. Das Cloud-Servicekonto AWS, das für die ECS-Ressourcen-Discovery Amazon erstellt wurde, wird auch für den Container-Image-Scan verwendet. Weitere Informationen zur Erkennung von ECS-Ressourcen Amazon finden Sie unter Discovery von Amazon-ECS-Ressourcen.

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Aktivieren Sie den Container-Image-Scan Muster für Discovery und Service-Mapping, indem Sie die Systemeigenschaft festlegen.
   a. Geben Sie im Navigationsfilter `sys_properties.list` ein.
   b. Geben Sie im Suchfeld **Name**`sn_itom_pattern.container_image_scan`ein.
   c. Legen Sie den Wert auf **true**fest.
2. Geben Sie in der URL-Leiste Folgendes ein:<instance> `.service-now.com/sn_itom_pattern_container_image_scan_status_list.do`, um den Scan-Status der Images zu überprüfen.
3. Wählen Sie den Image-Datensatz aus, um die Tabelle „Container-Image-BS-Pakete“ zu überprüfen.

Ergebnisse

Das Muster „Container-Image scannen“ findet die Image-BS-Pakete und erstellt Anwendungsdatensätze basierend auf der CI-Klasse des Image. Die Tabelle „Containerimage BS-Pakete“ befindet sich im Image-Datensatz. Das Muster erstellt auch Beziehungen zwischen den Configuration Items. Weitere Informationen zu den gesammelten Daten finden Sie unter Container-Image-Discovery.

Konfigurieren Sie die Generierung SBOM .

Aktivieren Sie die Erstellung von Software-Stücklisten (SBOM), und vermeiden Sie die Generierung von doppelten SBOM-Dateien durch Festlegen der Systemeigenschaften.

Vorbereitungen

Überprüfen Sie das folgende Setup:

- Now Platform, mindestens Release Utah.
- Muster für Discovery und Service-Mapping ist aktuell.
- CMDB CI-Klassenmodelle, ist aktuell.
- Visibility Content ist aktuell.
- MID-Server Anforderungen: 8 GB RAM mit 4 GB JVM und der Fähigkeit zum Scannen von Container-Images. Weitere Informationen finden Sie unter Container-Images scannen

Erforderliche Rolle: discovery_admin

Prozedur

1. Wählen Sie das Format SBOM aus.
   a. Geben Sie im Navigationsfilter `sys_properties.list` ein.
   b. Suchen Sie in der Liste **„Systemeigenschaften“** nach `sn_itom_pattern.sbom_format`, und wählen Sie den Datensatz aus.
   c. Legen Sie das Feld **Wert** auf das gewünschte Format fest.
   Die verfügbaren Formate sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- zyklondex
- spdx-json
- spdx

Hinweis: Wenn Sie den Wert auf **„Keine“** festlegen, wird die Erstellung der SBOM deaktiviert.

2. Legen Sie die Systemeigenschaft *sys_attachment* fest, um zu vermeiden, dass doppelte SBOM -Dateien generiert werden.
   a. Navigieren zu **Alle** > **Systemdefinition** > **Tabellen**
   b. Geben Sie im Formular **Tabellen** im Feld **Bezeichnung** `*attach ein`.
   c. Wählen Sie den **Anhangsdatensatz** aus.
   d. Wählen Sie die Registerkarte **Anwendungszugriff**.
   e. Aktivieren Sie die Checkbox **Kann löschen**.
   f. Wählen Sie **Aktualisieren**.

Nächste Maßnahme
Software-Stückliste herunterladen (SBOM)

Software-Stückliste herunterladen (SBOM)

Laden Sie eine Software-Stückliste (SBOM) herunter, um Einblick in die Komponenten des Containerimages zu erhalten, z. B. die installierten Betriebssystempakete.

Vorbereitungen
SBOM muss konfiguriert worden sein. Weitere Informationen finden Sie unter Konfigurieren Sie die Generierung SBOM ..

Erforderliche Rolle: discovery_admin

Prozedur

1. Geben Sie im Navigationsfilter `sn_itom_pattern_container_image_scan_status_list.do`ein.
2. Wählen Sie in der Liste Containerimage-Scanstatus das Image aus, für das Sie SBOM benötigen.
   Wenn der Scan-Status **„Keine“** anstatt **„Gescannt“**lautet, warten Sie, bis sich der Status ändert, bevor Sie den Bilddatensatz auswählen.
3. Laden Sie die Datei SBOM herunter, indem Sie im Abschnitt **Anhänge verwaltendie Option Herunterladen** auswählen.

Container-Image-Discovery

Die Anwendung Muster für Discovery und Service-Mapping verwendet das Muster „Container-Image scannen“, um Docker -Images und Betriebssystempaketdaten zu erkennen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Informationen zum Durchführen eines Container-Image-Scans finden Sie unter Container-Images scannen.

Das Muster „Container-Image scannen“ unterstützt Aqua Trivy ab Version 0.44.0. Die letzte validierte Version ist 0.51.0.

Ab Muster für Discovery und Service-Mapping Version 1.18.0 unterstützt das Muster „Container-Image scannen“ das Scannen von Container-Images in den folgenden Repositorys:

- Öffentliche Repositorys
- Selbstgehostete private Repositorys
- Amazon Elastic Container Registry (Amazon ECR), sowohl in öffentlichen als auch in privaten Repositorys

Von Discovery gesammelte Daten für Container-Image-Scans

Discovery füllt die Daten in CMDB aus, wenn das Muster „Container-Image scannen“ ausgeführt wird.

Feld	Beschreibung
Tabelle „Anwendung“ [cmdb_ci_appl].	
Name [name]	Name der Containeranwendung. Das erforderliche Namensformat für den MSSQL-Anwendungsdatensatz: ApplicationTableName@containerName Beispiel: MSFT SQL Instance@/sql1
Tabelle „Container-Umgebungsvariablen“ [cmdb_container_environment_variables].	
Container [container]	Name des Containers.
Schlüssel [key]	Name der Container-Umgebungsvariablen.
Wert [value]	Wert der Container-Umgebungsvariablen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Temporäre Tabellen für Container-Image-Scans

Hinweis: Wenn Sie Version 1.0.98 zum Sammeln der Daten verwenden, werden die angereicherten Skripts nur mit MSSQL unterstützt.

Während der horizontalen Erkennung erfasste Daten

Feld	Beschreibung
Status der Container-Image-Prüfung [sn_itom_pattern_container_image_scan_status]	
Bild [image]	Name des Containerimages.
Nachricht [message]	Fehler oder Probleme beim Scannen.
CI-Klasse [ci_class]	Die CI-Klasse des Image basierend auf den Befehlsdetails des Image.
Discovery-Status [discovery_status]	Der Discovery-Statusdatensatz des Bildscans.
Scan-Status [scan_status]	Der Scan-Status. Verfügbare Werte: • Keine – Das Bild wurde noch nicht gescannt. • In Bearbeitung: Der Bildscan wird ausgeführt. **Hinweis:** Wenn mindestens ein Bild verarbeitet wird, wird der nächste Scan nicht ausgelöst. • Gescannt: Das Bild wurde erfolgreich gescannt. • Fehler: Während des Bildscans ist ein Problem aufgetreten. Details finden Sie in der Nachrichtenspalte. • Übersprungen – Die Bild-URL ist nicht ordnungsgemäß formatiert oder nicht erreichbar.
Tabelle „Container-Image-BS-Pakete“ [sn_itom_pattern_container_image_os_packages].	
Bild [image]	Name des Containerimages.
Paketname [package_name]	Name des Softwarepakets.
Paketversion [package_version]	Version des Softwarepakets.
Paketbetreuer [package_maintainer]	Name des Paketbetreuers
Container-Ergänzungsskripts [sn_itom_pattern_container_enrich_scripts]	
Aktiv [active]	Gibt an, ob der Anreicherungsskript-Status aktiv ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während der horizontalen Erkennung erfasste Daten (Fortsetzung)

Feld	Beschreibung
CI-Typ [ci_type]	Der CI-Typ, für den das Anreicherungsskript gilt.
Bestellung [order]	Ausführungsreihenfolge eines bestimmten Skripts
Skript [script]	Der Name des Ergänzungsskripts.

Beziehungen

Diese Beziehungen werden erstellt, um die Containerimage-Discovery zu unterstützen.

CI	Beziehung	CI
cmdb_ci_appl	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_oslv_container
cmdb_ci_docker_container	Erweitert	cmdb_ci_oslv_container
cmdb_ci_oslv_container	Erweitert	cmdb_ci
cmdb_ci_oslv_container	Nur Referenz	cmdb_container_environment_variables
container_enrich_scripts	Erweitert	sys_metadata
cmdb_container_environment	Erweitert	cmdb_key_value
cmdb_ci_db_mssql_instance	Wird ausgeführt:Wird ausgeführt auf	cmdb_ci_docker_container

Zugehörige Informationen

Docker-Virtualisierung

Erkennung von Kubernetes

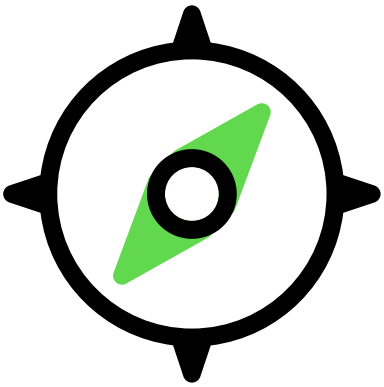
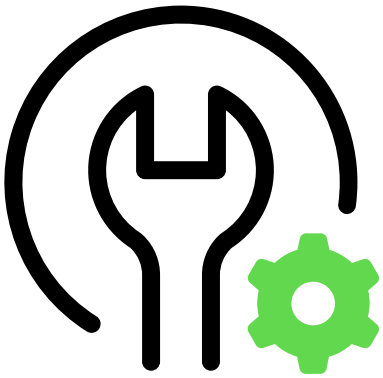
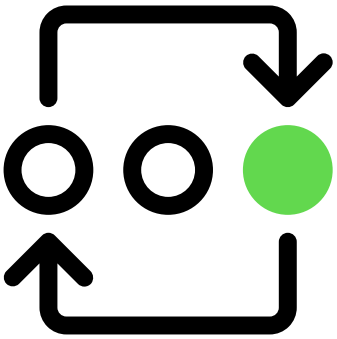
Firewall-Audits und Reporting

Verwenden Sie die Anwendung Firewall-Audits und Reporting, um Ihre Firewall-Sicherheitsrichtlinien, Geräte, Gerätegruppen und Managerinformationen zu untersuchen und einen Bestand zu erstellen. Darüber hinaus können Sie Anforderungen für neue Firewall-Regeln über die Anwendung Servicekatalog initiieren und innerhalb bestimmter Zeitrahmen Audits der Firewall-Sicherheitsrichtlinien durchführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Firewall-Audits und Reporting erkunden	Verwalten Firewall-Audits und Reporting	Firewall-Audits und Reporting – Referenz
		
Nutzen Sie Firewall-Audits und Reporting, um Bestand zu erstellen	Erfahren Sie, wie Sie den Firewall-Bestand einrichten	Machen Sie sich mit Dashboards und Berichtskalibrierung vertraut

Problembehandlung und Hilfe

- Was ist ein Firewall-Audit?
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Firewall-Audits und Reporting erkunden

Mit Firewall-Audits und Reportingkönnen Sie Ihre Firewall-Sicherheitsrichtlinien, Geräte, Gerätegruppen und Managerinformationen untersuchen und den Bestand davon durchführen. Darüber hinaus können Sie damit Anforderungen für neue Firewall-Regeln übermitteln und Sicherheitsrichtlinien innerhalb eines bestimmten Zeitrahmens prüfen.

Firewall-Audits und Reporting – Übersicht

Ein Firewall-Gerät fungiert als Netzwerksicherheitssystem, das den Datenverkehr basierend auf bestimmten Richtlinien überwacht und steuert. Es stellt eine Schutz Barriere zwischen vertrauenswürdigen internen und nicht vertrauenswürdigen externen Netzwerken her und integriert mehrere Sicherheitsrichtlinien zum Schutz vor Bedrohungen. Kontinuierliche Wartung und Audits sind für die Weiterentwicklung der Sicherheitsrichtlinien von entscheidender Bedeutung, um potenzielle Lücken zu schließen. Der Firewall-Auditprozess optimiert die Nachverfolgung und Aktualisierung von Regeln und stellt die Ausrichtung an den Sicherheitsrichtlinien des Unternehmens sicher. Firewall-Anbieter, darunter Panorama, bieten zentralisierte Manager für eine effiziente Kontrolle über Geräte und Richtlinien.

Firewall-Audits und Reporting – Workflow

Die Anwendung Firewall-Audits und Reporting ermöglicht dem ServiceNow Discovery-Prozess die Erkennung von Firewalls (derzeit Palo Alto Networks-Firewalls), CMDB-CIs für die Firewall-Geräte, Firewall-Managern, Firewall-Gerätegruppen und Firewall-Richtlinien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mithilfe von serverlosen Mustern. Auditaufgaben für Firewall-Richtlinien werden von Firewall-Managern oder -Geräten generiert. Über Servicekatalog können Sie zudem neue Firewall-Sicherheitsrichtlinien anfordern und ältere Firewall-Regelanforderungen, Auditanforderungen und Auditaufgaben archivieren, um die Systemperformance zu verbessern. Weitere Informationen finden Sie unter Transparenz des Firewall-Bestands.

Firewall-Audits und Reporting – Vorteile

Vorteil	Funktion	Anwender
Aktueller Bestand an Firewall-Sicherheitsrichtlinien, Geräten, Gerätegruppen und Managerinformationen durch dauerhaftes Speichern von Daten in CMDB durch regelmäßige Abfragen an einen Firewall-Manager.	Transparenz des Firewall-Bestands	Firewall-Administrator [sn_disco_firewall.firewall_admin]
Möglichkeit der Anforderung einer neuen Firewall-Regel mithilfe von Servicekatalog	Firewall-Regelanforderungen	Firewall-Anforderer [sn_disco_firewall.firewall_requester]

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Firewall-Audits und Reporting Rollen und Zuständigkeiten

Bestimmte Benutzer und Rollen zur Optimierung der Überwachung und Nachverfolgung von Anforderungen für neue Firewall-Regeln.

Die Konfigurationseinstellungen werden je nach zugewiesenen Rolle aktiviert oder deaktiviert.

Rolle	Verantwortlichkeiten
Firewall-Administrator [sn_disco_firewall.firewall_admin]	Verantwortlich für die Bearbeitung von Configuration Item (CI)-Attributen, die nicht von Discovery ausgefüllt werden, einschließlich „assigned_to“ und andere. Firewall-Administratoren können die Liste der Firewall-Manager mit spezifischen Details für jeden Manager anzeigen. Darüber hinaus sind sie berechtigt, das Dashboard anzuzeigen und zu bearbeiten, Audits über die Detailseite des Firewall-Managers zu initiieren, Richtlinien zu erstellen, zu ändern und anzuzeigen, Audit-Aufgaben zu bearbeiten und Richtlinienänderungen anzufordern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Verantwortlichkeiten
	Hinweis: Die Rolle „Firewall-Administrator“ enthält die Rolle „Firewall-Benutzer“. Diese Rolle wird nicht automatisch mit der Rolle „discovery_admin“ gewährt und muss dem Benutzer explizit zugewiesen werden.
Firewall-Anwender [sn_disco_firewall.firewall_user]	Verantwortlich für die schreibgeschützte Anzeige von Firewall-Dashboards und -Richtlinien. **Hinweis:** Diese Rolle enthält die Rolle „Firewall-Anforderer“.
Firewall-Anforderer [sn_disco_firewall.firewall_requester]	Verantwortlich für das Anfordern neuer Firewall-Regeln über Servicekatalog.

Firewall-Audits und Reporting konfigurieren

Richten Sie den Prozess ein, um Einblicke in das Erkennen und Kompilieren eines Bestands von Firewall-Sicherheitsrichtlinien, Geräten, Gerätegruppen und Managerinformationen zu erhalten.

Konfiguration – Übersicht

Bevor Sie Firewall-Audits und Reportingverwenden, müssen Sie die erforderlichen Plugins einrichten, die Aktivierung sicherstellen, Ihre Instanz auf die neueste Version aktualisieren und die Anwendung Firewall-Audits und Reporting von ServiceNow Storeherunterladen. Weitere Einzelheiten finden Sie unter Erste Schritte mit Firewall-Audits und Reporting.

Nachdem die Voraussetzungen erfüllt sind, können Sie mit den folgenden Aufgaben fortfahren.

Firewall-Audits und Reporting Aufgaben

Aufgabe	Beschreibung
Firewall-Richtlinien erkennen	Erkennen Sie Firewall-Richtlinien, einschließlich des Aufdeckens von Firewall-Geräten, -Richtlinien und Besitzergruppen, um eine zentralisierte Ansicht des Footprints zu gewährleisten.
Firewall-Audits und Reporting anpassen	Passen Sie Firewall-Audits und Reporting an, indem Sie die Eigenschaften Discovery von ändern, um bestimmte Aspekte anzupassen.
Firewall-Regelaudits, Regelanforderungen und Auditaufgaben archivieren	Verbessern Sie die Systemleistung, indem Sie Firewall-Regelanforderungen, Audit-Anforderungen und Audit-Aufgaben archivieren, die älter als ein bestimmter Zeitraum sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Firewall-Audits und Reporting Aufgaben (Fortsetzung)

Aufgabe	Beschreibung
Auditanforderung initiieren	Initiieren Sie Audits für einen bestimmten Firewall-Manager oder ein bestimmtes Gerät, um die Einhaltung der Sicherheitsrichtlinien ihrer Organisation sicherzustellen.

Erste Schritte mit Firewall-Audits und Reporting

Bevor Sie sich mit den Funktionen Firewall-Audits und Reporting von vertraut machen, müssen Sie die erforderlichen Anforderungen erfüllen, indem Sie das Plugin „“ installieren und aktivieren, Ihre Instanz aktualisieren und die Anwendung von ServiceNow Storeabrufen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Im ServiceNow Store werden regelmäßig neue Anwendungen und Updates für die von ServiceNow erstellten Anwendungen veröffentlicht. Wenn Sie bereits über die Anwendung verfügen, können Sie die neueste Version herunterladen, um Ihre bestehende Experience mit unseren Produkten zu verbessern. Da bei jeder Veröffentlichung einer Anwendung im Store neue Funktionen verfügbar sind oder Funktionen erweitert wurden, werden die in einem bestimmten Release verfügbaren Inhalte und Features in der Dokumentation mit der Versionsnummer angegeben.

Prozedur

1. Stellen Sie sicher, dass die folgenden Plugins installiert und aktiviert sind.
   - ITOM-Transparenz Plugin „“ [com.snc.itom.vis.license]
   - Plugin Discovery [com.snc.discovery]
   - Configuration Management for Scoped Apps (CMDB) [com.snc.cmdb.scoped]
2. Vergewissern Sie sich, dass Ihr System auf Yokohama oder höher aktualisiert wurde. Während des Upgrade-Prozesses wird das Plugin Firewall-Audits und Reporting [com.sn_disco_firewall] automatisch installiert, wenn die Plugins ITOM-Transparenz [com.snc.itom.vis.license] und Discovery [com.snc.discovery] bereits installiert sind.
3. Laden Sie die Anwendung Firewall-Audits und Reporting von ServiceNow Storeherunter.

Transparenz des Firewall-Bestands

Mit der Anwendung Firewall-Audits und Reporting können Sie Ihre Firewall-Sicherheitsrichtlinien, -Geräte, -Gerätegruppen und -Managerinformationen erkennen und inventarisieren.

ServiceNow Platform hilft Unternehmen dabei, mithilfe der zentralisierten Configuration Management Database (CMDB) den Überblick über ihre IT-Ressourcen zu behalten und Workflows für Anforderungs- und Change-Management-Prozesse zu automatisieren. Die Anwendung Firewall-Audits und Reporting ermöglicht Sicherheitsteams, alle Firewalls zusammen mit den zugehörigen Richtlinien, Firmware-Versionen und anderen Hardwareattributen zu erkennen. Das Serviceportal von ITSM hilft Kunden, Workflows zu digitalisieren, wenn sie neue Firewall-Regeln anfordern. In Kombination mit Incident Management- und Change-Management-Workflows von ITSM ermöglicht diese Lösung Transparenz im Erfüllungsprozess. Um Teams die Arbeit zu erleichtern, sind der Systembenutzer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und die Systemgruppen in der ServiceNow Platform für Richtlinien verantwortlich. Ein zentrales Dashboard bietet den Überblick über die Firewall-Umgebung und umfassende Transparenz über den Zustrom von Anforderungsdatensätzen, die in der Erfüllungswarteschlange des Firewall-Administrators landen.

Derzeit arbeitet ServiceNow mit Palo Alto Networks Panorama. In zukünftigen Versionen werden weitere Firewall-Anbieter hinzugefügt. Die Integration verwendet REST APIs und SNMP, um Firewall-Audits und Reporting mit dem Firewall-Bestand und den Firewall-Richtlinien zu verbinden.

Firewall-Richtlinien erkennen

Als Mitglied eines Sicherheitsteams können Sie Firewall-Geräte, -Richtlinien und -Besitzergruppen erkennen und erhalten so einen zentralen Überblick über den Footprint. Diese Daten werden in der ServiceNow CMDB aktualisiert. Richten Sie einen Zeitplan ein, um Ihre Firewall-Richtlinien zu erkennen, damit Sie die wertvollen Informationen Ihres Unternehmens im Auge behalten können.

Vorbereitungen

Erforderliche Rolle: admin oder discovery_admin

Für die Panorama-Integration benötigen Sie die Rolle „Superuser“ (schreibgeschützt).

Warum und wann dieser Vorgang ausgeführt wird

Administratoren, die für Discovery verantwortlich sind, können einen wiederkehrenden Zeitplan für die Discovery von Firewall-Richtlinien Palo Alto Networks für einrichten. Dieser Zeitplan nutzt das serverlose Muster und stellt eine Verbindung mit dem Palo Alto Firewall Manager her, um Informationen für die folgenden vier Configuration Items (CIs) in CMDBzu erkennen und zu aktualisieren.

- Panorama-Firewallmanager [cmdb_ci_firewall_manager_landschaft]
- Palo Alto-Firewall-Geräte [cmdb_ci_firewall_device_palo_alto]
- Panorama-Firewall-Gerätegruppe [cmdb_ci_firewall_device_group_landschaft]
- Panorama-Firewall-Sicherheitsrichtlinien [cmdb_ci_firewall_sec_policy_landschaft]

Prozedur

1. Erstellen Sie einen neuen Alias für Anmeldeinformationen vom Typ **„API-Schlüssel-Anmeldeinformationen“,** und **übermitteln Sie** die Anmeldeinformationen.
2. Geben Sie den API-Schlüssel für Panorama ein.
   Weitere Informationen hierzu finden Sie unter Aliasse für Anmeldeinformationen für Discovery .
3. Um einen Zeitplan Discovery zu erstellen, führen Sie die folgenden Schritte aus.
   a. Wählen Sie **Erkennen: Ohne Server**.
   b. Wählen Sie den entsprechenden **MID-Server**aus.
   c. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.
   Weitere Informationen zum Zeitplan Discovery finden Sie unter Horizontal-Discovery planen.
4. Wählen Sie auf der Registerkarte unten auf dem Bildschirm das Muster Ausführung ohne Server und dann **Neu**aus.
5. Führen Sie im Muster „Serverless Execution“ (Serverlose Ausführung) die folgenden Schritte aus.
   a. Geben Sie einen Namen ein.
   b. Wählen Sie **PaloAlto – Firewall Manager**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie **Untergeordnete Muster ausführen**aus.

d. Wählen Sie **Absenden**.

6. Navigieren Sie zu **Discovery Muster Startprogramm Parameter** und legen Sie die folgenden drei Parameter fest.
   - CredentialAlias: Geben Sie den neuen Aliasnamen für Anmeldeinformationen an, der in Schritt 1 erstellt wurde.
   - TrustInsecureHosts: Auf **„wahr“** setzen, um den Handshake zu umgehen.
   - URL: Geben Sie die Basis-URL des Panorama-Geräts ein.

     Beispiel: https://<PANORAMA_HOST>/api

7. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.

Firewall-Audits und Reporting anpassen

Ändern Sie die Discovery-Eigenschaften, um einige Aspekte von Firewall-Audits und Reporting anzupassen.

Vorbereitungen
Erforderliche Rolle: admin oder discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Discovery-Eigenschaften verwalten verschiedene Aspekte des horizontalen Discovery-Prozesses. In diesem Verfahren wird erläutert, wie Standardnamen für Richtlinienbesitzer- und Genehmigungsgruppen zum Genehmigen von Firewall-Regelaufgaben zugewiesen werden.

Prozedur

1. Um Discovery-Eigenschaftenzu bearbeiten, navigieren Sie zu **Alle** > **Discovery-Definition** > **Eigenschaften**.
   Weitere Informationen zu Eigenschaften finden Sie unter Discovery-Eigenschaften.
   - sn_disco_firewall.default.rule.task.policy.owner.group: Name Ihrer standardmäßigen Aufgabenbesitzergruppe
   - sn_disco_firewall.default.rule.task.approval.group: Name Ihrer standardmäßigen Genehmigungsgruppe
2. Bearbeiten Sie die Eigenschaften nach Bedarf.
   - sn_disco_firewall.default.rule.task.policy.owner.group: Name Ihrer standardmäßigen Aufgabenbesitzergruppe
   - sn_disco_firewall.default.rule.task.approval.group: Name Ihrer standardmäßigen Genehmigungsgruppe

   Diese Funktion spart Zeit, indem Ihre Standardbesitzergruppe und Genehmigungsgruppe in Anforderungen automatisch ausgefüllt werden.

Firewall-Regelaudits, Regelanforderungen und Auditaufgaben archivieren

Archivieren Sie Firewall-Regelanforderungen, Auditanforderungen und Auditaufgaben, die älter als ein bestimmter Zeitraum sind, um die Systemperformance zu verbessern. Sie können sie zu einem späteren Zeitpunkt vollständig aus der Archivtabelle löschen, um die Größe dieser Tabelle zu verringern.

Vorbereitungen
Stellen Sie sicher, dass das Plugin „Data Archiver“ [com.glide.uxdb] aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: firewall_admin

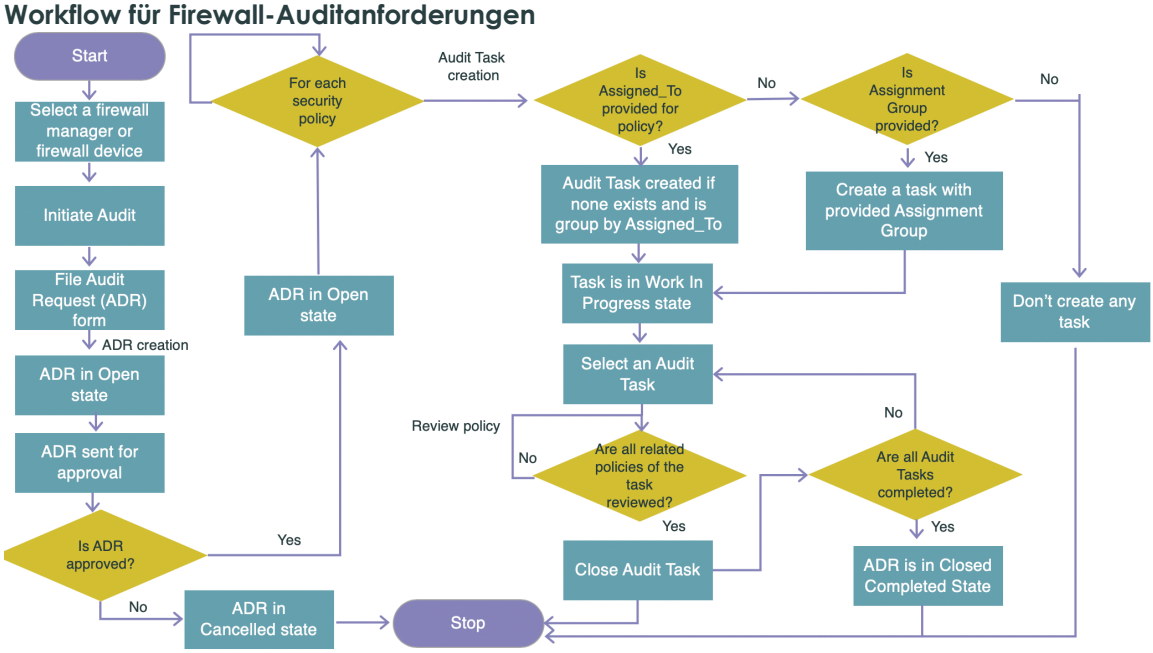
Prozedur

1. Aktivieren Sie mindestens eine **Firewall-Archivierungsregel**.
   Die folgenden Archivierungsregeln gehören zum Lieferumfang der Anwendung Firewall-Audits und Reporting, sind jedoch standardmäßig inaktiv. Um Regeln zu verwenden, müssen Sie sie aktivieren.
   - Archive Firewall Audit Request
   - Archival Firewall Audit Request Security Policy M2M
   - Archive Firewall Audit Task
   - Archival Firewall Audit Task Security Policy M2M
   - Archive Firewall Rule Task
   - Archival Firewall Rule Task Security Policy M2M
2. Navigieren zu **Archivregeln** > **Wählen Sie eine Firewall-Archivregel aus**.
3. Aktivieren Sie die Checkbox **Aktiv**.
   Das Plugin „Data Archiver“ [com.glide.auxdb] verschiebt täglich nicht mehr benötigte Daten aus primären Tabellen in einen Satz von Archivtabellen. Es sucht und archiviert Anforderungen und Aufgaben basierend auf der aktivierten und ausgewählten Archivierungsregel. Die Regel archiviert Daten aus der Primärtabelle, wenn die folgenden beiden Bedingungen erfüllt sind:
   - Status „Geschlossen - vollständig“
   - Aktualisiert vor mehr als 12 Monaten

Firewall-Audits

Firewall-Audits und Reporting bietet ein flexibles Audit-Framework, um den Besitz von Firewall-Richtlinien und die Notwendigkeit einer Firewall-Richtlinie nachzuverfolgen. Sie können ein zufälliges Audit auslösen, um Ihre Sicherheitshygiene für die Firewall-Richtlinie und den Besitz zu messen, sowie regelmäßig proaktive Audits durchführen.

Workflow für Firewall-Auditanforderungen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auditanforderung initiieren

Initiieren Sie Audits für einen bestimmten Firewall-Manager oder ein bestimmtes Gerät, um sicherzustellen, dass die Konfiguration den Sicherheitsrichtlinien Ihres Unternehmens entspricht.

Vorbereitungen

Erforderliche Rolle: firewall_admin

Prozedur

1. Um alle erkannten Firewall-Manager in Ihrem Netzwerk aufzulisten, navigieren Sie zu **Alle** > **Firewall-Audits und Reporting** > **Datensätze** > **Geräte oder Manager**.
2. Wählen Sie in der Liste den CI-Datensatz eines Firewall-Managers oder einen Gerätedatensatz aus.
3. Wählen Sie **Audit-Anforderung initiieren aus**.
4. Füllen Sie die Pflichtfelder im Formular aus.
5. Wählen Sie **Absenden**.

Nächste Maßnahme

Das Verfahren initiiert eine Audit für den Firewall-Manager, validiert sie und übermittelt die Audit-Aufgabe. Firewall-Audit-Aufgaben werden basierend auf dem Benutzer generiert, der der Firewall-Sicherheitsrichtlinie zugewiesen ist. Wenn in der Richtlinie kein festgelegter Benutzer angegeben ist, wird für diese Sicherheitsrichtlinie keine Audit-Aufgabe erstellt, und sie wird im Feld *`Excluded Policy List`* für Audit-Anforderungen platziert.

Daraufhin wird ein Audit für den Firewall-Manager angefordert, validiert und übermittelt. Firewall-Auditaufgaben werden auf Grundlage eines zugewiesenen Benutzers für die Firewall-Sicherheitsrichtlinie erstellt. Wenn die Richtlinie keinem Benutzer zugewiesen ist, wird keine Auditaufgabe für diese Sicherheitsrichtlinie erstellt, und sie wird der *`Excluded Policy List`* der Auditanforderungen hinzugefügt.

- Wenn *`Assigned To`* angegeben wird, wird die Audit-Aufgabe vom zugewiesenen Benutzer erstellt und gruppiert.
- Wenn *`Assigned To`* nicht angegeben ist und die Discovery-Eigenschaft *`sn_disco_firewall.default.rule.task.policy.owner.group`* nicht festgelegt ist, wird die Richtlinie zur Liste *`Excluded Policies`* hinzugefügt und es wird keine Audit-Aufgabe generiert.
- Wenn *`Assigned To`* nicht angegeben wird, aber die Discovery-Eigenschaft *`sn_disco_firewall.default.rule.task.policy.owner.group`* konfiguriert ist, wird die Audit-Aufgabe von der **Zuweisungsgruppe**erstellt und gruppiert.

Um zu überprüfen, ob die Audit-Aufgabe angefordert wurde, navigieren Sie zu **Audits** > **Audit-Anforderung**. Ihre Aufgabe sollte in der Liste angezeigt werden. Die Erstellung von Auditaufgaben findet im Hintergrund mit Subflows statt. Je nach Anzahl der Richtlinien müssen Sie möglicherweise warten, bis Auditaufgaben erstellt werden.

Die *`Assigned To`*-Person prüft alle in der zugehörigen Liste enthaltenen Richtlinien. Sie wählt die Aktion für jede Richtlinie aus und markiert die Aufgabe als *`Close Complete`*.

Firewall-Audits und Reporting verwenden

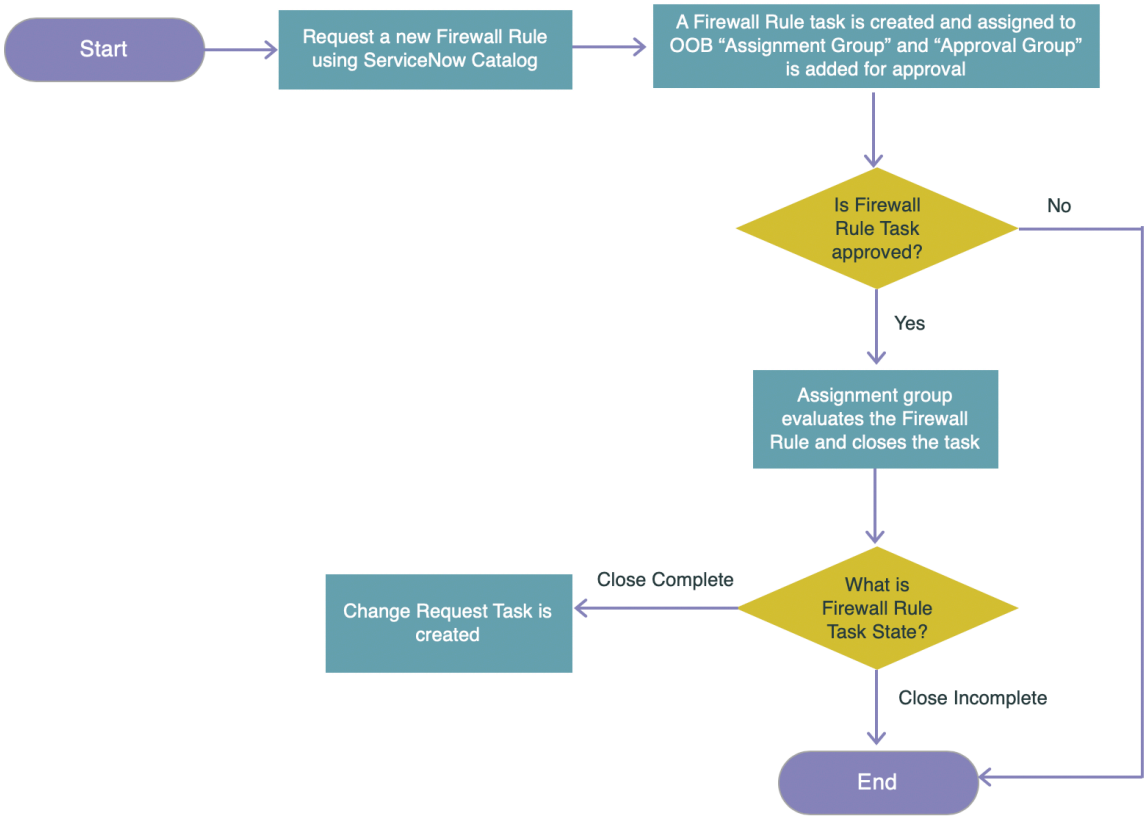
Firewall-Audits und Reporting ist eine leistungsstarke Anwendung zum Anfordern neuer Firewall-Regeln, wodurch die Verwaltung von IP-Adressen optimiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Firewall-Regelanforderungen

Verwenden Sie Servicekatalog, um neue Firewall-Richtlinien und -Regeln anzufordern.

Workflow zur Anforderung einer Firewall-Regel



Neue Firewall-Regel anfordern

Fordern Sie mit Servicekatalog eine neue Firewall-Regel an, um verschiedene IP-Adressen zu verwalten, die Netzwerksicherheit zu erhöhen und die sich ändernden Geschäftsanforderungen zu berücksichtigen.

Vorbereitungen

Stellen Sie sicher, dass der Katalog für Firewall-Audits und Reporting aktiviert ist.

Erforderliche Rolle: firewall_admin

Warum und wann dieser Vorgang ausgeführt wird

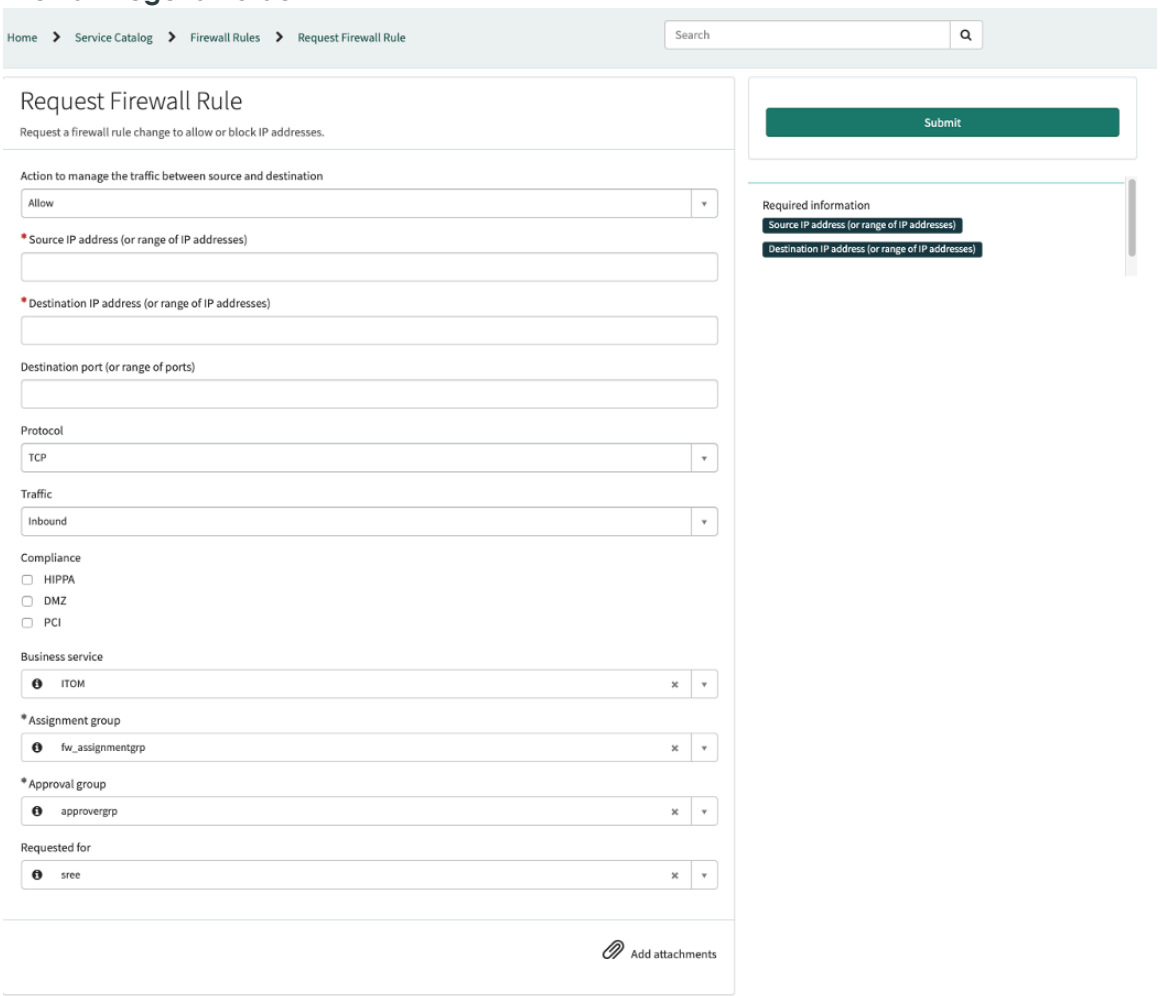
Administratoren initiieren Aufgaben, die automatisch zur Bewertung und Genehmigung an das Risikoteam weitergeleitet werden. Nach der Genehmigung implementieren Firewall-Administratoren reibungslos Changes, die alle durch automatisierte Workflows orchestriert werden.

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Firewall-Regeln**.
2. Wählen Sie **Firewall-Regel anfordern aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Firewall-Regel anfordern



3. Geben Sie die entsprechenden Informationen für die folgenden Pflichtfelder ein.

   - Source IP address (Quell-IP-Adresse)
   - Destination IP address (Ziel-IP-Adresse)
   - Zuweisungsgruppe

     Muss die Rolle *sn_disco_firewall.firewall_user* aufweisen.
   - Genehmigungsgruppe

     Muss die Rolle *approver_user* aufweisen.

4. Geben Sie die erforderlichen Details ein, oder wählen Sie sie aus.
5. Wählen Sie **Absenden**.
   Die Firewall-Regelaufgabe wird erstellt.

Nächste Maßnahme
Um die neue Regelaufgabe zu überprüfen, navigieren Sie zu **Regelanforderungen** > **Regelanforderungsaufgabe**. Ihre Anforderung sollte in der Liste sichtbar sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Firewall-Anforderungen genehmigen

Die Genehmigung von Firewall-Anforderungen gewährleistet kontrollierten Zugriff und Compliance, wobei Mitglieder der Genehmigergruppe befugt sind, Firewall-Audits und neue Firewall-Anforderungen zu überprüfen und zu genehmigen.

Vorbereitungen

Erforderliche Rolle: Mitglieder der angegebenen Genehmigergruppe **„approval_group“**, die in der Regelaufgabe angegeben ist.

Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Meine Genehmigungen**.
2. Wählen Sie das grüne Häkchen aus, um zu genehmigen.

Ergebnisse

- Die Zuweisungsgruppe bearbeitet dann die Anforderung und markiert sie als *`Close Complete`*.
- Sobald die assignment_group die Anforderung als *`Close Complete`* markiert hat, wird ein Subflow im Hintergrund ausgeführt, um eine Change-Anforderung zu erstellen, falls das Plugin „Change Request“ aktiviert ist.

> **Hinweis:** Die Change-Anforderung wird nur erstellt, wenn die Regelaufgabe *`Approved`* ist und den Status *`Close Complete`* aufweist.

Die Sicherheitsrichtlinie für Firewall-Regelaufgaben M2M entspricht der zugehörigen Liste *`Security policies`* in *`Rule task`*. Firewall-Administratoren können die Felder *`description`* und *`tag`* in einer Sicherheitsrichtlinie auf einem Panorama-Gerät hinzufügen. Sie können beim Erstellen oder Ändern von Sicherheitsrichtlinien in Panorama auch Firewall-Regelaufgabennummern und Change-Anforderungsnummern hinzufügen. Wenn die nächste Erkennung ausgeführt wird, füllt die M2M-Tabelle die Zuordnung zwischen:

- Firewall-Regelaufgabe und Firewall-Sicherheitsrichtlinie
- Firewall-Sicherheitsrichtlinie und Business Service, wenn der Business Service während der Firewall-Regelaufgabenanforderung bereitgestellt wird

Firewall-Audits und Reporting – Referenz

Referenzthemen enthalten zusätzliche Informationen zu den -Komponenten Firewall-Audits und Reporting, einschließlich Dashboards und Berichtskalibrierung.

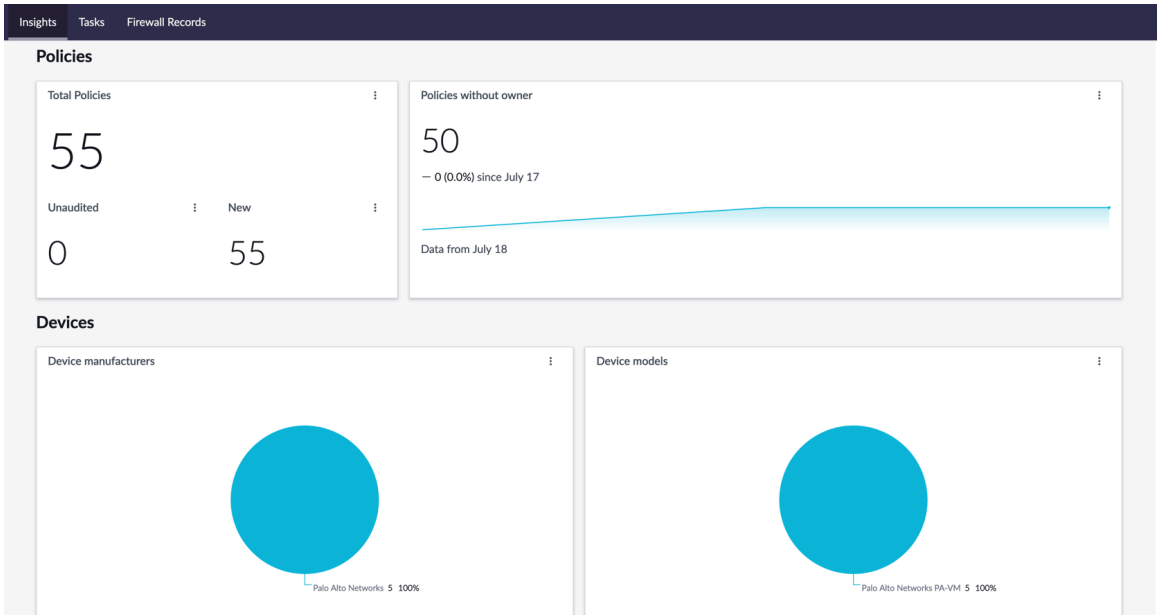
Dashboard des Firewall-Administratorarbeitsbereichs

Über das einheitliche Dashboard können Sicherheits- und Risikoteams Aufgaben, Change-Anforderungen und den gesamten Lebenszyklus des Firewall-Bestands überwachen und täglich oder manuell aktualisieren, um genaue und aktuelle Informationen zu erhalten.

Registerkarte „Firewall Insights (Firewall-Erkenntnisse)“

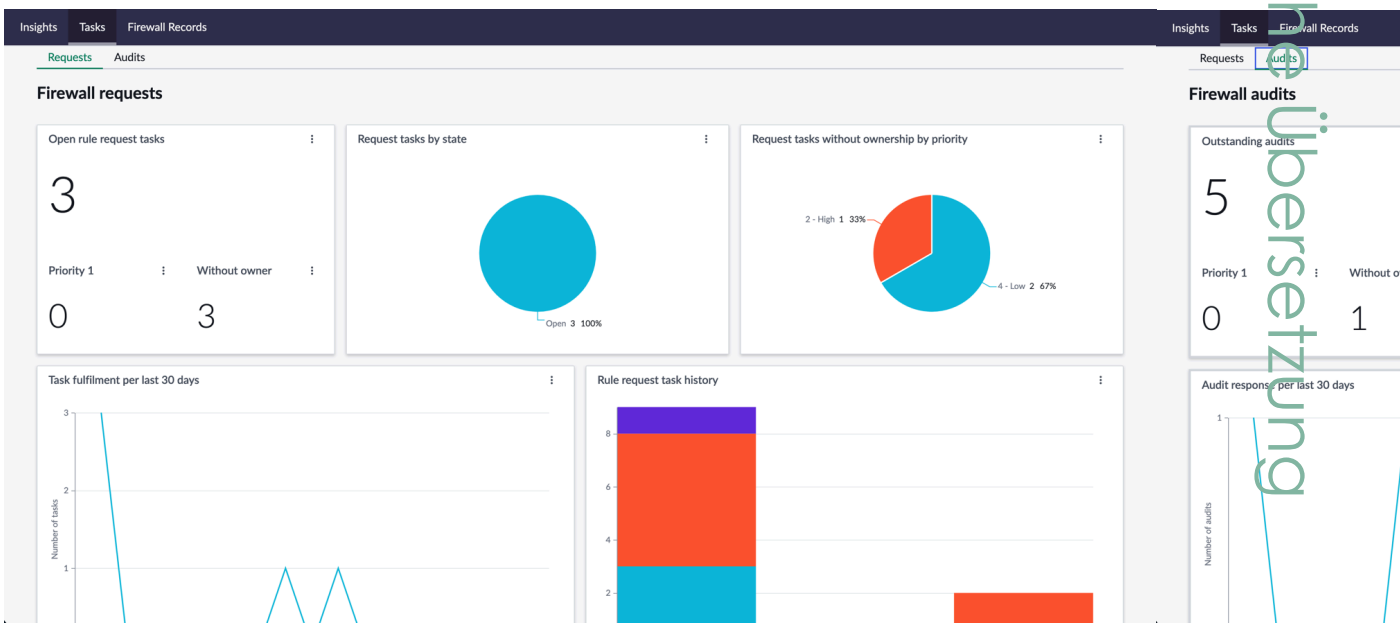
Die Registerkarte **„Einblicke“** bietet einen Snapshot von Firewall-Richtlinien und zugehörigen Geräten und zeigt Trends bei Richtlinien ohne Besitzer im Zeitverlauf. Verfolgen Sie neue und nicht geprüfte Richtlinien, und zeigen Sie die Verteilung von Geräteherstellern und -modellen innerhalb des Netzwerks an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Registerkarte „Requests and Audits (Anforderungen und Audits)“

Erkunden Sie auf der Registerkarte **Aufgaben** die Unterregisterkarten **Anforderungen** und **Audits**. Die Registerkarte **„Anforderungen** “ enthält Aufgliederungen der Anforderungsaufgaben nach Status und Eigentümer sowie die Erfüllungstrends im Zeitverlauf. In ähnlicher Weise werden auf der Registerkarte **Audits** ausstehende Audits nach Status und Verantwortlichkeit sowie Antworttrends im Zeitverlauf angezeigt.

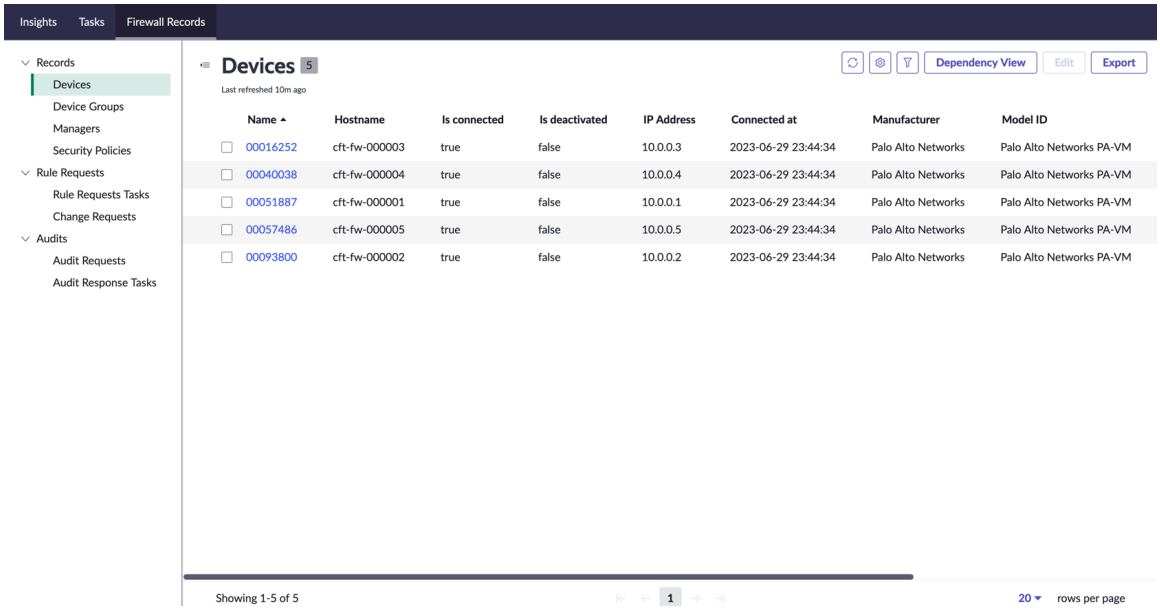


Registerkarte „Firewall-Datensätze“.

Die Registerkarte **„Firewall-Datensätze“** bietet konsolidierten Zugriff auf die Tabellen „Datensätze“, „Regelanforderungen“ und „Audits“. Benutzer können einzelne oder Gruppen von Datensätzen filtern, bearbeiten und exportieren. Die Unterregisterkarten **„Geräte“** und **„Sicherheitsrichtlinie“** enthalten eine Abhängigkeitsanzeige für ausgewählte Datensätze.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Endanwender und Rollen

Endanwender und Ziel	Erforderliche Rolle
Risikoteams	firewall_admin oder firewall_user
Sicherheit	firewall_admin oder firewall_user

Anwendungsfall

Um das Dashboard manuell zu aktualisieren, navigieren Sie zu **Performance Analytics** > **Datenerfasser** > **Aufträge** und wählen Sie **Firewall Scheduled Job (Geplante Firewall-Aufgabe)**. Öffnen Sie den Datensatz, und wählen Sie **Jetzt ausführen**, um die Dashboard-Elemente mit den neuesten Informationen zu aktualisieren.

Kalibrierung von Firewall-Audits und Reporting

Weitere Informationen zur Firewall-Audits und Reporting -Kalibrierung finden Sie im bereitgestellten Material.

Firewall-Audits und Reportingpattern

Palo Alto Firewall Manager

Dieses serverlose Muster nutzt die Funktion für große Nutzlast zur Beibehaltung von Sicherheitsrichtlinien. Discovery-Administratoren können einen Zeitplan mit diesem Muster erstellen. Wenn **„Untergeordnete Muster ausführen“** aktiviert ist, werden die folgenden untergeordneten Muster automatisch in der angegebenen Reihenfolge ausgeführt:

- Palo Alto Firewall Manager
- Palo Alto Firewall Devices
- Palo Alto Firewall Device groups
- Palo Alto Panorama Security policies

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennungen im Netzwerk ausführen

Sie können Erkennungen über Zeitpläne oder Skripts ausführen, um Konfigurationselemente zu erstellen, Subnetze zu definieren oder Ressourcen in AWS- und Azure-Clouds zu erkennen.

Voraussetzungen für die MID Server-Konfiguration

Stellen Sie vor dem Erstellen eines Discovery-Zeitplans sicher, dass Ihre MID Server ordnungsgemäß konfiguriert sind.

- **Unterstützte Applikationen**: Wählen Sie die Anwendungen aus, die den MID Server verwenden dürfen. Sie können die Anwendungsoption **ALLE** verwenden, damit alle Anwendungen den MID Server verwenden können.
- **IP-Bereiche**: Definieren Sie die IP-Adressbereiche, die der MID Server scannen kann. Um MID Server-Treffer zu finden, muss der im Erkennungszeitplan konfigurierte IP-Bereich in die Bereiche fallen, die von einem oder mehreren MID Servern unterstützt werden.

  Hinweis: Um die Sicherheit zu verbessern, beschränken Sie den Bereich auf die IP-Adresse, über die Sie die Kontrolle haben, und schließen Sie unnötige Bereiche aus.

- **Fähigkeiten**: Erstellen Sie die Fähigkeiten, die der MID Server unterstützt. Sie können die Fähigkeitenoption **ALLE** verwenden, damit alle Anwendungen den MID Server verwenden können.

Voraussetzungen für die Discovery-Konfiguration

Stellen Sie sicher, dass Ihre MID Server sich auf den erkannten Geräten authentifizieren können und dass sie ordnungsgemäß Konfigurationselemente klassifizieren können.

- **Anmeldeinformationen**: Konfigurieren Sie die MID Server mit den Anmeldeinformationen, die sie für die Abfrage der Geräte im Netzwerk benötigen. Der MID Server testet alle verfügbaren Anmeldeinformationen auf jedem erkannten Gerät und erzeugt dann eine Affinität für alle erfolgreichen Anmeldeinformationen. Weitere Informationen hierzu finden Sie unter Anmeldeinformationsaffinität für Discovery und Orchestration .
- **Klassifizierungen**: Die in der Basisplattform bereitgestellten Geräte- und Prozessklassifizierungen reichen normalerweise aus. Erstellen Sie nach Bedarf Klassifizierungen für die Geräte, Prozesse und Anwendungen im Netzwerk, die nicht von den Standardklassifizierern abgedeckt werden.

Erste Schritte zur Ausführung einer Erkennung

1. Verwenden Sie die Discovery-Konfigurationskonsole, um mit der Erkennung zu beginnen. Die Konsole bietet Konfigurationsoptionen, mit denen Sie die Gerätetypen, Anwendungen, Softwaredateien und Software-CIs auswählen können, die Discovery erkennen soll. Wenn Sie ein CI auswählen, das vom Scannen ausgeschlossen werden soll, deaktiviert die Instanz die/den zugehörige(n) Probe oder Klassifizierer, die/den Discovery zum Identifizieren des CI verwendet. Informationen zu den ersten Schritten finden Sie unter Discovery Konfigurationskonsole.
2. Ermitteln Sie die Art der Erkennung, die ausgeführt werden soll:
   - Führen Sie eine CI-Erkennung aus, um die Geräte, Computer und Anwendungen in Ihrem Netzwerk zu ermitteln. Das ist die häufigste Art der Erkennung. Führen Sie die CI-Erkennung über den Erkennungszeitplan aus. Sie können einen wiederkehrenden Zeitplan einrichten oder eine Erkennung bei Bedarf ausführen. Der Erkennungszeitplan bietet auch Konfigurationsoptionen für MID Server und die Shazzam-Port-Probe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Führen Sie eine Netzwerkerkennung aus, um die internen IP-Netzwerke in Ihrer Organisation zu ermitteln. Wenn Sie die IP-Adressbereiche in Ihrem Netzwerk bereits kennen, ist die Netzwerkerkennung nicht erforderlich. Diese Erkennung ist für Organisationen konzipiert, die in ihren Netzwerken keine vollständigen Kenntnisse der für Discovery verfügbaren IP-Adressen haben.
- Führen Sie eine serverlose Erkennung aus, um Anwendungen auf Hostcomputern zu ermitteln, ohne zunächst den Host erkennen zu müssen. Die serverlose Erkennung basiert auf Infrastrukturmustern zum Untersuchen von CIs auf einem Host. Bei dieser Art von Erkennung werden die Scanphase und Klassifizierungsphase der Erkennung übersprungen. Zur Verwendung dieser Art von Erkennung benötigen Sie profunde Kenntnisse über Muster. Informationen zu ersten Schritten mit Mustern finden Sie unter Muster und horizontale Erkennung.

3. Nachdem Sie eine Erkennung ausgeführt haben, überwachen Sie die Ergebnisse der Erkennung, und beheben Sie gegebenenfalls auftretende Fehler:
   - Verwenden Sie den Erkennungsstatus, um eine Zusammenfassung einer Erkennung anzuzeigen und auf die ECC-Warteschlange zuzugreifen, die die Aktivität von Probes und Sensoren sowie die tatsächliche XML-Nutzlast anzeigt, die an eine oder von einer Instanz gesendet wird.
   - Verwenden Sie das Discovery-Dashboard, um laufende Discovery-Vorgänge zu überwachen.
   - Verwenden Sie die Discovery-Homepage, um auf Details über alle Zeitpläne, Cloud-Ressourcen (virtuelle Computer), erkannten Geräte und zugehörigen Fehler zuzugreifen, die möglicherweise aufgetreten sind. Die Fehlerdetails schließen mögliche Nachbesserungsschritte ein.

Zugehörige Informationen

Discovery-Ressourcennutzung

Discovery Konfigurationskonsole

Verwenden Sie die Discovery-Konfigurationskonsole, um zu bestimmen, welche Art von CIs und CI-Informationen Sie erkennen möchten.

Standardmäßig findet Discovery alle Informationen in Ihrem Netzwerk, die in Probes und Mustern angegeben sind. Verwenden Sie die Steuerelemente in dieser Konsole, um die Daten auszuwählen, die Discovery der CMDB hinzufügt, die Ihre Organisation benötigt. Sie können die folgenden Aspekte von Discovery steuern:

- Die Discovery ganzer CI-Typen, z. B. Windows -Server.
- Die Erkennung bestimmter CI-Details, wie z. B. Betriebssysteminformationen auf -Servern Windows.
- Die Discovery von ARP-Daten für Netzwerke, UNIXund Windows -Geräte.
- Erkennung von Softwarepaketen, die von Ihnen hinzugefügte Stichwortbegriffe enthalten, zum Beispiel Hotfix und Sicherheitsupdate
- Dateibasiert Discovery von Software auf UNIX und Windows nach bestimmter Erweiterung oder bestimmtem Ordner, z. B. .cert oder .ext.

Hinweis: Discovery gibt alle Daten vom Ziel an die Instanz zurück, bevor die Konsoleneinstellungen angewendet werden. Wenn die Instanz die CMDB aktualisiert, ignoriert sie alle ausgeschlossenen Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen und Zugänglichkeit

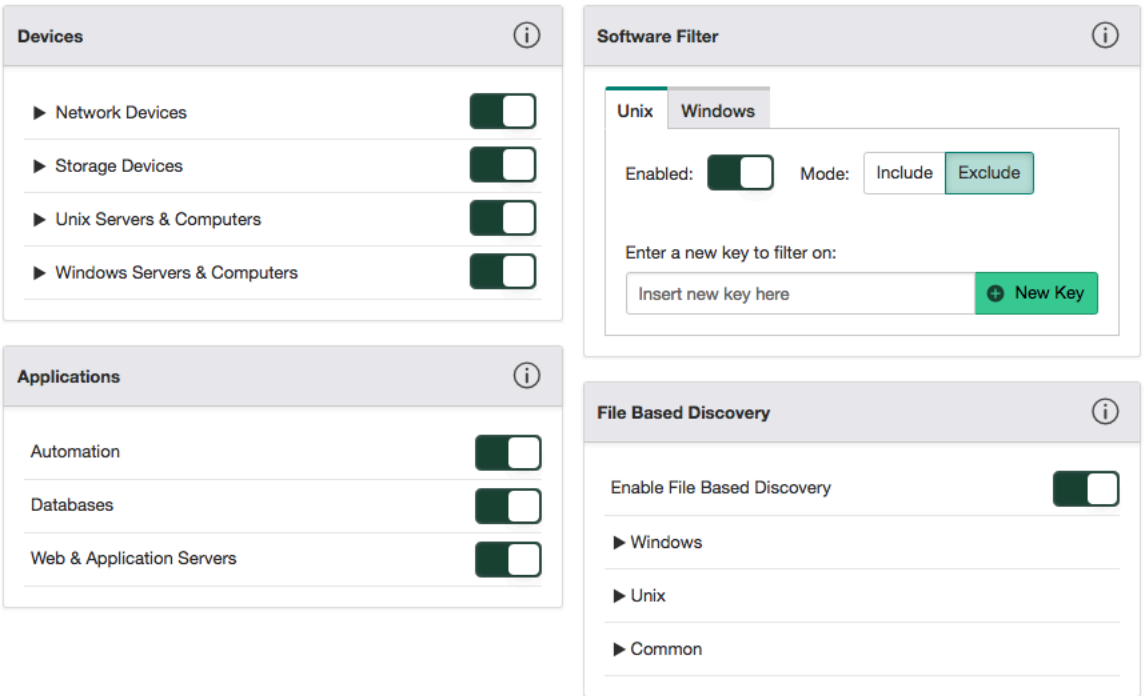
Wenn Sie Internet Explorer verwenden, müssen Sie Version 8 oder höher verwenden. Die Konfigurationskonsole unterstützt die Tastaturnavigation und Sprachausgabe.

Konsolenübersicht

Um die Konfigurationskonsole zu öffnen, navigieren Sie zu **Discovery-Definition** > **Konfigurationskonsole**.

Die Konsole ist in die folgenden Abschnitte unterteilt. Verwenden Sie die Umschalttasten, um verschiedene Optionen zu aktivieren (rechts zum Aktivieren, links zum Deaktivieren).

- **Geräte**: Netzwerkgeräte wie Drucker, Speichergeräte wie Speicher-Switches sowie Unix- und Windows-Computer
- **Anwendungen**: Automatisierungsanwendungen wie Puppet, Datenbanken wie MSSQL sowie Webserver wie Tomcat
- **Softwarefilter**: UNIX - und Windows -Anwendungen, die von Ihnen eingegebene Schlüsselwörter einbeziehen oder ausschließen
- **Dateibasierte Discovery**: Softwaredateien nach Pfad, Ordner und Erweiterungen, die gescannt oder ignoriert werden sollen



Geräteerkennung

Durch Deaktivieren der Erkennung von Gerätedaten auf oberster Ebene werden die zugehörigen Port-Probes und Musterbibliotheken deaktiviert. Beispielsweise wird durch das Blockieren von Netzwerkgeräten die Port-Probe „SNMP“ deaktiviert. Das Blockieren von Geräten auf der zweiten Ebene der Hierarchie hat folgende Auswirkungen:

- Geräteklassenkategorien deaktivieren Klassifizierer.
- Geräteinformationskategorien deaktivieren Probes und Musterbibliotheken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die Erkennung von ARP-Daten aktivieren oder deaktivieren. Diese Option ist standardmäßig deaktiviert. Nach dem Upgrade werden ARP-Daten nur erkannt, wenn Sie sie in der Discovery-Konfigurationskonsole aktivieren. ARP-Daten können in drei Geräteklassen gesteuert werden: Netzwerk, UNIXund Windows.

Mögliche Auswirkungen:

- Ohne ARP-Daten wird der Netzwerkpfad möglicherweise nicht untersucht, wenn Sie Service-Mapping mit L2 oder L3 Discoveryverwenden.
- Nach dem Upgrade und der erneuten Ausführung Discoveryvon werden die ARP-Daten für vorhandene Kunden nicht gefüllt. Alte Daten werden gemäß der Löschstrategie des sofort einsatzbereiten Verhaltens (OOB) automatisch gelöscht. Dies ist eine einmalige Aktivität, es sei denn, Sie ändern die OOB-Konfiguration. Daher müssen Sie Ihren Zeitplan Discovery basierend auf dem Gerätevolume ausführen.
- Wenn Sie die Netzwerkgeräte-Exploration für Netzwerkgeräte deaktiviert haben, sollten Sie auch ARP deaktiviert lassen, um das alte Verhalten vor dem Upgrade beizubehalten.

Anwendungserkennung

Die Deaktivierung der Erkennung von Anwendungsdaten wirkt sich auf alle Hostgeräte aus, auf denen die Anwendung ausgeführt wird. Wenn Sie beispielsweise Discovery so konfigurieren, dass -Datenbanken ignoriert werden, werden weder für Linux- noch für Windows -Datenbanken Informationen gesammelt. Wenn Sie das System hingegen so konfigurieren, dass ein Gerätetyp ignoriert wird, z. B. ein Windows -Server, werden die auf diesem Server ausgeführten Datenbanken nicht untersucht, auch wenn sie für die Erkennung konfiguriert sind. Die Instanz kann die auf einem Server ausgeführten Anwendungen erst identifizieren, nachdem sie diesen Server erkannt hat.

Wenn Sie ein Element aus dem Abschnitt **Applikationen** ausschließen, deaktiviert das System den entsprechenden Prozessklassifizierer. Die zu dieser Klassifizierung gehörenden Probes, einschließlich der Probe „Horizontal Pattern“, der Muster startet, werden nie gestartet.

Erkennung von Software

Sie können die Discovery von Softwarepaketen anhand der Stichwörter filtern, die sie für die Computer Windows und UNIX enthalten. Ein Stichwort kann ein beliebiger Begriff sein, der in einem Softwarepaketnamen enthalten ist. Stichwörter zum Filtern von Software werden in der Tabelle „Softwarefilterschlüssel“ [discovery_spkg_keys] gespeichert. Das System stellt keine Standardfilterschlüsselwörter für die Software UNIX bereit.

Wichtig: Die Softwarefilterung nach Stichwörtern erfolgt, nachdem die Probe ihre Nutzlast an die Instanz und nicht auf dem Zielhost zurückgegeben hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Standardschlüsselwörter werden für Windows bereitgestellt und standardmäßig herausgefiltert:

- Hotfix
- Sprachpaket
- Sicherheitsupdate

File-based Discovery

Sie können Discovery so konfigurieren, dass Pfade, Ordner und Erweiterungen für die dateibasierte Discovery gescannt oder ignoriert werden. Discovery scannt dann ein Windows - oder UNIX -Dateisystem mit diesen Einstellungen, um Dateifingerabdrücke zu identifizieren. Installierte Softwareprodukte, die mit diesen Attributen erkannt werden, werden mit Produkten in einer umfangreichen Bibliothek zur Softwarenormalisierung abgeglichen.

Auswirkungen auf Discovery-Tabellen

Diese Tabelle zeigt, was in Discovery-Tabellen deaktiviert ist, wenn Sie die Discovery-Konfigurationskonsole verwenden.

Bei Deaktivierung von	Deaktiviertes Feld
Gerätekategorien der obersten Ebene, zum Beispiel: • Netzwerkgeräte • Windows-Server und -Computer • Unix-Server und -Computer	In der Tabelle „Anschlussprobes“ [discovery_port_probe] ist das Feld **CIs** deaktiviert. Die Tabelle „Anschlussprobes“ [discovery_port_probe] wird aus der Tabelle „Protokollkategorie“ [discovery_category_protocol] referenziert.
Geräteklassen, zum Beispiel: • Windows 2008 Server • Linux-Server	In der Tabelle „Klassifizierer“ [discovery_classy] für den zugehörigen Klassifizierer ist das Feld **Aktiv** deaktiviert. Die Tabelle „Klassifizierer“ [discovery_classy] wird in der Tabelle „Geräteklassifizierungskategorie“ [discovery_category_device_class] referenziert.
Geräteinformationen, zum Beispiel: • Erkundung von Netzwerkgeräten • Windows-Speicher • ARP-Daten	Das Feld **Aktiv** ist in den Tabellen „Klassifiziererprobes“ [discovery_classifier_probe] und „ Discovery Muster [sa_pattern] für die zugehörige Probe bzw. das zugehörige Muster deaktiviert, die bzw. das die Identifizierung und Untersuchung des CI durchführt. Diese Tabellen werden von der Tabelle „Geräteinfokategorie“ [discovery_category_device_info] referenziert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bei Deaktivierung von	Deaktiviertes Feld
Applikationen	Das Feld **Aktiv** ist in der Tabelle „Prozessklassifizierer“ [discovery_classy] für den zugehörigen Prozessklassifizierer deaktiviert. Die Tabelle „Prozessklassifizierer“ [discovery_classy_proc] wird in der Tabelle „Anwendungskategorie“ [discovery_category_appl] referenziert.

Hinweis: Wenn Sie Muster für die Erkennung verwenden und die Erkennung von Geräteklassen oder Geräteinformationen deaktivieren, deaktiviert das System die Musterbibliotheken, die die Geräteinformationen sammeln. Wenn Sie beispielsweise über ein Muster Windows verfügen, in dem Sie eine gemeinsame Bibliothek erstellen, die BS-Informationen sammelt, und dann die Erfassung von BS-Daten deaktivieren, wird die gemeinsame Bibliothek, die BS-Daten sammelt, deaktiviert. Weitere Informationen zum Vorgang der gemeinsamen Bibliothek finden Sie unter KB1698521: Muster erstellen oder anpassen .

CIs aus der Erkennung ausschließen

Verwenden Sie die Discovery-Konfigurationskonsole, um zu bestimmen, welche Geräte und Anwendungen von der Erkennung ausgeschlossen werden sollen.

Vorbereitungen
Erforderliche Rolle: discovery_admin, admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Konfigurationskonsole**.
2. Wenn Sie bestimmte Geräte und Geräteinformationen ausschließen möchten, erweitern Sie die Kategorie für Gerätetypen.
3. Um zu sehen, welche Anwendungen sich deaktivieren lassen, bewegen Sie den Mauszeiger über den Anwendungstyp.
4. Klicken Sie auf den Umschalter, um die CIs zu deaktivieren, die Sie von der Erkennung ausschließen möchten.
   Die Instanz erstellt einen Update Set-Datensatz für alle Änderungen, die Sie an der Konsole vornehmen.

Zu erkennende Anwendungen und Geräte anpassen

Mithilfe der Discovery-Konfigurationskonsole können Sie Anwendungen und Geräte aktivieren und deaktivieren. Einige sind als sofort einsatzbereit aufgeführt, aber Sie können auch anpassen, welche spezifischen Anwendungen und Geräte Sie gemäß Ihren spezifischen Anforderungen in die Erkennung einschließen möchten.

Vorbereitungen
Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Passen Sie die Anwendungen an.
   a. Navigieren zu **Discovery-Definition** > **Anwendungskategorien**.
   b. Klicken Sie auf **Automatisierung**, **Datenbanken**oder **Web- und Anwendungsserver**.
   c. Entsperren Sie die Liste der Prozessklassifizierer.
   d. Um eine Anwendung aus der Liste zu entfernen, markieren Sie sie, und klicken Sie dann zum Entfernen auf **X**.
   e. Um sie der Liste hinzuzufügen, geben Sie den Namen in das Feld ein, und drücken Sie die **Eingabetaste**.
   f. Klicken Sie auf das **Schlosssymbol**.
   g. Klicken Sie auf **Aktualisieren**.
   Bei der nächsten Ausführung von Discovery werden die von Ihnen konfigurierten Typen spezifischer Anwendungen verarbeitet.
2. Passen Sie Geräte an.
   a. Navigieren zu **Discovery-Definition** > **Geräteinformationskategorien**.
   b. Um einen neuen Datensatz zu erstellen, klicken Sie auf **Neu**.
   c. Geben Sie die Details ein, und klicken Sie auf **Senden**.
   d. Um ein vorhandenes Gerät zu aktualisieren, klicken Sie auf eines der aufgelisteten Geräte.
   e. Nehmen Sie Änderungen vor, und klicken Sie auf **Aktualisieren** oder **Löschen**.

Zu erkennende Software filtern

Verwenden Sie die Discovery-Konfigurationskonsole, um die Software zu filtern, die Sie der CMDB hinzufügen.

Vorbereitungen

Erforderliche Rolle: discovery_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

Die Instanz erstellt einen Update Set-Datensatz für alle Änderungen, die Sie an der Konsole vornehmen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Konfigurationskonsole**.
2. Wählen Sie im Bereich „Softwarefilter“ die Registerkarte für das gewünschte Betriebssystem (**Unix** oder **Windows**) aus.
3. Fügen Sie Stichwörter zum Filtern von Softwarepaketen hinzu, bzw. löschen Sie sie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Um ein Stichwort hinzuzufügen, geben Sie es in das dafür vorgesehene Feld ein, und klicken Sie auf **Neuer Schlüssel**.

b. Um ein Stichwort zu löschen, klicken Sie auf das rote **x**-Symbol rechts neben dem Stichwort.

Discovery sucht nach Softwarepaketen, die diese Begriffe im ausgewählten Betriebssystem enthalten, und schließt sie entweder in die CMDB ein bzw. aus ihr aus. Zum Filtern von UNIX-Softwarepaketen stellt das System keine Standardstichwörter bereit, wohl aber für Windows:

- Hotfix
- Sprachpaket
- Sicherheitsupdate

4. Wählen Sie aus, ob Softwarepakete mit den Stichwörtern im Namen **einbezogen** oder **ausgeschlossen** werden sollen.
   - **Einbeziehen**: Es werden nur Softwarepakete hinzugefügt, die mit den Stichwörtern übereinstimmen.
   - **Ausschließen**: Es werden alle Softwarepakete hinzugefügt mit Ausnahme derjenigen, die mit den Stichwörtern übereinstimmen.
5. Deaktivieren Sie die Softwarefilterung für **UNIX** oder **Windows**.

   Wenn der Filter für ein Betriebssystem deaktiviert ist, werden alle erkannten Softwarepakete für dieses Betriebssystem der CMDB hinzugefügt, ohne dass eine Filterung stattfindet.

   Die Instanz erstellt einen Update Set-Datensatz für alle Änderungen, die Sie an der Konsole vornehmen.

Dateibasierte Discovery konfigurieren

Verwenden Sie die Discovery-Konfigurationskonsole zum Konfigurieren mehrerer Einstellungen, um Ihre gesamte installierte Software zu erkennen und zu verwalten.

Vorbereitungen

Erforderliche Rolle: discovery_admin, admin

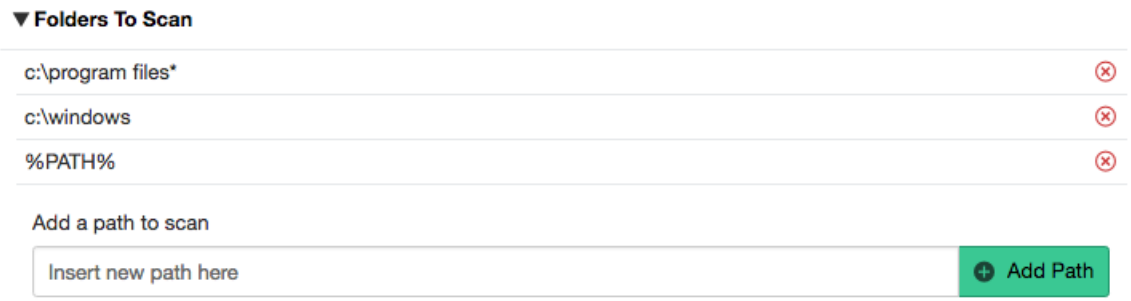
Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Konfigurationskonsole**.
2. Aktivieren Sie die File-based Discovery.
   Standardmäßig ist sie deaktiviert.
3. Wählen Sie anpassbare Optionen speziell für Windows- und UNIX-Computer sowie Optionen, die für beide Betriebssysteme gelten.
   Einige Optionen haben Standardwerte, andere (wie zu ignorierende Ordner und Erweiterungen) sind leer, bis Sie Werte hinzufügen.
4. Klicken Sie unter Windows und/oder UNIX auf den Pfeil, um die Zielpfadoptionen zu erweitern.
5. Konfigurieren Sie Standardoptionen.

   Zu scannende Ordner

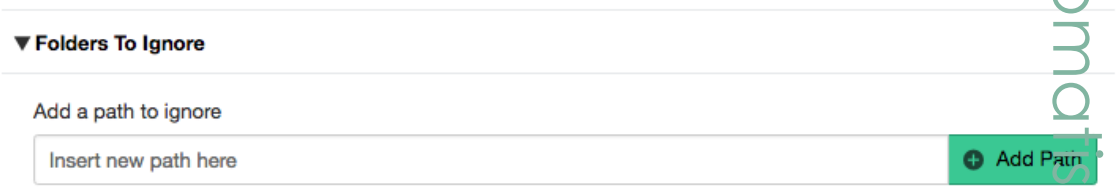
   Gibt an, nach welchen Ordnern unter Windows und/oder UNIX gescannt werden soll. Standardwerte werden aufgelistet. Sie können auch zusätzliche Pfade zum Scannen hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



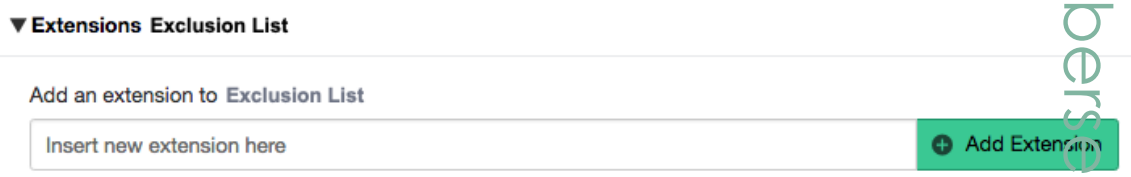
Zu ignorierende Ordner

Gibt an, welche Ordner und untergeordneten Ordner/Dateien in der Liste der zu scannenden Windows- oder UNIX-Ordner ignoriert werden sollen. Wenn Sie beispielsweise „C:\Programme“ als zu scannenden Ordner angegeben haben, können Sie zusätzlich „C:\Programme\Temp“ als zu ignorierenden Ordner angeben. Wenn die dateibasierte Discovery einen Windows-Server scannt, werden alle Dateien und Unterordner unter C:\Programme mit Ausnahme von C:\Programme\Temp gescannt.



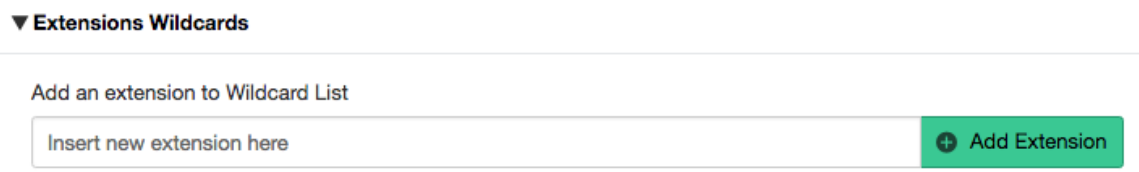
Ausschlussliste für Erweiterungen

Geben Sie Erweiterungen (.txt, .war, .exe usw.) an, die Sie für Windows ignorieren möchten.



Platzhalter für Erweiterungen

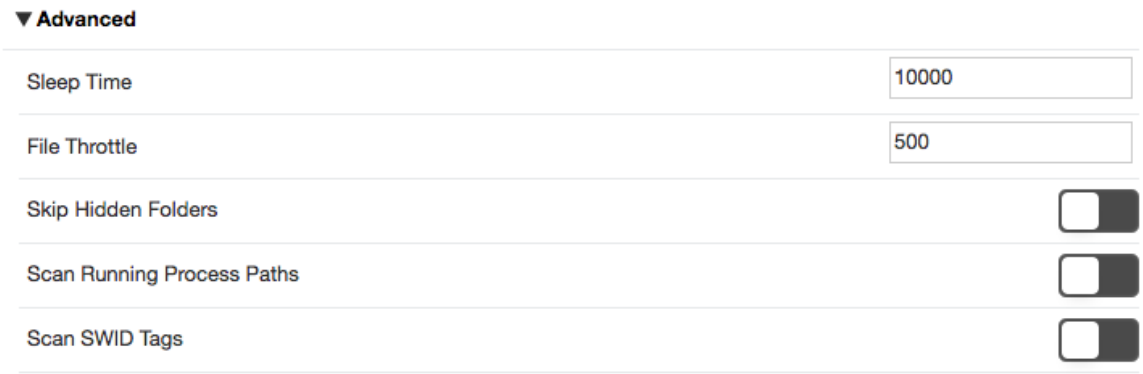
Geben Sie Erweiterungen (.cert, .crt usw.) an, nach denen Sie unter Windows immer scannen möchten. Dadurch können Sie nach Erweiterungen wie *.cert scannen, bei denen der Dateiname selbst möglicherweise nicht bekannt ist. Auf diese Weise können Sie Zertifikate (.cert oder .crt) und Java-Schlüsselspeicherdateien (.jks) erkennen.



6. Konfigurieren Sie **erweiterte Windows**-Einstellungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zeit Energiesparmodus

Legt die Dauer des Ruhezustands in Millisekunden während jedes Drosselintervalls beim Scannen nach Windows-Dateien fest. Der Standardwert ist 10000. Ändern Sie diesen Wert nur, wenn Sie ein fortgeschrittener Benutzer sind. Wenn Sie ein fortgeschrittener Benutzer sind und eine Änderung vornehmen müssen, stellen Sie sicher, dass Sie die Einstellung auf einen Wert ungleich 0 festlegen.

Dateidrosselung

Legt die Anzahl der Dateien fest, die vor dem Ruhezustand unter Windows gescannt werden soll. Der Standardwert ist 500. Ändern Sie diesen Wert nur, wenn Sie ein fortgeschrittener Benutzer sind. Wenn Sie ein fortgeschrittener Benutzer sind und eine Änderung vornehmen müssen, stellen Sie sicher, dass Sie die Einstellung auf einen Wert ungleich 0 festlegen.

Versteckte Ordner überspringen

Überspringt ausgeblendete Ordner auf Zielcomputern, wenn nach Dateisignaturen gesucht wird. Bei Windows-Geräten hängt die Sichtbarkeit eines Ordners von einem Ausgeblendet-Attribut ab, das für jeden Ordner festgelegt werden kann.

Laufende Prozesspfade scannen

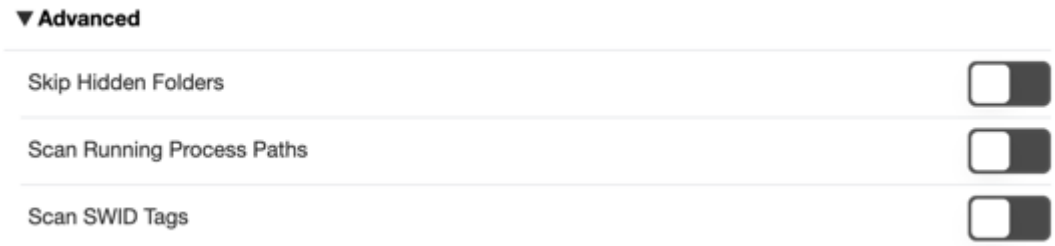
Aktiviert die Verwendung laufender Prozesspfade in der Liste der Zielpfade zum Scannen. Dadurch werden automatisch Pfade hinzugefügt, die bekanntermaßen laufende Prozesse enthalten und daher höchstwahrscheinlich Dateien von Interesse für die Bestimmung von Softwareinstallationen enthalten.

SWID-Tags Scannen

Scannt nach und analysiert SWID-Tags (Softwareidentifizierungs-Tags). Diese Option ist nur sichtbar, wenn SAMP aktiviert ist. Wenn „SWID-Tags Scannen“ aktiviert ist, werden das Softwareprodukt, der Herausgeber und die Version in der Nutzlast zurückgegeben, die direkt in die Softwareinstallationstabelle eingefügt wird, wobei die Software-Abgleich-API umgangen wird. Standardmäßig ist sie deaktiviert.

7. Konfigurieren Sie **erweiterte UNIX**-Einstellungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Versteckte Ordner überspringen

Überspringt ausgeblendete Ordner, wenn nach Dateisignaturen gesucht wird. Bei Unix-basierten Geräten sind dies Ordner, denen ein „.“ im Namen vorangestellt ist.

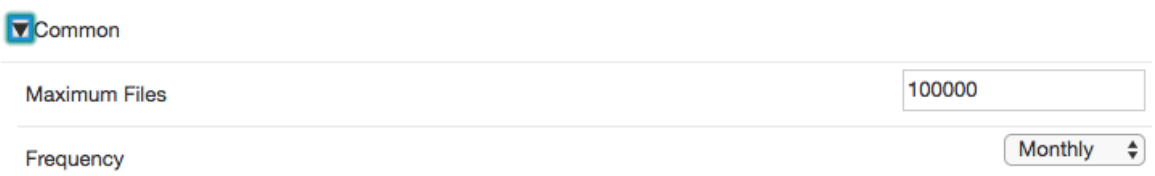
Laufende Prozesspfade scannen

Aktiviert die Verwendung laufender Prozesspfade in der Liste der Zielpfade zum Scannen. Dadurch werden automatisch Pfade hinzugefügt, die bekanntermaßen laufende Prozesse enthalten und daher höchstwahrscheinlich Dateien von Interesse für die Bestimmung von Softwareinstallationen enthalten.

SWID-Tags Scannen

Scannt nach und analysiert SWID-Tags (Softwareidentifizierungs-Tags). Diese Option ist nur sichtbar, wenn SAMP aktiviert ist. Wenn „SWID-Tags Scannen“ aktiviert ist, werden das Softwareprodukt, der Herausgeber und die Version in der Nutzlast zurückgegeben, die direkt in die Softwareinstallationstabelle eingefügt wird, wobei die Software-Abgleich-API umgangen wird. Standardmäßig ist sie deaktiviert.

8. Konfigurieren Sie **gemeinsame** Einstellungen für Windows oder UNIX.



Maximale Dateien

Legt die maximale Anzahl von Dateien fest, die erkannt werden sollen. Das ist die Anzahl der pro CI/IP gescannten Dateien.

Häufigkeit

Legt die Häufigkeit fest, mit der die dateibasierte Discovery für das CI ausgeführt wird.

Ergebnisse

Die dateibasierte Discovery ist jetzt aktiviert, konfiguriert und zur Ausführung bereit. Weitere Informationen finden Sie unter Dateibasierte Discovery ausführen.

Erstellen Sie Anmeldeinformationen für die Standardauthentifizierung

Erstellen Sie Anmeldeinformationen, um auf eine ServiceNow® -Instanz zuzugreifen.

Vorbereitungen

Erforderliche Rolle: system_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.
2. Wählen Sie **Neu**.
3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung**.
4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Anwendername	Name zum Identifizieren des Benutzers.
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: `100`

5. Wählen Sie **Absenden**.

Ergebnisse

Die Anmeldeinformationen für die Standardauthentifizierung zur Verwendung mit der Serverinstanz werden erstellt.

Horizontale Erkennung planen

Ein Discovery-Zeitplan bestimmt, wonach von der horizontalen Discovery gesucht wird, wann diese ausgeführt wird und welche MID Servers verwendet werden. Erstellen Sie einen Discovery -Zeitplan für Ihre lokale Umgebung oder einen Zeitplan zum Erkennen der -Ressourcen in Ihrem Cloud-Servicekonto.

Vorbereitungen

Stellen Sie sicher, dass Ihr Discovery-Zeitplan den bewährten Best Practices für Sicherheit entspricht, z. B. indem Sie den Bereich der Erkennungsziele beschränken und die sichersten Anmeldeinformationen verwenden.

Stellen Sie sicher, dass Sie Ihre Anmeldeinformationen testen , bevor Sie einen Zeitplan ausführen. Ungültige Anmeldeinformationen sind eine der Hauptursachen für fehlgeschlagene Erkennungen.

Erforderliche Rolle: admin, discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Mit einem Discovery-Zeitplan können Sie die horizontale Discovery starten, bei der Ihr Netzwerk mithilfe von Probes, Sensoren und Mustervorgängen nach CIs durchsucht wird. Verwenden Sie dieses Verfahren, um einen Zeitplan manuell über das Formular „Discovery-Zeitplan“ zu erstellen.

Service-Mapping bietet auch einen Discovery-Zeitplan für Discovery von oben nach unten. Weitere Informationen finden Sie unter Erkennung von oben nach unten mithilfe von Service-Mapping planen.

Verwenden Sie das Zeitplanmodul Discovery in der Anwendung Discovery für Folgendes:

- Konfigurieren Sie einen Zeitplan zum Erkennen von Ressourcen in Ihrem Cloud-Servicekonto.
- Konfigurieren Sie einen Zeitplan zum Erkennen von Zertifikaten aus URL-Scans.
- Konfigurieren Sie die Geräteidentifikation nach IP-Adresse oder anderen Kennungen.
- Stellen Sie fest, ob Anmeldeinformationen in Geräte-Probes verwendet werden.
- Benennen Sie den MID-Server, der für einen bestimmten Typ von Discovery verwendet werden soll.
- Erstellen oder deaktivieren Sie einen Zeitplan, mit dem gesteuert wird, wann die Discovery in Ihrem Netzwerk ausgeführt wird.
- Konfigurieren Sie die Verwendung mehrerer Shazzam-Probes für den Lastenausgleich.
- Konfigurieren Sie die Verwendung mehrerer MID Servers für den Lastausgleich.
- Führen Sie einen Discovery -Zeitplan manuell aus.
- Führen Sie Discovery für eine einzelne IP-Adresse aus.

Hinweis: Um die Ausführungsergebnisse Ihrer Zeitpläne sowohl für die IP-basierte als auch für Cloud-Discovery anzuzeigen, verwenden Sie die Zusammenfassungen auf der Discovery-Homepage. Die Homepage veröffentlicht die Details aller möglicherweise aufgetretenen Fehler und zeigt mögliche Aktionen zur Behebung von Problemen an.

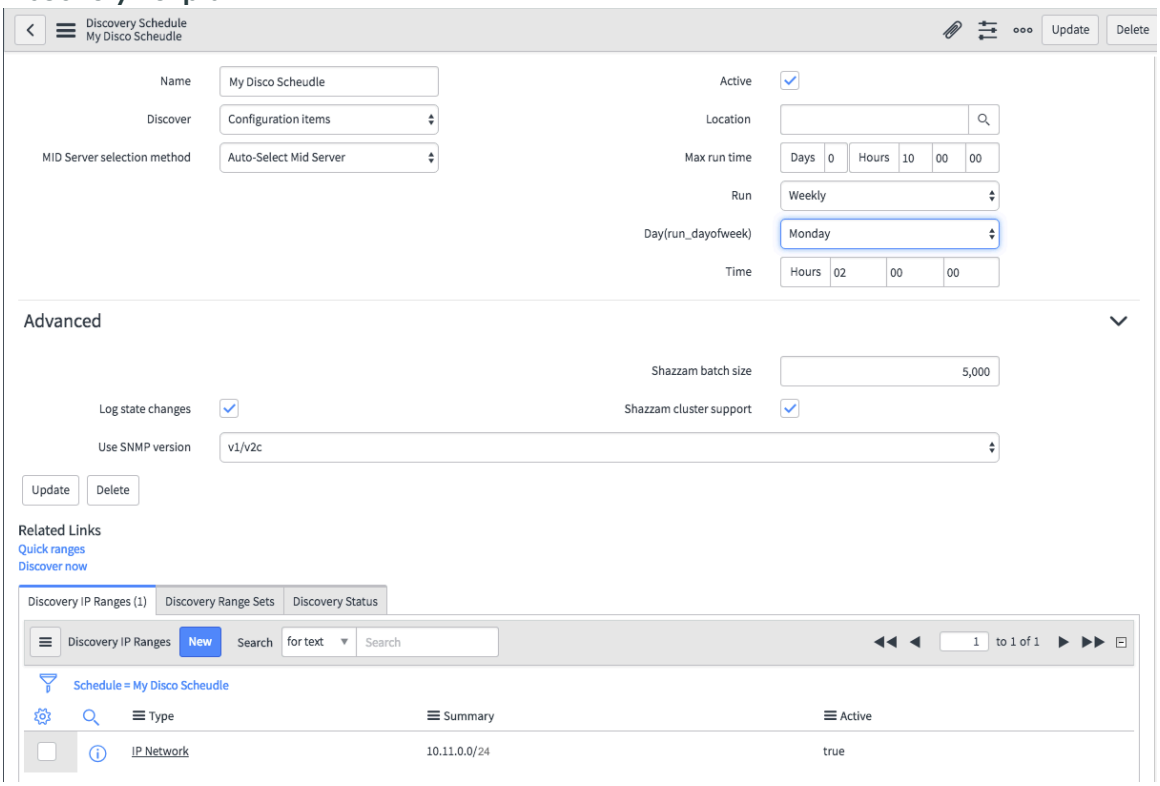
Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne** um einen neuen Datensatz zu erstellen.
2. Wählen Sie den Typ des Zeitplans zum Öffnen von:
   - **Neu**: Es wird ein neuer horizontaler Zeitplan für die Erkennung von Komponenten in Ihrem Netzwerk erstellt.
   - **Schnell-Discovery**: Führt einen horizontalen Discovery für eine einzelne IP-Adresse aus, ohne dass ein Zeitplan erforderlich ist.
   - **Einen Cloud-Discovery-Zeitplan erstellen**: Mit dem Discovery Manager-Assistenten wird ein Zeitplan für die Erkennung von Ressourcen in einem Cloud-Servicekonto erstellt.
3. Füllen Sie das Formular für Discovery-Zeitpläne aus, indem Sie die Felder in der Tabelle verwenden.
4. Klicken Sie mit der rechten Maustaste auf den Header des Datensatzes , und wählen Sie im Kontextmenü **Speichern** aus.
5. Um einen Bereich von zu erkennenden IP-Adressen zu erstellen, klicken Sie unter **Zugehörige Links** auf **Kurzbereiche**.

Hinweis: Um die Sicherheit zu verbessern, beschränken Sie den Bereich der Erkennungsziele, indem Sie unnötige Netzwerke und Geräte ausschließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery Zeitplan



Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Geben Sie einen eindeutigen, beschreibenden Namen für den Zeitplan ein.
Erkennen	Wählen Sie einen der folgenden Scantypen aus: ◦ **Konfigurationselemente**: Verwendet Discovery-Bezeichner dazu, Geräte mit CIs in der CMDB abzugleichen und die CMDB entsprechend zu aktualisieren. Führen Sie eine einfache Erkennung durch, indem Sie einen bestimmten MID-Server auswählen, um nach allen Protokollen (SSH, WMI und SNMP) zu scannen. Oder führen Sie erweiterte Erkennungen anhand von Discovery-Verhalten durch. Wenn Sie ein Verhalten auswählen, ist das Feld *MID Server* nicht verfügbar. **Hinweis:** Ein IPv6-Scan per Adressenliste ist im Discovery-Zeitplan für Konfigurationselemente zulässig. ◦ **IP-Adressen**: Scannt Geräte, ohne Anmeldeinformationen zu benutzen. Diese Scans erkennen alle aktiven IP-Adressen im angegebenen Bereich und erstellen Geräteverlaufsdatensätze, aktualisieren die CMDB jedoch nicht. Bei Scans von IP-Adressen werden auch mehrere IP-Adressen angezeigt, die auf einem einzelnen Gerät ausgeführt werden. Identifizieren Sie Geräte nach Klasse und Typ, zum Beispiel Windows-Computer und Cisco-Netzwerkgeräte. Die Eigenschaft *Max. Bereichsgröße* der Shazzam-Probe bestimmt die maximale Anzahl von IP-Adressen, die von Shazzam gescannt werden. Details siehe Shazzam-Probe konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ **Netzwerke**: Erkennt IP-Netzwerke (Router und Switches). Ergebnisse dieser Suche werden verwendet, um die IP-Netzwerktabelle [cmdb_ci_ip_network] in auszufüllen **Discovery** > **IP-Netzwerke** mit einer Liste von IP-Adressen und Netzwerkmasken. Netzwerkscans aktualisieren Router und Layer-3-Switches in der CMDB. ◦ **Service**: Es werden Services für die Anwendung Service-Mapping erkannt. Anweisungen dazu finden Sie unter Erkennung von oben nach unten mithilfe von Service-Mapping planen. ◦ **Ohne Server**: CIs werden gefunden, ohne dass eine Erkennung eines Hosts oder von CIs auf einem Proxy-Host ausgeführt werden muss, der sich bereits in der CMDB befindet. Weitere Informationen finden Sie unter Serverlose Erkennung. ◦ **Cloud-Applikation**: Erkennt nur die Cloud-Ressourcen für die von Ihnen angegebenen Muster. Anweisungen dazu finden Sie unter Cloud-Discovery erkunden. ◦ **Cloud-Ressourcen**: Erkennt Ressourcen für einen der unterstützten Cloud Provider. Diese Option wird nur angezeigt, wenn Sie Discovery unter einem Cloud-Servicekonto ausführen. Die Auswahl über einen neuen Discovery-Zeitplan ist nicht möglich. ◦ **Zertifikate**: Erkennt Zertifikate basierend auf URLs. Durch Auswahl dieser Option wird das Feld „Typ der Zertifikaterkennung“: „URL-Zertifikaterkennung“ hinzugefügt. Weitere Informationen finden Sie unter Zertifikaterkennung über individuelle URL-Scans ausführen.
Methode für MID-Server-Auswahl	Wählen Sie die Methode aus, die von Discovery zur MID-Server-Auswahl verwendet wird: ◦ **MID Server automatisch auswählen**: Lassen Sie zu, dass Discovery den MID-Server automatisch anhand der von Ihnen konfigurierten Discovery-IP-Bereiche auswählt. Um einen passenden MID-Server zu finden, müssen Sie MID Servers so konfigurieren, dass Folgendes verwendet wird: ▪ Die Discovery-Anwendung oder ALLE Anwendungen. Diese Einstellung gewährt Discovery Zugriff auf den MID-Server. ▪ Der IP-Bereich, der die Bereiche enthält, die Sie im Discovery-Zeitplan konfigurieren. **Hinweis:** Die automatische MID-Server-Auswahl wird bei IPv6 nicht unterstützt. ◦ **Spezifischer MID Server-Cluster**: Verwenden Sie einen vorkonfigurierten Cluster von MID Serversn. Wählen Sie das Cluster aus. Sie müssen kein Mitglied des Clusters angeben. Der MID-Server kann nicht Teil mehrerer Cluster sein, zum Beispiel eines Clusters, der den Lastenausgleich unterstützt, und eines Clusters, der Failover unterstützt. Sie können einen beliebigen Cluster hinzufügen, unabhängig von der Anwendung, der die MID Servers zugewiesen sind. Wenn Sie den Cluster auswählen, wird die Anwendung **Discovery** automatisch hinzugefügt, wenn sie für die MID Servers im Cluster nicht vorhanden ist. ◦ **Spezifischer MID Server**: Verwenden Sie nur einen MID-Server. Wenn dieser MID-Server Teil eines Clusters ist, wird nur dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	MID-Server verwendet. Das Cluster wird nicht verwendet. Sie können einen beliebigen MID-Server hinzufügen, unabhängig von der Anwendung, der er zugewiesen ist. Die Anwendung **Discovery** wird automatisch hinzugefügt, wenn sie dem von Ihnen ausgewählten MID-Server nicht bereits zugewiesen ist. Sie können einen spezifischen MID-Server für alle Arten von Discovery-Scans außer **Service** zuweisen. ◦ **Verhalten verwenden**: Verwenden Sie ein Verhalten, wenn für einen einzelnen Zeitplan die Verwendung mehrerer MID Servers erforderlich ist, damit eine der folgenden Aktivitäten ausgeführt werden kann: ▪ Scans, die mehrere Windows-Anmeldeinformationen erfordern ▪ Ein Zeitplan, der mindestens zwei bestimmte Protokolle (SNMP, SSH oder WMI) mit mehr als einem MID-Server ausführen muss. ▪ Lastenausgleich für umfangreiche Erkennungen, bei denen ein einzelner MID-Server nicht ausreicht. ▪ Scannen mehrerer Domänen **Hinweis:** Der Discovery-Zeitplan erzwingt Domänentrennung. Die zur Auswahl verfügbaren MID Servers müssen sich in derselben Domäne wie der Benutzer befinden, der den Zeitplan konfiguriert. Weitere Informationen finden Sie unter MID Server-Auswahlreihenfolge für Erkennungszeitpläne.
MID-Server	Wählen Sie den MID-Server für diesen Zeitplan aus. Dieses Feld ist verfügbar, wenn die *Methode für MID Server-Auswahl* auf *Spezifischer MID Server* festgelegt ist oder wenn eine Erkennung von IP-Adressen, Netzwerken oder Webservices durchgeführt wird. Um sicherzustellen, dass die von Ihnen ausgewählte MID-Server aktiv und validiert ist, sehen Sie sich das MID-Server-Dashboard an.
MID-Server-Cluster	Wählen Sie den MID-Server-Cluster für diesen Zeitplan aus. Dieses Feld ist verfügbar, wenn die *Methode für MID Server-Auswahl* auf *Spezieller MID Server-Cluster* festgelegt ist.
Verhalten	Wählen Sie ein Verhalten aus, das für die MID Servers in Ihrem Netzwerk konfiguriert ist. Dieses Feld ist nur verfügbar, wenn die *Methode für MID Server-Auswahl* auf *Verhalten verwenden* festgelegt ist.
Aktiv	Aktivieren Sie das Kontrollkästchen, um diesen Zeitplan zu aktivieren. Wenn Sie das Kontrollkästchen deaktivieren, wird der Zeitplan deaktiviert. Sie können über dieses Formular jedoch weiterhin manuell eine Erkennung mit den konfigurierten Werten ausführen.
Standort	Wählen Sie ein Verzeichnis aus, das den vom Zeitplan erkannten CIs zugewiesen werden soll. Wenn dieses Feld leer ist, wird kein Verzeichnis zugewiesen.
Max. Ausführungszeit	Legen Sie eine Zeitbegrenzung für die Ausführung dieses Zeitplans fest. Nach Ablauf der konfigurierten Zeit werden die verbleibenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Aufgaben für die Erkennung abgebrochen, auch wenn der Scan nicht abgeschlossen ist. Verwenden Sie dieses Feld, um die Systemlast auf ein gewünschtes Zeitfenster zu beschränken. Wenn in dieses Feld kein Wert eingegeben wird, wird dieser Zeitplan solange ausgeführt, bis er abgeschlossen ist.
„Ausführen“ und zugehörige Felder	Bestimmt den Ausführungszeitplan der Erkennung. Konfigurieren Sie die Häufigkeit im Feld **Ausführen** und in den anderen Feldern, die angezeigt werden, um eine genaue Zeit anzugeben. **Hinweis:** Für die Ausführungszeit wird immer die Systemzeitzone verwendet. Wenn Sie das optionale Feld **Als tz ausführen** hinzufügen, hat dies keine Auswirkungen auf die tatsächliche Ausführungszeit.
Statusänderungen protokollieren	Aktivieren Sie dieses Kontrollkästchen, um immer dann einen Protokolleintrag zu erstellen, wenn sich der Status während einer Erkennung ändert, zum Beispiel wenn sich die Einstellung für ein Gerät von *Aktiv* zu *Classifying (Wird klassifiziert)* ändert. Zeigen Sie die Erkennungsstatus in der zugehörigen Liste „Discovery-Geräte“ im Formular „Discovery-Status“ an. Die Felder *Abgeschlossene Aktivität* und *Aktuelle Aktivität* zeigen die Status an.
Shazzam-Batch-Größe	Geben Sie die Anzahl der IP-Adressen ein, die jede Shazzam-Probe scannen kann. Die Aufteilung der IP-Adressen in Batches verbessert die Performance, da die Klassifizierung für jeden Batch nach Abschluss des Batch beginnen kann, anstatt dass zunächst sämtliche IP-Adressen gescannt worden sein müssen. Die Probes werden sequenziell ausgeführt. Beispiel: Der Wert ist auf 1.000 festgelegt, und bei einer Erkennung werden 10.000 IP-Adressen mit einem einzelnen MID-Server gescannt. Es werden 10 Shazzam-Probes erstellt, wobei jede Probe 1000 IP-Adressen scannt. Standardmäßig beträgt die Batch-Größe 1000. Eine UI-Richtlinie erzwingt eine minimale Batch-Größe von 256, da Batch-Größen unter 256 IP-Adressen nicht von Clustering profitieren. Die Richtlinie konvertiert einen beliebigen Wert unter 256 in den Wert 0. Der Wert für dieses Feld darf den Wert nicht überschreiten, der in der Eigenschaft für die maximale Bereichsgröße für die Shazzam-Probe definiert ist.
Shazzam-Cluster-Unterstützung	Aktivieren Sie das Kontrollkästchen, um die Shazzam-Verarbeitung auf mehrere MID Servers in einem Cluster zu verteilen und die Leistung zu verbessern. Diese Einstellung wird mit der Shazzam-Batch-Größe verwendet. Beispielsweise wird ein Zeitplan zum Scannen von 100.000 IP-Adressen erstellt, wobei 10 MID Servers für die Ausführung der Arbeit zugewiesen werden. Jedem MID-Server sind 10.000 IP-Adressen zum Scannen zugewiesen. Wenn die Shazzam-Batch-Größe auf 5.000 IP-Adressen pro Probe festgelegt ist, führt der Zeitplan zwei Shazzam-Probes pro MID-Server (10.000 IP-Adressen/5.000 pro Batch) aus. Diese Probes werden nacheinander und nicht gleichzeitig ausgeführt.
SNMP-Version verwenden	Verwenden Sie dieses Feld, um die SNMP-Version anzugeben, die für diese Erkennung verwendet werden soll. Der Standardwert lautet **ALLE**. Sie können diesen Wert in **v1**, **v2c** oder **v3** ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Batch-Größe für URL-Zertifikat	Definieren Sie die Anzahl der URLs, die während der Discovery pro Batch erkannt werden sollen. Lassen Sie die Batch-Größe unverändert. Ändern Sie sie nur, wenn dies empfohlen wird.
Kurzbereiche	Definieren Sie zu scannende IP-Adressen und Adressbereiche, indem Sie IP-Adressen in mehreren Formaten (Netzwerk, Bereich oder Liste) in einer einzelnen kommagetrennten Zeichenfolge eingeben. Weitere Informationen finden Sie unter Schnell-IP-Bereich für Erkennungszeitplan erstellen.
Discovery starten	Verwenden Sie diesen Link, um diese Discovery sofort zu starten.
Zugehörige Listen	
IP-Bereiche	Diese zugehörige Liste definiert die IP-Adressbereiche, die mit diesem Zeitplan gescannt werden sollen. Wenn Sie einen einfachen CI-Scan (keine Verhalten) verwenden, definieren Sie die zu erkennenden IP-Adressen mit dieser zugehörigen Liste. **Hinweis:** Um die Sicherheit zu verbessern, beschränken Sie den Bereich der Erkennungsziele, indem Sie unnötige Netzwerke und Geräte ausschließen.
Discovery Bereiche	Diese zugehörige Liste definiert jedes Range Set, das in einem Zeitplan zur Überprüfung durch mindestens eine Shazzam-Probe festgelegt ist.
Discovery-Status	Diese zugehörige Liste zeigt die Ergebnisse aktueller und vergangener Ausführungen des Zeitplans an.
Zertifikat-URLs	Diese zugehörige Liste zeigt die URLs an, die mit diesem Zeitplan erkannt werden. Sie können URLs dieser Liste hinzufügen oder daraus löschen.

6. Definieren Sie die Häufigkeit der Zeitplanausführung wie in Ausführungsoptionen für Discovery-Zeitpläneбeschrieben.

Schnell-Discovery ausführen

Mit einer Schnell-Discovery bzw. mit DiscoverNow können Administratoren die Erkennung einer CI-Konfiguration für eine einzelne IP-Adresse ausführen, ohne dass ein Zeitplan benötigt wird.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Plattform wählt automatisch den richtigen MID Server für die Erkennung aus, wenn dieser mit der ausgewählten IP-Adresse verknüpft ist. Wenn für das Netzwerk, in dem diese Adresse angezeigt wird, kein MID Server konfiguriert ist, können Sie einen MID Server auswählen. Verwenden Sie diese Funktion, um neue Geräte im Netzwerk zu erkennen, sobald sie mit dem Netzwerk verbunden sind, anstatt auf eine regelmäßig durchgeführte, geplante Erkennung zu warten.

Um das System so zu konfigurieren, dass automatisch der zu verwendende MID Server ermittelt wird, richten Sie die IP-Bereichsfunktionen für jeden MID Server in Ihrem System ein.

Sie können DiscoverNow aus einem Discovery-Zeitplanformular oder Skript ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Schnell-Discovery mit einer IPv6-Zieladresse wird unterstützt.

Prozedur

1. Öffnen Sie Schnell-Discovery über einen der folgenden Navigationspfade:
   - Navigieren zu **Discovery** > **Discovery-Zeitpläne** und klicken Sie in der Kopfzeile auf **Schnell-Discovery**.
   - Navigieren zu **Discovery** > **Startseite** und klicken Sie unter der Kachel Zeitpläne **auf Discovery-Schnellstart**.

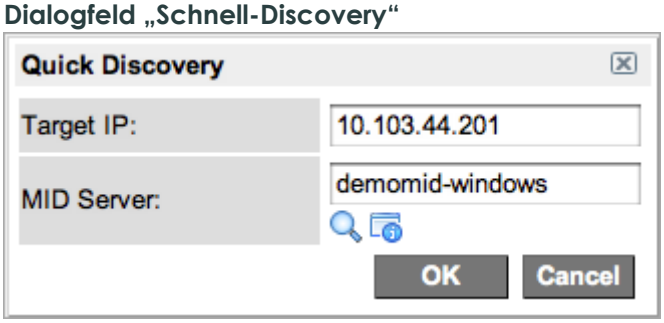
   Ein Dialogfeld wird angezeigt, in dem Sie zur Eingabe einer IP-Adresse und des Namens des zu verwendenden MID Servers aufgefordert werden. Nur MID-Server, die **In Betrieb** und **Überprüft** sind, stehen zur Verfügung.
2. Geben Sie die Ziel-IP-Adresse für eine Erkennung in das Feld **Ziel-IP** ein.

   Hinweis: DiscoverNow unterstützt derzeit keine IP-Netzwerkerkennung. Stellen Sie sicher, dass Sie nur eine einzelne IP-Adresse und nicht das gesamte Netzwerk eingeben, zum Beispiel 10.105.37.0/24.

   Wenn ein MID Server dem Subnetz zugewiesen ist, das die Ziel-IP-Adresse enthält, und derzeit den Betriebsstatus **In Betrieb** aufweist, wird der Name automatisch im Feld **MID Server** angezeigt. Wenn mehrere MID Server gefunden werden, wählt das System einen für Sie aus. Der Wert im Feld **MID Server** kann überschrieben werden, wenn Sie einen anderen MID Server auswählen möchten.

   Wichtig: Wenn der ausgewählte MID Server Teil eines Clusters mit Lastenausgleich und aus irgendeinem Grund nicht verfügbar ist, weist die Instanz Schnell-Discovery keinen anderen MID Server aus diesem Cluster zu. Sie müssen einen anderen MID Server aus der Liste der entsprechenden MID Server auswählen.
3. Wenn für dieses Netzwerk kein MID Server definiert ist, wählen Sie einen in der Liste der verfügbaren MID Server aus.

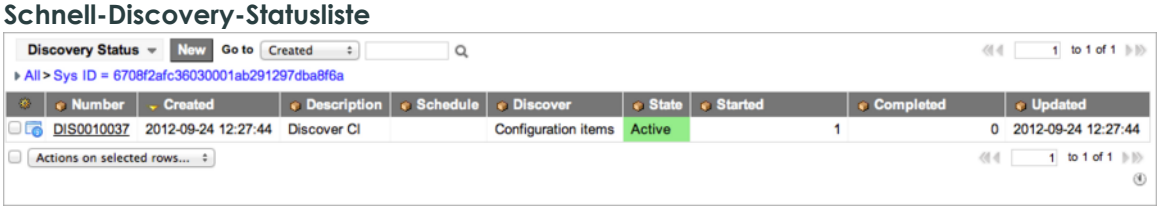
   Dialogfeld „Schnell-Discovery“

4. Klicken Sie auf **OK**, um die Erkennung auszuführen.

   Der Statusdatensatz für die Erkennung wird angezeigt. Die Spalte **Zeitplan** ist leer, da dieser Erkennung kein Zeitplan zugeordnet ist.

   Schnell-Discovery-Statusliste

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DiscoverNow aus einem Skript ausführen

Sie können DiscoverNow aus einem Skript ausführen, etwa aus einem Hintergrundauftrag, aus einer Geschäftsregel oder aus Webservices.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Erstellen Sie das folgende Skript:

```
var d = new Discovery();
var statusID = d.discoveryFromIP(TARGET_IP, TARGET_MIDSERVER);
```

   Die Methode *discoveryFromIP* nimmt zwei Argumente an: *IP* und *MID Server*. Das Argument *IP* ist obligatorisch, das Argument *MID Server* optional.

2. Geben Sie zur Auswahl des MID Servers entweder die *sys_id* oder den Namen des MID Servers als Argument an.
   Wenn Sie keinen MID Server benennen, versucht das System automatisch, einen gültigen Server zu finden. Gültige MID Server weisen den Status **In Betrieb** auf und können die angegebene IP-Adresse erkennen. Wenn das System einen gültigen MID Server erkennt und eine Discovery ausführt, gibt die Methode *discoveryFromIP* die *sys_id* des Discovery-Statusdatensatzes zurück. Wenn diese IP-Adresse von keinem MID Server erkannt wird, gibt die Methode den Wert **undefined** zurück.

   Wenn Sie TARGET_MIDSERVER manuell angeben, validiert das System den angegebenen Wert und stellt sicher, dass die Tabelle „MID Server“ den angegebenen MID Server-Datensatz enthält. Wenn die Validierung erfolgreich ist, gibt die Methode discoveryFromIP die sys_id des Statusdatensatzes der Erkennung zurück. Wenn die Validierung fehlschlägt, gibt die Methode den Wert **undefined** zurück.

Erkennungsergebnisse validieren

Validieren Sie die Ergebnisse Ihrer Erkennung, indem Sie auf die ECC-Warteschlange zugreifen, die XML-Nutzlast analysieren und das Discovery-Protokoll überprüfen.

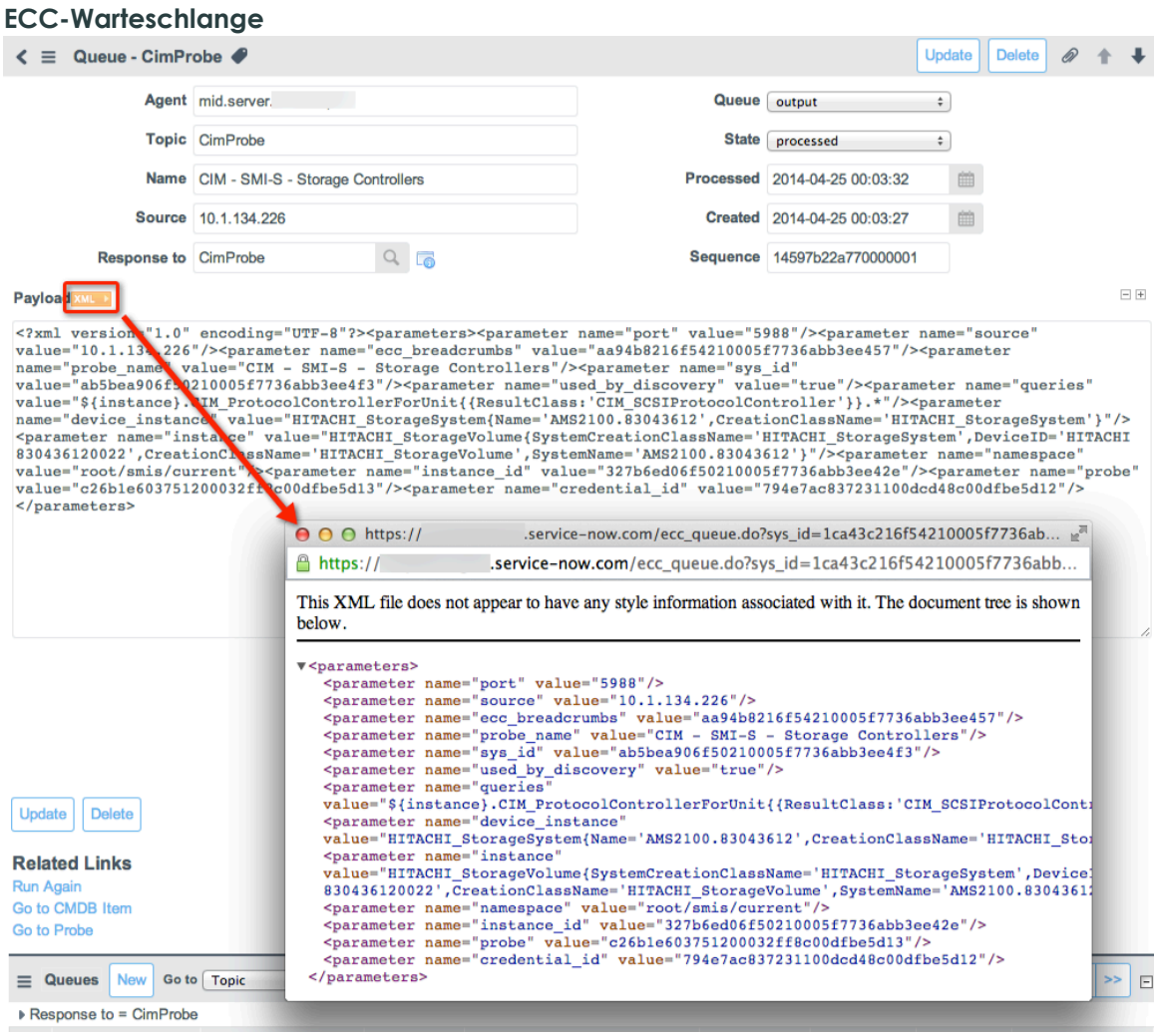
Vorbereitungen
Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Anfängliche Erkennungen ergeben häufig unerwartete Ergebnisse, zum Beispiel zuvor unbekannte Geräte und Prozesse oder fehlgeschlagene Authentifizierungen. Die Ergebnisse müssen auch bekannte Geräte genau identifizieren und die CMDB entsprechend aktualisieren. Machen Sie sich mit dem Netzwerk, das einer Erkennung unterzogen wird, und den zurückgegebenen Datentypen für die verschiedenen Erkennungstypen vertraut. Verwenden Sie das Discovery-Protokoll und die ECC-Warteschlange, um den Discovery-Prozess zu überwachen, wenn Daten von Probes oder Mustervorgängen zurückgegeben werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

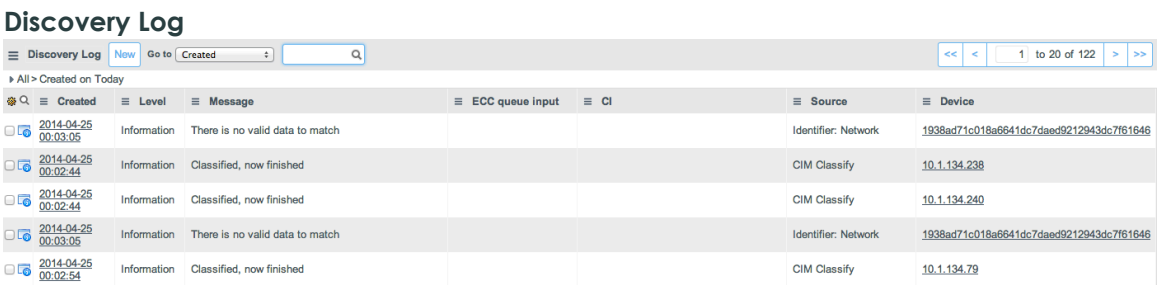
Prozedur

1. Klicken Sie auf das Symbol **XML** in einem Datensatz in der ECC-Warteschlange, um die tatsächliche Nutzlast einer Probe anzuzeigen.



2. Klicken Sie auf das Symbol **XML** in einem Datensatz in der ECC-Warteschlange, um die tatsächliche Nutzlast einer Probe anzuzeigen.
3. Verschaffen Sie sich im Formular „Discovery-Protokoll“ einen kurzen Überblick über die Performance der Probes.

   Um das Protokoll Discovery anzuzeigen, navigieren Sie zu **Discovery** > **Discovery-Protokoll**.



Das Discovery-Protokoll enthält die folgenden Informationen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Informationen
Erstellt	Zeigt den Zeitstempel der gestarteten Probe an. Klicken Sie auf diesen Link, um den Datensatz für die in dieser Liste gestartete Probe anzuzeigen.
Ebene	Zeigt den Typ der von dieser Probe zurückgegebenen Daten an. Mögliche Ebenen: ◦ Debuggen ◦ Fehler ◦ Informationen ◦ Warnung
Nachricht	Nachricht, die die Aktion beschreibt, die aufgrund der von der Probe zurückgegebenen Informationen durchgeführt wurde
Eingabe für ECC-Warteschlange	Zeigt den Namen der ECC-Warteschlange an, der der Protokollnachricht zugeordnet ist
CI	Das erkannte CI. Klicken Sie auf diesen Link, um den CMDB-Datensatz für dieses CI anzuzeigen.
Quelle	Zeigt den Namen der Probe an, die die Protokollnachricht generiert hat
Gerät	Zeigt die durch die Probe erkundete IP-Adresse an. Klicken Sie auf diesen Link, um alle Protokolleinträge für die Aktion zu untersuchen, die Discovery für diese IP-Adresse durchgeführt hat.

Hinweis: Wenn Sie eine aktive Erkennung abbrechen, beachten Sie die folgenden Informationen:

- Vorhandene Sensoraufträge, deren Ausführung gestartet wurde, werden sofort beendet.
- Vorhandene Sensoraufträge, die sich im Status **Bereit** befinden, deren Ausführung aber noch nicht gestartet wurde, werden aus dem System gelöscht.

4. Zeigen Sie die Discovery-Homepage an, um auf Details über alle Zeitpläne, Cloud-Ressourcen (virtuelle Computer), erkannten Geräte und zugehörigen Fehler zuzugreifen, die möglicherweise aufgetreten sind.
   Die Fehlerdetails schließen mögliche Nachbesserungsschritte ein.

MID Server-Auswahlreihenfolge für Erkennungszeitpläne

Bei der Suche nach einem MID-Server folgt die Anwendung Discovery der folgenden Reihenfolge.

Automatische Auswahl des MID Servers

Wenn Sie im Formular „Discovery-Zeitplan“ **MID Server automatisch auswählen** als **Methode für MID Server-Auswahl** auswählen, wird bei der Discovery die folgende Reihenfolge eingehalten.

Hinweis: Die automatische MID-Server-Auswahl wird bei IPv6 nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Discovery sucht nach einem MID-Server, für den auch ein entsprechender IP-Bereich konfiguriert ist.
2. Wenn kein MID Server diese Kriterien erfüllt, wird nach einem MID-Server mit der Anwendung **ALLE** gesucht, für die auch ein entsprechender IP-Bereich konfiguriert ist.
3. Wenn mehrere MID-Server die Kriterien erfüllen, wählt Discovery den ersten MID-Server mit dem Status **In Betrieb** aus. Wenn mehrere MID-Server aktiv sind, wird einer zufällig ausgewählt.
4. Wenn keiner aktiv ist, wird der für die Anwendung Discovery angegebene standardmäßige MID-Server verwendet, sofern dieser aktiv ist.
5. Wenn kein standardmäßiger MID Server aktiv ist, wird der für die Anwendung **ALLE** angegebene standardmäßige MID-Server verwendet, sofern dieser aktiv ist.
6. Wenn kein standardmäßiger MID-Server angegeben ist, durchläuft Discovery die vorherigen Schritte und sucht nach MID Servern mit dem Status **Angehalten** oder **Wird aktualisiert…**.

Hinweis: Wenn ein MID-Server angehalten ist oder aktualisiert wird, verarbeitet er Befehle erst, nachdem er in den Status **In Betrieb** zurückgekehrt ist.

MID Server-Cluster

Die folgenden Schritte werden ausgeführt, wenn Sie im Formular **Discovery** als **Methode für MID Server-Auswahl** die Option **Spezieller MID Server-Cluster** auswählen und das Cluster ein Lastenausgleichscluster ist:

1. **Discovery** verwendet den ersten MID-Server im Cluster, der mit dem Status **In Betrieb** gefunden wird.
2. Wenn mehrere MID-Server aktiv sind, wird einer zufällig ausgewählt. Wenn keine MID Servers gefunden werden, wird im Cluster nach MID Serversn mit dem Status **Angehalten** oder **Wird aktualisiert…** gesucht.

Die folgenden Schritte werden ausgeführt, wenn das Cluster ein Failover-Cluster ist:

1. **Discovery** verwendet den MID-Server mit dem niedrigsten Wert für **Reihenfolge**, der außerdem den Status **In Betrieb** aufweist.
2. Wenn kein MID Servers gefunden wird, wird im Cluster nach MID Serversn mit dem Status **Angehalten** oder **Wird aktualisiert…** gesucht, wobei der Server mit dem niedrigsten Wert für **Reihenfolge** ausgewählt wird.

Hinweis: **Discovery** ignoriert bei der Auswahl eines MID-Servers aus dem Cluster den standardmäßigen MID-Server und **ALLE** Anwendungen.

Port-Scanphase (Shazzam-Phase)

Während der Port-Scanphase erfasst Discovery alle Ziel-IP-Adressen. Sie werden gleichmäßig auf MID Servers aufgeteilt, die den Kriterien entsprechen (MID Servers sind für den Port-Scan qualifiziert). Die Shazzam-Batch-Größe, die Sie im Discovery-Zeitplan konfiguriert haben, bestimmt die Anzahl der IP-Adressen, die jede Shazzam-Probe scannen kann. In dieser Phase wird ermittelt, wie viel Arbeit jeder MID-Server während der Port-Scanphase verrichtet.

Beispiel: Drei qualifizierte MID Servers müssen 16.000 IP-Adressen scannen, und Sie verwenden die standardmäßige Shazzam-Batch-Größe von 5.000. Zwei der MID Servers verarbeiten 5.000 IP-Adress-Scans (jeweils eine Shazzam-Probe). Der andere MID-Server verarbeitet 6.000 IP-Adress-Scans, wozu er zwei Shazzam-Probes startet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Shazzam kann nur dann IP-Listen verarbeiten, die insgesamt 5.000 IP-Adressen (sowohl IPv4- als auch IPv6-Adressen) enthalten, wenn die Liste eine IPv6-Adresse enthält. Bei Zeitplänen, die IP-Adresslisten mit IPv6-Adressen enthalten, die über diese Grenze hinausgehen, wird der Discovery-Vorgang mit einer Fehlermeldung abgebrochen.

Zugehörige Informationen

MID Server-Pause

Clusterkonfiguration des MID Servers

File-based Discovery

Mithilfe von File-based Discovery können Sie identifizieren, welche Software auf Ihren Windows- und UNIX-Servern und -Geräten ausgeführt wird, selbst wenn keine Registrierungsinformationen verfügbar sind. Anschließend können Sie Datensätze Ihrer Softwarelizenzen verwalten, nach nicht lizenzierten Dateien suchen, unzulässige oder beschädigte Dateien erkennen und Bedrohungen durch unerwünschte Dateien bewerten.

Benötigte Plugins

Das Plugin „File-based Discovery“ [com.snc.discovery.file_based_discovery] ist für die Dateisignaturfilterung erforderlich. Ihr Abonnement für Discovery enthält dieses Plugin, Sie müssen jedoch die Aktivierung anfordern . Sobald das dateibasierte Plugin Discovery aktiv ist, wird auch das Plugin Software Asset Management - Dateisignatur-Normalisierung [com.snc.file_signature_normalization] aktiviert. Weitere Informationen zum Plugin Dateisignatur-Normalisierung finden Sie unter Dateisignaturnormalisierung .

Funktionsweise der dateibasierten Discovery

Die dateibasierte Discovery verbessert die Erkennung vorhandener installierter Software. Sie durchsucht Zielserver anhand einer bekannten Liste von Dateisignaturen und verarbeitet diese Dateien mit festgelegten Regeln. Die resultierenden Daten verbessern die Erkennung installierter Software und identifizieren nicht registrierte Softwareprodukte.

Die dateibasierte Discovery wird in der Erkundungsphase der normalen Discovery ausgelöst. Dateibasierte Discovery-Probes suchen in von Ihnen konfigurierten Pfaden nach bestimmten Dateierweiterungen oder Dateinamen. Die resultierenden Dateiinformationen werden in der Probe-Nutzlast zurückgegeben. Der Sensor versucht, die erkannten Dateien anhand der von der Probe zurückgegebenen Informationen (Name, Größe und Version der Datei) mit installierter Software abzugleichen. Die dateibasierte Discovery verwendet Dateisignaturen, um Software zu erkennen, die möglicherweise nicht registriert wurde. Diese Informationen werden dann in der Tabelle „Dateiinformationen“ [cmdb_file_information] mit einem Verweis auf das CI des Servers gespeichert. Sie können die von jedem CI gefundenen Dateien in einer zugehörigen Liste in dieser Tabelle anzeigen. Weitere Informationen finden Sie unter Zugehörige Liste der CI-Komponenten . Wenn eine Datei mit einem Softwareprodukt übereinstimmt, wenn Software Asset Management (SAM) aktiv ist, füllt Discovery die Produkt- und Herausgeberinformationen für diese Datei aus. Verwenden Sie diese Informationen, um zu verstehen, welche Software auf Ihrem Server ausgeführt wird, und um Bedrohungen durch unerwünschte Dateien zu bewerten. Discovery verwendet Listen bekannter Dateisignaturen für Windows und UNIX, um den Umfang der Suche zu beschränken. Der Filterprozess für Windows- und UNIX-Hosts wird unterschiedlich ausgeführt, da sich ihre Signaturlisten erheblich unterscheiden. Die viel kleinere UNIX-Signaturliste ist in der Probe „Unix - File Discovery“ enthalten und wird direkt am Ziel verarbeitet. Die Windows-Signaturliste ist viel größer und kann nicht auf dem Ziel verarbeitet werden. Die Probe „Windows - File Discovery“ durchsucht das Ziel nach bestimmten Dateierweiterungen und Pfaden und gibt diese Ergebnisse an den MID-Server zurück. Der MID-Server führt die Dateisignaturfilterung anhand der gesamten Windows-Liste durch. Anschließend sendet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

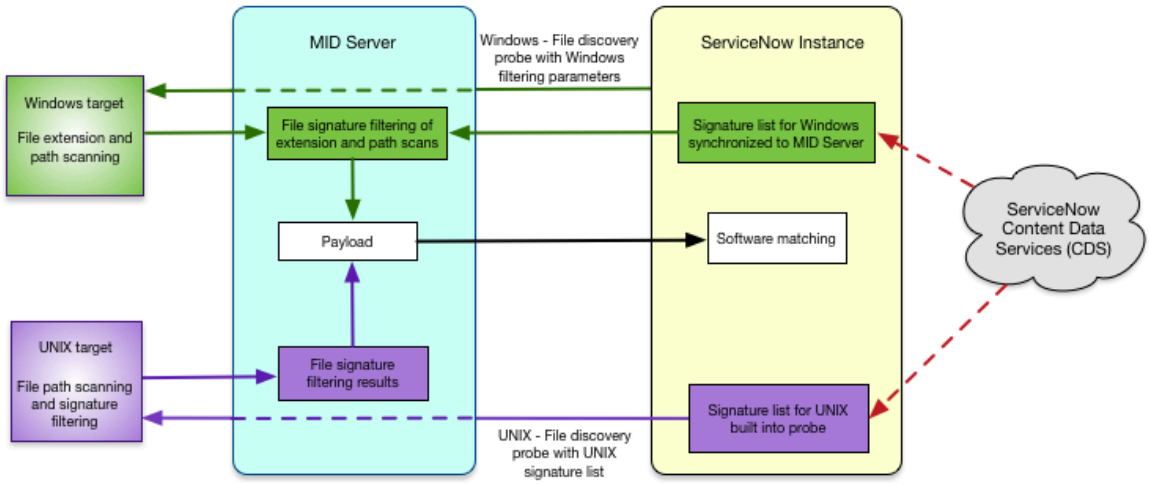
der MID-Server alle Dateiinformationen zur Normalisierung und zum Abgleich an die Instanz zurück.

Wenn SAMP für die Instanz aktiv ist, erstellt oder aktualisiert die dateibasierte Discovery identifizierte Softwareprodukte in der Tabelle „Softwareinstallation“ [cmdb_sam_sw_install] und aktualisiert die Lizenzen übereinstimmender Softwarepakete. Ohne SAMP werden keine Softwaredatensätze erstellt, und in die Tabelle „Dateiinformationen“ [cmdb_file_information] werden nur Dateiinformationen aufgenommen.

in der Discovery-Konfigurationskonsole können Sie SWID-Tags aktivieren. Wenn das SWID-Tag aktiviert ist und die dateibasierte Discovery ausgeführt wird, wird die Tabelle [cmdb_swid_tag] mit den SWID-Tag-Informationen gefüllt. Informationen zur auf einem bestimmten Computer installierten Software umfassen Name, Dateiinformationen, Herausgeber, Version, Installationsverzeichnis bzw. -gerät sowie Inhalt. Die Spalte „software_installation“ in [cmdb_swid_tag] ist ein Verweis auf die Tabelle [cmdb_sam_sw_install].

Hinweis: Das Base64-Paket ist eine Voraussetzung für alle UNIX - oder Linux -Server, um SWID-Tag-Dateien mit dateibasiertem Discoveryzu scannen.

Filterungs-Flow für dateibasierte Discovery

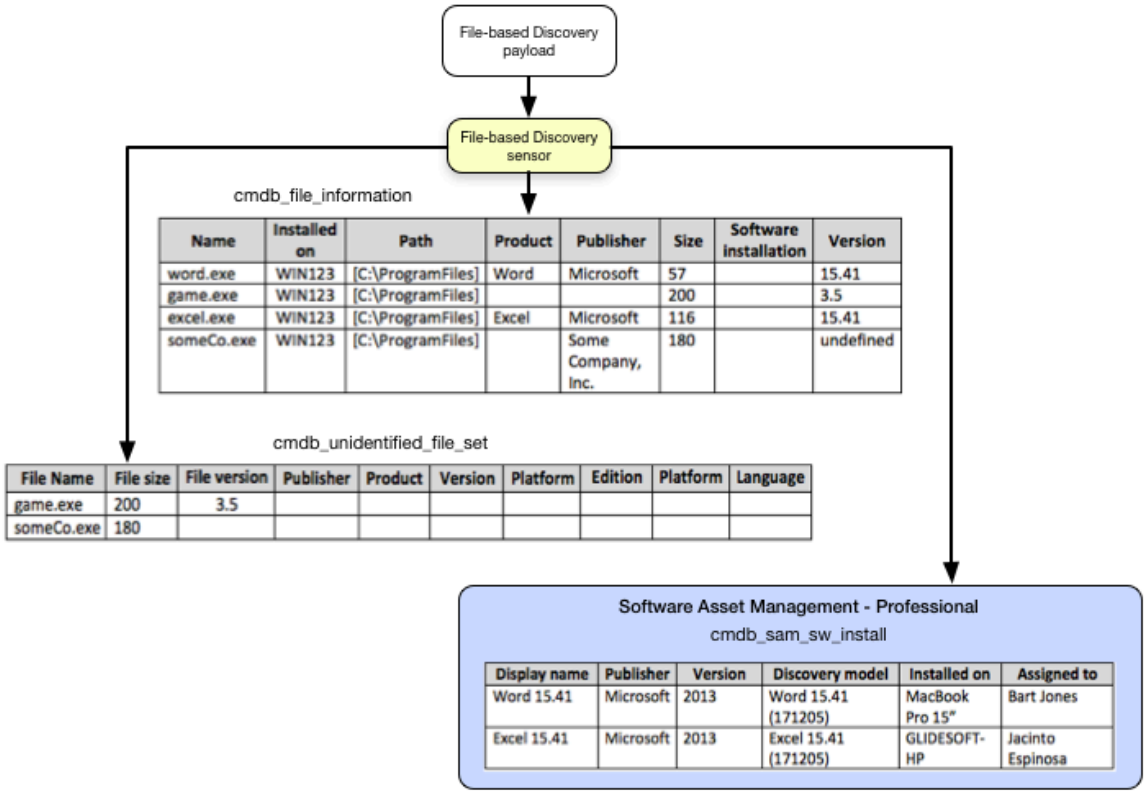


Bei der dateibasierten Funktion Discovery wird jede Datei, die nicht mit dem Normalisierungsprozess übereinstimmt, in die Tabelle „Nicht identifizierter Dateisatz“ [cmdb_unidentified_file_set] eingefügt. Sie können die Datensätze in dieser Tabelle aktualisieren und zusätzliche Details für zuvor nicht identifizierte Dateien angeben. Wenn Sie Werte für die Felder **Produkt** und **Herausgeber** für eine Datei angeben, können die Einstellungen in SAMP die dateibasierte Discovery aktivieren, um diese Datei für den Abgleich installierter Software in zukünftigen Erkennungen zu verwenden.

Hinweis: Sie können die dateibasierte Discovery jederzeit deaktivieren, indem Sie die entsprechende Einstellung in der Discovery-Konfigurationskonsole ändern. Wenn Sie die dateibasierte Discovery deaktivieren, bevor Scanergebnisse zurückgegeben werden, werden die Dateidaten ignoriert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellenschema für dateibasierte Discovery



Hinweis:

Dateibasierte Discovery bietet Unterstützung für Windows- und UNIX-Geräte. Die Probe UNIX ist POSIX-konform und sollte auf jedem Linux/Sularis-Server ausgeführt werden. ServiceNow bietet Unterstützung für die Windows-Versionen 2008, 2008R2, 2012R2, 2016, 2019 und höher mit PowerShell 3.0 bis 5.1. Wir unterstützen auch die AIX-Versionen 5.3, 6.1 und 7.1 sowie HP/UX 8.11.

Wenn Sie „File-based Discovery" unter Ubuntu Version 20 ausführen, modifizieren Sie die standardmäßige Bourne-Shell (sh) so, dass sie auf die Bourne-Again-Shell (bash) verweist.

Versionsinformationen werden für die Dateien nur mit Versionsinformationen gefüllt, die von Probes zurückgegeben werden. Nicht alle Dateien weisen Versionen auf. Dateien mit Erweiterungen wie exe, jar usw. weisen Versionen auf.

Reference

1. Referenzinformationen für dateibasierte Discovery

Dateibasierte Discovery ausführen

Führen Sie die dateibasierte Discovery aus, um die gesamte von Ihnen installierte Software zu erkennen, egal ob sie registriert ist oder nicht. Über die Discovery-Konfigurationskonsole können Sie die dateibasierte Discovery jederzeit aktivieren und konfigurieren.

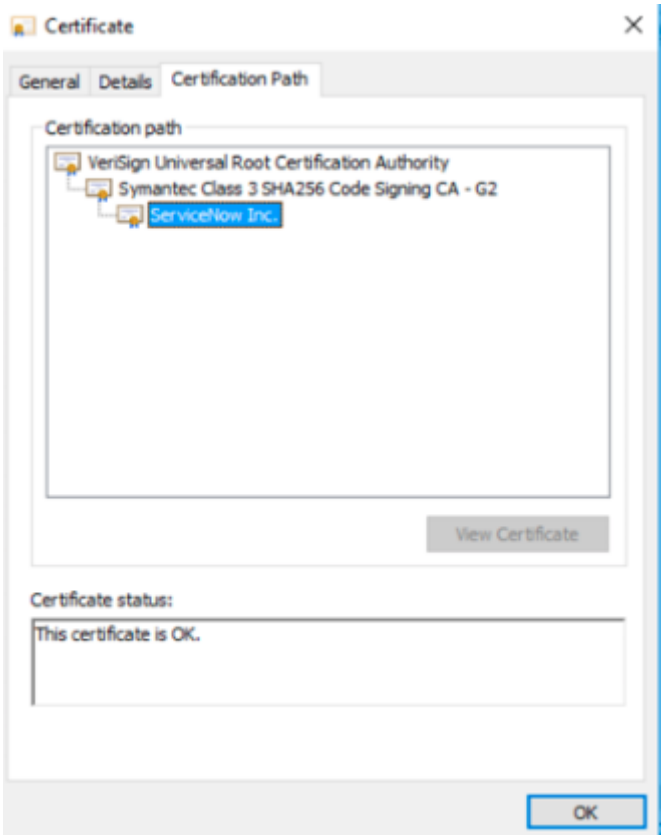
Vorbereitungen

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Richten Sie das PowerShell-Skript ein.
   Standardmäßig besitzt das Skript **filebaseddiscovery.ps1** eine ServiceNow-Signatur. Ihre Zertifikatkette wird bis zur Zertifizierungsstelle VeriSign Universal Root aufgelöst, der Windows standardmäßig vertraut. Da Powershell-Skripts von ServiceNow-Herausgeber signiert werden, fügen Sie den ServiceNow-Herausgeber Ihrem vertrauenswürdigen Herausgeber-Repository hinzu.



   Wenn die Ausführungsrichtlinie die Verwendung Ihres eigenen Zertifikats verlangt oder Sie Änderungen am Skript vornehmen müssen, signieren Sie das Skript erneut.

   a. Navigieren Sie zur Probe „Windows - File discovery“.
   b. Öffnen Sie den Probe-Parameter **filebaseddiscovey.ps1**.
   c. Kopieren Sie den Inhalt des Felds **Wert** in eine Datei.
   d. Nehmen Sie die erforderlichen Änderungen an der Datei vor, und entfernen Sie dann den (alten) Signaturblock am Ende der Datei.
   e. Signieren Sie das Skript erneut: https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.security/set-authenticodesignature?view=powershell-6 .

      Nach dem erneuten Signieren sollte die Datei einen neuen Signaturblock am Ende aufweisen.

   f. Kopieren Sie den gesamten Dateiinhalt, und ersetzen Sie den alten Wert im Probe-Parameter **filebaseddiscovery.ps1** aus Schritt b.

      Die dateibasierte Windows-Discovery sollte jetzt mit dem aktualisierten signierten Skript ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie Antivirensoftware verwenden, müssen Sie alle ServiceNow Windows PowerShell-Skripts einschließen, damit die Antivirensoftware dies nicht als Bedrohung ansieht.

2. Aktivieren Sie das Dateibasierte Plugin Discovery.
3. Aktivieren und konfigurieren Sie die dateibasierte Discovery.
   Mit der Discovery-Konfigurationskonsole können Sie die dateibasierte Discovery aktivieren und mehrere Komponenten konfigurieren, um Ihre gesamte installierte Software zu erkennen und zu verwalten.

   Um die Performance für bestehende Kunden nicht zu beeinträchtigen, ist die dateibasierte Discovery standardmäßig deaktiviert.
4. Dateibasierte Discovery-Scans konfigurieren
   Nach der Ausführung der Discovery und der Rückgabe von Dateiinformationen für ein CI wird die dateibasierte Discovery für dieses Ziel erst dann wieder ausgeführt, wenn das Intervall abgelaufen ist. Da die Ausführung von Scans für die dateibasierte Discovery die Performance beeinträchtigt, ist es wichtig zu bestimmen, wie häufig gescannt wird. Aus Leistungsaspekten wird jedoch davon abgeraten, ein häufigeres Intervall als „Monatlich“ auszuwählen.

   a. Erweitern Sie in der Discovery-Konfigurationskonsole den Eintrag **Verbreitet**, und geben Sie dann die maximale Anzahl der Dateien ein, die erkannt werden sollen.

      Hinweis: Das Erhöhen dieses Werts kann die Leistung beeinträchtigen.

   b. Legen Sie die **Häufigkeit** für die Ausführung der dateibasierten Discovery für das CI fest. Der Standardwert ist „Monatlich“.

      Hinweis: Die dateibasierte Discovery wird erst ausgelöst, wenn die erste Content Data Service-Synchronisierung (CDS) erfolgt. Bei der CDS-Synchronisierung kann es etwa 24 Stunden dauern, bis der erste Datensatz von CDS synchronisiert ist. Weitere Informationen hierzu finden Sie unter Normalisierung von Dateisignaturen .

Ergebnisse
Die dateibasierte Discovery sollte basierend auf der festgelegten Konfiguration ausgeführt werden. Anschließend können Sie die Ergebnisse im Discovery-Dashboard überwachen.

Reference

1. Referenzinformationen für dateibasierte Discovery

Lösung von Problemen bei der dateibasierten Discovery

Wenn Probleme beim Einrichten oder Ausführen der dateibasierten Discovery auftreten, führen Sie die hier aufgeführten Aktionen durch, um sie zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem	Ursache/Aktion
Fehlermeldung: Daten der Datei-Discovery noch nicht synchronisiert...	• Planen Sie genug Zeit ein, damit CDS die samp_file_*-Tabellen synchronisieren kann. • Überprüfen Sie die Tabelle cds_client_schedule, und überprüfen Sie, ob der Zeitstempel für die samp_file_*-Tabellen aktualisiert wurde.
Während der Erkennung wird die dateibasierte Discovery nicht ausgelöst.	• Die Funktion wurde nicht aktiviert. Überprüfen Sie die Konfigurationskonsole der Discovery-Definition, und stellen Sie sicher, dass die dateibasierte Discovery aktiviert ist. • Das Intervall zwischen den Scans ist zu lang. Überprüfen Sie die Intervalleinstellung für die Konfigurationskonsole der Discovery-Definition.
Während der Erkennung wird die dateibasierte Discovery nicht ausgelöst.	Überprüfen Sie die von der Discovery-Tabelle [discovery_private_properties] verwalteten internen Eigenschaften auf folgende Elemente. Geben Sie zum Anzeigen dieser Tabelle in den Navigationsfilter **discovery_private_properties.list** ein, und drücken Sie die **Eingabetaste**. • File_discovery.file_extensions_windows muss eine Liste der zu scannenden Windows-Dateierweiterungen enthalten. • File_discovery.unix_filename_timestamp muss einen anderen Zeitstempel als 1970 aufweisen. • File_discovery.windows_filename_timestamp muss einen anderen Zeitstempel als 1970 aufweisen.
Fehler im MID Server-Protokoll durch FileDiscoveryFilter oder MID Server-Problem generiert	• Überprüfen Sie, ob die Aufnahmeliste der dateibasierten Erkennung vorhanden ist. Die Aufnahmeliste befindet sich im MID Server-Installationsordner in `/agent/work`. Wenn sie nicht vorhanden ist, war die Synchronisierung nicht erfolgreich. • Überprüfen Sie den MID Server-Datensatz für die Instanz, um zu ermitteln, ob ein MID Server-Problem generiert wurde. • Der MID Server verwendet den geskripteten SOAP-Service GetMIDInfo, um die Aufnahmeliste zu synchronisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problem	Ursache/Aktion
	Überprüfen Sie, ob dieses Skript Fehler generiert hat. • Klicken Sie im MID Server-Datensatz auf den zugehörigen Link **Aktualisierung des Dateierkennungsfilter**, um die Dateinamen mit diesem MID Server zu synchronisieren.
PowerShell-Fehler	• Nehmen Sie das Skript in Ihre Virenschutzsoftware auf. • Fügen Sie den Herausgeber von ServiceNow dem Repository vertrauenswürdiger Herausgeber hinzu.

Reference

1. Referenzinformationen für dateibasierte Discovery

Referenzen für die dateibasierte Discovery

Das folgende Referenzmaterial enthält weitere Details zur dateibasierten Discovery.

Möglichkeiten zur Minimierung der Beeinträchtigung der Performance durch die dateibasierte Discovery

Das Scannen großer Netzwerke, insbesondere von Computern Windows, kann die Scan-Zeit erheblich verlängern. Darüber hinaus kann das Scannen von Dateien hohe CPU-Anforderungen auf den Zielcomputern und hohe Nutzlasten verursachen, die die Verarbeitungszeit erheblich verlängern. Um Leistungsprobleme zu vermeiden, können Sie mit der dateibasierten Discovery die Verarbeitung mit vielen der in der Discovery-Konfigurationskonsole konfigurierten Einstellungen optimieren.

- **Scannen in mehreren Phasen**: Probes werden in mehreren Phasen ausgelöst, um lange Scanzeiten zu reduzieren. Die erste Probe erstellt den Scanprozess auf dem Ziel. Dieser wird im Hintergrund ausgeführt. Nachfolgende Probes überprüfen bei jeder Ausführung von Discovery den Fortschritt dieses Scans und geben die Ergebnisse zurück, wenn der Scan abgeschlossen ist. Beispiel: Wenn ein Dateiscan über Schnell-Discovery oder einen Discovery-Zeitplan initiiert wird, werden keine Informationen zurückgegeben, wenn noch ein Hintergrundscan ausgeführt wird. Wenn der Scan bei der nächsten Erkennung des Servers abgeschlossen ist, gibt die Probe die Daten zurück.

  Wichtig: Beim Scannen in mehreren Phasen durch die dateibasierte Discovery werden Ergebnisse nicht sofort zurückgegeben. Erwarten Sie keine Ergebnisse von einem dateibasierten Scan, bis Discovery auf diesen Zielen erneut ausgeführt wird und die Liste der vom vorherigen Scan erkannten Dateien abruft.

- **Zu scannende Ordner**: Sie können sowohl den Umfang des Scans auf bestimmte Ordner beschränken als auch ausgeblendete Ordner scannen.
- **Zu scannende Erweiterungen**: Sie können sowohl alle Dateien für eine bestimmte Liste von Erweiterungen abrufen als auch bestimmte Dateierweiterungen beim Scannen ignorieren.
- **UNIX-Dateinamen scannen**: Da die Anzahl der eindeutigen Dateinamen, die zur Identifizierung der installierten Software auf UNIX verwendet werden, relativ gering ist, wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die vollständige Liste der Dateinamen in die Probe UNIX aufgenommen. Dadurch kann die Probe die ermittelten Dateien anhand der Signaturliste für das Ziel filtern. Es ist keine zusätzliche Filterung erforderlich, bis die Ergebnisse an die Instanz zurückgegeben werden.

- **Windows-Dateinamen scannen**: Für Windows dateibasiert Discoveryinitiiert die Probe keinen Scan des Ziels für die vollständige Signaturliste. Stattdessen generiert Discovery eine Liste von Dateierweiterungen, die die Probe mit dem Ziel abgleicht. Diese reduzierte Liste wird dann nach MID-Server für die gesamte Signaturliste Windows gefiltert.
- **Reduzierte Nutzlasten**: Durch Filtern der Scanergebnisse mit der Dateisignaturliste, bevor die Ergebnisse an die Instanz gelangen, reduziert Discovery die Größe der Nutzlast von Zielservern. Nur die Dateien aus den Zielen, die den in dieser Liste angegebenen Dateien entsprechen, werden an die Instanz zurückgegeben.
- **Scan-Drosselung**: Um die Auswirkungen auf die CPU- und E/A-Leistung Windows von auf Remotezielen zu reduzieren, wird Windows dateibasiert Discovery so konfiguriert, dass er während Scans gelegentlich in den Ruhezustand wechselt. Sie können dieses Verhalten mit den Discovery-Eigenschaften feinabstimmen. Durch die Drosselung von Windows -Scans können diese Scans länger dauern.

Tabellen der dateibasierten Discovery

Die folgenden Tabellen werden vom Plugin für die dateibasierte Discovery [com.snc.discovery.file_based_discovery] zum Speichern von Daten bereitgestellt:

Dateiinformationen [cmdb_file_information]

In dieser Tabelle werden alle Dateien (übereinstimmende und nicht übereinstimmende) gespeichert, die für ein bestimmtes CI erkannt wurden. Die Dateien sind in einer zugehörigen Liste mit CI-Computerdatensätzen verfügbar. In der Standardansicht werden die folgenden Spalten bereitgestellt:

- **Pfad**: Pfad, unter dem die Datei auf dem Ziel gefunden wurde
- **Produkt**: Software-Produktname. Dieses Feld wird gefüllt, wenn SAMP aktiviert ist und eine Übereinstimmung besteht.
- **Herausgeber**: Name des Herausgebers der Datei, zum Beispiel Oracle oder Microsoft. Dies ist eine Referenz auf die Unternehmenstabelle [core_company]. Dieses Feld wird gefüllt, wenn SAMP aktiviert ist und eine Übereinstimmung besteht.
- **Größe**: Größe der Datei
- **Softwareinstallation**: Name der installierten Software, die dieser Datei zugeordnet ist, aus der Tabelle „Softwareinstallation“ [cmdb_sam_sw_install]. Dieses Feld wird gefüllt, wenn SAMP aktiviert ist und eine Übereinstimmung besteht.
- **Version**: Version der Datei Derzeit nur für Windows.

Nicht identifizierter Dateisatz [cmdb_unidentified_file_set]

Diese Tabelle speichert alle von Discovery zurückgegebenen Dateien, die mit oder ohne SAMP nicht mit einem Softwareprodukt abgeglichen werden können. Discovery füllt Name, Größe und Version jeder nicht übereinstimmenden Datei im Datensatz. Diese optionalen Felder können verwendet werden, um die Datei weiter zu identifizieren und für zukünftige Dateizuordnungen verfügbar zu machen:

- Herausgeber
- Produkt
- Version

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Edition
- Plattform
- Sprache

Hinweis: Eine Funktion in Software Asset Management Professional (SAMP) ermöglicht die Freigabe von Signaturdaten in dieser Tabelle für Content Data Services (CDS). Bei aktivierter Datenfreigabe lädt das System automatisch Datensätze aus der Tabelle „Nicht identifizierter Dateisatz“ [cmdb_unidentified_file_set] in CDS hoch, wenn Sie die fehlenden Informationen ergänzen. Durch den Upload der identifizierten Dateien werden diese zur Verbesserung des zukünftigen Dateivergleichs verfügbar gemacht. Einzelheiten hierzu finden Sie unter Anwenderdefiniertes Softwareprodukt hinzufügen .

Dateibasierte Discovery – Fehlerbehebung

Wenn beim Einrichten oder Ausführen von Discovery Probleme auftreten, konsultieren Sie Lösung von Problemen bei der dateibasierten Discovery.

Zugehörige Informationen

File-based Discovery

Anwendungen basierend auf Fingerabdrücken erkennen

Erkennen Sie Anwendungen basierend auf Vorschlägen von ServiceNow Predictive Intelligence. Predictive Intelligence klassifiziert und kategorisiert die erkannten laufenden Prozesse automatisch als Fingerabdrücke der Anwendung und macht Vorschläge. ITOM-Transparenz nutzt Predictive Intelligence zur ersten Analyse erkannter Prozesse und empfiehlt Anwendungen, für die eine Erkennung durchgeführt werden sollte. Mit dieser Methode erstellt ITOM-Transparenz automatisch eine CI-Klasse für die Configuration Management Database (CMDB), einen Klassifizierer oder ein Muster für die neue Anwendungs-CI-Klasse.

Vorbereitungen

Führen Sie eine horizontale Erkennung für alle relevanten IP-Bereiche durch (siehe Beschreibung in IP-Netzwerke in Discovery-Range Sets konvertieren). Geben Sie alle relevanten Anmeldeinformationen für den Zugriff von ITOM-Transparenz auf die Anwendungen und Geräte an, die Sie erkennen möchten.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Erkennung von Anwendungen anhand von Fingerabdrücken ist besonders nützlich, wenn Sie keine Muster verwenden können, die standardmäßig oder über den ServiceNow Store verfügbar sind. Beispielsweise wenn Sie nicht standardmäßige, selbst entwickelte Anwendungen oder brandneue Anwendungen erkennen möchten.

Die Funktion Discovery von ITOM-Transparenz verwendet Application Dependency-Mapping (ADM), um an TCP-Ports ausgeführte Prozesse und Anwendungen zu erkennen, die diese Prozesse ausführen. Wenn Sie Anwendungen anhand von Fingerabdrücken erkennen, gehen Sie noch einen Schritt weiter. Die auf Fingerabdrücken basierte Erkennungsmethode analysiert Prozesse, die ADM nicht für die Erkennung verwendet hat.

Die auf Fingerabdrücken basierte Erkennung nutzt Algorithmen, um laufende Prozesse zu identifizieren und in Gruppen zu organisieren. Diese Prozessgruppen werden zu vorgeschlagenen Anwendungen oder Kandidaten. Sie überprüfen vorgeschlagene Anwendungen und wählen aus, welche erkannt werden sollen. Die Liste der vorgeschlagenen Anwendungen wird stündlich aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während der Fingerabdruckerkennung erstellte Muster werden sowohl für die horizontale Erkennung als auch für die Erkennung von oben nach unten verwendet. Damit Service-Mapping ein solches Muster korrekt ausführen kann, müssen Sie definieren, wann dieses Muster ausgeführt werden soll. Dazu legen Sie fest, vor oder nach welchem anderen Muster Service-Mapping dieses neue Muster ausführen soll.

Wenn Sie eine Anwendung basierend auf einem Anwendungsvorschlag erkennen, führt die auf Fingerabdrücken basierte Erkennung die folgenden Schritte aus:

1. Die auf Fingerabdrücken basierte Erkennung erstellt für die neue Anwendung eine CI-Klasse in der CMDB. Die neue CI-Klasse erweitert die CI-Klasse „Anwendung“ [cmdb_ci_appl] und verwendet standardmäßig den Prozessgruppennamen als Anzeigename der vorgeschlagenen CI-Klasse.
2. Die auf Fingerabdrücken basierte Erkennung erstellt einen Prozessklassifizierer für die Anwendungsgruppe, die erkannt werden soll. ADM verwendet den neuen Prozessklassifizierer, um das für die CI-Klasse erstellte neue Muster auszulösen. Die Priorität des Klassifizierers ist niedriger, um sicherzustellen, dass das System zuerst die mit ITOM-Transparenz verfügbaren Standardmuster oder benutzerdefinierte Muster verwendet.
3. Die auf Fingerabdrücken basierte Erkennung erstellt ein Erkennungsmuster des Anwendungstyps für die neue CI-Klasse. **Prozessklassifizierung erzwingen** ist aktiviert, um sicherzustellen, dass der MID-Server dieses Muster nur ausführt, wenn der für ein CI identifizierte Prozess den Klassifizierungskriterien für dieses Muster entspricht.

   Hinweis: Die Anwenderoberfläche von Service-Mapping bezieht sich auf CI-Klassen als CI-Typen.

4. ADM verwendet den Klassifizierer, um die horizontale Erkennung des Anwendungs-CI auszulösen.
5. ADM löst die Erkennung mit dem neuen Muster aus.
6. Nachdem das Muster die Erkennung abgeschlossen hat, wird das erkannte Anwendungs-CI in die entsprechende Tabelle der CMDB geschrieben.

Die auf Fingerabdrücken basierte Erkennung ist standardmäßig aktiviert.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**.
2. Klicken Sie auf **Fingerabdrücke der Anwendung**.
   Das Dashboard **Fingerabdrücke der Anwendung** wird geöffnet.
3. Zeigen Sie vorgeschlagene Anwendungen auf eine der folgenden Arten an:
   - Zeigen Sie im Tortendiagramm mit den **häufigsten Vorschlägen** die wichtigsten Vorschläge an, sortiert nach der Anzahl der Prozesse, aus denen diese Vorschläge hervorgehen. Die Prozessanzahl spiegelt sich in der Größe des jeweiligen Diagrammsegments wider. Klicken Sie auf das Segment, um die entsprechenden Vorschläge in einer gefilterten Liste anzuzeigen. Klicken Sie zum Ausblenden eines Vorschlags aus dem Diagramm auf den Namen des Vorschlags in der Diagrammlegende.
   - Um nur Vorschläge für Anwendungsserver anzuzeigen, klicken Sie auf die **Kachel für vorgeschlagene Anwendungsserver**. Die gefilterte Liste mit Vorschlägen für Anwendungsserver wird angezeigt.
   - Sie können auch **alle Vorschläge** anzeigen. Die ungefilterte Liste mit allen Vorschlägen wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie unter **Vorgeschlagener Gruppenname** auf den entsprechenden Vorschlag, zum Beispiel **Python**.
   Die Vorschlagsdetails werden im Formular **Anwendungsvorschlag** geöffnet.
5. Überprüfen Sie die Vorschlagsdetails unter Beachtung der folgenden Parameter:

Feld	Beschreibung
Vorgeschlagener Gruppenname	Der Name ITOM-Transparenz, der für den Vorschlag generiert wird. Dieses Feld ist bereits ausgefüllt, Sie können es jedoch bei Bedarf ändern.
Erweiterter Gruppenname	Die 10 wichtigsten Stichwörter, die weitere Informationen zum Prozess liefern. Predictive Intelligence extrahiert diese Stichwörter aus dem Prozess.
Vorgeschlagene CMDB CI-Klasse	Der Name der von ADM erstellten CMDB-CI-Klasse, wenn Sie sich für die Erkennung der vorgeschlagenen Anwendung entscheiden
Prozessanzahl	Die Anzahl der erkannten Prozesse, auf denen dieser Vorschlag basiert
Prozesse anzeigen	Klicken Sie, um die Beispielprozesse anzuzeigen, auf denen dieser Vorschlag basiert. Die Gesamtanzahl der Prozesse kann größer sein und beginnt bei 1000. Standardmäßig können 100 Beispielprozesse angezeigt werden.
Genauigkeit	Ein Validierungsalgorithmus überprüft die Qualität der Vorhersage. Der Algorithmus analysiert den Parameter des regulären Ausdrucks (ReGex) der Prozesse in diesem Vorschlag und in anderen Vorschlägen (Anwendungsgruppen). Wählen Sie Vorschläge mit höherer Regelgenauigkeit aus. Wenn die Genauigkeit niedrig ist, können Sie die ReGex-Definition des Prozesses manuell einstellen (siehe Beschreibung in Reguläre Ausdrücke für die auf Fingerabdrücken basierte Erkennung anpassen) **Hinweis:** Ändern Sie den Genauigkeitswert nicht manuell.
Prozessklassifizierer	Der vorgeschlagene reguläre Ausdruck, der im Klassifizierer verwendet wird. Falls definiert, verwendet ADM diesen regulären

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Ausdruck während der horizontalen Erkennung.
Regel ignorieren	Der Name des Prozesses, der mit der Aktion **Ignorieren** von der Erkennung ausgeschlossen wurde

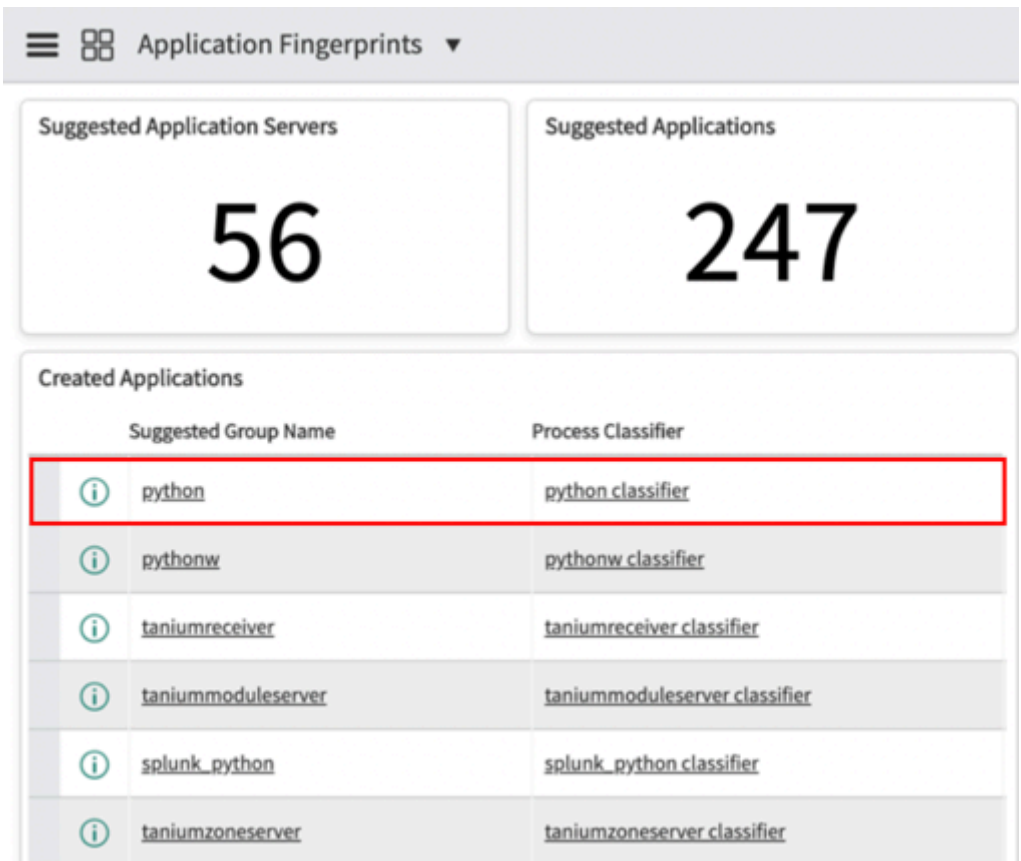
6. Wahlweise: Wenn dieser Vorschlag nicht relevant ist und Sie ihn nicht für die Erkennung verwenden möchten, führen Sie eine der folgenden Aktionen aus:
   - Klicken Sie auf **Ignorieren**, um Prozesse von der horizontalen Erkennung auszuschließen.

     Dieser Prozess wird der Tabelle „Prozesshandler“ [discovery_proc_handler] hinzugefügt, wobei der `Classify parameter` auf „false“ gesetzt wird. Discovery beendet die Überprüfung des Klassifizierers auf den ausgeschlossenen Prozess und führt keine Erkennung des CI durch, für das diese Prozesse ausgeführt werden.

   - Klicken Sie auf **Löschen**, um diesen Vorschlag aus der Vorschlagsliste zu entfernen.

     Der Vorschlag wird aus der Liste entfernt. Wenn Predictive Intelligence einem gelöschten Vorschlag neue Prozesse hinzufügt, wird er erneut in dieser Liste angezeigt.

7. Klicken Sie auf **Anwendung erkennen**.
   Die auf Fingerabdrücken basierte Erkennung erkennt ein Anwendungs-CI für den ausgewählten Vorschlag.
8. Überprüfen Sie im Dashboard **Fingerabdrücke der Anwendung**, ob die erkannte Anwendung unter **Created Applications (Erstellte Anwendungen)** angezeigt wird.

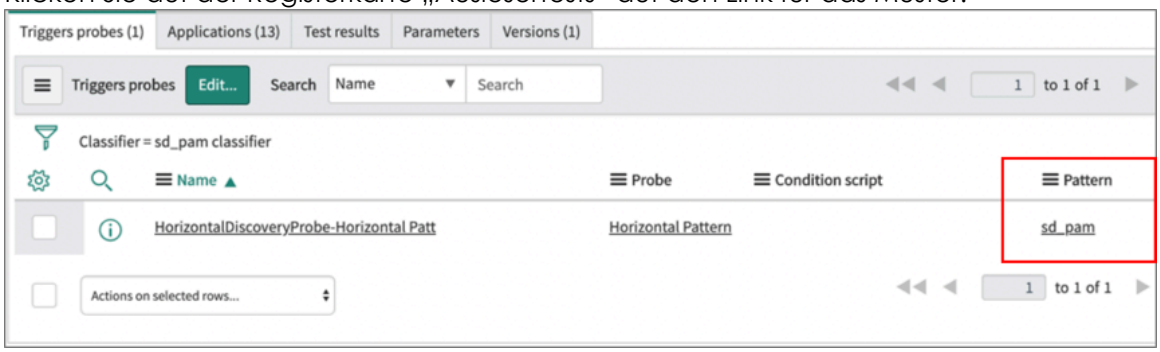


9. Konfigurieren Sie die Ausführungsreihenfolge für das automatisch erstellte Muster:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf den Prozessklassifizierer neben der neuen Anwendung.
Das Formular „Prozessklassifizierung“ wird geöffnet.

b. Klicken Sie auf der Registerkarte „Auslösertests“ auf den Link für das Muster.



Das Musterformular wird geöffnet.

c. Wählen Sie die Reihenfolge aus, in der dieses Muster immer ausgeführt wird:

- **Vor**
- **Nach**

d. Wählen Sie dann das andere zutreffende Muster aus.

> **Hinweis:** Wenn Sie sich nicht sicher sind, was die richtige Reihenfolge ist, oder wenn Sie dieses automatisch generierte Muster für die Erkennung von oben nach unten nicht verwenden möchten, konfigurieren Sie die Ausführungsreihenfolge als **After All (Nach allen)**.

e. Klicken Sie auf **Speichern**.

10. Wahlweise: Klicken Sie auf den Prozessklassifizierer neben der neuen Anwendung, um den Klassifizierer und das Muster anzuzeigen, das die auf Fingerabdrücken basierte Erkennung für dieses Anwendungs-CI erstellt.

11. Wahlweise: Wenn das Erkennungsergebnis nicht zufriedenstellend ist, kalibrieren Sie die Funktion der auf Fingerabdrücken basierten Erkennung.

Zugehörige Informationen

Predictive Intelligence

Dashboard „Fingerabdrücke der Anwendung“

Auf Fingerabdrücken basierte Erkennung kalibrieren

Nehmen Sie die Feineinstellung der Erkennung von Anwendungen auf Basis von Prozessen vor, wenn die Erkennungsergebnisse nicht zufriedenstellend sind.

Ändern Sie die Standardeinstellungen für die auf Fingerabdrücken basierte Erkennung, wenn diese Funktion überhaupt keine Vorschläge generiert. Darüber hinaus können Sie die generierten Vorschläge feinabstimmen, um sie relevant und nützlich zu machen.

Sicherstellen, dass die auf Fingerabdrücken basierte Erkennung Vorschläge generiert

Die auf Fingerabdrücken basierte Erkennung stützt sich auf die Predictive Intelligence zum Generieren von Vorschlägen für die Erkennung. Wenn das Dashboard **Fingerabdrücke der**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung keine Vorschläge anzeigt, stellen Sie sicher, dass die Predictive Intelligence korrekt konfiguriert ist.

Vorbereitungen

Standardmäßig ist die auf Fingerabdrücken basierte Discovery aktiviert. Stellen Sie sicher, dass die auf Fingerabdrücken basierte Discovery nicht deaktiviert wurde: Navigieren Sie zu **Alle** > **System Eigenschafts** > **Alle Eigenschaften**. Stellen Sie sicher, dass die folgende Eigenschaft nicht in der Liste angezeigt wird: *`sys_property process.clustering.appfingerprint.enabled`*.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn das Dashboard **Fingerabdrücke der Anwendung** keine Vorschläge anzeigt, gehen Sie wie folgt vor. Überprüfen Sie nach jeder Aktion, ob das Problem weiterhin besteht.

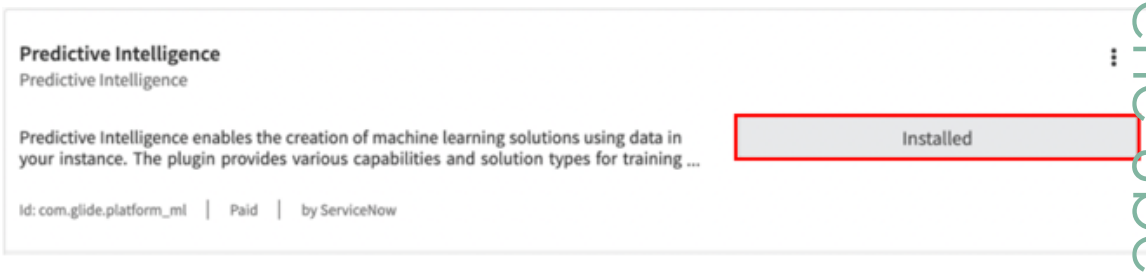
Prozedur

1. Stellen Sie sicher, dass Predictive Intelligence installiert und aktiv ist.

   a. Navigieren zu **Systemdefinition** > **Plugins**.

   b. Suchen Sie nach **Predictive Intelligence**.

   c. Stellen Sie sicher, dass das Plugin Predictive Intelligence installiert ist.



   Wenn Predictive Intelligence nicht installiert ist, klicken Sie auf die Schaltfläche **Installieren**.

   d. Klicken Sie auf die Kachel **Predictive Intelligence**.

   e. Stellen Sie im Formular „Predictive Intelligence“ sicher, dass der **Status** gleich **Aktiv** ist. Wenn der Status **Inaktiv** ist, klicken Sie unter **Zugehörige Links** auf den Link **Aktivieren/Reparieren**.

2. Stellen Sie sicher, dass der regelmäßige Auftrag zur Steuerung der auf Fingerabdrücken basierten Erkennung aktiviert und ordnungsgemäß konfiguriert ist.

   a. Navigieren zu **Systemdefinition** > **Geplante Aufgaben**.

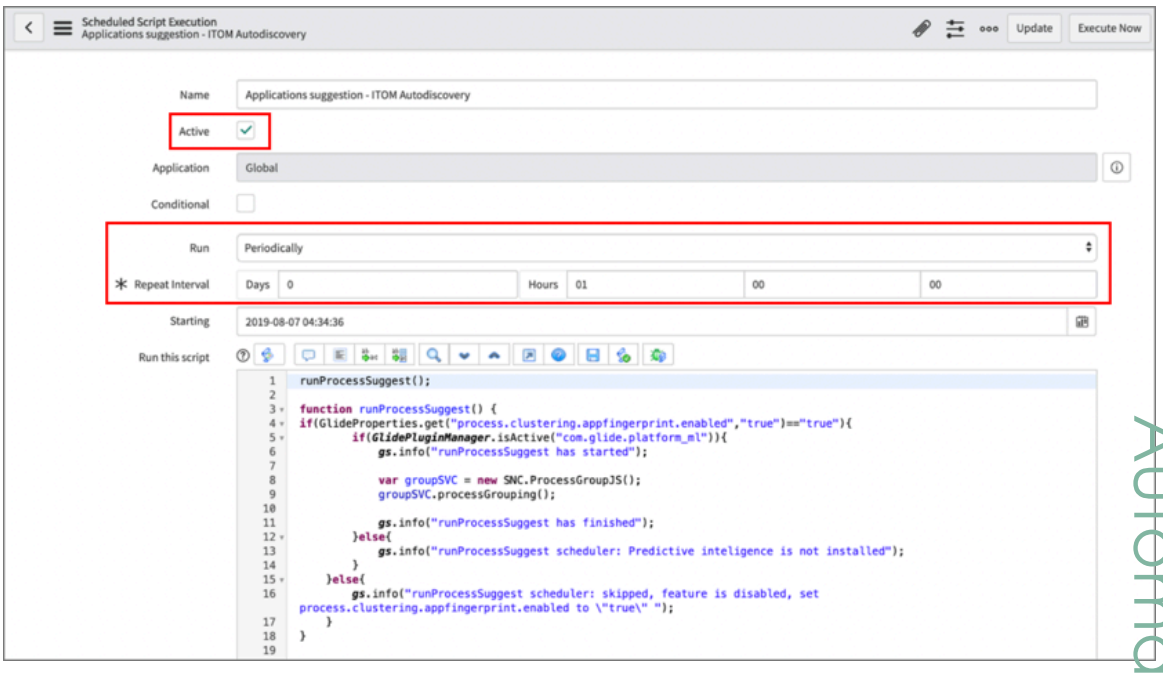
   b. Wählen Sie die regelmäßige Aufgabe *`Applications suggestion - ITOM Autodisco`* in der Liste aus.

   c. Stellen Sie sicher, dass das Kontrollkästchen **Aktiv** aktiviert ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Überprüfen Sie, ob die Erkennungshäufigkeit wie im folgenden Beispiel auf eine Stunde festgelegt ist:

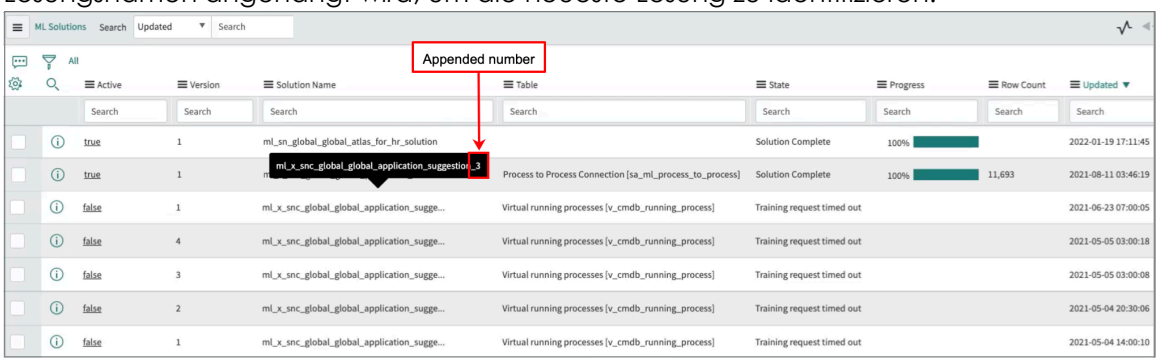


3. Prüfen Sie, ob die für die Gruppierung von Prozessen in Vorschlägen verantwortliche Clustering-Lösung aktiv ist.

a. Geben Sie im Feld **Filternavigator** des **Navigationsbereichs** `ml_solution.list` ein. Auf der Registerkarte **ML-Lösungen** werden alle Lösungen angezeigt, einschließlich Clusterlösungen.

b. Identifizieren Sie Clusterlösungen, indem Sie die Spalte **Tabelle** überprüfen. Vom System werden Clusterlösungen in der Tabelle „Virtuelle laufende Prozesse“ [v_cmdb_running_process] gespeichert.

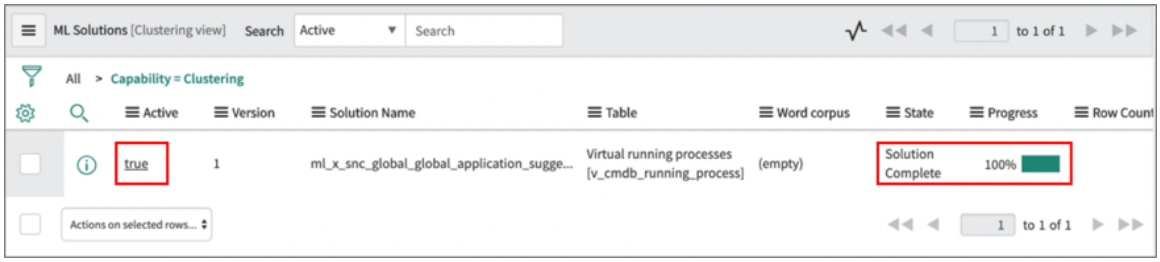
c. Wenn mehrere Clusterlösungen vorhanden sind, identifizieren Sie die neueste Lösung anhand des Zeitstempels in der Spalte **Aktualisieren**.
Alternativ dazu können Sie die Nummer verwenden, die vom System an den Lösungsnamen angehängt wird, um die neueste Lösung zu identifizieren.



d. Stellen Sie sicher, dass **Status** den Wert **Lösung abgeschlossen** und **Fortschritt** den Wert **100 %** aufweist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Wenn der Statuswert nicht Lösung abgeschlossen ist, konfigurieren Sie Predictive Intelligence wie in Konfigurationstipps für Predictive Intelligence beschrieben.

4. Prüfen Sie, ob die Clustering-Lösung genügend Prozessgruppen erstellt hat, die zu Vorschlägen werden.
   a. Navigieren zu **Systemdefinition** > **Tabellen** und suchen Sie die Tabelle Virtuelle laufende Prozesse [v_cmdb_running_process].
   b. Überprüfen Sie, ob diese Tabelle mehr als 1000 Datensätze enthält.
   c. Wenn weniger als 1000 Prozesse vorhanden sind, erkennen Sie weitere Prozesse, indem Sie eine horizontale Erkennung für zusätzliche IP-Bereiche oder Subnetze ausführen.
   d. Wenn nach der Erkennung zusätzlicher IP-Bereiche oder Subnetze immer noch weniger als 1000 Prozesse vorhanden sind, deaktivieren Sie die auf Fingerabdrücken basierte Erkennung.
5. Stellen Sie sicher, dass die Transaktion **„Anwendungsvorschlag – ITOM Autodisco“** nicht langsam geladen wird, wie unter Aktive Transaktion anzeigen und beenden beschrieben.
   Wenn diese Transaktion übermäßig lange ausgeführt wird, beenden Sie sie.

Feinabstimmung der Vorschläge der auf Fingerabdrücken basierten Erkennung

Passen Sie die Definitionen prozessbasierter Vorschläge an, bevor Sie die Erkennung starten. Normalerweise müssen Sie automatisch generierte Vorschläge optimieren, wenn die Genauigkeit weniger als 100 % beträgt. Predictive Intelligence erstellt Vorschläge und gibt die Genauigkeitsschätzung für jeden Vorschlag an. Die Ungenauigkeit kann dazu führen, dass erforderliche Anwendungen nicht erkannt werden oder dass zusätzlich zu den ordnungsgemäß erkannten Anwendungen falsche Anwendungen erkannt werden.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

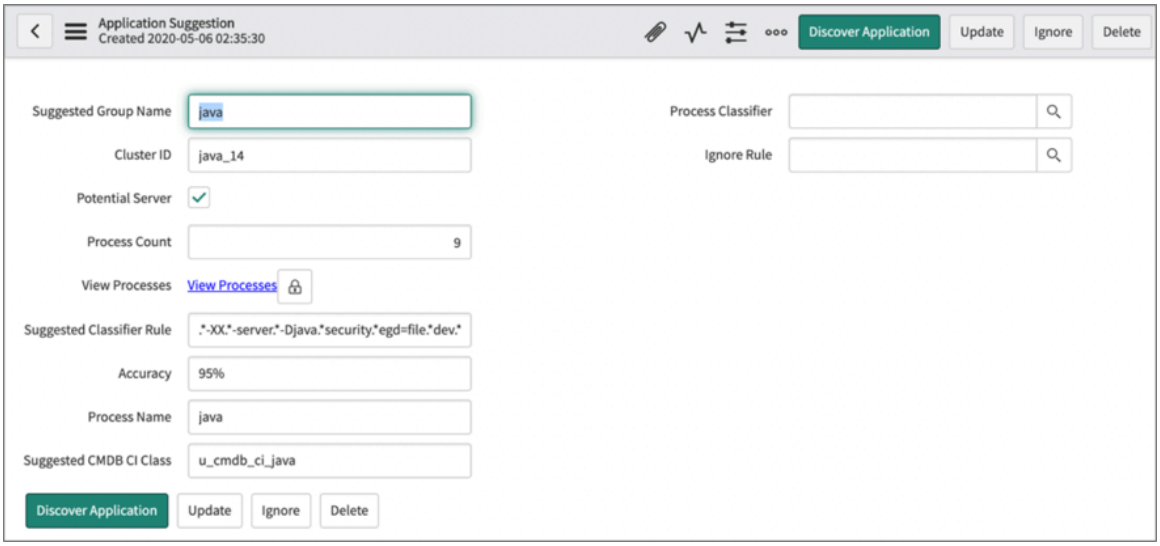
1. Navigieren zu **Alle** > **Discovery** > **Startseite**.
2. Klicken Sie auf **Fingerabdrücke der Anwendung**.
   Das Dashboard **Fingerabdrücke der Anwendung** wird geöffnet.
3. Navigieren Sie mit einer der folgenden Methoden zur Liste der Vorschläge:
   - Zeigen Sie im Tortendiagramm mit den **häufigsten Vorschlägen** die wichtigsten Vorschläge an, sortiert nach der Anzahl der Prozesse, aus denen diese Vorschläge hervorgehen.
   - Um nur Vorschläge für Anwendungsserver anzuzeigen, klicken Sie auf die **Kachel für vorgeschlagene Anwendungsserver**. Die gefilterte Liste mit Vorschlägen für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsserver wird angezeigt. Diese Liste ist auch so gefiltert, dass nur Vorschläge mit einer Genauigkeit von 100 % angezeigt werden.

- Sie können auch **alle Vorschläge** anzeigen. Die ungefilterte Liste mit allen Vorschlägen wird angezeigt.

4. Klicken Sie in der Liste „Anwendungsvorschläge“ auf den relevanten Vorschlag in der Spalte **Vorgeschlagener Gruppenname**.
   Das Formular „Anwendungsvorschlag“ wird geöffnet.



5. Um den Namen zu ändern, der für die auf Fingerabdrücken basierte Erkennung verwendet wird, geben Sie den gewünschten Namen in das Feld **Name** ein.
   Beispielsweise führen viele Anwendungen Java-Prozesse aus. Der vorgeschlagene Gruppenname für diese Gruppen lautet dann **Java**. Sie können einen Namen zuweisen, der die Anwendung, die Sie mithilfe dieses Vorschlags erkennen möchten, besser beschreibt (zum Beispiel `java_myweblogic`).
6. Um den für die CI-Klasse verwendeten Namen zu ändern, geben Sie den Namen der bevorzugten CI-Klasse in das Feld **Vorgeschlagene CMDB CI-Klasse** ein.
7. Um die Klassifiziererregel zu verfeinern, ändern Sie die regulären Ausdrücke im Feld **Vorgeschlagene Klassifiziererregel**.
   Fügen Sie dem regulären Ausdruck für die Erkennung einer Tomcat-Anwendung beispielsweise Versionsinformationen hinzu: `.*tomcat.* -Dopss.*version=12.1.3.*`
8. Klicken Sie auf **Aktualisieren**.
9. Wenn Sie nicht sicher sind, wie die Klassifiziererregel geändert werden kann, nehmen Sie nach der ersten Erkennung eine Feinabstimmung vor, wie unter Reguläre Ausdrücke für die auf Fingerabdrücken basierte Erkennung anpassen beschrieben.

Reguläre Ausdrücke für die auf Fingerabdrücken basierte Erkennung anpassen

Optimieren Sie den regulären Ausdruck in der Klassifiziererregel, um Discovery-Ergebnisse zu präzisieren. Predictive Intelligence extrahiert reguläre Ausdrücke aus Prozessen und weist sie Klassifiziererregeln als Teil der Erstellung von Vorschlägen zu. Wenn Sie mit den Erkennungsergebnissen nicht zufrieden sind oder die Vorschlagsgenauigkeit weniger als 100 % beträgt, ändern Sie den regulären Ausdruck.

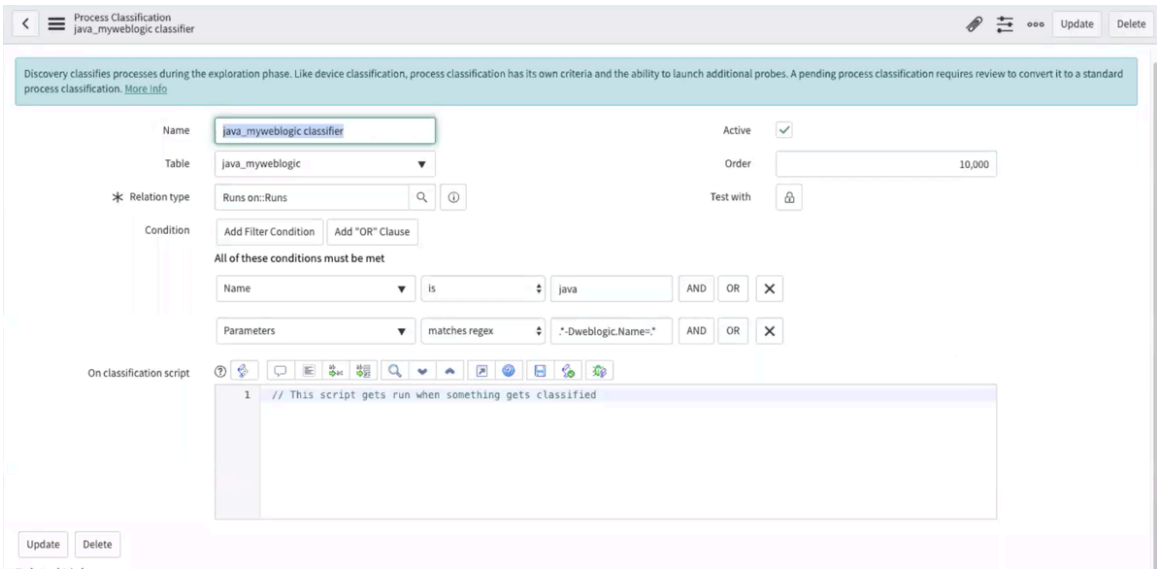
Vorbereitungen

Erforderliche Rolle: discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

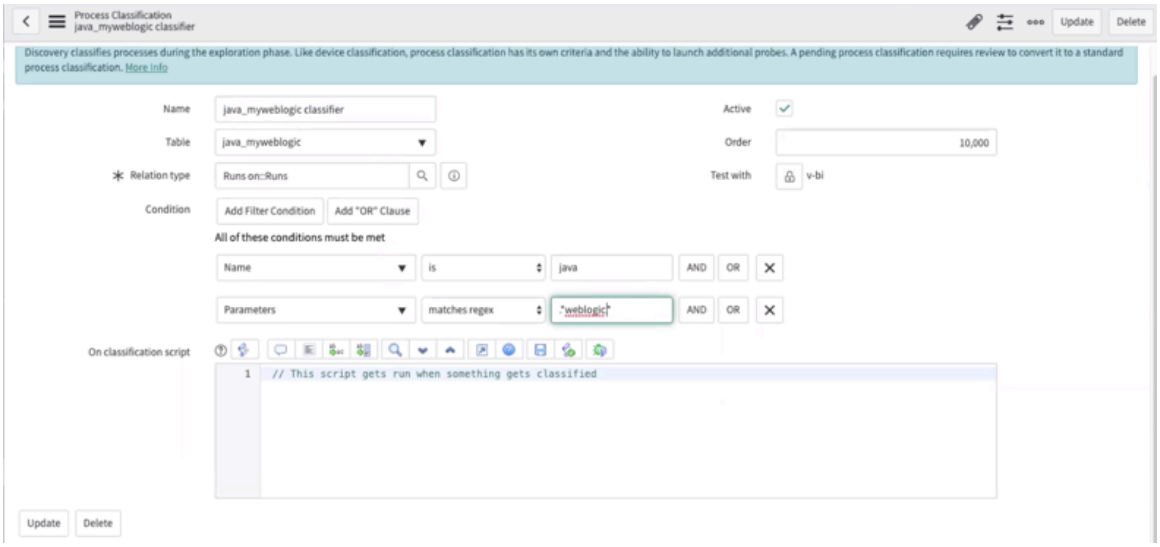
Prozedur

1. Navigieren zu **Alle** > **Anwendung** > **Modul**.
2. Klicken Sie auf **Anwendung erkennen**.
   Die auf Fingerabdrücken basierte Erkennung findet die Anwendung und erstellt eine CI-Klasse, einen Klassifizierer und ein Muster.
3. Klicken Sie in der Liste **Anwendungsvorschläge** auf den neu erstellten Prozessklassifizierer.
   Das Formular „Prozessklassifizierung“ wird geöffnet.



4. Beachten Sie den regulären Ausdruck im Wertfeld **Parameter** unter **Bedingung**, der von Predictive Intelligence automatisch ausgewählt wird.
   In diesem Beispiel lautet der Wert **."-DweblogicName=."**
5. Klicken Sie auf das **Vorhängeschloss**-Symbol neben **Testen mit**.
6. Klicken Sie auf das **Suchsymbol**, um den Server auszuwählen, auf dem Sie zusätzliche reguläre Ausdrücke testen möchten.
   Eine Liste mit allen erkannten Servern wird geöffnet.
7. Wählen Sie den Server aus, der die Anwendung ausführt, die Sie mithilfe des benutzerdefinierten Klassifizierers erkennen möchten.
   Der ausgewählte Server wird im Feld **Testen mit** angezeigt.
8. Klicken Sie mit der rechten Maustaste in den Header des Prozessklassifizierungsformulars, und wählen Sie **Speichern** aus.
   Das System führt einen Test aus und zeigt die Ergebnisse auf der Registerkarte **Testergebnisse** unten auf der Seite an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Überprüfen Sie auf der Registerkarte „Testergebnisse“ die Prozesse, die mithilfe der für diesen Klassifizierer konfigurierten regulären Ausdrücke erkannt wurden.
10. Passen Sie den regulären Ausdruck im Wertfeld „Parameter“ unter **Bedingungen** an. Beispiel: Formulieren Sie ihn allgemeiner: `".*weblogic.*"`
11. Klicken Sie mit der rechten Maustaste in den Header des Prozessklassifizierungsformulars, und wählen Sie **Speichern** aus.
    Das System führt den Test erneut aus und zeigt die Ergebnisse auf der Registerkarte **Testergebnisse** unten auf der Seite an.
12. Überprüfen Sie auf der Registerkarte „Testergebnisse“, ob die Fingerabdruckerkennung die Anwendungen wie erwartet erkannt hat.

Auf Fingerabdrücken basierte Erkennung deaktivieren

Die auf Fingerabdrücken basierte Erkennung ist standardmäßig aktiviert. Deaktivieren Sie die prozessbasierte Anwendungserkennung, wenn Predictive Intelligence nicht genügend Prozesse generiert.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Fügen Sie die Systemeigenschaft *sys_property* *process.clustering.appfingerprint.enabled* hinzu (siehe Systemeigenschaft hinzufügen) .
2. Um die Erkennung zu deaktivieren, geben Sie `false` in das Feld **Wert** ein.
3. Um die auf Fingerabdrücken basierte Erkennung wieder zu aktivieren, ändern Sie das Feld **Wert** in `true`.

Zugehörige Informationen

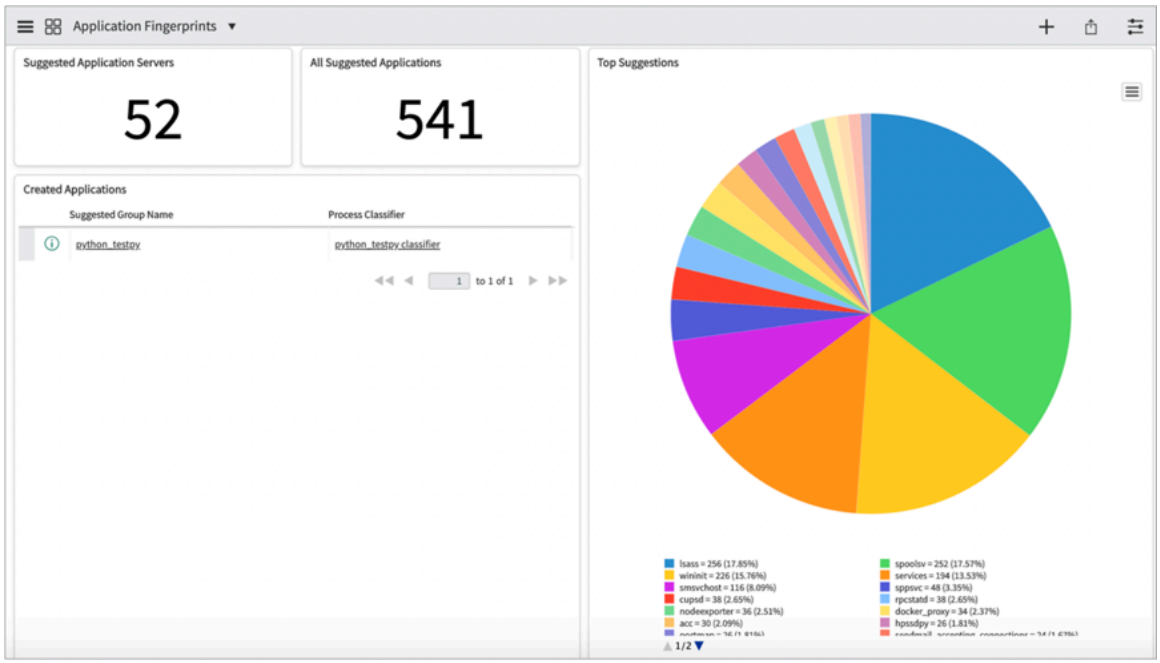
KB0826261: Advanced configuration and troubleshooting of fingerprint-based discovery (Erweiterte Konfiguration und Problembehandlung bei der auf Fingerabdrücken basierten Erkennung)

Leitfaden zur Fehlerbehebung bei ML-Verbindungsvorschlägen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard „Fingerabdrücke der Anwendung“

ITOM-Transparenz nutzt Predictive Intelligence zur ersten Analyse erkannter Prozesse und empfiehlt Anwendungen, für die eine Erkennung durchgeführt werden sollte. Mit dieser Methode erstellt ITOM-Transparenz automatisch eine CI-Klasse für die Configuration Management Database (CMDB), einen Klassifizierer oder ein Muster für die neue Anwendungs-CI-Klasse. Verwenden Sie das Dashboard „Fingerabdrücke der Anwendung“, um vorgeschlagene Anwendungen zu überprüfen.



Erforderliche Now Platform-Rollen

discovery_admin, führt die horizontale Erkennung mit Discovery aus.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
Administrator, der die horizontale Erkennung des IT-Netzwerks der Organisation durchführt	Überprüfen Sie Anwendungsvorschläge, und entscheiden Sie, welche Anwendungen anhand von Fingerabdrücken erkannt werden sollen. Durch Ausführen dieser Aktion werden die Ergebnisse der grundlegenden horizontalen Erkennung verbessert.

Indikatoren

Vorgeschlagene Anwendungsserver

Die gefilterte Liste mit Vorschlägen für Anwendungsserver wird angezeigt.

Vorgeschlagene Anwendungen

Die vollständige Liste mit Vorschlägen für Anwendungen wird angezeigt.

Erstellte Anwendungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Liste der Anwendungen, die das System basierend auf Fingerabdrücken erkannt hat.

Datenvisualisierungen

Titel	Typ	Quelltabelle	Beschreibung
Häufigste Vorschläge	Kreisdiagramm	Anwendungsvorschlag [cmdb_process_groups]	Ein Tortendiagrammbericht mit den häufigsten Vorschlägen, sortiert nach der Anzahl der Prozesse, aus denen diese Vorschläge hervorgehen. Die Prozessanzahl spiegelt sich in der Größe des jeweiligen Diagrammsegments wider. Klicken Sie auf das Segment, um die entsprechenden Vorschläge in einer gefilterten Liste anzuzeigen. Klicken Sie zum Ausblenden eines Vorschlags aus dem Diagramm auf den Namen des Vorschlags in der Diagrammlegende.

Netzwerk-Discovery

Bei der Netzwerkerkennung mit Discovery werden die internen IP-Netzwerke und Subnetze innerhalb Ihrer Organisation erkannt.

Hinweis: Wenn Sie die IP-Adressbereiche in Ihrem Netzwerk bereits kennen, ist die Netzwerkerkennung mit Discovery nicht erforderlich. Diese Erkennung ist für Organisationen konzipiert, die die für Discovery in ihren Netzwerken verfügbaren IP-Adressen nicht vollständig kennen.

Funktionsweise der Netzwerkerkennung

Mit den erfassten Informationen aktualisiert Discovery Router und Layer-3-Switches in der CMDB. Ein einzelner MID Server, der mit dem Scannen in einer konfigurierbaren Liste von Startroutern (oder Seed-Routern) beginnt, führt die Netzwerk-Discoveryaus. Normalerweise entsprechen die Startrouter den Standardroutern, die von allen MID Server-Hostcomputern im Netzwerk verwendet werden. Es können jedoch auch beliebige Router festgelegt werden. Der MID Server verwendet die Routertabellen der Startrouter, um andere Router im Netzwerk zu erkennen. Der MID Server breitet sich dann über das Netzwerk aus und verwendet gefundene Routertabellen, um andere Router zu erkennen. Dies wird solange fortgesetzt, bis die Erkundung aller Router und Switches abgeschlossen ist.

Konvertieren Sie nach der Netzwerkerkennung mit Discovery die gefundenen IP-Netzwerke in Range Sets von IP-Adressen, die Sie in Erkennungszeitplänen zum Erkennen von Konfigurationselementen (CI) verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie SNMP-Anmeldeinformationen oder (optional) SSH-Anmeldeinformationen . Port 161 muss für SNMP-Zugriff und Port 22 für SSH-Zugriff geöffnet sein.

Eigenschaften der Netzwerkerkennung

Die Standardwerte können für die meisten Erkennungen verwendet werden. Navigieren zu **Discovery-Definitionen** > **Eigenschaften** um die Eigenschaften zu bearbeiten.

Feld	Beschreibung
glide.discovery.bgp_router_disable	BGP-Routererkundung deaktiviert: Deaktivierung der Ausführung des Probe **SNMP – Routing** oder des Musters, wenn ein Router erkannt wird, von dem das BGP-Protokoll ausgeführt wird. Normalerweise ist diese Suche aufgrund der Größe von BGP-Routing-Tabellen inaktiv und weil solche Router im Allgemeinen nur am Rande großer Netzwerke arbeiten, wo eine weitere Netzwerk-Discovery irrelevant wäre. Dieser Wert könnte auf „falsch“ gesetzt werden, wenn Ihr Unternehmen nur BGP-Router als Edge-Router zwischen relativ kleinen Netzwerken (z. B. zwischen Gebäuden auf einem einzelnen Campus) verwendet. Wenn Sie die Tabelle [discovery_device_neightors] während der horizontalen Layer-2-Discovery der BGP-fähigen Geräte ausfüllen müssen, legen Sie die Eigenschaft **Deaktivieren der BGP-Routererkundung** auf **Nein**fest. Beachten Sie, dass das Aktivieren dieser Eigenschaft zu Leistungsproblemen führen kann, einschließlich Problemen aufgrund von unzureichendem Arbeitsspeicher auf dem MID-Server. • **Typ**: true | false • **Standardwert**: true
glide.discovery.debug.network_discovery	Debugging der Netzwerkerkennung: Ermöglicht die umfassende Protokollierung aller Netzwerk-Discovery-Aktivitäten auf der Instanz. • **Typ**: true | false • **Standardwert**: true • **Mehr erfahren**: Monitoring von Erkennungen und Problemlösung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
glide.discovery.discoverable.network.max.netmask.bits	Maximale Netzmaskengröße für auffindbare Netzwerke (Bits): Die maximale Anzahl von Bits in einer regulären Netzmaske für Netzwerke, die von einer Netzwerk-Discovery erkannt werden. Eine reguläre Netzmaske ist eine Netzmaske, die binär als eine Zeichenfolge von Einsen, gefolgt von einer Zeichenfolge von Nullen, ausgedrückt werden kann. Beispiel: 255.255.255.0 ist regulär, und 255.255.255.64 ist irregulär. Reguläre Netzwerke werden im Allgemeinen wie folgt ausgedrückt: 10.0.0.0/24, d. h. eine Netzwerkadresse von 10.0.0.0 mit einer Netzmaske von 255.255.255.0. Größere Bitzahlen bedeuten Netzwerke mit einer kleineren Anzahl von Adressen. Beispielsweise enthält das Netzwerk 10.128.0.128/30 vier Adressen: eine Netzwerkadresse (10.128.0.128), eine Broadcast-Adresse (10.128.0.131) und zwei verwendbare Adressen (10.128.0.129 und 10.128.0.130). Kleine Netzwerke werden normalerweise in Netzwerkgeräten konfiguriert, damit Loopback-Adressen oder Netzwerke bereitgestellt werden können, die ausschließlich von Punkt-zu-Punkt-Verbindungen verwendet werden. Da diese Arten von Netzwerken im Allgemeinen nicht von Netzwerk Discovery entdeckt werden müssen, wäre es nützlich, sie herauszufiltern. Wenn Sie diese Eigenschaft auf einen Wert von 1 bis 32 festlegen, können Sie die Größe der erkannten regulären Netzwerke begrenzen. Wenn Sie einen anderen Wert festlegen, werden alle Netzwerke erkannt. Unregelmäßige Netzwerke werden immer entdeckt. Der Standardwert ist 28, was bedeutet, dass reguläre Netzwerke mit 8 oder weniger Adressen nicht erkannt werden können. • **Typ**: Ganzzahl • **Standardwert**: 28
glide.discovery.network_owner_method	Auswahlmethode für Netzwerkrouter: Diese Eigenschaft steuert die Methode, die zur Entscheidung verwendet wird (während Netzwerk Discovery) welcher Router als Router ausgewählt werden soll, der einem bestimmten IP-Netzwerk zugeordnet werden soll. Die möglichen Werte sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Erster Router**: Der erste Router, der erkennt, dass das Netzwerk zugeordnet ist • **Letzter Router**: Der letzte Router, der erkennt, dass das Netzwerk zugeordnet ist • **Die meisten Netzwerke**: Der Router mit den meisten angehängten Netzwerken ist zugeordnet • **Wenigste Netzwerke**: Der Router mit den wenigsten verbundenen Netzwerken ist zugeordnet • **Typ**: Auswahlliste • **Standardwert**: Die meisten Netzwerke • **Zusatzoptionen**: Erster Router, Letzter Router, Die wenigsten Netzwerke
glide.discovery.physical_interface_types	Physikalische Schnittstellentypen: Eine durch Kommas getrennte Liste von Schnittstellentypen, die für die Netzwerkerkennung als physisch angesehen werden. Wenn ein Router (oder ein weiterleitungsfähiges Gerät) über eine Schnittstelle dieses Typs verfügt, werden die mit dieser Schnittstelle verbundenen Netzwerke als lokal mit diesem Gerät verbunden angesehen. Die Standardschnittstellentypen umfassen die Typen Ethernet, 802.11 und Token Ring. Schnittstellentypnummern sind in der SNMP MIB-2 definiert, insbesondere in der OID 1.3.6.1.2.1.2.2.1.3. • **Typ**: Zeichenfolge • **Standardwert**: 6,117,9,71,209
glide.discovery.switch_interface_types	Switch-Schnittstellentypen: Kommagetrennte Liste von Schnittstellentypen, die berücksichtigt werden. Schnittstellentypnummern sind in der SNMP MIB-2 definiert, insbesondere in der OID 1.3.6.1.2.1.2.2.1.3. Geräte mit beliebigen Schnittstellentypen, die NICHT in dieser Liste angezeigt werden, werden als Router klassifiziert, wenn sie über Weiterleitungsfunktionen verfügen. Eine vollständige Liste der Schnittstellentypnummern finden Sie auf der IANA-Website im Abschnitt „ifType-Definitionen.“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Typ**: Zeichenfolge • **Standardwert**: 7,8,9,26,53,62,69,71,78,115,117,209

Mehr erfahren

Was ist Netzwerk-Discovery?

Netzwerkerkennung ausführen

Konfigurieren Sie die Netzwerkennung mit Discovery über einen Discovery-Zeitplan.

Vorbereitungen

Erforderliche Rolle: keine

Konfigurieren Sie SNMP-Anmeldeinformationen oder (optional) SSH-Anmeldeinformationen . Port 161 muss für SNMP-Zugriff und Port 22 für SSH-Zugriff geöffnet sein.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**.
2. Klicken Sie auf **Neu**, und wählen Sie **Netzwerke** aus der Liste im Feld *Erkennen* aus.
3. Wählen Sie einen MID Server aus.

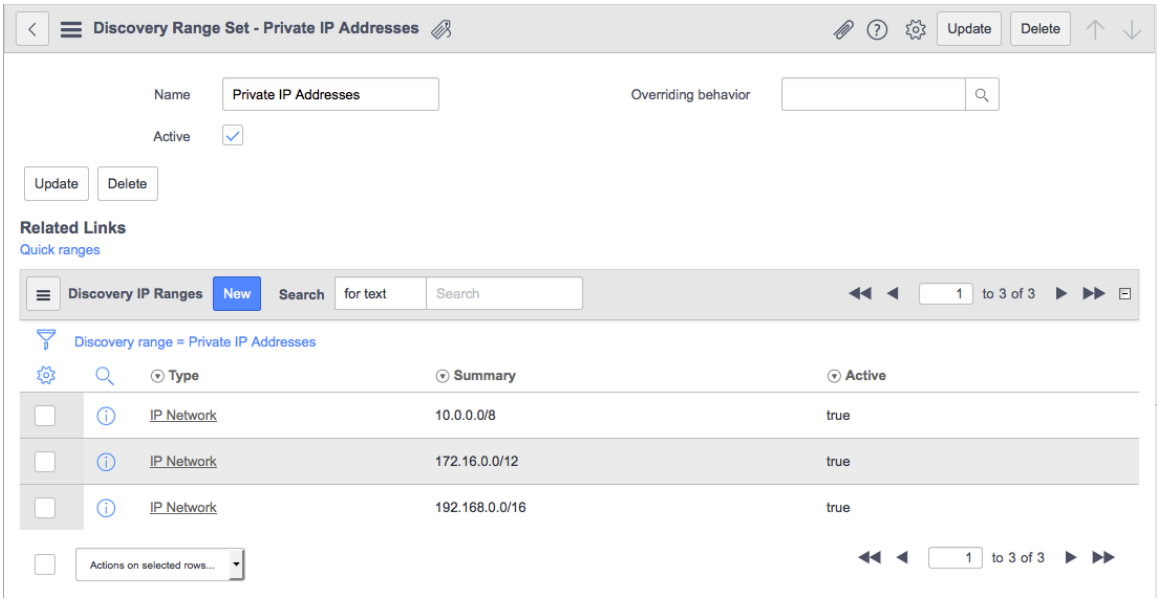
   Dieses Feld ist ein Pflichtfeld.
4. Füllen Sie das Formular einschließlich der Planungsfelder aus.
5. Klicken Sie mit der rechten Maustaste in die Headerleiste, und wählen Sie im Kontextmenü **Speichern** aus.

   Der Bereich **Zugehörige Links** wird mit zugehörigen Listen angezeigt.
6. Klicken Sie unter „Zugehörige Links“ auf **Private Netzwerk-Discovery-IPs**, um die Liste der standardmäßigen privaten IP-Netzwerke in der zugehörigen Liste *Discovery-IP-Bereiche* anzuzeigen.

   Die Standard-IP-Netzwerke in dieser Liste sind für jede von Ihnen durchgeführte Netzwerkerkennung mit Discovery verfügbar und für die meisten Erkennungen ausreichend.
7. Wenn Ihre Organisation über zusätzliche private IP-Adressen verfügt, klicken Sie auf **Neu**, um sie hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Private IP-Adressen

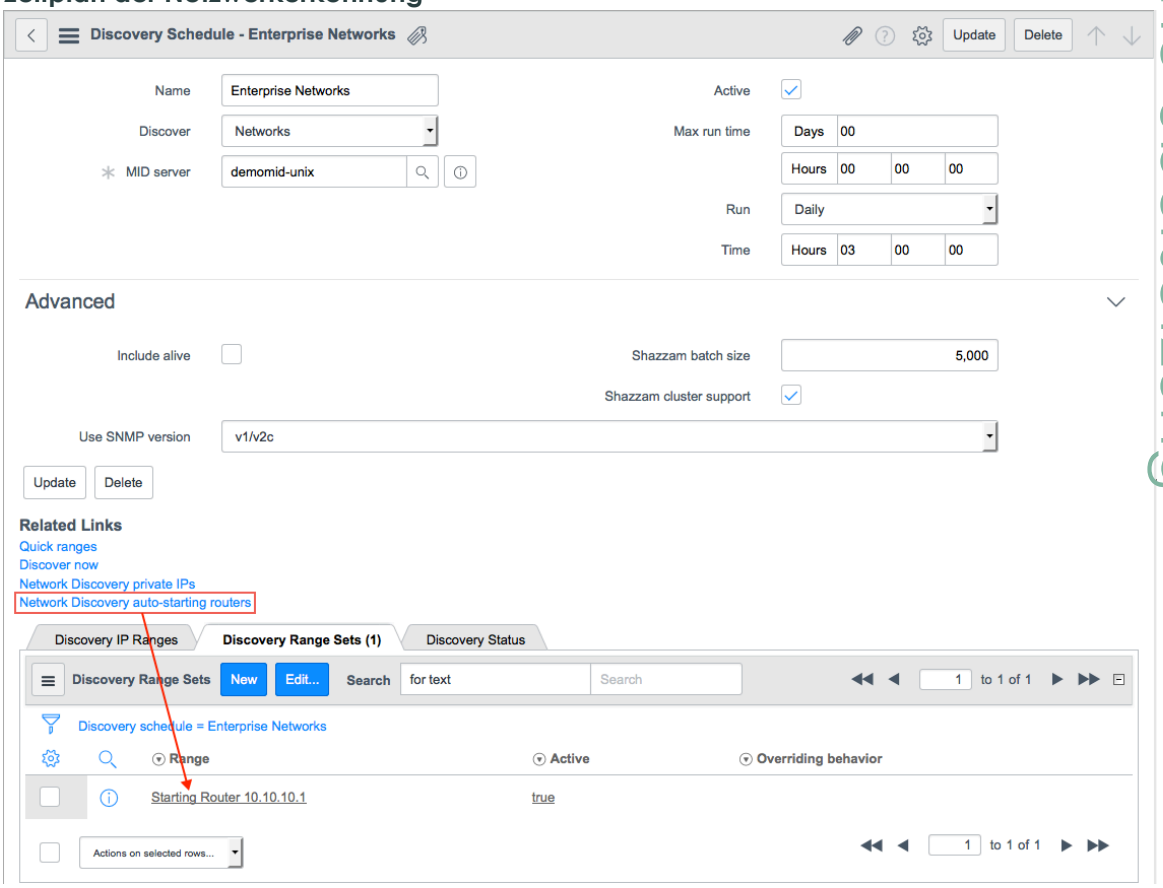


8. Fügen Sie dem Zeitplan in der Liste *Discovery-Range Sets* Startrouter hinzu.

   a. Klicken Sie auf den Link **Netzwerk-Discovery-Auto-Start-Router**, um die Liste mit dem Startrouter für jeden MID Server in Ihrem Netzwerk zu füllen.

   b. Klicken Sie auf **Bearbeiten**, um der Liste Router hinzuzufügen bzw. daraus zu löschen.

Zeitplan der Netzwerkerkennung



9. Führen Sie die Discovery manuell oder über den Zeitplaner aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Netzwerke in Discovery-Range Sets konvertieren

Nachdem Sie mit Discovery eine Netzwerkerkennung ausgeführt haben, müssen Sie die erkannten IP-Netzwerke in Range Sets konvertieren, um sie zur Erkennung anderer Geräte nutzen zu können.

Vorbereitungen

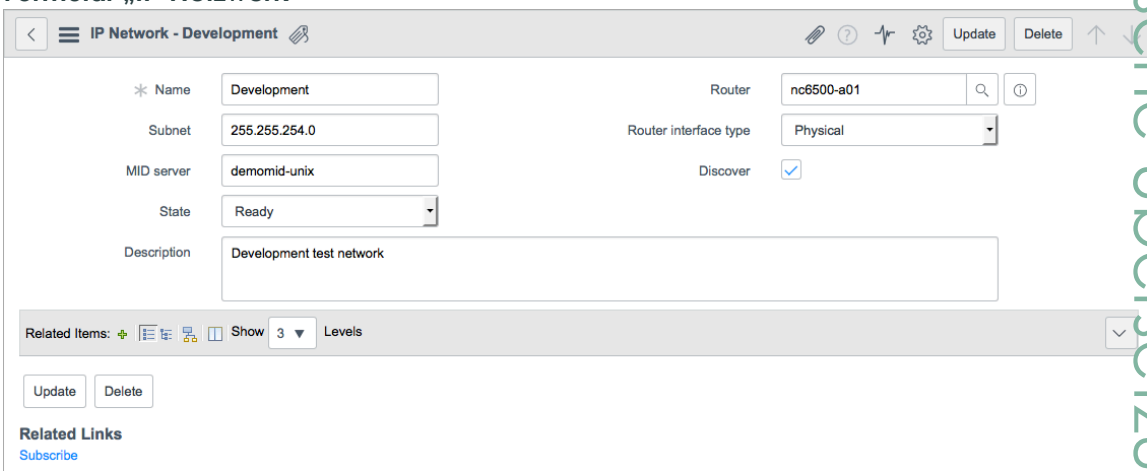
Erforderliche Rolle: agent_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Ausgabe und Artefakte** > **IP-Netzwerke**.
2. Klicken Sie auf **Neu**, um ein IP-Netzwerk hinzuzufügen.
3. Stellen Sie sicher, dass die folgenden Feldwerte bereitgestellt werden:
   - **Status**: Bereit
   - **Erkennen**: Aktiviert (true)
   - **Router**: Wählen Sie in der Liste einen Router aus. Dieses Feld darf nicht leer sein.

   Wenn Ihre IP-Netzwerke über eine Netzwerkerkennung mit Discovery erstellt wurden, werden diese Felder in der zugehörigen Liste *IP-Netzwerke* automatisch gefüllt. Wenn Sie die IP-Netzwerke jedoch manuell eingegeben haben und Sie Ihre IP-Netzwerke manuell in Range Sets konvertieren möchten, müssen Sie die Felder entsprechend bearbeiten.

Formular „IP-Netzwerk“



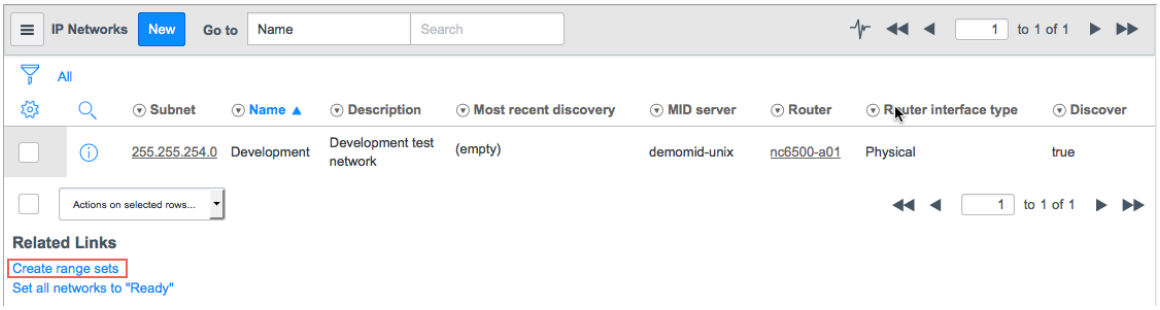
4. Klicken Sie auf **Aktualisieren**, um zur Liste der IP-Netzwerke zurückzukehren.
5. Klicken Sie unter **Zugehörige Links** auf **Range Sets erstellen**.

   Verwenden Sie diese Funktion, um alle IP-Netzwerke in der Liste in Range Sets zu konvertieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste der IP-Netzwerke



Die Seite Discovery-Status wird eingeblendet und zeigt den Fortschritt der Konvertierung an. Unter **Gestartet** und **Abgeschlossen** erhöht sich die Anzahl der IP-Netzwerke, bis alle Netzwerke konvertiert wurden.

Nächste Maßnahme

Fügen Sie Erkennungszeitplänen Discovery-Range Sets hinzu.

Einem Erkennungszeitplan Discovery-Range Sets hinzufügen

Nachdem Sie mithilfe einer Netzwerkerkennung Discovery-Range Sets erzeugt haben, fügen Sie diese Sätze einem Erkennungszeitplan hinzu. Dieser Prozess schränkt den Bereich der IP-Adressen ein, die Shazzam-Probes scannen können. Sie können auch ein Verhalten hinzufügen.

Vorbereitungen

Erforderliche Rolle: agent_admin oder admin

Prozedur

1. Öffnen Sie einen Erkennungszeitplan.
2. Klicken Sie in der zugehörigen Liste **Discovery-Range Sets** auf **Bearbeiten**, um ein vorhandenes Range Set hinzuzufügen, und verwenden Sie den Slushbucket, um das Range Set hinzuzufügen.
3. Klicken Sie im Formular **Discovery-Zeitplan** in der Spalte **Bereich** der zugehörigen Liste **Discovery-Range Sets** auf den Namen des Range Set.
4. Fügen Sie im Formular **Discovery Bereich** ein Discovery-Verhalten hinzu.
   Sie können auch das für diesen Zeitplan festgelegte Range Set aktivieren oder deaktivieren.
5. Klicken Sie mit der rechten Maustaste auf den Header, und wählen Sie **Speichern** aus.

Serverlose Erkennung

Discovery kann Anwendungen auf Hostcomputern suchen, ohne zunächst den Host erkennen zu müssen. Diese Art von Erkennung wird als serverlose Discovery bezeichnet.

Die serverlose Erkennung basiert auf Infrastrukturmustern zum Untersuchen von CIs auf einem Host. Bei dieser Art von Erkennung werden die Scanphase und Klassifizierungsphase der Erkennung übersprungen. Es gibt zwei Arten der serverlosen Erkennung: standardmäßig und hostbasiert. Beide Typen erfordern ein Infrastrukturmuster.

Standardmäßige serverlose Discovery

Bei der standardmäßigen serverlosen Erkennung werden CIs von Remoteanwendungen erkannt, die sich auf einem unbekannten Host befinden. Bei dieser Art der serverlosen Erkennung werden für die Suche nach CIs Protokolle wie REST und HTTP verwendet. Die IP-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Adresse des Hostcomputers ist nicht erforderlich. Sie definieren Eingabeparameter in einem Infrastrukturmuster, um eine Verbindung zu einer Remoteressource herzustellen. Verwenden Sie diese Art der Erkennung, wenn Sie webbasierte Anwendungen erkennen möchten.

Hostbasierte serverlose Erkennung

Mit der hostbasierten serverlosen Erkennung kann nach CIs gesucht werden, die sich auf einem bereits erkannten Hostcomputer befinden. Der Host fungiert als Proxy, über den Sie andere CIs finden. Sie führen Discovery nicht tatsächlich für den Host aus. Verwenden Sie diese Art von Erkennung in folgenden Fällen:

- Sie kennen die IP-Adresse der CIs nicht, die erkannt werden sollen, oder die CIs haben gar keine IP-Adressen.
- Die CIs befinden sich auf einem bereits erkannten Host-CI.

Für diese Art von Erkennung benötigen Sie auch ein Infrastrukturmuster, müssen aber keine Eingabeparameter wie bei der standardmäßigen serverlosen Erkennung definieren. Das Muster kann Vorgänge angeben, zum Beispiel eine WMI-Abfrage, die Abfragen auf einem Host ausführt. Nachdem Discovery eine Verbindung zum Host hergestellt hat, werden die Anmeldeinformationen des Hosts verwendet, um die Erkennung der CIs durchzuführen, die Sie im Muster erkunden. Sie müssen keine zusätzlichen Anmeldeinformationen angeben. Wenn Sie für das Muster den Debug-Modus ausführen, werden unter **Vorübergehende Variablen** Details zum Muster angezeigt. Sie können dann Mustervorgänge erstellen, die API-Aufrufe vom Host an die CIs tätigen, die Sie erkennen möchten.

Serverlose Erkennungszeitpläne

Die Infrastrukturmuster, die durch die serverlose Erkennung verwendet werden, werden durch einen Erkennungszeitplan und nicht durch einen Klassifizierer ausgelöst. Bei der serverlosen Erkennung werden Klassifizierer ignoriert. Verwenden Sie einen serverlosen Zeitplantyp für beide Arten der serverlosen Erkennung. Im serverlosen Zeitplan können Sie Folgendes angeben:

- Werte für Eingabeparameter im Muster, wenn Sie die standardmäßige serverlose Erkennung verwenden. Anweisungen dazu finden Sie unter Zeitplan für standardmäßige serverlose Erkennung erstellen.
- Ein Host-CI, wenn Sie eine Proxy-Host-basierte Erkennung verwenden. Weitere Informationen finden Sie unter Zeitplan für hostbasierte serverlose Erkennung erstellen.

Muster und Zeitplan für standardmäßige serverlose Erkennung erstellen

Um Anwendungs-CIs auf einem unbekannten Host zu erkennen, erstellen Sie ein Infrastrukturmuster für die standardmäßige serverlose Erkennung. Nachdem Sie das Muster erstellt haben, erstellen Sie einen Erkennungszeitplan, der das Muster auslöst.

Vorbereitungen
Erforderliche Rolle: cloud_admin, service_mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Zur Erkundung des CI müssen Sie im Muster Eingabeparameter angeben.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**.
2. Klicken Sie auf **Neu**.
3. Geben Sie ein Muster vom Typ **Infrastruktur** mit dem richtigen CI-Typ an, der für die CIs gilt, die Sie erkennen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

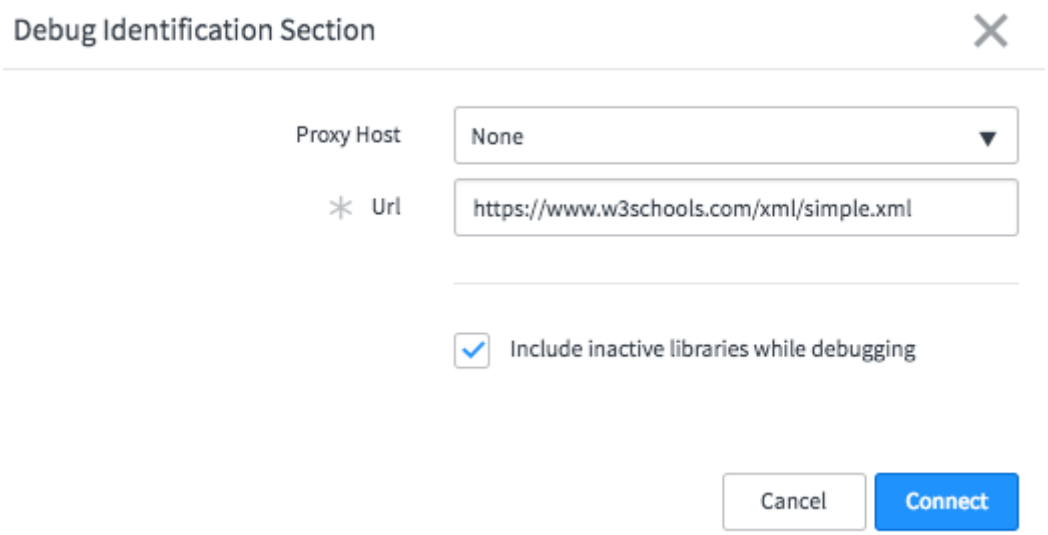
Unter Muster erstellen oder anpassen werden alle Formularfelder erläutert.

4. Erstellen Sie einen Identifizierungsabschnitt, und speichern Sie das Muster.
5. Klicken Sie auf die Registerkarte **Eingabeparameter** und dann auf **Neu**.
6. Geben Sie die Parameter ein, die zum Erreichen der serverlosen CIs erforderlich sind. Beispielsweise können Sie eine `URL` eingeben, um eine Remoteressource über eine HTTP-Anforderung zu erreichen.

   Hinweis: In einem serverlosen Erkennungszeitplan geben Sie die tatsächliche URL an.

7. Speichern Sie das Muster.
8. Wählen Sie die Registerkarte **Standard** aus, und klicken Sie dann auf den Namen des Identifizierungsabschnitts, um den Musterdesigner zu öffnen.
9. Erstellen Sie die erforderlichen Schritte zur Erkundung serverloser CIs.
   Erstellen Sie beispielsweise einen Vorgang vom Typ **HTTP Get-Aufruf**, um eine Remoteressource über eine URL zu erreichen. In diesem Fall geben Sie den Parameter `$url` im Feld **URL** an.
10. Um das Muster zu testen, klicken Sie auf **Debug-Modus**, und geben Sie Werte für die Eingabeparameter ein.
    Sie müssen keinen Wert für **Proxy-Host** eingeben. In diesem Beispiel stellen wir eine Verbindung zu einer Website her, die eine XML-Datei bereitstellt. Die Analysemethode für XML-Dateien ist bereits im HTTP Get-Aufruf definiert. Um den Mustervorgang zu testen, klicken Sie auf **Debug-Modus**, geben die URL ein, und klicken auf **Verbinden**.

Beispiel für Debugging eines HTTP Get-Aufrufs



11. Nachdem Sie eine Verbindung hergestellt und den Vorgang ausgeführt haben, wird der Inhalt im Feld **Ausgabe** angezeigt.

Zeitplan für standardmäßige serverlose Erkennung erstellen

Nachdem Sie ein Muster für die standardmäßige serverlose Erkennung erstellt haben, erstellen Sie einen Erkennungszeitplan und geben das Muster an. Discovery löst das Muster aus dem Zeitplan und nicht über den Klassifizierer aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass Sie Anmeldeinformationen für die Standardauthentifizierung für HTTP-Aufrufe im Muster haben.

Erforderliche Rolle: cloud_admin, service_mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können diesen Zeitplan erneut verwenden, um dasselbe Muster mit anderen Parametern auszuführen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Zeitpläne**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Ohne Server** im Feld **Discovery** aus.
   Unter Horizontale Erkennung planen werden die anderen Felder erläutert.
4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Klicken Sie in der zugehörigen Liste **Ausführungsmuster ohne Server** auf **Neu**.
6. Füllen Sie die Formularfelder aus (siehe Tabelle):

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Muster	Wählen Sie das Muster aus, das Sie für die standardmäßige serverlose Erkennung oder für die Proxy-Host-basierte Erkennung erstellt haben.
Proxy-Host	Lassen Sie dieses Feld leer. Dieses Feld bezieht sich auf das Proxy-Host-basierte Szenario.
Aktiv	Lassen Sie dieses Kontrollkästchen aktiviert, um die Musterausführungsdefinition zu verwenden.

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
8. Fügen Sie in der zugehörigen Liste **„Startprogrammparameter für Discovery-Muster“** die für das Muster erforderlichen Parameter hinzu, und geben Sie für jeden Parameter in der Spalte **„Wert“** einen Wert an.
9. Klicken Sie auf **Absenden**.
10. Definieren Sie so viele Datensätze für serverlose Ausführungsmuster wie erforderlich.
    Sie können dasselbe Muster starten, es muss jedoch jeweils unterschiedliche Parameter aufweisen.
11. Führen Sie die Erkennung aus, indem Sie auf **Discovery starten** klicken, oder warten Sie, bis die Erkennung durch den Zeitplan ausgelöst wird.

Ergebnisse

Überprüfen Sie den Discovery-Status, um das Discovery-Protokoll, die Geräteliste mit den ermittelten CIs und die ECC-Warteschlangendatensätze anzuzeigen. Beachten Sie, dass die Shazzam-Sonde nicht gestartet wurde und Discovery keine Klassifizierungs-Sonden ausgelöst hat.

Zugehörige Informationen

Discovery-Status

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster und Zeitplan für hostbasierte serverlose Erkennung erstellen

Um Anwendungs-CIs auf einem in der CMDB bekannten Host zu erkennen, erstellen Sie ein Infrastrukturmuster für die hostbasierte serverlose Erkennung. Nachdem Sie das Muster erstellt haben, erstellen Sie einen Erkennungszeitplan, der das Muster auslöst.

Vorbereitungen
Erforderliche Rolle: cloud_admin, service_mapping_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**.
2. Klicken Sie auf **Neu**.
3. Geben Sie ein Muster vom Typ **Infrastruktur** mit dem richtigen CI-Typ an, der für die CIs gilt, die Sie erkennen möchten.
   Unter Muster erstellen oder anpassen werden alle Formularfelder erläutert.
4. Erstellen Sie einen Identifizierungsabschnitt, und speichern Sie das Muster.
5. Fügen Sie dem Muster Vorgänge hinzu, um das CI zu erkennen, auf das Sie über den Host zugreifen können.
6. Zum Testen des Musters klicken Sie auf **Debug-Modus**, und geben Sie die IP-Adresse des Hosts ein.

Zeitplan für hostbasierte serverlose Erkennung erstellen

Discovery löst das Muster für die hostbasierte serverlose Erkennung aus dem Zeitplan und nicht über den Klassifizierer aus.

Vorbereitungen
Erforderliche Rolle: cloud_admin, service_mapping_admin oder admin

Stellen Sie sicher, dass Sie über Anmeldeinformationen für das Hostgerät verfügen, das als Proxy fungiert.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Zeitpläne**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Ohne Server** im Feld „Discovery“ aus.
   Unter Horizontale Erkennung planen werden die anderen Felder erläutert.
4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Klicken Sie in der zugehörigen Liste **Ausführungsmuster ohne Server** auf **Neu**.
6. Füllen Sie die Formularfelder aus (siehe Tabelle):

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Muster	Wählen Sie das Muster aus, das Sie für die hostbasierte Erkennung erstellt haben.
Proxy-Host	Wenn Sie die hostbasierte Erkennung verwenden, geben Sie ein vorhandenes CMDB-CI an. Discovery verwendet die Anmeldeinformationen dieses CI bei der Erkundung der CIs auf dem Host.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Lassen Sie dieses Kontrollkästchen aktiviert, um die Musterausführungsdefinition zu verwenden.

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

   Definieren Sie so viele Datensätze für serverlose Ausführungsmuster wie erforderlich. Sie können dasselbe Muster starten, es muss jedoch jeweils unterschiedliche Parameter aufweisen.

   Hinweis: Sie müssen keine Einträge in der zugehörigen Liste **Startprogrammparameter für Discovery-Muster** erstellen.

8. Führen Sie die Erkennung aus, indem Sie auf **Discovery starten** klicken, oder warten Sie, bis die Erkennung durch den Zeitplan ausgelöst wird.

Ergebnisse
Überprüfen Sie den Discovery-Status, um das Discovery-Protokoll, die Geräteliste mit den ermittelten CIs und die ECC-Warteschlangendatensätze anzuzeigen. Beachten Sie, dass die Shazzam-Sonde nicht gestartet wurde und Discovery keine Klassifizierungs-Sonden ausgelöst hat.

Discovery konfigurieren

Konfigurieren Sie die Elemente, die Discovery für die Erkundung Ihres Netzwerks benötigt, zum Beispiel Anmeldeinformationen, Zeitpläne und IP-Adressen.

Konfiguration – Übersicht

Discovery kann nach einem regulären, konfigurierbaren Zeitplan ausgeführt oder manuell gestartet werden. Die von Ihnen angegebenen IP-Adressbereiche informieren Discovery darüber, welche spezifischen Geräte untersucht werden sollen. Zum Abrufen nützlicher Informationen benötigt Discovery Anmeldeinformationen für Geräte in einem bestimmten Bereich, damit Discovery eine Verbindung zu den erkannten Geräten herstellen und verschiedene Probes für sie ausführen kann. Discovery vergleicht die erkannten Geräte mit Konfigurationselementen (CI) in der CMDB und aktualisiert alle passenden Geräte. Wenn Discovery kein passendes CI in der CMDB findet, wird ein CI erstellt.

Verfahrensweisen zur Konfiguration von Discovery

Über die folgenden Links erhalten Sie Informationen zur Konfiguration von Discovery für Ihre Umgebung. Zur Ausführung von Discovery müssen Sie nicht alle diese Verfahren durchführen. Die Plattform stellt viele Standardwerte bereit, die für die meisten Erkennungsvorgänge geeignet sind und die Sie für die Erkundung Ihres Netzwerks verwenden können. Um Discovery schnell verwenden zu können, verwenden Sie das Guided Setup, mit dessen Hilfe Sie die Einrichtung einer einfachen Erkennung beschleunigen können.

Verfahrensweisen zur Konfiguration

Konfiguration der Discovery-IP-Adresse	Discovery-Klassifizierer	Discovery-Status
Domänentrennung und Erkennung	Parameter der Discovery-Klassifizierung	Discovery Konfigurationskonsole

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verfahrensweisen zur Konfiguration (Fortsetzung)

SNMP-Unterstützung für Discovery	Discovery-Bezeichner	Discovery-Dashboard
Discovery und SCCM zusammen	Discovery-Eigenschaften	Discovery-Homepage

Discovery-Eigenschaften

Mit Discovery-Eigenschaften können Sie zahlreiche Aspekte des horizontalen Erkennungsprozesses steuern.

Navigieren zu **Discovery-Definition** > **Eigenschaften** um diese Eigenschaften zu bearbeiten:

IP-Eigenschaften

Feld	Beschreibung
glide.discovery.exclude_ip_sync_classes	Definiert CI-Klassen, deren IP-Adressen nicht ersetzt werden dürfen, wenn die von Discovery zurückgegebene Adresse nicht mit einer der NICs des Geräts übereinstimmt. Verwenden Sie eine durch Kommas getrennte Liste, um mehrere Klassen zu definieren. Vom System wird im CI-Datensatz standardmäßig die Verwaltungs-IP eines Lastenausgleichsmoduls verwendet, die von Discovery zurückgegeben wird, anstatt sie durch die IP-Adresse einer der NICs des Lastenausgleichsmoduls zu ersetzen. • **Typ**: Zeichenfolge • **Standardwert**: cmdb_ci_lb
glide.discovery.enforce_unique_ips	Eindeutige IP-Adressen erzwingen: Die IP-Adresse wird ignoriert, nachdem nachfolgende Geräte von Discovery gefunden worden sind, die dieselbe IP-Adresse verwenden. Jedes Mal, wenn ein Computer, ein Drucker oder ein Netzwerkgerät mit einer gültigen IP-Adresse erkannt wird, wird das IP-Adressfeld aller anderen Geräte mit derselben IP-Adresse gelöscht. Wenn inaktiv, wird die IP-Adresse für jedes Gerät gespeichert. • **Typ**: true | false • **Standardwert**: false

Netzwerkeigenschaften

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
glide.discovery.bgp_router_disable	BGP-Routererkundung deaktiviert: Deaktivierung der Ausführung des Probe **SNMP – Routing** oder des Musters, wenn ein Router erkannt wird, von dem das BGP-Protokoll ausgeführt wird. Normalerweise ist diese Suche aufgrund der Größe von BGP-Routing-Tabellen inaktiv und weil solche Router im Allgemeinen nur am Rande großer Netzwerke arbeiten, wo eine weitere Netzwerk-Discovery irrelevant wäre. Dieser Wert könnte auf „falsch“ gesetzt werden, wenn Ihr Unternehmen nur BGP-Router als Edge-Router zwischen relativ kleinen Netzwerken (z. B. zwischen Gebäuden auf einem einzelnen Campus) verwendet. Wenn Sie die Tabelle [discovery_device_neightors] während der horizontalen Layer-2-Discovery der BGP-fähigen Geräte ausfüllen müssen, legen Sie die Eigenschaft **Deaktivieren der BGP-Routererkundung** auf **Nein**fest. Beachten Sie, dass das Aktivieren dieser Eigenschaft zu Leistungsproblemen führen kann, einschließlich Problemen aufgrund von unzureichendem Arbeitsspeicher auf dem MID-Server. • **Typ**: true | false • **Standardwert**: true
glide.discovery.debug.network_discovery	Debugging der Netzwerkerkennung: Ermöglicht die umfassende Protokollierung aller Netzwerk-Discovery-Aktivitäten auf der Instanz. • **Typ**: true | false • **Standardwert**: true • **Mehr erfahren**: Monitoring von Erkennungen und Problemlösung
glide.discovery.discoverable.network.max.netmask.bits	Maximale Netzmaskengröße für auffindbare Netzwerke (Bits): Die maximale Anzahl von Bits in einer regulären Netzmaske für Netzwerke, die von einer Netzwerk-Discovery erkannt werden. Eine reguläre Netzmaske ist eine Netzmaske, die binär als eine Zeichenfolge von Einsen, gefolgt von einer Zeichenfolge von Nullen, ausgedrückt werden kann. Beispiel: 255.255.255.0 ist regulär, und 255.255.255.64 ist irregulär.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Reguläre Netzwerke werden im Allgemeinen wie folgt ausgedrückt: 10.0.0.0/24, d. h. eine Netzwerkadresse von 10.0.0.0 mit einer Netzmaske von 255.255.255.0. Größere Bitzahlen bedeuten Netzwerke mit einer kleineren Anzahl von Adressen. Beispielsweise enthält das Netzwerk 10.128.0.128/30 vier Adressen: eine Netzwerkadresse (10.128.0.128), eine Broadcast-Adresse (10.128.0.131) und zwei verwendbare Adressen (10.128.0.129 und 10.128.0.130). Kleine Netzwerke werden normalerweise in Netzwerkgeräten konfiguriert, damit Loopback-Adressen oder Netzwerke bereitgestellt werden können, die ausschließlich von Punkt-zu-Punkt-Verbindungen verwendet werden. Da diese Arten von Netzwerken im Allgemeinen nicht von Netzwerk Discovery entdeckt werden müssen, wäre es nützlich, sie herauszufiltern. Wenn Sie diese Eigenschaft auf einen Wert von 1 bis 32 festlegen, können Sie die Größe der erkannten regulären Netzwerke begrenzen. Wenn Sie einen anderen Wert festlegen, werden alle Netzwerke erkannt. Unregelmäßige Netzwerke werden immer entdeckt. Der Standardwert ist 28, was bedeutet, dass reguläre Netzwerke mit 8 oder weniger Adressen nicht erkannt werden können. • **Typ**: Ganzzahl • **Standardwert**: 28
glide.discovery.network_owner_method	Auswahlmethode für Netzwerkrouter: Diese Eigenschaft steuert die Methode, die zur Entscheidung verwendet wird (während Netzwerk Discovery) welcher Router als Router ausgewählt werden soll, der einem bestimmten IP-Netzwerk zugeordnet werden soll. Die möglichen Werte sind: • **Erster Router**: Der erste Router, der erkennt, dass das Netzwerk zugeordnet ist • **Letzter Router**: Der letzte Router, der erkennt, dass das Netzwerk zugeordnet ist • **Die meisten Netzwerke**: Der Router mit den meisten angehängten Netzwerken ist zugeordnet • **Wenigste Netzwerke**: Der Router mit den wenigsten verbundenen Netzwerken ist zugeordnet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Typ**: Auswahlliste • **Standardwert**: Die meisten Netzwerke • **Zusatzoptionen**: Erster Router, Letzter Router, Die wenigsten Netzwerke
glide.discovery.physical_interface_types	Physikalische Schnittstellentypen: Eine durch Kommas getrennte Liste von Schnittstellentypen, die für die Netzwerkerkennung als physisch angesehen werden. Wenn ein Router (oder ein weiterleitungsfähiges Gerät) über eine Schnittstelle dieses Typs verfügt, werden die mit dieser Schnittstelle verbundenen Netzwerke als lokal mit diesem Gerät verbunden angesehen. Die Standardschnittstellentypen umfassen die Typen Ethernet, 802.11 und Token Ring. Schnittstellentypnummern sind in der SNMP MIB-2 definiert, insbesondere in der OID 1.3.6.1.2.1.2.2.1.3. • **Typ**: Zeichenfolge • **Standardwert**: 6,117,9,71,209
glide.discovery.switch_interface_types	Switch-Schnittstellentypen: Kommagetrennte Liste von Schnittstellentypen, die berücksichtigt werden. Schnittstellentypnummern sind in der SNMP MIB-2 definiert, insbesondere in der OID 1.3.6.1.2.1.2.2.1.3. Geräte mit beliebigen Schnittstellentypen, die NICHT in dieser Liste angezeigt werden, werden als Router klassifiziert, wenn sie über Weiterleitungsfunktionen verfügen. Eine vollständige Liste der Schnittstellentypnummern finden Sie auf der IANA-Website im Abschnitt „ifType-Definitionen.“ • **Typ**: Zeichenfolge • **Standardwert**: 7,8,9,26,53,62,69,71,78,115,117,209

Andere Discovery-Eigenschaften

Feld	Beschreibung
com.snc.use_external_credentials	Ermöglicht die Verwendung des externen Speichers von Anmeldeinformationen. • **Typ**: true | false • **Standardwert**: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
glide.discovery.active_processes_filter	Active Processes Filter: Optimierung für die Zuordnung von Anwendungsabhängigkeiten. Filtert die aktiven Prozesse, die von zurückgegeben werden Discovery Nur für diejenigen, die eine Übereinstimmung in der Prozessklassifikationstabelle haben. • **Typ**: true | false • **Standardwert**: false
glide.discovery.adme.aggregation_interval	ADME – Aggregationsintervall (Sek): Wie oft (in Sekunden) sofortige Daten in Blöcke zusammengefasst werden. Es muss mindestens 60 Sekunden betragen und es muss ein Vielfaches des ADME-Abtastintervalls sein. • **Typ**: integer • **Standardwert**: 3600
glide.discovery.adme.base_dir_unix	ADME – Unix-Basisverzeichnis: Ein vorhandenes Verzeichnis auf den UNIX-Zielcomputern, die als Arbeitsbereich verwendet werden sollen. Muss ein absoluter Pfad zum Verzeichnis sein. • **Typ**: true | false • **Standardwert**: false
mid.powershell.target_base_dir	PowerShell – Zielbasisverzeichnis: Eine Netzwerkfreigabe auf den Ziel-Windows-Computern, die als Arbeitsbereich verwendet werden sollen. • **Typ**: Zeichenfolge • **Standardwert**: admin$\temp
glide.discovery.adme.max_total_samples	ADME – Maximale Anzahl Samples: Die Anzahl der vom Skript genommenen Samples. Die Ausführung des Skripts wird nach Abschluss dieser Probenanzahl beendet. • **Typ**: Ganzzahl • **Standardwert**: 100
glide.discovery.adme.rolling_window_size	ADME - Rollfende Fenstergröße. Wie viele kürzlich aggregierte Blöcke sollen gespeichert werden? Ein aggregierter Block besteht aus dem ADME-Aggregationsintervall und den ADME-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Abtastintervallabtastungen. Nur die neuesten Blöcke werden beibehalten. • **Typ**: Ganzzahl • **Standardwert**: 24
glide.discovery.adme.sampling_interval	ADME - Abtastintervall (Sek): Wie oft werden Prozess- und Verbindungsdaten in Sekunden erfasst? Muss mindestens 5 Sekunden betragen. • **Typ**: Ganzzahl • **Standardwert**: 120
glide.discovery.adm.update.applications	Steuert, ob Anwendungs-CIs basierend auf dem Status des laufenden Prozesses aktualisiert werden sollen. Wenn Discovery den Server erneut erkennt und feststellt, dass ein zuvor ausgeführter Prozess im Datensatz cmdb_running_process nicht mehr aktiv ist, wird Absent auf **true**festgelegt. Darüber hinaus wird install_status für das zugehörige Anwendungs-CI von „Installiert“ auf „Abwesend“ aktualisiert. Wenn der laufende Prozess für das zugehörige Anwendungs-CI bei nachfolgenden Scans wieder online ist, wird install_status auf „Installiert“ zurückgesetzt. **Hinweis:** Dieses Verhalten funktioniert nur für Anwendungs-CIs, die mithilfe von Mustern erkannt werden. • **Typ**: true | false • **Standardwert**: true (für zbooted-Instanzen oder neue Aktivierungen)
glide.discovery.allow_loopback_adapters	Loopback-Adapter-Filter: Ermöglicht, dass Netzwerk-Loopback-Adaptern auf SNMP-Geräten erkannt werden, anstatt bei der Erkennung herausgefiltert zu werden. Wenn diese Eigenschaft auf **wahr** festgelegt ist, werden Netzwerk-Loopback-Adressen erkannt und der CMDB hinzugefügt. • **Typ**: true | false • **Standardwert**: false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
glide.discovery.application_mapping	Anwendungszuordnung: Aktiviert den Anwendungszuordnungsteil von Discovery **Wichtig:** Durch das Deaktivieren dieser Eigenschaft wird die Erstellung von Beziehungen zwischen Anwendungen deaktiviert, aber nicht die ADM-Proben und -Sensoren deaktiviert und die Prozessklassifizierung wird nicht verhindert. • **Typ**: true | false • **Standardwert**: true • **Mehr erfahren**: Application Dependency Mapping (ADM) für Discovery
glide.discovery.certs.cert_admin_user_id	Zertifikatsbestand-Management: Enthält die Benutzer-ID des Benutzers, auf den in der Zertifikatsaufgabe und im Incident, die über einen geplanten Auftrag erstellt werden, verwiesen wird. • **Typ**: Zeichenfolge (maximal 40 Zeichen) • **Standardwert**: Zertifikat-Administrator
glide.discovery.certs.days_before_expiration_to_create_renewal_task	Zertifikatsbestand-Management: Zeitpunkt (Anzahl der Tage) vor Ablauf des Zertifikats, zu dem eine Erneuerungsaufgabe erstellt werden soll • **Typ**: Ganzzahl • **Standardwert**: 60
glide.discovery.certs.en_incident_creation_for_expired_certipts	Zertifikatsbestand-Management: Ermöglicht der geplanten Aufgabe, die Incidents für abgelaufene Zertifikate zu erstellen, z. B. Zertifikate, deren Gültigkeit nach dem aktuellen Systemdatum oder der aktuellen Systemuhrzeit liegt. Diese Eigenschaft ist standardmäßig aktiviert. • **Typ**: true | false • **Standardwert**: true
glide.discovery.certs.enable_renewal_task_creation_for_discovered_certificates	Zertifikatsbestand-Management: Aktiviert die Erstellung von Erneuerungsaufgaben für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	alle erkannten Zertifikate Diese Eigenschaft ist standardmäßig aktiviert. • **Typ**: true | false • **Standardwert**: true
glide.discovery.certs.slack_channel_id	Zertifikatsbestand-Management: Enthält die Slack-Kanal-ID, an die Zertifikatbenachrichtigungen gesendet werden. • **Typ**: Zeichenfolge • **Standardwert**: leer
glide.discovery.count.use_optimized_counter	Führt optimierten Code zum Aktualisieren der Anzahlen „discovery_status.started“ und „discovery_status.completed“ aus. Bei Festlegung auf **„wahr“**werden Business-Regeln für „discovery_status“ nicht ausgeführt, wenn „gestartet“ oder „abgeschlossen“ geändert wird. Es gibt zwei Ausnahmen: 1. Wenn eine Anforderung zum Inkrementieren der Startanzahlen ausgelöst wird und der Wert „discovery_status.state“ noch „Wird gestartet“ lautet. 2. Wenn „discovery_status.completed“ in den gleichen Wert geändert wird wie „discovery_status.started“. • **Typ**: true | false • **Standardwert**: true
glide.discovery.debug.ci_identification	CI-Identifikationsdebugging: Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird die Debug-Protokollierung (im CI-Identifikationsprotokoll) für die CI-Identifikation aktiviert. • **Typ**: true | false • **Standardwert**: false
glide.discovery.discover_aws_ec2_host_metadata	Bei der IP-basierten Discovery für einen bestimmten Host werden zusätzlich Probes ausgeführt, die AWS EC2-Metadaten abrufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Typ**: true | false • **Standardwert**: true
glide.discovery.discover_azure_host_metadata	Bei der IP-basierten Discovery für einen bestimmten Host werden zusätzlich Probes ausgeführt, die Azure-Metadaten abrufen. • **Typ**: true | false • **Standardwert**: true
glide.discovery.discover_software	Softwarepakete erkennen: Erkennen von Softwarepaketen aktivieren. • **Typ**: true | false • **Standardwert**: true • **Mehr erfahren**: Erkennung von allgemeinen Softwarepaketen
glide.discovery.domain.name.nbt	Legen Sie den BS-Domänennamen über NBT oder WMI fest. Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird der Windows-Domänenname von NBT festgelegt. Andernfalls wird sie von WMI festgelegt. • **Typ**: true | false • **Standardwert**: true
glide.discovery.enable_adme	ADME: Aktivieren Sie die erweiterte ADM-Sonde. Bei Festlegung auf **true**wird die erweiterte ADM-Probe ausgelöst und greift nur bei Bedarf auf die ADM-Probe zurück. • **Typ**: true | false • **Standardwert**: falsch
glide.discovery.enable_file_tracking	Aktivieren Sie das Tracking der Konfigurationsdatei als Teil des musterbasierten Horizontale Discovery. Wenn sie auf **true**festgelegt ist, können Sie vom System Pfade von Konfigurationsdateien für Anwendungen angeben, die von Mustern erkannt werden. Sie können nachverfolgte Konfigurationsdateien nachverfolgen und vergleichen. • **Typ**: true | false • **Standardwert**: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
glide.discovery.enable_mac_address_verification	Aktiviert die Überprüfung der MAC-Adresse, um festzustellen, ob ein Gerät seine IP-Adresse während einer Ermittlung geändert hat. Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird die MAC-Adresse eines erkannten Geräts von Discovery an den MID Server übergeben, damit von den Probes festgestellt werden kann, ob sich die IP-Adresse geändert hat, während Discovery ausgeführt wird. Wenn das Gerät geänderte IP-Adressen hat, beendet Discovery die Verarbeitung dieser IP-Adresse und aktualisiert das Protokoll Discovery mit einer Warnmeldung. Discovery beendet die Verarbeitung anderer IP-Adressen nicht. • **Typ**: true | false • **Standardwert**: falsch Öffnen Sie die Tabelle Systemeigenschaften [sys_properties], um diese Eigenschaft zu finden.
glide.discovery.enable.software_filter	Windows-Softwarefilter: Aktivieren Sie die Windows-Softwarefilter für Discovery . • **Typ**: wahr | falsch • **Standardwert**: true
glide.discovery.enable.software_simplify	Aktiviert die Bereinigung des Namens und der Version der Software. Bei Festlegung auf **true** werden alle angehängten Versionen oder häufig gefundenen Ausdrücke aus dem Namen sowie führende Nullen in der Version entfernt. Bei Festlegung auf **„false“**werden Rohdaten in der Tabelle beibehalten. Verwenden Sie mit der Eigenschaft **„glide.discovery.enable.software_simplify_sccm“**, um Diskrepanzen bei Softwaredaten zwischen Discovery und SCCM zu vermeiden. • **Typ**: true | false • **Standardwert**: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Sobald die Eigenschaft auf **false**festgelegt ist, um die Bereinigung zu deaktivieren, werden für eine bestimmte Software doppelte Datensätze generiert. Name und Version sind die primären Bezeichner.
glide.discovery.enable.software_simplify_sccm	Aktiviert die Bereinigung von SCCM-Software. Bei Festlegung auf **wahr**ändert Discovery den Namen der Software in den Namen von SCCM. Bei Festlegung auf **„false“**bereinigt Discovery den Namen nicht. Verwenden Sie mit der Eigenschaft **glide.discovery.enable.software_simplify,** um Diskrepanzen zwischen Softwaredaten und Discovery zu vermeiden. • **Typ**: true | false • **Standardwert**: falsch
glide.discovery.file_tracking.max_file_size	Dateiverfolgung: Die maximale Dateigröße für den Inhalt der verfolgten Konfigurationsdatei. • **Typ**: integer • **Standardwert**: 500000
glide.discovery.file_tracking.max_files_per_ci	Dateiverfolgung: Die maximale Anzahl verfolgter Konfigurationsdateien pro CI. • **Typ**: integer • **Standardwert**: 50
glide.discovery.file_tracking.change_limit_count	Dateiverfolgung: Anzahl der zulässigen Änderungen an einer verfolgten Konfigurationsdatei im definierten Zeitfenster. • **Typ**: integer • **Standardwert**: 4
glide.discovery.file_tracking.change_limit_days	Dateiverfolgung: Zeitfenster (in Tagen), das die Anzahl der Änderungen an einer verfolgten Konfigurationsdatei begrenzt. • **Typ**: integer • **Standardwert**: 7
glide.discovery.fqdn.regex	Regulärer Ausdruck für den DNS-Hostnamen und Domänennamen: Bei der standardmäßigen Analyse des vollqualifizierten Domänennamens (Fully

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Qualified Domain Name, FQDN) wird der erste Name durch Punkte getrennt als Hostname und der Rest des Namens als Domänenname ausgewählt. Beispielsweise hat „machine1.testlab.service-now.com“ den Hostnamen „machine1“ und den Domänennamen „testlab.service-now.com.“ Die Eigenschaft erlaubt den regulären Ausdruck mit zwei Erfassungsgruppen, wobei die erste Gruppe den Hostnamen und die zweite Gruppe den Domänennamen darstellt. • **Typ**: Zeichenfolge • **Standardwert**: ^([^.]+)\.((?:[^.]+\.)+[^.]+)$
glide.discovery.hostname.always_update	Aktualisieren Sie immer den Hostnamen. Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird der Hostname bei der Erkennung immer mit dem zuletzt entdeckten Wert aktualisiert, abhängig davon, ob die Quelle vertrauenswürdig ist. Beachten Sie, dass dies dazu führen kann, dass von Hand eingegebene Werte überschrieben werden. Diese Eigenschaft gilt nur für Probe-basierte Discovery. • **Typ**: true | false • **Standardwert**: true
glide.discovery.hostname.case	Groß- und Kleinschreibung des Hostnamens Wenn **Kleinschreibung** ausgewählt ist, wird der Hostname immer in Kleinschreibung konvertiert. Wenn **Großbuchstaben** ausgewählt ist, wird der Hostname immer in Großbuchstaben konvertiert. Wenn **No change (Kein Change)** ausgewählt ist, lassen Sie den Hostnamen unverändert. Dies betrifft in erster Linie Hostnamen, die mit NETBIOS ermittelt wurden. Einige nicht standardmäßige DNS-Systeme geben jedoch möglicherweise einen Teil oder den gesamten Namen in Großbuchstaben zurück. • **Typ**: Auswahlliste • **Standardwert:** Kleinschreibung • **Zusatzoptionen**: Großbuchstaben, Keine Änderung
glide.discovery.hostname.dns_nbt_trusted	DNS oder NetBIOS ist vertrauenswürdige Hostnamenquelle: Bei Festlegung auf **wahr** wird dem über DNS oder NetBIOS

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	erkannten Gerätenamen vertraut. Wenn aktiviert, wird der über DNS oder NBT gefundene Hostname von CI verwendet. **Hinweis:** Verwenden Sie für die Muster Linux, AIXund Solaris nicht den DNS-Namen als Hostnamen. • **Typ**: true | false • **Standardwert**: true
glide.discovery.hostname.include_domain	Schließt Domänennamen in Hostnamen ein: Bei Festlegung auf **wahr** wird der Domänenname als Teil des Hostnamens eingeschlossen. Zum Beispiel "bosco.service-now.com" anstelle von "bosco". **Hinweis:** Verwenden Sie für die Muster AIX und Solaris nicht den DNS-Namen als Hostnamen. • **Typ**: true | false • **Standardwert**: false
glide.discovery.hostname.snmp_trusted	SNMP ist vertrauenswürdige Hostnamenquelle: Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird dem über SNMP erkannten Gerätenamen vertraut. Wenn diese Option aktiviert ist, wird jeder über SNMP gefundene Gerätename verwendet, anstatt des Namens, der durch eine Reverse-DNS-Suche gefunden wurde. • **Typ**: true | false • **Standardwert**: false (Für Neukunden von Discovery, die in Yokohamabeginnen, ist der Standardwert „true“.)
glide.discovery.hostname.ssh_trusted	SSH ist vertrauenswürdige Hostnamenquelle: Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird dem über SSH erkannten Gerätenamen vertraut. Wenn diese Option aktiviert ist, wird jeder über SSH gefundene Gerätename verwendet, anstatt des Namens, der durch eine Reverse-DNS-Suche gefunden wurde. **Hinweis:** Verwenden Sie für die Muster Linux, AIXund Solaris nicht den DNS-Namen als Hostnamen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Typ**: true | false • **Standardwert**: false (Für Neukunden von Discovery, die in Yokohamabeginnen, ist der Standardwert „true“.)
glide.discovery.hostname.wmi_trusted	WMI ist vertrauenswürdige Hostnamenquelle: Wenn diese Eigenschaft auf **wahr** gesetzt ist, wird dem über WMI erkannten Gerätenamen vertraut. Wenn aktiviert, wird jeder über WMI gefundene Gerätename verwendet anstatt Der Name wurde durch eine Reverse-DNS-Suche gefunden. • **Typ**: true | false • **Standardwert**: False (Für neue Discovery Kunden, die in Yokohamabeginnen, ist der Standardwert „true“.)
glide.discovery.ip_based.active	Dadurch können Scans für alle IP-Adressen desselben Geräts im selben Discovery-Zeitplan den vollständigen Zyklus durchlaufen. Dies ist für Instanzen, die von Probe zu Muster migriert werden, auf **„wahr“** festgelegt, Discovery versucht keine zusätzliche IP-Adresserkennung. • **Typ**: true | false • **Standardwert**: true (Für Instanzen, die von Probe zu Muster migriert wurden.)
glide.discovery.ip_service_affinity	IP-Service-Affinität: Wenn diese Eigenschaft auf **wahr** gesetzt ist, ist die IP-Service-Affinität aktiviert. IP-Service-Affinität erlaubt Discovery den letzten Port der erkannten IP-Adresse zu speichern. **Hinweis:** Sie müssen ip_service_affinity-Datensätze aktivieren, wenn Sie mehrere SSH-Ports verwenden. • **Typ**: true | false • **Standardwert**: False (Für neue Discovery Kunden, die in Yokohamabeginnen, ist der Standardwert „true“.) • **Mehr erfahren**: IP-Service-Affinität für Discovery und Orchestration prüfen
glide.discovery.L3_mapping	Server und Netzwerkgeräte zu Routern und Layer-3-Switches zuordnen Wenn die Eigenschaft „L3-Zuordnung“ aktiviert ist,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	werden Server und Netzwerkgeräte den entsprechenden Routern und Layer-3-Switches zugeordnet. • **Typ**: true | false • **Standardwert**: true • **Mehr erfahren**: Netzwerk-Discovery
glide.discovery.log_message_length	Protokollnachrichtenlänge: Beschränkung der maximalen Nachrichtenlänge, die in der Tabelle „Discovery-Protokoll“ angezeigt wird. Ein Wert von 0 oder eine negative Zahl deaktiviert dieses Limit. • **Typ**: Ganzzahl • **Standardwert**: 200 • **Mehr erfahren**: Protokolle für horizontale Erkennung
glide.discovery.mark_esx_servers_as_absent	Wenn diese Eigenschaft auf „true“ festgelegt ist, werden die ESX-Server als „Abwesend“ anstatt als „Deaktiviert“ markiert, wenn der ESX-Server nicht in der Nutzlast gefunden wird. • **Typ**: true | false • **Standardwert**: false
glide.discovery.max_concurrent_invocations_per_schedule	Maximale Anzahl gleichzeitiger Aufrufe pro Zeitplan: Verhindert, dass eine unbegrenzte Anzahl von Aufrufen das System überschwemmt, wenn ein Zeitplan länger als die Zeit zwischen Aufrufen dauert. Der Wert ist eine ganze Zahl, die die maximale Anzahl automatisierter Aufrufe desselben Zeitplans festgelegt, die gleichzeitig ablaufen können. Wenn der Grenzwert erreicht wurde, werden nachfolgende geplante Aufrufe abgebrochen. Der Standardwert ist 3. Ein Wert von 0 oder eine negative Zahl deaktiviert diese Einschränkung. • **Typ**: Ganzzahl • **Standardwert**: 3 **Hinweis:** Diese Eigenschaft gilt nicht für Zeitpläne, für die die Konfiguration „Ausführen nach“ auf „Auch bei Abbruch“ festgelegt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
glide.discovery.network_discovery.functionality	Netzwerk-Discovery-Funktionalität: Die Funktionalität, die zum Erkennen von Netzwerken verwendet wird. Normalerweise sollte dies **Nur SNMP** sein. • **Typ**: Zeichenfolge • **Standardwert**: Nur SNMP
glide.discovery.perf.metrics.enable_collection	Ob Discovery-Leistungsmetriken gesammelt werden sollen. • **Typ**: true | false • **Standardwert**: true
glide.discovery.perf.metrics.rollup_by_build	Gibt an, ob einzelne Discovery-Leistungsmetriken in einer Rollup-Tabelle zusammengefasst werden sollen, die nach Discovery-Build gruppiert. • **Typ**: true | false • **Standardwert**: true
glide.discovery.perf.metrics.rollup_by_status	Gibt an, ob einzelne Discovery-Leistungsmetriken in einer Rollup-Tabelle zusammengefasst werden sollen, die nach Discovery-Status gruppiert. • **Typ**: true | false • **Standardwert**: true
glide.discovery.perf.metrics.rollup_by_target	Gibt an, ob einzelne Discovery-Leistungsmetriken in einer Rollup-Tabelle zusammengefasst werden sollen, die nach Ziel-IP-Adresse gruppiert. • **Typ**: true | false • **Standardwert**: true
glide.discovery.populate_software_instance_table	Bei Festlegung auf „true“ werden von Discovery folgende Tabellen für die Software-Erkennung gefüllt: `cmdb_software_instance` und `cmdb_sam_sw_install`. • **Typ**: true | false • **Standardwert**: falsch Verwenden Sie diese Eigenschaft nur, wenn Sie Software Asset Management mit Discovery in einer Version vor Jakarta verwenden und die Tabelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	`cmdb_software_instance` ausfüllen möchten. Öffnen Sie die Tabelle Systemeigenschaften [sys_properties], um diese Eigenschaft zu finden.
glide.discovery.roundingInterval.cpu	CPU-Geschwindigkeitsrundung: Geben Sie die Zahl ein, auf der die CPU-Geschwindigkeit gerundet werden soll. Die Einheiten sind in MHz. • **Typ**: Ganzzahl • **Standardwert**: 1
glide.discovery.roundingInterval.ram	Speicher-Rundung: Geben Sie die Zahl ein, auf die der Computer-RAM gerundet werden soll. Die Einheiten sind in MB. • **Typ**: Ganzzahl • **Standardwert**: 1
glide.discovery.schedule_monitoring.dry_run	Bestimmt, ob die Aufgabe im Probelaufmodus ausgeführt wird. Bei Festlegung auf **„true“**protokolliert die Aufgabe nur die Entscheidung im Discovery-Protokoll, ändert jedoch nicht den Status des Status. Andernfalls ändert die Aufgabe bei Bedarf den Status des Status. • **Typ**: true | false • **Standardwert**: false
glide.discovery.schedule_monitoring.schedule_types_to_identify	Bestimmt den Typ der nachzuverfolgenden Status. Der Wert kann unter dem Attribut „Erkennen“ im Zeitplan gefunden werden. • **Typ**: Zeichenfolge • **Standardwert-** CIs
glide.discovery.schedule_monitoring.stale_check_seconds	Bestimmt die Anzahl in Sekunden, in der ein Status als veraltet betrachtet wird. Ein veralteter Status ist ein Status, der in den letzten X Sekunden nicht aktualisiert wurde. • **Typ**: Ganzzahl • **Standardwert** 1200 (20 Minuten). Wenn nichts konfiguriert ist, entspricht der Standardwert dem doppelten Intervall des Auftrags.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
glide.discovery.sensors.fire_ssh_probe	Falls die VIPs (Virtuelle Lastenausgleichsmodul-Services) nicht als Teil der SNMP-Probe-Nutzlast zurückgegeben werden, lösen Sie die SSH-Probe aus. Wählen Sie diese Option aus, um den SSH-Port am Lastenausgleichsmodul zu verwenden, anstatt nur SNMP zu verwenden. • **Typ**: true | false • **Standardwert**: true
glide.discovery.sensors.netapp_native_7mode	Verwenden Sie für NetApp-Speicherserver im Modus „7“ die native Discovery anstelle von SMI-S.
glide.discovery.sensors.netapp_native_cluster_mode	Verwenden Sie für NetApp-Speicherserver im Cluster-Modus native Discovery anstelle von SMI-S.
glide.discovery.sensors.save_attachments	Speichern von ECC-Warteschlangenanhängen: Das normale Verhalten von Erkennungssensoren besteht darin, Anlagen an ECC-Warteschlangeneinträgen nach erfolgreicher Sensorbearbeitung zu löschen. Wenn diese Eigenschaft auf „wahr“ gesetzt wird, wird dieses Verhalten außer Kraft gesetzt und die Beibehaltung von Anhängen erzwungen. Dies ist normalerweise nur für Debugging-Zwecke nützlich. • **Typ**: true | false • **Standardwert**: true
glide.discovery.shazzam_ranges_json	JSON für IP-Bereiche in Shazzam verwenden: Bei Festlegung auf **wahr**codiert die Discovery IP-Bereiche von Shazzam im JSON-Format, wodurch die Größe der Nutzlast erheblich reduziert wird. • **Typ**: true | false • **Standardwert**: true
glide.discovery.shazzam_simplify_ranges	Wenn diese Eigenschaft auf **true** gesetzt ist, erkennt Shazzam, ob eine IP in mehreren Bereichen desselben Discovery-Zeitplans enthalten ist, und entfernt die doppelte IP aus allen Bereichen außer einem. Die Deduplizierung ist auf Zeitpläne mit einem einzigen Verhalten beschränkt. Zeitpläne mit mehreren Verhaltensweisen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	funktionieren, aber doppelte IPs werden nicht entfernt. • **Typ**: true | false • **Standardwert**: true
glide.discovery.software_filter_keys	Windows-Softwarefilter: Wenn der Windows-Softwarefilter aktiviert ist und der Name einer erkannten Software einen der durch Kommas getrennten Werte enthält, wird er herausgefiltert. • **Typ**: Zeichenfolge • **Standardwert** : Sprachpaket, Hotfix-Sicherheitsupdate
glide.discovery.software_sccm_managed	Windows-Software wird von SCCM verwaltet: Bei Festlegung auf **„wahr“**füllt Discovery keine Software für Computer-CIs aus, die auch von SCCM verwaltet werden. • **Typ**: true | false • **Standardwert**: false • **Mehr erfahren**: Discovery und SCCM zusammen
glide.discovery.use_cmdb_identifiers	CMDB-Bezeichner: Wenn diese Eigenschaft auf **wahr** gesetzt ist, werden Identifizierung und Abgleich von der CMDB-API durchgeführt und nicht über die alte Discovery-Implementierung. • **Typ**: true | false • **Standardwert**: true
glide.discovery.use_probe_results_cache	Probeergebnis-Cache verwenden: Bei Festlegung auf **true**wird der Cache überprüft und festgestellt, ob die Ergebnisse der Probe von einem Sensor verarbeitet werden müssen. Sie muss nur verarbeitet werden, wenn sich die Ergebnisse seit dem letzten Erkennungslauf geändert haben. • **Typ**: true | false • **Standardwert**: false • **Mehr erfahren**: Probes erstellen oder ändern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: In früheren Versionen war diese Eigenschaft standardmäßig **true**. Der Wert in dieser Eigenschaft wird während eines Upgrades auf Kingston nicht geändert.
glide.discovery.virtual_interface_types	Typen virtueller Schnittstellen: Liste der Schnittstellentypen (durch Kommas getrennt), die für die Netzwerkerkennung als „virtuell“ betrachtet werden können. Wenn also ein Router (oder ein Gerät, das Routing ausführen kann) über eine Schnittstelle dieses Typs verfügt, werden die an diese Schnittstelle angeschlossenen Netzwerke als virtuell mit diesem Gerät verbunden betrachtet. Die Standardschnittstellentypen enthalten den propVirtual-Typ. Schnittstellentypnummern sind in der SNMP MIB-2 definiert, insbesondere in der OID 1.3.6.1.2.1.2.2.1.3. • **Typ**: Ganzzahl • **Standardwert**: 53
glide.discovery.warn_minor_version	Bei geringfügigen Versionskonflikten warnen: Wenn diese Eigenschaft auf **wahr** gesetzt ist, werden Warnungen protokolliert, wenn bei der Verarbeitung der Discovery-Sensoren minor_version-Diskrepanzen erkannt werden. • **Typ**: true | false • **Standardwert**: false
glide.ecc_agent.validated.override	Eine Überschreibung des validierten Felds „ecc_agent“: Wenn diese Eigenschaft auf „wahr“ gesetzt ist, werden „ecc_agent“-Datensätze immer als gültig behandelt. • **Typ**: true | false • **Standardwert**: false Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften** um diese Eigenschaft zu finden.
glide.eccprobe.awsrestprobe.max_retries	Legen Sie fest, wie oft die AWS-Anforderung maximal erneut versucht werden soll, wenn ein Fehler vom Typ „Quotenbegrenzung überschritten“ auftritt. Der Höchstwert ist 10. Beachten Sie, dass Neuversuche ein exponentielles Backoff (2^x) aufweisen. Die Festlegung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	negativer Werte ist gleichbedeutend mit der Festlegung des Höchstwerts. • **Typ**: Ganzzahl • **Standardwert**: 4
glide.eccprobe.awsrestprobe.max_wait	Legen Sie die maximale Gesamtzeit (Sekunden) fest, innerhalb derer ein neuer Versuch der AWS-Anforderung erfolgt. Höchstwert: 2.046 Sekunden. Die Festlegung negativer Werte ist gleichbedeutend mit der Festlegung des Höchstwerts. • **Typ**: Ganzzahl • **Standardwert**: 30
glide.eccprobe.max_queued_probes_per_run	Legen Sie die maximale Anzahl von Probes fest, die von einem Knoten während einer Ausführung aufgenommen werden können. • **Typ**: Ganzzahl • **Standardwert**: 20
glide.eccprobe.node_agent_id	ECC-Warteschlangeneinträge mit „mid.server.${VALUE}“ werden von den Knoten aufgenommen und verarbeitet. Dieser muss eindeutig sein und darf nicht mit einem MID Server-Namen identisch sein. • **Typ**: Zeichenfolge • **Standardwert**: NODE_AGENT
sn_disco_firewall.default.rule.task.policy.owner.group	Firewall-Audits und Reporting: Gibt den Namen der Zuweisungsgruppe an, die Firewall-Regelaufgaben besitzt oder diesen zugewiesen ist • **Typ**: Zeichenfolge (maximal 40 Zeichen) • **Standardwert**: Aufgabenbesitzer-Gruppenname
sn_disco_firewall.default.rule.task.approval.group	Firewall-Audits und Reporting: Gibt den Namen der Genehmigungsgruppe an, die zum Genehmigen der Firewall-Regelaufgaben verwendet wird. • **Typ**: Zeichenfolge (maximal 40 Zeichen) • **Standardwert**: Genehmigungsgruppenname

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
sn_disco_certmgmt.enable_csr_generation	Aktiviert die automatische CSR-Generierung in den Formularen Zertifikatbestand und -management , **Neues Zertifikat anfordern** und **Neues Zertifikat anfordern (automatisiert)**. Diese Funktion ist standardmäßig aus Sicherheitsgründen deaktiviert. • Typ: Wahr | Falsch • Standardwert: falsch
sn_disco_certmgmt.private_key_size	Ändert die Größe des privaten Schlüssels, wenn die automatische CSR-Generierung in den Formularen „Zertifikatbestand und Verwaltung **– Neues Zertifikat anfordern“** und **„Neues Zertifikat anfordern (automatisiert)“** verwendet wird. Diese Eigenschaft akzeptiert folgende Werte: 512 | 1024 | 2048 | 4096. • Typ: Ganzzahl • Standardwert: 2048

Konfiguration der Discovery-IP-Adresse

Verwenden Sie eine oder mehrere Methoden in beliebiger Kombination, um das Netzwerk oder Netzwerksegment für die Abfrage von Discovery zu definieren. Sie können bestimmte IP-Bereiche in Ihre Abfrage einbeziehen oder daraus ausschließen.

Hinweis: Wenn Sie die IP-Adressen in Ihrem Netzwerk nicht kennen, führen Sie zuerst eine Netzwerk-Discovery aus, um zunächst die IP-Netzwerke zu ermitteln. Konvertieren Sie anschließend die IP-Netzwerke in Range Sets von IP-Adressen.

Wenn Ihre Integrationen die Tabellen sys_metadata und sys_update_xml füllen, müssen Sie die Aktualisierungs- und Metadatendatensätze nach dem Import von discovery_range_item oder discovery_range_item_ip löschen.

IPv6-Adressen werden für IP-Adressbereiche oder IP-Netzwerke nicht unterstützt.

Es gibt drei Typen von IP-Sammlungen:

Typ der IP-Sammlung	Beschreibung
IP-Adressenliste	Verwenden Sie IP-Adresslisten, um einzelne Adressen zur Abfrage hinzuzufügen. Diese Adressen sind in keinem vorhandenen IP-Bereich oder IP-Netzwerk enthalten. Sie können die IP-Adresse des Geräts oder einen Hostnamen (DNS-Namen) eingeben. Wenn Sie einen Hostnamen eingeben, muss er einer IP-Adresse zugeordnet sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ der IP-Sammlung	Beschreibung
IP-Adressbereich	Sie können willkürliche IP-Adressbereiche für die Abfrage definieren. Dieser Prozess stellt eine gute Möglichkeit dar, ausgewählte Segmente eines Netzwerks oder Subnetzes einzubeziehen. Discovery liegen jedoch keine Informationen darüber vor, ob der IP-Bereich Adressen für private Netzwerke oder Broadcast-Adressen enthält, und scannt alle Adressen im Bereich. Wenn Netzwerk- und Broadcast-Adressen enthalten sind, sind die Ergebnisse ungenau. Zum Erkennen von IP-Netzwerken konfigurierte Erkennungen sind genauer als Erkennungen, die für IP-Adressbereiche konfiguriert sind. Es sollten nur diejenigen IP-Adressen in Ihrem Bereich einbezogen werden, die für verwaltbare Geräte im öffentlichen Netzwerk reserviert sind. **Hinweis:** Um mögliche Leistungsprobleme zu vermeiden, beschränken Sie Erkennungszeitpläne auf einen maximalen Bereich von /16 oder nicht mehr als 65.000 IPs. Sie können die Erkennungszeitpläne auch in noch kleinere IP-Adressbereiche aufteilen.
IP-Netzwerk	Sie können auch ein gesamtes IP-Netzwerk scannen. Ein IP-Netzwerk umfasst den Bereich der verfügbaren IP-Adressen in diesem Netzwerk. Der Scan umfasst auch die Netzwerkadresse (die niedrigste Adresse im Bereich) und die Broadcast-Adresse (die höchste Adresse im Bereich). Nachdem Sie die Netzwerkerkennung durchgeführt haben, konvertieren Sie die gefundenen IP-Netzwerke in Range Sets, die Sie zur Erkennung anderer Geräte verwenden. IP-Netzwerke werden in CIDR-Schreibweise dargestellt. Beispiele für die CIDR-Schreibweise: • 192.168.0.0/24 • 10.11.128.192/26 Netzwerk- oder Broadcast-Adressen für ein Netzwerk werden von Discovery nicht gescannt. Die entsprechenden Bereiche für die beiden Netzwerke: • 192.168.0.1–192.168.254 • 10.11.128.193–10.11.128.254 Die Broadcast-Adresse verhindert und bewirkt erhebliche Fehler in den Discovery-Daten. Alle Geräte im Netzwerk werden zurückgegeben. Dies gilt auch für die Netzwerkadresse, durch die eine willkürliche Anzahl von redundanten Geräten hinzugefügt werden kann. Diese integrierte Steuerung macht IP-Netzwerke zur besten Methode, um festzulegen, welche IP-Adressbereiche abgefragt werden sollen.

Eigenschaften der IP-Adressauswahl

Sie können Systemeigenschaften verwenden, um die Auswahl der IP-Adressen für die angegebenen CI-Klassen zu steuern.

Verwenden Sie die folgenden Eigenschaften, um zu bestimmen, ob das System die von Discovery zurückgegebene IP-Adresse im CI-Datensatz eines Geräts ersetzen soll, wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Adresse nicht mit der einer Netzwerkschnittstelle (NIC) auf dem Gerät übereinstimmt. Das ist wichtig für die Erkennung von Geräten mit Verwaltungs-IP-Adressen, die sich von IP-Adressen unterscheiden, die einer oder mehreren NICs auf dem Gerät zugeordnet sind. Da die Verwaltungs-IP-Adresse eines Geräts im Erkennungszeitplan für dieses Gerät verwendet wird, handelt es sich hierbei um die Adresse, die von Discovery zurückgegeben wird. Verwenden Sie die folgenden Eigenschaften, um zu bestimmen, welche IP-Adresse für CIs einer beliebigen Klasse verwendet werden soll.

Feld	Beschreibung
glide.discovery.exclude_ip_sync_classes	Definiert CI-Klassen, deren IP-Adressen nicht ersetzt werden dürfen, wenn die von Discovery zurückgegebene Adresse nicht mit einer der NICs des Geräts übereinstimmt. Verwenden Sie eine durch Kommas getrennte Liste, um mehrere Klassen zu definieren. Vom System wird im CI-Datensatz standardmäßig die Verwaltungs-IP eines Lastenausgleichsmoduls verwendet, die von Discovery zurückgegeben wird, anstatt sie durch die IP-Adresse einer der NICs des Lastenausgleichsmoduls zu ersetzen. • **Typ**: Zeichenfolge • **Standardwert**: cmdb_ci_lb
glide.discovery.enforce_unique_ips	Eindeutige IP-Adressen erzwingen: Die IP-Adresse wird ignoriert, nachdem nachfolgende Geräte von Discovery gefunden worden sind, die dieselbe IP-Adresse verwenden. Jedes Mal, wenn ein Computer, ein Drucker oder ein Netzwerkgerät mit einer gültigen IP-Adresse erkannt wird, wird das IP-Adressfeld aller anderen Geräte mit derselben IP-Adresse gelöscht. Wenn inaktiv, wird die IP-Adresse für jedes Gerät gespeichert. • **Typ**: true | false • **Standardwert**: false

Schnell-IP-Bereich für Erkennungszeitplan erstellen

In Schnellbereichen können Administratoren IP-Adressen definieren, die in einer durch Kommas getrennten Zeichenfolge durchsucht werden, ohne dass separate Datensätze erstellt werden müssen.

Vorbereitungen

Erforderliche Rolle: Discovery admin.

Für Kurzbereiche werden nur MID Server verwendet, die aktiv und validiert sind. Für die MID Server muss die Anwendung Discovery angegeben sein (oder ALLE Anwendungen), und die IP-Bereiche müssen konfiguriert sein, wenn Sie die automatische Auswahlfunktion im Erkennungszeitplan verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können IP-Adressen in einem der folgenden Formate eingeben:

- Ein IP-Bereich, der durch einen Schrägstrich und die Anzahl der Bits im Subnetz festgelegt ist. Beispielsweise durchsucht der String 10.10.10.0/24 24-Bit-IP-Adressen von 10.10.10.0 bis 10.10.10.254.
- Ein IP-Bereich, der durch einen Bindestrich definiert wird. Der String 10.10.11.0-10.10.11.165 durchsucht beispielsweise die IP-Adressen von 10.10.11.0 bis 10.10.11.165.
- Eine durch Kommas getrennte Liste bestimmter IP-Adressen. Beispiel: Mit der Zeichenfolge 10.0.2.1,10.0.2.15 werden die IP-Adressen 10.0.2.1 und 110.0.2.15 gescannt.

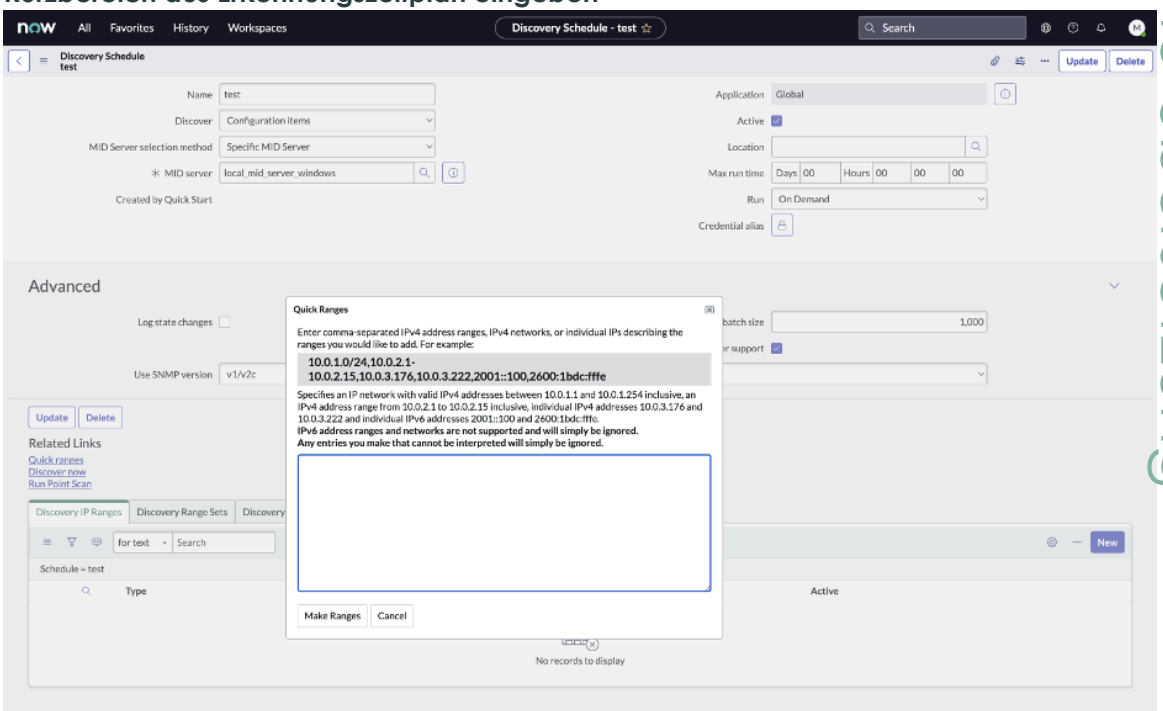
Hinweis: IPv6-Adressbereiche und -Netzwerke werden nicht unterstützt und entsprechend ignoriert. Alle anderen Eingaben, die nicht interpretiert werden können, werden ebenfalls ignoriert.

Prozedur

1. Klicken Sie im Formular „Discovery-Zeitplan“ auf den zugehörigen Link **Kurzbereiche**.
2. Geben Sie die IP-Bereiche und spezifischen IP-Adressen ein, die gescannt werden sollen.
3. Klicken Sie auf **Bereiche erstellen**.

Hinweis: Die Schnittstelle für den Kurzbereich dient nur zur Eingabe von IP-Adressen und kann nicht zum Bearbeiten von bereits übermittelten IP-Adressen verwendet werden.

Kurzbereich aus Erkennungszeitplan eingeben



Die Instanz zeigt die Einträge automatisch im richtigen Format an.

4. Wählen Sie zum Ändern von IP-Adressbereichen die IP-Adressdatensätze in der zugehörigen Liste **Discovery-Range Sets** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Bereiche mit Import Sets in Erkennungszeitpläne importieren

Eine Methode zur Eingabe einer großen Anzahl von IP-Netzwerken in Discovery-Zeitpläne ist die Verwendung von Importsätzen.

Vorbereitungen

Erforderliche Rolle: Discovery_Admin

Warum und wann dieser Vorgang ausgeführt wird

Allgemeine Gruppen von IP-Adressen, die als Bereiche bezeichnet werden, können in erweiterten Erkennungszeitplänen verwendet werden.

Hinweis: Sie können auch die IPAM-Integration verwenden, um eine große Anzahl von IP-Netzwerken in Discovery-Zeitpläne einzugeben. Weitere Informationen finden Sie unter IPAM-Integration.

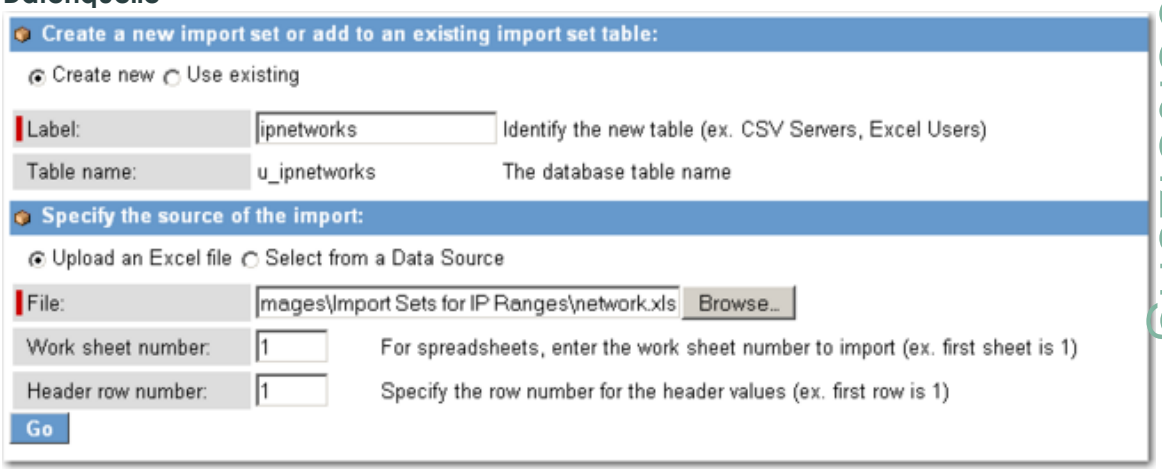
Verwenden Sie eine Datenquelle, die zugeordnet werden kann. Schließen Sie die folgenden Felder ein:

- Start-IP: Die erste IP-Adresse im Bereich (einschließlich)
- Ende-IP: Die letzte IP-Adresse im Bereich (einschließlich)

Prozedur

1. Navigieren zu **Alle** > **System-Importsätze** > **Daten laden**.
2. Identifizieren Sie die Datei oder Datenquelle, die die gewünschten Informationen enthält.
3. Erstellen Sie einen Tabellennamen, zum Beispiel `ipnetworks`.
4. Klicken Sie auf **Excel-Datei hochladen**, und navigieren Sie zur Quelldatei.
5. Klicken Sie auf **Start**, um die Datei zu importieren.

Datenquelle



6. Navigieren zu **System-Importsätze** > **Transformationszuordnung erstellen** und ordnen Sie die Elemente in der Excel-Tabelle den Feldern der CMDB in der Tabelle „IP-Bereich“ `[ip_address_range]` der Zieltabelle zu.
7. Weisen Sie der Transformationszuordnung einen eindeutigen und aussagekräftigen Namen zu.
8. Übermitteln Sie das Formular, und klicken Sie dann in der zugehörigen Liste **Feldkarten** auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Ordnen Sie die Felder in der Excel-Tabelle den Feldern in der Tabelle „IP-Bereich“ `[ip_address_range]` zu.
   Für die folgenden Adressfelder benötigen Sie Werte: **Start-IP** und **Ende-IP**.
10. Klicken Sie auf den zugehörigen Link **Zuordnungsassistent**, und verwenden Sie die angezeigten Listen, um die Felder zwischen Tabelle und Datenquelle (der Excel-Tabelle in diesem Beispiel) aufzulösen.
11. Klicken Sie auf **Speichern**.

    Daraufhin wird wieder das Formular „Tabellen-Transform Map“ angezeigt.
12. Klicken Sie unter „Zugehörige Links“ auf **Umwandeln**, um die Daten in die entsprechenden Felder in der Tabelle „IP-Bereich“ `[ip_address_range]` zu verschieben.

    Die importierten IP-Bereiche können jetzt in jedem erweiterten Erkennungszeitplan verwendet werden.

IP-Bereiche aus einem Discovery-Range Set ausschließen

Sie können einen Bereich von IP-Adressen angeben, die Sie aus Ihrer Discovery-Abfrage ausschließen möchten.

Vorbereitungen

Erforderliche Rolle: Discovery-Administrator- oder Agent-Administratorrolle zum Hinzufügen oder Bearbeiten einer Ausschlussliste.

Vor der Ausführung eines Erkennungszeitplans wird die Gesamtanzahl der ausgeschlossenen IP-Adressen berechnet. Wenn mehr als 500.000 ausgeschlossene IP-Adressen vorhanden sind, wird die Erkennung abgebrochen, und über DiscoveryLogger wird ein Fehler in Bezug auf den Status protokolliert.

Hinweis: Das Ausschließen von IP-Adressen wird für IPv6-Bereiche oder -Subnetze nicht unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery Bereiche**.
2. Wählen Sie eines der Range Sets aus.
3. Wählen Sie einen der Typen in der zugehörigen Liste **Discovery-IP-Bereiche** aus.
4. Klicken Sie in der zugehörigen Liste **Discovery-Bereichselement ausschließen** auf **Neu**.
5. Geben Sie eine IP-Start- und IP-Endadresse ein, um den auszuschließenden Bereich zu erstellen.
6. Klicken Sie auf **Absenden**.

Globale Ausschlussliste für IP-Adressen und -Bereiche verwenden

Mithilfe der globalen Ausschlussliste können Administratoren globale IP-Ausschlusslisten definieren, die für alle Discovery-Zeitpläne gelten, anhand denen Konfigurationselemente, IP-Adressen oder Netzwerke erkannt werden. Die Liste hilft, den Zugriff auf sensible IPs zu verhindern, da sie die Erkennung blockiert, wenn sich die IP-Adresse in der Ausschlussliste befindet. Diese Funktion gilt nur für die horizontale Discovery ab Yokohama.

Vorbereitungen

Erforderliche Rolle: Discovery-Administrator- oder Agent-Administratorrolle zum Hinzufügen oder Bearbeiten einer Ausschlussliste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Globale IP-Ausschlussbereiche sind standardmäßig aktiv. Deaktivieren Sie das Kontrollkästchen „Aktiv“, um sie zu deaktivieren. Dadurch werden die Datensätze inaktiv, und die Einträge werden nicht aus Discovery ausgeschlossen. Sie können der globalen Ausschlussliste eine einzelne IP-Adresse oder einen IP-Bereich hinzufügen. Die Tabelle „IP-Ausschlussliste“ [ip_exclusion] verweist auf vorhandene IP-Erfassungstabellen und unterstützt drei Arten von Sammlungen: IP-Adressliste, IP-Adress-Subnetz und IP-Adressbereich.

Hinweis: Die Verwendung einer globalen Ausschlussliste für IP-Adressen und -Bereiche wird für IPv6-Adressen nicht unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Globaler IP-Ausschluss** > **IP-Ausschluss**.
2. Klicken Sie auf **Neu**, um einen neuen IP-Ausschlussdatensatz zu erstellen.
3. Klicken Sie im Feld „IP ausgeschlossen“ auf das Suchsymbol, um das Fenster „IP-Sammlungen“ aufzurufen.
4. Wählen Sie eine der aufgeführten IP-Sammlungen aus, oder klicken Sie auf **Neu**, um den Assistenten für IP-Sammlungen aufzurufen.
5. Wählen Sie im Assistenten für IP-Sammlungen eine der drei Arten von Sammlungen aus, die Sie erstellen möchten, und füllen Sie die erforderlichen Details aus.
   Für jeden Typ können Sie eine Beschreibung hinzufügen, warum Sie bestimmte IP-Adressen ausschließen möchten bzw. welche IP-Adressen ausgeschlossen werden.
   - IP-Adressbereich

     Füllen Sie die Details aus, und klicken Sie auf **Absenden**. Dieser neue Bereich wird der IP-Ausschlussliste hinzugefügt.

   - IP Address Subnet (IP-Adressen-Subnetz)

     Füllen Sie die Details aus, und klicken Sie auf **Absenden**. Dieses neue Subnetz wird der IP-Ausschlussliste hinzugefügt.

   - IP-Adressenliste

     Geben Sie den Namen ein, und **Speichern** Sie. Die zugehörige Liste wird am unteren Rand des Seite angezeigt. Wählen Sie in der Sammlungsliste ein vorhandenes Element aus, oder klicken Sie auf **Neu**, um eine neue Liste zu erstellen. Klicken Sie auf **Aktualisieren**. Merken Sie sich den von Ihnen erstellten Namen. Dieser neue Name wird der Sammlungsliste hinzugefügt. Wählen Sie diesen Namen aus der Liste aus, und klicken Sie erneut auf **Absenden**. Diese neue Adressliste wird der IP-Ausschlussliste hinzugefügt.
6. Navigieren zu **Discovery** > **Discovery-Zeitpläne** und wählen Sie einen Zeitplan aus.
7. Wenn der Zeitplan für die Erkennung von Konfigurationselementen, IP-Adressen oder Netzwerken vorgesehen ist, können Sie unten auf der Seite die Registerkarte „Globaler IP-Ausschluss“ sehen.

Ergebnisse

Wenn die geplante Discovery ausgeführt wird, wird die Erkennung aller IP-Adressen übersprungen, die Teil des aktiven Datensatzes für den globalen IP-Ausschluss sind. Alle anderen IP-Adressen sollten erkannt werden.

Wenn Sie versuchen, eine Schnell-Discovery auszuführen, die eine ausgeschlossene IP enthält, wird eine Fehlermeldung angezeigt, und Discovery wird nicht ausgelöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Domänentrennung und Erkennung

Die Domänentrennung wird in Discovery unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Standard

- Umfasst alle Aspekte des **Basis** -Supports.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

Beispiel-Anwendungsfall: Ein Administrator muss in der Lage sein, Kommentare beim Schließen eines Datensatzes für einen Mandanten obligatorisch zu machen, für andere hingegen nicht.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Übersicht über Domänentrennung

Service Provider (SPs) verwenden Domänentrennung, um Daten für jeden Kunden zu trennen. Benutzer in einer bestimmten Domäne können Daten nur in ihrer eigenen oder einer untergeordneten Domäne anzeigen. SPs haben üblicherweise die Kontrolle über die oberste Domäne, wodurch sie Daten aller Domänen anzeigen können. Da die Unterstützung der Domänentrennung in Discovery als **Standard** gilt, erfolgt keine delegierte Verwaltung an die untergeordneten Domänen. Die SPs müssen die administrative Kontrolle behalten.

Funktionsweise der Domänentrennung in Discovery

Mehrere Domänen können durch einen einzelnen MID Server unterstützt werden. In Releases vor Kingston konnte jeder MID Server nur eine einzelne Domäne unterstützen. In neueren Releases ist das Trennen von Domänen nach MID Server nützlich, wenn die Domäne groß ist oder wenn sich die Ressourcen der Domäne im Rechenzentrum eines Kunden und nicht in dem eines SP befinden. Für Discovery auf MID Servern, die eine einzelne Domäne unterstützen, werden die erkannten CIs der Domäne des MID-Benutzers zugewiesen, der für die Authentifizierung gegenüber der ServiceNow-Instanz verwendet wird. Bei MID Servern mit mehreren Domänen werden die erkannten CIs der Domäne des Benutzers zugewiesen, der den Erkennungszeitplan erstellt hat.

Discovery implementiert die Trennung von Datendomänen durch den MID Server, indem während der Sensorverarbeitung die Identität des MID Server-Benutzers gewechselt wird. Discovery verwendet die Domäne, in der sich der MID Server-Benutzer befindet, um zu bestimmen, in welche Domäne die erkannten Daten eingefügt werden sollen. Discovery-Konfigurationsinformationen, einschließlich Klassifizierer, Bezeichner, Probes und Sensoren, werden nicht nach Domänen getrennt.

Service Provider verwenden in der Regel die IP-basierte Erkennung. In Fällen, in denen der SP die Netzwerkadressierung steuert, teilen sie den Adressraum auf ihre Kunden auf,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

um sicherzustellen, dass jede Domäne über einen eigenen IP-Adressraum verfügt. Der SP weist einem Kunden oder einer Domäne ein oder mehrere Subnetze zu und erstellt Erkennungszeitpläne für diese Subnetze.

Wenn der SP die Rechenzentren von Kunden remote verwaltet, kommt es häufig zu Überschneidungen zwischen Adressräumen, die von verschiedenen Kunden verwendet werden. In diesen Fällen kann der SP die Netzwerkadressübersetzung (NAT) für den IP-Bereich verwenden und einen Erkennungszeitplan ausführen.

Sobald die CIs der richtigen Domäne zugewiesen sind, werden Transparenz und Kontrolle über den Lese-/Schreibzugriff von der Plattform über die Domänenhierarchie bereitgestellt. Zeitpläne sind für Benutzer in ihren jeweiligen Domänen sichtbar. Domänenübergreifende Zeitplantransparenz ist nicht möglich, außer für den SP, der die übergeordnete Domäne steuert und für den alle Domänen sichtbar sind.

Domänentrennung für MID Server-Dateien

Sie können Versionen dieser spezifischen MID Server-Richtlinieneinträge erstellen, die nur ein MID Server aus derselben Domäne verwenden kann. Diese Prozesstrennung wird für Datensätze in Tabellen unterstützt, die die MID Server-synchronisierten Dateien [ecc_agent_sync_file] erweitern:

- MID Server-MIB-Datei [ecc_agent_mib]
- MID Server-JAR-Datei [ecc_agent_jar]
- MID Server-Skriptdatei [ecc_agent_script_files]

Standardmäßig sind alle Datensätze in diesen Tabellen Mitglieder der globalen Domäne. Ein Benutzer kann die globale Standarddomäne überschreiben und eine Version dieser Richtlinien zur Verwendung in der eigenen Domäne des Benutzers erstellen.

Hinweis: Anlagen in MIB- oder JAR-Dateisätzen werden möglicherweise nicht wie in einer Umgebung angezeigt, in der die Domäne nicht getrennt ist. Die Anhänge werden nicht angezeigt, weil die Tabelle **Anhänge** [sys_attachment] durch Daten getrennt ist. Wenn Daten zwischen Domänen aufgeteilt werden, kann ein Datensatz in einer untergeordneten Domäne nicht auf Datensätze in einer übergeordneten Domäne zugreifen.

Anweisungen zum Einrichten der Domänentrennung über den MID-Server finden Sie unter MID-Server-Domänentrennung .

Domänengetrennte Tabellen

Datensätze in allen Tabellen, die die Tabelle „Grundlegendes Configuration Item“ [cmdb] erweitern, können nach Domänen getrennt werden. Darüber hinaus können Datensätze auch in den folgenden Tabellen nach Domänen getrennt werden:

- Seriennummer [cmdb_serial_number]
- TCP-Verbindung [cmdb_tcp]
- Fibre-Channel-Initiator [cmdb_fc_initiator]
- Fibre Channel-Ziele [cmdb_fc_target]
- IP-Adresse zu DNS-Name [cmdb_ip_address_dns_name]
- Service [cmdb_ip_service_ci]
- Virtuelles KVM-Gerät [cmdb_kvm_device]
- Load Balancer-Service-VLAN [cmdb_lb_service_vlan]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Load Balancer VLAN-Schnittstelle [cmdb_lb_vlan_interface]
- Switch-Anschluss [cmdb_switch_port]

Zugehörige Informationen

Domänentrennung für Service Provider

Empfohlene Domain Separation-Verfahren für Service Provider

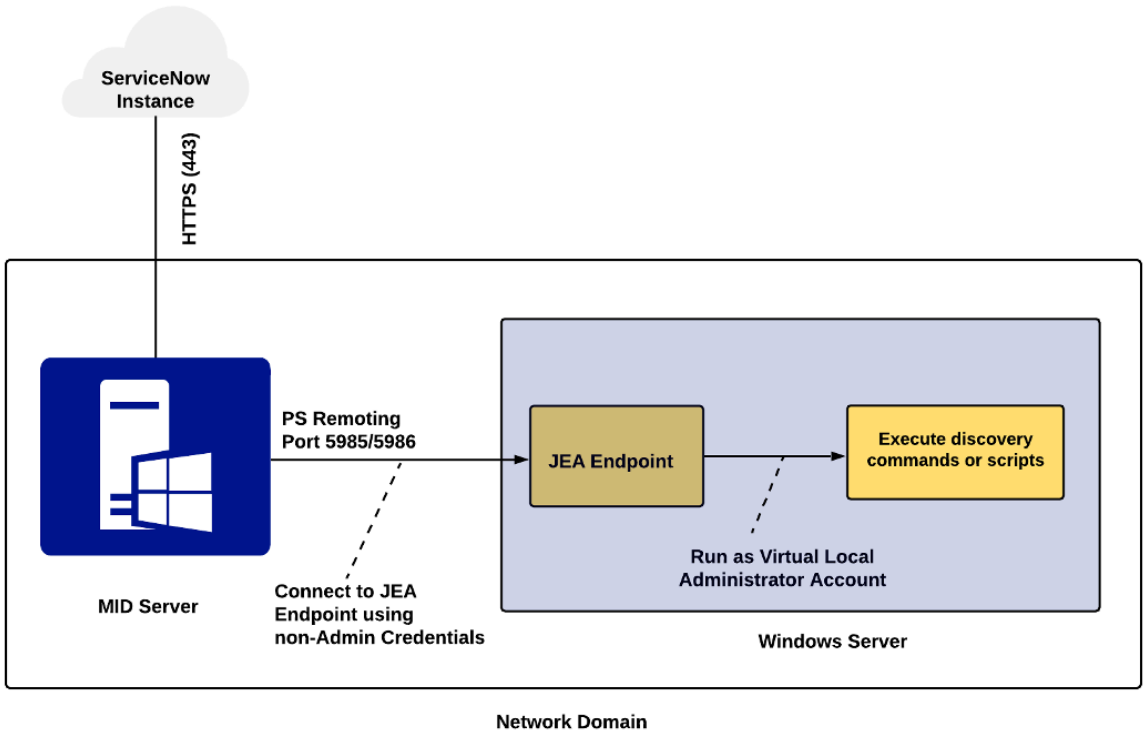
Discovery-Verhalten

Discovery-Dashboard

Microsoft Just Enough Administration (JEA) für Discovery

Microsoft JEA verbessert die Sicherheit, indem Benutzern ohne Administratorrechte der beschränkte Zugriff auf die für Discovery erforderlichen Befehle, Skripts und ausführbaren Dateien ermöglicht wird. Dadurch kann der MID-Server Informationen über einen Windows-Computer erfassen, ohne dass für das Ziel vollständige Administratorrechte erforderlich sind.

Microsoft JEA ermöglicht eine rollenbasierte Administration über PowerShell-Remoting, das Windows Remote Management (WinRM) zur Verwaltung der Kommunikation und Authentifizierung verwendet. Dieses Framework bietet eine sichere und zuverlässige Methode für die Verwaltung von Computern, die das HTTP-Protokoll verwenden. PowerShell-Remoting verwendet insgesamt zwei Ports (5985, 5986) für HTTP und HTTPS, was einfacher zu sichern ist als die Vielzahl von Ports, die bei der dynamischen WMI-Portzuordnung verwendet werden. Weitere Informationen zu Microsoft JEA finden Sie unter Just Enough Administration .



Anforderungen für die Erkennung mit JEA

- ServiceNow-Instanz, auf der Release Rome oder höher ausgeführt wird.
- MID Server und Zielserver müssen Teil einer Windows-Domäne sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die JEA-Anmeldeinformationen, die nicht über Administratorrechte verfügen, müssen Anmeldeinformationen auf Domänenebene sein.
- Auf den Windows-Zielcomputern muss PowerShell 5.0 oder Windows Management Framework 5.1 installiert sein.
- Auf den Ziel-Windows-Computern muss PowerShell-Remoting aktiviert sein.

Hinweis: Zur Verbesserung der Sicherheit gibt es ab Rome ein neues Profil namens JEA v2. Microsoft rät davon ab, im JEA-Profil einen anderen Sprachmodus als **NoLanguage** anzugeben. JEA v2 legt den Sitzungstyp explizit auf **RestrictedRemoteServer** und den Sprachmodus auf **NoLanguage** fest, um zu verhindern, dass Benutzer am Endpunkt Skripts ausführen und Sicherheitsbeschränkungen umgehen können. ServiceNow unterstützt das vorhandene Beispielprofil in KB0782125 nicht mehr. Befolgen Sie die Anweisungen in KB0965705 , um JEA v2-Profile einzurichten und bereitzustellen.

JEA-Profile

Discovery mit JEA erfordert Profile, die aus einer PowerShell-Sitzungskonfiguration und mindestens einer PowerShell-Rollenfunktionsdatei bestehen. Sie können mehrere PowerShell-Rollenfunktionsdateien und mehrere Benutzergruppen erstellen, um die Rollen bei Bedarf verschiedenen Gruppen zuzuweisen. Ein Beispielprofil wird in KB0965705 als Referenzimplementierung bereitgestellt und dient als Ausgangspunkt. Die Konfigurationsdatei in der KB unterstützt zum Zeitpunkt der Erstellung alle sofort einsatzbereiten horizontalen Windows-Muster. ServiceNow ist nicht verantwortlich für die Bereitstellung und Einrichtung von JEA-Profilen auf Remotecomputern.

Microsoft bietet über die folgenden Links eine detaillierte Dokumentation:

- JEA-Rollenfunktionen
- JEA-Sitzungskonfiguration

Basiserkennung mit JEA-Beispielprofil

Das in KB0965705 bereitgestellte JEA-Beispielprofil wurde so konfiguriert, dass es viele grundlegende CIs und Attribute erkennt. Das Profil kann geändert werden und sollte nur als Baseline für die Erkennung mit JEA dienen.

Bei der Basiserkennung werden die folgenden Schlüsselattribute von Windows-Servern (cmdb_ci_win_server) und Windows-Desktops (cmdb_ci_computer) erkannt:

- Hostname
- DNS-Name
- Seriennummer
- Betriebssystem
- BS-Version
- BS-Service Pack
- Festplattenspeicher
- RAM
- Anzahl CPU-Kerne
- CPU-Anzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CPU-Hersteller
- CPU-Typ

Darin eingeschlossen sind die folgenden CIs:

- Netzwerkadapter (cmdb_ci_network_adapter)
- Dateisystem (cmdb_ci_file_system)
- Speichergeräte (cmdb_ci_disk)
- Installierte Software (cmdb_software_instance)
- Laufende Prozesse (cmdb_running_process)
- Speichermodule (cmdb_ci_memory_module)
- Seriennummern (cmdb_serial_number)
- TCP/IP-Verbindung (cmdb_tcp)
- CI-IPs (cmdb_ci_ip_address)
- DNS-Namen für CIs (cmdb_ci_dns_name)
- Windows-Cluster (cmdb_ci_win_cluster, cmdb_ci_win_cluster_node, cmdb_ci_win_cluster_resource)
- Nachverfolgte Konfigurationsdateien (cmdb_ci_config_file_tracked)

Außerdem können die folgenden Anwendungs-CIs erkannt werden:

- MSSQL-DB unter Windows (cmdb_ci_db_mssql_instance)
- MySQL-DB unter Windows (cmdb_ci_db_mysql_instance)
- Oracle-DB unter Windows (cmdb_ci_db_mssql_instance)
- WebSphere unter Windows (cmdb_ci_app_server_websphere)

Zur Erkennung mit dem Beispielprofil werden die folgenden Probes und Muster verwendet:

- Windows - Classify (Probe)
- Windows OS - Servers (Muster)
- Windows OS - Desktops (Muster)
- Windows - Installed Software (Probe)
- Windows - ADM (Multi-Probe)
- My SQL Server On Windows (Muster)
- MSSql DB On Windows (Muster)
- Oracle DB on Windows (Muster)
- Windows - WebSphere - Cell (Probe)
- Windows - WebSphere - Web Applications (Probe)
- Windows - WebSphere - Web Services (Probe)

Instanz für die Erkennung mit JEA vorbereiten

Um die ServiceNow®-Instanz für Discovery mit Microsoft Just Enough Administration (JEA) zu konfigurieren, definieren Sie die Windows-Anmeldeinformationen mit dem Domänennamen, und legen Sie die MID-Server-Konfigurationsparameter entsprechend fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: admin, discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen** und klicken Sie auf **Neu**.
2. Klicken Sie in der Liste mit den verfügbaren Anmeldeinformationsarten auf **Windows-Anmeldeinformationen**.
3. Erstellen Sie die Anmeldeinformationen für Nicht-Administratoren in folgendem Format für den **Benutzernamen**: *domain|user name*.
4. Senden Sie den Datensatz ab.
5. Navigieren zu **Alle** > **MID-Server** > **Server**.
6. Wählen Sie einen zu konfigurierenden **MID-Server** aus der Liste der MID-Server aus.
7. Wählen Sie die zugehörige Liste **Konfigurationsparameter** aus.
8. Legen Sie die folgenden Konfigurationsparameter für den MID-Server wie angegeben fest:

   a. **mid.windows.management_protocol:** Dieser Parameter ist für die Erkennung mit JEA erforderlich.
   Der Standardwert lautet WMI, er muss jedoch auf MID Servern, die die Erkennung mit JEA verwenden, auf WinRM gesetzt werden.

   b. **mid.powershell.jea.endpoint**: Dieser Parameter ist für Discovery mit JEA erforderlich. Dieser Parameter gibt den Namen des JEA-Endpunkts an, mit dem der MID Server auf Remotehosts eine Verbindung herstellt. Der Endpunktname wird beim Registrieren einer Konfigurationsdatei erstellt und darf nicht mit dem Namen der Konfigurationsdatei selbst verwechselt werden. Die Einstellung wirkt sich auf den gesamten MID Server aus, einschließlich WinRM-Remotesitzungen, die von Discovery auf dem MID Server erstellt wurden und auf diesen Endpunkt verweisen.

   Beispiel: Der PowerShell-Befehl **Register-PSConfiguration -name JEA_DISCO_V2 -path <session_configuration_file>** legt den Endpunktnamen auf JEA_DISCO_V2 fest. In diesem Fall muss **mid.powershell.jea.endpoint** auf JEA_DISCO_V2 aktualisiert werden.

9. Wahlweise: Verwenden Sie die folgenden MID-Server- und Systemeigenschaft, um Probleme zu beheben:

   a. **mid.probe.collekt_debug_info**: Dies ist eine optionale MID-Server-Eigenschaft zum Sammeln von Debug-Informationen.
   Wenn diese Eigenschaft auf „true“ festgelegt ist, erfasst der MID Server Debug-Informationen zu Anmeldeinformationen und speichert sie in der Nutzlast der ECC-Eingabenachricht. Dies hat keine Auswirkungen auf die Funktionsweise von JEA.

   b. **glide.discovery.log_debug_info**: Dies ist eine optionale Systemeigenschaft zum Sammeln von Debug-Informationen.
   Wenn diese Eigenschaft auf „true“ festgelegt ist, extrahiert der Erkennungssensor die Debug-Informationen aus der ECC-Eingabenachricht und schreibt diese in die Erkennungsprotokolltabelle, sodass sie beim Überprüfen des Erkennungsstatus sichtbar ist.

SNMP-Unterstützung für Discovery

Discovery bietet Unterstützung für die SNMP-Versionen 1, 2c und 3. Wenn Sie über aktive SNMP-v3-Anmeldeinformationen verfügen, sind die gültigen Optionen für die SNMP-Version

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„v3“ oder „Alle“. Wenn Sie über aktive SNMP-v1- oder SNMP-v2-Anmeldeinformationen (Community-Zeichenfolge) verfügen, sind gültige Optionen für die SNMP-Version „v1“, „v2c“ oder „Alle“. Der Standardwert ist „Alle“.

MID Server unterstützen standardmäßig alle SNMP-Protokollversionen. Sie können einen MID Server so einstellen, dass er nur bestimmte Versionen von SNMP unterstützt.

Informationen zu SNMP-Anmeldeinformationen finden Sie unter SNMP-Anmeldeinformationen .

SNMP-Probe-Parameter können bei der Erkennung eines SNMP-Geräts verwendet werden. Weitere Informationen finden Sie unter SNMP-Probeparameter.

SNMPv3-Benutzeranmeldeinformationen in Discovery hinzufügen

Richten Sie Ihre Anmeldeinformationen so ein, dass Discovery auf SNMPv3-Ziele zugreifen kann.

Vorbereitungen

Erforderliche Rolle: Administrator

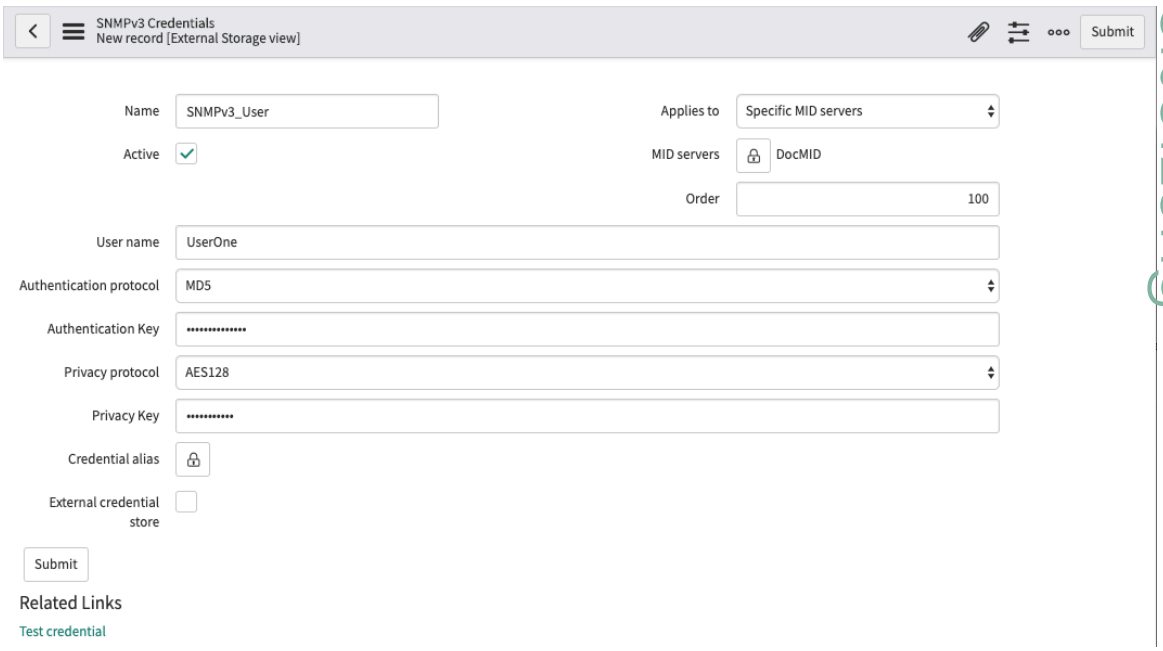
Warum und wann dieser Vorgang ausgeführt wird

Es ist auch ein MID Server-Parameter zum Steuern der SNMP-Versionen verfügbar. Weitere Informationen finden Sie unter MID-Server-Parameter .

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **SNMPv3-Anmeldeinformationen**.
4. Füllen Sie das Formular mithilfe der Felder in der Tabelle.

Formular für SNMPv3-Anmeldeinformationen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SNMPv3-Anmeldeinformationsfelder

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für diese Anmeldeinformationen. Zum Beispiel könnten Sie sie **SNMP-Community Atlanta** nennen.
Aktiv	Aktivieren oder deaktivieren Sie diese Anmeldeinformationen.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
MID-Server	Wählen Sie einen oder mehrere MID Server aus der Liste der verfügbaren MID Server aus. Die in diesem Datensatz konfigurierten Anmeldeinformationen stehen den MID Servern in dieser Liste zur Verfügung. Dieses Feld ist nur verfügbar, wenn Sie **Spezifische MID-Server** im Feld **Gilt für** auswählen.
Reihenfolge	Reihenfolge (Reihenfolge), in der Discovery diese Anmeldeinformationen bei dem Versuch, sich bei Geräten anzumelden, ausprobiert. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Anmeldeinformationen dieselbe (oder keine) Reihenfolgennummer haben, werden die Anmeldeinformationen von der Instanz in zufälliger Reihenfolge ausprobiert.
Benutzername	Geben Sie den SNMP-Benutzernamen ein. Vermeiden Sie in Benutzernamen führende oder nachfolgende Leerzeichen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachfolgende Leerzeichen im Benutzernamen erkennt.
Authentifizierungsprotokoll	Wählen Sie den Authentifizierungstyp aus, der für diese Anmeldeinformationen verwendet werden soll. Die Auswahlmöglichkeiten sind: ◦ MD5 ◦ SHA-1 ◦ SHA-224 ◦ SHA-256 ◦ SHA-384 ◦ SHA-512
Authentifizierungsschlüssel	Geben Sie den mit diesen Anmeldeinformationen zu verwendenden Authentifizierungsschlüssel ein.
Datenschutzprotokoll	Wählen Sie das Verschlüsselungsprotokoll für diese Anmeldeinformationen aus. Die Auswahlmöglichkeiten sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	◦ 3DES ◦ AES128 ◦ AES192 ◦ AES256 ◦ DES
Datenschutzschlüssel	Geben Sie den Schlüssel ein, der dem ausgewählten Datenschutzprotokoll zugeordnet ist.
Nachweis-ID	Geben Sie den für externe Anmeldeinformationen in der JAR-Datei, die für einen externen Anmeldeinformationsanbieter auf den MID Server hochgeladen wurde, konfigurierten eindeutigen Schlüssel ein. Das Feld **Nachweis-ID** darf maximal 40 Zeichen lang sein. Dieses Feld ist nur sichtbar, wenn das Kontrollkästchen **Externer Speicher für Berechtigungsnachweise** aktiviert ist.
Datenschutz-Anmeldeinformations-ID	Geben Sie den für SNMPv3-Anmeldeinformationen konfigurierten Datenschutzkonto-Schlüssel in CyberArk ein. Wenn Sie ein Datenschutzprotokoll in CyberArk verwenden, muss dieses Feld denselben Wert aufweisen wie das Feld **Name** für das CyberArk-SNMPv3-Datenschutzkonto. Dieses Feld ist für SNMPv3 nur sichtbar, wenn Sie im Feld **Anmeldeinformationsspeicher-Typ** die Option **CyberArk** auswählen. Wenn Sie keinen Datenschutzschlüssel für CyberArk verwenden, lassen Sie dieses Feld leer.
Anmeldeinformationsalias	Lassen Sie zu, dass Ersteller von Workflows, jeder Aktivität in einem Orchestration-Workflow einzelne Anmeldeinformationen zuweisen, oder weisen Sie jedem Vorkommen desselben Aktivitätstyps in einem Orchestration-Workflow unterschiedliche Anmeldeinformationen zu.
Externer Anmeldeinformationsspeicher	Aktivieren Sie dieses Kontrollkästchen, um ein externes Speichersystem für Anmeldeinformationen zu verwenden. Wenn ein externer Speicher aktiviert ist, wird das Feld **Nachweis-ID** angezeigt. Eine externe Speicherung von Anmeldeinformationen ist nur verfügbar, wenn das External Credential Storage-Plugin aktiviert und die Ansicht **Externer Speicher** ausgewählt ist.
Anmeldeinformationsspeicher-Typ	Wählen Sie den Provider für den externen Speicher aus. Wählen Sie **CyberArk** nur aus, wenn Sie einen SNMPv3-Datenschutzschlüssel für CyberArk verwenden. Das Feld **Datenschutz-Anmeldeinformations-ID** wird zur Eingabe des Schlüssels angezeigt.
Kontext verwenden	Aktivieren Sie dieses Kontrollkästchen, um einen Kontextwert für diese Anmeldeinformationen hinzuzufügen. Dieses Feld wird in der **Discovery**-Ansicht angezeigt. Kontexte werden derzeit für externe Anmeldeinformationsspeicher nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	Hinweis: Ein Kontext ist eine Sammlung von Verwaltungsinformationen, auf die SNMPv3-Anmeldeinformationen zugreifen, in denen auf eine bestimmte OID verwiesen wird. Auf Kontexte wird manchmal verwiesen, damit Informationen über das Gerät gesammelt werden können, auf die mit den normalen Anmeldeinformationen nicht zugegriffen werden kann. Ein Kontext kann vom Hersteller bereitgestellt oder separat konfiguriert werden. Wenn Sie über mehrere SNMPv3-Anmeldeinformationen mit demselben Benutzernamen und denselben Schlüsseln verfügen, einige Ihrer Geräte jedoch einen Kontext benötigen und andere nicht, müssen Sie für jedes Gerät separate Datensätze erstellen.
Kontextname	Geben Sie den Kontextnamenswert für diese Anmeldeinformationen ein. Diese Option sollte nur verwendet werden, wenn Sie über Geräte verfügen, die diesen Wert für einen vollständigen Zugriff benötigen. Dieses Feld wird angezeigt, wenn das Kontrollkästchen **Kontext verwenden** aktiviert ist.

SNMPv3-Sicherheitsoptionen

Option	Zu konfigurierende Felder
noAuthNoPriv-Sicherheit	◦ **Authentifizierungsprotokoll:** Keins ◦ **Datenschutzprotokoll:** Keins ◦ **Authentifizierungsschlüssel:** Leer lassen ◦ **Datenschutzschlüssel:** Leer lassen
authNoPriv-Sicherheit	◦ **Authentifizierungsprotokoll:** Festgelegt ◦ **Datenschutzprotokoll:** Leer lassen ◦ **Authentifizierungsschlüssel:** Festgelegt ◦ **Datenschutzschlüssel:** Leer lassen
authPriv	◦ **Authentifizierungsprotokoll:** Festgelegt ◦ **Datenschutzprotokoll:** Festgelegt ◦ **Authentifizierungsschlüssel:** Festgelegt ◦ **Datenschutzschlüssel:** Festgelegt

SNMP-Version für Erkennungszeitplan festlegen

Sie müssen auch die SNMP-Version festlegen, nachdem Sie die entsprechenden Anmeldeinformationen ausgewählt haben.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Es ist auch ein MID Server-Parameter zum Steuern der SNMP-Versionen verfügbar. Weitere Informationen finden Sie unter MID-Server-Parameter .

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Zeitpläne**> *Ihren Discovery-Zeitplan.*
2. Wählen Sie im Feld **SNMP-Version verwenden** die entsprechende Version aus.

   Der Standardwert lautet **ALLE**. Sie können den Wert in **v1**, **v2c** oder **v3** ändern.

Discovery und SCCM zusammen

Verwenden Sie die folgenden Richtlinien, um häufige Probleme zu vermeiden, wenn Sie Discovery und System Center Configuration Manager (SCCM) gemeinsam verwenden.

Sie müssen entscheiden, ob Sie AI- oder Nicht-AI-Softwaredatenquellen (AI = Asset-Intelligenz) verwenden. Da die Softwarekorrelationsdaten für jede dieser Datenquellen unterschiedlich nachverfolgt werden, sollten Sie vermeiden, zwischen beiden hin- und herzuwechseln. Wenn Sie zwischen Datenquellen wechseln müssen, entfernen Sie vor dem Wechsel alle von SCCM importierten Softwareinstallationsdatensätze.

Wenn Software Asset Management nicht aktiviert ist, werden Softwareinstallationsdatensätze in der Tabelle „Softwareinstanz“ [cmdb_software_instance] gespeichert. Wenn Software Asset Management aktiviert ist, werden Softwareinstallationsdatensätze in der Tabelle „Softwareinstallation“ [cmdb_sam_sw_install] gespeichert.

Hinweis: Wenn Datensätze vor dem Wechsel nicht entfernt werden, sind möglicherweise doppelte Datensätze vorhanden. Falls AI- und Nicht-AI-Daten gemischt wurden, löschen Sie die Tabelle „Softwareinstallation“.

Übersicht über Service Graph Connector für MicrosoftMicrosoft Azure Event Hubs SCCM

Verwenden Sie Service Graph Connector für MicrosoftMicrosoft Azure Event Hubs SCCM, um Daten aus SCCM in die ServiceNow-Instanz abzurufen. Weitere Informationen finden Sie unter Service Graph Connector für Microsoft SCCM .

Hinweis: Wenn Sie Ihre Instanz auf eine Version von Now Platform aktualisieren, die keine Unterstützung für Ihre SCCM-Version bietet, können Sie diese Version weiterhin verwenden. Alle neuen Instanzen erfordern jedoch die Verwendung einer unterstützten SCCM-Version.

Upgrade auf neue Version

Die ServiceNow-SCCM-Integrationen sind in sich abgeschlossen und können unabhängig vorhanden sein. Für sie werden jeweils eigene Importsatztabellen, Datenquellen und Transformationszuordnungen verwendet. Von allen SCCM-Integrationen werden jedoch Daten in dieselben Tabellen innerhalb der ServiceNow-CMDB umgewandelt. So vermeiden Sie, dass die Daten von einer anderen Quelle überschrieben werden:

- Verwenden Sie eine einzige SCCM-Integration, und deaktivieren Sie alle anderen geplanten SCCM-Importe.
- Führen Sie einen vollständigen Import durch, um die Tabellen „cmdb_software_instance“, „cmdb_sam_sw_install“ und andere Tabellen alter SCCM-Daten zu löschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Softwaredaten mit SCCM oder Discovery erfassen

Wenn Discovery und SCCM auf einem System aktiviert sind, können sich die von beiden Tools erkannten Softwaredatensätze gegenseitig überschreiben.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Um festzulegen, wie Softwaredaten erfasst werden, konfigurieren Sie die Eigenschaft *glide.discovery.software_sccm_managed*.

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **Eigenschaften**.
2. Legen Sie die Eigenschaft **Windows-Software wird von SCCM verwaltet** (*glide.discovery.software_sccm_managed*) entsprechend fest.
   Wenn diese Eigenschaft auf **Ja** festgelegt wird, wird die Software für Computer-CIs in der CMDB durch SCCM gefüllt. Ein interner Prozess bestimmt, dass der Computer von SCCM verwaltet wird, und Discovery füllt die Softwaredatensätze für Windows-Softwaredaten nicht. Die folgende Nachricht auf Informationsebene wird in die Discovery-Protokolldatei geschrieben.

   ```
   Software wird nicht gefüllt, da das CI von SCCM verwaltet wird
   ```

   Wenn das Kontrollkästchen deaktiviert ist, wird die Eigenschaft auf **Nein** festgelegt, und das System verwaltet Softwaredaten mit Windows.
3. Klicken Sie auf **Speichern**.

> **Wichtig:** Wenn die SCCM-Integration aktiv ist, bevor Discovery aktiviert wird, und die Eigenschaft aktiviert ist, ignoriert Discovery das Füllen der Software für alle CIs, die auch über SCCM importiert werden. Wenn Discovery vor der SCCM-Integration aktiviert wird, können sich Softwareinstallationsdaten aus beiden Quellen vermischen.

Nächste Maßnahme

Verwenden Sie diese Discovery-Eigenschaften, um Diskrepanzen bei Softwaredaten zwischen Discovery und SCCM zu vermeiden: *glide.discovery.enable.software_simplify* und *glide.discovery.enable.software_simplify_sccm*. Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Discovery-Klassifizierer

Ein Klassifizierer teilt Discovery mit, welche Probes für die Identifizierungs- und Erkundungsphase der Erkennung ausgelöst werden sollen. Klassifizierer können auch die Probe „Horizontal Pattern“ auslösen, der anstelle von zusätzlichen Probes ein Muster für die Identifizierung und Erkundung startet.

Im Wesentlichen startet der Klassifizierer die Identifizierungsphase. Diese wird von Discovery verwendet, nachdem die Klassifizierungs-Probe wichtige Parameter an die Instanz zurückgegeben hat, die Discovery mitteilen, was als Nächstes zu tun ist.

In den meisten Fällen ist es nicht erforderlich, einen Klassifizierer zu erstellen oder einen Klassifizierer zu ändern. Wenn Sie jedoch Probleme mit der horizontalen Erkennung haben, sollten Sie gegebenenfalls die Bedingungen überprüfen, die bestimmen, wann ein Klassifizierer basierend auf den Parametern, die die Klassifizierungs-Probe an die Instanz zurückgibt, ausgeführt wird. Oder wenn Sie eine neue Art von CI erkennen möchten, die Discovery noch nicht erkennt, können Sie einen eigenen Klassifizierer erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierung von Geräten, Prozessen und IP-Adressen

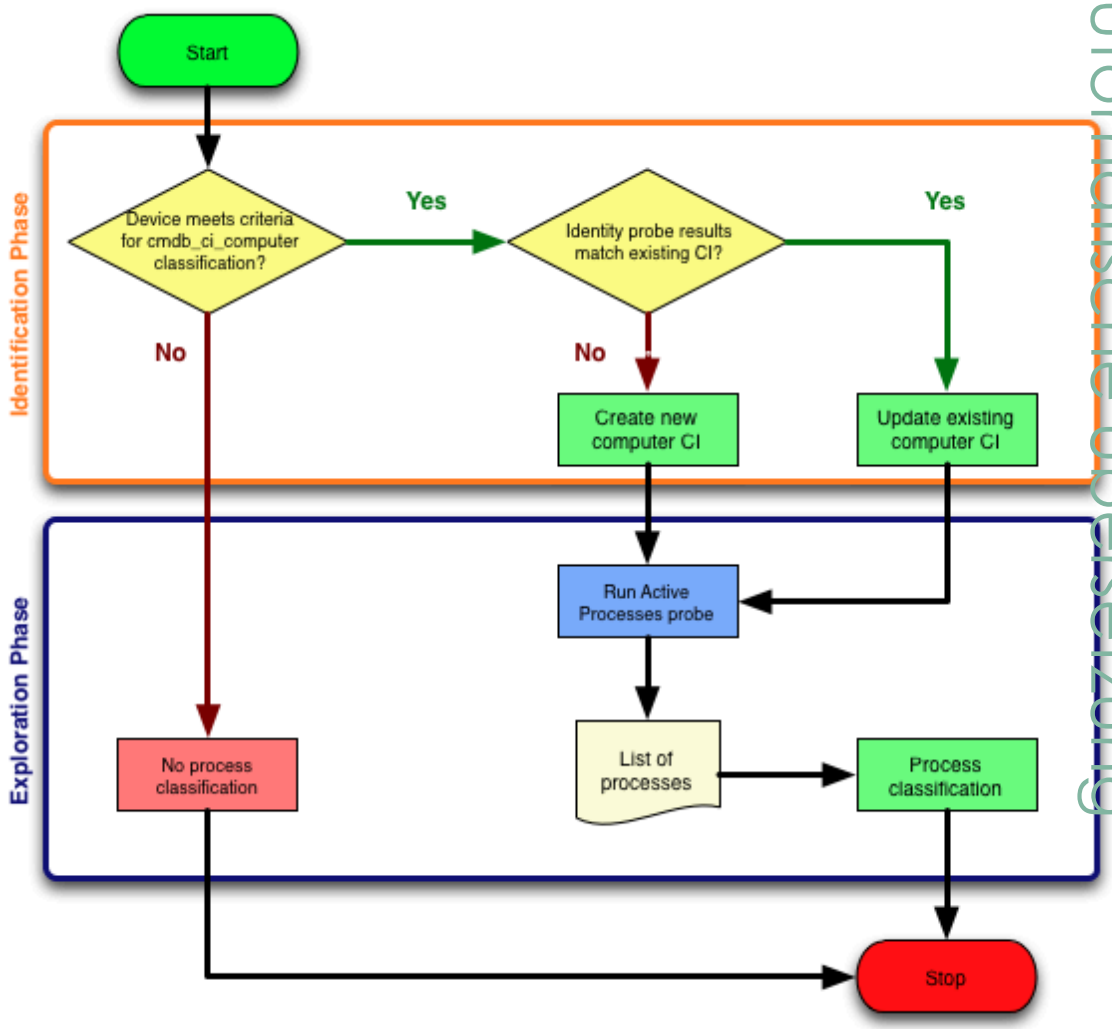
Die Discovery-Klassifizierung lässt sich in drei Typen unterteilen: Geräteklassifizierung, Prozessklassifizierung und IP-Adressklassifizierung (bzw. IP-Scan-Klassifizierung):

Geräteklassifizierung

Die Klassifizierung der tatsächlichen Gerätetypen, zum Beispiel ein Computer mit Windows, ein Computer mit einer Flavour-Version oder UNIX oder LINUX, ein Router, ein Switch oder ein Lastenausgleichsmodul usw.

Wenn Discovery ein Computer-CI erkennt, wird eine aktive Prozess-Probe ausgelöst, um die Erkundung des Computer-CI voranzutreiben. Discovery vergleicht die Ergebnisse der aktiven Prozess-Probe mit den Prozessklassifizierungsbedingungen, um festzustellen, ob eine Übereinstimmung vorliegt.

Workflow der Klassifizierung von Computer-CIs



Automatische Übersetzung

Ab dem Madrid-Release kann der horizontale Erkennungsprozess Geräte mit HTTP klassifizieren.

Von allen Protokollen, die Discovery verwenden (einschließlich WMI, SSH und SNMP), hat HTTP standardmäßig die niedrigste Priorität. Discovery verwendet die HTTP-Klassifizierung nur unter folgenden Umständen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Shazzam stellt fest, dass die Ports für den HTTP- (80) - und HTTPS-Verkehr (443) offen sind.
- Der horizontale Erkennungsprozess schlägt für die Port-Sonden mit höherer Priorität (WMI, SSH und SNMP) fehl, wenn die Ports für diese Protokolle nicht geöffnet sind oder wenn die Erkennung dieser Protokolle fehlschlägt. Der horizontale Erkennungsprozess kann beispielsweise fehlschlagen, wenn SSH- und SNMP-Anmeldeinformationen nicht konfiguriert oder falsch sind.

Hinweis: Siehe Port-Sonden für weitere Informationen zur Funktionsweise von Port-Scanning und die Prioritäten der verschiedenen Protokolle.

Die HTTP-Klassifizierung startet die Sonde **HTTP Klassifizierung**, um das Gerät zu klassifizieren. Die Sonde **HTTP - Klassifizierung** führt eine GET-Anforderung für jedes Gerät für jede HTTP-Klassifizierung aus. Die URL der Anfrage setzt sich wie folgt zusammen: `PROTOCOL://IP:PORT/PATH`, wobei Folgendes gilt:

Weitere Informationen zu Port-Probes finden Sie unter Port-Sonden. Anweisungen zum Erstellen eines HTTP-Klassifizierern finden Sie unter HTTP-Klassifizierung erstellen.

Prozessklassifizierung

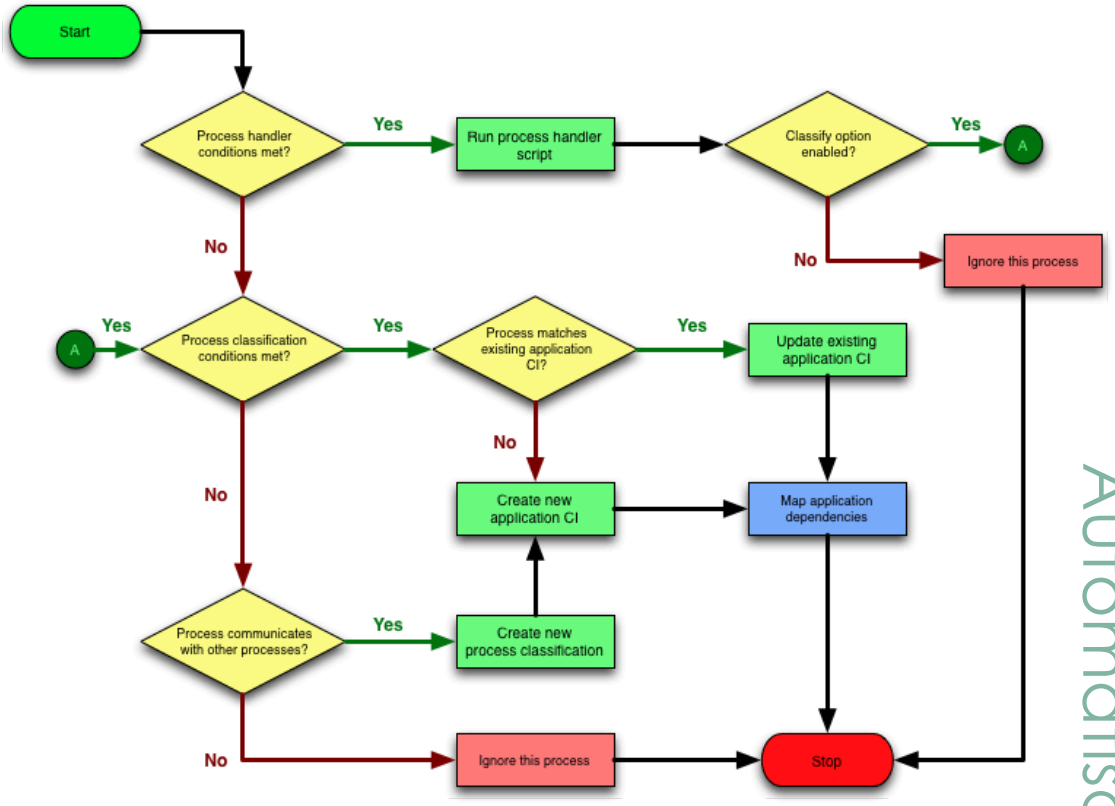
Das ist die Klassifizierung von Anwendungen basierend auf laufenden Prozessen.

Nachdem Geräte in der Tabelle „Computer“ [cmdb_ci_computer] und deren Erweiterungen identifiziert wurden, klassifiziert Discovery Prozesse während der letzten Phase der Erkennung: der Erkundungsphase. Genau wie in der Geräteklassifizierung gibt es auch in der Prozessklassifizierung eigene Klassifizierungskriterien und die Möglichkeit, Probes zu starten. Im Gegensatz zur Geräteklassifizierung werden jedoch bei der Prozessklassifizierung untergeordnete Konfigurationselemente (CIs) mit Beziehungen der Art *Wird ausgeführt auf::Wird ausgeführt* erstellt. Standardmäßig enthält Discovery Klassifizierungen für die gängigsten Prozesse.

Wenn ein Prozess den Klassifizierungskriterien entspricht, legt Discovery fest, ob das Prozess-Handler-Skript ausgeführt werden soll. Dieses Skript ändert die Parameterdaten, um Discovery dabei zu unterstützen zu erkennen, ob der Prozess ein vorhandenes oder neues Anwendungs-CI darstellt. Noch vor der Prozessklassifizierung verhindern Discovery-Prozess-Handler die Erstellung doppelter CIs, indem Parameter herausgefiltert werden, von denen bekannt ist, dass sie inkonsistente Werte enthalten. Jedes Mal, wenn Discovery ein Anwendungs-CI hinzufügt oder aktualisiert, wird auch die Zuordnung von Anwendungsabhängigkeiten des Anwendungs-CI von anderen CIs in der CMDB bestimmt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow der Klassifizierung von Prozessen



IP-Adressklassifizierung (IP-Scan)

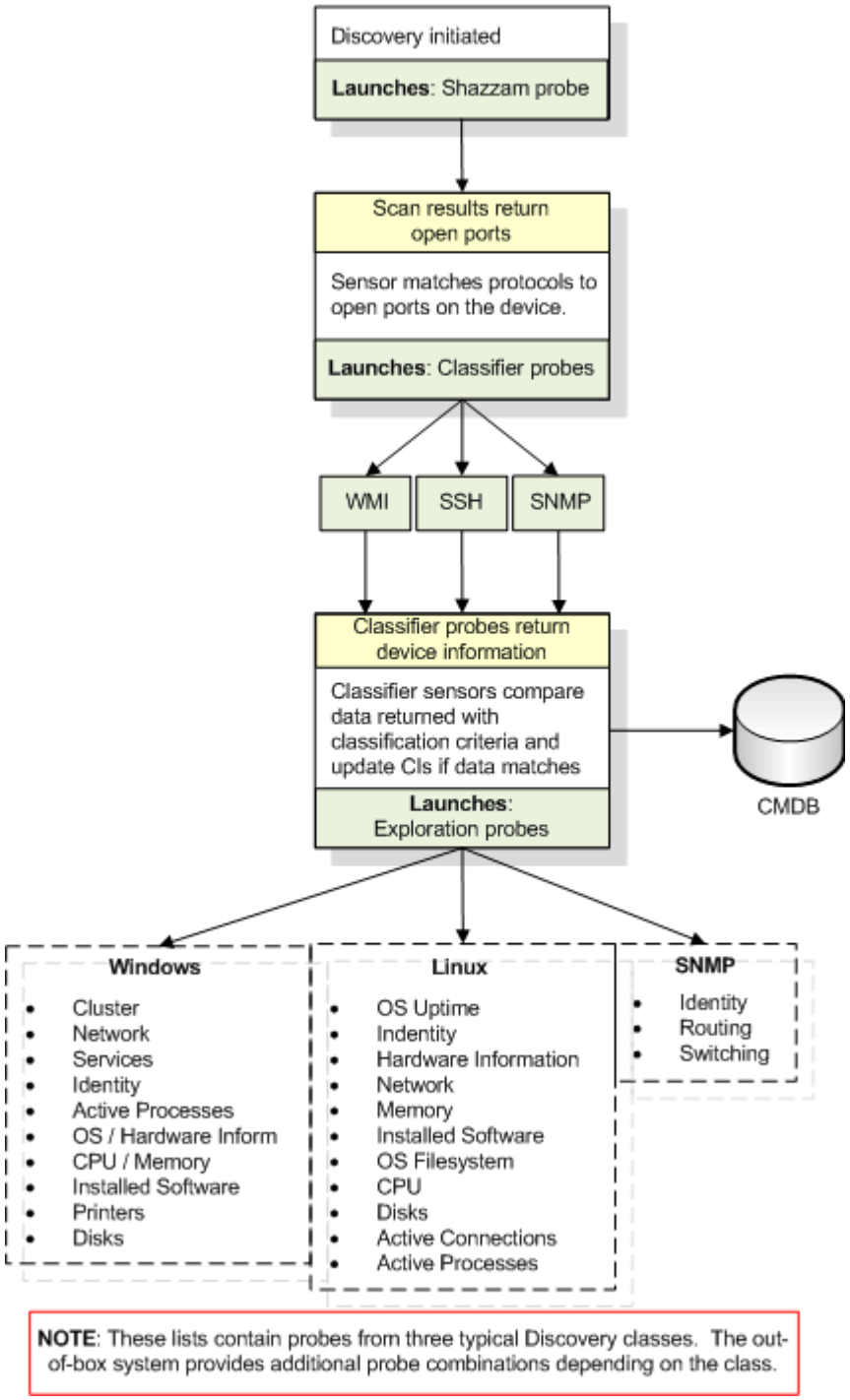
Die Erkennung von IP-Adressen erfolgt ohne Anmeldeinformationen, was bedeutet, dass Geräte und Software nur anhand der gefundenen offenen Ports und Banner identifiziert werden, ohne dass Sie Anmeldeinformationen erstellen müssen. Wenn die Klassifizierungskriterien für ein Gerät im IP-Scan-Modus erfüllt sind, aktualisiert Discovery automatisch das CI in der CMDB. Nachdem ein Gerät ordnungsgemäß klassifiziert wurde, startet Discovery die für diese Geräteklasse konfigurierten Erkundungs-Probes und beginnt mit der Erfassung detaillierter Informationen über das CI.

Im Discovery-Standardsystem löst die Linux-Klassifizierung elf Erkundungs-Probes aus, die Informationen wie Datenträgergröße, Arbeitsspeicher und die Anzahl der aktuellen Verbindungen zurückgeben. Die Daten dieser Probes werden zu unterschiedlichen Zeiten zurückgegeben und in der ECC-Warteschlange gespeichert, bis die Verarbeitung abgeschlossen ist.

Dieses Diagramm zeigt den Verarbeitungsablauf für die Klassifizierung und Überprüfung von Geräten mit einem IP-Scan (keine Bezeichner):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Scan-Klassifizierung



Unter Klassifizierung für Erkennung von IP-Adressen finden Sie weitere Details zu den Parametern, die Klassifizierern für diesen Typ von Erkennung zur Verfügung stehen.

Klassifiziererkriterien

Klassifizierer stellen auch Kriterien bereit, mit denen Sie angeben können, wann Discovery den Klassifizierer unter den von Ihnen definierten Bedingungen verwenden soll. Die Kriterien basieren auf den Parametern, die eine Klassifizierer-Probe an Discovery zurückgibt. Kriterien werden mit dem Parameter, einem Operator und einem Wert erstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Bei Bedingungsfiltern in Prozessklassifizierungen wird die Groß- und Kleinschreibung beachtet.

Klassifizierer und Muster

Zur Identifizierung und Erkundung von CIs kann Discovery anstelle von Probes auch Muster verwenden. Discovery löst Muster über die Probe „Horizontal Discovery“ aus, die für einen Klassifizierer angegeben werden kann. Sie können eigene Muster erstellen und über die Probe „Horizontal Discovery“ einem Klassifizierer hinzufügen. Anweisungen dazu finden Sie unter Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen. Möglicherweise verwenden Sie bereits eines der vordefinierten Muster, die mit Discovery bereitgestellt werden. Sie können dies überprüfen, indem Sie im Klassifizierer überprüfen, ob die Probe „Horizontal Pattern“ angegeben ist.

Debugging-Informationen zur Klassifizierung protokollieren

Fügen Sie die folgende Systemeigenschaft hinzu, um Debugging-Informationen zu Klassifizierungen zu protokollieren. Die resultierenden Protokolleinträge listen den Namen jedes ausgeführten Klassifizierers auf sowie alle Namen und Werte, die den Kriterien im Klassifizierer zur Verfügung stehen.

Systemeigenschaft	Beschreibung
`glide.discovery.debug.classification`	Aktiviert Debugging-Informationen für die Prozessklassifizierung. • **Typ**: true | false • **Standardwert**: false • **Speicherort**: Der Tabelle „Systemeigenschaften“ [sys_properties] hinzufügen

Möglichkeiten der Discovery-Klassifizierung

- Erstellen oder ändern Sie einen Erkennungsklassifizierer, wenn Sie CIs klassifizieren möchten, die von Discovery noch nicht klassifiziert werden, oder wenn Sie andere Probes auslösen möchten, die sich noch nicht in einem Klassifizierer befinden. Sie können Klassifizierer ändern, die Discovery für die Standard-CI-Erkennung, für Prozessklassifizierer für Anwendungen und für Klassifizierer basierend auf IP-Adress-Scans verwendet.

  Bevor Sie Klassifizierer ändern, prüfen Sie die Parameter, die für jeden Klassifizierertyp verfügbar sind.

- Wenn sich Windows-Computer in Ihrem Netzwerk befinden, können Sie anstelle von WMI das WinRM-Protokoll verwenden, um für eine effizientere Datenübertragung und Ausführung von Remotebefehlen zu sorgen. Standardmäßig verwendet Discovery WMI. Anweisungen zu den Klassifiziereränderungen, die Sie mit WinRM vornehmen können, finden Sie unter Windows-Remoteverwaltung für Klassifizierung verwenden.
- Wenn Sie Windows-Computer haben, die als Server fungieren, und Sie möchten, dass sie nach ihrer Funktion und nicht nach dem Betriebssystem klassifiziert werden, können Sie die Kriterien des Klassifizierers „Windows“ ändern. Anweisungen dazu finden Sie unter Neuklassifizierung von Windows Workstation-Computers als Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-CI-Klassifizierung erstellen

Eine CI-Klassifizierung ermöglicht Discovery die Erkennung der gängigsten Betriebssysteme, Netzwerkgeräte und Prozesse.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

⚠ **Warnung:** Das Hinzufügen von SNMP-OID-Klassifizierungen mit einer Net-SNMP-Modul-OID ab 1.3.6.1.4.1.8072.3.2 oder einer Windows-Betriebssystem-OID ab 1.3.6.1.4.1.311.1.1.3 kann zu einer falschen Klassifizierung von Geräten und falschen Modellnamen führen und ist nicht mehr zulässig. Dies sind Vorlagensystem-OIDs, die auf einem Gerät verbleiben können, wenn der Hersteller sie nicht durch spezifische OIDs für ihr eigenes Modell ersetzt. Beispielsweise kann eine Check Point Smart-1 3050 Firewall, die Linux als Betriebssystem verwendet, die OID für einen Linux-Server (1.3.6.1.4.1.8072.3.2.10) aufweisen. Das führt dazu, dass die Firewall falsch klassifiziert wird. Wenn mindestens zwei Geräte dieselbe OID aufweisen, konfigurieren Sie Klassifizierungskriterien, die die Geräte voneinander unterscheiden. Weitere Details hierzu finden Sie in KB0751287 .

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung**.
2. Wählen Sie den Typ der Klassifizierung aus, die Sie erstellen möchten.
3. Klicken Sie in der Liste der Klassifizierungen für den ausgewählten Typ auf **Neu**.
4. Füllen Sie das Formular anhand der Felder in der Tabelle aus.

Felder im Klassifizierungsformular

Feld	Eingabewert
Name	Name des Konfigurationselements (CI)
OID	SNMP-System-OID zum Abgleich dieses Geräts. Wenn der OID-Wert mit dem eines SNMP-Geräts übereinstimmt, verwendet Discovery die Informationen, um die CMDB mit dem angegebenen Hersteller, Modell und Klassifizierer zu füllen.
Operator	Operator zur Bestimmung der Übereinstimmung und der SNMP-OID. Die Auswahlmöglichkeiten lauten **Ist** und **Beginnt mit**. Dieses Feld ist nur für Klassifizierer vom Typ „SNMP-System-OIDs“ verfügbar.
Aktiv	Aktiviert oder deaktiviert diesen Klassifizierer. Wenn ein Klassifizierer deaktiviert ist, stoppt das System die Klassifizierung auf dieser Ebene und startet keine Klassifizierer niedrigeren Ranges. Beispiel: Wenn der Klassifizierer für Windows 2008 Server deaktiviert ist, beendet das System die Erkennung an dieser Stelle und startet den Klassifizierer für Windows 2012 Server nicht.
Reihenfolge	Reihenfolge (Sequenz), in der die Plattform diesen Klassifizierer ausführt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

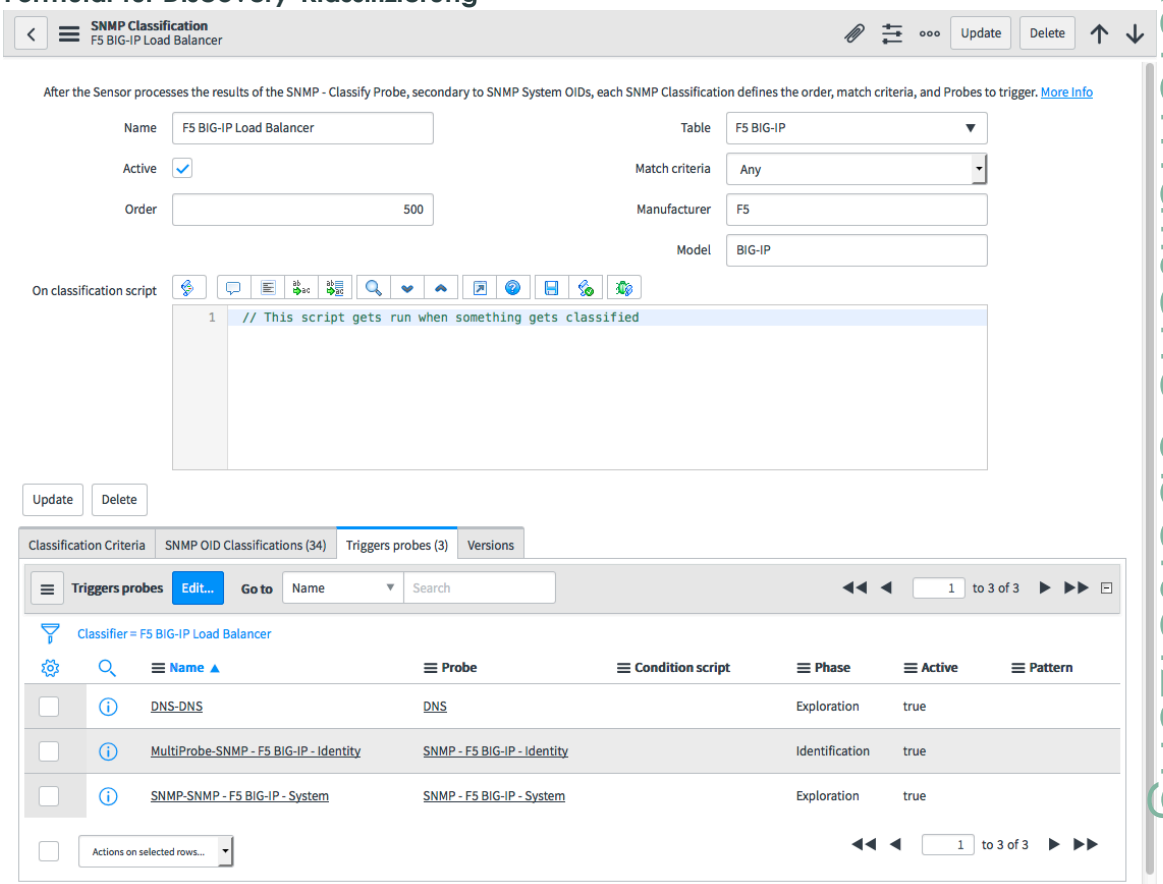
Feld	Eingabewert
Tabelle	Tabelle für diese Klassifizierung. Beispiel: Wenn dieser Datensatz einen Linux-Server klassifiziert, wählen Sie die Tabelle „Linux-Server“ [cmdb_ci_linux_server] aus.
Klassifizierung	Klassifizierung eines SNMP-Geräts, zum Beispiel **A10 Load Balancer**. Dieses Feld ist nur für Klassifizierer vom Typ „SNMP-System-OIDs“ verfügbar.
Beziehungstyp	Typ der Beziehung für diesen Klassifizierer, zum Beispiel **Wird ausgeführt auf::Wird ausgeführt**. Dieses Feld ist nur für Anwendungs- und Prozessklassifizierer verfügbar.
Kriterien anpassen	Kriterien, die erfüllt sein müssen, um dieses Gerät zu klassifizieren. Die Auswahlmöglichkeiten lauten, bezogen auf Parameter, **Beliebig** und **Alle**.
Hersteller	Name des Herstellers eines Netzwerkgeräts. Dieses Feld ist nur für Klassifizierer vom Typ „SNMP“ und „SNMP-System-OIDs“ verfügbar.
Modell	Modellnummer eines Netzwerkgeräts. Dieses Feld ist nur für Klassifizierer vom Typ „SNMP“ und „SNMP-System-OIDs“ verfügbar.
Beim Klassifikations-Skript	Skript, das ausgeführt wird, wenn die Klassifizierungskriterien erfüllt sind. Verwenden Sie dieses Skript, um spezielle Aufgaben auszuführen, nachdem ein Gerät klassifiziert wurde. Es besteht die Möglichkeit, die Hashmap `g_probe_parameters` aus einem Klassifizierungsskript zu verwenden, um Probe-Parameter für alle konfigurierten, ausgelösten Probes festzulegen. Beispielsweise wird mit diesem Code der Parameter *`node_port`* für alle ausgelösten Probes auf 16001 festgelegt: `(JS), g_probe_parameters['node_port'] = 16001; //`
Zugehörige Listen	
Klassifizierungskriterien	Kriterien, die aus bestimmten Parametern und den Werten gebildet werden, die sie enthalten müssen, um Geräte, die Discovery im Netzwerk erkennt, mit CIs in der CMDB abzugleichen. Eine detaillierte Beschreibung dieser Parameter finden Sie unter Parameter der Discovery-Klassifizierung.
SNMP-OID-Klassifizierungen	Eindeutige „Fingerabdrücke“ aller SNMP-Geräte, die im Lieferumfang des Basisprodukts von Discovery enthalten sind. Benutzer können OIDs für SNMP-Geräte hinzufügen, die sich nicht in dieser Liste befinden. Diese zugehörige Liste ist nur für SNMP-Geräte verfügbar.
Auslösertests	Erkundungs-Probes, die Discovery startet, um detaillierte Informationen über ein CI zu sammeln, das im Netzwerk klassifiziert wurde. Wenn Sie Muster für die horizontale Erkennung verwenden möchten, fügen Sie die Probe Horizontal Pattern in die Spalte **Probe** ein, und geben dann das Muster in der Spalte **Muster** an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	⚠ **Warnung:** Geben Sie Ihr Muster nicht in der Spalte **Probe** an. Wählen Sie die Probe „Horizontal Pattern“ aus, die das angegebene Muster startet.
Versionen	Listet Versionen dieses Klassifizierers auf. Bei jeder Änderung des Klassifiziererdatensatzes wird eine neue Version erstellt. Um eine vorherige Version wiederherzustellen, öffnen Sie den gewünschten Datensatz, und wählen Sie **Diese Version wiederherstellen** unter **Zugehörige Links** aus.

Dieses Beispiel zeigt ein ausgefülltes CI-Klassifizierungsformular mit definierten Erkundungs-Probes. Anweisungen zum Erstellen von Probes finden Sie unter Discovery-Probes und -Sensoren. Die hier definierten Probes werden gestartet, wenn das Gerät ordnungsgemäß klassifiziert ist, es sei denn Discovery ist so konfiguriert, dass es nach der Klassifizierung anhält.

Formular für Discovery-Klassifizierung



Automatische Übersetzung

Discovery-Prozessklassifizierung erstellen

Eine Prozessklassifizierung ermöglicht Discovery die Erstellung eines bestimmten CI-Typs aus Informationen, die während der Identifizierungs- und Erkundungsphase gesammelt wurden.

Vorbereitungen

Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein Prozess die Klassifizierungskriterien erfüllt, verwendet Discovery den Prozessklassifizierungsdatensatz zum Erstellen eines CI. Sie können Discovery auch dazu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

veranlassen, vorhandene CIs zu aktualisieren oder bestimmte Prozesse zu ignorieren, indem Sie einen Prozess-Handler erstellen.

Hinweis: Dot-Walking wird auf dem übergeordneten Element, das den Prozessbefehl ausführt, nicht unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **Prozesse**.
2. Klicken Sie auf **Neu**.
3. Geben Sie Werte in die Klassifizierungsfelder ein (siehe Tabelle).

Klassifizierungsfelder

Feld	Eingabewert
Tabelle	Wählen Sie die Tabelle aus, in der diese Klassifizierung CI-Datensätze generiert. Diese Tabelle muss eine Erweiterung der Anwendungstabelle [cmdb_ci_appl] sein.
Beziehungstyp	Wählen Sie den CI-Beziehungstyp für diese Klassifizierung aus. Das Beziehungsfeld ist nur für Prozess- und Scan-Anwendungsklassifizierungen verfügbar. Für Discovery-Prozessklassifizierungen wird normalerweise einer der folgenden Beziehungstypen verwendet: ◦ *Wird ausgeführt auf::Wird ausgeführt*: Definiert die Beziehung einer Anwendung mit dem Host, auf dem sie ausgeführt wird. Diese Beziehung wird aus der Perspektive des Hosts und der Anwendung ausgedrückt. Beispiel: Meine Datenbankanwendung wird auf server001 ausgeführt::server001 führt meine Datenbankanwendung aus. ◦ *Abhängig von::Verwendet von*: Definiert die Beziehung einer Anwendung, die mit einer anderen Anwendung kommuniziert. Diese Beziehung wird aus der Perspektive der jeweiligen Anwendung ausgedrückt. Beispiel: Die Anwendung Tomcat ist von der Datenbank MySQL abhängig::Die Datenbank MySQL wird von Tomcat verwendet. ◦ *Virtualisiert von::Virtualisiert*: Definiert die Beziehung eines virtuellen Computers mit ihrem Host. Diese Beziehung wird aus der Perspektive des virtuellen Computers und des Hosts ausgedrückt. Beispiel: server001 wird virtualisiert von Server ESX::Server ESX virtualisiert server001.
Aktiv	Wählen Sie diese Option aus, um den Prozessklassifizierungsdatensatz zu aktivieren. Nur aktive Prozessklassifizierungen können Anwendungs-CI-Datensätze erstellen.
Reihenfolge	Geben Sie die Reihenfolge ein, in der Discovery diese Prozessklassifizierung ausführen soll, wenn für eine Tabelle mehrere Klassifizierungen verfügbar sind. Discovery führt Prozessklassifizierungen von der niedrigsten zur höchsten Ordnungszahl aus.
Testen mit	Listet das Host-CI auf, bei dem die Bedingungen einer automatisch generierten Prozessklassifizierung erfüllt wurden. Verwenden Sie dieses Feld, um Änderungen an der Prozessklassifizierung zu testen. Auf diese

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	Weise können Sie sicherstellen, dass sich die aktualisierte Klassifizierung wie erwartet verhält.
Bedingung	Verwenden Sie den Condition Builder, um die Übereinstimmungs- und Klassifizierungskriterien für die Prozessklassifizierung zu erstellen. Dieses Feld ersetzt sowohl das Feld **Kriterien anpassen** als auch die zugehörige Liste **Klassifizierungskriterien**. Der Upgrade-Prozess konvertiert alle vorhandenen Klassifizierungskriterien in Bedingungen. **Hinweis:** Bei Bedingungsfiltern in Prozessklassifizierungen wird die Groß- und Kleinschreibung beachtet. **Hinweis:** Nur die folgenden Bedingungen funktionieren: ◦ Name ◦ PID ◦ PPID ◦ command ◦ parameters ◦ listening_on_ports ◦ connecting_to_ports ◦ connecting_to ◦ key_parameters ◦ classify
Beim Klassifikations-Skript	Geben Sie ein Skript ein, das ausgeführt werden soll, wenn Bedingung und Klassifizierungskriterien erfüllt sind. Verwenden Sie dieses Skript, um spezielle Aufgaben auszuführen, nachdem ein Gerät klassifiziert wurde. Es besteht die Möglichkeit, die Hashmap `g_probe_parameters` aus einem Klassifizierungsskript zu verwenden, um Probe-Parameter für alle konfigurierten, ausgelösten Probes festzulegen. Beispiel: Der folgende Code legt den Parameter `'node_port'` für alle ausgelösten Probes auf 16001 fest: `g_probe_parameters['node_port'] = 16001;` Unter Objekte vom Typ „Bei Klassifikations-Skript“ für Discovery finden Sie weitere Beispiele und eine Liste der Objekte, die Sie für diese Art von Skript verwenden können.
Auslösertests	Wählen Sie die Erkundungs-Probes aus, die von Discovery gestartet werden sollen. Diese Probes erfassen detaillierte Informationen über ein klassifiziertes CI. Discovery startet diese Probes nicht, wenn es so konfiguriert ist, dass es nach der Klassifizierung anhält. Wenn Sie Muster für die horizontale Erkennung verwenden möchten, fügen Sie die Probe Horizontal Pattern in die Spalte **Probe** ein, und geben dann das Muster in der Spalte **Muster** an.

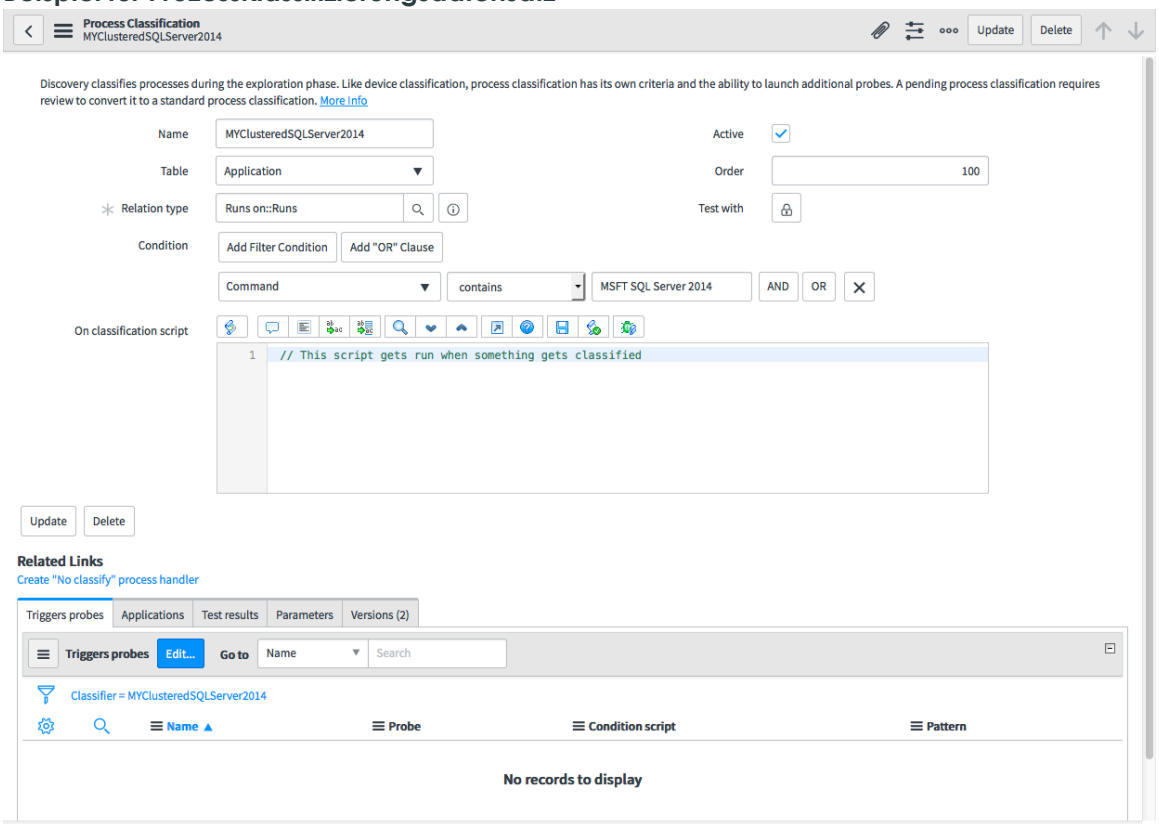
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	⚠ **Warnung:** Geben Sie Ihr Muster nicht in der Spalte **Probe** an. Sie müssen die Probe „Horizontal Pattern“ auswählen, die das angegebene Muster startet.
Anwendungen	Verwenden Sie diese zugehörige Liste, um die Anwendungs-CIs anzuzeigen, die dieser Prozessklassifizierung entsprechen.
Testergebnisse	Verwenden Sie diese zugehörige Liste, um anzuzeigen, wie Discovery Prozesse auf dem im Feld **Testen mit** angegebenen Host klassifiziert und bessere Klassifizierungsbedingungen erzielt werden.
Parameter	Verwenden Sie diese zugehörige Liste, um die Parameter anzuzeigen, die diesem Prozess zugeordnet sind, und um bessere Klassifizierungsbedingungen zu erzielen. Unter Parameter der Discovery-Klassifizierung finden Sie eine Liste der Parameter, die Sie verwenden können.
Versionen	Verwenden Sie diese zugehörige Liste, um vorherige Versionen des Prozessklassifizierungsdatensatzes anzuzeigen.

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.
5. Geben Sie Elemente aus zugehörigen Listen ein.
6. Klicken Sie auf **Aktualisieren**.

Example:

Beispiel für Prozessklassifizierungsdatensatz



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Führen Sie eine Erkennung über den Erkennungszeitplan aus, um nach Anwendungen zu suchen. Sie können auch Prozess-Handler erstellen oder ändern, die die Erstellung doppelter CIs basierend auf Prozessklassifizierungen verhindern, wenn dies ein Problem für Ihre Umgebung darstellt.

Objekte vom Typ „Bei Klassifikations-Skript“ für Discovery

Verwenden Sie ein Bei Klassifikations-Skript in einem Prozessklassifizierer, um einen Anwendungsdatensatz anzupassen. Diese Art von Skript wird in Prozessklassifizierern verwendet.

Standardname der Anwendung ändern

Standardmäßig weisen Anwendungsnamen das folgende Format auf: `<Name des Prozessklassifizierers>@<Name des Computer-CI, auf dem sich der Prozess befindet>;`

Beispiel: Für einen MySQL-Server, der auf Computer „computerA“ ausgeführt wird, lautet der Anwendungsname `mysql@machineA`.

Sie können das Feld **Beim Klassifikations-Skript** im Prozessklassifizierungsdatensatz verwenden, um den standardmäßigen Anwendungsnamen an Ihre geschäftlichen Anforderungen anzupassen. Das folgende Skript ändert beispielsweise den standardmäßigen Anwendungsnamen, um ein Suffix hinter dem Prozessklassifizierer einzufügen:

```
var computerName = g_sensor.deviceGR.name;
var processClassiferName = g_classification.name;
current.name = processClassiferName + "999" + "@" + computerName;
```

In diesem Beispiel wird der Name des Anwendungsdatensatzes in `mysql999@machineA` geändert.

Eine weitere gängige Technik ist die Festlegung des Anwendungsnamens basierend auf den Variablen name, command und parameter. Ein Eclipse-Prozess kann beispielsweise die folgenden Werte für diese Variablen aufweisen:

Name	"eclipse"
command	"/glide/eclipse/Eclipse.app/Contents/MacOS/eclipse"
parameter	"-psn_0_1884620"

Wenn eine Eclipse-Anwendung auf Computer „computerA“ ausgeführt wird, benennt ServiceNow die Anwendung in „eclipse@computerA“ um. Das folgende Skript hängt den Parameterwert als Teil des Anwendungsnamens an.

```
var computerName = g_sensor.deviceGR.name;
var processClassiferName = g_classification.name;
current.name = processClassiferName + parameters + "@" + computerName;
```

In diesem Beispiel wird der Name des Anwendungsdatensatzes in „eclipse-psn_0_1884620@computerA“ geändert.

Manchmal ist es hilfreich, Werte an die ausgelösten Probes in der Prozessklassifizierung zu übergeben. Erstellen Sie dazu ein benutzerdefiniertes Skript, das ein Name/Wert-Paar für das Objekt `g_probe_parameters` definiert. Beispiel:

```
g_probe_parameters['processCommand'] = command;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Beispiel übergibt das Skript den Parameter `processCommand` mit dem Wert der Variablen `command`, wenn ein Klassifizierungsdatensatz eine Probe auslöst.

Skriptobjekte

Verwenden Sie im Skript die folgenden Objekte:

Skriptobjekt	Beschreibung
aktuell	Verweist auf ein JavaScript-Objekt mit [property:value]-Paar, um den Anwendungsdatensatz zu aktualisieren. (Es handelt sich dabei nicht um ein tatsächliches GlideRecord-Objekt der Anwendung.)
g_sensor	Verweist auf die Sensorklasse des ausgeführten Prozesses. Dieses Objekt enthält ein deviceGR-Objekt, das auf den CI-Datensatz des Computers verweist, auf dem sich der Prozess befindet.
g_classification	Verweist auf den Prozessklassifiziererdatensatz selbst
Name	Verweist auf den Prozessnamen
command	Verweist auf den Prozessbefehl
parameters	Verweist auf die Prozessparameter
g_probe_parameters	Ein JavaScript-Objekt, das die Übergabe von Parametern an die ausgelösten Probes ermöglicht

Zugehörige Informationen

Discovery-Prozess-Handler erstellen

Discovery-Prozess-Handler erstellen

Prozess-Handler verhindern, dass doppelte CIs entstehen, indem vor der Prozessklassifizierung Parameter mit bekanntermaßen inkonsistenten Werten herausgefiltert werden. Sie können neue Klassifizierer erstellen oder vorhandene bearbeiten.

Vorbereitungen

Erforderliche Rolle: keine

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **Prozesshandler**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular „Prozesshandler“ aus.

Formular „Prozesshandler“

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für den Prozess-Handler-Datensatz ein.
Aktiv	Aktivieren Sie das Kontrollkästchen zum Ausführen des Prozess-Handler.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Klassifizieren	◦ Aktivieren Sie das Kontrollkästchen, um die Klassifizierung aller Datensätze zu laufenden Prozessen [cmdb_running_process] zu aktivieren, die den Bedingungen dieses Prozess-Handler entsprechen. ◦ Deaktivieren Sie das Kontrollkästchen, um die Klassifizierung aller Datensätze zu laufenden Prozessen [cmdb_running_process] zu deaktivieren, die den Bedingungen dieses Prozess-Handler entsprechen.
Bedingung	Wählen Sie die Bedingungen aus, die den Prozess-Handler zum Ausführen des Skripts auslösen. In den meisten Fällen enthält diese Bedingung entweder spezifische Namen von ausführbaren Dateien oder bestimmte Parameter.
Skript	Geben Sie in die Tabelle „Laufender Prozess“ [cmdb_running_process] das JavaScript ein, das Sie für den aktuellen Datensatz ausführen möchten, wenn die **Bedingung** erfüllt ist. Die `current`-Variable verweist auf einen GlideRecord eines laufenden Prozesses. Das Skript sollte `current.parameters` auf bestimmte Werte untersuchen, Zeichenfolgen ersetzen, um diese Werte zu bearbeiten, und das Ergebnis in `current.key_parameters` speichern. ServiceNow verwendet das Feld **key_parameters** zusammen mit dem Prozessnamen, um zu bestimmen, ob der Prozess auf einem bestimmten Computer eindeutig ist. Weitere Optionen finden Sie unter Objekte vom Typ „Bei Klassifikations-Skript“ für Discovery.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Führen Sie eine Erkennung über den Erkennungszeitplan aus, um nach Anwendungen zu suchen, und überprüfen Sie dann die Ergebnisse in der CMDB für die gefundenen Anwendungen.

HTTP-Klassifizierung erstellen

Ein HTTP-Klassifizierer ermöglicht dem horizontalen Erkennungsprozess, Geräte über das HTTP-Protokoll zu finden.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können zusätzliche HTTP-Klassifizierungen erstellen, wenn Sie Geräte über HTTP/REST anstatt über ein anderes Protokoll klassifizieren möchten. Verwenden Sie die HTTP-Klassifizierung nur für die Geräteerkennung, nicht für die Anwendungserkennung.

Hinweis: Standardmäßig wird der Klassifizierer „F5 HTTP“ bereitgestellt, um F5-Lastenausgleichsmodule mit REST zu klassifizieren. Das Muster **F5 LB REST** wird ebenfalls für die Erkundung des Geräts bereitgestellt. Sie müssen keinen neuen HTTP-Klassifizierer für F5-Lastenausgleichsmodule erstellen.

Von allen Protokollen, die Discovery verwenden (einschließlich WMI, SSH und SNMP), hat HTTP standardmäßig die niedrigste Priorität. Discovery verwendet die HTTP-Klassifizierung nur unter folgenden Umständen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Shazzam stellt fest, dass die Ports für den HTTP- (80) - und HTTPS-Verkehr (443) offen sind.
- Der horizontale Erkennungsprozess schlägt für die Port-Sonden mit höherer Priorität (WMI, SSH und SNMP) fehl, wenn die Ports für diese Protokolle nicht geöffnet sind oder wenn die Erkennung dieser Protokolle fehlschlägt. Der horizontale Erkennungsprozess kann beispielsweise fehlschlagen, wenn SSH- und SNMP-Anmeldeinformationen nicht konfiguriert oder falsch sind.

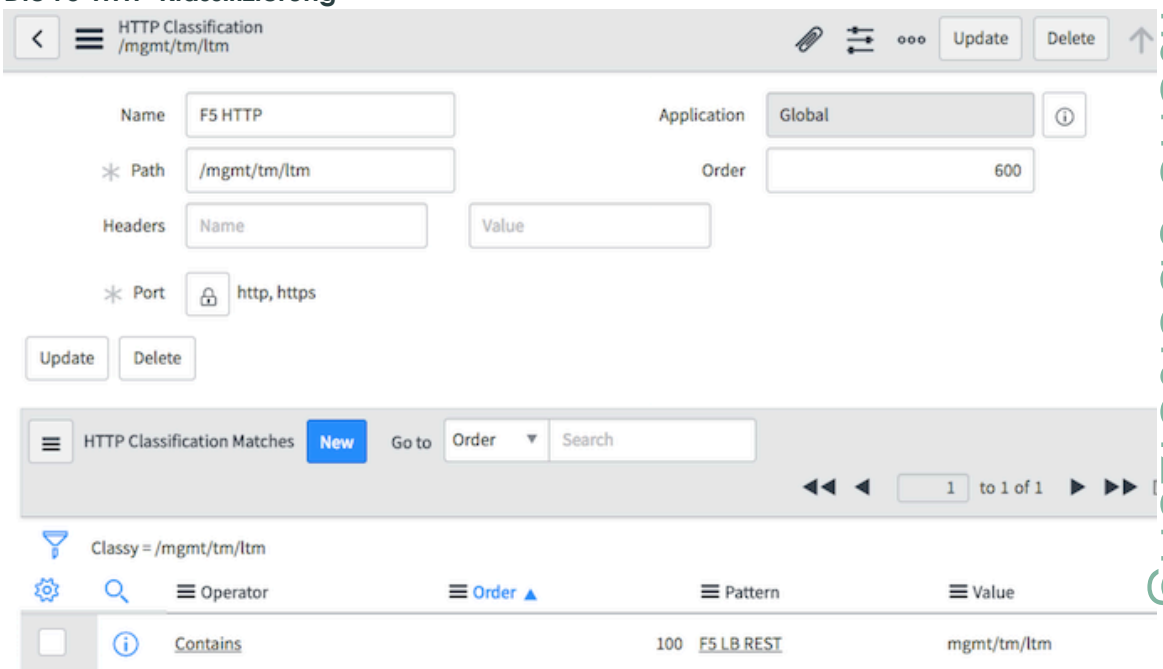
Hinweis: Siehe Port-Sonden für weitere Informationen zur Funktionsweise von Port-Scanning und die Prioritäten der verschiedenen Protokolle.

Die HTTP-Klassifizierung startet die Sonde **HTTP Klassifizierung**, um das Gerät zu klassifizieren. Die Sonde **HTTP - Klassifizierung** führt eine GET-Anforderung für jedes Gerät für jede HTTP-Klassifizierung aus. Die URL der Anfrage setzt sich wie folgt zusammen: `PROTOCOL://IP:PORT/PATH`, wobei Folgendes gilt:

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **HTTP**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle):

Die F5-HTTP-Klassifizierung



Feld	Beschreibung
Name	Geben Sie einen Namen für den Klassifizierer ein.
Pfad	Geben Sie den Pfad für die HTTP-GET-Anforderung ein.
Header	Fügen Sie einen Optionsheader mit einem Wert hinzu. Sie können eine Variable im Format `${variable}` anstatt eines statischen Wertes verwenden. Die unterstützten Header hängen vom REST-Webservice-Provider ab, zu dem Sie eine Verbindung herstellen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	möchten. In der Dokumentation Ihres Web Service Providers erfahren Sie, welche Header gültig oder erforderlich sind.
Port (IP-Dienst)	Wenn Sie möchten, dass dieser Klassifizierer einen benutzerdefinierten Port verwendet, der nicht bereits ein Standardwert in der Tabelle IP-Dienst [cmdb_ip_service] ist, führen Sie folgende Schritte aus: **a.** Wählen Sie das Suchsymbol, um die Liste der IP-Services anzuzeigen. **b.** Wählen Sie **Neu** aus und erstellen Sie eine Port-zu-Protokoll-Zuordnung. **c.** Wählen Sie diese Port-zu-Protokoll-Zuordnung dafür im Feld **Port**. Viele häufig verwendete Protokolle sind standardmäßig bereits Ports zugeordnet, z. B. `http` zu Port 80 und `https` zu Port 443. Wenn Sie eine dieser standardmäßigen Port-zu-Protokoll-Zuordnungen verwenden möchten, geben Sie keine Werte in das Feld **Port** ein. Die HTTP-Port-Sonde verwendet standardmäßig den richtigen Port.
Reihenfolge	Geben Sie eine Zahl ein, die die Priorität dieses Klassifizierers darstellt. Wenn Discovery mehr als einen zutreffenden Klassifizierer verwendet, wird der Klassifizierer mit niedriger **Rang-**Nummer verwendet.
Protokoll [optional] Dieses Feld ist standardmäßig nicht sichtbar. Sie müssen das Formular konfigurieren, um es hinzuzufügen.	Wenn Sie eine eindeutige Port-zu-Protokoll-Zuordnung für das Fel **Port** konfigurieren, geben Sie in das Feld eine optionale Protokollüberschreibung ein, die Discovery mit diesem Klassifizierer verwendet. Wenn Sie beispielsweise Port 5000 und das HTTP-Protokoll verwenden möchten, fügen Sie die 5000/HTTP-Port-zu-Protokoll-Zuordnung zum Feld **Port** hinzu, und wählen Sie dann **http** im Feld **Protokoll**.

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.

   Ein Datensatz wird in der Tabelle „HTTP-Klassifizierungen“ [discovery_classy_http] erstellt.

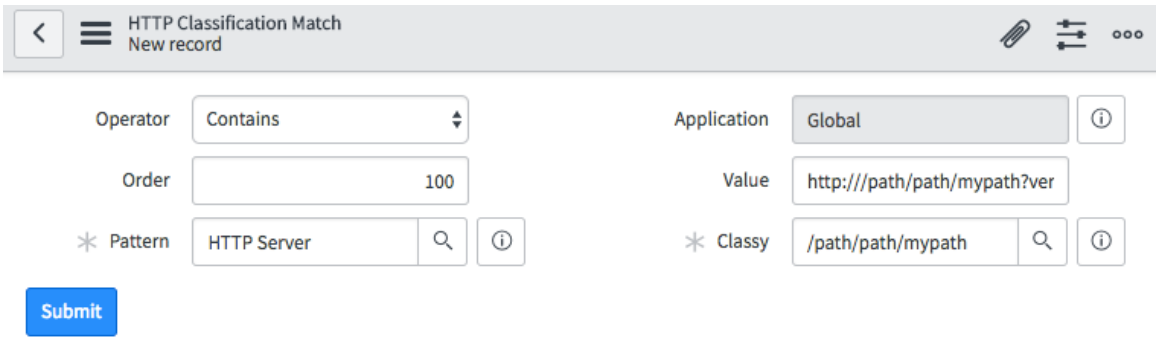
   Die zugehörige Liste „Übereinstimmung der HTTP-Klassifizierung“ wird angezeigt. Diese zugehörige Liste enthält Kriterien, die Sie für den Abgleich mit dem Hauptteil der Antwort auf die von Discovery gesendete GET-Anforderung konfigurieren können.

5. Definieren Sie in der zugehörigen Liste „Übereinstimmung der HTTP-Klassifizierung“ die Kriterien, und geben Sie das für diesen Klassifizierer zu startende Muster an:
   Die Kriterien müssen erfüllt sein, damit Discovery diesen HTTP-Klassifizierer verwenden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf **Neu**.

b. Füllen Sie die Felder des Formulars „Übereinstimmung der HTTP-Klassifizierung“ aus (siehe Tabelle).



Feld	Beschreibung
Operator	Wählen Sie den Operator aus, mit dem das System die Bedingung bewertet: ▪ **Enthält** ▪ **Ist gleich** ▪ **Regulärer Ausdruck**
Reihenfolge	Geben Sie eine Zahl ein, die die Priorität dieser Bedingung darstellt. Wenn Discovery mehr als eine zutreffende Bedingung findet, wird die Bedingung mit niedriger Rang-Nummer verwendet.
Muster	Geben Sie das Muster an, das nach einer korrekten Übereinstimmung gestartet werden soll. Dieses Muster muss HTTP verwenden, um das Gerät zu ermitteln.
Wert	Geben Sie den Wert ein, den der Rumpf der zurückgegebenen REST-Methode haben muss.

c. Klicken Sie auf **Absenden**.

d. Wenn für verschiedene Versionen des Geräts, das Sie erkennen möchten, unterschiedliche Muster vorhanden sind, definieren Sie so viele HTTP-Klassifizierungsübereinstimmungen, wie erforderlich sind.

Klassifizierung für Erkennung von IP-Adressen

Discovery bietet eine Möglichkeit, Geräte zu klassifizieren, die über die IP-Adresserkennung erkannt werden, auch wenn keine Anmeldeinformationen verfügbar sind.

Wenn Sie keine CI-Erkennung, sondern eine Erkennung für IP-Adressen ausführen, geht Discovery von bestimmten Annahmen in Bezug auf die Geräte und Anwendungen aus, die auf den Geräten an den als offen vorgefundenen Ports ausgeführt werden. Die Klassifizierungsparameter für diesen Erkennungstyp werden anders generiert als bei Scans, bei denen Anmeldeinformationen verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Syntax zum Erstellen von Parametern wird von den Feldern abgeleitet, die von der Shazzam-Probe zurückgegeben werden, wenn eine Discovery für IP-Adressen ausgeführt wird. Parameter für CIs und Anwendungen werden auf dieselbe Weise gebildet. Die Shazzam-Probe erstellt eine XML-Datei mit den folgenden Feldern:

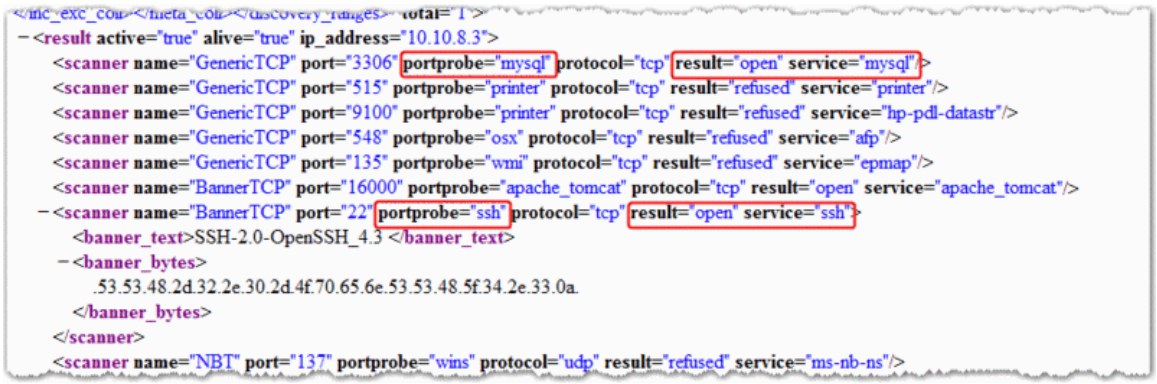
- **Name**
- **port**
- **portprobe**
- **protocol**
- **Ergebnis**
- **service**

Hinweis: Optionale Felder, die zum Bilden von Parametern verwendet werden können, werden als untergeordnete Tags unter den Standardfeldern angezeigt. Beispiel hierfür sind die Felder **sysDescr** und **banner_text**.

Parameter werden im Format <portprobe.service.field> ausgedrückt. Der Wert für *field* kann aus jedem der Felder oder untergeordneten Tags in der XML-Datei stammen. Beispielsweise klassifizieren die folgenden Parameter ein Gerät als UNIX-Server und erkennen eine MySQL-Installation:

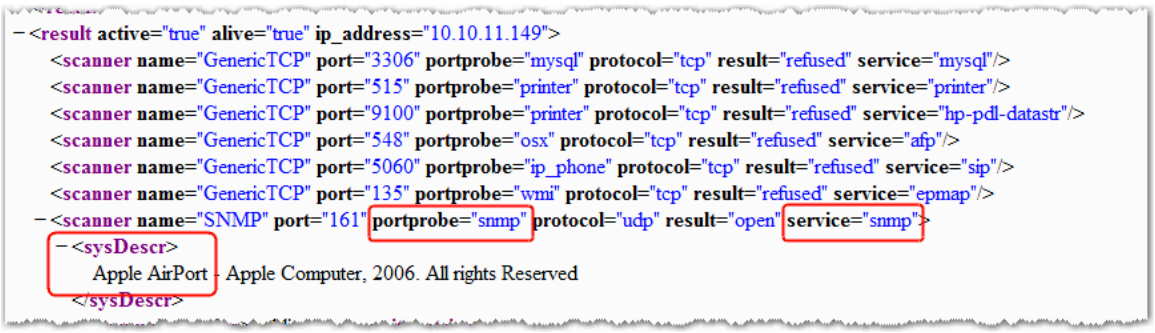
- *ssh.ssh.result*
- *mysql.mysql.result*

Diese Parameter wurden von den Werten in der folgenden XML-Datei abgeleitet, die von einer Shazzam-Probe generiert wurde, die einen IP-Scan durchführt. Das Feld *result* hat den Wert *open* für die Ports 22 und 3306 auf dem Zielgerät zurückgegeben. Das Feld *service* zeigt die Services an, die normalerweise über diese Ports kommunizieren.



Das Feld *sysDescr* kann je nach Hersteller zusätzliche Informationen zu Geräten bereitstellen. Diese XML-Datei der Shazzam-Probe zeigt Folgendes über Port 161 auf dem Gerät bei IP 10.10.11.149:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



In den Klassifizierungskriterien kann der folgende Parameter mit **sysDescr** erstellt werden, der einen Apple AirPort-WLAN-Router zurückgibt:

```
snmp.snmp.sysDescr  contains  Apple AirPort
```

Klassifizierer für Erkennung von IP-Adressen ändern

Wenn Sie eine Erkennung vom Typ „IP-Adresse“ ausführen, scannen Port-Probes Geräte ohne Anmeldeinformationen. Anschließend kann Discovery die zu verwendenden Klassifizierer bestimmen. Sie können Port-Probes und zusätzliche Klassifizierer für die Erkennung von IP-Adressen hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Obwohl für die Suche nach Windows - oder UNIX -Geräten mit dieser Art von Prüfung keine Anmeldeinformationen erforderlich sind, sind für SNMP-Geräte dennoch - Anmeldeinformationen erforderlich. Indem bestimmt wird, welche Ports auf den zu scannenden Geräten offen sind, kann die IP-Adressklassifizierung zum Beispiel den Gerätetyp (Computer, UPS usw.), das Betriebssystem, ausgeführte Anwendungen und Versionsnummern erkennen.

Hinweis: Die IP-Adressklassifizierung versucht, Geräte zu klassifizieren, wenn keine Anmeldeinformationen verfügbar sind. Discovery verwendet jedoch Anmeldeinformationen, wenn sie verfügbar sind, auch wenn die IP-Adressklassifizierung konfiguriert ist.

Führen Sie die folgenden Schritte aus, um die IP-Adressklassifizierung zu verwenden:

Prozedur

1. Ermitteln Sie, welche Ports für die Klassifizierung verwendet werden sollen, und führen Sie ein Scan-Programm wie *Nmap* für bestimmte IP-Adressen aus, um zu entscheiden, welche Ports die gewünschten Informationen über ein Gerät oder eine Anwendung offenbaren.

   Der Scan kann verschiedene Arten von Daten offenlegen, die für die Konfiguration von Klassifizierungsparametern hilfreich sind. Ein Nmap-Scan zeigt Portnummern, ihren Status (offen oder geschlossen), ihre Servicenamen und alle verfügbaren Versionsinformationen an. Anhand der im folgenden Beispiel zurückgegebenen Portinformationen können Kriterien für die Klassifizierung von UNIX-Servern (Port 22), MySQL (Port 3306) und Apache Tomcat (Port 16000) erstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Host is up (0.035s latency).
Not shown: 65521 closed ports
PORT      STATE    SERVICE     VERSION
22/tcp    open     ssh         OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey: 1024 d9:77:8b:68:1a:3a:b3:80:c3:a4:60:ba:61:7c:6f:65 (DSA)
|_2048 12:ed:36:6c:aa:dc:51:a0:ce:59:45:c9:c8:42:9b:85 (RSA)
80/tcp    open     http        Apache httpd 2.2.3 ((Red Hat))
|_html-title: Test Page for the Apache HTTP Server on Red Hat Enterprise Linux
111/tcp   open     rpcbind     2 (rpc #100000)
| rpcinfo:
| 100000  2    111/udp  rpcbind
| 100024  1    655/udp  status
| 100000  2    111/tcp  rpcbind
|_100024  1    658/tcp  status
443/tcp   open     ssl/http    Apache httpd 2.2.3 ((Red Hat))
|_html-title: Test Page for the Apache HTTP Server on Red Hat Enterprise Linux
658/tcp   open     status      1 (rpc #100024)
1720/tcp  filtered H.323/Q.931
2000/tcp  filtered cisco-sccp
3306/tcp  open     mysql       MySQL (unauthorized)
5060/tcp  filtered sip
10000/tcp open     http        Webmin httpd
|_html-title: Site doesn't have a title (text/html).
|_http-favicon: Unknown favicon MD5: 5B9D90CA66BB985FA0D070E0E02D93F4
16000/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
16001/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
16003/tcp open     http        Apache Tomcat/Coyote JSP engine 1.1
| robots.txt: has 1 disallowed entry
|_/
|_html-title: DBSymphony
```

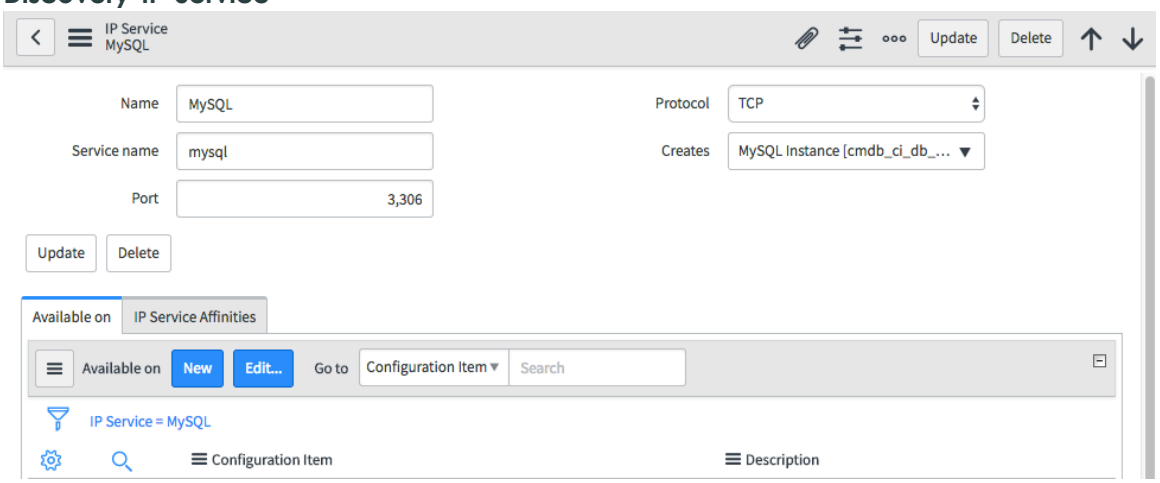
2. Fügen Sie einen IP-Service und eine Port-Probe hinzu.

Das sofort einsatzbereite System stellt Probes für einige der am häufigsten verwendeten Ports bereit, für eine effektive IP-Adressüberprüfung werden jedoch zusätzliche Port-Probes benötigt.

a. Navigieren zu **Discovery-Definition** > **IP-Services** und klicken Sie auf *Neu*.

b. Erstellen Sie einen neuen IP-Servicedatensatz mit der Portnummer und dem Service aus dem Nmap-Scan. In diesem Beispiel ordnen Sie den Service *mysql* zu Port 3306 zu und fügen das CI (*sanops02*), auf dem der Service ausgeführt wird, der zugehörigen Liste *Verfügbar am* hinzu.

Discovery-IP-Service



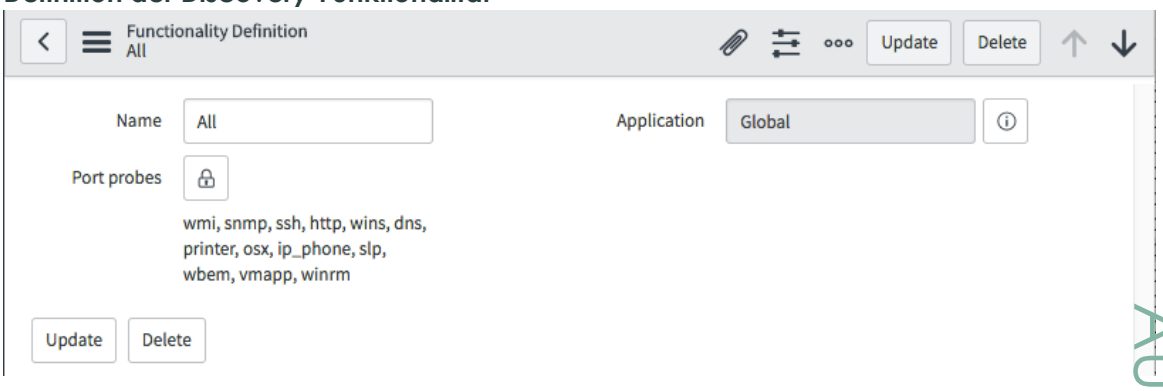
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Um Standard Discoveryzu verwenden, navigieren Sie zu **Discovery-Definition** > **Funktionalitätsdefinition** und wählen Sie den Datensatz für **Alle**aus.

d. Fügen Sie die neuen Port-Probes der Liste hinzu. Dadurch wird Discovery mitgeteilt, welche Port-Probes für IP-Adress-Scans ausgeführt werden sollen.

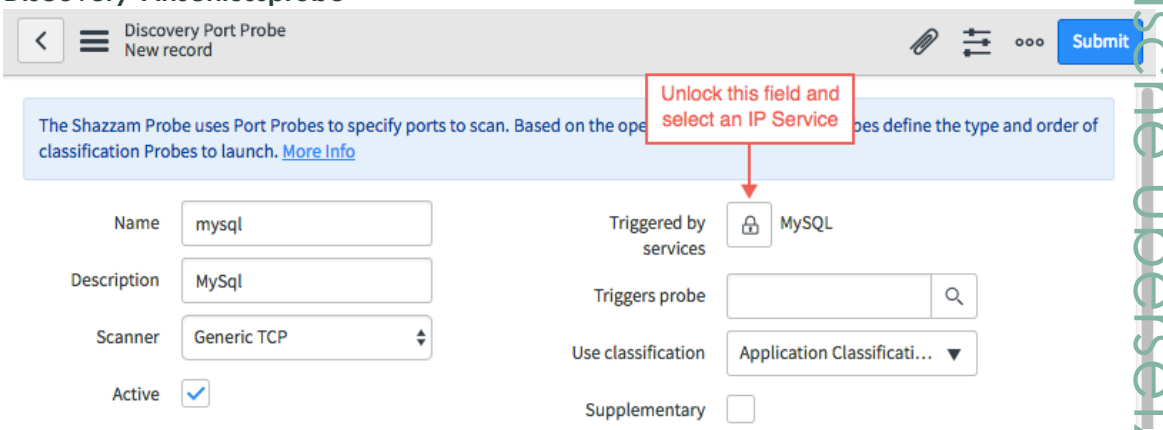
Definition der Discovery-Funktionalität



e. Speichern Sie den Datensatz, und navigieren Sie zu **Discovery-Definition** > **Anschlussprobes** und klicken Sie auf **Neu**.

f. Erstellen Sie eine Port-Probe mit dem soeben definierten neuen IP-Service.

Discovery-Anschlussprobe



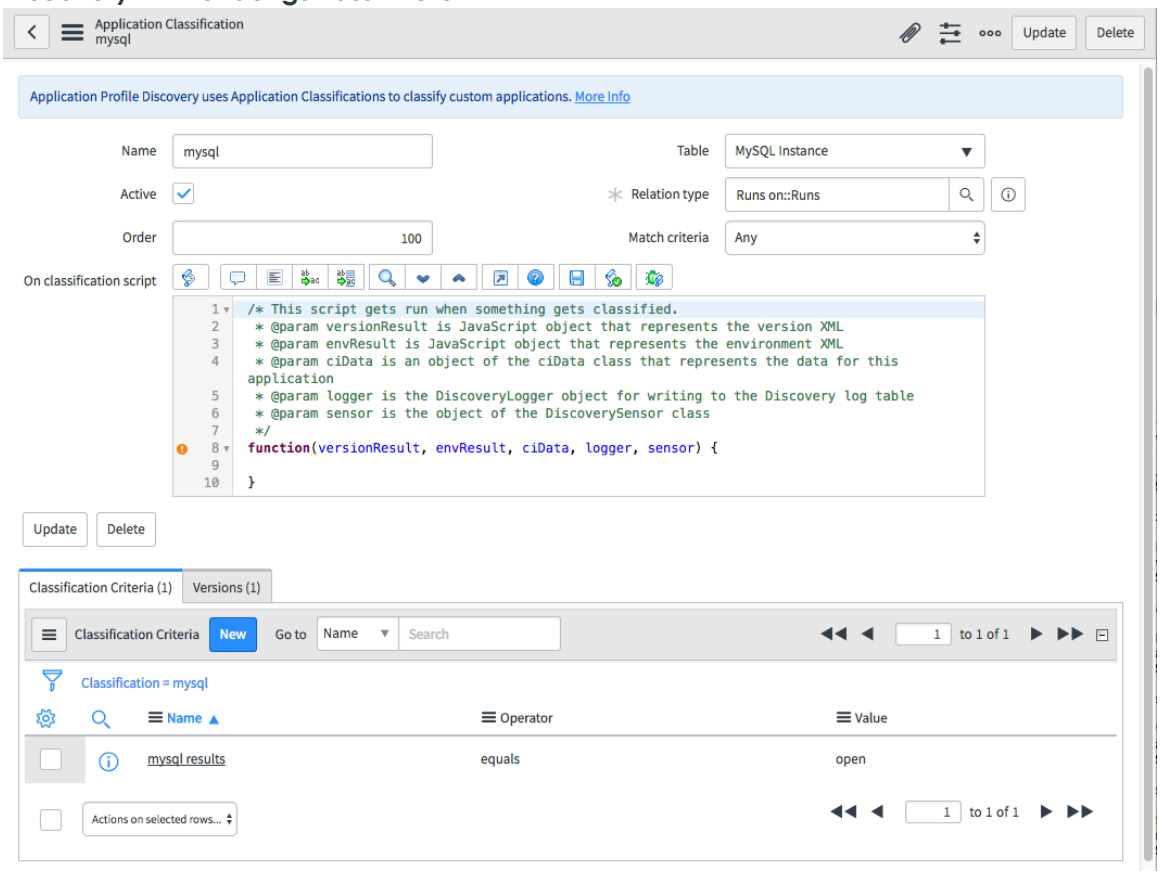
3. Erstellen Sie eine neue Klassifizierung, und fügen Sie den Parameter zum Scannen von IP-Adressen hinzu.

   In diesem Beispiel haben Sie einen Anwendungsklassifizierer erstellt, der Apache Tomcat anhand der Portinformationen erkennt, die durch den Nmap-Scan ermittelt wurden. Im folgenden Abschnitt finden Sie Details zum Bilden von Parametern für IP-Adress-Scans.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Anwendungsklassifizierer



4. Wahlweise: Erstellen Sie in der zugehörigen Liste „Klassifizierungskriterien“ einen Kriterienfilter, der bestimmt, wann dieser Klassifizierer auf die erkannten Geräte angewendet wird.
   Unter den Parametern zur IP-Adressklassifizierung finden Sie eine Liste der Parameter, die Sie verwenden können.

Nächste Maßnahme

Führen Sie eine Erkennung von IP-Adressen über den Erkennungszeitplan aus, um nach Geräten zu suchen.

Windows-Remoteverwaltung für Klassifizierung verwenden

Sie können die Erkennung von Windows-Hosts mit dem WinRM-Protokoll (Windows-Remoteverwaltung) konfigurieren.

Vorbereitungen

- Installieren und konfigurieren Sie im lokalen Netzwerk einen Windows-MID Server.
- Der Service WinRM muss auf allen zur Erkennung fähigen Windows-Hosts aktiviert sein.

Erforderliche Rollen: discovery_admin, agent_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig verwendet das System für die Geräteklassifizierung von Windows-Hosts das WMI-Protokoll. Um für eine effizientere, ressourcenschonendere Datenübertragung und Ausführung von Remotebefehlen zu sorgen, können Administratoren stattdessen das WinRM-Protokoll verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Aktivieren Sie den Service WinRM auf allen Windows-Hosts, die zur Erkennung vorgesehen sind.
2. Navigieren zu **Discovery** > **MID-Server**.
3. Wählen Sie den MID Server aus, den Sie für die Erkennung von Windows-Hosts verwenden möchten.
   Das System zeigt den MID Server-Datensatz an.
4. Klicken Sie in der zugehörigen Liste „Konfigurationsparameter“ auf **Neu**.
   Daraufhin wird der Datensatz eines MID Server-Konfigurationsparameters angezeigt.
5. Wählen Sie in der Auswahlliste des Felds **Parametername** den Parameter **mid.windows.management_protocol** aus.
6. Geben Sie den Wert **WinRM** ein.

MID Server-Konfigurationsparameter

7. Klicken Sie auf **Absenden**.
   Das System zeigt den MID Server-Datensatz an.
8. Wahlweise: Fügen Sie nach Bedarf weitere Protokollparameter der Windows-Remoteverwaltung hinzu.

Zusätzliche WinRM-Parameter

Parameter	Beschreibung	Standard	Erfordert einen Neustart des MID Servers
mid.powershell_api.winrm.remote_port	Gibt den Kommunikationsport an, den der MID Server für die Kommunikation mit dem WinRM-Protokoll verwendet	5985	Nein
mid.powershell_api.session_pool.max_size	Gibt die maximale Anzahl von Sitzungen an, die im Pool pro Zielhost zulässig sind.	2	Ja
mid.powershell_api.session_pool.max_size	Gibt die maximale Anzahl von Sitzungen an, die im Sitzungspool zulässig sind.	25	Ja
mid.powershell_api.idle_session_timeout	Gibt den Wert für den Timeout	60.0	Ja

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung	Standard	Erfordert einen Neustart des MID Servers
	von Powershell-Sitzungen im Leerlauf in Sekunden an.		

Nächste Maßnahme
Führen Sie eine Erkennung über den Erkennungszeitplan aus, um Windows-Computer in Ihrem Netzwerk zu finden.

Neuklassifizierung von Windows Workstation-Computers als Server

Standardmäßig klassifiziert Discovery Computer, die bestimmte Windows-Betriebssysteme verwenden, automatisch als Workstations. Möglicherweise möchten Sie jedoch bestimmte Computer in Ihrem Netzwerk, die als Server fungieren, nach ihrer Funktion und nicht nach dem Betriebssystem klassifizieren.

Vorbereitungen
Erforderliche Rolle: keine

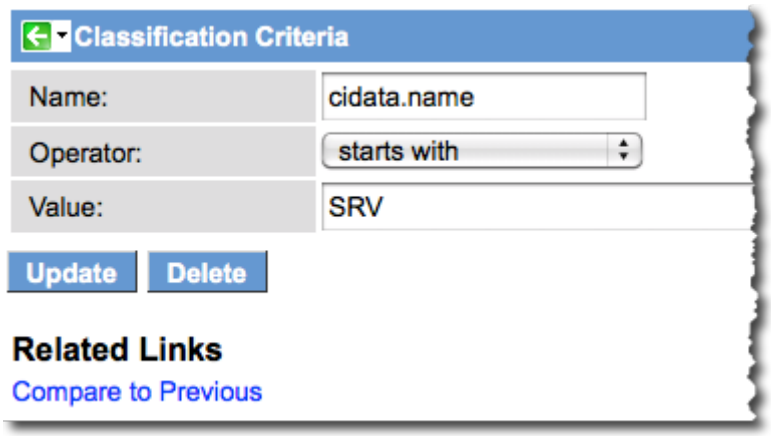
Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie die folgenden Variablen (mit **cidata** als Präfix), um eine Bedingung für die Neuklassifizierung zu erstellen. Um die Neuklassifizierung beispielsweise basierend auf der IP-Adresse eines Computers durchzuführen, verwenden Sie *`cidata.ip_address`*.

- Name
- dsn_domain
- os_domain
- ip_address
- serial_number

Das folgende Verfahren reklassifiziert alle Betriebssysteme von Windows-Workstations (Windows Vista, XP oder Windows 7), die als Server fungieren.

Prozedur
1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **Windows**.
2. Erstellen Sie einen neuen Klassifizierungsdatensatz, zum Beispiel: Windows XP Server.
3. Wählen Sie als Tabelle „Windows Server“ `[cmdb_ci_win_server]` aus.
4. yxcvbnm,ooiuztreq12345tKlicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern** aus dem Kontextmenü.
   Die zugehörigen Listen **Klassifizierungskriterien** und **Auslösertests** werden angezeigt.
5. Konfigurieren Sie die folgenden **Klassifizierungskriterien**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Name	Wählen Sie in der Liste oben eine Variable zur Verwendung als Klassifizierungskriterium aus. Geben Sie etwa für eine Neuklassifizierung eines Computers nach dem Namen `cidata.name` ein. Dies funktioniert unabhängig vom Betriebssystem für Server mit einer einheitlichen Benennungskonvention wie SRV001, SRV002 usw.
Operator	Wählen Sie einen Operator für die Klassifizierungsbedingung aus. In Netzwerken mit Servern, die gemäß einer bestimmten Konvention benannt sind, können Sie **Beginnt mit** oder **Enthält**auswählen.
Wert	Geben Sie den Wert für die Bedingung ein. In unserem Beispiel eines Netzwerks mit Servernamenskonvention würde dieser Wert dem Stamm dieser Konvention entsprechen, zum Beispiel **SRV**. Diese Bedingung klassifiziert alle Computer als Server, deren Computername SRVXXX lautet.

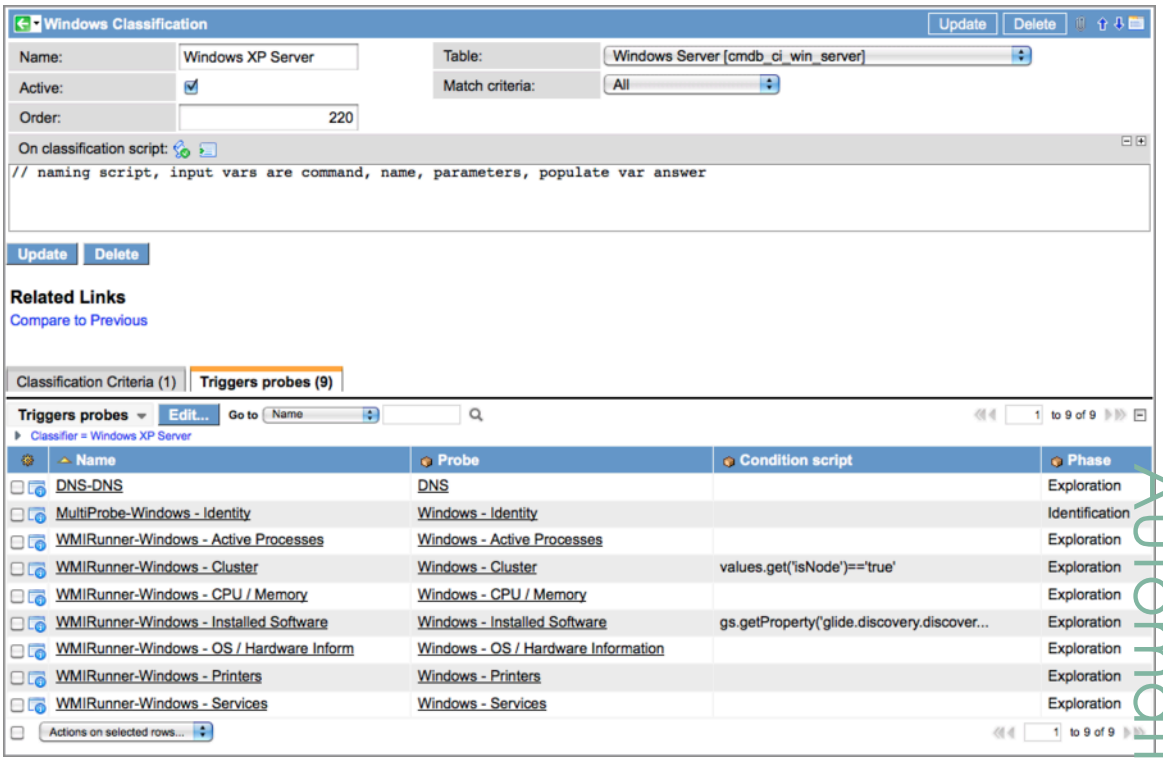
6. Wählen Sie die zugehörige Liste **Löst Probe aus** aus, und fügen Sie die entsprechenden Probes hinzu.

   a. Kopieren Sie die Liste der Probes aus einer anderen Windows-Serverklassifizierung, einschließlich der *Bedingungsskripts*.

   b. Stellen Sie sicher, dass die Probe **Windows - Identity** eine Phase vom Typ **Identifizierung** aufweist (Standardwert ist **Erkundung**).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das ausgefüllte Formular sieht wie folgt aus:



Nächste Maßnahme

Führen Sie eine Erkennung über den Erkennungszeitplan aus, um Windows-Computer in Ihrem Netzwerk zu erkennen, und prüfen Sie dann die Tabelle cmdb_ci_win_server und zugehörige Tabellen, um zu sehen, wie Daten in der CMDB gefüllt werden.

Parameter der Discovery-Klassifizierung

Die folgenden Parameter sind für Discovery-Klassifizierer verfügbar.

Hinweis: Bei Bedingungsfiltern in Prozessklassifizierungen wird die Groß- und Kleinschreibung beachtet.

Unix-Parameter

Die UNIX-Parameter definieren die Merkmale verschiedener Computertypen wie Linux, Solaris und HP-UX, die mit dem SSH-Protokoll (Version 2) kommunizieren.

Parameter	Beschreibung
Ausgabe	Die Rohausgabe der Klassifizierer-Probe (uname -a)
Typ	Gibt die Klassifizierung UNIX zurück
IP-Adresse	Gibt die IP-Adresse des erkannten Geräts zurück
Name	Der Name des Betriebssystems für dieses UNIX-CI. Beispiel: Linux oder HP-UX

Windows-Parameter

Windows-Parameter identifizieren Windows-Computer, die mit dem WMI-Protokoll kommunizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
isNode	Gibt an, ob die Instanz ein Knoten ist
Typ	Gibt die Klassifizierung *windows* zurück
isVIP	Gibt an, ob dieses CI eine virtuelle Maschine mit einer virtuellen IP-Adresse ist
ip_address	Gibt die IP-Adresse des erkannten Geräts zurück
Name	Name der Windows-Version
cidata.name	Hostname des Windows-Betriebssystems

SNMP-Parameter

SNMP-Parameter können die Eigenschaften verschiedener Gerätetypen wie Router, Switches und Drucker definieren.

Parameter	Beschreibung
powering	Der Wert *true* gibt an, dass das Gerät eine unterbrechungsfreie Stromversorgung (UPS) ist.
hosting	Der Wert *true* gibt an, dass das Gerät Programme hosten kann. Hosts sind Allzweckcomputer wie Server.
netware	Der Wert *true* gibt an, dass auf dem Gerät das Betriebssystem Netware ausgeführt wird.
Weiterleitung	Der Wert *true* gibt an, dass das Gerät über Weiterleitungsfunktionalität im Netzwerk verfügt.
ip_address	Gibt die IP-Adresse zurück, über die das jeweilige Gerät erkannt wurde. Ein Gerät kann über mehrere IP-Adressen verfügen.
sysdescr	Erforderliches beschreibendes Feld auf jedem beliebigen SNMP-Gerät, das nützliche Klassifizierungsdaten wie Betriebssystem und Version enthalten kann.
vlans	Der Wert *true* gibt an, dass das Gerät ein VLAN (Virtual Local Area Network) hosten kann.
hint_router	Der Wert *true* gibt an, dass Discovery ermittelt hat, dass das Gerät ein Router ist. Dieses Feld gilt nur für Geräte, die sowohl als Router als auch als Switch verwendet werden können.
block_router_exploration	Wenn dieser Parameter auf *true* gesetzt ist, startet Discovery keine Erkundungs-Probes für erkannte Router. Dieser Parameter wird nur für die Discovery im Netzwerk verwendet.
switching	Der Wert *true* gibt an, dass das Gerät über Netzwerk-Switching-Funktionalität verfügt.
mfr_apc	Der Wert *true* gibt an, dass das Gerät eine von American Power Conversion (APC) hergestellte unterbrechungsfreie Stromversorgung (UPS) ist.
printing	Der Wert *true* gibt an, dass das Gerät über Druckfunktionen verfügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
block_switch_exploration	Wenn dieser Parameter auf *true* gesetzt ist, startet Discovery keine Erkundungs-Probes für erkannte Switches. Dieser Parameter wird nur für die Discovery im Netzwerk verwendet.

Prozessparameter

Prozessparameter identifizieren Prozesse wie jene, die von LDAP, Apache-Servern und JBoss-Servern verwendet werden.

Parameter	Beschreibung
parameter	Die zur Ausführung des Prozesses verwendeten Parameter
command	Der zum Ausführen des Prozesses verwendete Befehl
Ausgabe	Die vollständige Ausgabe der aktuellen Zeile der Prozess-Probe
Typ	Gibt den Prozesstyp an (zum Beispiel *unix* oder *windows*).
PID	Die vom Betriebssystem eines Geräts generierte *Prozess-ID* zur Identifizierung eines laufenden Prozesses. Im Allgemeinen ist dieser Parameter kein praktisches Klassifizierungskriterium, da der Wert nicht statisch bleibt. Dies gilt jedoch nicht für Prozesse, die in einer Appliance ausgeführt werden, die nie neu gestartet wird.
Name	Name des erkannten Prozesses. In einigen Fällen ist dieser Parameter nicht zuverlässig, da mehrere Prozesse denselben Namen erhalten können. Unter Windows geben beispielsweise mehrere Prozesse für diesen Parameter *scvhost.exe* zurück.

IP-Service-Affinität für Discovery und Orchestration prüfen

Sie können in der Tabelle „IP-Services“ nach einer Liste von IP-Adressen suchen, die einem Protokoll zugeordnet sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die Tabelle „IP-Services“ ordnet einen Port einem Protokoll zu. Für häufig verwendete Port-Protokoll-Kombinationen werden standardmäßig Zuordnungen bereitgestellt, z. B. Port 80 für HTTP, Port 22 für SSH und Port 161 für SNMP.
Mithilfe der Systemeigenschaft `glide.discovery.ip_service_affinity` kann sich Discovery den letzten Port der erkannten IP-Adresse merken. Diese Eigenschaft ist standardmäßig auf **false** festgelegt.

Wichtig: Sie sollten IP-Services nur dann ändern, wenn Ihre Organisation benutzerdefinierte Ports verwendet.

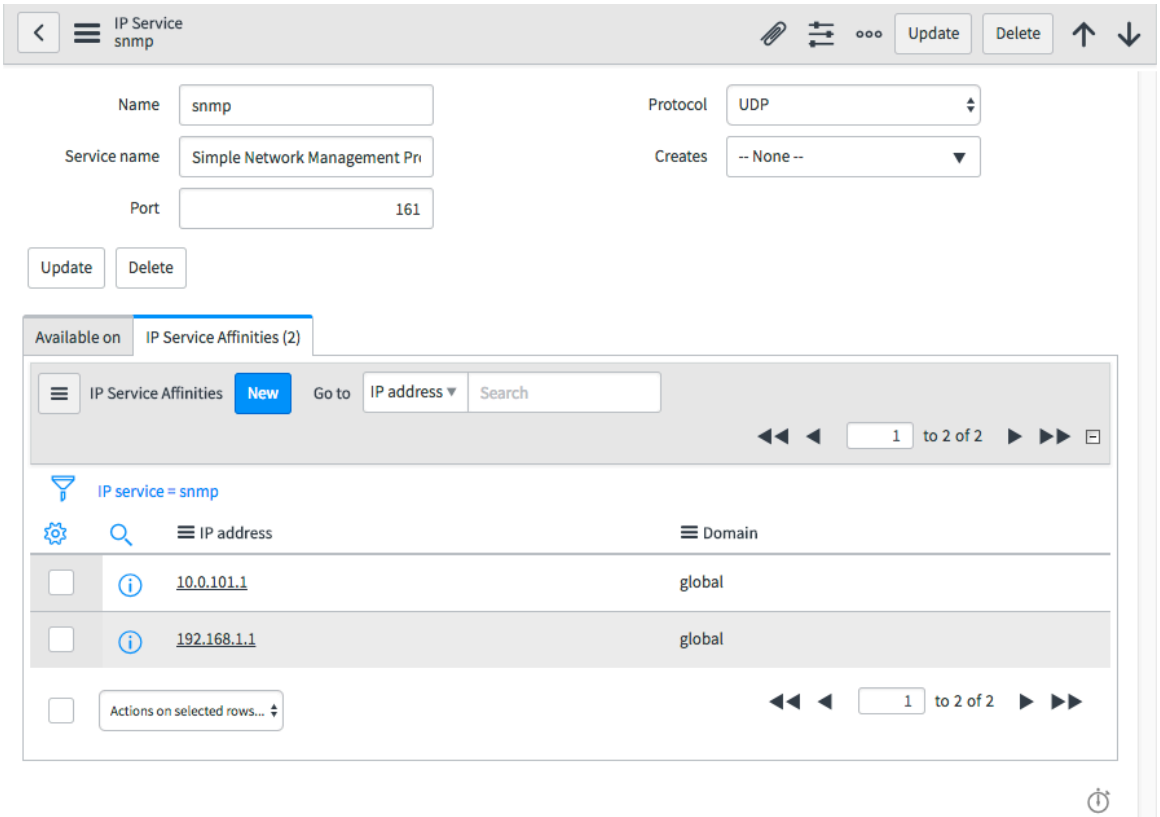
Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **IP-Services**.
2. Filtern Sie die Liste, um den entsprechenden IP-Service zu finden.
3. Klicken Sie auf den Namen des Service, um zu dieser IP-Serviceseite zu gelangen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Registerkarte **IP-Serviceaffinitäten**, um die Liste der IP-Adressen anzuzeigen, die diesem Service zugeordnet sind.

IP-Serviceaffinitäten



Discovery-Bezeichner

Nachdem Discovery ein CI klassifiziert hat, wird anhand von Bezeichnern bestimmt, ob das Gerät bereits in der CMDB vorhanden ist.

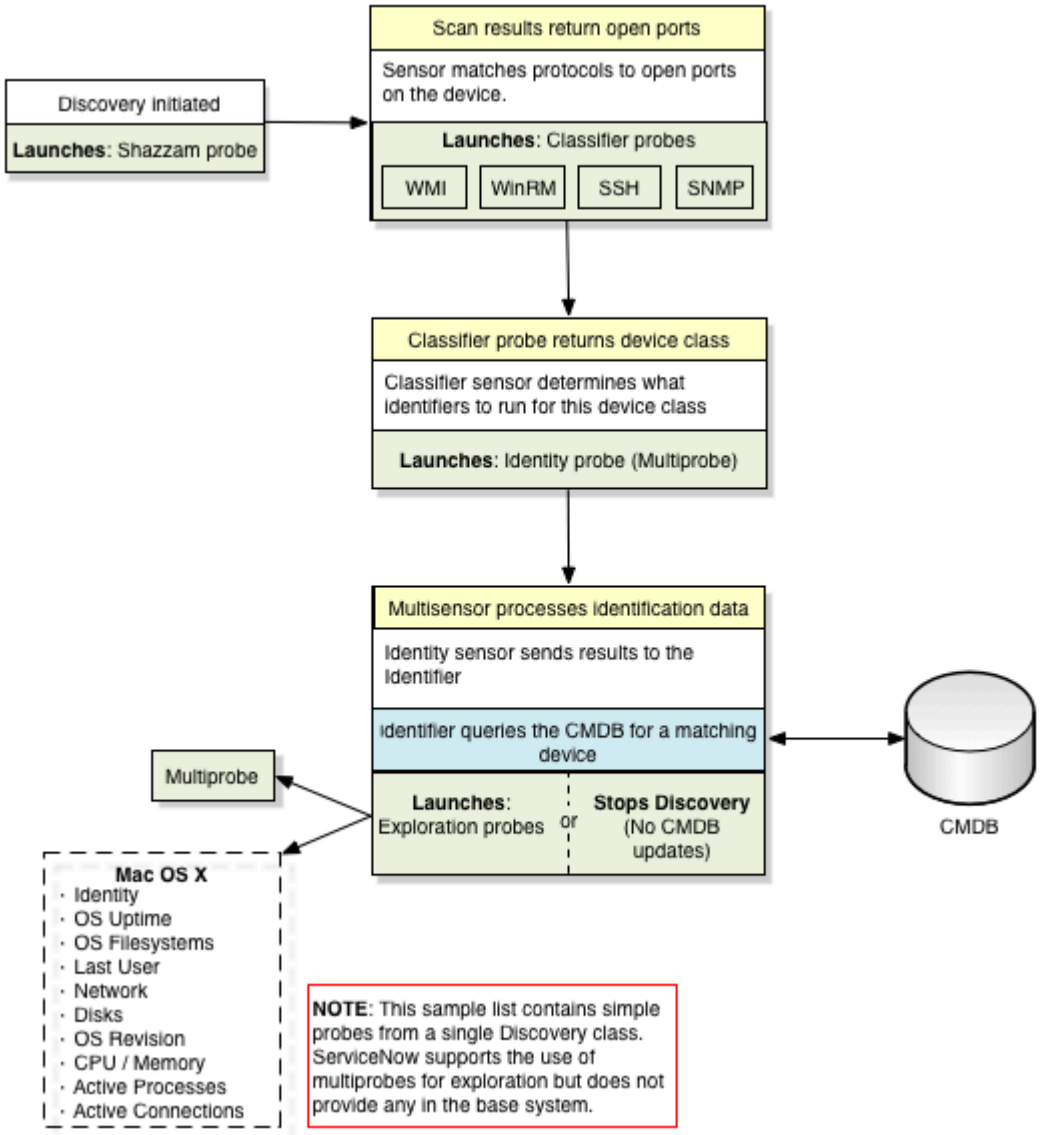
Discovery startet spezielle Identitäts-Probes, die Identifizierungsdaten für jedes Gerät sammeln und diese Daten in die Bezeichner einspeisen, die die Aktion bestimmen, die Discovery für das jeweilige Gerät ausführen muss. Bezeichner bestimmen genau die Identität des Geräts, um die Erstellung doppelter CIs zu verhindern. Dieser Identifizierungsschritt erfolgt nur für Erkennungen vom Typ „Konfigurationselement“, nicht für andere Erkennungstypen.

Die Identitäts-Probe im Discovery-Basissystem kann so konfiguriert werden, dass sie das Gerät auf Informationen wie Seriennummer, Name und Netzwerk-ID abfragt. Die Ergebnisse dieses Scans werden von einem Identitätssensor verarbeitet, der die Ergebnisse dann an den Bezeichner übergibt. Der Bezeichner versucht dann, ein passendes Gerät in der CMDB zu finden. Wenn der Bezeichner ein passendes CI findet, aktualisiert der Bezeichner das CI, oder es geschieht nichts. Wenn der Bezeichner kein passendes CI finden kann, wird entweder ein neues CI erstellt, oder es geschieht nichts. Wenn Discovery so konfiguriert ist, dass die Ausführung fortgesetzt wird, startet der Bezeichner die Erkundungs-Probes, die im Klassifizierungsdatensatz konfiguriert sind, um zusätzliche Informationen zum Gerät zusammenzutragen. Bei Erkundungs-Probes kann es sich um Multi-Probes oder einfache Probes handeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Seriennummern werden für eine genaue Asset-Nachverfolgung benötigt. Wenn Sie Baseline Probes, Sensoren oder Muster geändert haben, müssen Sie verifizieren, dass Seriennummern weiterhin erkannt werden. Darüber hinaus dürfen Sensoren oder Muster nicht so konfiguriert werden, dass die Syntax der Seriennummer geändert wird, z. B. durch Hinzufügen eines benutzerdefinierten Präfixes. Nicht dem Standard entsprechende Seriennummern können dazu führen, dass die Nachverfolgung von Assets ungenau ist.

Dieses Diagramm zeigt den Verarbeitungsablauf für die Klassifizierung und Überprüfung von Geräten mit konfigurierten Bezeichnern.



Tabellen für CMDB-Bezeichner

Tabelle	Beschreibung
Bezeichner [cmdb_identifier]	Speichert alle Regeln für Bezeichner
Bezeichner-Eintrag [cmdb_identifier]	Speichert alle Attribute für Bezeichner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regeln für Bezeichner

Das Discovery-Standardsystem enthält die folgenden Regeln für Bezeichner, die jeweils einem bestimmten CI-Typ (Feld **sys_class_name** im CI-Datensatz) oder der Tabelle im Feld **Betrifft** zugeordnet sind und die entsprechenden Attribute für die Erkennung von CIs aus der angegebenen Tabelle enthalten. Wo erforderlich, um alle möglichen Vorkommen eines Attributs zu erkennen, werden Tabellen aus zugehörigen Listen (**Tabelle durchsuchen**) in die Regel einbezogen. Weitere Informationen finden Sie unter Eine CI-Identifizierungsregel erstellen oder bearbeiten .

Regeln für CMDB-Bezeichner

Regel	Gilt für Tabelle/Attribute	Tabelle/Attribute durchsuchen
ESX-Serverregel	ESX-Server [cmdb_ci_esx_server]: correlation_id	keine
Hardwareregel	Hardware [cmdb_ci_hardware] • serial_number • serial_number_type • Name • ip_address • mac_address	• Seriennummer [cmdb_serial_number] ◦ serial_number ◦ serial_number_type • Netzwerkadapter [cmdb_ci_network_adapter] ◦ ip_address ◦ mac_address
Speicherserverregel	Speicherserver [cmdb_ci_storage_server] • cim_object_path • Name • serial_number • serial_number_type • mac_address • ip_address	• Seriennummer [cmdb_serial_number] ◦ serial_number ◦ serial_number_type • Netzwerkadapter [cmdb_ci_network_adapter] ◦ ip_address ◦ mac_address
WBEM-Serviceregel	WBEM-Service [cmdb_ci_wbem_service]: cim_object_path	keine

Abgleichstrategie für Hardwareregel

sys_class_name kann kein Attribut für unabhängige Regeln wie cmdb_ci_hardware sein. Wenn Ihre Discovery-Identifizierungsstrategie davon abhängig ist, dass ein CI mit einer bestimmten Klasse abgeglichen wird, müssen Sie für jede Klasse, die Sie für den Abgleich verwenden möchten, eine neue Regel erstellen und diese Klasse im Feld **Betrifft** des Bezeichnerformulars angeben.

Beispielsweise können Sie einen Bezeichner für einen Linux-Server mit anderen Attributen als der Hardwareregel erstellen. Möglicherweise möchten Sie den Computernamen, die IP-Adresse und die MAC-Adresse zur Identifizierung verwenden. Dies ist eine Lösung für

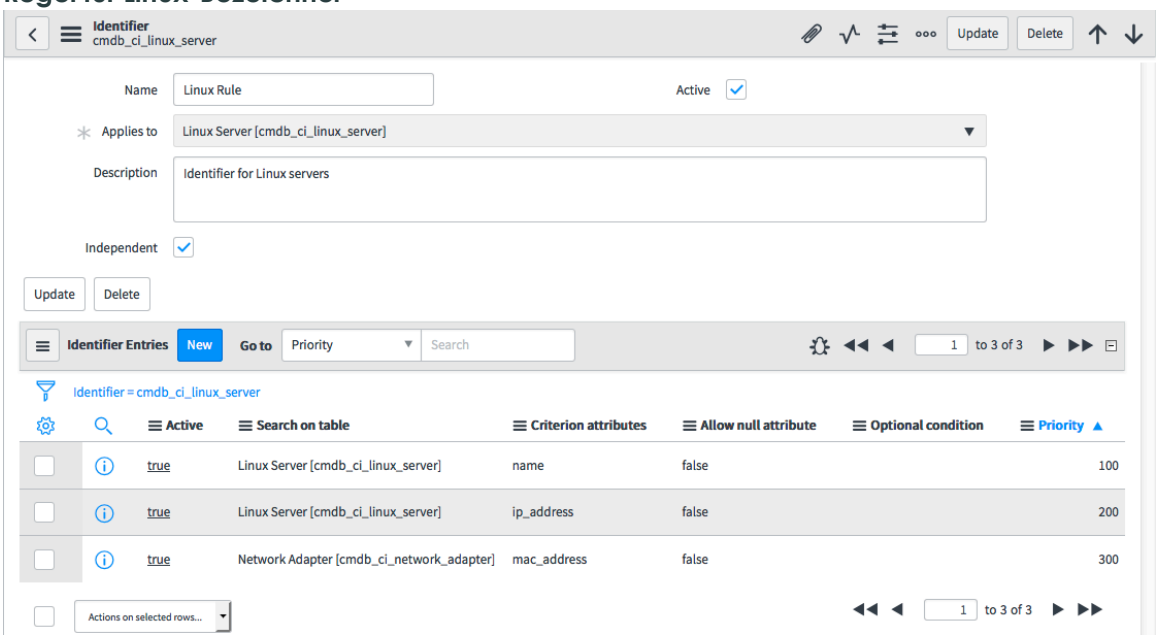
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerke, die NIC-Bonding oder -Teaming verwenden, um die verfügbare Bandbreite zu erhöhen. Verbundene Schnittstellen scheinen dasselbe physische Gerät zu sein und dieselben IP- und MAC-Adresse zu verwenden. Durch die Verwendung des Attributs **name** kann Discovery zwischen den einzelnen Schnittstellen im verbundenen Kanal unterscheiden.

Wichtig: Wenn Sie einen Bezeichner mit dem Attribut **name** erstellen, vermeiden Sie es, die Namen der Adapter zu ändern. Discovery kann vorhandene CIs für umbenannte Adapter nicht auflösen. Discovery kennzeichnet den Installationsstatus dieses CIs als „Abwesend“ und erstellt ein anderes CI.

Ihre neue Regel würde wie folgt aussehen:

Regel für Linux-Bezeichner

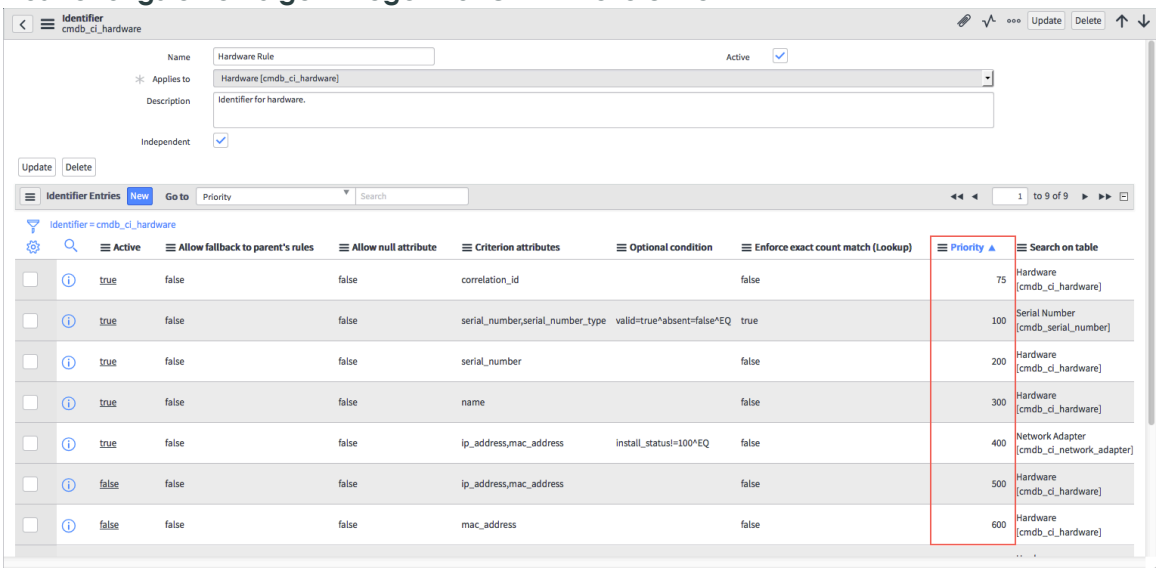


Auswertungsreihenfolge für Discovery-Bezeichner

Benutzerdefinierte Bezeichner müssen andere Werte für die *Reihenfolge* aufweisen als die der Standardbezeichner. Discovery analysiert Bezeichner und Attribute der Reihe nach von niedrigen Zahlen zu hohen. Sie können Bezeichner erstellen, die vor oder nach den Standardbezeichnern ausgeführt oder mit den Bezeichnern des Basissystems gemischt werden. Deaktivieren Sie das Kontrollkästchen **Aktiv**, um zu verhindern, dass der jeweilige Bezeichner bzw. die jeweilige Regel ausgeführt wird. Die Auswertungsreihenfolge für CMDB-Bezeichner ist in jeder Regel festgelegt und steuert nur die Analysereihenfolge der Attribute in der jeweiligen Regel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswertungsreihenfolge in Regeln für CMDB-Bezeichner



Eigenschaften zur Verarbeitung doppelter CIs

Mit den Eigenschaften, die mit „Identifizierung und Abgleich“ installiert werden, können Sie steuern, wie Discovery doppelte CIs verarbeitet. Verwenden Sie die Eigenschaften `glide.identification_engine.skip_duplicates` und `glide.identification_engine.skip_duplicates.threshold`. Weitere Informationen finden Sie unter Eigenschaften für Identifizierung und Abgleich .

Eigenschaften, die Bezeichnerversionen steuern

Alle Instanzen verwenden Kennungen aus dem CMDB Identification and Reconciliation Framework. Bei Upgrades von früheren Versionen als Geneva werden die veralteten Kennungen beibehalten. Sie können jedoch mithilfe einer Eigenschaft zu den neuen Kennungen wechseln: `glide.discovery.use_cmdb_identifiers`. Wenn Sie ein Upgrade von einer Version vor Geneva durchgeführt haben, müssen Sie diese Eigenschaft manuell hinzufügen und auf `true` setzen, um die neuen Kennungen zu verwenden. Wenn Sie ein Upgrade von Geneva oder späteren Versionen durchgeführt haben, ist diese Eigenschaft in der Tabelle Systemeigenschaften [sys_properties] verfügbar. Um die Funktionalität in benutzerdefinierten veralteten Kennungen zu erhalten, müssen Sie diese in das neue Format der CMDB-Bezeichnerregeln konvertieren, bevor Sie diese Eigenschaft aktivieren. Das System konfiguriert Ihre benutzerdefinierten Kennungen nicht automatisch erneut für das neue Framework.

Hinweis: Wenn die Service-Zuordnung aktiv ist, werden die neuen Kennungen aus dem „CMDB Identification and Reconciliation Framework“ unabhängig vom Eigenschaftswert verwendet.

Funktionsweise von Discovery-Bezeichnern

Wenn Discovery die Klasse eines Geräts bestimmt hat, wird eine Identitäts-Probe gestartet, die so konfiguriert ist, dass sie mindestens einen Befehl mit einer einzigen Authentifizierung ausführt.

Die Identitäts-Probe im Discovery-Basissystem kann so konfiguriert werden, dass sie das Gerät auf Informationen wie Seriennummer, Name und Netzwerk-ID abfragt. Die Ergebnisse dieses Scans werden von einem Identitätssensor verarbeitet, der die Ergebnisse dann an den Bezeichner übergibt. Der Bezeichner versucht dann, ein passendes Gerät in der CMDB zu finden. Wenn der Bezeichner ein passendes CI findet, aktualisiert der Bezeichner das CI, oder es geschieht nichts. Wenn der Bezeichner kein passendes CI finden kann, wird

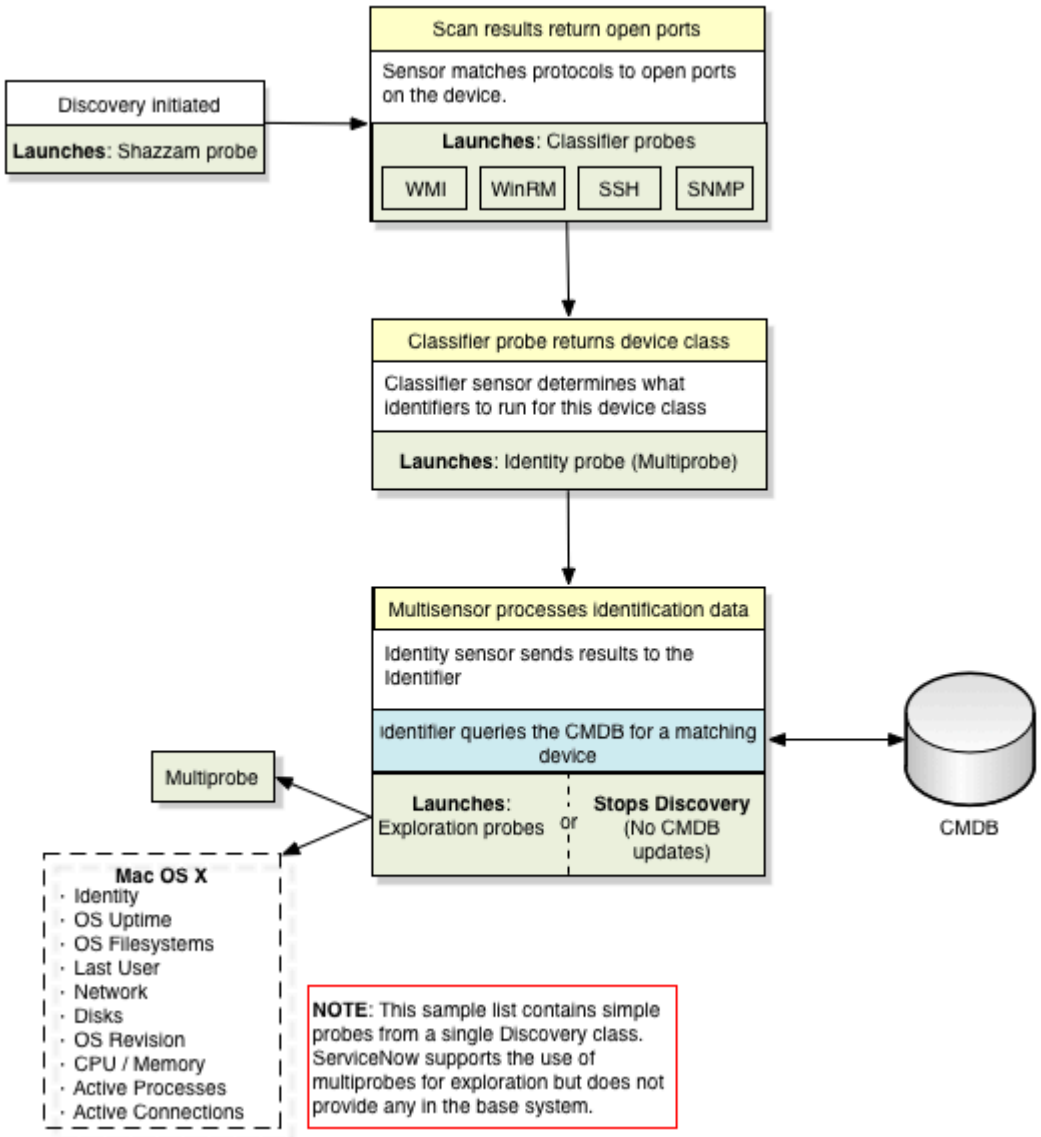
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

entweder ein neues CI erstellt, oder es geschieht nichts. Wenn Discovery so konfiguriert ist, dass die Ausführung fortgesetzt wird, startet der Bezeichner die Erkundungs-Probes, die im Klassifizierungsdatensatz konfiguriert sind, um zusätzliche Informationen zum Gerät zusammenzutragen. Bei Erkundungs-Probes kann es sich um Multi-Probes oder einfache Probes handeln.

Hinweis: Wenn Sie Muster für Discoveryverwenden, wird die Identitätsprobe nicht verwendet. Discovery verwendet die entsprechenden Bezeichnerregeln basierend auf dem CI-Typ, den Sie erkennen möchten, wie in den Mustervorgängen angegeben. Von den Vorgängen im Muster und diesen Bezeichner-Regeln werden die Identifizierungs- und Untersuchungsphasen der Erkennung durchgeführt.

Dieses Diagramm zeigt den Verarbeitungsablauf für die Klassifizierung und Überprüfung von Geräten mit konfigurierten Bezeichnern.

Discovery-Bezeichner



Identitäts-Probes in Discovery konfigurieren

Identitäts-Probes sind Multi-Probes, die mindestens eine einfache Probe enthalten und zum Extrahieren bestimmter Informationen von verwaltbaren Geräten konfiguriert sind. Sie können Ihre eigene Identitäts-Multi-Probe erstellen, um CIs zu identifizieren, die von Discovery noch nicht identifiziert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: discovery_admin, admin

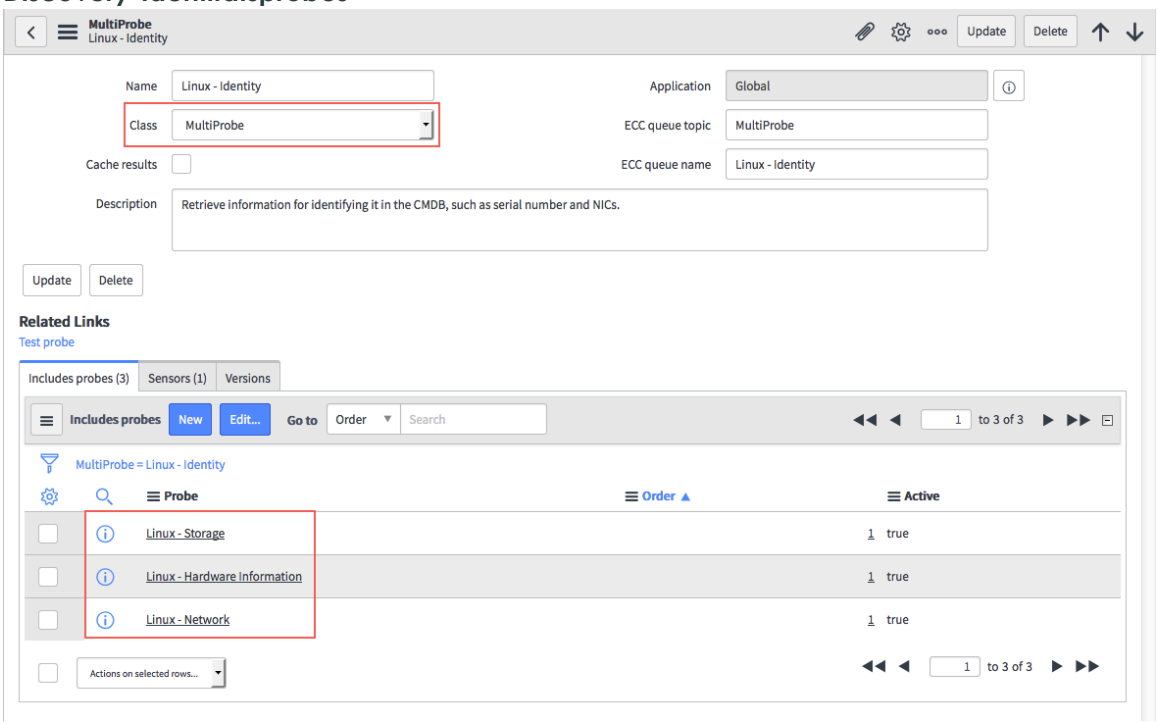
Warum und wann dieser Vorgang ausgeführt wird
Identitäts-Probes geben Informationen wie die Seriennummern von Geräten (es können mehrere pro Gerät vorhanden sein), den Computernamen und die Netzwerkidentifizierung (MAC-Adresse) zurück. Beispielsweise enthält die im System bereitgestellte Multi-Probe *Linux - Identity* zwei einfache SSH-Probes, die so konfiguriert sind, dass sie Hardware- und Netzwerkinformationen zum jeweiligen Gerät zurückgeben. Nachdem die Probe diese Informationen erkannt hat, übergibt sie die Daten an einen Multisensor, der für die Verarbeitung von Identitätsinformationen konfiguriert ist.

Hinweis: Eine Multi-Probe kann keinen weiteren Multi-Probe enthalten.

Prozedur
1. Navigieren zu **Alle** > **Discovery-Definition** > **Probes**.
2. Wählen Sie eine Probe in der Liste aus, dessen **Klasse** *Multi-Probe* lautet.
3. Stellen Sie sicher, dass der Umfang auf **Global** festgelegt ist.
4. Klicken Sie in der zugehörigen Liste **Enthält Probes** auf **Bearbeiten**, um einfache Probes auszuwählen, die in diese Multi-Probe aufgenommen werden sollen.
5. Klicken Sie auf **Neu**, um eine neue einfache Probe zu erstellen.

Example:

Discovery-Identitätsprobes



Nächste Maßnahme
Identitätssensoren in Discovery konfigurieren, die Teil der Identitäts-Probes sind.

Identitätssensoren in Discovery konfigurieren

Wenn Sie eine Identitäts-Multi-Probe anpassen, können Sie auch einen Multisensor dafür konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: discovery_admin, admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Multisensoren übergeben die von den Identitäts-Probes zurückgegebenen Daten an die Discovery-Bezeichner. Die Bezeichner durchsuchen dann die CMDB nach übereinstimmenden CIs. Wenn die Identität eines Geräts aufgelöst wird, übergeben die Bezeichner den Ergebnisstatus für das Gerät an die Multisensoren, die entsprechend reagieren, indem sie entweder Erkundungs-Probes starten oder Discovery für dieses Gerät stoppen.

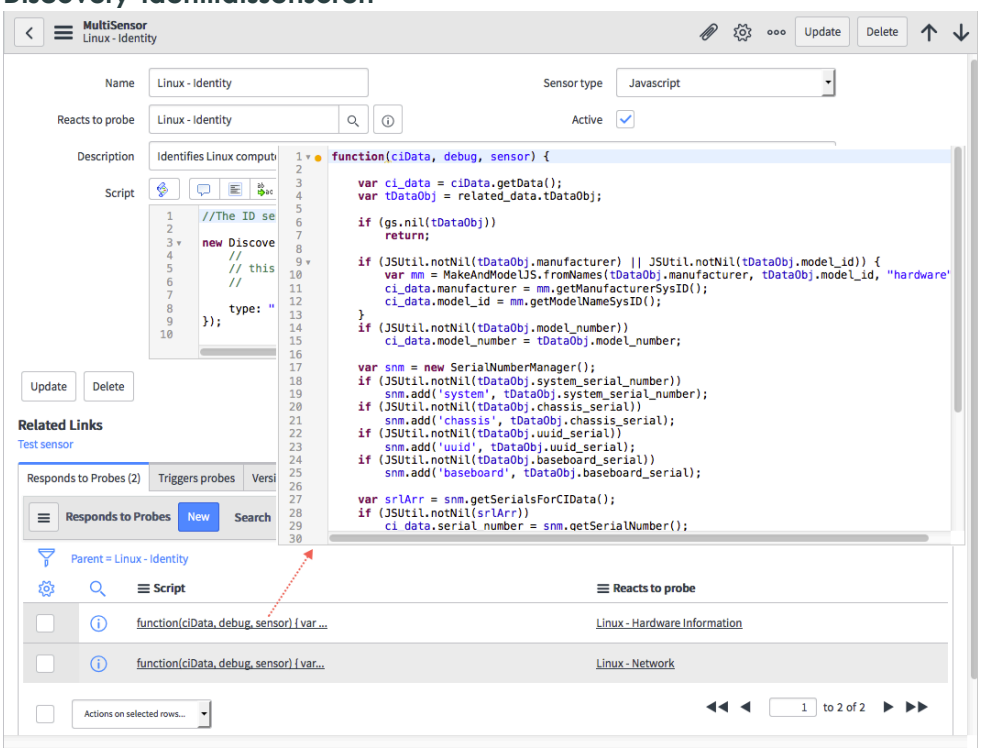
Prozedur
1. Navigieren zu **Alle** > **Discovery-Definition** > **Sensoren**.
2. Wählen Sie vorhandene Identitäts-Multisensoren in der Liste aus.

   Hinweis: Zur Vermeidung von Verwechslungen müssen die in der Instanz bereitgestellten Multisensoren dieselben Namen wie die entsprechenden Multi-Probes aufweisen.

   Die zugehörige Liste **Reagiert auf Probes** enthält die einfachen Probes, die Daten an diese Multisensoren übergeben. Das sind dieselben einfachen Probes, die in der Liste „Enthält Probes“ im entsprechenden Multi-Probe-Datensatz angezeigt werden.
3. Klicken Sie für jede Probe in der Liste auf den Link **Skript**, um das Skript anzuzeigen, das von den Multisensoren zur Verarbeitung der Daten von der Probe ausgeführt wird.

Example:

Discovery-Identitätssensoren



Nächste Maßnahme
Führen Sie eine Erkennung über den Erkennungszeitplan aus, um nach CIs zu suchen und sicherzustellen, dass sie in der CMDB korrekt identifiziert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seriennummertypen zur Identifizierung

Wenn Discovery CIs findet, werden deren Seriennummern in der Tabelle „Seriennummer“ [cmdb_serial_number] aufgelistet, damit sie leicht zu identifizieren sind. Seriennummertypen variieren je nach CI, wie in den folgenden Beispielen beschrieben.

Wichtig: Seriennummern werden für eine genaue Asset-Nachverfolgung benötigt. Wenn Sie Baseline Probes, Sensoren oder Muster geändert haben, müssen Sie verifizieren, dass Seriennummern weiterhin erkannt werden. Darüber hinaus dürfen Sensoren oder Muster nicht so konfiguriert werden, dass die Syntax der Seriennummer geändert wird, z. B. durch Hinzufügen eines benutzerdefinierten Präfixes. Nicht dem Standard entsprechende Seriennummern können dazu führen, dass die Nachverfolgung von Assets ungenau ist.

Linux

Im Ergebnis von dmidecode | cat entspricht der Wert auf der linken Seite dem, wonach Discovery sucht. Der Wert auf der rechten Seite gibt an, wie die Nummer in der Tabelle „Seriennummer“ [cmdb_serial_number] gespeichert wird.

```
Serial Number : system_serial_number

UUID : uuid_serial

Serial Number : baseboard_serial

Serial Number : chassis_serial
```

Windows

Für Win32-WMI-Klassen entspricht der Wert auf der linken Seite dem Namen, unter dem die Nummer in der Tabelle „Seriennummer“ [cmdb_serial_number] gespeichert wird. Der Wert auf der rechten Seite entspricht dem WMI-Wert.

```
('system' : Win32_ComputerSystemProduct.IdentifyingNumber);

('uuid' : Win32_ComputerSystemProduct.UUID);

('chassis' : Win32_SystemEnclosure.SerialNumber);

('bios' : Win32_BIOS.SerialNumber);

('baseboard' : Win32_BaseBoard.SerialNumber);
```

SNMP

Für SNMP basiert die folgende Zuordnung auf dem Code. Die physischen Typen der Seriennummern stammen aus allen Instanzen von iso.org.dod.internet.mgmt.mib-2.entityMIB.

```
'cisco_stack' :
 'iso.org.dod.internet.private.enterprises.cisco.workgroup.ciscoStackMIB.
chassisGrp.chassisSerialNumberString'

'cisco_chassis' :
 'iso.org.dod.internet.private.enterprises.cisco.temporary.chassis.chassi
sId'
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
'foundry' :
 'iso.org.dod.internet.private.enterprises.foundry.products.switch.snChas
sis.snChasGen.snChasSerNum'

'apc_pdu' :
 'iso.org.dod.internet.private.enterprises.apc.products.hardware.masterSw
itch.sPDUIdent.sPDUIdentSerialNumber'

'printer' :
 'iso.org.dod.internet.mgmt.mib-2.printmib.prtGeneral.prtGeneralEntry'

'standard' :
 'iso.org.dod.internet.private.enterprises.apc.products.hardware.ups.upsI
dent.upsAdvIdent.upsAdvIdentSerialNumber'
```

Discovery-Status

Der Discovery-Status bietet eine Zusammenfassung einer Erkennung, die über einen Zeitplan gestartet wurde. Sie können eine Erkennung, die gerade ausgeführt wird, auch über das Statusformular abbrechen.

Hinweis: Discovery-Zeitpläne, die über eine definierte Anzahl von Minuten keine Statusaktualisierungen aufweisen, werden automatisch vom Auftrag „Discovery-Statusüberwachung“ analysiert. Standardmäßig gilt dieser Auftrag für Discovery-Zeitpläne, die Konfigurationselemente erkennen. Weitere Informationen finden Sie im Artikel zum Discovery-Statusüberwachungsauftrag in der Now Support Knowledge Base.

Um auf das Formular „Discovery-Status“ zuzugreifen, navigieren Sie zu **Discovery** > **Status** und öffnen Sie den Statusdatensatz für eine Discovery.

Jeder Datensatz in der Statusliste stellt die Ausführung einer Erkennung nach einem Zeitplan dar und zeigt allgemeine Informationen wie das Datum der Erkennung, den Modus, die Anzahl der an Geräte gesendeten Probe-Nachrichten und die Anzahl der verarbeiteten Sensordatensätze an. Ein Statusdatensatz enthält Daten, die Ihnen bei der Fehlerbehebung bei einer fehlgeschlagenen Erkennung helfen können. Verwenden Sie diese Daten, um Fehler im Verhalten einzelner Probes und Sensoren zu beheben oder diese Elemente sogar separat auszuführen. Verwenden Sie die Statussteuerungen, um in Probe-/Sensor-Threads für eine bestimmte Erkennung an beliebiger Stelle einzutreten, und folgen Sie dann dem Prozess in beide Richtungen. Sie können auch leicht erkennen, welche Klassifizierungs-Probe ausgeführt wurde und ein bestimmtes Gerät erkannt hat, indem Sie die Spalte der Klassifizierungs-Probe in der Geräteliste anzeigen.

- **Aktualisieren**: Aktualisiert die zugehörigen Registerkarten, einschließlich **Discovery-Protokoll** und **ECC-Warteschlange** für noch laufende Erkennungsvorgänge.
- **Discovery-Zeitleiste**: Die Discovery-Zeitleiste ist eine grafische Anzeige einer Erkennung, die Informationen zu allen verwendeten Probes und Sensoren enthält.
- **Discovery log entries (Discovery-Protokolleinträge)**: Das Discovery-Protokoll zeigt Informationen wie Klassifizierungsfehler, CMDB-Updates und Authentifizierungsfehler an. Ein Discovery-Protokolldatensatz wird für jede Aktion erstellt, die einem Erkennungsstatus zugeordnet ist.

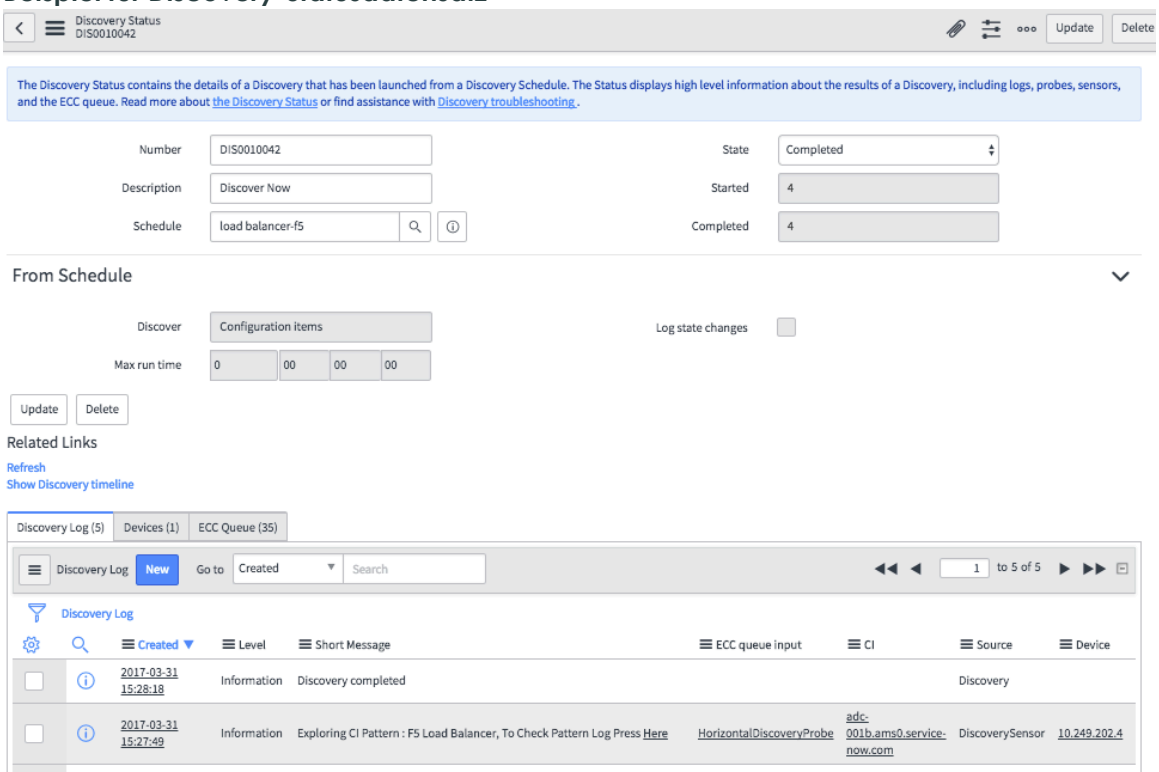
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **ECC queue entries (ECC-Warteschlangeneinträge)**: Einträge in der ECC-Warteschlange stellen einen zusammenhängenden Flow der Aktivitäten von Probes und Sensoren sowie die tatsächliche XML-Nutzlast bereit, die an eine oder von einer Instanz gesendet wird.
- **Device history (Geräteverlauf)**: Der Geräteverlauf bietet eine Zusammenfassung aller während der Erkennung gescannten Geräte und der Aktionen, die Sensoren in der CMDB ausgeführt haben.

Hinweis: Standardmäßig werden Discovery-Datensätze in der Statusliste nur jeweils über einen Zeitraum von 30 Tagen angezeigt.

Der folgende Discovery-Statusdatensatz zeigt die Erkennung eines Lastenausgleichsmoduls mithilfe eines Musters.

Beispiel für Discovery-Statusdatensatz



Feld	Beschreibung
Nummer	Eine automatisch generierte Nummer für den Datensatz
Beschreibung	Art dieser Discovery-Ausführung. Normalerweise lautet die Beschreibung *Geplant*. Wenn Sie Discovery jedoch manuell über einen Zeitplan ausgeführt haben, wird im Feld *Beschreibung* für den Datensatz *Discovery starten* angezeigt.
Zeitplan	Name des Erkennungszeitplans
Status	Status der Erkennung: • **Wird gestartet** • **Aktiv**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• **Abgeschlossen** • **Abgebrochen**
„Gestartet“ und „Abgeschlossen“	Die Anzahl der während der Erkennung gestarteten und abgeschlossenen Probes
Quelle	Optionales schreibgeschütztes Feld, das die Quelle der Erkennung anzeigt, zum Beispiel **Discovery planen** oder **Schnell-Discovery**. Wenn die Quelle der Discovery ein API-Aufruf war, lautet die Quelle **DiscoveryAPI**.
Über Zeitplan (schreibgeschützte Zeitplandaten)	
Erkennen	Zeigt den Discovery-Typ an. Mögliche Typen: **Konfigurationselemente**, **IP-Adressen**, **Netzwerke**oder **Prozesse/Verbindungen** (ADM).
Maximale Laufzeit	Zeigt die maximale Dauer der Ausführung von Discovery nach diesem Zeitplan an
Statusänderungen protokollieren	Gibt an, dass Statusänderungen während dieser Discovery protokolliert wurden. Diese Status werden in den Feldern *Letzter* und *Aktuell* in der Liste **Discovery Devices** (Erkennungsgeräte) in diesem Formular angezeigt.

Zugehörige Informationen

Horizontale Erkennung planen

Erkennung über Discovery-Status abbrechen

Sie können eine Erkennung manuell über den Discovery-Statusdatensatz abbrechen, während sie ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Status**.
2. Klicken Sie auf eine **Nummer**, um den Statusdatensatz zu öffnen.
3. Klicken Sie auf **Discovery abbrechen** unter **Zugehörige Links**.
   Discovery abbrechen ist nur für aktive Erkennungen verfügbar.

Ergebnisse

Wenn ein Discovery-Status abgebrochen wird, werden alle zugehörigen Sensortransaktionen sofort beendet und alle geplanten Sensoraufträge aus dem System gelöscht.
Nach dem Abbruch wird für den Bereinigungsstatus die **Abgeschlossene Anzahl** angezeigt, und der Abbruch wird im Discovery-Protokoll protokolliert. In der Tabelle „Warteschlange“ [ecc_queue] werden alle Datensätze auf den Status **Fehler** gesetzt, die zu Sensoren gehören, die die Transaktionsmengenregel überschreiten.

Discovery-Zeitleisten

Eine Discovery-Zeitleiste generiert die grafische Anzeige eines Discovery-Statusdatensatzes, einschließlich Informationen zu allen für die Erkennung verwendeten Probes und Sensoren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie Discovery-Zeitachsen, um Folgendes anzuzeigen:

- Den Flow von Probes und Sensoren, einschließlich derer, die mit Mustern im Rahmen einer Erkennung verwendet werden
- Die Dauer der einzelnen Probes und Sensoren, die während einer Erkennung ausgeführt wurden, und der Zeitanteil, der in der Warteschlange verbracht wurde und für die Verarbeitung erforderlich war
- Tooltips mit zusätzlichen Daten zu einer Probe und einem Sensor
- Datensätze aus der ECC-Warteschlange

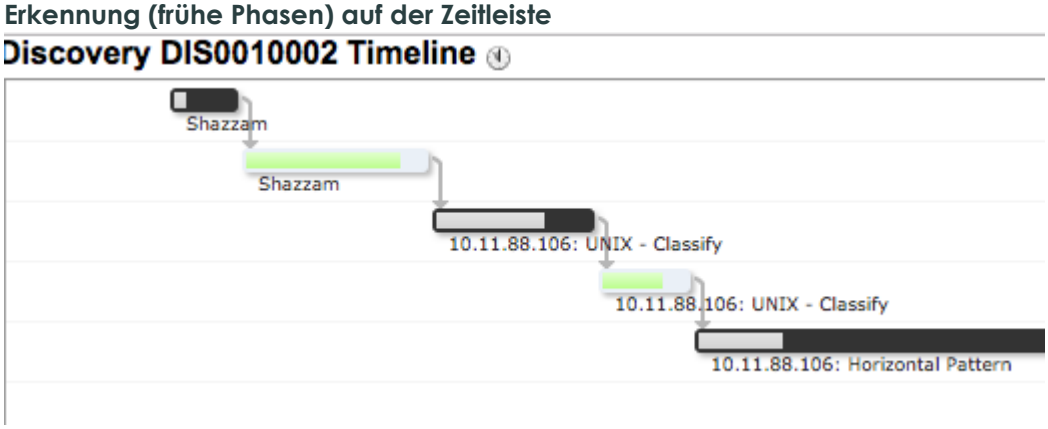
Größe der Erkennungen in der Zeitleiste

Zeigen Sie Zeitleisten für eine gesamte Erkennung oder für einzelne Geräte in einer Erkennung an. Im vorkonfigurierten System beträgt die maximale Größe der Erkennung, die in einer Zeitleiste angezeigt werden kann, 300 Einträge in der ECC-Warteschlange (150 Probes und 150 Sensoren). Um größere Erkennungen anzuzeigen, ändern Sie die Standardeinstellung der Eigenschaft *glide.discovery.timeline.max.entries*.

Beispiel: Discovery-Zeitachsen

Dieses Beispiel zeigt die Discovery-Zeitleiste für die ersten beiden Phasen der Erkennung (Port-Scan und Klassifizierung):

Erkennung (frühe Phasen) auf der Zeitleiste



In diesem Beispiel werden die Shazzam-Probe und der Sensor ausgeführt, gefolgt von der Klassifizierer-Probe „Unix“ und dem Sensor. Der Klassifizierer ruft die Probe „Horizontal Pattern“ auf, die ein bestimmtes Muster ausführt.

Discovery-Zeitleiste anzeigen

Eine Discovery-Zeitleiste generiert die grafische Anzeige eines Discovery-Statusdatensatzes, einschließlich Informationen zu jeder ausgeführten Probe, jedem Sensor und jedem Muster.

Vorbereitungen

Erforderliche Rolle: admin, discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

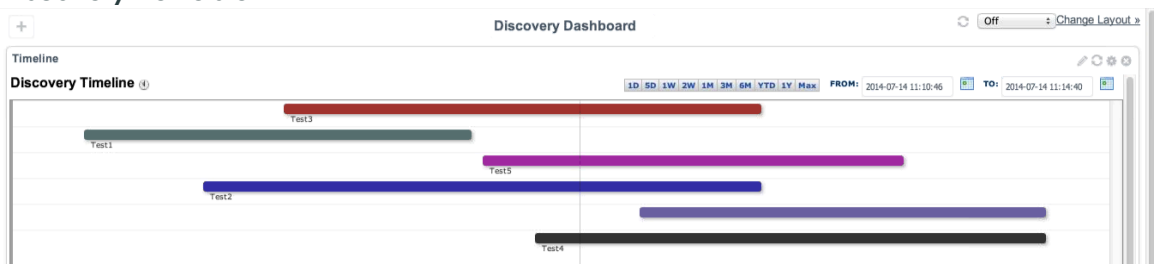
1. Navigieren zu **Alle** > **Discovery** > **Status**.
2. Wählen Sie in der Datensatzliste eine Discovery aus.
3. Klicken Sie auf den zugehörigen Link **Discovery-Zeitleiste anzeigen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Löschen Sie die Warnung, und wählen Sie dann die zugehörige Liste **Geräte** aus.
5. Klicken Sie auf die IP-Adresse eines Geräts.
6. Klicken Sie im Gerätedatensatz auf den zugehörigen Link **Discovery-Zeitleiste anzeigen**.

   Die Discovery-Zeitleiste für dieses Gerät wird angezeigt.

Discovery-Zeitleiste



7. Verwenden Sie den rosa Schieberegler am unteren Rand der Zeitleiste, um die Perspektive zu ändern.

   a. Bewegen Sie den Schieberegler von rechts nach links, um alle Aufgaben auf einer langen Zeitleiste anzuzeigen.

   b. Passen Sie die Endpunkte des Schiebereglers an, um die Vergrößerung zu ändern. Ein schmaler Schieberegler zoomt näher an die Zeitspannen heran und bietet eine detailliertere Ansicht komplexer Zeitleisten. Ein breiter Schieberegler vergrößert die Ansicht und macht einen größeren Teil der Zeitleiste auf dem Bildschirm sichtbar.

8. Verwenden Sie den Auswahlbereich oben im Bildschirm, um den sichtbaren Zeitrahmen anzupassen.
9. Klicken Sie auf **Max.**, um die Zeitleiste auf die Länge der Discovery zu beschränken.

   Die Zeitskala wird automatisch auf die Länge der Discovery angepasst. Der verfügbare Zeitskalenbereich reicht von einem Tag bis zu einem Jahr.

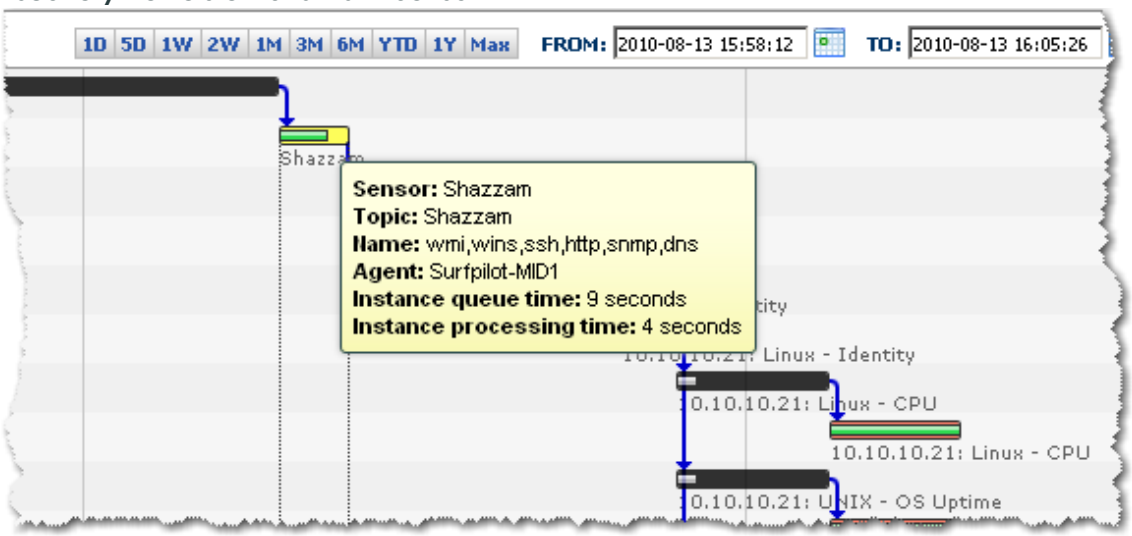
   Tooltips

   Discovery -Zeitleisten zeigen Leistungsdaten zu Probes und Sensoren sowie CI-Informationen in Tooltips an. Bewegen Sie den Mauszeiger über eine Zeitspanne, um die zugehörigen Daten anzuzeigen. Probes werden als schwarze Zeitrahmen angezeigt. Die Warteschlangenzeit einer Probe wird als silberner Balken innerhalb der Spanne angezeigt, und die Verarbeitungszeit wird durch den verbleibenden Platz dargestellt. Sensorzeitspannen werden rot und die Warteschlangenzeit als grüner Balken angezeigt. Ausgewählte Zeitspannen beliebiger Art werden gelb angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

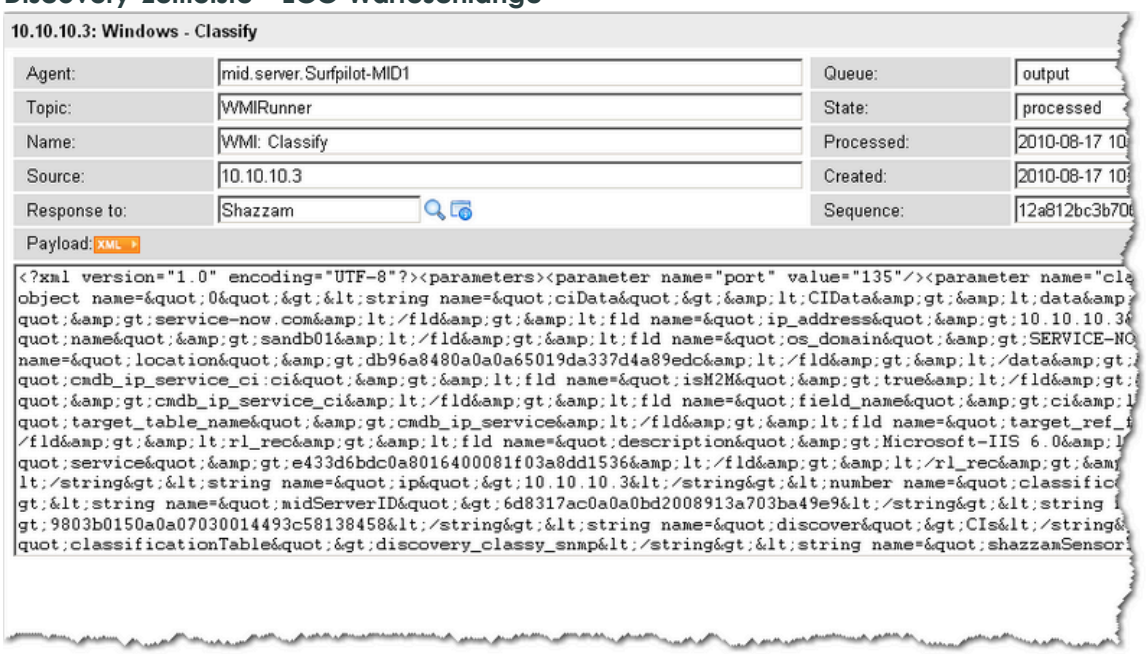
Discovery-Zeitleiste – Shazzam-Sensor



ECC-Warteschlange

Doppelklicken Sie auf eine Zeitspanne, um den Datensatz der ECC-Warteschlange für diese Probe oder diesen Sensor zu öffnen.

Discovery-Zeitleiste – ECC-Warteschlange



ECC-Warteschlange für Discovery

Die ECC-Warteschlange (External Communication Channel) ist ein Verbindungspunkt zwischen einer Instanz und anderen integrierten Systemen – in den meisten Fällen MID Server.

Inhalte der ECC-Warteschlange

Die ECC-Warteschlange enthält Datensätze, die während aller Phasen der Erkennung erstellt werden. Jeder Datensatz ist im Wesentlichen eine Nachricht von der Instanz und einem anderen System, die als **Ausgabe** klassifiziert ist, oder eine Nachricht von einem aus Sicht der Instanz externen System, die als **Eingabe** klassifiziert ist. ECC-Warteschlangendatensätze

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

stellen einen zusammenhängenden Flow der Aktivitäten von Probes und Sensoren sowie die tatsächliche XML-Nutzlast bereit, die an eine oder von einer Instanz gesendet wird.

Datensätze der ECC-Warteschlange automatisch löschen

Wenn Discovery in einer Instanz ausgeführt wird, kann die Größe dieser Tabelle mehrere Gigabyte betragen. Die meisten der erfassten Daten sind unnötig, einige Einträge können jedoch für die Behebung von Problemen mit Discovery wichtig sein. Beispiel: Wenn Discovery die Laufwerke auf einem bestimmten Windows-Server nicht ordnungsgemäß erfasst, suchen Sie in der ECC-Warteschlange nach den Daten, die von der Probe „Windows - System Information“ zurückgegeben werden. Sie sollten ECC-Warteschlangendaten von Discovery mindestens einen Monat lang aufbewahren.

Standardmäßig werden Datensätze in der ECC-Warteschlange automatisch gelöscht, die älter als 7 Tage sind. Sie können den Löschzeitplan festlegen, indem Sie den Tabellenrotationsplan für die ECC-Warteschlange aktualisieren. Die Namen für die Tabellenrotation lauten wie folgt:

- *ecc_queue_event*
- *ecc_queue*

Auf ECC-Warteschlange zugreifen

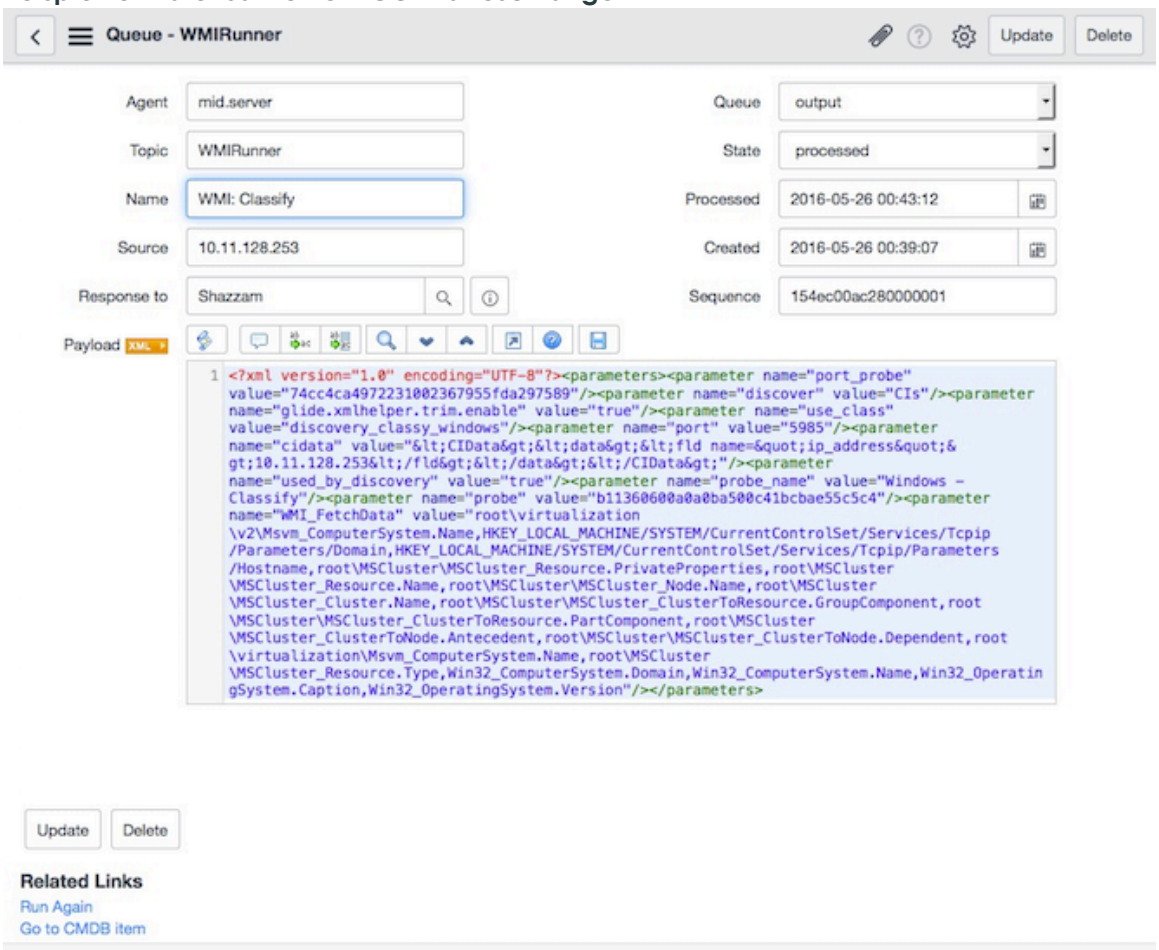
Sie können über einen der folgenden Pfade auf die ECC-Warteschlange zugreifen:

- **Discovery** > **Ausgabe und Artefakte** > **ECC-Warteschlange**
- **ECC** > **Warteschlange**

Die folgende Abbildung enthält ein Beispiel für einen Datensatz in der ECC-Warteschlange. Dieser Datensatz zeigt, dass eine WMI-Klassifizierer-Probe zur Ausführung angewiesen und verarbeitet wurde. Eine Beschreibung der einzelnen Felder finden Sie unter Die MID-Server-ECC-Warteschlange .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Datensatz einer ECC-Warteschlange



Statusangaben der ECC-Warteschlange

Eingabe- und Ausgabenachrichten werden nacheinander weiter verarbeitet, bis die Erkennung abgeschlossen oder beendet wird. Sie können die ECC-Warteschlange überwachen, um zu sehen, wie Datensätze während der Erkennung gefüllt werden, und um den Status der einzelnen Datensatzänderungen anzuzeigen. Eingabedatensätze der ECC-Warteschlange werden von Geschäftsregeln (Business Rules, BR) verarbeitet. Nicht alle Business-Regeln, die ECC-Warteschlangeneingaben verarbeiten, setzen Eingaben auf „Verarbeitet“. Daher ist zu erwarten, dass einige ECC-Warteschlangeneingaben im Status „Bereit“ verbleiben. Der Prozess läuft wie folgt ab:

1. Wenn neue Probe-Anweisungen für einen MID Server verfügbar sind, erstellt das System einen Datensatz vom Typ **Ausgabe** mit dem Status **Bereit**.
2. Der MID Server startet dann die Verarbeitung der Probe-Anweisungen, und der Status wird in **In Verarbeitung** geändert, bevor er schließlich auf **Verarbeitet** gesetzt wird.
3. Wenn ein Ergebnis an den MID Server zurückgegeben wird und zum Senden an die Instanz bereit ist, erstellt das System einen Datensatz vom Typ **Eingabe** mit dem Status **Bereit**.
4. Während das System die Nutzlast verarbeitet, wird der Status in **In Verarbeitung** geändert, bevor er schließlich auf **Verarbeitet** gesetzt wird.

   Wenn Fehler auftreten, wird der Status in **Fehler** geändert. Sie können die Fehler in fehlgeschlagenen Erkennungen beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Debuggen Sie die Verarbeitung von ECC-Warteschlangendatensätzen

Um einen Skript-Debugger verwenden zu können, verarbeiten Sie die Nutzlast in derselben Sitzung wie der Debugger. Überprüfen Sie die Business-Regel, die den jeweiligen ECC-Warteschlangendatensatz verarbeitet, und den tatsächlichen Code, der die Nutzlast verarbeitet.

Eigenschaften und Parameter, die sich auf die ECC-Warteschlange auswirken

Mit den folgenden Eigenschaften lassen sich Aspekte der ECC-Warteschlange steuern:

Eigenschaft	Beschreibung
Anhänge der ECC-Warteschlange speichern	Das normale Verhalten von Erkennungssensoren besteht darin, Anhänge an ECC-Warteschlangeneinträgen nach erfolgreicher Sensorbearbeitung zu löschen. Durch Aktivierung dieser Eigenschaft wird dieses Verhalten außer Kraft gesetzt, Anhänge werden beibehalten. Dies ist normalerweise nur für Debugging-Zwecke nützlich. Standort: Navigieren Sie zu **Discovery-Definition** > **Eigenschaften** um die Eigenschaft zu aktivieren.

Zugehörige Informationen

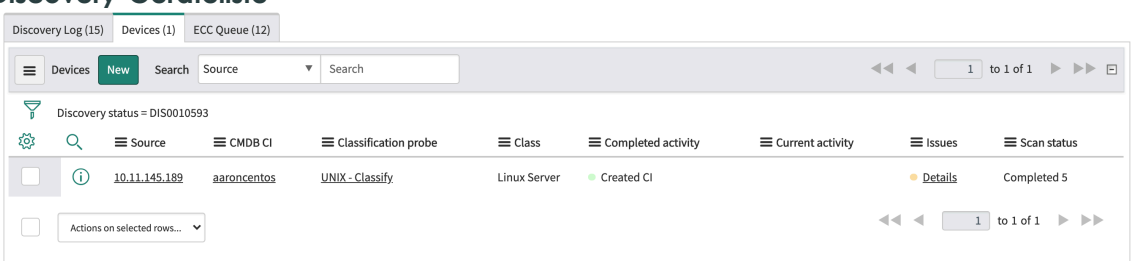
Den Inhalt der ECC-Warteschlange für einen MID Server verwalten

Discovery-Geräteverlauf

Die zugehörige Liste **Geräte** im Formular „Discovery-Status“ enthält eine zusammenfassende Liste aller gescannten Geräte.

Während einer Discovery werden über die Liste aktuelle und abgeschlossene Aktivitäten nachverfolgt, und der inkrementelle Zähler für Scans wird angezeigt. Wenn Discovery für ein Gerät abgeschlossen ist, wird die endgültige Disposition in der Spalte *Abgeschlossene Aktivität* angezeigt. Erfolgreiche Erkennungen, die zu aktualisierten oder erstellten CIs führen, werden grün hervorgehoben. Wenn ein Geräteverlauf oder ein doppelter IP-Datensatz erstellt wird, wird auch die Klassifizierungs-Probe eingetragen. Um die Protokolleinträge für Fehler (zum Beispiel Verbindungsfehler) für ein bestimmtes Gerät anzuzeigen, klicken Sie auf den Link **Details** in der Spalte *Probleme*.

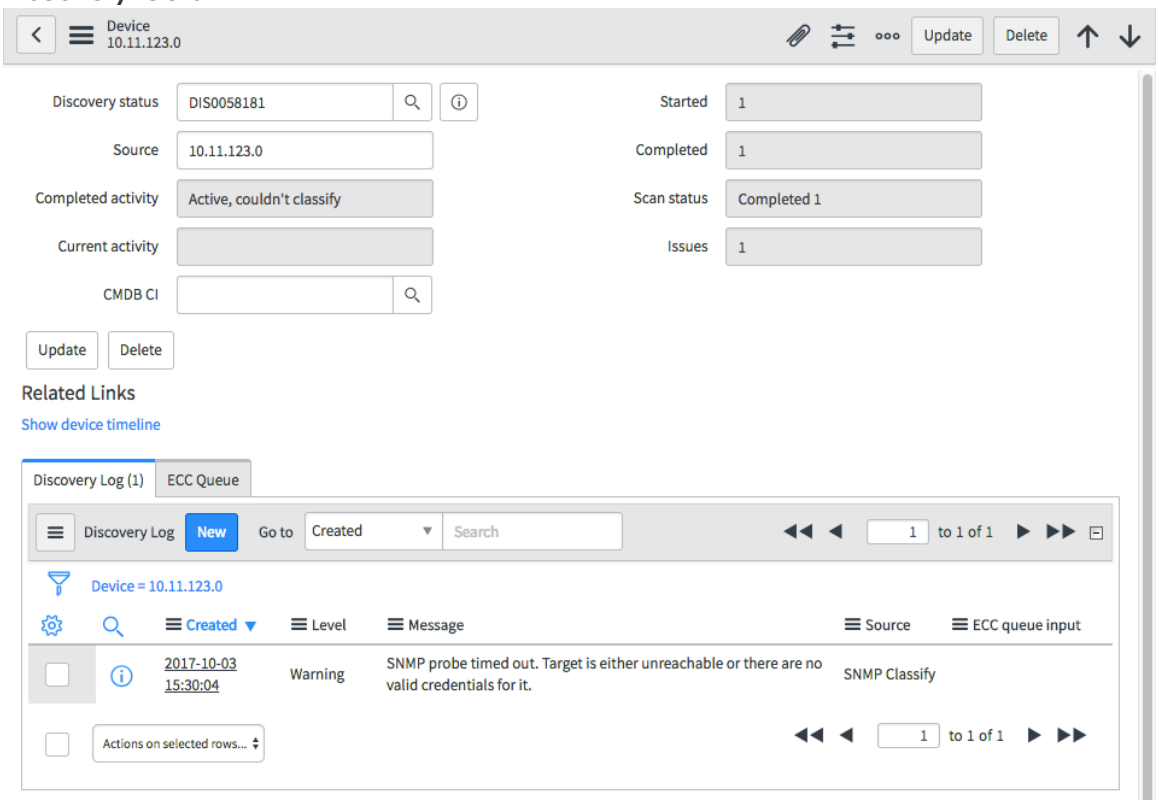
Discovery-Geräteliste



Klicken Sie auf die IP-Adresse eines Geräts in dieser Liste, um Details zu diesem Gerät anzuzeigen. Die Protokollergebnisse für dieses Gerät werden in der Liste unten im Formular angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Gerät



In diesem Formular sind die folgenden Felder verfügbar:

Feld	Eingabewert
Quelle	IP-Adresse des erkannten Geräts
Abgeschlossene Aktivität	Gibt das Ergebnis der Discovery für dieses Gerät oder die letzte abgeschlossene Aktivität für eine in Bearbeitung befindliche Discovery an, zum Beispiel *Identifiziertes CI*. Erfolgreiche Ergebnisse werden in Grün angezeigt.
Aktuelle Aktivität	Aktuelle Scan-Aktivität für dieses Gerät für eine in Bearbeitung befindliche Discovery, zum Beispiel *CI wird aktualisiert*
CMDB CI	Name des Geräts, wie in der CMDB angezeigt
Gestartet	Anzahl der ausgeführten gerätespezifischen Probes. Diese Zahl enthält nicht die universellen Probes Shazzam und Ping, die anfänglich ausgeführt werden.
Abgeschlossen	Anzahl der Sensordatensätze, die aus den ausgeführten gerätespezifischen Probes erstellt wurden
Scan-Status	Zeigt die endgültige Anzahl von Scans einer abgeschlossenen Discovery oder einen inkrementellen Zähler der Scans für eine in Bearbeitung befindliche Discovery an. Beispiel: Scan 17 von 19
Probleme	Zeigt die Anzahl der Probleme an, die während der Discovery dieses Geräts aufgetreten sind. Wählen Sie die zugehörige Liste **Discovery-Protokoll** aus, um diese Probleme anzuzeigen.
Felder, die durch die Konfiguration des Formulars hinzugefügt werden können:	
DNS-Namen	Zeigt DNS-Namen für jedes erkannte Gerät an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während verschiedener Phasen von Discoverywerden im Feld **„Abgeschlossene Aktivität“** im Datensatz „discovery_device_history“ möglicherweise unterschiedliche Werte angezeigt.

Potenzielle Werte für „Abgeschlossene Aktivität“ in „discovery_device_history“.

Wert	Wann dieser Wert möglicherweise angezeigt wird	Bedeutung
Gängige Beispiele		
Lebhaft, nicht aktiv, nicht klassifiziert	Nach Shazzam	Das Gerät antwortet, hat jedoch keine offenen (aktiven) Ports, für die die Klassifizierung ausgeführt werden kann.
Aktiv	Nach Shazzam	Das Gerät verfügt über offene (aktive) Ports, für die potenziell eine Klassifizierung ausgeführt werden kann.
Classified (Klassifiziert)	Nach Klassifizierungsprobe	Wir konnten den Gerätetyp klassifizieren und fahren mit der Identifizierungsphase fort.
Aktiv, konnte nicht klassifiziert werden	Nach Klassifizierungsprobe	Der Gerätetyp konnte nicht klassifiziert werden. Manchmal enthält dieser Wert auch einen Grund, warum die Klassifizierung nicht möglich war. Beispiel: Aktiv, konnte nicht klassifiziert werden: Keine WMI-Verbindung.
Erstelltes CI	Nach der Identifizierungsprobe/dem Muster oder nach der Ausführung der Business-Regel „Discovery – Device Complete“ (für neues CI)	Neues CI wurde basierend auf Identifizierungsergebnissen erstellt.
Identifiziertes CI	Nach Identifizierungsprobe/-muster	Vorhandenes CI wurde basierend auf Identifizierungsergebnissen gefunden.
Identifiziert, zusätzliche IP ignoriert	Nach Identifizierungsprobe/-muster	Gerät wurde bereits über eine andere IP im gleichen Discovery -Status erkannt.
Aktualisiertes CI	Nach bestimmten Explorationsprobes/-mustern oder nach der Ausführung der Geschäftsregel „Discovery – Device Complete“ (für vorhandenes CI)	CI wurde mit zusätzlichen Informationen aktualisiert.
Weniger häufige Beispiele		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Potenzielle Werte für „Abgeschlossene Aktivität“ in „discovery_device_history“. (Fortsetzung)

Wert	Wann dieser Wert möglicherweise angezeigt wird	Bedeutung
Nicht klassifiziert	Nach Shazzam (nur für Discovery ohne Anmeldeinformationen, und der Erkennungswert im Zeitplan Discovery ist auf IP-Adressen festgelegt)	Für Discovery der Ziel-IP ohne Anmeldeinformationen konnte kein Abgleich mit einem vorhandenen CI in der Instanz gefunden werden.
Classified (Klassifiziert)	Nach Shazzam (nur für Discovery ohne Anmeldeinformationen, und der Erkennungswert im Zeitplan Discovery ist auf IP-Adressen festgelegt)	Für die Ziel-IP ohne Anmeldeinformationen Discovery konnten wir eine Übereinstimmung mit einem vorhandenen CI in der Instanz herstellen.
Aktiv, Windows-Cluster-VIP	Nach Windows – Klassifizieren	Das Gerät ist ein Windows-Cluster-VIP und wird als solcher aktualisiert.
Klassifiziert, aber nicht deaktiviert	Nach Klassifizierungsprobe	Wir haben eine Übereinstimmung mit einem Klassifizierertyp hergestellt, aber der Klassifizierer selbst ist deaktiviert.
Klassifiziert, konnte nicht identifiziert werden	Nach Identifizierungsprobe/-muster	Vorhandener CI-Datensatz konnte nicht erstellt oder mit bestehendem CI-Datensatz abgeglichen werden.
Identifiziert, CI wird nicht aktualisiert	Nach Identifizierungsprobe/-muster	Wir konnten einen CI-Datensatz ordnungsgemäß identifizieren, entscheiden uns jedoch, das CI nicht zu aktualisieren.

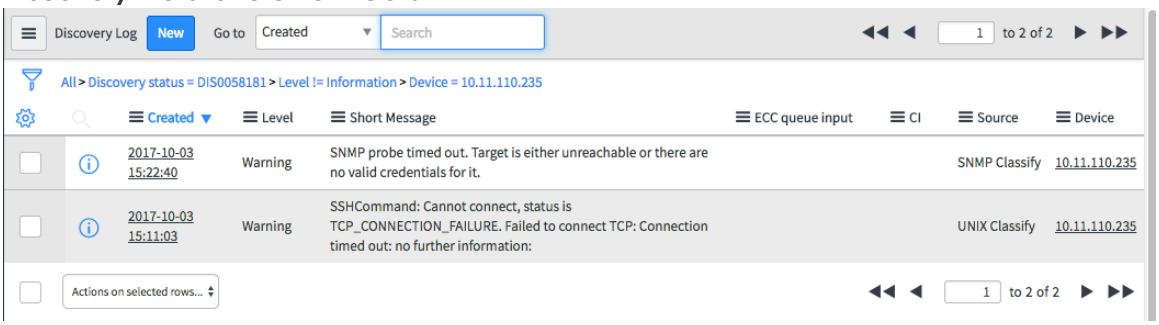
Jedes Gerät, das die folgenden Klassen oder eine der untergeordneten Klassen enthält, wird in der Discovery-Geräteverlaufstabelle angezeigt.

- Computer [cmdb_ci_computer]
- Netzwerkausrüstung [cmdb_ci_netgear]
- PDU [cmdb_ci_pdu]
- Drucker [cmdb_ci_printer]
- UPS [cmdb_ci_ups]

Wenn Probleme aufgetreten sind oder eine Discovery nicht abgeschlossen werden konnte, klicken Sie auf den Link **Details**, um die Protokolldatensätze für das Problem anzuzeigen. Der Ausfall einer Probe gilt als Problem, auch wenn das Gerät schließlich ordnungsgemäß klassifiziert und in der CMDB aktualisiert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Details zu einem Gerät



Adress-Scan-Daten

Wenn Discovery nur nach IP-Adressen (ohne Anmeldeinformationen oder Bezeichner) scannt, werden keine Aktualisierungen an der CMDB vorgenommen. Alle erkannten IP-Adressen werden in dieser Liste angezeigt, einschließlich mehrerer IP-Adressen für dasselbe Gerät. Die Ergebnisse von IP-Adress-Scans enthalten geringfügig andere Informationen als die Ergebnisse eines CI-Scans. Da dem IP-Adress-Scan keine CMDB-Aktivität zugeordnet ist, zeigt die Spalte *Abgeschlossene Aktivität* nur den Klassifizierungsstatus an.

Mögliche Status sind:

- *Classified (Klassifiziert)*
- *Nicht klassifiziert*
- *Alive, not classified (Aktiv, nicht klassifiziert)*

Bei klassifizierten Geräten kann Discovery den Gerätetyp in der Spalte *Aktuelle Aktivität* angeben. Beispielsweise können Netzwerkgeräte als Cisco-Netzwerkgeräte klassifiziert werden und ein Computer als Windows-Computer.

Protokolle für horizontale Erkennung

Das System sammelt Protokolle, um die Aktivität widerzuspiegeln, die während einer horizontalen Erkennung basierend auf Mustern und Probes stattfindet. Verwenden Sie die Protokolle, um den Erkennungsprozess zu optimieren oder Probleme zu beheben.

Für die horizontale Erkennung werden vom System Protokolle der folgenden Typen generiert:

Probe-basiert

Die Protokolle für die Probe-basierte horizontale Erkennung decken Klassifizierungsfehler, CMDB-Aktualisierungen und Authentifizierungsfehler ab. Ein Discovery-Protokolldatensatz wird für jede Aktion erstellt, die einem Erkennungsstatus zugeordnet ist.

Hinweis: Das Discovery-Protokoll zeigt auch Fehler an, die während der Identifizierung auftreten, indem Protokolleinträge aus dem Protokoll der Identifizierungs-Engine übernommen werden. Weitere Informationen zur Identifizierungs-Engine und zu möglichen Fehlern finden Sie unter Ausführungsprotokolle untersuchen .

Musterbasiert

Die Protokolle für musterbasierte horizontale Erkennung enthalten die Informationen über Erkennungen, die mit Mustern durchgeführt wurden. Der Protokolldatensatz einer horizontalen Erkennung wird für eine komplette horizontale Erkennung erstellt, die die Ergebnisse aller im Muster angegebenen Vorgänge enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokolle für horizontale Erkennung prüfen

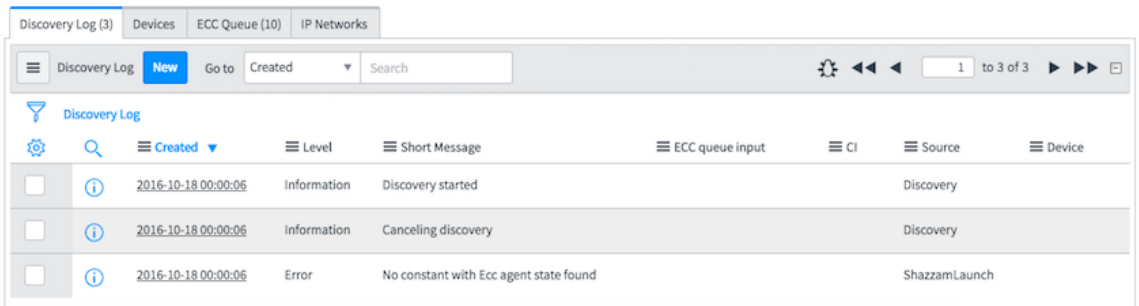
Greifen Sie auf die Protokolle zu, um den Erkennungsprozess zu verstehen und zu optimieren.

Vorbereitungen

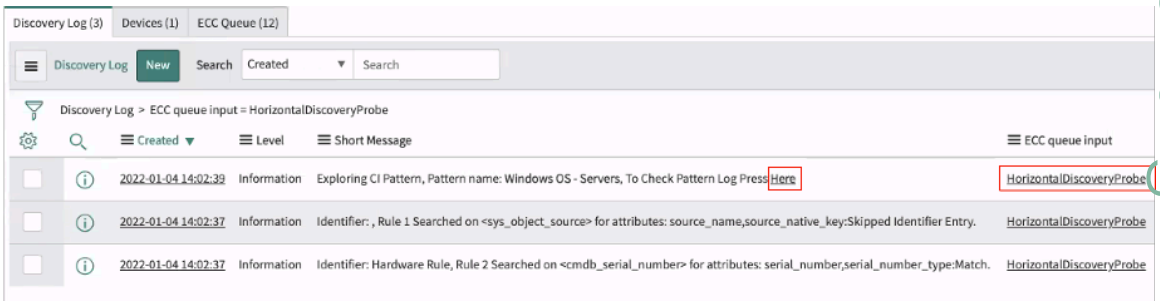
Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Status**.
2. Öffnen Sie einen Datensatz vom Typ Discovery-Status.
   In der zugehörigen Liste **Discovery-Protokoll** werden die Protokolle für die Probe-basierte Erkennung angezeigt. Weitere Informationen finden Sie unter Details zu Discovery-Protokollen.



3. Wahlweise: Suchen Sie die gewünschten Informationen zum relevanten Protokolleintrag:
   - Wählen Sie den Link in der Spalte **CI** aus, um den Datensatz für dieses CI zu öffnen.
   - Wählen Sie den Link in der Spalte **Erstellt** aus, um den Protokolldatensatz anzuzeigen.
   - Wählen Sie den Link der IP-Adresse in der Spalte **Gerät** aus, um die Protokolldatensätze für ein bestimmtes Gerät anzuzeigen.
4. Um Protokolle für die musterbasierte Erkennung anzuzeigen, klicken Sie bei einem Protokolleintrag mit dem Wert **HorizontalDiscoveryProbe** für **ECC-Warteschlangeneingabe** auf den Link **Hier**.

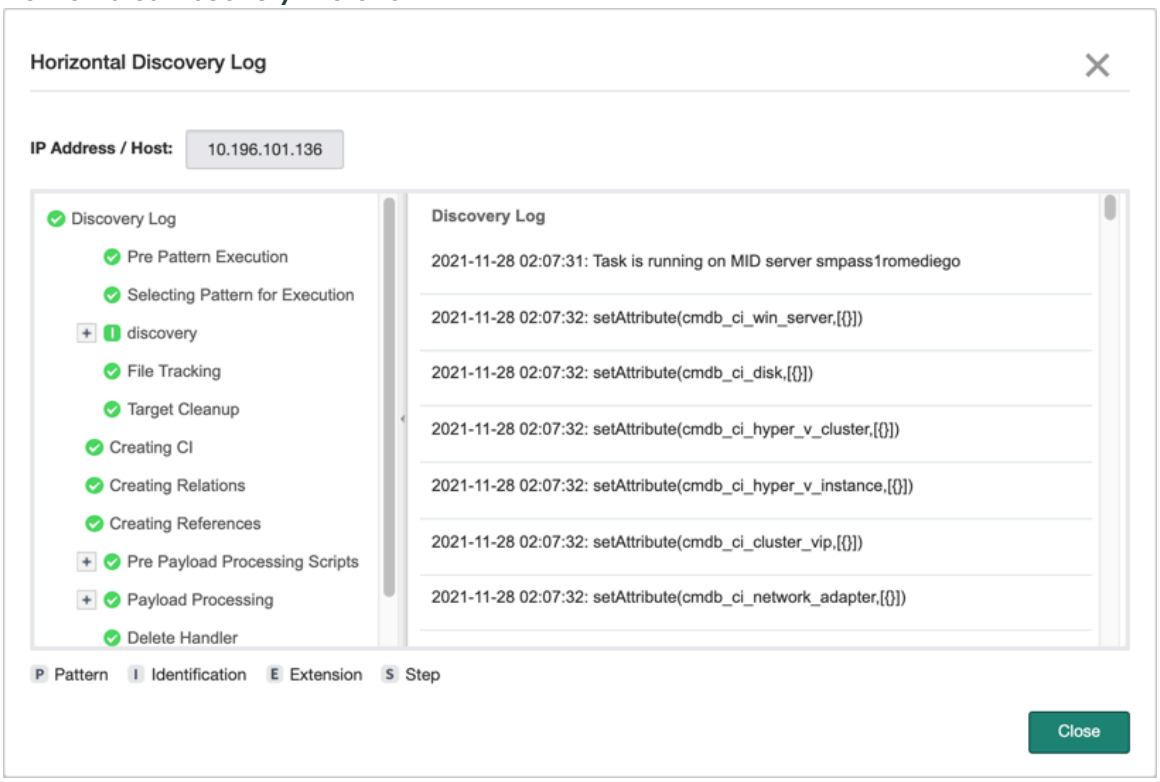


Das Fenster „Horizontales Discovery-Protokoll“ wird geöffnet und zeigt die Liste der musterbasierten Protokolleinträge an. Informationen zu protokollierten Erkennungsphasen finden Sie unter Details zu Discovery-Protokollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Horizontales Discovery-Protokoll



5. Wählen Sie ein Element in der linken Spalte aus, um weitere Informationen dazu in der rechten Spalte anzuzeigen.
6. Wahlweise: Um das Muster zu debuggen, wählen Sie den Namen des Identifizierungsabschnitts und dann die Schaltfläche **Debuggen** aus.
7. Um zum Protokolldatensatz zurückzukehren, wählen Sie **Schließen** aus.

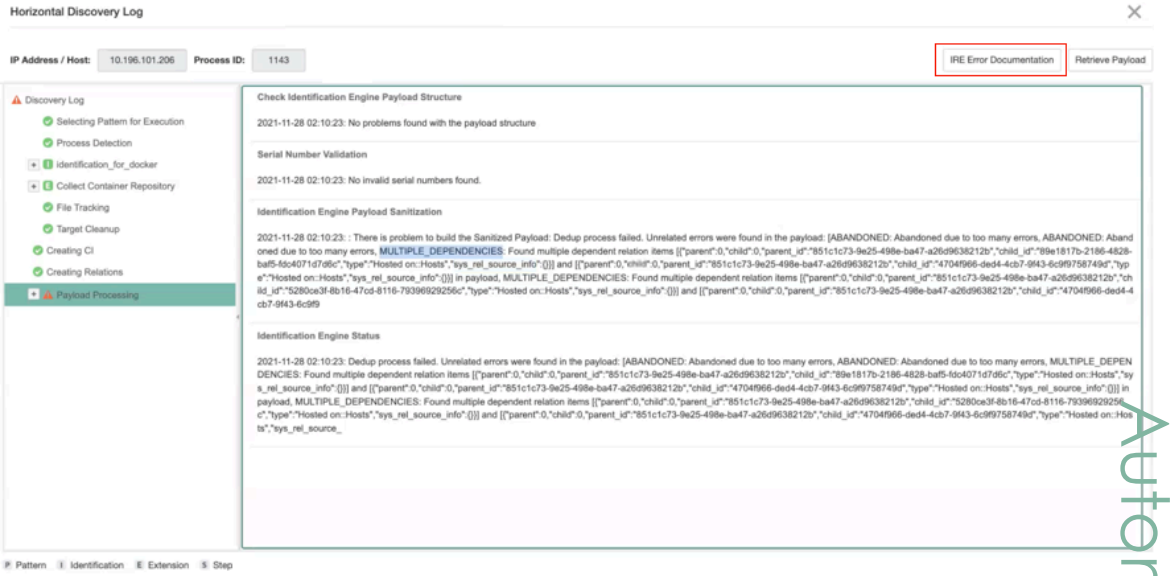
Nächste Maßnahme

- Um die musterbasierte Erkennung zu optimieren oder Probleme zu beheben, rufen Sie die Nutzlast wie unter KB0998923: Retrieve Payload Feature (Nutzlastfunktion abrufen) erläutert ab.
- Validiert Befehle, die in der musterbasierten Discovery verwendet werden, wenn einer der folgenden Fehler vorliegt:
  - Authentifizierungsproblem
  - Autorisierungs-/Berechtigungsproblem
  - Keine gültigen Anmeldeinformationen vorhanden
  - IP-Adresse nicht erreichbar von MID Server
  - Befehl mit falscher Syntax

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn bei der Verarbeitung der Nutzlast ein Fehler auftritt, wählen Sie die Schaltfläche **IRE-Fehlerdokumentation** aus, um mehr über den aufgetretenen Fehler der Identification and Reconciliation Engine (IRE) und dessen Behebung zu erfahren.



Zugehörige Informationen

Identification and Reconciliation Engine (IRE)

KB0854603: Zeitüberschreitung bei Muster-Debugger-Sitzung

Change-Aufbewahrungszeit für Probe-basierte Discovery-Protokolle

Sie können konfigurieren, wie lange Protokolleinträge für die Probe-basierte horizontale Erkennung in Discovery aufbewahrt werden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig werden im Protokoll der Probe-basierten Erkennung Informationen 30 Tage bzw. 2.592.000 Sekunden lang aufbewahrt.

Prozedur

1. Öffnen Sie die Tabelle „Automatisch entleeren“, indem Sie `sys_auto_flush.list` in den Navigationsfilter eingeben.
2. Öffnen Sie den Datensatz **discovery_status**.
3. Ändern Sie den Wert im Feld **Alter in Sekunden**.
4. Damit die Änderung sofort wirksam wird, führen Sie den Tabellenbereinigungsauftrag in der Tabelle „Zeitplan“ [sys_trigger] aus.
5. Klicken Sie auf **Aktualisieren**.

Validiert Befehle, die in der musterbasierten Discovery verwendet werden

Validieren Sie Musterbefehle, um sich zu vergewissern, dass sie vom MID-Server erfolgreich ausgeführt werden können. Normalerweise können -Befehle fehlschlagen, wenn Sie nicht die Anmeldeinformationen konfiguriert haben, die zum Ausführen dieser Befehle in Ihrer Instanz ServiceNow erforderlich sind. Eine weitere häufige Ursache für einen Befehlsfehler ist, dass die für die Discovery verwendeten IP-Adressen nicht erreichbar sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Vergewissern Sie sich, dass Sie über die folgenden Anwendungen verfügen:

- Verbesserungen des Musterdesigners (sn_itom_pde)
- Muster für Discovery und Service-Mapping (sn_itom_pattern)

Überprüfen Sie das Protokoll für horizontale Erkennung basierend auf Mustern, wie in Protokolle für horizontale Erkennung prüfen beschrieben.

Bevor Sie Befehle zum ersten Mal validieren oder nachdem Sie die Muster angepasst haben, aktualisieren Sie die Liste der für die Validierung verfügbaren Befehle:

1. Navigieren zu **Alle** > **Musterdesigner** > **Tool zur Befehlsvalidierung** > **Befehlsliste**.
2. Wählen Sie **Befehlsliste neu laden**aus.

Um Anmeldeinformationen in einem IP-Bereich oder IP-Netzwerk testen zu können, installieren Sie die Skripteinbindung ParseIPRanges, die dem KB-Artikel KB1123625: Command Validation Tool (Befehlsvalidierungs-Tool) angefügt ist.

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Unabhängig davon, ob Sie die Erkennung mithilfe von Mustern oder Probes durchführen, werden vom MID-Server Befehle für den Zugriff auf Konfigurationselemente (Configuration Items, CIs) ausgeführt. Die meisten Befehle erfordern Anmeldeinformationen, damit sie ausgeführt werden können. Darüber hinaus müssen Sie die Rolle eines Benutzers mit erweiterten Rechten annehmen, um einige dieser Befehle auszuführen. Wenn die erforderlichen Anmeldeinformationen fehlen, schlägt die Discovery fehl.

Für die musterbasierte Discovery können Sie alle Befehle, die von einem bestimmten Muster verwendet werden, gleichzeitig validieren.

Sie können Discovery-Befehle auch validieren, um zu überprüfen, ob die für die Discovery verwendeten IP-Adressen erreichbar sind. Manchmal sind IP-Adressen falsch, oder die Server, von denen diese IP-Adressen verwendet werden, sind ausgefallen.

Wenn Sie Befehle validieren, die Applicative-Anmeldeinformationen enthalten, überprüft das Tool zur Befehlsvalidierung das Modul Verbindungen und Anmeldeinformationen und verwendet die dort konfigurierten Applicative-Anmeldeinformationen.

Prozedur

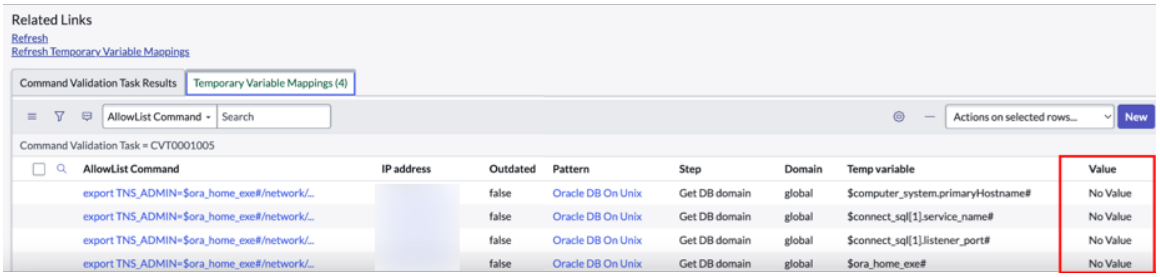
1. Navigieren zu **Alle** > **Musterdesigner** > **Tool zur Befehlsvalidierung** > **Neu erstellen:**.
2. Wahlweise: Um alle von einem Muster verwendeten Befehle zu validieren, wählen Sie **Validate All Pattern Commands (Alle Musterbefehle validieren)**.
3. Füllen Sie die Felder wie in Formular „Aufgaben zur Befehlsvalidierung“ für die musterbasierte Discovery beschrieben aus.
4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Wahlweise: Wenn von Ihnen ausgewählte Befehle temporäre Variablen enthalten, fügen Sie die Werte für diese Variablen hinzu, bevor Sie diese Befehle validieren.

   a. Wählen Sie unter **Zugehörige Linksdie Option Zuordnungen vorübergehender Variablen neu laden aus**.
   Das Tool erstellt eine Liste aller temporären Variablen für die ausgewählten Befehle und IPs.

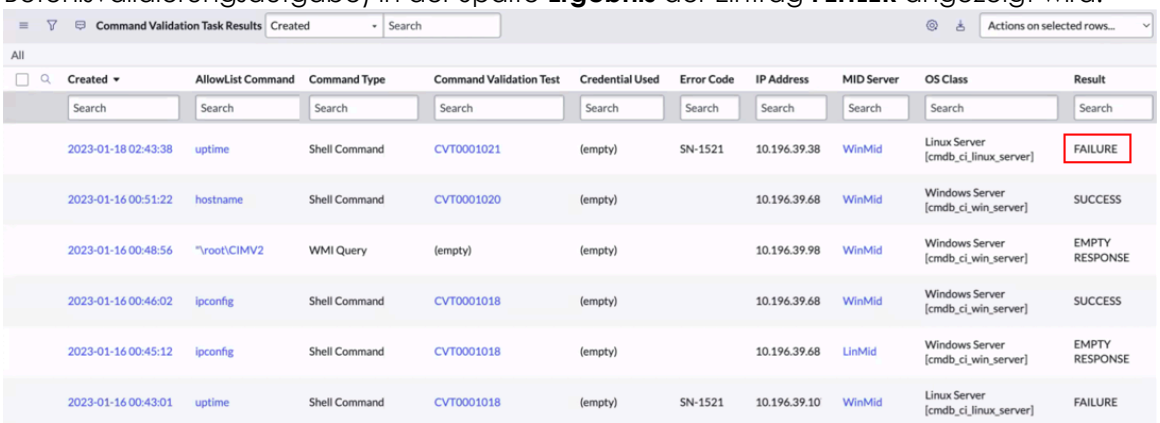
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Wählen Sie die Registerkarte **Zuordnungen temporärer Variablen** aus, und geben Sie die Werte für die temporären Variablen ein.

Registerkarte „Zuordnungen temporärer Variablen“.



6. Wählen Sie **Run Command Validation** (Befehlsvalidierung ausführen) aus.
7. Überprüfen Sie, ob im Abschnitt **Command Validation Task Results** (Ergebnisse der Befehlsvalidierungsaufgabe) in der Spalte **Ergebnis** der Eintrag **FEHLER** angezeigt wird.

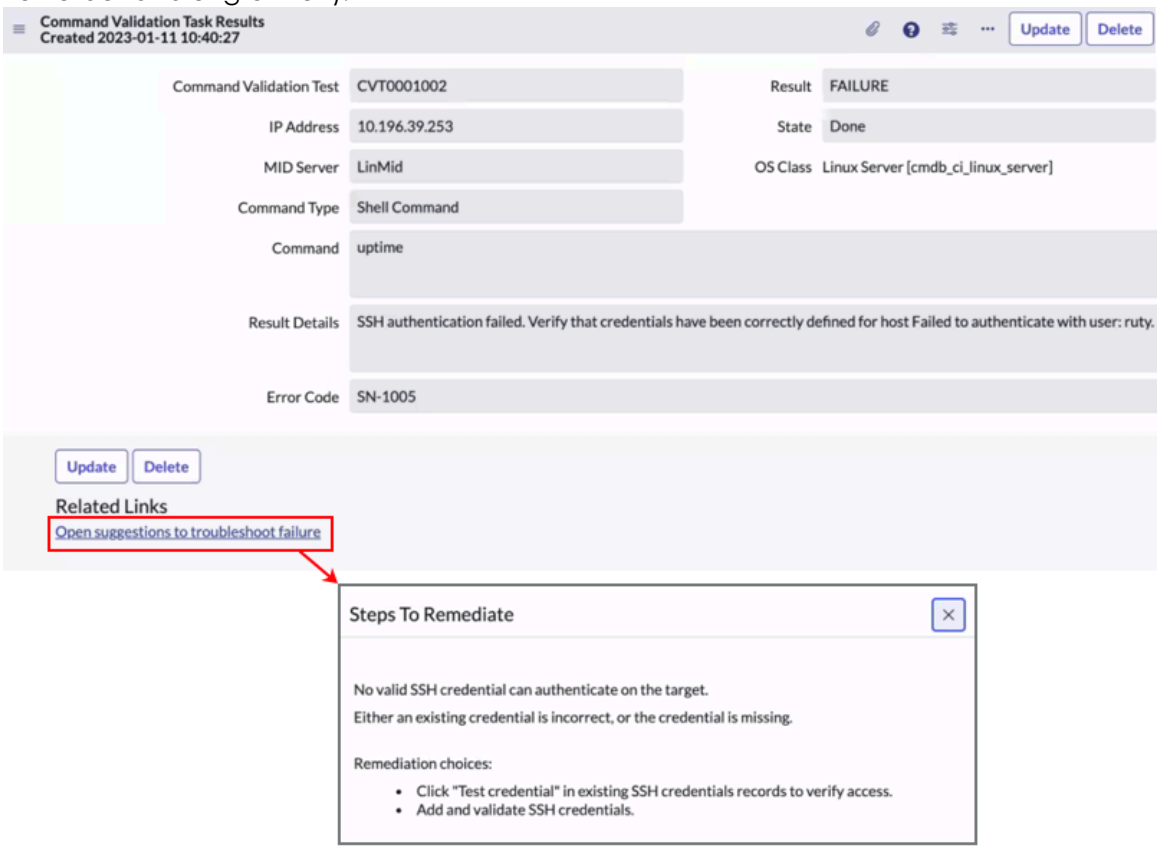


8. Wählen Sie den Link in der Spalte **Befehlsvalidierungstest** aus.
9. Überprüfen Sie die Beschreibung im Feld **Ergebnisdetails**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

1. Klicken Sie auf den Link **Open suggestions to troubleshoot failure** (Vorschläge zur Fehlerbehandlung öffnen).



2. Folgen Sie den Anweisungen im Fenster **Schritte zur Korrektur**.

Zugehörige Informationen

Erste Schritte mit Anmeldeinformationen

Befehlsliste für Befehle, die für die musterbasierte Discovery verwendet werden

Discovery-CLI-Befehle

Muster und horizontale Erkennung

Ein Muster entspricht einer Reihe von Vorgängen, die Discovery mitteilen, welche CIs in Ihrem Netzwerk zu finden sind, welche Anmeldeinformationen verwendet werden sollen und welche Tabellen in der CMDB gefüllt werden sollen.

Dieses Thema setzt voraus, dass Ihnen die Phasen der horizontalen Erkennung bekannt sind. Wenn Sie den Prozess der horizontalen Erkennung für Probes und Muster wiederholen möchten, konsultieren Sie die folgenden Themen:

- Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren
- Prozess-Flow der horizontalen Erkennung mit Mustern

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutzung von Mustern durch Discovery

Ein Muster erfüllt die gleiche Funktion wie eine Probe: es identifiziert und erkundet ein Ziel-CI. Discovery verwendet Muster nur während der letzten beiden Erkennungsphasen: Identifizierung und Erkundung.

Wenn Sie die horizontale Erkennung mit Mustern starten, werden die Phasen „Scannen“ und „Klassifizierung“ so ausgeführt, als würden Sie keine Muster verwenden (nur mit Probes und Sensoren). Nach Abschluss der Klassifizierungsphase überprüft Discovery die Auslöser-Probes im Klassifizierer, um zu sehen, welche Probe zu starten ist. Wenn die Probe *`Horizontal Pattern`* als Auslöser-Probe angegeben ist, startet Discovery sowohl die Probe *`Horizontal Pattern`* als auch das von ihr angegebene Muster.

Unterschiede zwischen Probes und Mustern

Die wichtigsten Unterschiede zwischen der Verwendung von Mustern für die horizontale Erkennung und der Durchführung der horizontalen Erkennung nur mit Probes sind in der folgenden Tabelle aufgeführt:

Thema	Horizontale Erkennung mit Probes	Horizontale Erkennung mit Mustern
Erkennungsphasen	Probes werden während aller vier Erkennungsphasen ausgeführt.	Muster werden nur während der Identifizierungs- und Erkundungsphase ausgeführt. Discovery verwendet dennoch die Shazzam-Probe und die Port-Probes, um die Erkennung zu starten.
Erkennung neuer CIs	Discovery stellt mehrere sofort einsatzbereite Probes und Sensoren bereit. Wenn Sie jedoch neue CIs erkennen oder die Daten ändern möchten, die Discovery in die CMDB füllt, müssen Sie neue Probes und Sensoren erstellen oder die vorhandenen anpassen. Dazu benötigen Sie Kenntnisse in Java und JavaScript und müssen wissen, wie Probes mit anderen Probes und Sensoren zusammenarbeiten.	Discovery stellt in jedem Hauptrelease und im ServiceNow App Store weitere Muster bereit. Wenn Sie ein neues Muster erstellen oder ein vorhandenes anpassen möchten, können Sie den Musterdesigner verwenden, eine benutzerfreundliche Oberfläche, mit der Sie Schritte erstellen und Werte eingeben können.
Funktionsunterstützung	Unterstützt alle standardmäßigen Netzwerk- und CI-Erkennungen. Bestimmte Anwendungen werden ohne Muster nicht unterstützt. Unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte finden Sie eine vollständige Liste.	Zusätzlich zu allen standardmäßigen Erkennungsverfahren unterstützen Muster Folgendes: • Cloud Discovery • Nachverfolgung von Konfigurationsdateien • CI-Löschungsstrategien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Thema	Horizontale Erkennung mit Probes	Horizontale Erkennung mit Mustern
ECC-Warteschlange und Problembehandlung	Je nachdem, wie viele Probes gestartet werden, erstellt Discovery mehrere Datensätze in der ECC-Warteschlange. Zum Beheben von Problemen mit der horizontalen Erkennung müssen Sie mehrere Datensätze der ECC-Warteschlange analysieren, um die von Discovery abgerufenen Daten anzuzeigen.	Discovery erstellt für das Muster nur einen zusätzlichen ECC-Warteschlangen-Datensatz. Zur Behebung von Problemen mit der horizontalen Erkennung während der Identifizierung und Erkundung müssen Sie für das Muster nur einen ECC-Warteschlangen-Datensatz analysieren.
Performance	Je nachdem, welche Art von Ziel-CI Sie identifizieren und erkunden möchten, kann Discovery während der Identifizierungsphase mehrere Probes und dann während der Erkennungsphase zusätzliche Probes auslösen. Es ist möglich, dass die horizontale Erkennung mit Probes aufgrund des zusätzlichen Overhead beim Auslösen und Verarbeiten vieler Probes länger dauern kann.	Discovery löst ein Muster während der Identifizierungs- und Erkundungsphase aus. Alle Vorgänge, die Discovery ausführen muss, befinden sich im Muster. Discovery kann sie der Reihe nach ausführen, bis das Muster abgeschlossen ist. Daher kann die Mustererkennung zu einer schnelleren Leistung führen.

Muster für die Erkennung von oben nach unten sowie für die horizontale Erkennung

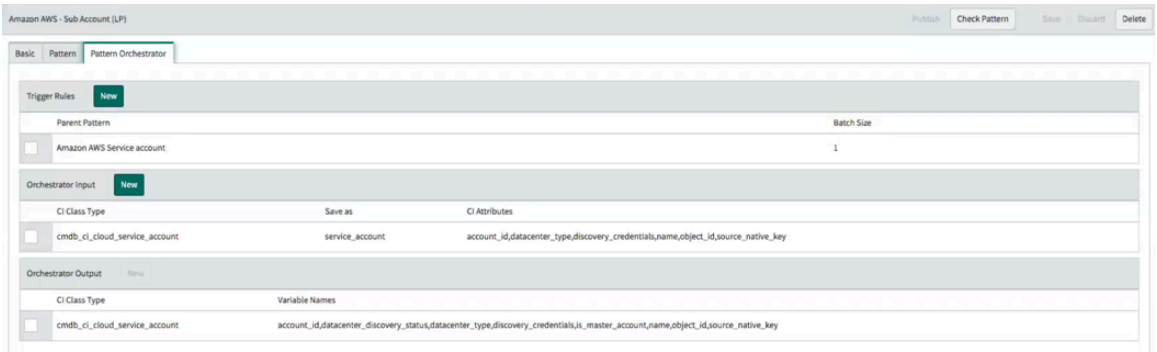
Sowohl Discovery als auch Service Mapping können dasselbe Muster für die horizontale Erkennung und die Erkennung von oben nach unten verwenden. Sie werden jedoch unterschiedlich bearbeitet. Unter Muster erstellen oder anpassen finden Sie Informationen zu den einzelnen Schritten. Wenn Sie ein Muster verwenden, das ausschließlich für die Erkennung von oben nach unten verwendet wurde, und es für die horizontale Erkennung verwenden möchten, müssen Sie einige Änderungen vornehmen. Anweisungen dazu finden Sie unter Muster für horizontale Erkennung verwenden.

Muster-Orchestrator

Der Muster-Orchestrator ist ein Prozess, mit dem eine Erkennung mehrere Muster im Zusammenhang mit einer Datensammlung hierarchisch auslösen kann. Dies dient der Behebung von Problemen mit großen Datensätzen (oder großen Nutzlasten), die langsame Erkennungen und OOM-Probleme (Out-of-Memory) auf einem MID Server verursachen können.

Auf den Muster-Orchestrator wird über die Registerkarte **Pattern Orchestrator (Muster-Orchestrator)** im **Musterdesigner** zugegriffen. Die Registerkarte enthält drei neue Tabellen: **Auslöserregeln**, **Orchestrator-Eingabe** und **Orchestrator-Ausgabe**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Tabelle **Auslöserregeln** gibt das übergeordnete Muster im Feld **Übergeordnetes Muster** an. Das Feld **Batchgröße** gibt an, wie viele Elemente vom übergeordneten Muster bis zum untergeordneten Muster ausgelöst werden sollen. Für **Batchgröße** sind die Optionen **Count (Anzahl)**, **Alle** und **Use Parent Context Only (Nur übergeordneten Kontext verwenden)** verfügbar.

- **Count (Anzahl)** muss eine Zahl für **Anzahl der Batch-Größen** angeben. Das untergeordnete Muster wird jedes Mal ausgelöst, wenn das übergeordnete Muster die angegebene Anzahl von CIs sendet.
- **Alle** verwendet alle vom übergeordneten Muster gesendeten CIs und löst das untergeordnete Element einmal aus.
- **Use Parent Context Only (Nur übergeordneten Kontext verwenden)** stützt sich auf die Ausgabeeinstellungen des übergeordneten Musters, um festzulegen, welches untergeordnete Muster ausgelöst werden soll. Dies ist nützlich, wenn zwei Muster dasselbe übergeordnete Element haben, Sie aber eines vor dem anderen auslösen müssen.

Die **Orchestrator-Eingabe** verwendet das Feld **CI-Typ**, um CI-Typen aus dem übergeordneten Muster oder dem übergeordneten Muster des übergeordneten Elements zu akzeptieren. Das Feld **Gespeichert als** speichert den Namen des CI-Typs, der im Muster verwendet werden soll. Servicekonten sind ein Sonderfall und müssen den Namen service_account aufweisen. Das Feld **CI-Attribute** verwendet alle Ausgaben des übergeordneten Musters, um die zu verwendenden Attribute auszuwählen.

Die **Orchestrator-Ausgabe** steuert, welche Daten an nachfolgende Muster gesendet werden. Sie besitzt die Felder **CI-Klassentyp**, wobei es sich um den Typ des CI handelt, das erkannt wird, und **Variablennamen**, das die Variablen angibt, die als Eingaben für untergeordnete Muster übergeben werden sollen. Variablen, die nicht in **Variablennamen** angegeben sind, werden nicht an untergeordnete Muster gesendet. Die Variable **source_native_key** kann manuell hinzugefügt werden, indem Sie im Feld **Variablennamen** nach ihr suchen.

Nativer Schlüssel der Quelle

In einigen Situationen kann ein Muster partielle Informationen über ein CI abrufen, während ein anderes Muster partielle Informationen über dasselbe CI abruft. Anstatt redundante Datensätze zu erstellen oder partielle Informationen zu verwerfen, werden die Informationen in der Tabelle „CMDB-IRE – teilweise Payloads“ [cmdb_ire_partial_payloads_list] gespeichert. Nachdem genügend Muster partielle Informationen gesammelt haben, können diese Daten korreliert werden, um vollständige Informationen über das CI bereitzustellen.

Paginierung

Eine weitere Möglichkeit, den Arbeitsspeicher des MID Servers zu entlasten, besteht in der Paginierung. Die Paginierung unterteilt eine große Nutzlast in kleinere, geordnete Segmente, die als Seiten bezeichnet werden. Die Paginierung begrenzt die maximale Größe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

empfangener Elemente und generiert ein Token. Sobald diese Seite verarbeitet wurde, wird das Token jeweils an die nächste Seite übergeben, die dann verarbeitet wird, bis alle Seiten abgeschlossen sind.

Die Paginierung wird über die Tabelle „Benutzerdefinierte Vorgänge“ [sa_custom_operation] gesteuert. Das Feld **Ist paginierungsfähig** ist im Formular standardmäßig ausgeblendet und kann dem Formular mit den Steuerelementen für **Formular personalisieren** hinzugefügt werden. Sobald dies auf „true“ gesetzt ist, enthält das zugeordnete Muster im Musterdesigner das Feld **Paginiert**. Indem Sie das Feld **Paginiert** auf „true“ einstellen, wird dieser Schritt im Muster mit Paginierung ausgeführt.

Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen

Zur Verwendung eines Musters für die Identifizierungs- und Erkundungsphase der horizontalen Erkennung müssen Sie den Klassifizierern für die zu erkennenden CIs die Probe „Horizontal Pattern“ hinzufügen.

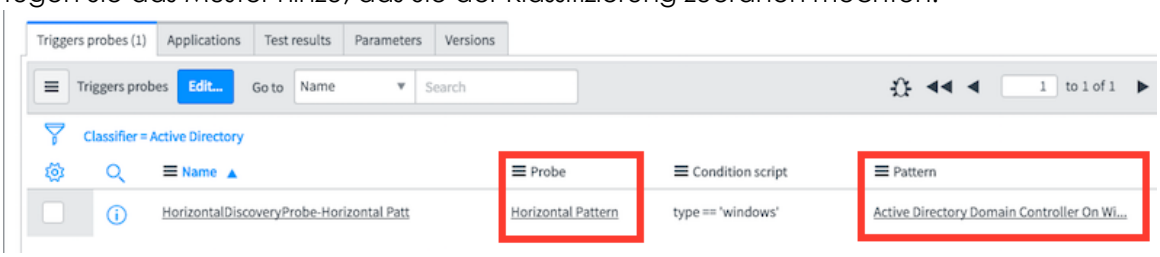
Vorbereitungen
Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Warnung: Dieses Verfahren ist nur für benutzerdefinierte Klassifiziererdatensätze oder solche gedacht, die standardmäßig kein Muster enthalten. Wenn Sie Ihre CMDB jedoch bereits mithilfe von Probes aus diesem Klassifizierer mit Daten gefüllt haben und dann zur Verwendung von Mustern wechseln, werden von Discovery möglicherweise doppelte CIs erstellt. Führen Sie dieses Verfahren deshalb nur aus, wenn Sie Discovery nie mit Probes für diesen Klassifiziererertyp ausgeführt haben.

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **{Klassifiziererertyp}**.
2. Öffnen Sie den Klassifiziererdatensatz.
3. Klicken Sie auf die zugehörige Liste **Löst Probe aus**.
4. Deaktivieren Sie die vorhandenen Identifizierungs- und Erkundungs-Probes.
5. Klicken Sie auf **Bearbeiten**, und fügen Sie die Probe **Horizontal Pattern** hinzu.
   Die Probe wird in der zugehörigen Liste angezeigt.
6. Doppelklicken Sie in der zugehörigen Listenansicht in das Feld unter der Spalte **Muster**, und fügen Sie das Muster hinzu, das Sie der Klassifizierung zuordnen möchten.



7. Entfernen Sie die anderen Probes aus der zugehörigen Liste **Löst Probe aus**, bzw. deaktivieren Sie sie.

Hinweis: Wenn Sie ein Muster löschen, wird die Probe „Horizontal Pattern“ nicht automatisch aus dem Klassifizierer entfernt. Sie müssen für die horizontale Probe ein anderes Muster auswählen, oder Sie können wieder zur Verwendung von Identifizierungs- und Erkundungs-Probes wechseln, die für den Klassifizierer spezifisch sind. Wenn Sie die horizontale Probe ohne angegebenes Muster verwenden, wird die Erkundung nach der Klassifizierungsphase beendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster für horizontale Erkennung verwenden

Wenn Sie ein neues Muster verwenden möchten oder bereits über ein Muster verfügen, das Sie für die Erkennung von oben nach unten verwendet haben, können Sie das Muster für die horizontale Erkennung mit einigen Änderungen am entsprechenden Klassifizierer verwenden.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

⚠ **Warnung:** Dieses Verfahren ist nur für benutzerdefinierte Klassifiziererdatensätze oder solche gedacht, die standardmäßig kein Muster enthalten. Wenn Sie Ihre CMDB jedoch bereits mithilfe von Probes aus diesem Klassifizierer mit Daten gefüllt haben und dann zur Verwendung von Mustern wechseln, werden von Discovery möglicherweise doppelte CIs erstellt. Führen Sie dieses Verfahren deshalb nur aus, wenn Sie Discovery nie mit Probes für diesen Klassifizierertyp ausgeführt haben.

Prozedur

1. Stellen Sie sicher, dass Discovery das Muster verwenden kann:

   a. Navigieren zu **Musterdesigner** > **Discovery-Muster**.

   b. Öffnen Sie das Muster.
   Anwendungsmuster, die von Service Mapping verwendet werden, sind als Typ **1: Anwendung** angegeben.

   c. Stellen Sie in den **Identifizierungsabschnitten** auf der Registerkarte, **Standard** sicher, dass mindestens ein Bereich verfügbar ist, der einen Einstiegspunkt der Art **TCP** oder **Alle** ermöglicht.
   Erstellen Sie andernfalls einen entsprechenden Bereich. Den Identifizierungsschritten können Sie weitere Informationen zum Erstellen eines neuen Musters entnehmen.

   d. Speichern Sie das Muster.

2. Erstellen oder ändern Sie in der Instanz die Klassifizierung für den CI-Typ, den Sie erkennen möchten.
   Konfigurieren Sie den Klassifizierer wie folgt:

   a. Navigieren zu **Discovery-Definition** > **CI-Klassifizierung** > **{Klassifizierungstyp}**.

   b. Öffnen Sie den relevanten Klassifizierer.

   c. Konfigurieren Sie den Klassifizierer wie folgt:

   - **Beziehungstyp**: Wählen Sie **Wird ausgeführt auf::Wird ausgeführt** aus (nur für Prozessklassifizierer).
   - **Bedingung**: Konfigurieren Sie dieselbe Bedingung, die Sie im Muster definiert haben.
   - Zugehörige Liste **Auslösertests**: Fügen Sie die Probe „Horizontal Pattern“ hinzu, und fügen Sie dann der Spalte **Muster** das verwendete Muster hinzu.

   Unter Discovery-CI-Klassifizierung erstellen finden Sie eine Beschreibung der anderen Felder im Klassifizierer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Führen Sie das Muster im Debug-Modus aus, um es zu testen. Wenn Sie sicher sind, dass das Muster funktioniert, können Sie die Erkennung ausführen, indem Sie einen Erkennungszeitplan einrichten oder eine Erkennung bei Bedarf ausführen. Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Discovery-Probes und -Sensoren

Discovery-Probes und -Sensoren führen die Datenerfassung durch und aktualisieren die CMDB.

Mit jeder Version ersetzen Muster viele Sonden und Sensoren für Discovery. Erwägen Sie das Erstellen neuer Muster oder das Bearbeiten vorhandener Muster, wenn Sie anpassen möchten, was Discovery finden kann. Die Informationen zu Sonden und Sensoren sind für Kunden gedacht, die noch keine Muster verwenden, und für Kunden, die bereits benutzerdefinierte Sonden haben, die beim Upgrade beibehalten werden. Siehe Muster und horizontale Erkennung für weitere Informationen zu Mustern.

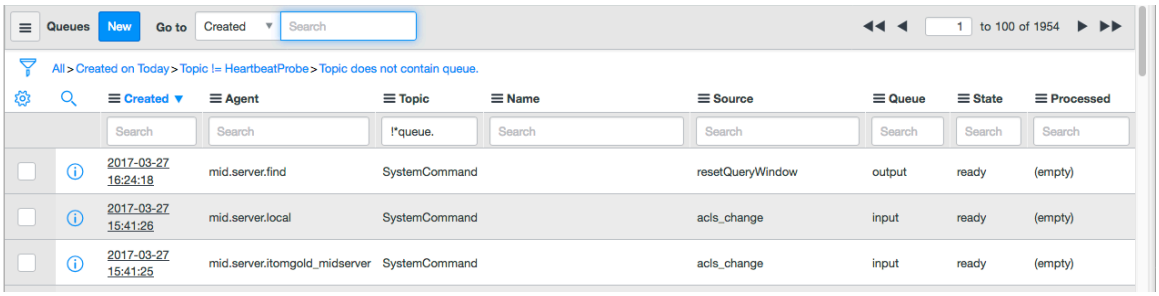
Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Erkennungsphasen

Discovery verwendet während der ersten beiden Erkennungsphasen (Scan-Phase und Klassifizierungsphase) stets Probes und Sensoren. Für die letzten beiden Phasen, Identifizierungsphase und Erkundungsphase, kann Discovery Probes und Sensoren oder Muster verwenden. Dieses Thema bezieht sich nur auf Probes und Sensoren. Erläuterungen der einzelnen Phasen finden Sie unter Discovery erkunden. Siehe Muster und horizontale Erkennung für weitere Informationen zu Mustern.

Probes, Sensoren und ECC-Warteschlange

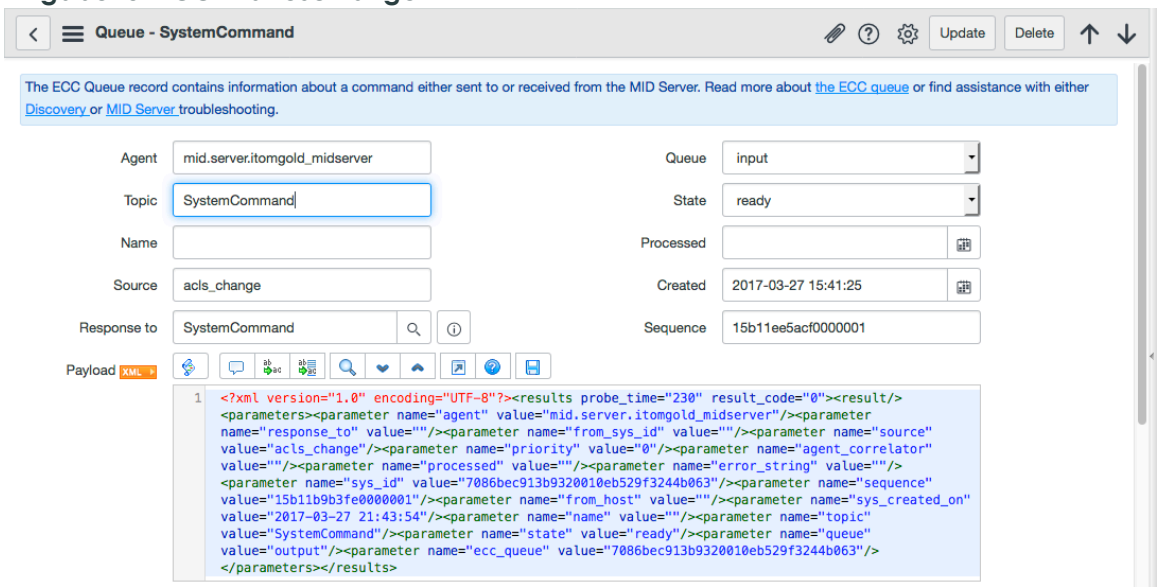
Die Probe erfasst Informationen, die vom Sensor verarbeitet werden. Beide erhalten ihre Anweisungen aus der ECC-Warteschlange. Ein Arbeiterauftrag auf dem MID Server überwacht die Warteschlange auf Arbeit. Die Überwachung sucht nach Einträgen, bei denen das Feld *Warteschlange* den Wert *Ausgabe* und das Feld *Status* den Wert *Bereit* aufweist.



Der MID Server verarbeitet dann alle ausgegebenen ECC-Nachrichten, führt die erforderlichen Probes aus und gibt die Probe-Ergebnisse an die ECC-Warteschlange zurück. Diese Ergebnisse werden als Einträge vom Typ *Eingabe* in der ECC-Warteschlange abgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabe für ECC-Warteschlange



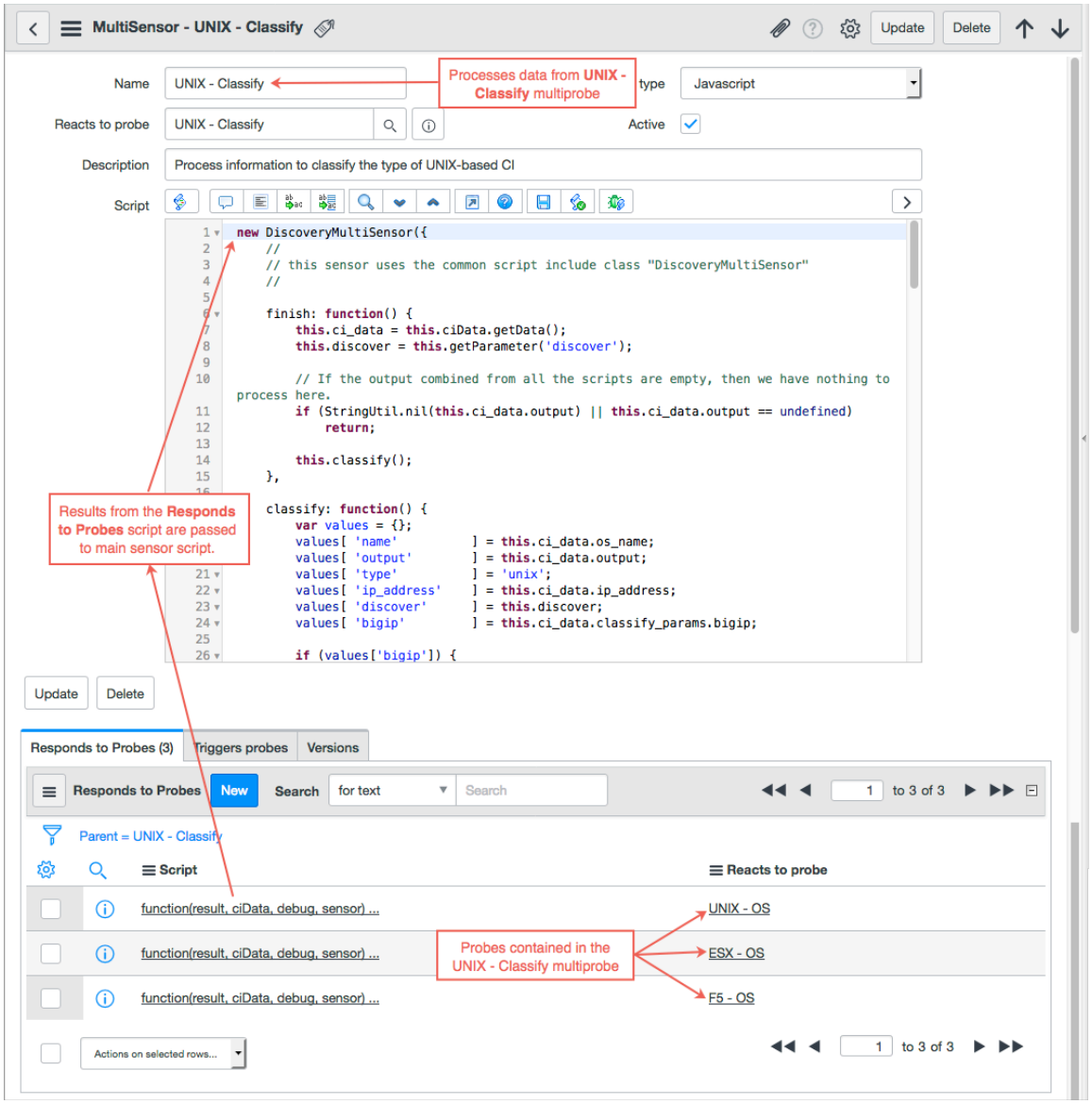
Nachdem ein Eintrag in die Tabelle der ECC-Warteschlange eingefügt wurde, wird eine Geschäftsregel ausgelöst (beim Einfügen), die diese Informationen aufnimmt und sie durch einen *Sensorprozessor* verarbeiten lässt. Die Aufgabe des Sensorprozessors besteht darin, alle für diese eingegebenen Daten relevanten Sensoren zu ermitteln und zur Verarbeitung weiterzuleiten. Diese Sensoren aktualisieren letztlich die CMDB.

Funktionsweise der Zusammenarbeit von Probes und Sensoren

Der MID Server startet Probes, um Informationen über ein Gerät zu erfassen. Die Probe sendet die Informationen zur Verarbeitung an den Sensor zurück. Wenn für die Probe ein Nachverarbeitungsskript definiert ist, führt das Nachverarbeitungsskript einige Schritte zur Datenverarbeitung auf dem MID Server aus, bevor Daten an den Sensor in der ServiceNow-Instanz zurückgesendet werden. Andernfalls senden die Probes alle erfassten Daten zurück, und der Sensor erledigt die Datenverarbeitung. In beiden Fällen aktualisiert der Sensor die CMDB.

Eine Multi-Probe ist eine Probe, die mehrere Probes enthält. Multisensoren verarbeiten die Daten von Multi-Probes. Zur Verarbeitung der Daten von Multi-Probes enthalten Multisensoren einzelne Skripts, mit denen die Daten von jeder in einer Multi-Probe enthaltenen Probe verarbeitet werden, sowie ein Multisensor-Hauptskript. Die einzelnen Skripts übergeben die von ihnen verarbeiteten Daten an das Multisensor-Hauptskript.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Probe-Typen

Gerät	Probe-Typ
Windows Computer und Server	WMI-Remoteabfragen, Shell-Befehle
UNIX- und Linux-Server	Shell-Befehl (über SSH-Protokoll, Version 2). Discovery unterstützt alle Bourne-kompatiblen Shells.
Speicher	CIM-/WBEM-Abfragen
Drucker	SNMP-Abfragen
Netzwerkgeräte (Switches, Router usw.)	SNMP-Abfragen
Webserver	HTTP-Headerprüfung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gerät	Probe-Typ
Unterbrechungsfreie Stromversorgungen (USV)	SNMP-Abfragen

Liste der Discovery-Probes

Für Discovery ist eine Vielzahl von Probes zur Erkennung von Elementen in Ihrem Netzwerk verfügbar.

Die folgenden Probes sind in Discovery enthalten.

Die Bezeichnung des PPP-Skripts in der Tabelle gibt an, ob eine Probe ein PPP-Skript (Probe Post-Processing) enthält, das auf dem MID Server ausgeführt wird. Das PPP-Skript wandelt Probe-Ergebnisse in eine JSON-Zeichenfolge um und gibt die Zeichenfolge zur Sensorverarbeitung an die ServiceNow-Instanz zurück.

Um Probes und ihre Beschreibungen anzuzeigen, navigieren Sie zu **Discovery-Definition** > **Probes**.

Die CIM-Probe

Die CIM-Probe verwendet WBEM-Protokolle, um einen bestimmten CIM-Server, den CIM Object Manager, nach einer Reihe von Datenobjekten und Eigenschaften abzufragen.

Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

Die folgenden Parameter können an die CIM-Probe übergeben werden:

CIM-Test

Parameter	Beschreibung	Standardwert
Quelle	[Erforderlich] Der erste Host, zu dem eine Verbindung hergestellt werden soll	Keine
port	Der Port, zu dem eine Verbindung hergestellt werden soll. Wenn der Wert leer ist, wird er durch den Parameter „schema“ bestimmt: http = 5988, https = 5989.	5988 oder 5989
schema	[Erforderlich] Das zu verwendende Schema: „http“ oder „https“.	http
namespace	[Erforderlich] Der CIM-Namespace. Kann durch eine Abfrage überschrieben werden.	Keine
queries	[Erforderlich] Eine durch Semikolon getrennte Liste von Abfragen der CIM-Probe, für die Ergebnisse verarbeitet und zurückgegeben werden sollen	Keine
Wiederholungen	Die Anzahl der Wiederholungsversuche, wenn eine Abfrage aufgrund von Problemen mit der Netzwerkverbindung fehlschlägt	2
connection_timeout	Die Anzahl von Millisekunden, die eine Probe zum Herstellen einer Verbindung mit einem Server benötigt	5000
socket_timeout	Die Anzahl von Millisekunden, die eine Probe Daten lesen muss	5000

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In CIM Intermediate Query Language (CimIQL) werden Schlüssel, Filter und Dot-Walking verwendet, um CIM-Schemen zu durchlaufen.

Parametererweiterung

Die Abfragesprache CIM unterstützt die mit Standard-SNC vorverarbeitete Erweiterung von Probe-Parametern. Platzieren Sie Variablen in Abfragen, indem Sie wie folgt ihren Namen einkapseln:

```
${foobar}.CIM_RunningOS[0].Name
CIM_ComputerSystem.${barfoo}
```

Der Text ${foobar} wird durch den Inhalt des an die CIM-Probe übergebenen Probe-Parameters foobar ersetzt. Dasselbe gilt für barfoo.

CIMIQL

CimIQL (CIM Intermediate Query Language) ist eine Zwischensprache, die darauf ausgelegt ist, den Prozess der Abfrage von CIM-Providern zu vereinfachen.

CimIQL unterstützt derzeit den standardmäßigen WBEM-Protokollstapel (Web-Based Enterprise Management). In Zukunft können jedoch weitere wie Web Services-Management (WS-MAN) hinzugefügt werden. Die Syntax der Abfragesprache leiht sich Elemente der Abfragesprache WMI von MicrosoftMicrosoft Azure Event Hubs und des wbemcli-Befehls von UNIX. Die Bibliothek CimIQL ist eine reine Java-Implementierung.

Hinweis: CimIQL wird „simicle“ ausgesprochen.

CimIQL-Syntax

Die CimIQL-Syntax umfasst zahlreiche Elemente, darunter eine Abfrage und verschiedene Token.

Beschreibungen der Elemente der CimIQL-Syntax

Element	Beschreibung
Erklärung	Das einfachste Element von CimIQL ist eine gültige . Anweisungen enthalten mehrere durch einen Punkt (.) getrennte Abfragen.
Abfrage	Eine stellt eine einzelne protokollunabhängige Anforderung auf hoher Ebene dar. Jede Abfrage besteht aus verschachtelten Sprachkomponenten und Unterkomponenten, die als Token bezeichnet werden.
Token	Ein beschreibt einen bestimmten lexikalischen Aspekt der CimIQL-Syntax.
Vorgangstoken	Das erste Token jeder Abfrage muss ein sein, das den gesamten auszuführenden logischen Vorgang darstellt.
Komponententoken	Ein ist eine Unterkomponente eines Vorgangs-Tokens.
Ergebnis	Jede Abfrage wird mit einem Ergebnis kombiniert, das dann als Eingabe für die nächste Abfrage in der Anweisung bereitgestellt wird. Ein besteht aus einer Reihe von Objekten und ihren Eigenschaften.

CimIQL-Vorgangstoken

Die CimIQL-Probe erfordert Vorgangstoken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jeder der folgenden Kernvorgänge besitzt ein entsprechendes Gegenstück im Standard CIM Operations over HTTP .

CimIQL-Vorgangstoken – Übersicht

Rückgabewert	Details	Äquivalent CIM Operation over HTTP
Klassenobjekt	Get Object Ruft ein einzelnes Objekt einer bestimmten Klasse ab, indem alle eindeutigen Schlüssel (als Schlüsseltoken) und alle optionalen Parametertoken getrennt durch Kommata angegeben werden	GetInstance
Klassenobjekt	Enumerate Objects Ruft Objekte ab, die mit einem Satz von Bedingungstoken und Parametertoken übereinstimmen	EnumerateInstances
Klassenobjekt	Enumerate Associated Objects Ruft Objekte ab, die den einzelnen Ergebnissen der vorherigen Abfrage zugeordnet sind	Assoziationen
Anweisungsergebnisse	Substitution Ein no-op-Token, das die Ergebnisse einer zuvor benannten Anweisung als Eingabe für die nächste Abfrage der eigenen Anweisung verwendet	Referenz auf Ergebnisse einer benannten Anweisung

Token „Get Object“

<Klassenname>{<Schlüsseltoken>,<Parametertoken>,...}

- Ruft ein einzelnes Objekt einer bestimmten Klasse ab, indem alle ihre eindeutigen Schlüssel (als Schlüsseltoken Schlüsseltoken) und alle optionalen Parameter angegeben werden. Parameter Token, getrennt durch Kommas. Dieses Token wird auch als bezeichnet.
- <Klassenname> entspricht dem CIM-Klassennamen (Groß-/Kleinschreibung beachten) des gewünschten Objekts. Standardmäßig werden Objekte der angegebenen Klasse und aller erweiterten Klassen abgerufen.
- Schlüssel- und Parametertoken sind von einem Paar geschweiften Klammern { ... } eingeschlossen.
- Dieses Token darf nur als erste Abfrage in einer Anweisung verwendet werden.
- Rückgabe: Klassenobjekt
- Beispiel:

```
CIM_ComputerSystem{CreationClassName='Linux_ComputerSystem',Name='runti
me'}.*
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Token „Enumerate Objects“

<Klassenname>{{<Bedingungstoken>,<Parametertoken>,...}}<Array-Index-Token> ODER <Klassenname><Array-Index-Token>

- Ruft Objekte ab, die mit einem Satz von Bedingungstoken und Parametertoken übereinstimmen Dieses Token wird auch als bezeichnet.
- Bedingungstoken und Parametertoken sind von zwei Paar geschweiften Klammern {{ ... }} eingeschlossen. Die geschweiften Klammern sind optional, wenn keine Bedingungen oder Parameter erforderlich sind.
- <Klassenname> entspricht dem CIM-Klassennamen (Groß-/Kleinschreibung beachten) der gewünschten Objekte. Standardmäßig werden Objekte der angegebenen Klasse und aller erweiterten Klassen abgerufen.
- Das Indextoken ist optional.
- Dieses Token darf nur als erste Abfrage in einer Anweisung verwendet werden.
- Rückgabe: Klassenobjekt
- Beispiel:

```
CIM_ComputerSystem{{Name!='runtime'}}.*
```

Token „Enumerate Associated Objects“

<Name der Assoziationsklasse>{{<Eigenschaftenfiltertoken>,<Parametertoken>,...}}<Array-Index-Token> ODER <Name der Assoziationsklasse><Array-Index-Token>

- Ruft Objekte ab, die den einzelnen Ergebnissen der vorherigen Abfrage zugeordnet sind
- Bedingungstoken und Parametertoken sind von zwei Paar geschweiften Klammern {{ ... }} eingeschlossen. Die geschweiften Klammern sind optional, wenn keine Eigenschaftenfilter oder Parameter erforderlich sind.
- Der <Name der Assoziationsklasse> ist der Name der M:N- oder 1:N-Klasse, die zwei Objekte miteinander verknüpft. Standardmäßig werden Objekte der angegebenen Klasse und aller erweiterten Klassen abgerufen.
- Das <Parametertoken> ResultClass kann angegeben werden, um Ergebnisse basierend auf dem Klassennamen des resultierenden Objekts zu filtern.
- Das Indextoken ist optional.
- Dieses Token darf nicht als erste Abfrage in einer Anweisung verwendet werden.
- Rückgabe: Klassenobjekt
- Beispiel:

```
CIM_ComputerSystem{{Name='runtime'}}[2].*
```

Substitutionstoken

${<Anweisungsname>}

- Ein no-op-Token, das die Ergebnisse einer zuvor benannten Anweisung als Eingabe für die nächste Abfrage der eigenen Anweisung verwendet
- Rückgabe: keine
- Beispiel:

```
$(lastComputer).ElementName
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CimIQL-Komponententoken

Die CimIQL-Probe erfordert Komponententoken, die Unterkomponenten von operativen Token sind.

Die folgenden Token sind Unterkomponenten von Vorgangstoken.

CimIQL-Komponententoken – Übersicht

Token	Details
Eigenschaften-Token	* ODER <Eigenschaftsname>,<Eigenschaftsname>,... Gibt an, welche Eigenschaften für jedes Objekt des endgültigen Ergebnissatzes zurückgegeben werden müssen
Abfragetrennzeichen-Token	an. (Punkt) Trennt Abfragen
Index-Token	[Index] Verringert die Ergebnisse einer vorhergehenden Abfrage auf ein einzelnes Objekt am angegebenen Ganzzahlindex
Schlüssel-Token	<Schlüsselname>='<Wert>' Gleicht eine Objekteigenschaft, die als Schlüssel festgelegt ist, mit einem genauen Wert ab
Bedingungs-Token	<Eigenschaftsname><Bedingungsoperator><eingeschlossener Wert> Gleicht eine einzelne Eigenschaft eines Objekts basierend auf der angegebenen Bedingung ab
Parameter-Token	<Parametername>:'<Wert>' Übergibt einen Parameter nach <Parametername> an den aufgerufenen Vorgang. Der Parameter kann je nach Parameter während der CimIQL-Vorverarbeitung oder vom CIMOM auf Anforderung verwendet werden.

Eigenschaftstoken

* ODER <Eigenschaftsname>,<Eigenschaftsname>,...

- Gibt an, welche Eigenschaften für jedes Objekt des endgültigen Ergebnissatzes zurückgegeben werden müssen
- Mit dem Platzhalter * werden alle verfügbaren Eigenschaften zurückgegeben. Andernfalls wird jeder gewünschte Eigenschaftsname in einer kommagetrennten Liste bereitgestellt.
- Dieses Token ist am Ende jeder Anweisung erforderlich.
- Beispiel:

```
CIM_ComputerSystem[0].*
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abfragebegrenzertoken

an. (Punkt)

- Trennt Abfragen
- Beispiel:

```
CIM_ComputerSystem.PrimaryOwnerContact
```

Indextoken

[Index]

- Verringert die Ergebnisse einer vorhergehenden Abfrage auf ein einzelnes Objekt am angegebenen Ganzzahlindex
- Dieses Token ist immer optional.
- Beispiel:

```
CIM_ComputerSystem[0].*
```

Schlüsseltoken

<Schlüsselname>='<Wert>'

- Gleicht eine Objekteigenschaft, die als Schlüssel festgelegt ist, mit einem genauen Wert ab
- <Schlüsseltoken> entspricht dem Namen der als Schlüssel verwendeten Eigenschaft.
- Beispiel:

```
CIM_ComputerSystem{CreationClassName='Linux_ComputerSystem',Name='runti
me'}.*
```

Bedingungstoken

<Eigenschaftsname><Bedingungsoperator><eingeschlossener Wert>

- Gleicht eine einzelne Eigenschaft eines Objekts basierend auf der angegebenen Bedingung ab
- <Eigenschaftsname> entspricht dem Namen der Eigenschaft für den Abgleich.
- Der <Bedingungsoperator> legt fest, wie der tatsächliche Wert einer Eigenschaft mit dem erwarteten Wert verglichen wird. Die verfügbaren Operatoren sind *gleich* (=) und *ungleich* (! =).
- Der <eingeschlossene Wert> muss einer der folgenden Möglichkeiten entsprechen:
  - Literaler Wert, in einfachen Anführungszeichen '...' Beispiel: foo='bar'
  - Regulärer Ausdruck, zwischen Schrägstrichen /.../ Beispiel: foo=/bar.*/
- Beispiel:

```
CIM_ComputerSystem{{Name!='runtime'}}.*
```

Parametertoken

<Parametername>:'<Wert>'

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Übergibt einen Parameter nach <Parametername> an den aufgerufenen Vorgang. Der Parameter kann je nach Parameter während der CimIQL-Vorverarbeitung oder vom CIMOM (Common Information Model Object Manager) auf Anforderung verwendet werden.
- Beispiel:

```
CIM_ComputerSystem.CIM_RunningOS{{ResultClass:'Win32_ComputerSystem'}
}.*
```

CimIQL-Tutorial

Dies ist ein Tutorial anhand von Beispielen, bei dem jedes Beispiel auf dem vorherigen Beispiel aufbaut.

CimIQL-Tutorial

Reihenfolge	CimIQL-Anweisung	Ergebnis
1	CIM_ComputerSystem[0].*	Ruft da aller Ins CIM_C und de unterge Elemen Eigensc
2	CIM_ComputerSystem.PrimaryOwnerContact	Ruft alle CIM_C und de unterge Elemen eine Ei Primary
3	CIM_ComputerSystem{CreationClassName='Linux_ComputerSystem',Name='runtime'}.*	Ruft ein eindeu CIM_C und de unterge Elemen Schlüss im Iden angeg
4	CIM_ComputerSystem{{Name!='runtime'}}.*	Ruft alle und un Elemen CIM_C ab, die Name- „runtim Das Filt filtert In heraus, der ang

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CimIQL-Tutorial (Fortsetzung)

Reihenfolge	CimIQL-Anweisung	Ergebnis
		Eigensc enthalt
5	CIM_ComputerSystem{{Name=/^run.*$/}}.*	Ruft alle und un Elemen CIM_C ab, der dem re Ausdru den Sc entspric **Hir** reg erf ein An Das Filt filtert In heraus, der ang Eigensc enthalt
6	CIM_ComputerSystem{{Name='runtime'}}[2].*	Ruft da aller Ins CIM_C und de unterge Elemen Instanz Eigensc aufweis Die Rei Vorgär Abfrag 1. Serve CIM_ und u Elem 2. Ergeb auf d Eigen 3. Zweit abfra Filter

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CimIQL-Tutorial (Fortsetzung)

Reihenfolge	CimIQL-Anweisung	Ergebnis
7	CIM_ComputerSystem.CIM_RunningOS[0].Name	Ruft die Name CIM_O Instanz CIM_C Instanz Das mit CIM_Ru ist der N Assozia das End
8	CIM_ComputerSystem.CIM_RunningOS{{Name=/CentOS/}}[0].Name	Ruft die Name CIM_O Instanz CIM_C Instanz CIM_O Instanz Eigensc „CentO

CimIQL-Ergebnisse

Ergebnisse der CIM-Probe werden als XML-Dokument eingebettet im <output>-Element an den Probe-Sensor übergeben.

Im Folgenden finden Sie ein kommentiertes Beispiel für ein CimQuery-Batch-Ergebnis.

```
<!-- document root -->
 <cimqueryset>
 <!-- A single query and query result. Multiple <cimquery> tags may be
 provided. -->
 <cimquery>
   <!-- The original query, enclosed by CDATA. -->

 <query><!CDATA[[>CIM_ComputerSystem[0].PrimaryOwnerContact<! ]]></query>
   <!-- The resulting data is enclosed within a single <result> tag. -->
   <result>
     <!-- A single class instance result. Multiple <instance> tags may be
 provided.
          Special tags are prefixed with an underscore character. -->
     <instance>
       <!-- The instance's CIM classname -->
       <_classname>Linux_ComputerSystem</_classname>
       <!-- A set of this instances identifying keys. Always provided,
 regardless of property filters.
            Within here, each key is provided as <KeyName>VALUE</KeyName>
 with the VALUE enclosed as CDATA. -->
       <_key>
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
<CreationClassName><![CDATA[Linux_ComputerSystem]]></CreationClassName>
        <Name><![CDATA[runtime]]></Name>
      </_key>
      <!-- Each property that matches the query's property filter will
be provided here, in the same format as keys;
           As <PropertyName>VALUE<PropertyName> where VALUE is enclosed
as CDATA -->

<PrimaryOwnerContact><![CDATA[root@runtime]]></PrimaryOwnerContact>
    </instance>
  </result>
</cimquery>
</cimqueryset>
```

DNS probe

DNS-Probes bestimmen die DNS-Namen für Konfigurationselemente (CI).

Die standardmäßige Probe „DNS Name Resolver“ ist eine ressourcenschonende und schnelle Probe. Er erreicht seine Geschwindigkeit dadurch, dass er parallel auf dem MID Server ausgeführt wird. Die Probe nutzt eine DNS-Suche des MID Server-Host-BS, um den verwalteten DNS-Cache zu verwenden. Die Probe verwendet auch die Datei „hosts“ des Betriebssystems.

Diese Leistungsverbesserungen können deaktiviert werden, indem die veraltete DNS-Probe entweder mit MID Server-Eigenschaften oder -Parametern wiederhergestellt wird. Die Namen der MID Server-Eigenschaften/-Parameter lauten [mid.probe.use_veralteter_forward_dns] und [mid.probe.use_legacy_reverse_dns]. Weitere Informationen finden Sie unter MID-Server-Parameter und MID-Server-Eigenschaften .

Definitionen von DNS-Probes

Probe	Beschreibung
DNS	Bestimmt DNS-Namen von Geräten. Besitzt den Parameter ip_addresses
DNSLookupProbe	Löst die IP-Adresse eines Hosts auf
DNSNameResolver	Löst den DNS-Namen einer IP-Adresse auf

Port-Sonden

Probe	Beschreibung
dns	Ausgelöst durch „dns“. Verwendet den Scanner „DNS Name Resolver“ und die Klassifizierung „Prozessklassifizierung“ [discovery_classy_proc]

Probe „Horizontal Pattern“

Von Discovery wird die Probe für horizontale Muster dafür verwendet, Muster für die horizontale Erkennung zu starten.

Die Probe „Horizontal Pattern“ arbeitet mit dem Sensor „Horizontal Discovery“, damit Discovery Muster für die Erkennung verwenden kann. Wenn Nachrichten von dieser Probe in der ECC-Warteschlange angezeigt werden, werden sie mit dem Namen der ECC-Warteschlange *Pattern Launcher* gefolgt vom Namen des Musters angezeigt. Die Probe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

enthält den Sensor *Horizontal Discovery Sensor*, der die tatsächlichen Aktualisierungen der CMDB basierend auf Identifizierungsregeln durchführt.

Wenn Sie Ihren eigenen Geräte- oder Prozessklassifizierer erstellen und Muster für die Erkennung verwenden möchten, müssen Sie diese Probe im Klassifiziererdatensatz angeben. Sie müssen diese Probe oder den Sensor „Horizontal Discovery“ nicht ändern.

Nutzlast aufteilen

Wenn Discovery Muster verwendet, um bestimmte Geräte wie Lastenausgleichsmodule zu finden, können große Datenmengen an die ECC-Warteschlange gesendet werden. Um große Datenmengen besser verarbeiten zu können, kann die Probe „Horizontal Pattern“ die Nutzlast in Blöcke aufteilen und dann mehrere ECC-Warteschlangen-Datensätze erstellen.

Steuern Sie mithilfe von Eigenschaften, wie der MID Server Nutzlasten aufteilt und verarbeitet. Weitere Informationen finden Sie unter Eigenschaften des MID-Servers .

PowerShell-Probe

Die PowerShell-Probe führt PowerShell V2-Skripts auf dem MID Server-Host aus.

PowerShell-Skripts sind als Probe-Parameter mit dem Dateinamen als Parameternamen definiert. Es ist als Probe-Typ „Probe“ verfügbar, indem „PowerShell“ als ECC-Warteschlangenthema der Probe angegeben wird.

PowerShell-Probe-Parameter

Parametername	Beschreibung
Quelle	[Erforderlich] Der erste Host, zu dem eine Verbindung hergestellt werden soll **Standardwert:** Keine
<script name>.ps1	[Erforderlich] Der Dateiname des auszuführenden PowerShell-Skripts. Ersetzen Sie *<script name>* durch ein gültiges Dateinamenpräfix. **Standardwert:** Keine
powershell_command_parameter_passing	Gibt an, ob Skriptparameter in der Befehlszeile übergeben werden sollen. Unabhängig vom Wert dieses Parameters macht ServiceNow alle Skriptparameter in der Befehlszeile automatisch für PowerShell-Skripts als Umgebungsvariablen verfügbar. **Standardwert:** false
powershell_param_<script parameter name>	Übergibt zusätzliche Parameter an das auszuführende PowerShell-Skript. Jeder Parameter wird dem Skript als Umgebungsvariable im Format *$env:SNC_<script parameter name>* angezeigt. Parameter mit diesem Präfix gelten nicht als verschlüsselt und werden unverändert an das Skript

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametername	Beschreibung
	übergeben. Stellen Sie sicher, dass Sie den entsprechenden Parameter zwischen *powershell_param_<script parameter name>* und *powershell_<script parameter name>* auswählen. Die Verwendung des falschen Präfix führt zu Fehlern in der PowerShell-Ausführung, die an die Instanz in der ECC-Warteschlangeneingabe zurückgegeben werden. **Standardwert:** Keine
powershell_<script parameter name>	Übergibt zusätzliche Parameter an das auszuführende PowerShell-Skript. Jeder Parameter wird dem Skript als Umgebungsvariable im Format *$env:SNC_<script parameter name>* angezeigt. Der MID Server geht davon aus, dass alle Parameter mit diesem Präfix verschlüsselt sind, und versucht, sie zu entschlüsseln. Stellen Sie sicher, dass Sie den entsprechenden Parameter zwischen *powershell_param_<script parameter name>* und *powershell_<script parameter name>* auswählen. Die Verwendung des falschen Präfix führt zu Fehlern in der PowerShell-Ausführung, die an die Instanz in der ECC-Warteschlangeneingabe zurückgegeben werden. **Standardwert:** Keine
debug	Aktiviert die Debug-Protokollausgabe während der Ausführung der Probe. **Standardwert:** false
credentials_debug	Zeigt einen <credentials_debug>-Abschnitt in der ECC-Warteschlange an, der Ihnen bei der Behebung von Problemen mit den Anmeldeinformationen helfen kann. Wenn Sie diese Eigenschaft auf „true“ setzen, werden Informationen zur Behandlung von Problemen mit Anmeldeinformationen in der ECC-Warteschlange ausgegeben, auch wenn die Anmeldeinformationen erfolgreich sind. **Standardwert:** false

Skripting-Anforderungen

Alle benutzerdefinierten PowerShell-Skripts müssen Umgebungsvariablen verwenden, um nichtboolesche Befehlszeilenparameter zu übergeben. Ersetzen Sie nichtboolesche Parameter im Abschnitt *Param()* des Skripts durch Skriptvariablen mit demselben Namen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie die Skriptvariable als Teil der Umgebung mit einem SNC_-Präfix. Dadurch wird ein Zeichenfolgenparameter wie der folgende:

```
Param([string]$paramName)
```

zu einer Skriptvariablen wie der folgenden:

```
if(test-path env:\SNC_paramName) {
    $paramName = $env:SNC_paramName
}
```

Beispielsweise enthält diese Parameterdefinition aus dem Skript PSScript.ps1 mehrere Zeichenfolgenparameter, die als Skriptvariablen neu definiert werden müssen:

```
Param([string]$computer, [string]$script, [string]$user,
 [string]$password, [boolean]$useCred, [boolean]$isDiscovery,
 [boolean]$debug)
```

Das Definieren der nichtbooleschen Parameter als Skriptvariablen führt zu folgendem Skripttyp:

```
Param([boolean]$useCred, [boolean]$isDiscovery, [boolean]$debug)

# Copy the environment variables to the params
if(test-path env:\SNC_computer) {
  $computer=$env:SNC_computer
}

if(test-path env:\SNC_script) {
  $script=$env:SNC_script
}

if(test-path env:\SNC_user) {
  $user=$env:SNC_user
  $password=$env:SNC_password
}
```

Benutzerdefinierte PowerShell-Probe erstellen

Sie können Ihre eigene PowerShell-Probe erstellen und Probe-Parameter konfigurieren.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **Probes**.
2. Klicken Sie auf **Neu**.
3. Tragen Sie die folgenden Werte ein.
   - **Name**: Beliebiger eindeutiger Name
   - **Probe**-Typ: Probe
   - **ecc_queue_topic**: Powershell
4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile des Formulars, und klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie in der zugehörigen Liste **Probe Parameter** auf **Neu**.
6. Erstellen Sie einen Probe-Parameterdatensatz für jeden Parameter.
7. Klicken Sie auf **Absenden**.

Probe „SCPRelay“

Die *Probe „SCP Relay“* kopiert eine einzelne Datei oder den Inhalt eines Verzeichnisses von einem Host auf einen anderen und verwendet dabei den MID-Server als Relay.

Die Probe „SCP Relay“ verwendet dieselben Parameter wie die Probe „SSHCommand“. Die Befehle können innerhalb bzw. außerhalb des Kontexts eines Terminals (tty) und mit bzw. ohne sudo gesendet werden (für Befehle wie lsof, die im Kontext von root ausgeführt werden müssen, um die benötigten Informationen auszugeben). Wenn Befehle im Kontext eines Terminals gesendet werden, wird der Pfad automatisch erweitert, um eine Reihe von Standardpfaden einzubeziehen (dafür kann der Parameter path_override verwendet werden). Wenn der Zielcomputer der lokale Computer ist, wird SSH nicht verwendet. Stattdessen wird eine lokale Shell ausgeführt, um den Befehl auszuführen.

Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

Die folgenden Parameter können an die *Probe „SCP Relay“* übergeben werden:

Parameter

Parameter	Beschreibung	Standardwert
debug	Aktiviert die Debug-Protokollierung	false
debug_ssh	Aktiviert die J2SSH-Debug-Protokollierung **agent.log** **Hinweis:** Diese Protokolldatei kann schnell größer werden und sollte deaktiviert werden, wenn sie nicht benötigt wird.	false
timeout	Legt den Verbindungstimeout für Socket-Verbindungen in ms fest	60000
path_override	Überschreibt die Standardpfade, die vor der Ausführung eines Befehls festgelegt wurden.	keine
keyboard_interactive	Bei „true“ wird die Verwendung des SSH-Anmeldemodus „keyboard_interactive“ erzwungen.	false
must_sudo	Bei „true“ wird die Ausführung des Befehls über sudo erzwungen.	false
run_in_terminal	Bei „false“ wird die Ausführung von SSH-Befehlen in einem SSH-Terminal deaktiviert (viele Befehle werden dadurch unwirksam).	Wahr
long_runner	Falls vorhanden, wird dadurch ein SSH-Befehl mit langer Ausführungszeit angegeben.	false
set_path	Bei „false“ wird die Festlegung der Umgebungsvariablen für den Pfad vor der Ausführung des Befehls deaktiviert.	Wahr

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter (Fortsetzung)

Parameter	Beschreibung	Standardwert
rm_override	Falls vorhanden, wird der standardmäßige rm-Befehl ("/sbin/rm -f") mit dem angegebenen Wert überschrieben.	keine
Quelle	Host oder IP als Quelle des Kopiervogangs	erforderlich
source_port	SSH-Port der Quelle (standardmäßig 22)	erforderlich
from_file	Name der Datei, die aus der Quelle kopiert werden soll	erforderlich
target	Host oder IP als Ziel des Kopiervogangs	erforderlich
target_port	SSH-Port des Ziels (standardmäßig 22)	erforderlich
to_file	Name der Datei, die auf das Ziel kopiert werden soll	erforderlich

SNMP-Probes

SNMP-Probes verwenden das SNMP-Protokoll, um ein bestimmtes Gerät nach einer Liste von OIDs abzufragen, die dann durchlaufen und deren Ergebnisse an die Sensoren zurückgegeben werden. MID Servers bieten standardmäßig Unterstützung für alle SNMP-Protokollversionen. Sie können einen MID-Server so einstellen, dass er nur bestimmte Versionen von SNMP unterstützt.

Discovery bietet Unterstützung für die SNMP-Versionen 1, 2c und 3. Der Standardwert ist ALLE. Wenn Sie eine der Versionen auswählen, aber nicht über die Anmeldeinformationen dieser Version verfügen, wird die Option „SNMP-Version verwenden“ auf ALLE zurückgesetzt.

Hinweis: Anmeldeinformationen für die SNMP-Version müssen „active=true“ sein. Wenn eine bestimmte Version inaktiv ist, wird die Einstellung ebenfalls auf ALLE zurückgesetzt. Es wird eine Nachricht ähnlich der folgenden angezeigt: `--- In dieser Instanz sind keine SNMP-Anmeldeinformationen vom Typ „snmpv3“ aktiv. „SNMP-Version verwenden“ zurück auf „Alle“ setzen.`

SNMP-Muster

Das Muster „Network Router“ ersetzt die verschiedenen SNMP-bezogenen Probes zur Erkennung von Routern und Switches. Eine Liste der Muster finden Sie unter Verfügbare Discovery-Muster.

SNMP-Probe-Parameter

Dies ist die Liste der Parameter, die an SNMP-Probes übergeben werden kann.

Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

Parameter	Beschreibung	Standardwert
oid_spec_list	Eine Liste mit OID-Spezifikationen, eine pro Zeile. Jede Spezifikation muss eines der folgenden beiden Formate aufweisen:	erforderlich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung	Standardwert
	• *walk {OID}*: Durchläuft die OID und alle untergeordneten Elemente • *table {OID} {OID Children}*: Durchläuft alle Einträge in der Tabelle und gibt nur die angegebenen untergeordneten Elemente zurück (zum Beispiel „iso.org.dod.internet“) {OID Child} bezieht sich auf eine kommagetrennte Liste von untergeordneten Knoten in den Einträgen für die angegebene Tabelle. Beispiel: „ifEntry.ifIndex,ifEntry.ifDescr,ifEntry.ifType“ sind untergeordnete OID-Elemente der Tabelle „iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable“. Der Einfachheit halber kann das Präfix des Tabelleneintrags weggelassen werden. (Die vorherigen untergeordneten Elemente können als „ifIndex,ifDescr,ifType“ angegeben werden.) Alle untergeordneten Elemente können einen Filterqualifizierer in Klammern einschließen. Beispiel: Das untergeordnete Element „entPhysicalContainedIn(=0)“ gibt zurückgegebene Tabelleneinträge nur an, wenn der Wert von „entPhysicalContainedIn“ gleich 0 ist. Die im Ausdruck unterstützten Operatoren lauten wie folgt: • `=` : ist gleich • `!=` : ist nicht gleich • `#` : enthält Wenn mehrere untergeordnete Elemente über einen Filterausdruck verfügen, wird der Eintrag bei einer Übereinstimmung mit einem der untergeordneten Elemente gelesen. Alle Inhalte einschließlich und hinter „//“ werden ignoriert (Kommentare). Alle OIDs, die nicht mit „1.3.6.1“ oder „iso.org.dod.internet“ beginnen, beginnen der Einfachheit halber automatisch mit „1.3.6.1“.	
Quelle	IP-Adresse oder Hostname des Geräts, auf dem SNMP abgefragt werden soll	erforderlich
index	Der nach der Community-Zeichenfolge anzuwendende Index zur Indizierung der Community-Zeichenfolge im Cisco-Stil (für VLAN-Abfrage)	0
credential_id	Die sys_id einer bestimmten Anmeldeinformation, die bevorzugt zu verwenden ist. Dieser Parameter ist nur zum internen Gebrauch bestimmt und wird nicht unterstützt.	keine
credential_tag	Das Anmeldeinformations-Tag, das verwendet werden muss. Dieser Parameter ist nur zum internen Gebrauch bestimmt und wird nicht unterstützt.	keine
timeout	Zeitüberschreitungswert (in Millisekunden) für die Wartezeit auf eine Antwort anstelle des Standardwerts.	1500

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung	Standardwert
	Sie können diesen Parameter verwenden, um den Konfigurationsparameter *mid.snmp.request.timeout* des SNMP-MID Servers zu überschreiben. **Hinweis:** Wenn *use_getbulk* auf *true* festgelegt ist, gilt der Zeitüberschreitungswert für eine einzelne GETBULK-Anforderung.	
established_session_timeout	Intervall (in Millisekunden), über das auf eine Antwort gewartet wird, nachdem mindestens eine Antwort empfangen wurde. Längere Werte können zur Erfassung vollständiger und genauer Daten nützlich sein. Sie können diesen Parameter verwenden, um den Konfigurationsparameter *mid.snmp.session.timeout* des SNMP-MID Servers zu überschreiben.	500
debug	Aktiviert die Debug-Protokollierung Legen Sie diesen Parameter für den Debug-Modus auf „true“ fest.	false
request_interval	Intervall (in Millisekunden) zwischen aufeinanderfolgenden Anforderungen für eine OID, wenn keine Antwort empfangen wurde, bis der Zeitüberschreitungswert (oder established_session_timeout) erreicht wird. Wenn dieser Wert mindestens auf den Wert für die Zeitüberschreitung (oder established_session_timeout) festgelegt ist, wird nur eine einzelne Anforderung für eine bestimmte OID gesendet. Wenn Sie den Wert für die Zeitüberschreitung (oder established_session_timeout) ändern, passen Sie request_interval gleichzeitig an, um zu vermeiden, dass zu viele oder zu wenige Anforderungen für dieselbe OID gesendet werden, je nachdem, was für eine bestimmte Umgebung angemessen ist.	400
request_delay	Intervall (in Millisekunden) zwischen dem Empfang einer Antwort und der Übertragung der nächsten Anforderung. Der Standardwert ist 0 (keine Verzögerung). Dieser Wert kann festgelegt werden, um die Gesamtrate einer SNMP-Abfrage zu verlangsamen.	0
result_format	Gibt JSON-formatierte Nutzlasten für die folgenden Probes zurück: • SNMP - F5 BIG-IP - System • SNMP - Netscaler - System • SNMP - Routing Dieser Parameter gibt Daten in einem kompakteren Format zurück, um Sensorausfälle oder Speicherprobleme auf einem Knoten zu verhindern, wenn die Nutzlast groß wird. Ändern Sie diesen Wert nicht, und löschen Sie diesen Parameter nicht. **Warnung:** Die Verwendung dieses Parameters mit anderen Probes führt zum Ausfall des Sensors.	JSON

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung	Standardwert
use_getbulk	Aktiviert die Verwendung von SNMP GETBULK-Anforderungen zum Abrufen von tabellarischen Daten von SNMP-Geräten, anstatt mehrere SNMP GETNEXT-Anforderungen zu verwenden. Für tabellarische Daten ist GETBULK effizienter. Unabhängig vom Anforderungstyp geben bestimmte Geräte möglicherweise keine Ergebnisse zurück, wenn sie mit anderen Aufgaben beschäftigt sind. Dieser Parameter wird zur Konfiguration auf Probe-Ebene verwendet. GETBULK kann auch für einen einzelnen MID Server oder global für alle MID Server festgelegt werden. Einstellungen werden in ihrer Prioritätsfolge aufgelistet: • Parameter für SNMP-Probes • MID Server-Konfigurationsparameter • MID Server-Eigenschaften Die Parameter *established_session_timeout*, *request_interval*, und *request_delay* werden ignoriert, wenn *use_getbulk* auf **true** festgelegt ist. Stattdessen ist der Parameter *retries* verfügbar. Die Konfiguration der Zeitüberschreitung ist identisch mit *use_getscalar*. Standardmäßig verwenden die folgenden Probes GETBULK-Anforderungen (Parameterwert gleich *true*). • SNMP - Switch - Vlan • SNMP - Switch - BridgePortTable • SNMP - Switch - ForwardingTable • SNMP - Switch - SpanningTreeTable • SNMP - Network - ArpTable • SNMP - Layer 2 Protocol Caches • SNMP - F5 BIG IP - System (nur für Service Mapping-Kunden) **Hinweis:** Der *timeout*-Wert dieser Probes beträgt 5000.	false
use_getscalar	Ermöglicht das vereinfachten Abrufen und Verarbeiten von skalaren Werten von SNMP-Geräten. Die Parameter *established_session_timeout*, *request_interval* und *request_delay* werden ignoriert, wenn *use_getscalar* auf **true** festgelegt ist. Stattdessen sind die Parameter *retries* und *timeout* verfügbar. Die Konfiguration der Zeitüberschreitung ist identisch mit *use_getbulk*.	false
Wiederholungen	Die Anzahl der zusätzlichen Versuche, die Discovery unternimmt, um eine einzelne GETBULK-Anforderung (siehe *use_getbulk*) oder eine GETNEXT-Anforderung	2

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung	Standardwert
	abzuschließen, wenn der Parameter *use_getscalar* auf **true** festgelegt ist.	

MIB-Modul laden

Sie können ein zusätzliches Management Information Base-Modul (MIB) laden, indem Sie einen neuen ecc_agent_mib-Datensatz erstellen und die tatsächliche MIB-Datei an den Datensatz anhängen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
MIBs werden nur während des Starts von MID Servern geladen. Beim Starten des MID-Servers werden die folgenden MIB-Module geladen:

- Module, die mit der MID Server-Software gebündelt sind. Diese MIBs sind definierte Branchenstandards.
- Module, die in jeder Instanz enthalten sind. Diese MIBs werden vom Hersteller für Discovery bereitgestellt, um bestimmte Informationen von einem Gerät zu extrahieren.

Sie können alle Fehler im Zusammenhang mit dem Laden von MIB-Modulen im Agent-Protokoll anzeigen.

Hinweis: Durch das Hinzufügen einer MIB-Datei können Sie OID-Werte zusätzlich zur numerischen Notation in Zeichenfolgen-/ASN-Schreibweise anfordern. Es wird jedoch nicht garantiert, dass zusätzliche Informationen abgerufen werden. Es bietet einfach eine andere Möglichkeit, neue OIDs zu definieren, die erkannt werden sollen.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **SNMP-MIBs**.
2. Überprüfen Sie, ob Abhängigkeiten erfüllt sind.
   Wenn die neue MIB Abhängigkeiten von anderen MIBs aufweist, muss die MIB, die die Abhängigkeit füllt, vorhanden sein, bevor Sie den neuen Datensatz erstellen. Durchsuchen Sie die vorhandenen MIBs, um sicherzustellen, dass die erforderlichen MIBs bereits geladen sind. Ist dies nicht der Fall, führen Sie das folgende Verfahren aus, um sie der Instanz ebenfalls hinzuzufügen.
3. Klicken Sie auf **Neu**, um einen neuen Datensatz zu erstellen.
   Das Formular „MIB-Datei für MID Server“ wird geöffnet, um einen neuen ecc_agent_mib-Datensatz zu erstellen.
4. Verwenden Sie die folgenden Informationen, um das Formular auszufüllen:
   - **Name**: Name der MIB
   - **Version**: Version der MIB
   - **Quelle**: Geben Sie in diesem Feld an, wo die MIB abgerufen wurde, zum Beispiel eine URL.
   - **Beschreibung**: Die Beschreibung, die in der Tabelle ecc_agent_mib angezeigt wird
   - **Aktiv**: Dieses Kontrollkästchen gibt an, ob das MIB-Modul in der Instanz aktiviert oder deaktiviert ist.
5. Klicken Sie auf das Symbol „Anlage hinzufügen“ ( ) oben rechts, um die tatsächliche MIB-Datei an den neuen Datensatz anzuhängen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der MIB-Name muss mit einem alphabetischen Zeichen beginnen. Die verbleibenden Zeichen müssen eines der folgenden sein: alphanumerisch, Bindestrich (-) oder Unterstrich (_). Der Dateiname darf keine Erweiterung aufweisen. Sie können die vorhandenen MIBs für Beispiele referenzieren. Verwenden Sie den tatsächlichen Namen der MIB sowohl für den Namen des MIB-Datensatzes als auch für den Namen des Anhangs. Dies ist jedoch nicht erforderlich.

6. Wählen Sie **Absenden**.

Nächste Maßnahme

Aktualisieren Sie das entsprechende Muster oder die entsprechende Probe, um die spezifischen OID-Werte abzufragen, die in der neuen MIB definiert sind.

SNMP Probe MIB Module

Ein MIB-Modul (Management Information Base) ist eine Datenbank zur Verwaltung von Elementen in einem Netzwerk.

Ihre Instanz enthält Objektdefinitionen aus den gängigsten MIB-Dateien (Management Information Base). Prüfen Sie vor dem Hinzufügen einer neuen Objektdefinition die Liste der MIB-Module, um sicherzustellen, dass die Objektdefinitionen noch nicht verfügbar sind. Die Instanz enthält Objektdefinitionen aus den gängigsten MIB-Dateien (Management Information Base). Die Tabelle „MIB-Datei für MID Server“ [ecc_agent_mib] ist nach Domänen getrennt. Sie können Versionen dieser Richtlinien erstellen, die nur ein MID-Server aus derselben Domäne verwenden kann. Anweisungen hierzu finden Sie unter Domain Separation für MID-Server einrichten .

Die folgende Tabelle enthält die MIBs, die automatisch geladen werden. Die mit dem MID Server gebündelten MIBs sind in der Instanz nicht sichtbar. Die MIBs in der Tabelle ecc_agent_mib sind standardmäßig in der Instanz enthalten und können im angezeigt werden **MID-Server** > **SNMP-MIBs** Modul.

Wichtig: MIB-Dateien in einer ServiceNow-Instanz besitzen keine Dateierweiterung. Wenn die Systemeigenschaft **glide.attachment.extensions** in Ihrer Instanz eine Liste mit für den Import zulässigen Dateierweiterungen enthält, werden MIB-Dateien nicht geladen. Um sicherzustellen, dass MIB-Dateien geladen werden können, fügen Sie den Dateien vor dem Laden eine temporäre Erweiterung hinzu, zum Beispiel **.mib**, und listen Sie diese Erweiterung dann in der Eigenschaft **glide.attachment.extensions** auf. Wenn Sie die Datei laden, entfernt eine Geschäftsregel, die die **Compliance der MIB-Dateinamen** sicherstellt, diese Erweiterung aus der Datei, bevor sie den Datensatz in die Tabelle ecc_agent_mib einfügt.

MIB-Modul (Management Information Base)

Gebündelt mit dem MID Server	Enthalten in der Instanz
ATM-MIB	A10 AX MIB
BRIDGE-MIB	A10 COMMONS MIB
DISMAN-EVENT-MIB	CISCO-SMI
ENTITY-MIB	CISCO-STACK-MIB
EtherLike-MIB	CISCO-TC
FRAME-RELAY-DTE-MIB	CISCO-VTP-MIB
HOST-RESOURCES-MIB	F5-BIGIP-COMMON-MIB
HOST-RESOURCES-TYPES	F5-BIGIP-LOCAL-MIB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MIB-Modul (Management Information Base) (Fortsetzung)

Gebündelt mit dem MID Server	Enthalten in der Instanz
IANA-ADDRESS-FAMILY-NUMBERS-MIB	F5-BIGIP-SYSTEM-MIB
IANAifType-MIB	FOUNDRY-SN-AGENT-MIB
IP-MIB	FOUNDRY-SN-ROOT-MIB
IP-FORWARD-MIB	LanMgr-Mib-II-MIB
IPMROUTE-STD-MIB	MSFT-MIB
IPV6-MIB	NetWare-Host-Ext-MIB
ISDN-MIB	NetWare-Server-MIB
RFC-1212	PowerNet-MIB
RFC-1215	QMS-MIB
RFC1155-SMI	
RFC1213-MIB	
RFC1398-MIB	
RFC1406-MIB	
RMON2-MIB	
RSVP-MIB	
SNMPv2-SMI	
SNMPv2-TC	
UPS-MIB	

Probe „SSHCommand“

Eine Probe mit *SSHCommand* als Name für das ECC-Warteschlangenthema führt einen Shell-Befehl auf dem Zielhost aus und gibt die resultierende Ausgabe an den Sensor zurück.

Discovery unterstützt sh- und bash-Befehle (Bourne-Shell und Bourne-again-Shell). Geben Sie Shell-Skriptbefehle in das Feld *ECC-Warteschlangenname* der Probe ein. Das Shell-Skript kann Variablen und Dateivorgänge verwenden, die von der UNIX-Ziel-Shell unterstützt werden.

- Die SSH-Engine ist bei neuen Instanzen standardmäßig aktiviert.
- Kunden mit aktualisierten Instanzen können ServiceNow SSH für eine bestimmte Probe manuell aktivieren, indem sie den Parameter use_snc_ssh auf „true“ setzen. Alternativ können Sie SSH für alle Probes auf dem MID Server aktivieren, indem Sie den MID Server-Parameter mid.ssh.use_snc auf „true“ setzen.

Hinweis: Um Netzwerkgeräte wie Router und Switches zu erkennen, verwenden Sie SNMP-Anmeldeinformationen und keine SSH-Anmeldeinformationen.

Parameter für SSHCommand

Für die Probe „SSHCommand“ sind mehrere Parameter verfügbar.

Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametertabelle

Parameter	Beschreibung
allow_unsupported_shells	Ermöglicht einem Probe-Designer, einen Befehl auf einem Gerät ohne unterstützte Shell auszuführen. Ohne Shell gilt: • Es können keine Pfadinformationen angegeben werden. • Es können keine Skripts ausgeführt werden, da keine Möglichkeit besteht, Skriptparameter zu verarbeiten. • Der im Feld **ECC-Warteschlangenname** des Probe-Formulars angegebene Text ist der Rohbefehl, der auf dem Gerät ausgeführt wird. Beispielsweise können Sie eine Probe entwerfen, um die Version eines Cisco-Switch anzuzeigen, auf dem NX-OS ausgeführt wird. Der Befehl, den der Switch versteht, lautet `show version`. Um dies zu erreichen, fügen Sie den Befehl `show version` in das Feld **ECC-Warteschlangenname** ein und fügen den Parameternamen `allow_unsupported_shells` mit dem Wert **true** hinzu. Dieser Parameter ist nur für `sncssh` wirksam. Für j2ssh wird er nicht unterstützt. Die derzeit unterstützten Shells lauten sh, bash, ksh, csh und tcsh. • Typ: Zeichenfolge, „true“ oder „false“ • Standardwert: false
Quelle	[Erforderlich] Gibt den ersten Host an, zu dem eine Verbindung hergestellt werden soll • Typ: Zeichenfolge (URL) • Standardwert: keiner
port	Gibt den Zielport für die Verbindung an • Typ: Ganzzahl (Port) • Standardwert: 22
debug	Gibt an, ob SSH-Debug-Informationen in die Protokolldatei geschrieben werden sollen. Die Parameterverwendung hängt davon ab, ob der ServiceNow-SSH-Client aktiviert ist. Wenn der SSH-Client von ServiceNow aktiviert ist, funktioniert dieser Parameter wie folgt: • Typ: Zeichenfolge • Standardwert: false Die folgenden Zeichenfolgenwerte sind für den SSH-Client von ServiceNow gültig:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametertabelle (Fortsetzung)

Parameter	Beschreibung
	◦ true: Aktiviert SSH-Debug-Informationen in der Protokolldatei. ◦ false: Deaktiviert SSH-Debug-Informationen in der Protokolldatei. ◦ <IP-Adressen>: Gibt an, für welche IP-Bereiche SSH-Debug-Informationen in der Protokolldatei aktiviert werden sollen. Sie können IP-Adressen in den folgenden Formaten eingeben: ▪ Ein IP-Bereich, der durch einen Schrägstrich und die Anzahl der Bits im Subnetz definiert ist. Beispielsweise durchsucht der String 10.10.10.0/24 24-Bit-IP-Adressen von 10.10.10.0 bis 10.10.10.254. ▪ Ein IP-Bereich, der durch einen Bindestrich definiert wird. Der String 10.10.11.0-10.10.11.165 durchsucht beispielsweise die IP-Adressen von 10.10.11.0 bis 10.10.11.165. ▪ Eine durch Kommas getrennte Liste bestimmter IP-Adressen. Zum Beispiel durchsucht der String 10.10.11.200.10.10.11.235 die IP-Adressen 10.10.11.200 und 10.10.11.235. ◦ deferred: Gibt an, dass SSH-Debug-Informationen im Speicher protokolliert werden sollen, sofern keine Fehler oder Warnungen auftreten. Wenn ein Fehler oder eine Warnung auftritt, veröffentlicht die Plattform die Debug-Informationen in der Protokolldatei. Dadurch wird sichergestellt, dass nur der Teil der Protokolldatei aufgezeichnet wird, der sich auf den Fehler oder die Warnung bezieht. Wenn kein Fehler oder keine Warnung erkannt wird, löscht die Plattform die nicht verwendeten Protokolldaten aus dem Speicher, sobald die Sitzung geschlossen wird. In jeder Sitzung werden bis zu 1000 Protokollnachrichten gespeichert. Wenn die Sitzung 1000 Protokollnachrichten überschreitet, verwirft das verzögerte Protokoll die älteste Protokollnachricht, um Platz für die neueste Protokollnachricht zu schaffen. Wenn der SSH-Client von ServiceNow deaktiviert ist, aktiviert bzw. deaktiviert dieser Parameter SSH-Debug-Informationen in der Protokolldatei: • Typ: true | false • Standardwert: false
debug_ssh	Gibt an, ob der veraltete SSH-Client Debug-Informationen in die Protokolldatei `agent/logs/agent.log` schreibt. **Hinweis:** Diese Protokolldatei kann schnell größer werden und sollte deaktiviert werden, wenn sie nicht benötigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametertabelle (Fortsetzung)

Parameter	Beschreibung
	Der ServiceNow-SSH-Client verwendet diesen Parameter nicht. • Typ: true | false • Standardwert: false
timeout	Legt den Socket-Verbindungstimeout für den veralteten SSH-Client fest. Der ServiceNow-SSH-Client verwendet diesen Parameter nicht. • Typ: Ganzzahl (Millisekunden) • Standardwert: 60.000
path_override	Gibt an, wie die Standardpfade geändert werden können, die vor der Ausführung eines Befehls festgelegt wurden. Geben Sie einen oder mehrere durch Doppelpunkt (:) getrennte Überschreibungspfade ein. Der Standardpfad ist / usr/sbin: /usr/bin:/bin:/sbin. Der SSH-Client von ServiceNow akzeptiert die folgenden Präfixe vor dem Wert path_overide. • append: Hängt den Überschreibungspfad an das Ende des Hostpfads an. Dies ist das Standardverhalten. • replace: Ersetzt den Hostpfad durch den Wert path_overide. • prepend: Stellt den Überschreibungspfad dem Hostpfad voran. • Typ: Zeichenfolge (eine durch Doppelpunkte getrennte Liste von Verzeichnissen) • Standardwert: keiner
keyboard_interactive	Bestimmt, ob der SSH-Anmeldemodus keyboard_interactive erzwungen wird • Typ: true | false • Standardwert: false
must_sudo	Bestimmt, ob SSH-Befehle über sudo ausgeführt werden **Hinweis:** Der Probe-Parameter „must_sudo“ wirkt sich auf alle Muster aus. Auf Unix- oder Linux-Hosts können bei der Musterausführung viele verschiedene Befehle ausgeführt werden, an einige darf kein sudo angehängt sein. • Typ: Wahr | Falsch • Standardwert: false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametertabelle (Fortsetzung)

Parameter	Beschreibung
run_in_terminal	Bestimmt, ob SSH-Befehle in einem SSH-Terminal ausgeführt werden • Typ: true | false • Standardwert: ◦ SSH-Client von ServiceNow: false ◦ Veralteter SSH-Client: true
set_path	Bestimmt, ob die Probe die PATH-Variable der Sitzung ändern darf. Standardmäßig wird die PATH-Variable während des Sitzungs-Setup auf `/usr/sbin:/usr/bin:/bin:/sbin` festgelegt. • Typ: true | false • Standardwert: true
rm_override	Überschreibt den Standardbefehl zum Entfernen `(/bin/rm -f)` mit dem angegebenen Wert • Typ: Zeichenfolge • Standardwert: keiner
use_snc_ssh	Aktiviert den SSH-Client von ServiceNow. Der SSH-Client von ServiceNow ist bei neuen Instanzen standardmäßig aktiviert. Durch das Aktivieren des SSH-Clients von ServiceNow wird der veraltete SSH-Client deaktiviert. • Typ: true | false • Standardwert: true
command_timeout_ms	Anzahl von Millisekunden, die ein SSH-Befehl ausgeführt werden darf, bevor eine Zeitüberschreitung auftritt (Standardeinstellung pro MID Server konfigurierbar). Der veraltete SSH-Client verwendet diesen Parameter nicht. • Typ: Ganzzahl • Standardwert: Wert des MID Server-Parameters mid.ssh.command_timeout_ms
channel_timeout_ms	Gibt den Zeitraum in Millisekunden an, die ein MID Server während der Verarbeitung eines SSH-Befehls auf Aktivität wartet. Wenn der MID Server im angegebenen Zeitüberschreitungsfenster keine Aktivität erkennt, beendet dieser Parameter den Befehl. • Typ: Ganzzahl (Millisekunden) • Standardwert: 300000 (5 Minuten)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parametertabelle (Fortsetzung)

Parameter	Beschreibung
preserve_sudo_environment	Gibt an, ob Sudo verwendet werden soll, um die Umwelt für SSH zu erhalten. Dieser Parameter ist nur wirksam, wenn die sudo-Umgebung auf dem geprüften Host den Schalter `-E` unterstützt. • Typ: true | false • Standardwert: false
credentials_debug	Zeigt einen <credentials_debug>-Abschnitt in der ECC-Warteschlange an, der Ihnen bei der Behebung von Problemen mit den Anmeldeinformationen helfen kann. Wenn Sie diese Eigenschaft auf „true“ setzen, werden Informationen zur Behandlung von Problemen mit Anmeldeinformationen in der ECC-Warteschlange ausgegeben, auch wenn die Anmeldeinformationen erfolgreich sind. Weitere Informationen finden Sie unter Problembehandlung bei Anmeldeinformationen .

Pfad für SSHCommand

Die Probe „SSHCommand“ berechnet den Standardpfad aus den folgenden Quellen.

- MID Server-Parameter: mid.ssh.path_override
- Parameter für die Probe „SSH Command“: path_override
- Standardpfad des Benutzers: Shell-Konfigurationsdatei

Wenn Sie den Parameter zum Überschreiben des MID Server-Pfads festlegen, hängt Discovery diesen Pfad an den Standardpfad an. Wenn Sie den Probe-Pfadparameter festlegen, verwendet Discovery diesen Pfad anstelle des Standardpfads. Discovery hängt den Standardausführungspfad eines Benutzers stets an die MID Server- und Probe-Parameterpfade an.

Standardpfad

Standardmäßig sucht der MID Server unter den folgenden Pfaden nach SSH-Befehlen:

- /usr/sbin
- /usr/bin
- /bin
- /sbin

Shell-Skriptoptionen

Die Probe „SSHCommand“ unterstützt die folgenden Skripting-Optionen im Feld *ECC-Warteschlangenname*.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle der Shell-Skripting-Optionen

Summary	Syntax	Beschreibung
Variable	${variable}	Ersetzt das Token durch den Wert der Variablen. Beispielsweise gibt ${catalina_home} den Installationsort eines Tomcat-Servers an.
Datei einschließen	${File:file_name.sh}	Behandelt den Inhalt der angegebenen Datei als Shell-Skript. Beispielsweise führt ${File:findcat.sh} das Shell-Skript findcat aus.

SSH-Befehle, die während der probebasierten Discovery keinen privilegierten Benutzer erfordern

In diesen Tabellen werden die SSH-Befehle angezeigt, die während der Horizontal-Discovery von den Probes Discovery auf Zielgeräten ausgeführt werden. Diese SSH-Befehle erfordern keine erhöhten Berechtigungen zum Ausführen.

Betriebssysteme

Informationen zu den von Service-Mapping während der Erkennung von oben nach unten verwendeten Befehlen finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern und Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern.

AIX-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
lsattr	*-El sys0 -a modelname -F value*
lslpp	*-Lc*
/etc/ifconfig	*-au; netstat -in*
instfix	*-i | grep AIX_ML*
oslevel	*-r*
echo `lsattr	*-El sys0 -a systemid | cut ...*

Linux-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
arp	*-n*
bash	*variable*
cat	*/sys/hypervisor/compilation/compiled_by*
cat	*/sys/devices/virtual/dmi/id/product_uuid*
grep MemTotal	*/proc/meminfo*
ifconfig	*-a && route -n*
sh	*variable*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HP-UX-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
ps	*-elx*
echo itick_per_usec/D	*| adb -k /stand/vm...*
sh	*variable*
Modell	
uname	*-i*
swlist	*-l product | grep -v 'PH._'*
echo 'memory_installed_in_machine/D'	*| a...*

Solaris-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
kstat	*cpu_info*
pkginfo	*-l | egrep 'PKGINST|NAME|CATEGO...*
prtconf	*| grep Memory*
ifconfig	*-a; netstat -pnr -f inet*
arp	*-an*
showrev	*-p*
sneep	*-T*
bash	*variable*

Mac-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
system_profiler	• *SPHardwareDataType SPMemoryDataType -xml* • *SPSerialATADataType SPSASDataType SPFireWireDataType -xml* • *SPNetworkDataType -xml;ifconfig | grep '|Winet6|W'* • *SPSoftwareDataType -xml* • *SPHardwareDataType -xml*
letzte	*| grep -m 1 console*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
ps	*awwxo pid,ppid,command | sed -n '/<defunct>/!p'*
sh	*variable*
cat	*variable*
Variable	*-version*
uname	*-a*
df	*-kP*
uptime;env	*LC_ALL=C date '+%a %b %e %H:%M %Z %Y'*

Webserver

Apache-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
httpd_command	*-V*

Tomcat-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
cat	*variable*
find -L ${dirname}	*-name web.xml -print 2>/dev/null*

NGINX-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	• *get-nginxcfg* • *get-nginx-ver*

Datenbanken

Oracle-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SQL-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
cat	*variable*
Variable	*-V*

HBase-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
cat	*variable*
sh	*variable*
Variable	*-lv | grep ^${processID}*

Anwendungen

ESX - OS-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*

F5 - OS-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*

HAProxy-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
Variable	*-v*

JBoss-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
find	*-name web.xml -print*
cat	*variable*

KVM-Befehle

Befehl (ECC-Warteschlangenname)	Parameter
sh	*variable*
virsh	*Various capabilities*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SSH-Befehle, die während der probebasierten Discovery einen privilegierten Benutzer erfordern

Diese Tabellen zeigen die SSH-Befehle an, die von den Probes Discovery während der Horizontal-Discovery ausgeführt werden. Zur Ausführung dieser SSH-Befehle sind erweiterte Berechtigungen erforderlich.

Betriebssystembefehle, die erweiterte Rechte erfordern

Diese Beispiele setzen voraus, dass der Benutzername **Disco** lautet. Ersetzen Sie den tatsächlichen Anwendernamen, und vergewissern Sie sich, dass die Pfade für die Befehle mit den Pfaden im System übereinstimmen.

Hinweis: Sudo-Befehle funktionieren nicht mit Anmeldeinformationen für private Schlüssel, da kein Passwort vorhanden ist, das für den Sudo-Befehl angegeben werden muss. Eine Lösung ist das Hinzufügen der Option *NOPASSWD* zur Sudo-Konfiguration. Zum Beispiel könnten Sie Folgendes eingeben: `disco ALL=(root) NOPASSWD:/usr/sbin/dmidecode,/usr/sbin/lsof,/sbin/ifconfig`.

Informationen zu Befehlen, die keine erweiterten Rechte erfordern, finden Sie unter SSH-Befehle, die während der probebasierten Discovery keinen privilegierten Benutzer erfordern.

Informationen zu den von Service-Mapping während der Erkennung von oben nach unten verwendeten Befehlen finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern und Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern.

UNIX und Linux

Befehl	Zweck
HP-UX	
adb	Erfasst CPU-Geschwindigkeit und Speicher. **Zeilenbeispiel für /etc/sudoers**: `Disco ALL=(root) /usr/bin/adb`
Alle *Linux*	
dmidecode	Sammelt Informationen über die Hardware, einschließlich der Seriennummer des Motherboard. **Zeilenbeispiel für /etc/sudoers**: `Disco ALL=(root) /sbin/dmidecode`
fdisk	Sammelt die Informationen über Datenträger und Größen im System. **/etc/sudoers Zeilenbeispiel**: `Disco ALL=(root) /usr/bin/fdisk -l`
multipath	Erfasst Gerätezuordnungen für MultiPath Input Ausgabe (MPIO). **/etc/sudoers-Zeilenbeispiel**: `Disco ALL=(root) /usr/bin/multipath -ll`
Linux **und** *Solaris*	
dmsetup	Untersucht ein Volume auf niedriger Ebene. **Beispiel für die Zeile „/etc/sudoers“**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

UNIX und Linux (Fortsetzung)

Befehl	Zweck
	• `Disco ALL=(root) /usr/bin/dmsetup table *` • `Disco ALL=(root) /usr/bin/dmsetup ls`
Alle *UNIX*-Versionen	
lsof	Ermittelt die Beziehung zwischen Prozessen und den Verbindungen, die zum System hergestellt werden. **Zeilenbeispiel für /etc/sudoers**: `Disco ALL=(root) /sbin/lsof`
oratab	Gewährt Lesezugriff auf die oratab-Datei zum Suchen der Oracle -Startseite und der Profildatei.
Solaris	
iscsiadm	Ruft qualifizierte iSCSI-Namen (IQNs) ab. **/etc/sudoers-Zeilenbeispiel**: `${sudo:iscsiadm list target -S}`
fcinfo	Ruft World Wide Port Names (WWPNs) für Ports ab. **/etc/sudoers-Zeilenbeispiel**: `${sudo:fcinfo remote-port -sl -p $port}`
prtvtoc	Liefert Informationen zu Datenträgerpartitionen. **Zeilenbeispiel für /etc/sudoers**: `Disco ALL=(root) /usr/bin/prtvtoc`
/usr/bin/ps	Führt laufende Prozesse auf. Alternativ zur Ausführung mit Root-Zugriff können Sie die Rolle proc_owner hinzufügen **Zeilenbeispiel für /etc/sudoers**: `Disco ALL=(root) /usr/bin/ps`
/usr/ucb/ps	Führt laufende Prozesse auf. Fügen Sie als Alternative zur Ausführung mit Stammzugriff eine proc_owner-Rolle hinzu. Die Verwendung des Befehls `/usr/ucb/ps` ist ab Solaris 11 veraltet. Da Discovery die Verwendung dieses Befehls für alle Solaris -Versionen erfordert, müssen Sie das ucb-Dienstprogramm manuell auf Solaris 11-Systemen installieren. Anweisungen dazu finden Sie in KB0564262 . **Zeilenbeispiel für /etc/sudoers**: `Disco ALL=(root) /usr/ucb/ps`

vCenter-Probes und Probe-Parameter

vCenter-Probes scannen virtuelle Computer mit der Produkt-Suite vSphere von VMware. Jede Probe scannt nach verschiedenen Arten von Daten wie Netzwerke, NICs und Tags. Die Unterstützung für die Probe „VMware - vCenter“, die in früheren Releases alle vCenter-Objekte erkannte, wurde ab dem Istanbul-Release eingestellt, und sie wurde durch mehrere Probes ersetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upgradebedingte Änderungen

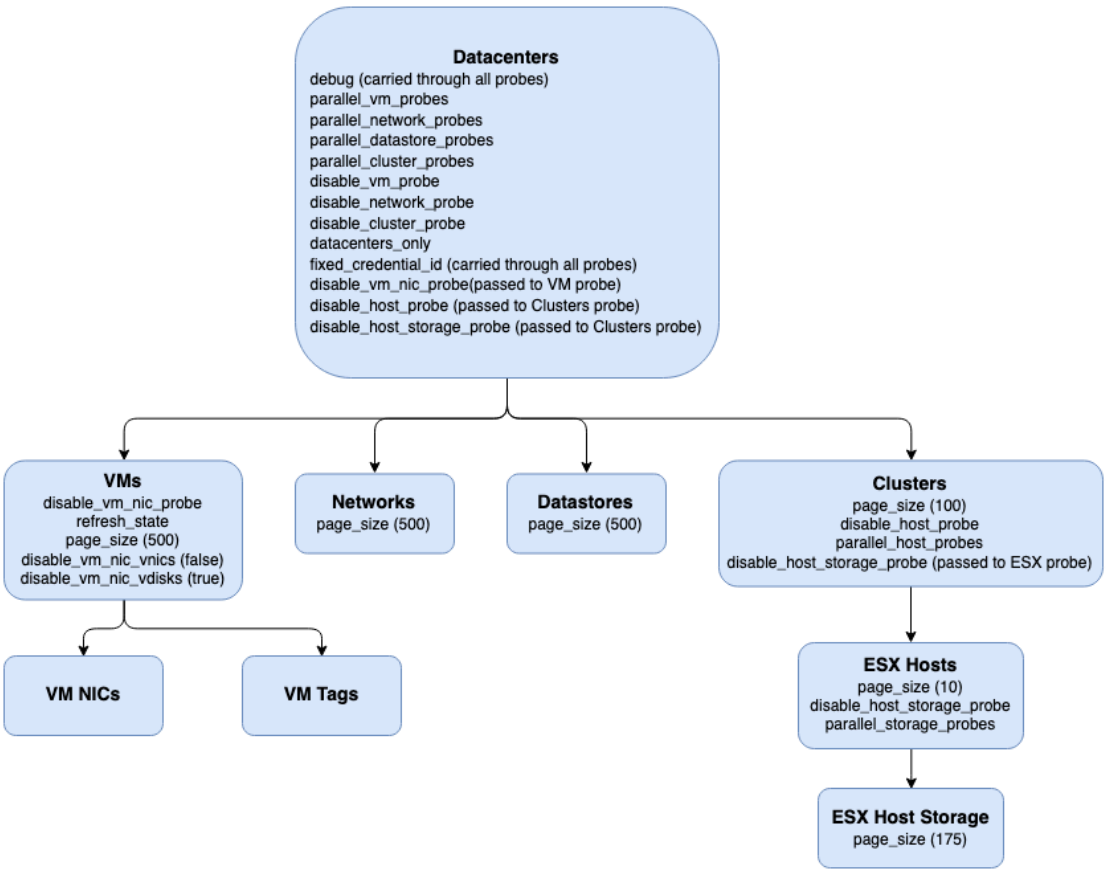
In upgegradeten Systemen sind der Prozessklassifizierer vCenter und die Port-Probe vmapp so konfiguriert, dass sie den Probe „VMware -vCenter Datacenters“ auslösen. Diese Probe löst dann die Probes aus, die einzelne vCenter-Objekte wie Hosts, Speicher und Datenspeicher erkennen. Die veraltete Probe „VMware - vCenter“ befindet sich noch im System, wird jedoch in der aktualisierten Instanz nicht mehr ausgelöst.

Verfügbare vCenter-Probes und Probe-Parameter

Mit vCenter-Probe-Parametern können Sie die Probes für die Objekte deaktivieren, an deren Erkennung Sie nicht interessiert sind. Sie können auch die Größe der Nutzlast einer Probe reduzieren, indem Sie eine Seitengröße angeben.

Wichtig: Beachten Sie vor dem Deaktivieren einer Probe mögliche Abhängigkeiten der Probe. Wenn die Probe, die Sie deaktivieren, eine andere Probe auslöst, wird auch die abhängige Probe deaktiviert und kann keine Daten erfassen.

Beziehung von vCenter-Elementen zu Probe-Parametern



Die folgenden Parameter sind für vCenter-Probes verfügbar.

Hinweis: Sofern nicht anders angegeben, werden diese Parameter in der Plattform standardmäßig nicht festgelegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vCenter-Probe-Parameter

Probe	Parameter
VMware – vCenter-Rechenzentren	• datacenter_only (Cloud Provisioning and Governance) • debuggen • disable_vm_probe • disable_network_probe • disable_datastore_probe • disable_cluster_probe • datacenters_only • fixed_credential_id (Cloud Provisioning and Governance) • disable_vm_nic_probe • disable_host_probe • disable_host_storage_probe • vcenter_timeout: Standard 10.000 Millisekunden (10 Sekunden)
VMWare – vCenter-VMs	• disable_vm_nic_probe • disable_vm_nic_vnics (auf **false** gesetzt) • disable_vm_nic_vdisks (auf **wahr** – nur für Discovery – und **falsch** festgelegt, wenn Cloud Provisioning and Governance aktiviert ist) • disable_vm_tags_probe • refresh_state (Cloud Provisioning and Governance) • page_size (100) **Hinweis:** Bei den Einstellungen für die Parameter „vnics“ und „vdisks“ wird das Standardverhalten von vCenter Discovery beibehalten.
VMware – vCenter-VM-Tags*	keine
VMware – vCenter-VM-NICs	keine
VMware – vCenter-Netzwerke	page_size (500)
VMware – vCenter-Datenspeicher	page_size (500)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vCenter-Probe-Parameter (Fortsetzung)

Probe	Parameter
VMware – vCenter-Cluster	• disable_host_probe • disable_host_storage_probe • page_size (1000)
VMware – vCenter-ESX-Hosts	• disable_host_storage_probe • page_size (10)
VMware – vCenter-ESX-Host-Speicher	page_size (175)
VMware – vCenter-ESX-Host-Lizenz	keine
VMware vCenter-VM-Leistung	Diese Probe stützt sich auf die für vCenter konfigurierten Statistikintervalle. Standardmäßig sind die folgenden Intervalle verfügbar: • 5 Minuten (300 Sekunden) – diese Daten werden 24 Stunden lang gespeichert. • 30 Minuten (1.800 Sekunden) – diese Daten werden eine Woche lang gespeichert. • 2 Stunden (7.200 Sekunden) – diese Daten werden einen Monat lang gespeichert. • 24 Stunden (86.400 Sekunden) – diese Daten werden ein Jahr lang gespeichert. Die folgenden Eigenschaften unterstützen diese Probe: • data_sampling_weeks_frame: Zeitraum, für den die Daten von der Probe abgerufen werden, in Wochen • data_sampling_minutes: Zeit zwischen der Entnahme der Datenstichproben • Metriken: erfasste Metriken (CPU/ Arbeitsspeicher/Netzwerk/Laufwerk) Diese Probe wird nur von Bewertung der Cloud-Migration verwendet. **Wichtig:** Um die Standardwerte für diese Probe zu ändern, stimmen Sie sich mit dem Administrator ab, der für die vCenter-Verwaltung verantwortlich ist. Weitere Informationen finden Sie in der VMware-Dokumentation .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

* Weitere Informationen finden Sie unter VMware-Tags.

Beachten Sie beim Festlegen dieser Parameter Folgendes:

- **Deaktivierung**: Sie deaktivieren Probes, indem Sie den Parameter in der auslösenden Probe festlegen. Beispiel: Wenn Sie an der Erkennung von Speicher nicht interessiert sind, legen Sie den Parameter *disable_host_storage_probe* in der Probe „VMWare - vCenter ESX Hosts“ auf **true** fest.
- **Seitengröße**: Der Parameter für die Seitengröße steuert die Anzahl der mit einer einzelnen Probe zu erkennenden CIs. Verwenden Sie diesen Parameter, um die Größe der Nutzlast zu begrenzen, indem die Anzahl der vCenter-Elemente reduziert wird, die von einer Probe gleichzeitig erkannt werden. Die in Klammern angegebene Seitengröße entspricht der Standardeinstellung im Basissystem.
- **Debugging:** Legen Sie den Parameter debug in der Probe „VMWare - vCenter Datacenters“ fest, um Debugging für alle vCenter-Probes zu ermöglichen. Beim Debugging werden die vCenter-Rohdaten in jeder Probe-Nutzlast zurückgegeben.

Benutzerdefinierte Probes mit der Discovery-Erweiterung für vCenter auslösen

Mit der Discovery-Erweiterung für vCenter können Sie zusätzliche Attribute von derzeit erkannten CI-Typen oder Attribute neuer CI-Typen erfassen, indem Sie benutzerdefinierte Probes von einem vorhandenen Sensor auslösen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Datensätze des vCenter-Sensors unterstützen die Auslösung benutzerdefinierter Probes. Diese verwenden bedingte Skripts zur Erfassung von Daten, die Discovery normalerweise nicht erfasst, oder zur Erkennung von selbst erstellten CI-Typen.

Wichtig: Die vCenter-Erweiterung dient zum Erstellen einer einzelnen benutzerdefinierten Probe, die die vorhandene Discovery-Funktionalität erweitert. Sofern Sie als Benutzer nicht mit erweitertem Skripting vertraut sind, versuchen Sie nicht, Ihre neue Probe/Ihren neuen Sensor so zu konfigurieren, dass eine zusätzliche Probe gestartet wird.

Prozedur

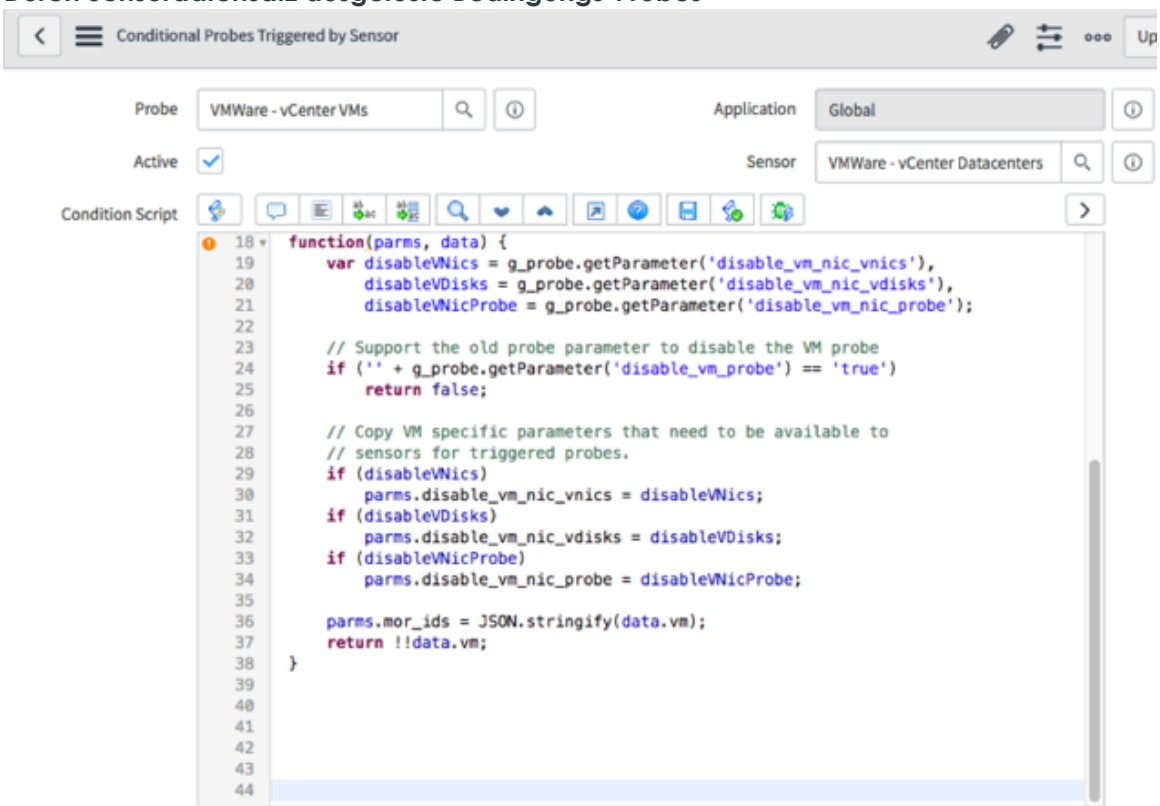
1. Navigieren zu **Alle** > **Discovery-Definition** > **Sensoren**.
2. Wählen Sie einen vCenter-Sensordatensatz aus.
   Es ist wichtig, eine neue Probe zum richtigen Zeitpunkt auszulösen. Wenn Sie beispielsweise zusätzliche Informationen über virtuelle Computer in Ihrem Netzwerk erkennen möchten, lösen Sie Ihre Probe über den Sensor „VMware - vCenter VMs“ aus. Wenn Sie Ihre benutzerdefinierte Probe über den Sensor „VMware - vCenter Datacenters“ auslösen, werden die neue Probe und die vorhandene VM-Probe parallel ausgeführt. Dadurch kann die Erstellung oder Aktualisierung von VM-Datensätzen verhindert werden.
3. Klicken Sie auf die zugehörige Liste **Auslösertests**.
4. Klicken Sie auf **Neu**, um eine neue Probe zu erstellen, die von diesem Sensor ausgelöst werden soll, oder auf **Bearbeiten**, um der Liste eine vorhandene Probe hinzuzufügen.
   Sie können auch einen vorhandenen Probe-Datensatz als Vorlage für eine eigene neue Probe verwenden, indem Sie den Datensatz öffnen und im Kontextmenü die Option **Einfügen und beibehalten** auswählen.
5. Klicken Sie auf das Informationssymbol rechts neben dem Probe-Namen, um den Datensatz **Durch Sensor ausgelöste Bedingungs-Probes** zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Zeigen Sie das Skript an.
   Das Skript übergibt die Argumente **parms** und **data** an die Funktion und verwendet dabei Werte, die vom auslösenden Sensor an sie übergeben wurden. Das Skript konfiguriert das Objekt **parms**, aus dem die Probe-Parameter abgeleitet werden. Das Skript gibt **true** zurück, um die Probe auszulösen, oder **false**, um sie abzubrechen.

   In diesem Beispiel sind die **parms**-Argumente des Sensors „VMware - vCenter Datacenters“ allesamt Probe-Parameter, die von der Probe „Datacenters“ unterstützt werden. Das Argument **data** ist ein Objekt, das bis zu 4 Arrays mit den Namen **vm**, **datastore**, **network** und **cluster** enthält.

Durch Sensordatensatz ausgelöste Bedingungs-Probes



Windows Probes und Berechtigungen

Discovery greift auf Geräte und Software zu, indem es als bestimmter Benutzer Befehle auf Computern Windows von ausführt.

Die meisten Probes erfordern Zugriff auf Windows-Klassen, -Eigenschaften und -Registrierungseinträgen. Bestimmte Probes erfordern zudem zusätzlichen Zugriff auf Windows-Verzeichnisse und -Ressourcen. Die Sicherheitsrichtlinien variieren je nach Organisation, daher gibt es keine bestimmte Rolle oder Berechtigung. Vergewissern Sie sich, dass der Benutzer Windows über `lokale Administratorrechte` für diese Windows -Komponenten verfügt.

Administrative Freigaben

Windows administrative Freigaben sind ausgeblendete Serverressourcen, die Discovery verwendet, um die Ergebnisse von Prozessen, die von bestimmten Probes ausgeführt werden, vorübergehend zu speichern. Die Skriptdatei MID-Server *`LaunchProc.psm1`* startet den Prozess, schreibt ihre Ausgabe in die Administratorfreigabe auf dem Computer und ruft dann die Ergebnisse für MID-Serverab. Der Zugriff auf administrative Freigaben ist auf Benutzer mit Administratorrechten für das Ziel beschränkt. Beispiel: Benutzer, lokal oder in der Domäne, die zur lokalen Administratorgruppe gehören.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ab Release New York rufen alle Windows -Proben, die das WMI-Protokoll verwenden, die Skriptdatei *LaunchProc.psm1* auf und schreiben standardmäßig in den Freigabeordner „admin$“. Wenn auf jedem Ziel Windows eine andere Netzwerkfreigabe bereitgestellt ist, kann der Ordner durch Aktualisieren der MID-Server-Eigenschaft *mid.powershell.target_base_dir*geändert werden.

Windows Klassen

Die meisten Windows-Probes greifen auf Windows-Klassen und -Eigenschaften zu, die in diesen Klassen enthalten sind. Einige Windows -Klassen geben keinen Datei-Namespace-Pfad an. Wenn kein expliziter Pfad angegeben ist, verwendet ServiceNow„`root\cimv2\`“. <Class> standardmäßig festgelegt.

Hinweis: Discovery von Cluster-VIP wird nicht unterstützt.

Windows Klassen

Probe	Windows-Klasse	Eigenschaft
Hyper-V - Cluster	`root\MSCluster\MSCluster_ClusterToNode`	**Abhängig**
Hyper-V - Cluster	`root\MSCluster\MSCluster_ClusterToNode`	**Antecedent**
Hyper-V - Cluster	`root\MSCluster\MSCluster_Resource`	**Typ**
Hyper-V - Resource Pools	`root\virtualization\Msvm_ResourcePool`	**ResourceSubType**
Hyper-V - Resource Pools	`root\virtualization\Msvm_ResourcePool`	**Name**
Hyper-V - Resource Pools	`root\virtualization\Msvm_ResourcePool`	**Kapazität**
Hyper-V - Resource Pools	`root\virtualization\Msvm_ResourcePool`	**AllocationUnits**
Hyper-V - Resource Pools	`root\virtualization\Msvm_ResourcePool`	**InstanceID**
Hyper-V - Virtual Machines	`root\virtualization \Msvm_MemorySettingData`	**VirtualQuantity**
Hyper-V - Virtual Machines	`root\virtualization \Msvm_ComputerSystem`	**ElementName**
Hyper-V - Virtual Machines	`root\virtualization \Msvm_ComputerSystem`	**TimeOfLastStateChange**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Hyper-V - Virtual Machines	root\virtualization\Msvm_LogicalDisk	**NumberOfBlocks**
Hyper-V - Virtual Machines	root\virtualization \Msvm_MemorySettingData	**AllocationUnits**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**ChassisSerialNumber**
Hyper-V - Virtual Machines	root\virtualization \Msvm_SyntheticEthernetPortSettingData	**InstanceID**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**BIOSGUID**
Hyper-V - Virtual Machines	root\virtualization \Msvm_ComputerSystem	**Beschreibung**
Hyper-V - Virtual Machines	root\virtualization \Msvm_ComputerSystem	**Name**
Hyper-V - Virtual Machines	root\virtualization\Msvm_LogicalDisk	**BlockSize**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**BIOSSerialNumber**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**BaseBoardSerialNumber**
Hyper-V - Virtual Machines	root\virtualization \Msvm_VirtualSystemSettingData	**SystemName**
Hyper-V - Virtual Machines	root\virtualization\Msvm_LogicalDisk	**ElementName**
Hyper-V - Virtual Machines	root\virtualization\Msvm_LogicalDisk	**SystemName**
Hyper-V - Virtual Machines	root\virtualization \Msvm_ProcessorSettingData	**VirtualQuantity**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Hyper-V - Virtual Machines	`root\virtualization \Msvm_ProcessorSettingData`	**InstanceID**
Hyper-V - Virtual Machines	`root\virtualization \Msvm_ComputerSystem`	**EnabledState**
Hyper-V - Virtual Machines	`root\virtualization \Msvm_SyntheticEthernetPortSettingData`	**ElementName**
Hyper-V - Virtual Machines	`root\virtualization \Msvm_MemorySettingData`	**InstanceID**
Hyper-V - Virtual Networks	`root\virtualization\Msvm_VirtualSwitch`	**Name**
Hyper-V - Virtual Networks	`root\virtualization\Msvm_VirtualSwitch`	**ElementName**
Hyper-V - Virtual Networks	`root\virtualization \Msvm_ActiveConnection`	**Antecedent**
Hyper-V - Virtual Networks	`root\virtualization \Msvm_ActiveConnection`	**Abhängig**
Windows - Active Processes	`Win32_Prozess`	**Beschreibung**
Windows - Active Processes	`Win32_Process`	**CreationDate**
Windows - Active Processes	`Win32_Process`	**CommandLine**
Windows - Active Processes	`Win32_Process`	**Beschriftung**
Windows - Active Processes	`Win32_Process`	**Priorität**
Windows - Active Processes	`Win32_Process`	**ProcessId**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Windows - Active Processes	`Win32_Process`	**ParentProcessId**
Windows - Active Processes	`Win32_Process`	**Name**
Windows - Active Processes	`Win32_Process`	**ExecutablePath**
Windows - Classify	`root\MSCluster\MSCluster_Node`	**Name**
Windows - Classify	`Win32_ComputerSystem`	**Domäne**
Windows - Classify	`root\MSCluster\MSCluster_Resource`	**Name**
Windows - Classify	`root\MSCluster\MSCluster_Resource`	**Typ**
Windows - Classify	`root\MSCluster\MSCluster_Resource`	**PrivateProperties**
Windows - Classify	`root\virtualization \Msvm_ComputerSystem`	**Name**
Windows - Classify	`root\MSCluster\MSCluster_ClusterToNode`	**Abhängig**
Windows - Classify	`root\MSCluster\MSCluster_ClusterToNode`	**Antecedent**
Windows - Classify	`root\MSCluster \MSCluster_ClusterToResource`	**PartComponent**
Windows - Classify	`root\MSCluster \MSCluster_ClusterToResource`	**GroupComponent**
Windows - Classify	`Win32_OperatingSystem`	**Beschriftung**
Windows - Classify	`root\MSCluster\MSCluster_Cluster`	**Name**
Windows - Classify	`Win32_ComputerSystem`	**Name**
Windows - Cluster	`root\MSCluster\MSCluster_Cluster`	**Name**
Windows - Cluster	`root\MSCluster\MSCluster_Network`	**AddressMask**
Windows - Cluster	`root\MSCluster \MSCluster_ClusterToResource`	**GroupComponent**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Windows - Cluster	root\MSCluster\MSCluster_Resource	**Typ**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Characteristics**
Windows - Cluster	root\MSCluster\MSCluster_ResourceGroup	**Name**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToQuorumResource	**PartComponent**
Windows - Cluster	root\MSCluster \MSCluster_ResourceGroupToResource	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_Network	**Adresse**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**PrivateProperties**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**Status**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Flags**
Windows - Cluster	root\MSCluster\MSCluster_ResourceGroup	**PrivateProperties**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToQuorumResource	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_ResourceGroupToResource	**GroupComponent**
Windows - Cluster	root\MSCluster \MSCluster_NodeToActiveGroup	**GroupComponent**
Windows - Cluster	root\MSCluster\MSCluster_Network	**Beschreibung**
Windows - Cluster	root\MSCluster\MSCluster_Cluster	**Status**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**Beschriftung**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Status**
Windows - Cluster	root\MSCluster\MSCluster_ClusterToNode	**Abhängig**
Windows - Cluster	root\MSCluster\MSCluster_ResourceType	**Beschreibung**
Windows - Cluster	root\MSCluster \MSCluster_NodeToNetworkInterface	**GroupComponent**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Windows - Cluster	root\MSCluster \MSCluster_NodeToActiveGroup	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_Network	**Name**
Windows - Cluster	root\MSCluster\MSCluster_Cluster	**Beschriftung**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToNetworkInterface	**GroupComponent**
Windows - Cluster	root\MSCluster\MSCluster_Node	**NodeInstanceID**
Windows - Cluster	root\MSCluster\MSCluster_ClusterToNode	**Antecedent**
Windows - Cluster	root\MSCluster\MSCluster_ResourceType	**PrivateProperties**
Windows - Cluster	root\MSCluster \MSCluster_NodeToNetworkInterface	**PartComponent**
Windows - Cluster	root\MSCluster \MSCluster_ResourceToPossibleOwner	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Name**
Windows - Cluster	root\MSCluster \MSCluster_NetworkInterface	**Adresse**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToNetworkInterface	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Beschreibung**
Windows - Cluster	root\MSCluster \MSCluster_NodeToActiveResource	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_ResourceType	**DisplayName**
Windows - Cluster	root\MSCluster\MSCluster_Event	**Typ**
Windows - Cluster	root\MSCluster \MSCluster_ResourceToPossibleOwner	**GroupComponent**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**Name**
Windows - Cluster	root\MSCluster \MSCluster_NetworkInterface	**Netzwerk**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToNetwork	**PartComponent**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Windows - Cluster	root\MSCluster\MSCluster_Node	**Status**
Windows - Cluster	root\MSCluster \MSCluster_NodeToActiveResource	**GroupComponent**
Windows - Cluster	root\MSCluster\MSCluster_ResourceType	**Name**
Windows - Cluster	root\MSCluster\MSCluster_Event	**Name**
Windows - Cluster	root\MSCluster \MSCluster_NetworkInterface	**DeviceID**
Windows - Cluster	root\MSCluster\MSCluster_Resource	**Beschreibung**
Windows - Cluster	root\MSCluster \MSCluster_NetworkInterface	**Beschreibung**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToNetwork	**GroupComponent**
Windows - Cluster	root\MSCluster\MSCluster_Node	**Beschriftung**
Windows - Cluster	root\MSCluster \MSCluster_ResourceToDependentResource	**Abhängig**
Windows - Cluster	root\MSCluster\MSCluster_ResourceGroup	**Status**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToResourceGroup	**PartComponent**
Windows - Cluster	root\MSCluster \MSCluster_ResourceTypeToResource	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_Cluster	**Beschreibung**
Windows - Cluster	root\MSCluster \MSCluster_NetworkInterface	**Name**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToResource	**PartComponent**
Windows - Cluster	root\MSCluster\MSCluster_Node	**PrivateProperties**
Windows - Cluster	root\MSCluster \MSCluster_ResourceToDependentResource	**Antecedent**
Windows - Cluster	root\MSCluster\MSCluster_ResourceGroup	**Beschreibung**
Windows - Cluster	root\MSCluster \MSCluster_ClusterToResourceGroup	**GroupComponent**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Windows - Cluster	root\MSCluster \MSCluster_ResourceTypeToResource	**GroupComponent**
Windows - CPU / Memory	Win32_PhysicalMemory	**DeviceLocator**
Windows - CPU / Memory	Win32_PhysicalMemory	**TypeDetail**
Windows - CPU / Memory	Win32_PhysicalMemory	**FormFactor**
Windows - CPU / Memory	Win32_PhysicalMemory	**MemoryType**
Windows - CPU / Memory	Win32_PhysicalMemory	**DataWidth**
Windows - CPU / Memory	Win32_PhysicalMemory	**TotalWidth**
Windows - CPU / Memory	Win32_PhysicalMemory	**BankLabel**
Windows - CPU / Memory	Win32_PhysicalMemory	**Status**
Windows - CPU / Memory	Win32_Processor	**Hersteller**
Windows - CPU / Memory	Win32_Processor	**NumberOfCores**
Windows - CPU / Memory	Win32_PhysicalMemory	**Geschwindigkeit**
Windows - CPU / Memory	Win32_Processor	**MaxClockSpeed**
Windows - CPU / Memory	Win32_Processor	**NumberOfLogicalProcessor**
Windows - CPU / Memory	Win32_PhysicalMemory	**SerialNumber**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Windows - CPU / Memory	`Win32_Processor`	**Name**
Windows - CPU / Memory	`Win32_PhysicalMemory`	**PartNumber**
Windows - CPU / Memory	`Win32_PhysicalMemory`	**Kapazität**
Windows - CPU / Memory	`Win32_PhysicalMemory`	**Hersteller**
Windows - CPU / Memory	`Win32_PhysicalMemory`	**Tag**
Windows - Disks	`Win32_LogicalDisk`	**Größe**
Windows - Disks	`Win32_LogicalDisk`	**FreeSpace**
Windows - Disks	`Win32_LogicalDisk`	**DeviceID**
Windows - Disks	`Win32_LogicalDisk`	**FileSystem**
Windows - Disks	`Win32_LogicalDisk`	**DriveType**
Windows - Disks	`Win32_LogicalDisk`	**Beschreibung**
Windows - Disks	`Win32_LogicalDisk`	**VolumeSerialNumber**
Windows - Disks	`Win32_LogicalDisk`	**VolumeName**
Windows - Get IIS Information	`root \MicrosoftIISv2\IIsWebServerSetting`	**SecureBindings**
Windows - Get IIS Information	`root \MicrosoftIISv2\IIsWebServerSetting`	**Name**
Windows - Get IIS Information	`root \MicrosoftIISv2\IIsWebServerSetting`	**LogFileDirectory**
Windows - Get IIS Information	`root\MicrosoftIISv2\IIsWebInfo`	**MinorIIsVersionNumber**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Windows - Get IIS Information	root\MicrosoftIISv2\IIsWebInfo	**MajorIisVersionNumber**
Windows - Get IIS Information	root \MicrosoftIISv2\IIsWebServerSetting	**ServerComment**
Windows - Get IIS Information	root \MicrosoftIISv2\IIsWebServerSetting	**ServerBindings**
Windows - Hardware Information	Win32_ComputerSystemProduct	**UUID**
Windows - Hardware Information	Win32_ComputerSystemProduct	**IdentifyingNumber**
Windows - Hardware Information	Win32_SystemEnclosure	**ChassisTypes**
Windows - Hardware Information	Win32_BIOS	**SerialNumber**
Windows - Hardware Information	Win32_SystemEnclosure	**SerialNumber**
Windows - Hardware Information	Win32_BaseBoard	**SerialNumber**
Windows - Installed Software	Win32_OperatingSystem	**Beschriftung**
Windows - Network	Win32_NetworkAdapterConfiguration	**Index**
Windows - Network	Win32_NetworkAdapterConfiguration	**DHCPEnabled**
Windows - Network	Win32_NetworkAdapterConfiguration	**MACAddress**
Windows - Network	Win32_NetworkAdapterConfiguration	**IPSubnet**
Windows - Network	Win32_NetworkAdapterConfiguration	**IPAddress**
Windows - Network	Win32_NetworkAdapter	**Index**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Windows - Network	Win32_NetworkAdapterConfiguration	**Beschriftung**
Windows - Network	Win32_NetworkAdapter	**Hersteller**
Windows - Network	Win32_NetworkAdapterConfiguration	**DefaultIPGateway**
Windows - Network	Win32_NetworkAdapter	**NetConnectionID**
Windows - Network	Win32_NetworkAdapterConfiguration	**IPEnabled**
Windows - OS Information	Win32_OperatingSystem	**CSDVersion**
Windows - OS Information	Win32_OperatingSystem	**Version**
Windows - OS Information	Win32_ComputerSystem	**UserName**
Windows - OS Information	Win32_ComputerSystem	**Modell**
Windows - OS Information	Win32_ComputerSystem	**Hersteller**
Windows - OS Information	Win32_Processor	**AddressWidth**
Windows - OS Information	Win32_OperatingSystem	**Beschreibung**
Windows - Printers	Win32_Printer	**Name**
Windows - Printers	Win32_TCPIPPrinterPort	**HostAddress**
Windows - Printers	Win32_TCPIPPrinterPort	**Name**
Windows - Printers	Win32_Printer	**PortName**
Windows - Printers	Win32_Printer	**DeviceID**
Windows - Services	Win32_Service	**ProcessId**
Windows - Services	Win32_Service	**ServiceType**
Windows - Services	Win32_Service	**StartName**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Klassen (Fortsetzung)

Probe	Windows-Klasse	Eigenschaft
Windows - Services	`Win32_Service`	**DisplayName**
Windows - Services	`Win32_Service`	**Status**
Windows - Services	`Win32_Service`	**StartMode**
Windows - Services	`Win32_Service`	**PathName**
Windows - Services	`Win32_Service`	**DesktopInteract**
Windows - Services	`Win32_Service`	**Name**
Windows - Services	`Win32_Service`	**AcceptStop**
Windows - Services	`Win32_Service`	**AcceptPause**

Windows Registrierungseinträge

Für Discovery Windows die -Proben sind mehrere Windows -Registrierungseinträge verfügbar.

Hinweis: Der Sensor „Windows - Installierte Software“ wendet einen Zeitstempel von 00:00:00 auf den in der Registrierung abgerufenen Wert „install_date“ ab. Die Installationszeit aller Windows -Software ist unabhängig von der Zeitzone und wird auf Mitternacht des Tages festgelegt, an dem sie installiert wurde. Beispiel: Ein Installationsdatum von **2.19.2017** in der Registrierung Windows wird im Fenster CMDBals **2.19.2017 00:00:00** angezeigt.

Probe	Windows-Registrierungseinträge
Windows - Classify	`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/Hostname`
Windows - Classify	`HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/Tcpip/Parameters/Domain`
Windows - Find APD File Location	`HKEY_LOCAL_MACHINE/SOFTWARE/APD/APD/CONFIGPATH`
Windows - Installed Software	`HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/InstallDate`
Windows - Installed Software	`HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/DisplayVersion`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe	Windows-Registrierungseinträge
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows NT/CurrentVersion/ProductId
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ ProductId
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ Installer/UserData/*/Products/*/InstallProperties/InstallDate
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/ CurrentVersion/Uninstall/*/DisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ Uninstall/*/ParentDisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ Installer/UserData/*/Products/*/InstallProperties/ DisplayVersion
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ Uninstall/*/UninstallString
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/ Windows/CurrentVersion/Installer/UserData/*/Products/ */InstallProperties/Publisher
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Internet Explorer/ Version
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ Installer/UserData/*/Products/*/InstallProperties/DisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ Uninstall/*/Publisher
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/ Windows/CurrentVersion/Installer/UserData/*/Products/ */InstallProperties/ProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Office/ */Registration/*/ProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ Installer/UserData/*/Products/*/InstallProperties/ProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/ Uninstall/*/DisplayVersion

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe	Windows-Registrierungseinträge
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/DisplayVersion
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Office/*/Registration/*/DigitalProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/Publisher
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Uninstall/*/DisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Installer/UserData/*/Products/*/InstallProperties/DisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/UninstallString
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Office/*/Registration/*/DigitalProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Internet Explorer/Registration/ProductId
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/Publisher
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Internet Explorer/svcVersion
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Office/*/Registration/*/ProductID
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/InstallDate
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Wow6432Node/Microsoft/Windows/CurrentVersion/Uninstall/*/ParentDisplayName
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows/CurrentVersion/Uninstall/*/InstallDate
Windows - Installed Software	HKEY_LOCAL_MACHINE/Software/Microsoft/Windows NT/CurrentVersion/DigitalProductID

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe „WMIRunner“

„WMI Runner“ ist ein Probe-Typ, der über die Schnittstelle WMI (Windows Management Instrumentation) Daten aus Windows-Betriebssystemen abruft. IPv6 bietet Unterstützung für WMI Runner.

Die Probe verarbeitet mehrere benutzerspezifische WMI-Pfade, die abgefragt werden sollen, mit einem Basisformat einer nativen WMI-Abfrage. Alle zu prüfenden Felder müssen eindeutig benannt sein (innerhalb der Domäne der Probe). Die an den Sensor zurückgegebenen Probe-Ergebnisse liefern die für jedes abgefragte Feld gefundenen Daten, indiziert nach dem Namen.

Beim Erstellen einer WMI-Probe müssen der Probe-Typ auf „WMI-Probe“ und das ECC-Warteschlangenthema auf „WMIRunner“ festgelegt werden.

Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

Die folgenden Parameter können an die WMI-Probe übergeben werden:

Parameter für die Probe „WMIRunner“

Parameter	Beschreibung	Standardwert
Quelle	Host, zu dem eine Verbindung hergestellt werden soll	
port	Port, zu dem eine Verbindung hergestellt werden soll	
debug	Aktiviert die Debug-Protokollierung	false
wmi_timeout	Zeitüberschreitung für die tatsächliche WMI-Probe in Sekunden. Mit diesem Parameter können Sie das Zeitüberschreitungsintervall für einzelne Windows-Probes ändern. Dieser Wert überschreibt den Wert im MID Server-Parameter windows_probe_timeout, der eine Zeitüberschreitung für alle von einem bestimmten MID Server gestarteten Probes festlegt. Die Probe „Windows - Installed Software“ ist mit einem Zeitüberschreitungswert von 15 Minuten konfiguriert.	300 (Sekunden)
process_timeout	Zeitüberschreitung für den das Skript ausführenden Prozess in Sekunden. Dieser Parameter ist nur zum internen Gebrauch bestimmt und wird nicht unterstützt.	wmi_timeout + 10 (Sekunden)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter für die Probe „WMIRunner“ (Fortsetzung)

Parameter	Beschreibung	Standardwert
credentials_debug	Zeigt einen <credentials_debug>-Abschnitt in der ECC-Warteschlange an, der Ihnen bei der Behebung von Problemen mit den Anmeldeinformationen helfen kann. Wenn Sie diese Eigenschaft auf „true“ setzen, werden Informationen zur Behandlung von Problemen mit Anmeldeinformationen in der ECC-Warteschlange ausgegeben, auch wenn die Anmeldeinformationen erfolgreich sind. Weitere Informationen finden Sie unter Problembehandlung bei Anmeldeinformationen .	falsch

Hinweis: Die Standardzeitüberschreitung für WMI/PowerShell beträgt 5 Minuten. Nur die Probe „Windows - Installed Software“ hat einen Standardzeitüberschreitungswert von 15 Minuten. Wenn Sie einem Probe-Parameter `wmi_timeout` hinzufügen, kann dies die Standardzeitüberschreitung eines Windows-Probe ändern.

Port-Sonden

Port-Probes werden in Discovery von der Shazzam-Probe verwendet, um Protokollaktivitäten an offenen Ports auf gefundenen Geräten zu erkennen.

Wenn eine Port-Probe auf ein Protokoll stößt, das verwendet wird, überprüft der Shazzam-Sensor den Port-Probe-Datensatz, um zu bestimmen, welche Klassifizierungs-Probe gestartet werden soll. Die gängigen Protokolle WMI, SSH, SNMP und HTTP im Basissystem besitzen Prioritätszahlen, die die Reihenfolge steuern, in der sie gestartet werden.

Die Priorität lautet wie folgt:

- 1 - WMI
- 2 - SSH
- 3 - SNMP
- 4 - HTTP

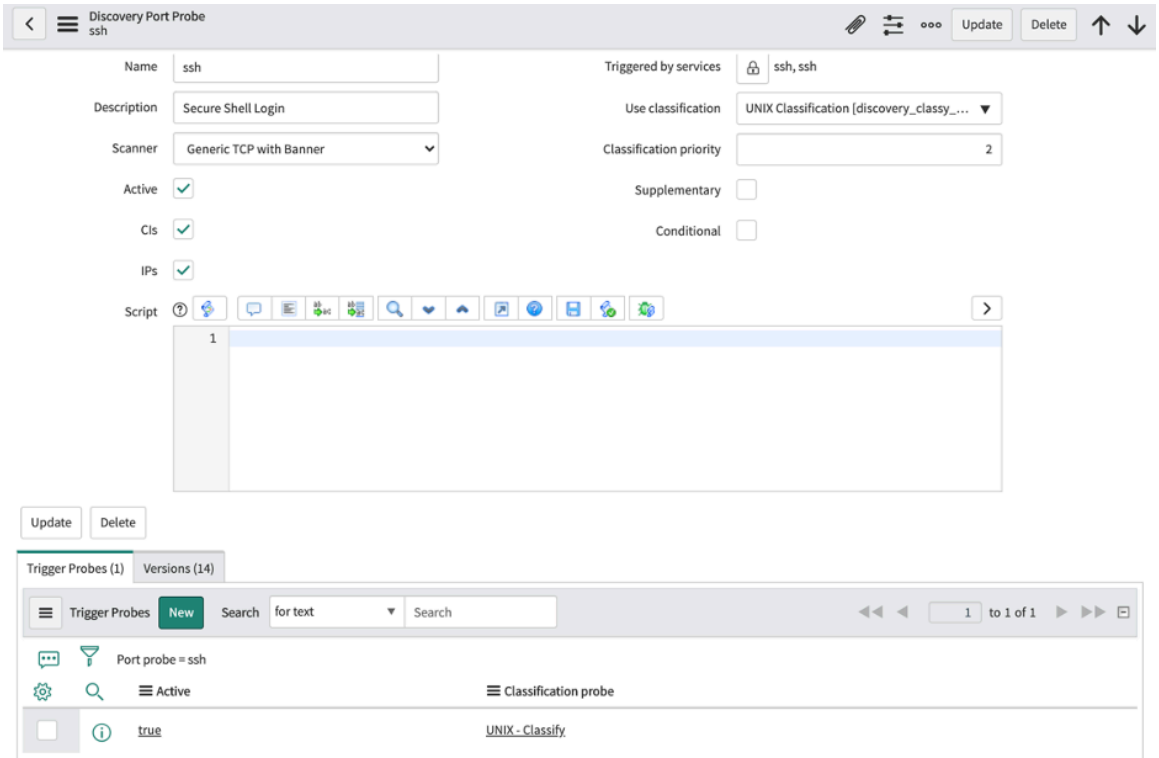
Im Basissystem wird die WMI-Probe immer zuerst gestartet. Wenn sie auf einem Gerät erfolgreich ist, werden keine anderen Port-Probes für dieses Gerät gestartet. Wenn die WMI-Probe nicht erfolgreich ist, wird die SSH-Probe gestartet, um Informationen über das Gerät zu erfassen. Wenn diese nicht erfolgreich ist, wird die SNMP-Probe gestartet. Mit dieser Methode kann Discovery Geräte ordnungsgemäß klassifizieren, wenn darauf mehrere Protokolle ausgeführt werden (zum Beispiel SSH, SNMP und HTTP).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Discovery-Anschlussprobe“

Um auf das Port-Probe-Formular zuzugreifen, navigieren Sie zu **Discovery-Definition** > **Anschlussprobes**.

Um einer Port-Probe mehrere Klassifizierungs-Probes hinzuzufügen, erstellen Sie eine Verknüpfung zwischen der Port-Probe und der eigentlichen Klassifizierungs-Probe. Unten im Formular können Sie weitere Auslöser-Probes hinzuzufügen. Auf diese Weise wirkt sich eine fehlgeschlagene Klassifizierung nicht auf die anderen aus, sodass die Discovery-Leistung verbessert werden kann.



Das Formular „Anschlussprobe“ enthält die folgenden Felder:

Port-Sonden

Feld	Eingabewert
Name	Einfacher Name der Port-Probe, der ihre Funktionalität widerspiegelt (zum Beispiel SNMP)
Beschreibung	Definition des Akronyms für das Protokoll. (SSH steht zum Beispiel für Secure Shell Login.)
Scanner	Shazzam-Techniken zur Erkundung von Ports. Einige davon sind protokollspezifisch, andere generisch. Für eine WMI-Port-Probe wird beispielsweise der Scanner-Wert „Generic TCP“ und für die SNMP-Port-Probe der Wert „SNMP“ verwendet.
Aktiv	Gibt an, ob diese Port-Probe aktiviert oder deaktiviert ist
CIs	Gibt an, ob diese Port-Probe für die Erkennung von Konfigurationselementen aktiviert oder deaktiviert ist
IPs	Gibt an, ob diese Port-Probe für die Erkennung von IP-Adressen aktiviert oder deaktiviert ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Port-Sonden (Fortsetzung)

Feld	Eingabewert
Durch Services ausgelöst	Gibt an, welche Services die Portnutzung definieren. Verwenden Sie diese Einstellung, um eine nicht standardmäßige Portnutzung zu definieren und die Portnummer an das Protokoll zu koppeln.
Klassifizierung verwenden	Benennt die entsprechende Klassifizierungstabelle basierend auf dem untersuchten Protokoll
Klassifizierungspriorität	Legt die Priorität fest, mit der die jeweilige Port-Probe ausgeführt wird. Wenn die erste Port-Probe fehlschlägt, wird die nächste Probe auf dem Gerät ausgeführt usw., bis die richtigen Daten zurückgegeben werden. Dies ermöglicht die richtige Klassifizierung eines Geräts, auf dem zwei Protokolle wie SSH und SNMP ausgeführt werden. Die Standardprioritäten für die Discovery-Protokolle lauten: • 1 - WMI • 2 - SSH • 3 - SNMP • 4 - HTTP
Ergänzend	Startet zusätzliche Klassifizierungen in der Reihenfolge ihrer Priorität, nachdem eine Identifizierung mit höherer Priorität erfolgreich ausgeführt wurde
Bedingt	Führt diese Port-Probe aus, wenn eine der nicht bedingten Probes einen offenen Port zurückgibt. Die bedingten Port-Probes im Basissystem versuchen, die Namen von Windows-Geräten und DNS-Namen aufzulösen. Diese Port-Probes benötigen zusätzliche Ressourcen und werden nur verwendet, wenn Aktivität an offenen Ports erkannt wurde.
Skript	Auszuführendes Skript.

Shazzam-Probe, Port-Probes und Protokolle

Das Scannen von Ports ist der erste Schritt im Discovery-Prozess. Die Shazzam-Probe führt Port-Scans durch, und zwar unabhängig davon, ob Sie Muster für die horizontale Erkennung verwenden. In der folgenden Tabelle sind die bekannten Ports und Protokolle aufgeführt, die von Discoveryverwendet werden.

Nach dem Upgrade auf Discovery-Administratorarbeitsbereich Version 1.3.1 (Store August 2024) können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** und verwenden Sie das erweiterte Dashboard.

Im Basissystem sind mehrere Port-Probes verfügbar. Jede Port-Probe verwendet einen IP-Service. Hierbei handelt es sich um einen Datensatz, der Discovery mitteilt, welcher Port für ein bestimmtes Protokoll verwendet werden soll. Prüfen Sie diese Tabelle, bevor Sie Ports mit einer Firewall blockieren.

Wichtig: Stellen Sie sicher, dass Sie keine Ports blockieren, die Discovery benötigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-Port-Probes und -IP-Services

Name der Standard-Port-Probe	Geräteklassifizierung	Standard-IP-Service und -Port
dns	Prozessklassifizierung [discovery_classy_proc]	dns (Port 53)
http	HTTP-Klassifizierung [discovery_classy_http]	http (Port 80) und https (Port 443)
ip_phone	SNMP-Klassifizierung [discovery_classy_snmp]	sip (Port 5060)
osx	Applikationsklassifizierung-Ergebnisse scannen [discovery_classy_scan_app]	afp (Port 548)
Drucker	Applikationsklassifizierung-Ergebnisse scannen [discovery_classy_scan_app]	hp-pdl-datastr (Port 9100) und printer (Port 515)
slp	Prozessklassifizierung [discovery_classy_proc]	slp (Port 427)
snmp	SNMP-Klassifizierung [discovery_classy_snmp]	snmp (Port 161)
ssh	UNIX-Klassifizierung [discovery_classy_unix]	ssh (Port 22)
tls_ssl_certs		tls_ssl_certs • SSL-Ports: 443, 8443, 9443, 636 (ldaps), 993 (imaps), 995 (popssl), 989, 990 • StartTLS-Ports: 25 (smtp), 110, 143, 389, 21, 587 (smtp)
vmapp	Anwendungsklassifizierung [discovery_classy_appl]	vmapp_https (Port 5480) und vmapp6_https (Port 9443)
wbem	CIM-Klassifizierung [discovery_classy_cim]	wbem_https (Port 5989)
winrm	Windows-Klassifizierung [discovery_classy_windows]	winrm (Port 5985) und winrm_ssl (Port 5986)
wins	Prozessklassifizierung [discovery_classy_proc]	ms-nb-ns (Port 137)
wmi	Windows-Klassifizierung [discovery_classy_windows]	epmap (Port 135)

Diese Tabelle zeigt andere gängige Ports und Protokolle, die von Discovery verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Ports und -Protokolle

Name	Servicename	Port	Details	Erstellen/Einfügungen	Protokoll
afp	Apple File Protocol	548			TCP
BEA-Weblogik		7001		cmdb_ci_app_server	TCP
dns	Domain Name Service	53	Zum Auflösen des Namens jeder IP-Adresse		TCP/ UDP
epmap	Microsoft RPC (WMI, DCOM)	135	Windows-Systeme		TCP
ftp		21			TCP
hp-pdl-datastr	Printer PDL Data Stream	9100	HP-Drucker		TCP
http	HyperText Transfer Protocol	80	Webserver	cmdb_ci_web_server	TCP
https	HyperText Transfer Protocol over Secure Socket	443	Sichere Webserver	cmdb_ci_web_server	TCP
IBM DB2		50000			TCP
IBM MQSeries		1414			TCP
IBM Websphere		9080			TCP
IBM Web sphere SSL		9443			TCP
IMAPS		993			TCP
pip (Internet Print Protocol)	IP Phone/ Session Initiation Protocol	5060			TCP
LDAP		389			TCP
LDAPs		636			TCP
Microsoft NetBIOS		139			TCP
Microsoft-ds		445			TCP
ms-nb-ns		137			UDP
Microsoft SQL server		1433			TCP
MySQL		3306			TCP
Nagios NRPE		5666			TCP
NFS		2049			TCP/ UDP
Oracle TNS		1521			TCP
POP3		110			TCP

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Ports und -Protokolle (Fortsetzung)

Name	Servicename	Port	Details	Erstellen/Einfügungen	Protokoll
postgresql		5432		cmdb_ci_database	TCP
Drucker	Drucker	515	Drucker		TCP
sip	SIP (Session Initiation Protocol)	5060			TCP
slp	Service Location Protocol (SLP)	427			TCP/ UDP
smtp	TCP	25			
smux (SNMP Multiplexing)		199			
snmp	Simple Network Management Protocol	161	Netzwerkgeräte		UDP
snmptrap		162			UDP
ssh	Secure Shell Service	22	Unix-Systeme		TCP
sunrpc		111			TCP
telnet		23			TCP
TIBCO Rendezvous		7500			TCP
Tomcat HTTP		8080			TCP
vmapp6_https		9443			TCP
vmapp_https	vCenter Server Appliance Web Interface mit https	5480			TCP
wbem_https	CIM-XML über HTTPS (WBEM)	5989	CIM-Klassifizierung		TCP
wins	Windows Internet Name Service	137	NetBIOS-Namensauflöser		UDP

Windows und dynamische Ports

Unterstützte Windows -Computer können dynamische Portbereiche von 49152 bis 65535 für TCP und UDP haben.

Shazzam-Probe konfigurieren

Wenn Sie Discovery ausführen, erkennt die Shazzam-Probe Ihre aktiven Netzwerkgeräte, indem sie bestimmte Ports in bestimmten IP-Adressbereichen scannt. Wenn die Liste der zu scannenden IP-Bereiche groß ist, können Sie die Shazzam-Nutzlast für die JSON-Codierung konfigurieren, um ihre Größe zu reduzieren.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können das Verhalten einzelner Shazzam-Probes mit grundlegenden und erweiterten Parametern steuern.
Anweisungen zum Konfigurieren der Sondenparameter finden Sie unter Probe-Parameter festlegen .

Hinweis: Die Shazzam-Nutzlast wird durch die folgenden MID-Server-Eigenschaften gesteuert. Diese Eigenschaften müssen dem MID Server nicht hinzugefügt werden. Die Shazzam-Probe greift auf ihre Standardwerte zurück.

- Die Eigenschaft **shazzam.chunk_size** steuert die maximale Anzahl von IP-Adressen, die Shazzam parallel scannen kann.
- Die Eigenschaft **mid.shazzam.regulator.interval_ms** legt das Intervall fest, in dem Shazzam Pakete starten kann.
- Die Eigenschaft **mid.shazzam.regulator.packets_per_interval** legt die Anzahl von Paketen fest, die Shazzam im Zeitintervall starten kann.

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **Probes**.
2. Wählen Sie **Shazzam** aus.
3. Fügen Sie der zugehörigen Liste **Probe Parameter** Parameter hinzu, oder bearbeiten Sie sie.
4. Konfigurieren Sie die Shazzam-Parameter.
   Zur Feinabstimmung der Shazzam-Probe stehen die folgenden Parameter zur Verfügung. Die folgenden Werte sind nur im Probe-Datensatz definiert.

Erweiterte Shazzam-Parameter

Parameter	Beschreibung
BannerTCP_waitForConnectMS	Legt die Anzahl von Millisekunden fest, die der Scanner BannerTCP auf die Herstellung einer Verbindung wartet **Standardwert**: 1500
debug	Aktiviert bei Einstellung auf **true** die Debug-Protokollierung **Standardwert:** false
delay_wbem	Verzögert die Klassifizierung von Systemen mit einem offenen WBEM-Port bis zum endgültigen Shazzam-Sensorauftrag. Bei einem umfangreichen Zeitplan, der viele WBEM-Ports erkennt, kann die Verzögerung der Klassifizierung bis zum letzten Sensorauftrag dazu führen, dass dem Knoten nicht mehr genügend Arbeitsspeicher zur Verfügung steht. Wenn Sie diesen Parameter auf **false** setzen, kann die Klassifizierung dieser Systeme für alle Shazzam-Sensoraufträge erfolgen. **Standard**: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
DNS_alternativePort	Überholt
DNS_waitForResponseMS	Legt die Anzahl von Millisekunden fest, die der Scanner DNS auf eine Antwort wartet **Standardwert**: 1000
GenericTCP_waitForConnectMS	Legt die Anzahl von Millisekunden fest, die der Scanner GenericTCP auf die Herstellung einer Verbindung wartet **Standardwert**: 1000
HTTP_waitForConnectMS	Legt die Anzahl von Millisekunden fest, die der Scanner HTTP auf die Herstellung einer Verbindung wartet **Standardwert**: 500
HTTP_waitForResponseMS	Legt die Anzahl von Millisekunden fest, die der Scanner HTTP auf eine Antwort wartet **Standardwert**: 500
NBT_alternativePort	Überholt
NBT_waitForResponseMS	Legt die Anzahl von Millisekunden fest, die der Scanner NBT auf eine Antwort wartet **Standardwert**: 500
Shazzam_report_inactive	Bei **true** werden Geräte gemeldet, die zwar eingeschaltet, aber inaktiv sind. Beispiel: Ein Gerät weist keine offenen Ports auf, lehnt jedoch mindestens eine Portverbindungsanforderung ab. **Standard**: true
scanner_log	Aktiviert bei Einstellung auf **true** die Scannerprotokollierung Diese Protokollierungsinformationen werden in der Antwort der Shazzam-Probe angezeigt. **Standardwert:** false
shazzam_report_dead	Bei **true** werden Geräte mit inaktiven IP-Adressen gemeldet. Etwa ein Gerät, bei dem alle Ports geschlossen sind **Standardwert:** false
SNMP_alternativePort	Überholt
SNMP_tapIntervalMS	Legt die Anzahl von Millisekunden fest, die der Scanner SNMP zwischen Taps wartet **Standardwert**: 1000

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
SNMP_taps	Legt die Anzahl der Taps (Anforderungen) fest, die der Scanner SNMP versucht **Standardwert**: 2
SNMP_waitForResponseMS	Legt die Anzahl von Millisekunden fest, die der Scanner SNMP nach dem letzten Tap auf eine Antwort wartet **Standardwert**: 1000
TLS_keepOriginalCertificate	Wenn Discovery bei der Einstellung **true** ausgeführt wird, wird das Feld certificate_file in cmdb_ci_certificate mit dem ursprünglichen Zertifikat gefüllt. Beachten Sie, dass sich dadurch die Nutzlastgröße erhöhen kann. **Standardwert:** false

Shazzam-Nutzlastgröße steuern

Eine Systemeigenschaft konvertiert Shazzam-Nutzlasten in JSON-Zeichenfolgen, wodurch deren Größe erheblich reduziert wird. Diese Einstellung verhindert, dass Knoten bei der Erkennung einer große Anzahl von IP-Bereichen durch einen einzelnen Zeitplan der Arbeitsspeicher ausgeht.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die Eigenschaft `glide.discovery.shazzam_ranges_json` wird für neue Instanzen auf `true` gesetzt. Diese Einstellung codiert die Nutzlast als JSON-Zeichenfolge. Die Eigenschaft kann von Administratoren konfiguriert werden und ist im verfügbar **Discovery-Definition** > **Eigenschaften** Modul. Die Eigenschaftsbezeichnung im Modul lautet **Verwenden Sie JSON für IP-Bereiche in Shazzam**.

In upgegradeten Instanzen ist diese Eigenschaft auf `false` festgelegt und standardmäßig nicht sichtbar. Durch manuelles Hinzufügen der Eigenschaft zu Ihrer aktualisierten Instanz wird die Funktion aktiviert, aber nicht zu hinzugefügt **Discovery-Definition** > **Eigenschaften** Modul. Um die JSON-Codierung zu aktivieren und dem Modul hinzuzufügen, importieren Sie den Update Set, das Sie über KB0687626 erhalten.

Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein, und drücken Sie die `Eingabetaste`.
2. Klicken Sie in der Liste der Systemeigenschaften auf **Neu**.
3. Füllen Sie das Formular mit den folgenden Feldwerten aus:
   - **Name**: glide.discovery.shazzam_ranges_json
   - **Beschreibung**: Codiert die Shazzam-Nutzlast in JSON
   - **Wert**: true
4. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Sensoren

Jede Probe in Discovery muss über einen entsprechenden Sensor zur Verarbeitung der zurückgegebenen Daten verfügen.

Beispiel: Wenn eingehende Daten das Ergebnis einer WMI-Probe sind, wird der WMI-Sensor zur Verarbeitung der Nutzlast ausgelöst.

Hinweis: Wenn Sie eine Multi-Probe erstellen, müssen Sie einen Multisensor erstellen, um die von dieser Probe zurückgegebenen Daten zu verarbeiten. Weitere Informationen finden Sie unter Multi-Probes und Multisensoren.

Navigieren zu **Discovery** > **Discovery-Definition** > **Sensoren** und bearbeiten oder erstellen Sie einen Sensor.

Tabelle der Sensorfelder

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Probe-Namen ein.
Reagiert auf Probe	Wählen Sie die Probe aus, deren Nutzlast dieser Sensor verarbeiten muss.
Sensorklasse [sys_class_name]	Wählen Sie den Typ des zu erstellenden Sensors aus: • Import-Export-Zuordnung: Diese Option wird derzeit nicht verwendet. • MultiSensor: Multisensoren verarbeiten die Daten, die von Multi-Probes zurückgegeben werden. Wählen Sie diesen Typ aus, um einen Multisensor zu erstellen, der auf die in einer Multi-Probe verwendeten einfachen Probes antwortet. • Sensor: Wählen Sie diesen Typ aus, wenn es sich bei dem Sensor um einen einfachen Sensor handelt, der auf eine einfache Probe antwortet.
Beschreibung	Geben Sie eine optionale Beschreibung der Sensorfunktion ein.
Sensortyp [sensor_type]	Geben Sie an, wie die Ergebnisse der Probe verarbeitet werden. • Klassifizierung: Dieses Feld wird derzeit nicht verwendet. • Java: Dieses Feld wird derzeit nicht verwendet. • Javascript: Von einer Probe zurückgegebene Daten werden außerhalb der Anwendung im Sensor selbst verarbeitet und sind für den Benutzer sichtbar. Dies ist der gängigste Sensortyp. • Mehrzeiliger Text: Dieses Feld wird derzeit nicht verwendet. • XML: Die XML-Daten der Probe sind in Teile zerstückelt. Einige Teile können zum Starten anderer Probes verwendet werden, die der ursprüngliche Sensor benötigt, um alle erforderlichen Informationen über ein Gerät zu füllen.
Aktiv	Wählen Sie diese Option aus, um den Sensor zu aktivieren oder zu deaktivieren.
Skript	Geben Sie das Skript ein, das bei der Verarbeitung der Probe ausgeführt werden soll. Sie können in einem Sensorskript

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle der Sensorfelder (Fortsetzung)

Feld	Beschreibung
	die Hashmap g_probe_parameters verwenden, um Probe-Parameter für alle konfigurierten, ausgelösten Probes festzulegen. Beispielsweise wird durch diesen Code der Parameter *node_port* für alle ausgelösten Probes auf 16001 festgelegt. `g_probe_parameters['node_port']=16001;`
Reagiert auf Probes	Verwenden Sie diese zugehörige Liste, um die einfache Probe in einer Multi-Probe anzugeben, deren Nutzlast dieser Multisensor verarbeiten muss. Diese Liste ist nur für Multisensoren verfügbar.
Auslösertests	Verwenden Sie diese zugehörige Liste, um anzugeben, welche Probes dieser Sensor für zusätzliche Erkundungen starten kann.
Die folgenden Felder können durch Konfiguration des Formulars hinzugefügt werden:	
Feld	Beschreibung
Agent	Geben Sie den ECC-Warteschlangentyp ein, mit dem dieser Sensor abgeglichen werden soll.
Standardeinstellungen übernehmen	Wählen Sie diese Option aus, um die Standardwerte des Sensors zu übernehmen.
Klassifizierungstyp	Wählen Sie den Klassifizierungstyp aus, der dem Sensor zugeordnet ist.
Zusammenfügen	Geben Sie das Feld für den Abgleich ein, anhand dem bestimmt wird, ob eine Zusammenfügung erfolgen soll.
Bedingungsskript	Erstellen Sie eine vordefinierte Anforderung für die Ausführung dieses Sensors.
Datenoption	Wählen Sie aus, wie importierte Sensordaten behandelt werden sollen. Verfügbare Optionen: • Einfügen und Aktualisieren • Nur einfügen • Nur aktualisieren
Externe Namen	Geben Sie einen Namen ein, um die Sensordaten zu kennzeichnen.

Sensortransaktion abhängig von der Dauer abbrechen

Standardmäßig bricht diese Regel die Sensortransaktion ab, wenn die Ausführung länger als 20 Minuten dauert.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Ausführung der Discovery-Sensortransaktion länger als 20 Minuten dauert, werden die folgenden Aktionen ausgeführt:

- Der zugeordnete Eingabedatensatz der ECC-Warteschlange wird auf den Fehlerstatus festgelegt.
- Die *Anzahl der Erkennungen mit abgeschlossenem Status* wird aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fehlermeldungen werden protokolliert, zum Beispiel:

```
Sensor error when processing Linux - Storage: Transaction cancelled:
 maximum execution time exceeded
```

- Die Erkennung wird fortgesetzt.

  Dieses Verhalten ist die Folge der Transaktionsmengenregel für Discovery-Sensoren. Diese Regel ist standardmäßig aktiviert.

  Sie können die Regel deaktivieren, und Sie können die Zeitspanne ändern, die verstreichen soll, bevor die Regel in Kraft tritt. Für den Zugriff auf diesen Datensatz ist die Administratorrolle erforderlich.

Prozedur

1. Um die Regel zu deaktivieren, navigieren Sie zu **Systemdefinition** > **Mengenregeln**. Das Plugin **Transaction Quotas** muss aktiv sein.
2. Suchen Sie nach dem Namen `*Discovery`, um die Regelliste zu filtern.
3. Klicken Sie in der Namensspalte auf **Discovery-Sensoren**.
4. Um die Zeitspanne zu ändern, bearbeiten Sie das Feld **Höchstdauer** für die Regel. Der Wert wird in Sekunden angegeben.

Erkennungs-Probes verwalten

In Discovery sind zahlreiche Erkennungs-Probes und zugehörige Sensoren enthalten. Probes oder Sensoren müssen nur selten geändert werden. Möglicherweise müssen Sie jedoch Parameter festlegen, um das Verhalten einer bestimmten Probe zu steuern oder Versionen benutzerdefinierter Probes ausrichten.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Vorgehensweise

Mit Probes und Sensoren sind folgende Aktionen möglich:

Probes des Basissystems überprüfen

Informationen über im Basissystem vorhandene Probes finden Sie in der Liste der Discovery-Probes. Probes müssen für Klassifizierer aktiv sein, damit Discovery die Probes auslösen kann. Allerdings sind nicht alle Probes für Klassifizierer aktiv, da Probes und Sensoren durch immer mehr Muster ersetzt werden. Eine Liste der Muster finden Sie unter Verfügbare Discovery-Muster.

Probes erstellen oder ändern

Sie können eine neue Probe erstellen, um zusätzliche CIs zu erkennen, die Discovery mit den Probes oder Mustern des Basissystems nicht erkennen kann. Sie können aber auch vorhandene Probes ändern, um zusätzliche Informationen zum CI-Typ zu sammeln. Nachdem Sie eine Probe erstellt oder geändert haben, testen Sie sie. Sie können auch Multi-Probes und Multisensoren erstellen. Weitere Informationen finden Sie unter Discovery-Multi-Probe erstellen.

Upgrade auf die neueste Version einer Probe oder eines Sensors durchführen

Wenn Sie Ihre Instanz upgraden, wird auch Discovery zusammen mit Komponenten wie Probes und Sensoren aktualisiert. Probes und Sensoren, die Sie angepasst haben, werden jedoch nicht aktualisiert. Sie müssen die Anpassungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in eine Textdatei kopieren, die Probes und Sensoren aktualisieren und danach die Anpassungen erneut anwenden. Weitere Informationen finden Sie unter Versionen benutzerdefinierter Probes und Sensoren angleichen.

Probe-Parameter festlegen

Probe-Parameter steuern verschiedene Aspekte der Funktionsweise von Probes. Da alle Probes im Basissystem bereitgestellt werden, sind bestimmte Parameter zulässig. Diese sind in der Liste der Discovery-Probes angegeben. Unter Probe-Parameter festlegen finden Sie Anweisungen zum Festlegen von Parametern.

Probe-Berechtigungen prüfen

Für bestimmte Probes sind Berechtigungen erforderlich, damit Sie für die Zielcomputer und CIs ausgeführt werden können, die zur Erkennung vorgesehen sind. Weitere Informationen finden Sie unter Berechtigungen für Discovery-Probes.

Probes erstellen oder ändern

Erstellen Sie eine neue Probe zur Erkennung zusätzlicher CIs, oder ändern Sie eine vorhandene Probe, um zusätzliche Informationen zu erfassen. Nachdem Sie eine Probe erstellt oder geändert haben, testen Sie sie.

Vorbereitungen

Erforderliche Rolle: Administrator

Wichtig: Sie benötigen fortgeschrittene Skriptkenntnisse, um Sonden oder die zugehörigen Sensoren zu modifizieren. Viele vorhandene Sonden bieten Parameter, die Sie einstellen können, anstatt die Sonde selbst zu ändern. Weitere Informationen finden Sie unter Probe-Parameter festlegen.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Probes**.
2. Klicken Sie auf den Namen der Probe, die Sie ändern möchten.
3. Ändern Sie die Formularfelder (siehe Tabelle).

Feld	Beschreibung
Klasse	Wählen Sie die Probe für das Betriebssystem des abzufragenden Geräts aus. ◦ AWS-Test: Wählen Sie diese Klasse aus, um Ihre Ressourcen in einer AWS-Cloud abzufragen. ◦ **CIM-Test**: Wählen Sie diesen Probe-Typ aus, um einen CIM-Server mit WBEM-Protokollen abzufragen. ◦ **Mehrfachprobe**: Wählen Sie diesen Probe-Typ aus, um eine oder mehrere einfache Probes eines beliebigen Typs auszuführen oder Probes verschiedener Typen zu mischen. Dieser Probe-Typ kann mehrere Abfragen gleichzeitig ausführen, die alle Ergebnisse gleichzeitig zurückgeben. Es ist nicht möglich, Multi-Probes zu anderen Multi-Probes hinzuzufügen. ◦ **Probe**: Wählen Sie diesen generischen Typ aus, um eine Probe-Klasse zu definieren. Geben Sie den Namen der Probe-Klasse im Feld *ECC-Warteschlangenthema* an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ **SNMP-Probe**: Wählen Sie diesen Probe-Typ für Netzwerkgeräte wie Router aus. ◦ **WMI-Probe**: Wählen Sie diesen Probe-Typ für Windows-Geräte aus.
ECC-Warteschlangenthema	Geben Sie einen beschreibenden Begriff für die Funktionsweise der Probe ein. Die Probe verwendet diese Bezeichnung als Feld **Thema** für eingehende ECC-Warteschlangennachrichten. Der Begriff muss nicht eindeutig sein. Beispielsweise können alle UNIX-Probes für das ECC-Warteschlangenthema den Wert **SSHCommand** aufweisen. Standardmäßig verwenden Probes die folgenden ECC-Warteschlangenthemen: ◦ CimProbe ◦ Multi-Probe ◦ PowerShell-Probe ◦ SCPRelay ◦ SSHCommand ◦ SNMP ◦ WMIRunner
ECC-Warteschlangenname	Geben Sie entweder einen beschreibenden, für Benutzer verständlichen Namen oder den tatsächlichen Befehl ein, den die Probe ausführen soll. Beispiel: Wenn der Wert im Feld für das ECC-Warteschlangenthema **SSHCommand** lautet, geben Sie den tatsächlichen Shell-Befehl zur Ausführung in dieses Feld ein.
Cache-Ergebnisse	Wählen Sie diese Option aus, um die Ergebnisse dieser Probe zwischenzuspeichern und die Erkennungsleistung insgesamt zu verbessern. Der Cache für Probe-Ergebnisse sollte nur für die Probes und Sensoren aktiviert werden, deren Ausgabe sich wahrscheinlich nicht ändert. Beispielsweise werden Ergebnisse des Sensors „Linux - CPU“ zwischengespeichert, da sich CPU-Informationen nur selten ändern. Der Cache ist standardmäßig für Probes und Sensoren im Basissystem aktiviert, deren Ausgabe sich wahrscheinlich nicht ändert. ⚠ **Warnung:** Aktivieren Sie den Cache weder für Klassifizierungs-Probes noch für Identifizierungs-Probes. Darüber hinaus sollten Sie den Cache nicht für Probes aktivieren, die zusätzliche Probes auslösen, da deren Auslösung dadurch möglicherweise verhindert wird.
Klassischer Modus	Wählen Sie diese Option aus, um die Ergebnisse dieser Probe zwischenzuspeichern. Wählen Sie diese Option aus, um das Nachverarbeitungsskript auf der ServiceNow-Instanz anstatt auf dem MID Server zu debuggen. Dieser Modus ist nur gültig, wenn ein Postprozessorskript vorhanden ist. Verwenden Sie den klassischen Modus zum Debuggen von Nachverarbeitungsskripts in der Testumgebung. Von der Verwendung des klassischen Modus in der Produktionsumgebung rät ServiceNow ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Postprozessorskript	Definieren Sie ein optionales Nachverarbeitungsskript, das auf dem MID Server ausgeführt wird. Das Skript akzeptiert Probe-Ergebnisse als Eingabe und gibt eine JSON-Zeichenfolge aus, die an die Instanz zurückgesendet wird, damit sie von Sensoren als Eingabe verwendet werden kann. Verwenden Sie diese Art von Skript, um Aufgaben wie das Analysieren von Daten durchzuführen. Alle Probe-Nachverarbeitungsskripts und deren zugehörigen Sensoren haben Zugriff auf die folgenden globalen Variablen: ◦ `current`: Legt das Attribut als aktuell fest. Dieselbe Funktionalität ist auch für Sensoren verfügbar. Dabei handelt es sich um Attribute des erkannten Geräts. ◦ `related_data`: Alle zusätzlichen Daten, die von den Nachverarbeitungsskripts der Probes übergeben werden sollen, zum Beispiel `related_list` Alle Probe-Nachverarbeitungsskripts und deren zugehörigen Sensoren haben Zugriff auf die folgenden Methoden: ◦ `log(string)`: Protokolliert die Zeichenfolge zum MID Server und zu den ServiceNow-Instanzprotokolldateien ◦ `getParameter(param)`: Ruft den Parameter aus der Nutzlast der ECC-Warteschlange ab

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Ändern Sie diese zugehörigen Listen bei Bedarf.

Zugehörige Liste	Beschreibung
Probe Parameter	Parameter, die die Funktionalität von Probes steuern. Anweisungen dazu finden Sie unter Probe-Parameter festlegen.
Sensoren, die auf diese Probe reagieren	Die Sensoren, die von dieser Probe verwendet werden
Enthalten in MultiProbe	Gibt an, ob diese Probe mit anderen Probes als Multi-Probe enthalten ist
MultiSensor-Skripts	Skripts, die für mehrere Sensoren ausgeführt werden
Versionen	Die Version der Probe. Wenn **Status** auf **Aktuell** festgelegt ist, stellt die Probe die aktuelle Version der Instanz dar. Andernfalls haben Sie nicht die aktuelle Version und müssen möglicherweise eine Neuausrichtung durchführen. Anweisungen dazu finden Sie unter Versionen benutzerdefinierter Probes und Sensoren angleichen.

6. Klicken Sie auf **Probe testen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Geben Sie im Fenster „Probe testen“ die IP-Adresse des Ziels ein, und wählen Sie den MID Server aus.
   Nur MID Server, die den Status **In Betrieb** und **Validiert** aufweisen, können ausgewählt werden.
8. Klicken Sie auf **OK**.
9. Prüfen Sie die ECC-Warteschlange für den MID Server, und zeigen Sie die Ergebnisse an.

Nächste Maßnahme

Fügen Sie der zugehörigen Liste **Löst Probe aus** die Probe des entsprechenden Klassifizierers hinzu. Unter Discovery-CI-Klassifizierung erstellen finden Sie Beschreibungen der Felder und zugehörigen Listen im Klassifiziererformular.

Berechtigungen für Discovery-Probes

Zur Ausführung diverser Probes sind zusätzliche Berechtigungen erforderlich.

Aktive Verbindungen erkennen

Discovery verwendet die Probe „Windows - Active Connections“, um Informationen über aktive Verbindungen abzurufen. Für die Funktion Application Dependency Mapping muss diese Probe funktionieren.

Aktive Verbindungen erkennen

Probes	Zusätzliche Berechtigungen
Windows - Active Connections	Fähigkeit zum Aufrufen des Objekts *\root \CIMV2:Win32_Process* Lese- und Schreibzugriff auf die Freigabe $admin

Anwendungsprofile erkennen

Discovery verwendet die folgenden Probes für den Zugriff auf Informationen über Anwendungsprofile.

Anwendungsprofile erkennen

Probes	Zusätzliche Berechtigungen
Windows - Get APD Environment Files Windows - Get APD Env File Content Windows - Get APD Version File Content	Fähigkeit zum Aufrufen des Objekts *\root \CIMV2:Win32_Process* Lese- und Schreibzugriff auf die Freigabe $admin Schreibzugriff auf das Verzeichnis %SystemRoot%\temp

VMware-Workstations erkennen

Discovery verwendet die Probe **Windows - Get VMware Workstation**, um Informationen über unter Windows installierte virtuelle VMware-Computer abzurufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VMware-Workstations erkennen

Probes	Zusätzliche Berechtigungen
Windows - Get VMware Workstation	Fähigkeit zum Aufrufen des Objekts *\root\CIMV2:Win32_Process* Lese- und Schreibzugriff auf die *admin$ share* Schreibzugriff auf das Verzeichnis *%SystemRoot%\temp* Konfigurieren Sie die **PATH**-Variable so, dass sie den Pfad zum Befehl `vmrun.exe` enthält. Dieser Befehl befindet sich normalerweise im `Installationsverzeichnis` der VMware-Workstation.

MSSQL erkennen

Discovery verwendet die Probe „Windows - MSSQL“, um Informationen über unter Windows installierte MicrosoftMicrosoft Azure Event Hubs SQL Server abzurufen.

MSSQL erkennen

Probes	Zusätzliche Berechtigungen
Windows - MSSQL	• Zugriff auf das Objekt *Win32_Process* • Zugriff auf das Objekt *Win32_Service* • Zugriff auf das Objekt *Win32_NetworkAdapterConfiguration* • Zugriff auf das Objekt *Microsoft.SqlServer.Management.Smo* • Berechtigung zum Ausführen des Befehls *nbtstat* • Zugriff auf HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\InstalledInstances • Zugriff auf HKLM\SOFTWARE\Microsoft\MSSQLServer\$instanceName \SuperSocketNetLib\Tcp\TcpPort, wobei *$instanceName* einem Array möglicher Werte entspricht.

Probe-Parameter festlegen

Verwenden Sie Probe-Parameter, um das Verhalten einer bestimmten Probe bei jeder Auslösung zu steuern.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Die folgenden Parameter sind für alle Probe-Typen verfügbar:

Parameter	Beschreibung
`Quelle`	[Erforderlich] Der erste Host, zu dem eine Verbindung hergestellt werden soll • Typ: Zeichenfolge (URL) • Standardwert: keiner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie die Probe, oder wählen Sie diejenige, für die Sie Parameter festlegen möchten.
2. Klicken Sie in der zugehörigen Liste *Probe Parameter* auf **Neu**.
3. Füllen Sie die Felder entsprechend aus (siehe Tabelle).

Das Formular „Probe Parameter“ enthält die folgenden Felder.

Felder im Formular „Probe Parameter“

Feld	Beschreibung
Name	Geben Sie den Parameternamen ein. Jeder Probe-Typ besitzt eine eigene Liste verfügbarer Parameter.
Wert	Geben Sie den Parameterwert oder das Skript gemäß den Anforderungen des Parameters ein.
Wertskript	[Optional] Geben Sie das Skript ein, das der Parameter ausführen soll, wenn Sie im Feld *Wert* noch kein Skript angegeben haben.
Probe	Zeigt die Probe an, auf die sich dieser Parameter bezieht.

Versionen benutzerdefinierter Probes und Sensoren angleichen

Wenn Sie eine Probe oder einen Sensor angepasst und auf eine neue Version einer Instanz aktualisiert haben, müssen Sie die Versionen der/des benutzerdefinierten Probe und Sensors auf die aktuelle Version angleichen.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Probes und Sensoren weisen eine Haupt- und eine Nebenversion auf.

Hauptversion

Eine umfassende Versionsänderung spiegelt eine Änderung in der erwarteten Ausgabe einer Probe wider, zum Beispiel das Hinzufügen oder Entfernen eines Zielattributs, eine Formatänderung, zum Beispiel XML oder JSON, oder eine Änderung eines Probe-Parameterskripts.

Nebenversion

Eine geringfügige Versionsänderung bezieht sich auf kleine Korrekturen, die sich nicht auf das Ergebnis oder die Verarbeitung der Daten auswirken.

Ein Sensor und die entsprechende Probe müssen dieselbe Hauptversion aufweisen. Es wird empfohlen, dass sie auch dieselbe Nebenversion haben. Durch diesen Versionsabgleich wird sichergestellt, dass die von der Probe zurückgesendeten Daten vom Sensor verstanden und ordnungsgemäß verarbeitet werden. Alle Mitglieder eines Multi-Probe-Bündels müssen dieselbe Haupt- und Nebenversion aufweisen.

Standardmäßig verfolgt Discovery schwerwiegende Versionskonflikte und zeigt Versionskonfliktfehler im Abschnitt „Aktive Discovery-Fehler“ im Discovery-Dashboard und im Discovery-Protokoll an. Sie können festlegen, ob Discovery Nichtübereinstimmungen der Nebenversion nachverfolgt, indem Sie die Discovery-Eigenschaft **Bei geringfügigen Versionskonflikten warnen** (`glide.discovery.warn_minor_version`) aktivieren. Nichtübereinstimmungen der Nebenversion werden im Discovery-Protokoll nachverfolgt, aber nicht im Discovery-Dashboard angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Versionen für Multi-Probes und Multisensoren werden wie folgt geprüft:

- Die Versionen der einzelnen Probes, die in Multi-Probes enthalten sind, werden mit den „Reagiert auf Probes“-Skripts verglichen, die ihre Daten verarbeiten.
- Die Versionen der „Reagiert auf Probes“-Skripts und des Multisensor-Hauptskripts werden verglichen.

Wenn eine Probe und der entsprechende Sensor nicht dieselbe Hauptversion besitzen, verarbeitet der Sensor während einer Erkennung keine Informationen, sondern sendet Fehlermeldungen an die Protokolldatei. Fehler werden auch im Discovery-Dashboard angezeigt, wenn Sie einen Erkennungsauftrag ausführen. Wenn die Hauptversion identisch ist, die Nebenversion jedoch nicht, werden von einem Sensor während einer Erkennung Informationen verarbeitet.

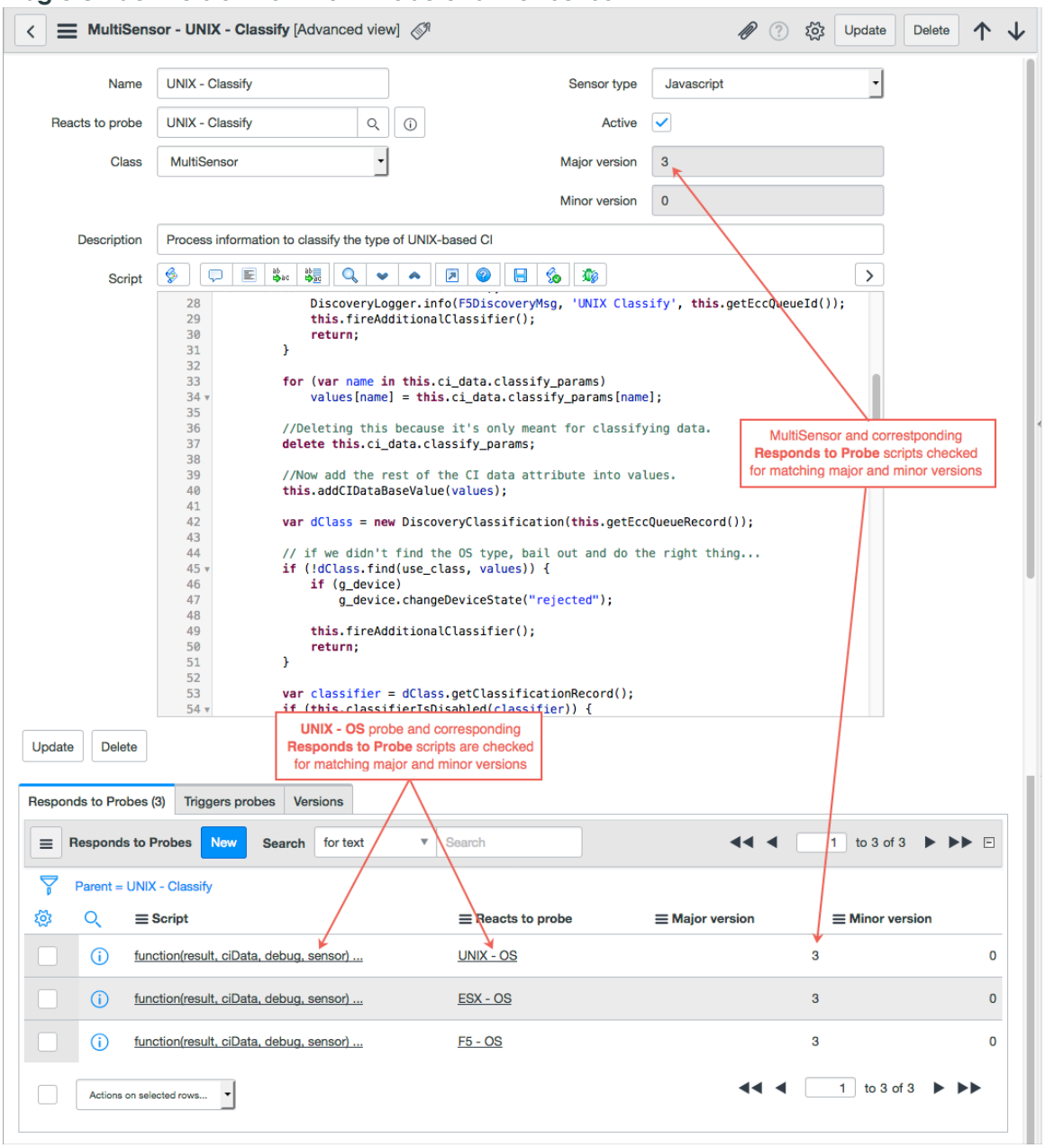
So verwenden Sie die aktuellste Version einer Probe, die verfügbar ist:

Prozedur

1. Speichern Sie die Anpassungen, die Sie an einer Probe/einem Sensor vorgenommen haben, in einer Textdatei, um sie später erneut anwenden zu können.
2. Navigieren zu **Discovery** > **Dashboard**.
3. Suchen Sie im Abschnitt **Aktive Discovery-Fehler** nach Versionskonflikten, und notieren Sie die Probe oder den Sensor, die/der den Fehler verursacht hat.
4. Navigieren zu **Discovery-Definition** > **Probes** oder **Discovery-Definition** > **Sensoren** und wählen Sie die Probe oder den Sensor aus, für die Sie ein Upgrade durchführen möchten.
5. Fügen Sie dem Formular die Felder **Hauptversion** und **Nebenversion** hinzu, wenn Sie die Versionen im Formular anzeigen möchten.
6. In einem Multisensor können Sie die Hauptversion anhand der Versionen der Probes in der zugehörigen Liste **Reagiert auf Probes** überprüfen, die den Sensor verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abgleich der Version von Multi-Probe und Multisensor



7. Klicken Sie auf die zugehörige Liste **Versionen**.
8. Suchen Sie nach einer Version, deren **Status** gleich **Zurück** und deren **Quelle** gleich **System-Upgrades** ist.
9. Klicken Sie auf den Datumslink in der Spalte **Erstellt** für diese Version, um den Versionsdatensatz zu öffnen.
10. Klicken Sie auf **Diese Version wiederherstellen**.
11. Navigieren Sie zurück zum Formular für die Probe oder den Sensor, und überprüfen Sie, ob die Hauptversion korrekt ist.
12. Wenden Sie Ihre Anpassungen erneut auf die Probe oder den Sensor an.
13. Stellen Sie sicher, dass Ihre Anpassungen für die neue Version der Probe oder des Sensors gültig sind, indem Sie eine Erkennung in Ihrer Testumgebung ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Multi-Probes und -Multisensoren

Multi-Probes enthalten mindestens eine einfache Probe, die dafür konfiguriert ist, bestimmte Informationen von verwaltbaren Geräten zu extrahieren, indem mehrere Abfragen mit einer einzelnen Authentifizierung ausgeführt werden.

Sie können Multi-Probes so planen, dass sie jederzeit im Erkennungsprozess ausgeführt werden können, um die Erkundung effizienter zu gestalten. Multi-Probes werden häufig als Identitäts-Probes verwendet. Identitäts-Probes fragen für Geräte Informationen wie Name und Seriennummer ab und verwenden dann die Ergebnisse dieser Abfragen, um vorhandene CIs in der CMDB zu aktualisieren.

Zum Verarbeiten der von einer Multi-Probe zurückgegebenen Daten müssen Sie Multisensoren erstellen, die Skripts ausführen, die die von den Multi-Probes zurückgegebenen Daten verarbeiten. Multisensoren heißen in der Regel genauso wie ihre entsprechenden Multi-Probes.

Hinweis: Die entsprechenden Multisensoren tragen in der Regel denselben Namen wie die Multi-Probes.

Die folgenden Multi-Probes sind im Basissystem enthalten.

Multi-Probe	Enthaltene Probes
AIX - ADM	• AIX - Active Processes: Ruft aktive laufende Prozesse ab • Unix - Active Connections: Ruft Informationen über aktive Verbindungen ab
AIX - Identity	• AIX - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs • AIX - Serial Number: Ruft AIX-Seriennummern ab
CIM - Identity	CIM - Computer System: Ruft CIM-Computersysteme über SMI-S ab
CIM - Identity - WBEM Service	CIM - CIMOM: Untersucht den WBEM-Service, CIMOM
HP-UX - ADM	• HP-UX - Active Processes: Ruft aktive laufende Prozesse ab • Unix - Active Connections: Ruft Informationen über aktive Verbindungen ab
HP-UX - Identity	• HP-UX - Hardware Serial Number: Ruft HP-UX-Seriennummern ab • HP-UX - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs
Linux - Identity	• Linux - Hardware Information: Ruft DMI-(BIOS-)Informationen ab • Linux - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multi-Probe	Enthaltene Probes
Mac OS X - Identity	• Mac OS X - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs • Mac OS X - CPU/Memory: Ruft CPU- und Speicherinformationen ab
SNMP - A10 - Identity	• SNMP - A10 - Identity - Serial: Teil der Multi-Probe „SNMP - Load Balancer - Identity“, die zum Identifizieren des A10-Lastenausgleichsmoduls verwendet wird • SNMP - Identity Info: Identifiziert ein SNMP-Gerät
SNMP - ACE - Identity	• SNMP - Identity Info: Identifiziert ein SNMP-Gerät • SNMP - ACE - Identity - Serial: Teil der Multi-Probe „SNMP - Load Balancer - Identity“, die zum Identifizieren des ACE Load Balancers verwendet wird
SNMP - Alteon - Identity	• SNMP - Alteon - Identity - Serial: Teil der Multi-Probe „SNMP - Load Balancer - Identity“, die zum Identifizieren des Alteon-Lastenausgleichsmoduls verwendet wird • SNMP - Identity Info: Identifiziert ein SNMP-Gerät
SNMP - AppDirector - Identity	• SNMP - AppDirector - Identity - Serial: Teil der Multi-Probe „SNMP - Load Balancer - Identity“, die zum Identifizieren des AppDirector-Lastenausgleichsmoduls verwendet wird • SNMP - Identity Info: Identifiziert ein SNMP-Gerät
SNMP - F5 BIG-IP - Identity	• SNMP - F5 BIG-IP - Identity - Serial: Ruft die für diesen Lieferanten global eindeutige Seriennummer des BIG-IP-Gehäuses ab • SNMP - Identity Info: Identifiziert ein SNMP-Gerät
SNMP - Identity	SNMP - Identity Info: Identifiziert Drucker-CIs
SNMP - Load Balancer - Identity	• SNMP - F5 BIG-IP - Identity - Serial: Ruft die für diesen Lieferanten global eindeutigen Seriennummern des BIG-IP-Gehäuses ab • SNMP - Identity Info: Identifiziert SNMP-Geräte
SNMP - Netscaler - Identity	• SNMP - Netscaler - Identity - Serial: Ruft die für diesen Lieferanten global eindeutige Seriennummer des Netscaler-Gehäuses ab • SNMP - Identity Info: Identifiziert SNMP-Geräte
Solaris - ADM	• Solaris - Active Processes: Ruft aktive laufende Prozesse ab • Unix - Active Connections: Ruft Informationen über aktive Verbindungen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Multi-Probe	Enthaltene Probes
Solaris - Identity	• Solaris - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs. • Solaris - Serial Number: Ruft Seriennummern für Solaris-Geräte ab †
Unix - ADM	• Unix - Active Processes: Ruft aktive laufende Prozesse ab • Unix - Active Connections: Ruft Informationen über aktive Verbindungen ab
UNIX - Classify	• ESX - OS: Identifiziert ESX-Computer • UNIX - OS: Wird nach der Probe „ESX - OS“ ausgeführt, um das Betriebssystem für SSH-Geräte zu bestimmen, die nicht als ESX identifiziert wurden
Windows - ADM	• Windows - Active Processes: Ruft aktive laufende Prozesse ab • Windows - Active Connections: Ruft Informationen über aktive Verbindungen ab
Windows - Identity	• Windows - Network: Bestimmt Netzwerkschnittstellen, IPs und MACs. • Windows - OS/Hardware Information: Sucht auf einem Windows-Computer nach WMI-Informationen
Windows - Storage 2008	• Windows - Storage 2008 - PS: Ruft Datenträger- und Dateisysteminformationen für Windows 2008 und frühere Versionen ab • Windows - Storage 2008 - WMI: Ruft Datenträger- und Dateisysteminformationen für Windows 2008 und frühere Versionen ab
Windows - Storage 2012	• Windows - Storage 2012 - WMI: Ruft Datenträger- und Dateisysteminformationen für Windows 2012 und höher ab • Windows - Storage 2012 - PS: Ruft Datenträger- und Dateisysteminformationen für Windows 2012 und höher ab

Hinweis: † Für diese Probe ist die Installation eines Befehlszeilentools von Oracle namens SNEEP erforderlich. Melden Sie sich zum Herunterladen und Installieren dieses Tools auf der Oracle-Website an. Nach der Installation dieses Tools wird die Probe **Solaris - Serial Number** automatisch ausgeführt, wenn Discovery ein Solaris-Gerät erkennt. Für Fujitsu PRIMEPOWER-Geräte müssen Sie diese Probe mit Root-Anmeldeinformationen ausführen.

Einer Multi-Probe eine einfache Probe hinzufügen

Sie können einer Multi-Probe über die zugehörige Liste *Enthält Probes* einfache Probes hinzufügen.

Vorbereitungen
Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

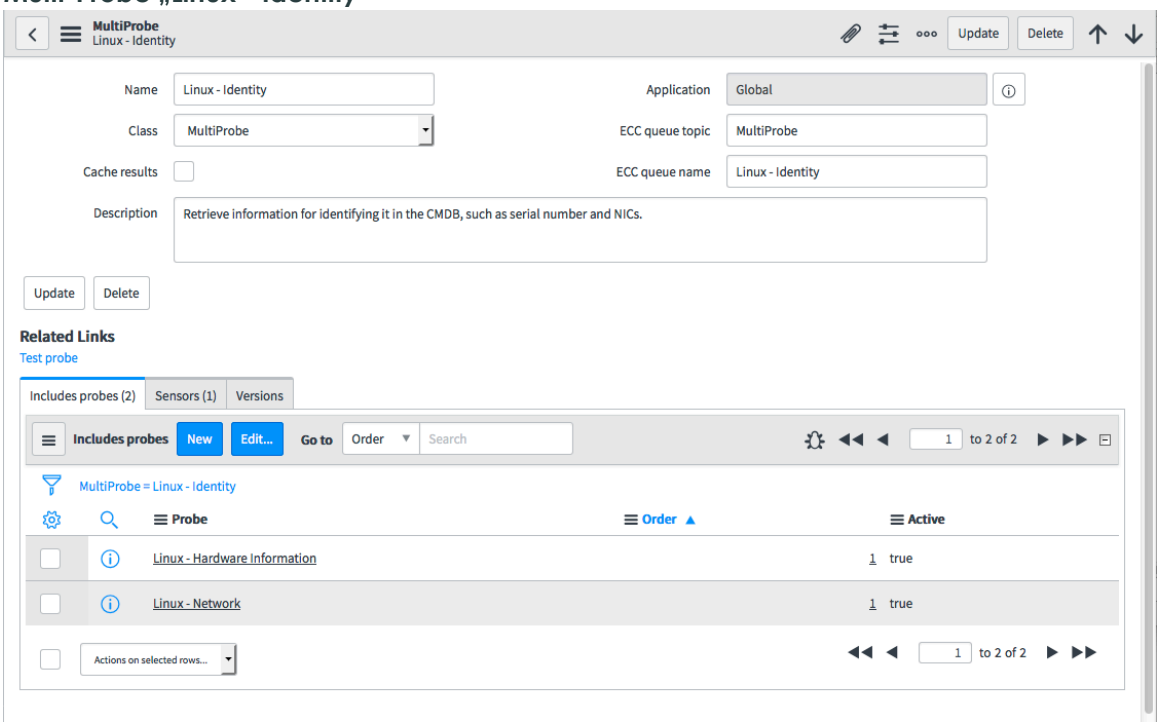
Sie können einer Multi-Probe einfache Probes beliebiger Typen hinzufügen und bei Bedarf Probe-Typen mischen.

Warnung: Fügen Sie der zugehörigen Liste *Enthält Probes* keine Multi-Probe hinzu.

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definitionen** > **Probes**.
2. Öffnen Sie eine Multi-Probe aus der Liste.
   Die Multi-Probe-Bezeichnung wird in der Spalte **ECC-Warteschlangenthema** angezeigt.

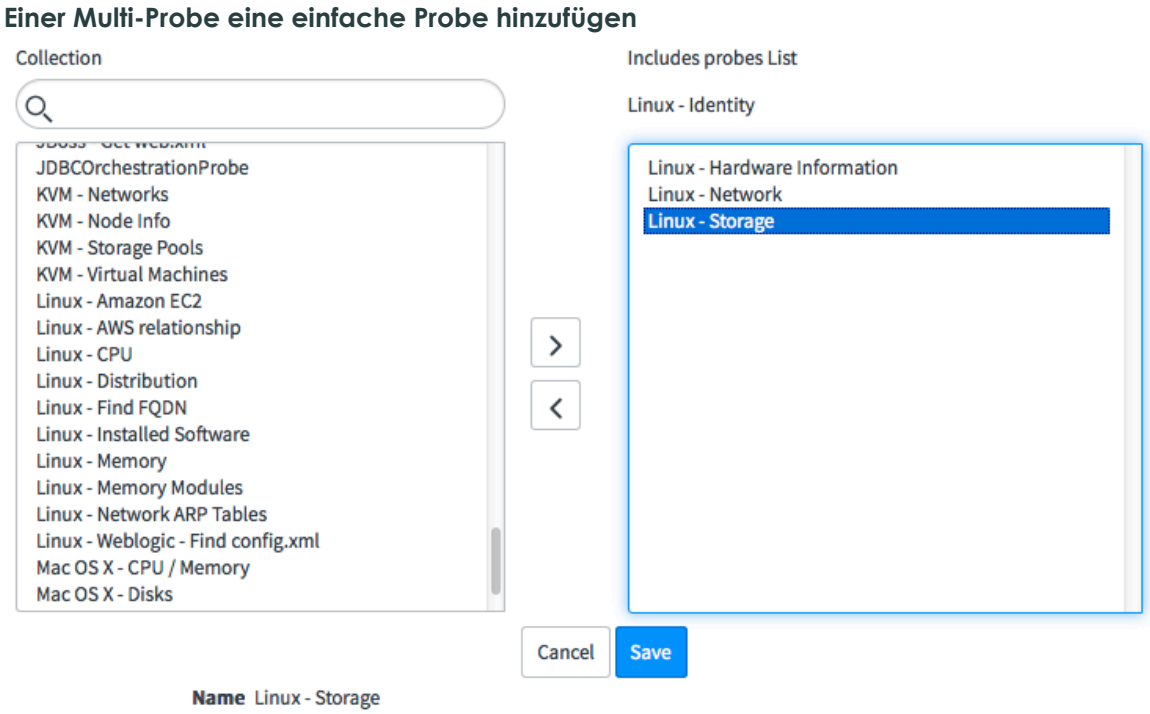
Multi-Probe „Linux - Identity“



3. Klicken Sie im Multi-Probe-Datensatz in der zugehörigen Liste **Enthält Probes** auf **Neu**.
4. Wählen Sie in der Erfassungsliste in der linken Spalte eine einfache Probe aus, und verschieben Sie sie in die Liste der enthaltenen Probes.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Speichern**.

Discovery-Multi-Probe erstellen

Sie können die in der Plattform bereitgestellten standardmäßigen Multi-Probes und Multisensoren verwenden oder eigene erstellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Probes**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular mit den folgenden Einstellungen aus:
   - Probe-Typ: Multi-Probe
   - ECC-Warteschlangenthema: Multi-Probe
4. In der zugehörigen Liste *Enthält Probes* können Sie die Probes hinzufügen, die Sie in der Multi-Probe einschließen möchten.
5. Klicken Sie auf **Speichern**.

Discovery-Multisensor erstellen

Erstellen Sie einen Multisensor, um die Daten zu verarbeiten, die von einer Multi-Probe zurückgegeben werden.

Vorbereitungen

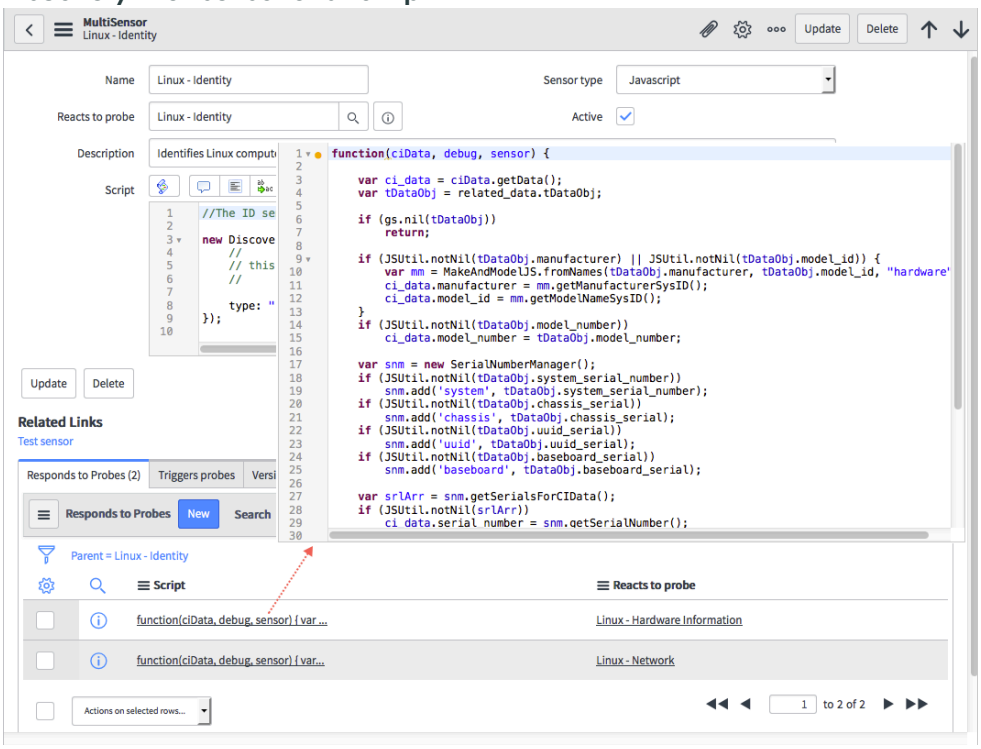
Erforderliche Rolle: Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Discovery-Multisensor und -Skript



Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery-Definition** > **Sensoren**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular mit den folgenden Einstellungen aus:
   - *Sensortyp*: Multisensor
   - *ECC-Warteschlangenthema*: Multisensor
   - *Reagiert auf Probe*: Wählen Sie die Probe aus, deren Nutzlast dieser Sensor verarbeiten muss.
   - *Sensortyp*: Wählen Sie eine der folgenden Optionen aus.
     - *Javascript*: Von einer Probe zurückgegebene Daten werden außerhalb der Anwendung im Sensor selbst verarbeitet und sind für den Benutzer sichtbar. Dies ist der gängigste Sensortyp.
     - *XML*: Die XML-Daten der Probe sind in Teile zerstückelt. Einige Teile können zum Starten anderer Probes verwendet werden, die der ursprüngliche Sensor benötigt, um alle erforderlichen Informationen über ein Gerät zu füllen.
4. Klicken Sie mit der rechten Maustaste auf den Formularheader und wählen Sie **Speichern** aus.
5. Klicken Sie in der zugehörigen Liste *Reagiert auf Probes* auf **Neu**.
6. Füllen Sie das Formular mit den folgenden Einstellungen aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *Reagiert auf Probe*: Wählen Sie die Probe in der Multi-Probe aus, auf die dieser Sensor reagiert. Der Sensor muss funktional mit der Probe verknüpft sein, etwa über die Netzwerk-ID oder Seriennummer.
- *Skript*: Geben Sie ein Skript ein, das vor dem Skript im Multisensor ausgeführt werden soll. Dieses Skript definiert, wie die von jeder Probe zurückgegebenen Daten verarbeitet werden sollen.

7. Klicken Sie auf **Speichern**.

Beispiel für benutzerdefinierte Discovery-Probe und -Sensor: CI mit Textdateiwerten füllen

Mithilfe dieser benutzerdefinierten Discovery-Probe können Sie eine Textdatei von einem Windows-Computer lesen und ein CI in der CMDB mit den Werten aus der Datei füllen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
In diesem Beispiel wollte der Benutzer von *BGinfo* erstellte Dateien lesen.

Hinweis: Wenn Sie die Probe und den Sensor fertiggestellt haben, platzieren Sie die Probe in der entsprechenden Windows-Klassifizierung unter **Discovery-Definition** > **CI-Klassifizierung** > **Windows**.

Prozedur

1. Navigieren zu **Discovery-Definition** > **Probes**und klicken Sie dann auf **Neu**.
2. Füllen Sie die folgenden Felder aus:
   - *Name*: Eindeutiger und beschreibender Name für die Probe
   - *Probe-Typ*: Wählen Sie **Probe** aus.
   - *Beschreibung*: Beschreiben Sie die Funktionalität dieser Probe.
   - *Verwendet von Discovery*: Aktivieren Sie dieses Kontrollkästchen.
   - *ECC-Warteschlangenthema*: Der Name der Probe, die der MID Server ausführen soll. In diesem Beispiel wird *WMIRunner* verwendet.
   - *ECC-Warteschlangenname*: In diesem Beispiel wird der beschreibende Name *WMI: BGInfo files* verwendet.
3. yxcvbnm,ooiuztreq12345tKlicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern** aus dem Kontextmenü.
4. Wechseln Sie im Probe-Formular zur Registerkarte „Probe Parameter“, und klicken Sie auf **Neu**.
5. Geben Sie `WMI_GetFiles.js` als Namen für diesen Parameter ein.
6. Kopieren Sie das folgende Skript in das Feld *Skript*, und bearbeiten Sie es nach Bedarf.
7. Klicken Sie auf **Absenden**.

```
//
 // Use ServiceNow WMIAPI to gather stats
 //
 var CMD_RETRIES = 3;
 var scanner = getScanner();
 if (scanner) {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  var output = "";
  for(var i = 0; i < CMD_RETRIES; i++) {
     output = scanner.winExec("%SystemRoot%\\system32\\cmd.exe /C type
\\\"C:\\Information Systems\\BgInfo\\*.txt\\\"");
     if (output)
        break;
  }
  scanner.appendToRoot("output", output);
}
```

8. Navigieren zu **Discovery-Definition** > **Sensoren**und klicken Sie dann auf **Neu**.

   Füllen Sie die folgenden Felder aus:

   - *Name*: Verwenden Sie den Namen der entsprechenden Probe. In diesem Beispiel wird *Windows - Get BGInfo files* verwendet.
   - *Reagiert auf Probe*: Der Name der im vorherigen Verfahren erstellten Probe: *Windows - Get BGInfo files*
   - *Sensortyp*: Wählen Sie den Typ des zu erstellenden Sensors aus, in diesem Beispiel *Sensor*.
   - *Beschreibung*: Beschreibt die Funktion dieses Sensors
   - *Skript*: Kopieren Sie das folgende Skript in das Feld *Skript*, und bearbeiten Sie es nach Bedarf.
   - *Sensortyp*: Bestimmt, wie die Antwort der Probe verarbeitet wird - in diesem Beispiel *JavaScript*

9. Klicken Sie auf **Absenden**.

```
new DiscoverySensor({ data: {}, process: function(result) {

        this.parseOutput(result.output);
        this.update(this.data);
    },

 parseOutput: function(output) {
        var currentFile;
        var files = {};

 if (output.startsWith("<wmi")) {
            var bgout = new XMLHelper(output).toObject();
            if (!bgout)
                return;

 output = bgout.output;
        }

 var lines = output.split(/\n/);

 for(var i = 0; i < lines.length; i++) {
            var line = lines[i];
            if (line.startsWith("C:\\Information Systems\\BgInfo\\")) {
                currentFile = line.substr(30);
                files[currentFile] = "";
            } else if (currentFile) {
                var newLine = line.trim();
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                if (newLine)
                    files[currentFile] += (files[currentFile]? "\n" :
"") + newLine;
            }
        }

this.data['u_jack_id'] = files['JackID.txt'];
this.data['warranty_expiration'] = files['Warranty.txt'];
this.data['po_number'] = files['Ponum.txt'];},
type: "DiscoverySensor"

});
```

Erweiterte Discovery-Konfiguration

Sie können mehrere zusätzliche Discovery-Komponenten konfigurieren, zum Beispiel Application Dependency Mapping, die ECC-Warteschlange und Erweiterungen für den MID Server.

gMSA-Konfiguration für Discovery

Gruppenverwaltete Servicekonten (gMSAs) sind verwaltete Domänenkonten, die Sie zum Absichern von Services verwenden. gMSAs können für Discovery ohne Anmeldeinformationen verwendet werden.

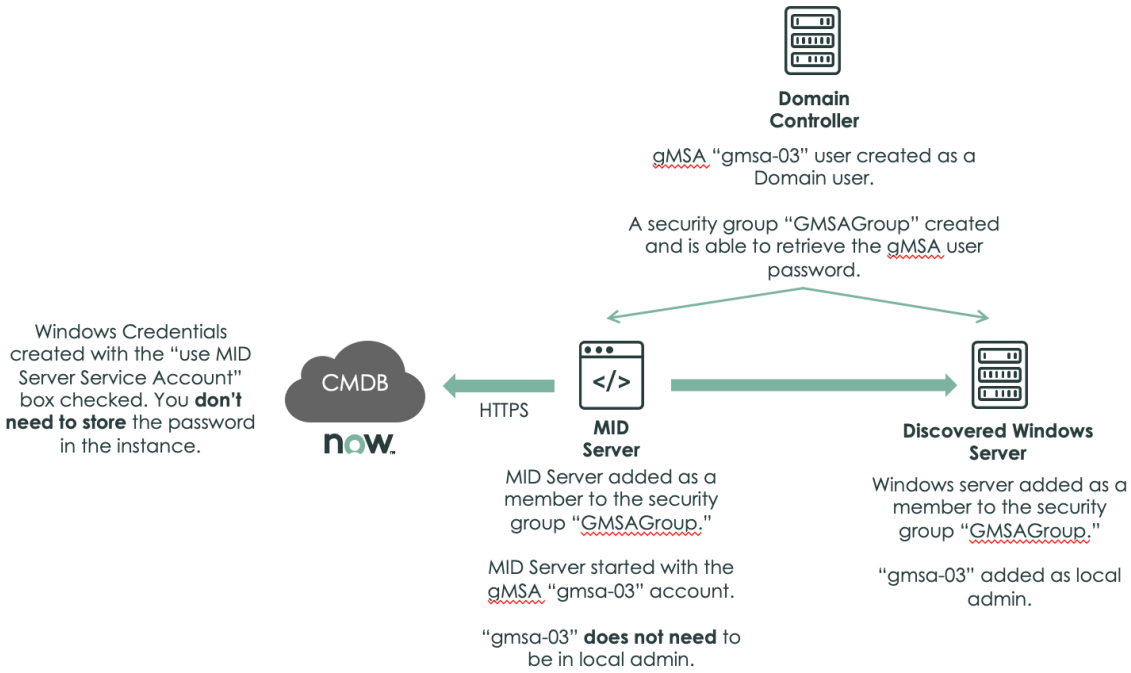
Vorteile

Nachdem Sie Discovery für die Verwendung von gMSA konfiguriert haben, wird die Passwortverwaltung für dieses Konto vom Windows-Betriebssystem verarbeitet. Daher können Sie Windows Discovery ausführen, ohne die Anmeldeinformationen für die ServiceNow-Instanz freizugeben. Es ergeben sich unter anderem die folgenden Vorteile:

- Sie müssen gMSA-Passwörter nicht selbst verwalten.
- Sie können den Zyklus der gMSA-Passwortrotation für eine bessere Sicherheit auswählen.
- Sie müssen das Passwort nicht in der ServiceNow-Instanz speichern.
- Der gMSA-Benutzer muss nicht Mitglied einer Domänenadministratorgruppe sein.
- Der als MID-Server-Servicekonto verwendete gMSA-Benutzer muss sich nicht in der lokalen Administratorgruppe des MID-Servers befinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Ansicht von Discovery mit gMSA



gMSA für Discovery konfigurieren

Zur Verwendung von gMSAs für ohne Anmeldeinformationen Discovery

Vorbereitungen

Erforderliche Rolle: admin

Prozedur

1. Erstellen Sie in der PowerShell-Befehlszeile mit den folgenden Befehlen einen KDS-Stammschlüssel auf einem Domänencontroller:

   ```
   Add-KdsRootKey -EffectiveImmediately
   ```

   oder

   ```
   Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))
   ```

2. Richten Sie Ihr gMSA und Ihre Sicherheitsgruppen mit den Informationen zu gruppenverwalteten Servicekonten unter https://docs.microsoft.com ein.
3. Starten Sie MID-Server mit dem gMSA-Account. Befolgen Sie dabei die Anweisungen zur Verwendung von gMSA: MID-Server unter Windows installieren
4. Erstellen Sie Windows-Anmeldeinformationen für die Instanz und aktivieren Sie das Kontrollkästchen **MID Server-Service-Account verwenden**.
5. Starten Sie Discovery auf dem Server, auf dem der MID-Server gehostet wird, und auf einem anderen Computer.

Erkennung ohne Anmeldeinformationen mit Nmap

Wenn die Instanz aufgrund eines Authentifizierungsfehlers ein Konfigurationselement (CI) nicht identifiziert, kann Discovery oder Service Mapping ausgewählte Nmap-Befehle (Network Mapper) mit einem MID Server ausführen, um ohne Anmeldeinformationen einige Basisinformationen über das CI zu sammeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein MID-Server-Administrator kann Nmap auf einzelnen MID-Servern installieren , die auf einem Windows-Host ausgeführt werden. Diese MID Server können dann einige Basisinformationen über CIs in Ihrem Netzwerk erkennen, wenn die normale Authentifizierung fehlschlägt.

Wichtig: Selbst gehostete Kunden, deren Netzwerksicherheit keine Downloads von `install.service-now.com` zulässt, muss Nmap manuell auf ihrem System installieren und konfigurieren. Beziehen Sie sich auf Installieren von Nmap auf einem selbst gehosteten System für Anweisungen.

Durch eine anmeldedatenlose Erkennung können Host- und Anwendungs-CIs erstellt und geändert werden, wenn Anmeldeinformationen fehlen oder falsch konfiguriert sind. Wenn eine auf Anmeldeinformationen basierende Erkennung erfolgreich durchgeführt wird, nachdem Nmap ein CI erstellt hat, gleicht das System die Informationen ab, die für die einzelnen Erkennungstypen gesammelt wurden.

Von Nmap erkennbare Elemente

Die während einer anmeldedatenlosen Erkennung ausgeführten Nmap-Befehle bieten folgende Möglichkeiten:

- Führen Sie eine umgekehrte DNS-Namensauflösung durch, um den Host anhand der IPv4-Adresse zu identifizieren.
- Geben Sie die MAC-Adresse des Hosts zurück, wenn sich dieser im selben Subnetz befindet wie der Host, der den Nmap-Befehl ausführt.
- Erkennen Sie auf einem Zielhost installierte Anwendungen.
- Erkennen Sie das Betriebssystem eines Zielhosts und die BS-Version.

Hinweis:

Die anmeldedatenlose Erkennung klassifiziert Router und Switches als Hardware. Dadurch werden keine CIs speziell für sie erstellt oder aktualisiert.

Die Erkennung ohne Anmeldeinformationen sollte nur in bekannten Subnetzen verwendet werden, in denen Anmeldeinformationen nicht praktikabel sind, und sollte nicht langfristig verwendet werden.

Nmap-Discovery-Scans ohne Anmeldeinformationen auf Cloud-Computing-Plattformen

Es stellt in vielen Fällen einen Verstoß gegen die Nutzungsbedingungen dar, Nmap-Scans zu oder von einer beliebigen Ressource innerhalb eines Cloud-Computing-Services wie Amazon Web Service, Microsoft Azure, IBM Cloud oder Google Cloud Platform auszuführen. Die Amazon Web Service(AWS)-Umgebung beispielsweise ist streng reguliert und erfordert die Erlaubnis von AWS über das Formular AWS-Schwachstellen-/Penetrationstestanforderung . Nicht autorisierte Tests mit AWS-Services oder AWS-eigenen Ressourcen sind nicht zulässig. Aus diesem Grund ist eine Erkennung ohne Anmeldeinformationen in einer Cloud-Computing-Serviceumgebung nicht angezeigt. Wenn ein Verstoß gegen die entsprechenden Richtlinien vorliegt, kann dies zur Beendigung des Services führen. Bitte wenden Sie sich an Ihren Platform Service Provider, um Informationen über Einschränkungen oder Berechtigungsanforderungen für die Ausführung von Nmap zu erhalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Nmap installierte Komponenten

Das Plugin „Discovery - IP Based“ [com.snc.discovery.ip_based], das die Nmap-Funktionalität bereitstellt, wird automatisch aktiviert, wenn entweder Discovery oder Service-Mapping aktiv ist. Das Plugin „Discovery - IP Based“ stellt die folgenden Nmap-Komponenten bereit:

Komponente	Beschreibung
Systemeigenschaft	Die Eigenschaft **mid.discovery.credentialless.enable** aktiviert oder deaktiviert Nmap für alle MID Server, auf denen Nmap installiert ist und die mit der Instanz verbunden sind. Diese Eigenschaft wird mit dem Plugin „Discovery“ installiert und ist standardmäßig aktiviert. Sie kann von einem Systemadministrator konfiguriert werden.
MID Server-Eigenschaften	Die folgenden Eigenschaften aus der Tabelle „MID Server-Eigenschaft“ [ecc_agent_property] sollten nicht konfiguriert werden: • **mid.nmap.version**: Version von Nmap, die auf MID Servern in Ihrer Umgebung installiert ist. Dieses Feld wird im Formular „MID Server“ [ecc_agent] angezeigt, nachdem Nmap installiert wurde. • **nmap.safe.scripts**: Definiert die Liste der Nmap-Skripts, die als sicher für die Verwendung während der Ausführung der Nmap-Phase zur Anwendungsversionserkennung (Befehlsoption -sV) klassifiziert sind • **nmap.npcap.version**: Die Version von Npcap, die mit Nmap installiert wird. Das Nmap-Installationsprogramm kann nur Upgrades von vorhandenen Npcap-Installationen durchführen, auf die es stößt.
Felder	• **Discovery-Port ohne Anmeldeinformationen [cl_port]**: Optionales Feld in der Anwendungstabelle [cmdb_ci_appl], in dem die Nummer eines Ports angezeigt wird, der durch die anmeldedatenlose Erkennung gescannt wurde. Anhand dieser Portnummer wird bestimmt, ob die CMDB das CI für eine von Nmap zurückgegebene Anwendung enthält oder ob ein neues CI erstellt werden muss. • **Discovery-Quelle [discovery_source]**: Optionales Feld in der Tabelle „Konfigurationselement“ [cmdb_ci], dem die Option **CredentiallessDiscovery**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponente	Beschreibung
	hinzugefügt wird. Diese Option zeigt an, dass die anmeldedatenlose Erkennung zum Erstellen eines CI verwendet wurde.
Nmap-Fähigkeit für MID Server	Die **Nmap-** MID-Server-Fähigkeiten werden dem MID-Server hinzugefügt, wenn Nmap installiert wird, und werden automatisch entfernt, wenn Nmap deinstalliert wird. Nur MID Server mit dieser Fähigkeit können anmeldedatenlose Erkennungen ausführen. Ein Systemadministrator kann diese Fähigkeit nicht manuell hinzufügen oder entfernen. Selbst gehostete Kunden mit der Wartungsrolle können die Nmap-Fähigkeit ändern oder löschen, sollten dies jedoch unterlassen. Service Mapping prüft nicht, ob die **Nmap-** Fähigkeit vorhanden ist, und wählt den MID-Server nur anhand der IP-Adresse aus. Um sicherzustellen, dass Service-Mapping keinen MID-Server ohne **Nmap-** Fähigkeit auswählt, installieren Sie Nmap auf allen MID-Servern, die den IP-Adressbereichen zugewiesen sind, für die Discovery ohne Anmeldeinformationen verfügbar sein soll. Wenn Service-Mapping einen MID-Server für Discovery ohne Anmeldeinformationen auswählt, der nicht über Nmap-Fähigkeiten verfügt, wird diese Fehlermeldung in der Zuordnung am Standort des erkannten CI angezeigt: `Nmap ist nicht auf dem MID-Server installiert. Stellen Sie sicher, dass alle MIDs, die für die Verarbeitung der ausgewählten IP-Adresse konfiguriert sind, über eine Nmap-Fähigkeit verfügen. Nmap-Stammverzeichnispfad ist nicht vorhanden:<path>` **Hinweis:** Die MID Server-Fähigkeit **ALLE** schließt die **Nmap**-Fähigkeit nicht ein.
Npcap	Npcap ist die Paketerfassungsbibliothek von Nmap für Windows. Mit Npcap kann Nmap schnell Port-Scans durchführen und die Familie des Betriebssystems identifizieren, das auf dem Ziel ausgeführt wird. Pro MID Server-Host wird nur eine Kopie von Npcap installiert. Da Npcap von anderen Anwendungen verwendet werden kann, wird Npcap

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponente	Beschreibung
	bei der Deinstallation von Nmap nicht automatisch deinstalliert. Sie müssen Npcap manuell deinstallieren, nachdem Sie sich davon überzeugt haben, dass keine weiteren Abhängigkeiten vorhanden sind.
Muster	• **Credentialless Discovery Network Device**: Scannt eine Host-IP-Adresse mit einem Nmap-Befehl, um den Host zu identifizieren. Dieses Muster startet das Skript **Credentialless Discovery Network Device – PreLaunch**, um die Liste der zu untersuchenden Ports aus der IP-Service-Tabelle [cmdb_ip_service] abzurufen. Ändern Sie dieses Skript nicht. • **Credentialless Discovery Application**: Scannt einen Port an einer IP-Adresse mithilfe eines Nmap-Befehls, um den Anwendungsservice zu identifizieren, der diesen Port aktiv abhört. Service Mapping startet dieses Muster, wenn alle auf Anmeldeinformationen basierten Portklassifizierungsschritte fehlschlagen. Discovery erstellt ein CI in der Anwendungstabelle [cmdb_ci_appl], wenn der Port geöffnet ist und den Service anhand des Namens und des Produkts identifizieren kann. Wenn der Service auf keinen der Scan-Versuche reagiert, konsultiert Nmap die Registrierung von Nmap-Services und ermittelt, welcher Service wahrscheinlich auf diesem Port ausgeführt wird. Wenn Nmap erraten muss, welche Anwendung auf einem gescannten Port ausgeführt wird, erstellt das Muster „Credentialless Discovery Application“ kein Anwendungs-CI und aktualisiert auch kein vorhandenes CI.
MID Server-Skripteinbindungen	• **SetCredentialLessDeviceClassName**: Bestimmt, welches Host-CI nach erfolgreicher Ausführung des Nmap-Befehls erstellt oder aktualisiert wird. Ändern Sie dieses Skript nicht. • **CredentialLessApplicationClassNameMapper**: Ordnet das Serviceprodukt, den Servicenamen und zusätzliche Serviceinformationen, die von Nmap für den gescannten Port bereitgestellt werden, einer unterstützten Anwendungstabelle in der Instanz zu. Systemadministratoren können dieses Skript ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponente	Beschreibung
	• **SetCredentialLessApplicationClassName**: Stellt sicher, dass das Skript *CredentialLessApplicationClassNameMapper* nur einmal aufgerufen wird. Ändern Sie dieses Skript nicht.
System-Skripteinbindung	Die Skripteinbindung *CredentiallessDiscoveryAjax* wird für die Instanz ausgeführt und erledigt die Installation und Deinstallation von Nmap auf Windows MID Servern, die über UI-Aktionen im Formular ausgeführt werden. Ändern Sie dieses Skript nicht.

Hosterkennung ohne Anmeldeinformationen

Eine Hosterkennung ohne Anmeldeinformationen findet statt, wenn ein gescannter Host zwar in Betrieb, aber inaktiv ist oder wenn alle konfigurierten, auf Anmeldeinformationen basierten Klassifizierungs-Probes fehlgeschlagen sind.

Vorgehensweise zum Starten des Hosterkennungsmusters

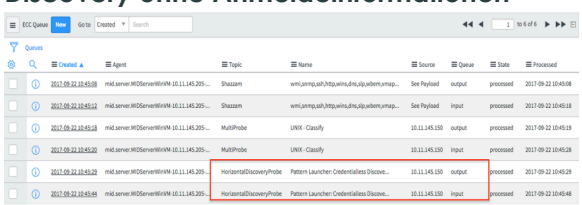
Wenn die Shazzam-Probe einen Host scannt, der zwar in Betrieb, aber inaktiv ist, und wenn auf Anmeldeinformationen basierte Klassifizierungs-Probes fehlschlagen, startet die horizontale Erkennung das Muster „Credentialless Discovery Network Device“, um Hostinformationen zu erfassen. Wenn für den gescannten Host kein CI definiert ist, startet Service Mapping die Probe HorizontalDiscoveryProbe, die wiederum das Muster Credentialless Discovery Network Device startet. Dieses Muster versucht, ein neues CI zu erstellen, wenn für den gescannten Host noch kein CI existiert, oder ein vorhandenes CI in der Hardwaretabelle [cmdb_ci_hardware] zu aktualisieren.

Wichtig: Damit das Muster Credentialless Discovery Network Device gestartet werden kann, muss die Systemeigenschaft *mid.discovery.credentialless.enable* auf **true** festgelegt sein. Zum Deaktivieren legen Sie diese Eigenschaft auf **false** fest.

ECC-Warteschlangeneinträge

Das System erstellt die folgenden Einträge in der ECC-Warteschlange, während die HorizontalDiscoveryProbe ausgeführt wird.

Discovery ohne Anmeldeinformationen



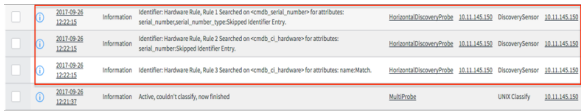
Protokollnachrichten

Diese Protokollnachrichten werden während der Ausführung der HorizontalDiscoveryProbe veröffentlicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokollnachrichten (Fortsetzung)

Host-Bezeichner ohne Anmeldeinformationen

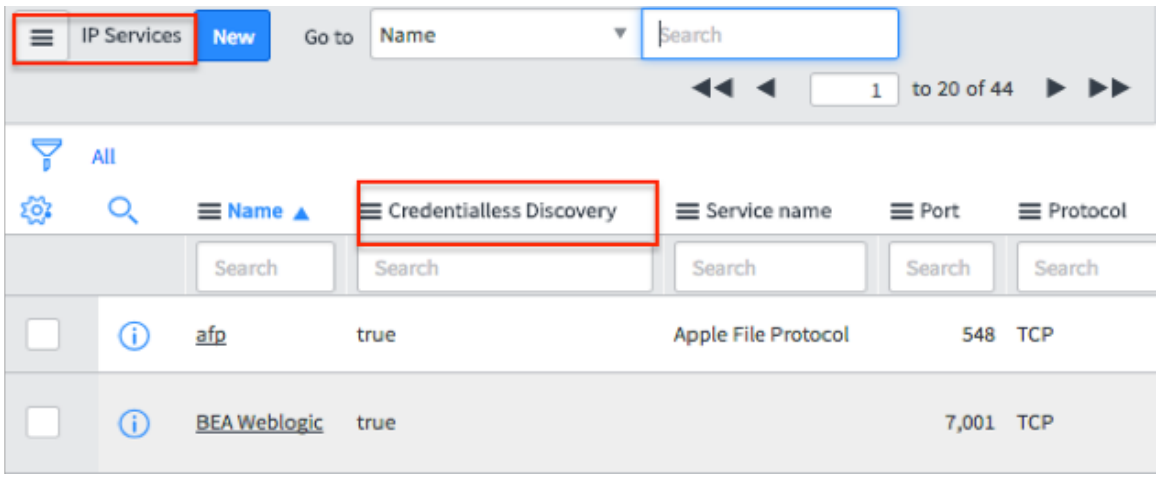


Nmap-Befehl

Der auf dem MID Server ausgeführte Nmap-Befehl bestimmt, ob der Host in Betrieb ist. Unter Verwendung der IP-Adresse und einer Liste von Ports, die durch das Muster an Nmap übergeben werden, führt Nmap eine umgekehrte DNS-Namensauflösung durch, um den der IP-Adresse zugeordneten Hostnamen zu identifizieren. Wenn mehrere Hostnamen konfiguriert sind, wird der erste von Nmap zurückgegebene Name verwendet. Wenn kein Hostname konfiguriert ist, wird zum Erstellen des Host-CI die IP-Adresse des Remotehosts verwendet. Die in der Nmap-Installation enthaltene Npcap-Paketerfassungsbibliothek identifiziert die Familie des Hostbetriebssystems. Wenn sich der gescannte Host in demselben Subnetz wie der Windows-MID Server-Host befindet, der Nmap ausführt, wird die MAC-Adresse des Remotehosts zurückgegeben.

Hinweis: Die Liste der Ports, für deren Scan Nmap während der Hosterkennung ohne Anmeldeinformationen konfiguriert ist, wird in der Tabelle „IP-Service“ [cmdb_ip_service] gespeichert, die bearbeitet werden kann. Standardmäßig sind alle Ports zum Scannen verfügbar. Um die Verwendung eines beliebigen Ports für einen Nmap-Scan zu blockieren, legen Sie den Wert in der Spalte **Discovery ohne Berechtigung [cl_discovery]** auf **false** fest.

Liste der Ports ohne Anmeldeinformationen



Host-CIs erstellen oder aktualisieren

Nach der erfolgreichen Ausführung des Musters „Credentialless Discovery Network Device“ wird das MID Server-Skript `SetCredentiallessDeviceClassName` ausgeführt, um die Betriebssystemfamilie des erkannten Hosts zu identifizieren. Die Systemklasse des Host-CI basiert auf der Betriebssystemfamilie, die von Nmap zurückgegeben wird. Wenn die BS-Familie einem der sechs unterstützten Serverbetriebssysteme entspricht, verwendet das System eine von der Basisklasse „Hardware“ [cmdb_ci_hardware] abgeleitete Serverklasse (zum Beispiel „Linux Server“ [cmdb_ci_linux_server]). Wenn keine Übereinstimmung gefunden wird, verwendet das System die Basisklasse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn das Problem mit den Anmeldeinformationen gelöst ist und Discovery erneut ausgeführt wird, aktualisiert die Instanz das von der anmeldedatenlosen Erkennung erstellte Host-CI mit der Seriennummer, dem Hostnamen und der Systemklasse, die von der auf Anmeldeinformationen basierenden Erkennung bereitgestellt werden.

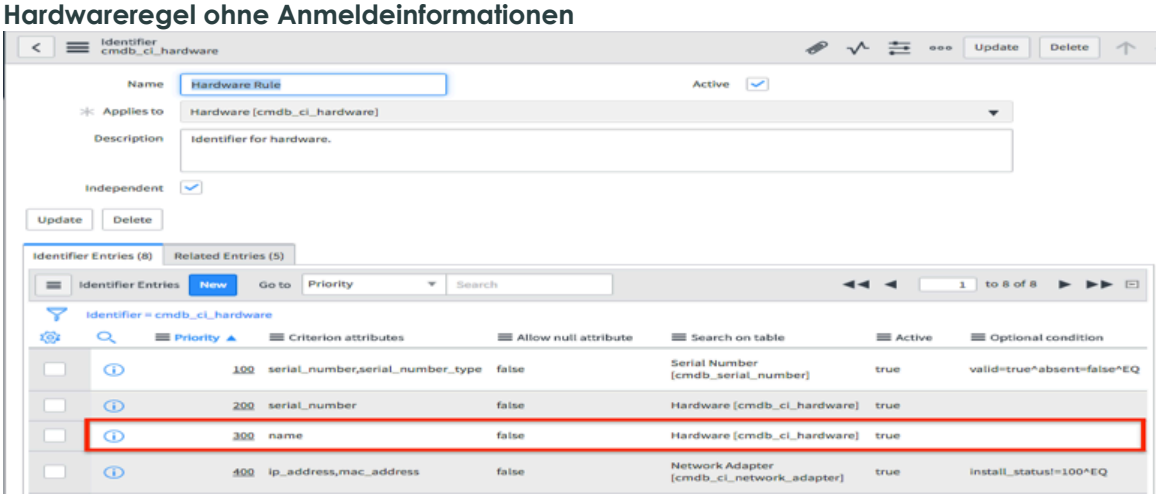
Unterstützte BS-Familien

BS-Familie	CI-Tabelle
AIX	cmdb_ci_aix_server
HP-UX	cmdb_ci_hpux_server
Linux	cmdb_ci_linux_server
Solaris	cmdb_ci_solaris_server
OS X oder iOS	cmdb_ci_osx_server
Windows	cmdb_ci_win_server
Nicht definiert	cmdb_ci_hardware

Hardwareidentifizierung

Das Plugin „Discovery - IP Based“ [com.snc.discovery.ip_based] fügt der Hardwareregel für die Basistabelle „Hardware“ [cmdb_ci_hardware] einen Bezeichner hinzu, der dem **Namen** des Host-CI für Nmap-Scans entspricht. Die Hardwareregel wird sowohl von der auf Anmeldeinformationen basierenden als auch der anmeldedatenlosen Erkennung verwendet.

Hardwareregel ohne Anmeldeinformationen



Anwendungserkennung ohne Anmeldeinformationen

Die Anwendungserkennung ohne Anmeldeinformationen versucht, einen Anwendungsservice zu identifizieren, der einen bestimmten Port an einer bestimmten IP-Adresse aktiv abhört.

Muster zur Anwendungserkennung

Service Mapping startet das Muster „Credentialless Discovery Application“, wenn alle auf Anmeldeinformationen basierten Portklassifizierungsschritte fehlschlagen. Das Muster führt auf einem Windows-MID Server mit installiertem Nmap einen Nmap-Befehl aus, der so konfiguriert ist, dass er eine Anwendungs-/Versionserkennung für eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bestimmte IP-Adresse und einen bestimmten Port des Remotehosts durchführt. Wenn der von Nmap gescannte Port offen ist, führt das Muster die MID Server-Skripteinbindung *CredentiallessApplicationClassNameMapper* aus, die das Serviceprodukt, den Servicenamen und zusätzliche Informationen zuordnet, die von Nmap für eine unterstützte ServiceNow-Anwendungstabelle bereitgestellt werden. Wenn das Skript das zurückgegebene Produkt einer entsprechenden Tabelle zuordnen kann, die von der Basisanwendungstabelle [cmdb_ci_appl] abgeleitet ist, übergibt das Skript diese Informationen an das Muster. Das Muster übergibt die Übereinstimmung an den Discovery-Bezeichner, um gegebenenfalls ein CI erstellen oder abgleichen zu können. Wenn die von Nmap zurückgegebenen Informationen mit keiner abgeleiteten Tabelle übereinstimmen, verwendet die Instanz die Basisanwendungstabelle [cmdb_ci_appl], um das CI zu erstellen.

Wichtig: Damit das Muster „Credentialless Discovery Application“ gestartet werden kann, muss die Systemeigenschaft *mid.discovery.credentialless.enable* auf **true** festgelegt sein. Zum Deaktivieren legen Sie diese Eigenschaft auf **false** fest.

Beispiel-Scan

Die folgenden Informationen wurden vom Port-Scan einer Nmap-Anwendungs-/Versionserkennung auf einem Linux-Testsystem zurückgegeben. Sie veranschaulichen den Typ der Anwendungsdaten, die von Nmap-Scans zurückgegeben werden können.

Informationen	Port
Portstatus	open
Servicename	ssh
Serviceprodukt	OpenSSH
Zusätzliche Serviceinformationen	Protocol 2.0

Standardmäßige Anwendungszuordnungen

Die MID Server-Skripteinbindung *CredentiallessApplicationClassNameMapper* ist mit einer Teilmenge der gängigsten Anwendungstabellen konfiguriert, die für Discovery und Service Mapping verfügbar sind. Ein Benutzer mit der Rolle agent_admin kann diese Skripteinbindung bearbeiten, um zusätzliche CI-Tabellen hinzuzufügen, die von der Anwendungserkennung ohne Anmeldeinformationen zur Zuordnung zu einer abgeleiteten CI-Anwendungsklasse verwendet werden kann.

Diese Tabelle zeigt Beispiele für Übereinstimmungen, die von Nmap auf einem Testsystem zurückgegeben wurden und die von CMDB Identification and Reconciliation in definierte Produkte aufgelöst wurden. In vielen Fällen war der von Nmap zurückgegebene Servicename nicht erforderlich, um eine Übereinstimmung zu bestimmen. Stattdessen waren in der Tabelle aufgeführte Servicenamen erforderlich, um eine Übereinstimmung zu bestimmen.

Von Nmap zurückgegebene Produkte, die nicht in definierte Discovery-Produkte aufgelöst werden können, haben das folgende Namensformat: **<**serviceProduct**>:<**serviceExtrainfo**>:<**serviceName**>**. Wenn ein beliebiger Wert in dieser Zeichenfolge NULL ist, wird er aus dem Namen gelöscht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **serviceProduct**: Von Nmap zurückgegebene Serviceproduktinformationen
- **serviceExtrainfo**: Alle zusätzlichen Informationen, die Nmap über die Anwendung zurückgibt und die zur Identifizierung der Anwendung beitragen könnten, zum Beispiel Protokollinformationen
- **serviceName**: Name des installierten Service oder Daemon des Produkts

Beispiele für gute Entsprechungen, die gelöst wurden

Nmap-Antwort			Skriptantwort - Bezeichnereingabe	
Serviceprodukt	**Servicename**	**Zusätzliche Serviceinformatione**	**Erkanntes Produkt**	**CI-Anwendungstabelle**
Apache Tomcat/Coyote JSP Engine 1.1	N/V	NULL	Tomcat	cmdb_ci_app_server_tomcat
Apache httpd 2.2.10 ((Linux/ SUSE))	N/V	NULL	Apache-Webserver	cmdb_ci_apache_web_server
IBM HTTP Server	N/V	Abgeleitet von Apache	Apache-Webserver	cmdb_ci_apache_web_server
IBM DB2-Datenbankserver (QDB2/LINUX)	N/V	NULL	DB2-Instanz	cmdb_ci_db_db2_instance
Microsoft Exchange smtpd	smtp	NULL	Exchange-Clientzugriffsserver	cmdb_ci_exchange_cas
Microsoft Exchange 2010-Protokollkopierer	msexchange-logcopier	NULL	Exchange-Postfach	cmdb_ci_exchange_mailbox_ser
JBoss-Service httpd	N/V	NULL	JBoss	cmdb_ci_app_server_jboss
Microsoft IIS httpd 6.0	N/V	NULL	Microsoft iis-Webserver	cmdb_ci_microsoft_iis_web_serve
Microsoft SQL Server 2005 9.00.4035; SP3	N/V	NULL	Microsoft SQL Server	cmdb_ci_db_mssql_instance
MongoDB 2.5.1	N/V	NULL	MongoDB-Instanz	cmdb_ci_db_mongodb_instance
MySQL 5.5.51	N/V	NULL	MySQL-Instanz	cmdb_ci_db_mysql_instance
nginx 1.4.6 (Ubuntu)	N/V	NULL	Nginx-Webserver	cmdb_ci_nginx_web_server
PostgreSQL-DB	N/V	NULL	PostgreSQL-Instanz	cmdb_ci_db_postgresql_instance
Oracle WebLogic Server	N/V	NULL	Weblogic	cmdb_ci_app_server_weblogic
IBM WebSphere MQ 6.0	N/V	NULL	IBM WebSphere MQ	cmdb_ci_appl_ibm_wmq

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für gute Entsprechungen, die gelöst wurden (Fortsetzung)

Nmap-Antwort			Skriptantwort - Bezeichnereingabe	
Serviceprodukt	Servicename	Zusätzliche Serviceinformatione	Erkanntes Produkt	CI-Anwendungstabelle
IBM WebSphere Application Server 6.1	N/V	NULL	IBM Websphere	cmdb_ci_app_server_websphere
OpenSSH : ssh	N/V	NULL	OpenSSH	cmdb_ci_appl
Oracle-Instanz	N/V	NULL	Oracle-Datenbank	cmdb_ci_db_ora_instance
Oracle-Instanz	N/V	NULL	Oracle TNS Listener	cmdb_ci_db_ora_instance
product-A	service-B	NULL	product-A:service-B	cmdb_ci_appl
product-A	service-B	extrainfo-C	product-A:extrainfo-C:service-B	cmdb_ci_appl

Beispiele für nicht eindeutig übereinstimmende Anwendungen

In diesem Beispiel stimmen die von Nmap zurückgegebenen Informationen mit keiner abgeleiteten Tabelle überein. Die Instanz muss die Basisanwendungstabelle [cmdb_ci_appl] verwenden, um das CI zu erstellen.

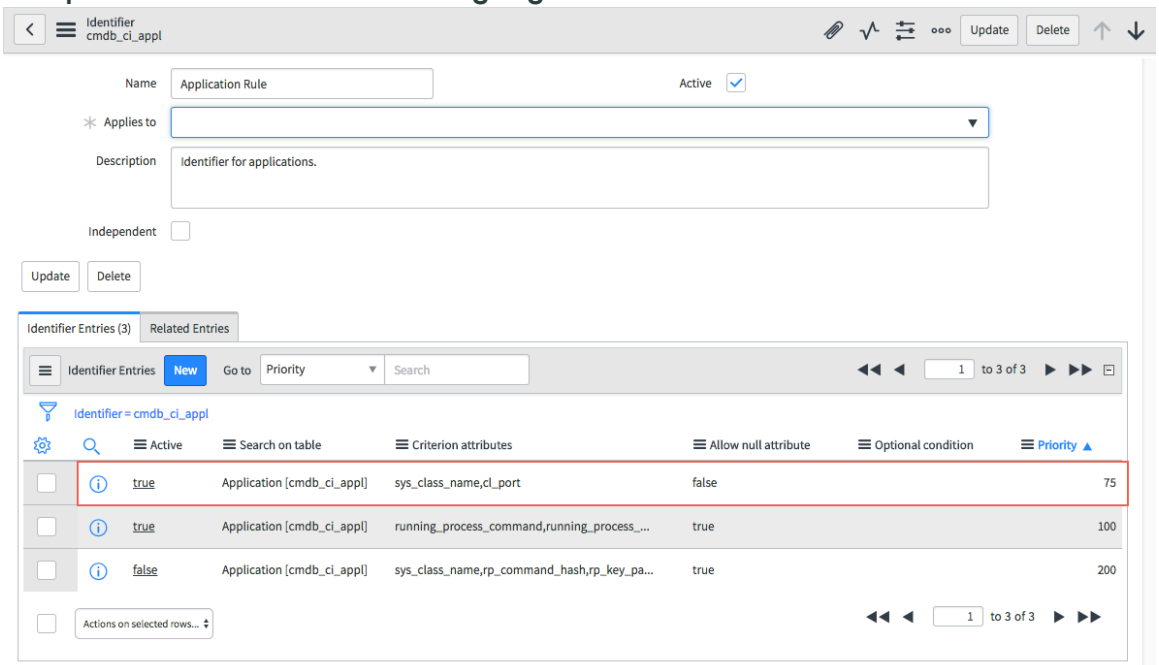
Gescannte Anwendung	Nmap-Antwort			Skriptantwort - Bezeichnereingabe	
	Serviceprodukt	Servicename	Zusätzliche Serviceinformati	Erkanntes Produkt	CI-Anwendungstab
ExchangeHub	Microsoft Windows RPC	msrpc	„null“	Microsoft Windows RPC:msrpc	cmdb_ci_appl
HAProxy Lastenausgleich	IBM HTTP Server (Abgeleitet von Apache)	http	„null“	IBM HTTP Server (Abgeleitet von Apache):http	cmdb_ci_appl
SharePoint	Oracle-Datenbank	http	„null“	Oracle Database:http	cmdb_ci_appl
SharePoint	Oracle-Instanz	N/V	„null“	Oracle-Datenbank	cmdb_ci_appl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsidentifizierung

Das Plugin „Discovery - IP Based“ [com.snc.discovery.ip_based] fügt der Anwendungsregel für die Anwendungstabelle [cmdb_ci_appl] einen Bezeichner hinzu, der dem sys_class_name und cl_port für Nmap-Scans entspricht.

Nmap-Bezeichner für die Anwendungsregel



Nmap-Befehle und mit der anmeldedatenlosen Erkennung erfasste Daten

Nmap wird beim Erfassen von Daten in Phasen ausgeführt und führt einen kontrollierten Satz sicherer Befehle mit zwei Mustern zum Untersuchen von Anwendungen und Geräten aus.

Von Nmap bei der Hosterkennung zurückgegebene Daten

Für einen Host, von dem Nmap feststellt, dass er in Betrieb ist, gibt Nmap die folgenden Daten zurück:

- **Betriebssystemfamilie**: Wenn die Betriebssystemfamilie eine der sechs unterstützten Serverbetriebssystemfamilien ist, wird ein Host-CI verwendet, das der entsprechenden Serverklasse zugeordnet ist, um das Host-CI zu erstellen oder zu aktualisieren.
  Wenn die von Nmap zurückgegebene Betriebssystemfamilie nicht zu den unterstützten Serverbetriebssystemen gehört, wird ein Host-CI erstellt oder mithilfe der Hardwarebasisklasse [cmdb_ci_hardware] aktualisiert.
- **MAC-Adresse**: Wenn sich der gescannte Host im selben Subnetz wie der MID Server-Host unter Windows befindet, der die Nmap-Befehle ausführt, gibt Nmap die MAC-Adresse des Remotehosts zurück.

Von Nmap während der Hosterkennung ausgeführte Befehle

Der MID Server übergibt die IP-Adresse eines Remotehosts an den Nmap-Befehl und eine Reihe von Ports, die der IP-Servicetabelle entnommen sind. Der Host muss von Nmap gemeldet werden, damit er in Betrieb ist. Der Host ist in Betrieb, wenn der von Nmap zurückgegebene Portstatus **Offen** oder **open/filtered (Offen/Gefiltert)** lautet. Wenn gemeldet wird, dass der Host in Betrieb ist, wird die zurückgegebene Betriebssystemfamilie untersucht, um die Klasse zu bestimmen, die zum Erstellen oder Aktualisieren des Host-CI verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
-PS	Mit der Option TCP-SYN wird bestimmt, ob der Host online ist. Diese Option sendet ein leeres TCP-Rohpaket mit dem SYN-Flag an alle in der Scan-Liste angegebenen Ports. Nmap meldet, dass der Host online ist, wenn ein SYN/ACK-TCP-Paket zurückgegeben wird und wenn ein RST zurückgegeben wird, wodurch angegeben wird, dass der Port geschlossen ist. Der Nmap-Hostcomputer unterbricht die neu entstehende Verbindung mit einem RST anstelle eines ACK, da die SYN/ACK-Antwort aus dessen Sicht unerwartet ist. Wenn mehrere Port-Probes angegeben sind, werden sie parallel gesendet. Anforderungen: • Rohpaketberechtigungen • Muss unter UNIX als Root ausgeführt werden • Administratorrechte unter Windows
-PA	Erkennt Paketfilterungsgeräte. Diese Option ist eine TCP-ACK-Hosterkennung mit einer angegebenen Liste von Ports. Wenn keine Liste definiert ist, wird der Standardport 80 verwendet. Nmap sendet ein leeres TCP-Rohpaket mit gesetztem ACK-Flag. Diese Aktion bestätigt Daten über eine hergestellte TCP-Verbindung und veranlasst den Remotehost, mit einem RST-Paket zu antworten. Wenn der Remotehost mit einem RST-Paket antwortet, weiß Nmap, dass der Host online ist. Die ACK-Ping-Probe kann die Paketfilterung von TCP-SYN-Paketen durch zustandslose Paketfilterung, Netzwerkentitäten wie Firewalls, Router und Host-Routingtabellen/Firewall-Software überwinden. Stateful-Firewalls verwerfen unerwartete Pakete, wodurch das ACK-Paket verworfen wird, was die Wahrscheinlichkeit erhöht, dass die SYN-TCP-Probe durchkommt. Anforderungen: • Rohpaketberechtigungen • Muss unter UNIX als Root ausgeführt werden • Administratorrechte unter Windows **Hinweis:** Beide Pakettypen, Ping-SYN (-PS) und Ping ACK (-PA), können zusammen im selben Scan-Versuch konfiguriert werden.
-O	Aktiviert die BS-Erkennung für einen Remotehost und gibt den Namen des Anbieters, das zugrunde liegende BS, die BS-Generation und den Gerätetyp wie Router oder Switch an Nmap verwendet Fingerprinting anhand des TCP/IP-Stapels, um die auf dem Host ausgeführte Betriebssystemfamilie zu bestimmen. Nmap sendet eine Reihe von TCP- und UPD-Paketen an den Host und untersucht die Antworten. Nachdem die Antworten gründlich getestet wurden, vergleicht Nmap die Ergebnisse mit seiner Datenbank **nmap-os-db** und gibt die BS-Details aus, wenn eine Übereinstimmung vorliegt. Wenn Nmap das Betriebssystem nicht erraten kann und mindestens ein offener und ein geschlossener

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
	Port gefunden wurden, werden ein Fingerabdruck und eine URL generiert, die an `nmap.org` übermittelt werden können. Bei der BS-Erkennung werden keine Skripts der Nmap Scripting Engine (NSE) verwendet. Die BS-Erkennung wird nach der Erkennung der Anwendungs-/Serviceversion ausgeführt, wodurch die Genauigkeit der BS-Erkennung verbessert wird. Die Ergebnisse der beiden Scan-Typen können sich jedoch widersprechen. Die BS-Erkennung wird auf der TCP-Transportschicht ausgeführt, während die Versionserkennung für die Anwendung bzw. den Service auf einer höheren Ebene im TCP-Stapel ausgeführt wird. Anforderungen: • Rohpaketberechtigungen • Muss unter UNIX als Root ausgeführt werden • Administratorrechte unter Windows
-p	Liste der zu scannenden Ports
-T4	Aggressive Timing-Vorlage von Nmap
-v	Zum Aktivieren ausführlicher Details. Dieser Befehl wird normalerweise verwendet, um Betrachtern der Standardausgabe den Fortschritt anzuzeigen. Dies kann jedoch dazu führen, dass die Skripts der Nmap Scripting Engine (NSE) zusätzliche Details enthalten.
-Pn	Zum Deaktivieren des Standard-Ping. Mit diesem Befehl wird die anfänglichen Scan-Phase der Nmap-Hosterkennung übersprungen, und alle Hosts werden so behandelt, als wären sie online. Verwenden Sie diesen Befehl, wenn Sie einen Port-Scan durchführen möchten, auch wenn die von den Discovery-Standard-Probes ausgeführten Ports keinen offenen Port finden.
-r	Scannt Ports nacheinander ohne Randomisierung
--reason	Gibt den Grund an, aus dem Nmap einen Port mit einem bestimmten Status klassifiziert hat
--system-dns	Anstelle der DNS-Namensserver wird für die umgekehrte DNS-Suche der DNS-Resolver des Betriebssystems verwendet. Diese Option ist langsamer als die Verwendung von DNS-Servern, da sie jeweils nur eine IP-Adresse auflösen kann, während mehrere rDNS-Anforderungen parallel ausgeführt werden. Der zurückgegebene Wert stimmt jedoch mit dem vom MID Server zurückgegebenen Wert überein, der zum Erstellen von Host-CIs verwendet wird.
-X -	Leitet `stdout` an eine XML-Datei um
2> <Datenpfad>	Leitet Fehlermeldungen, die Nmap an `stderr` geschrieben hat, zur angegebenen Datei um

Von Nmap während der Anwendungserkennung zurückgegebene Daten

Für einen Host, von dem Nmap feststellt, dass er in Betrieb ist, gibt Nmap die folgenden Daten zurück:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Portstatus**:
  - **Offen**: Eine Anwendung akzeptiert an dem Port aktiv TCP- (oder UDP-)Pakete.
  - **open|filtered (Offen|Gefiltert)**: Nmap kann nicht bestimmen, ob ein Port offen oder gefiltert ist. Ein offener Port gibt möglicherweise keine Antwort zurück, wenn UDP-, IP-Protokoll-, FIN-, NULL- und Xmas-Scans von Nmap verwendet werden.
- **Servicename**: Name des Service, der an dem Service-Port aktiv TCP- (oder UDP-)Pakete akzeptiert
- **Serviceprodukt**: Name der Anwendung, die an dem von Nmap identifizierten offenen Port ausgeführt wird
- **Zusätzliche Serviceinformationen**: Alle zusätzlichen, von Nmap zurückgegebenen Informationen, die Discovery zum Identifizieren der Anwendung verwenden kann

Von Nmap während der Anwendungserkennung ausgeführte Befehle

Der MID Server übergibt dem Nmap-Befehl eine IP-Adresse für einen Remotehost und einen zu scannenden Port. Nmap versucht, die Anwendung zu identifizieren, die den Port aktiv abhört, und bestimmt dann, ob ein neues CI erstellt oder ein vorhandenes aktualisiert werden soll. Der Host muss von Nmap gemeldet werden, damit er in Betrieb ist.

Zur Kursbestimmung verwendet Nmap die folgenden Informationen:

- Serviceprodukt
- Servicename
- Zusätzliche Serviceinformationen
- Status des gescannten Ports

Hinweis: Die Werte für das Serviceprodukt und den Servicenamen dürfen nicht NULL sein, und der Servicename darf nicht mit einem Fragezeichen enden. Nmap fügt Servicenamen ein Fragezeichen hinzu, wenn die Anwendung, die den gescannten Port abhört, erraten werden muss. Die Instanz erstellt oder aktualisiert kein Anwendungs-CI, wenn Nmap den Anwendungsnamen nicht aus der statischen Registrierungsdatei `nmap-services` abrufen kann.

Befehl	Beschreibung
-sS	TCP-SYN-Port-Scan (Stealth). Dies ist die standardmäßige Scan-Option, die niemals TCP-Verbindungen herstellt. Scans können zwischen **offenen**, **geschlossenen** und **gefilterten** Ports unterscheiden. Der TCP-SYN-Scan implementiert einen halboffenen Reset, der die Anforderung abbricht, bevor die Verbindung hergestellt werden kann. Der Port ist **offen** (die Anwendung horcht), wenn ein SYN/ACK zurückgegeben wird. Der Port ist **geschlossen**, wenn ein RST zurückgegeben wird. Wenn nach mehreren erneuten Übertragungen keine Antwort eingeht, wird der Port als **gefiltert** markiert. Der Port wird auch als gefiltert markiert, wenn ein ICMP-Fehler „nicht erreichbar“ (Typ 3, Code 1,2,3,9,10,13) empfangen wird. Anforderungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
	• Rohpaketberechtigungen • Ausführung als Root • Windows-Administratorrechte
-sV	Probes öffnen Ports, um Serviceprotokoll, Anwendungsname, Versionsnummer, Hostname, Gerätetyp, BS-Familie und verschiedene Details wie die SSH-Protokollversion zu bestimmen. Wenn Nmap eine Antwort erhält, die nicht mit der Datenbank übereinstimmt, werden ein Fingerabdruck und eine URL zur Übermittlung an **nmap.org** ausgegeben. Nmap sucht in seiner statischer Registrierungsdatei `nmap-services` nach der Portnummer, um den Namen eines Anwendungsservice zu bestimmen, der den Port möglicherweise aktiv abhört. Der von Nmap zurückgegebene Servicename wird mit einem Fragezeichen versehen, das anzeigt, dass Nmap seine Identität erraten musste. Die Instanz erstellt oder aktualisiert kein Anwendungs-CI, wenn Nmap die Anwendung an einem offenen Port errät. **Hinweis:** Dieser Befehl erfordert keine Rohpaketberechtigungen.
--datadir	Pfad zu dem Verzeichnis, das den sicheren Satz von Nmap-Skripts enthält, die während der Anwendungs-/Versionserkennung ausgeführt werden sollen
-p	Einzelner zu scannender Port
-T4	Aggressive Timing-Vorlage von Nmap
-v	Zum Aktivieren ausführlicher Details. Dieser Befehl wird normalerweise verwendet, um Betrachtern der Standardausgabe den Fortschritt anzuzeigen. Dies kann jedoch dazu führen, dass die Skripts der Nmap Scripting Engine (NSE) zusätzliche Details enthalten.
-Pn	Zum Deaktivieren des Standard-Ping. Mit diesem Befehl wird die anfänglichen Scan-Phase der Nmap-Hosterkennung übersprungen, und alle Hosts werden so behandelt, als wären sie online. Verwenden Sie diesen Befehl, wenn Sie einen Port-Scan durchführen möchten, auch wenn die von den Discovery-Standard-Probes ausgeführten Ports keinen offenen Port finden.
-r	Scannt Ports nacheinander ohne Randomisierung
--reason	Gibt den Grund an, aus dem Nmap einen Port mit einem bestimmten Status klassifiziert hat
--system-dns	Anstelle der DNS-Namensserver wird für die umgekehrte DNS-Suche der DNS-Resolver des Betriebssystems verwendet. Diese Option ist langsamer als die Verwendung von DNS-Servern, da sie jeweils nur eine IP-Adresse auflösen kann, während mehrere rDNS-Anforderungen parallel ausgeführt werden. Der zurückgegebene Wert stimmt jedoch mit dem vom MID Server zurückgegebenen Wert überein, der zum Erstellen von Host-CIs verwendet wird.
-X -	Leitet `stdout` an eine XML-Datei um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
2> <Datenpfad>	Leitet Fehlermeldungen, die Nmap an `stderr` geschrieben hat, zur angegebenen Datei um

PowerShell für Discovery und Service-Mapping

MID Server verwenden PowerShell und PowerShell Remoting für den Zugriff auf Konfigurationselemente (CIs) während der horizontalen Erkennung und der Erkennung von oben nach unten. Überprüfen Sie die MID Server-Parameter und Skripteinbindungen, Probe-Parameter und Anmeldeinformationen für die Verwendung von PowerShell.

PowerShell dient zur Steuerung und Automatisierung der Verwaltung von Windows-Servern und -Anwendungen.

MID Servers können PowerShell für die direkte Kommunikation mit Windows-Servern verwenden, wobei sowohl WMI- als auch WinRM-Protokolle verwendet werden. Für Windows-Services, die das WinRM-Protokoll verwenden, richtet der PowerShell-Prozess eine sichere PSSession ein (PowerShell-Remoting-Sitzung) ein, bis MID-Server die Abfrage eines Windows-Servers beendet. Bei Windows-Servern, die das WMI-Protokoll verwenden, sendet der PowerShell-Prozess jeden PowerShell-Befehl mit Anmeldeinformationen.

PowerShell ist auch die bevorzugte Methode für die Erkennung in mehreren Windows-Domänen. PowerShell ermöglicht es einem einzelnen MID-Server, sich auf Servern in verschiedenen Domänen mit in der Instanz gespeicherten Anmeldeinformationen zu authentifizieren.

Wenn Sie die MID Servers nicht für die Verwendung von PowerShell und PowerShell Remoting konfigurieren, verwenden die MID Servers WMI.

Wie PowerShell Discovery funktioniert

Die folgenden Beschreibungen erläutern, wie MID Server PowerShell zum Bereitstellen von Probes verwenden.

Probe und Sensor

Wenn eine Windows-Maschine mit PowerShell klassifiziert und eine MSSQL-Instanz erkannt wird, wird eine Probe namens *`Windows - MSSQL`* gestartet. Die Probe gibt die SQL-Datenbankkataloge und -version an einen passenden Sensor zurück.

Probe Parameter

Der Probe-Parameter *`WMI_ActiveConnections.ps1`* enthält ein Skript, das `netstat.exe` auf einem Zielserver ausführt, wenn PowerShell aktiviert ist. Dieses Skript extrahiert die Informationen zu Windows-Serververbindungen, z. B. Prozess-IDs, Ports und IP-Adressen.

Berechtigungen

Discovery verwendet PowerShell-Anmeldeinformationen von Windows aus der Tabelle „Anmeldeinformationen“ [discovery_credentials] oder die Anmeldeinformationen des Domänenadministrators des MID-Server-Services. Wenn Discovery in der Tabelle „Anmeldeinformationen“ keine PowerShell-Anmeldeinformationen vom Typ (Windows) finden kann, werden die Anmeldeinformationen des Service MID-Server verwendet.

MID-Server-Skripteinbindungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Skripteinbindungen wurden für PowerShell-Erkennungen hinzugefügt. Diese Skripts werden auf dem MID Server ausgeführt, um die Skripte zu generieren, die Discovery für WMIRunner und PowerShell verwendet.

- GenerateWMIScriptJS: Generiert ein Javascript-Skript für die Probe „WMIRunner“.
- GenerateWMIScriptPS1: Generiert ein PowerShell-Skript für die PowerShell-Erkennung.

MID Server-Parameter für PowerShell

Optionale Parameter für den MID Server finden Sie unter MID Server-Parameter für PowerShell. Nachdem Sie die Einstellung für einen Parameter geändert haben, müssen Sie den MID-Server-Service neu starten.

PowerShell-Versionsanforderungen

MID Server, die PowerShell verwenden, müssen auf einem unterstützten Windows-Betriebssystem installiert sein. ServiceNow unterstützt die folgenden PowerShell-Versionen.

Version 3.0

- Regelmäßig Discovery
- Application Dependency Mapping (ADM)
- Dateibasierte Discovery
- PowerShell 3.0 unterstützt Windows Server 2003 nicht.

Version 4.0

- Regelmäßig Discovery
- Application Dependency Mapping (ADM)
- Dateibasierte Discovery

Version 5.0

- Regelmäßig Discovery
- Application Dependency Mapping (ADM)
- Dateibasierte Discovery

Hinweis: PowerShell-Version 6.0 wird **nicht** unterstützt. Viele der cmdlets, von denen die Erkennung abhängig ist, wurden aus dieser Version entfernt. Beispielsweise sind nur cmdlets mit WinRM für Remotevorgänge verfügbar.

Windows PowerShell-Ausführungsrichtlinien

Windows PowerShell hat vier verschiedene Ausführungsrichtlinien. Kunden können die Richtlinien für die Skriptausführung mit ihren Gruppenrichtlinieneinstellungen festlegen. Weitere Informationen finden Sie auf der Microsoft-Website für die PowerShell - Dokumentation.

- Restricted: Es können keine Skripte ausgeführt werden. Windows PowerShell kann nur im interaktiven Modus verwendet werden.
- AllSigned: Nur Skripte, die von einem vertrauenswürdigen Herausgeber signiert wurden, können ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- RemoteSigned: Heruntergeladene Skripte müssen von einem vertrauenswürdigen Herausgeber signiert werden, bevor sie ausgeführt werden können.
- Unrestricted: Keine Einschränkungen, alle Skripte können ausgeführt werden.

Hinweis: Wenn Sie eine andere Richtlinie als „Unrestricted“ haben, muss das Skript signiert werden.

MID Server zur Verwendung von PowerShell einrichten

Konfigurieren Sie MID-Server in Ihrer Organisation für die Verwendung von PowerShell für die Horizontal- und die Top Down-Discovery von Windows -Servern.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: Dies ist standardmäßig aktiviert.

PowerShell Version 2.0 wird nicht unterstützt. Daher wird ein Upgrade auf eine höhere Version empfohlen. Wenn der MID-Server erkennt, dass er über Version 2.0 verfügt, funktioniert er möglicherweise nur teilweise. Der MID-Server erstellt einen Datensatz in der Problemtabelle mid_server mit einer Meldung, die besagt, dass PowerShell Version 2 veraltet ist. Ein Upgrade von PowerShell auf Version 5 wird empfohlen.

Prozedur

1. Laden Sie PowerShell herunter, und installieren Sie es auf allen MID-Server, die für die Erkennung Windows von -Computern konfiguriert sind.
   Wenn auf dem Host eine kompatible PowerShell verfügbar ist, müssen Sie nichts weiter tun.
2. Legen Sie fest, welche Anmeldeinformationen MID-Server für PowerShell verwenden.
   - Um Windows-Computer mit Anmeldeinformationen aus der Anmeldeinformationstabelle zu erkennen, legen Sie den Parameter *mid.powershell.use_credentials* auf **true** fest. Die Verwendung von Anmeldeinformationen aus der Anmeldeinformationstabelle ist das Standardverhalten, wenn PowerShell aktiviert ist.
   - Um zu erzwingen, dass Discovery und Service-Mapping die Anmeldeinformationen des MID-Server-Servicebenutzers verwenden, legen Sie den Parameter *mid.powershell.use_credentials* für den MID Server auf **false** fest. Der MID-Server-Service benötigt Anmeldeinformationen des Domänenadministrators, um Zugriff auf die Windows-Computer in der Domäne zu erhalten.
3. Wahlweise: Konfigurieren Sie bei Bedarf erweiterte Parameter für PowerShell und PowerShell-Remoting für jeden MID-Server separat.
   Obwohl Sie PowerShell deaktivieren können, indem Sie *mid.use_powershell* und *mid.sa.prefer_powershell*ändern, ist diese Methode veraltet und sollte nicht verwendet werden.

PowerShell-Remoting für Discovery

Probe-Entwickler können das PowerShell-Framework zur Remoteausführung verwenden, um die Remoteausführung von Skripts auf Zielgeräten automatisch zu verarbeiten. Das einheitliche Framework beseitigt Inkonsistenzen bei der Remoteausführung, erhöht die Effizienz und verbessert die Stabilität.

Anforderungen

Zur Verwendung des PowerShell-Framework für die Remoteausführung müssen die folgenden Anforderungen erfüllt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der MID Server muss in der Lage sein, auf die Netzwerkfreigabe des Ziels zu schreiben und von dieser zu lesen.
- Das Remoteziel muss über PowerShell 3 oder höher (bis 5.1) verfügen.
- Für MID Server, die WinRM oder WMI verwenden und das Skript auf das Remoteziel kopieren sollen, müssen die Bereiche MachinePolicy und UserPolicy auf „Nicht definiert“ festgelegt sein. Wenn das Skript nicht kopiert wird, kann die Ausführungsrichtlinie eine beliebige andere, einschließlich „Beschränkt“, sein.

Weitere Informationen finden Sie unter MID Server zur Verwendung von PowerShell einrichten.

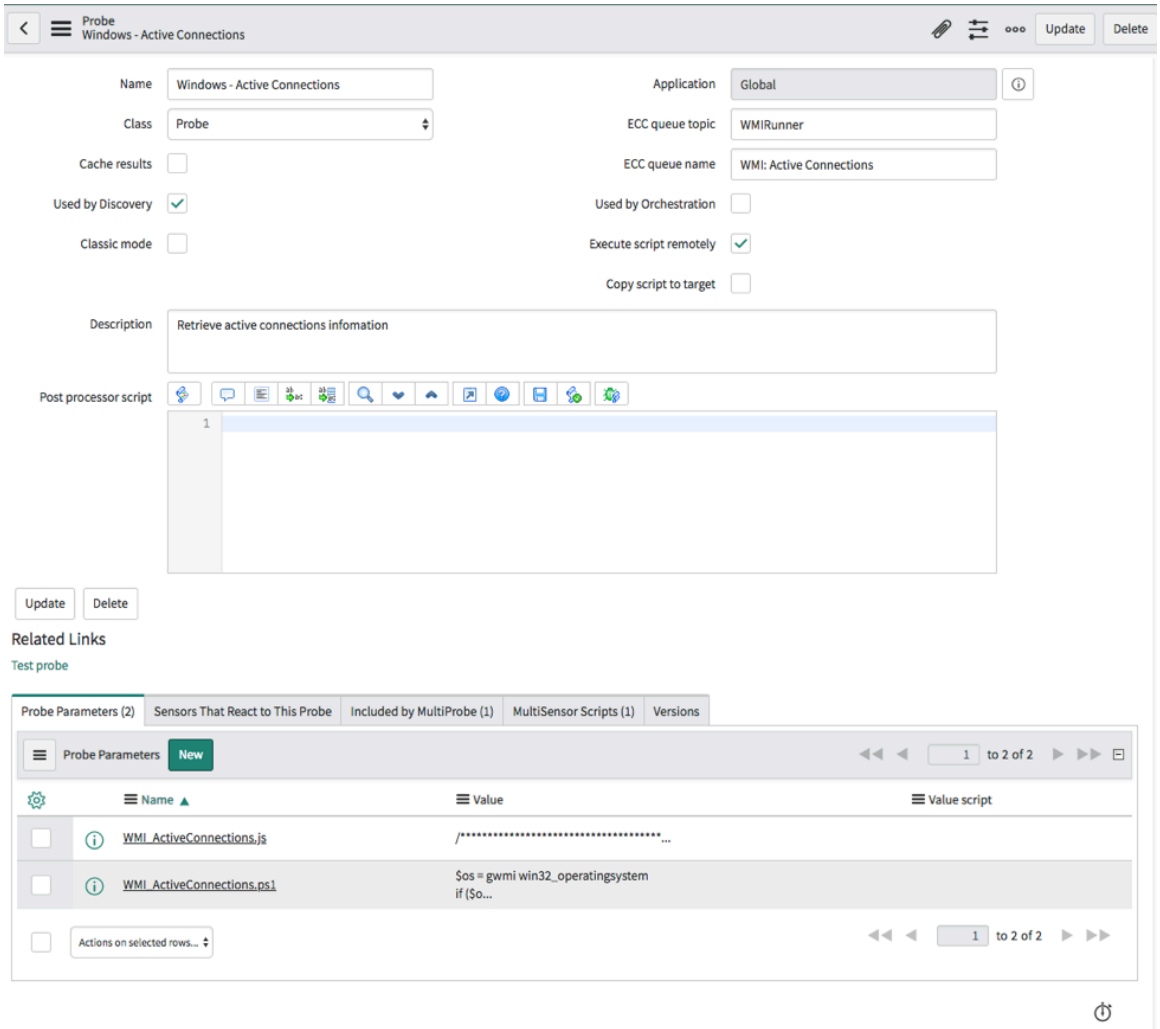
Anwendungserkennung

Das PowerShell-Framework zur Remoteausführung bietet Optionen zum Kopieren von Dateien auf das Remoteziel, wenn ein Scan ausgeführt wird. Das Kopieren von Dateien auf das Ziel ist für Probes wie „Windows - File discovery“ wichtig, da das Skript sich selbst auf dem Remoteziel aufruft, um einen neuen Prozess zu starten. Auf MID Servern, die WMI zur Remoteausführung von Skripts verwenden, kann ein launchProcess-Fehler auftreten, wenn das Skript zu lang ist. Durch das Kopieren des Skripts auf das Remoteziel wird dieser Fehler behoben. Das Kopieren eines Skripts auf ein Remoteziel kann dazu führen, dass das Skript auf dem Ziel von Virenschutzsoftware markiert wird. Um Probleme mit Virenschutzsoftware zu vermeiden, fügen Sie die Skripts der Liste der zulässigen Elemente der Virenschutzanwendung hinzu.

Probe-Konfiguration

Im Folgenden finden Sie die Konfigurationsseite der Probe „Windows - Active Connections“, der in der Multi-Probe „Windows - ADM“ enthalten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Kontrollkästchen **Skript remote ausführen** wird angezeigt, wenn das ECC-Warteschlangenthema WMIRunner oder PowerShell lautet. Wenn das Kontrollkästchen aktiviert ist, werden Skripts auf dem Remoteziel ausgeführt. Andernfalls werden Skripts auf dem MID Server ausgeführt.

Das Kontrollkästchen **Skript in Ziel kopieren** wird angezeigt, wenn **Skript remote ausführen** aktiviert ist. Wenn **Skript in Ziel kopieren** aktiviert ist, wird das Skript auf das Ziel kopiert und dort ausgeführt. Wenn **Skript in Ziel kopieren** deaktiviert ist, wird das Skript auf dem Ziel ausgeführt, ohne es zu kopieren.

Entwicklung von PowerShell-Probes

Das PowerShell-Framework zur Remoteausführung stellt eine einheitliche Methode zum Ausführen von in einem Probe-Parameter enthaltenen PowerShell-Skripts auf einem Remotezielserver dar. Das Framework beseitigt die Notwendigkeit, dass Probe-Entwickler für die Remoteausführung eigenen Code verfassen müssen, wodurch Inkonsistenzen zwischen Entwicklern auftreten könnten. Das Framework verarbeitet die Remoteausführung von Skripts automatisch, weswegen Probe-Entwickler Skripts so schreiben, als ob die Probe Informationen lokal erfassen würde.

Das Framework verarbeitet die Remoteausführung unabhängig davon, ob der MID Server für WMI oder WinRM konfiguriert ist. Wenn der MID Server für WMI konfiguriert ist, führt die Probe mithilfe von launchProcess Befehle auf dem Remoteziel aus. Die Verwendung von launchProcess erschwert die Remoteausführung und kann zu Fehlern führen. Ein für WinRM

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

konfigurierter MID Server verwendet jedoch nicht launchProcess und ist daher effizienter und stabiler.

Von Discovery ausgeführte PowerShell-Befehle

Diese Seite enthält die PowerShell-Cmdlets und ihre Parameter, die Discovery zur Steuerung und Automatisierung der Verwaltung von Windows-Servern und -Anwendungen ausführt. Enthalten sind die Probe-Parameter und MID Server-Skripts, die die Befehle enthalten.

Cmdlet/Parameter	Beschreibung
Add-Content • Pfad • Codierung • Wert	Hängt Inhalte an ein angegebenes Element oder eine angegebene Datei an. Sie können den Inhalt angeben, indem Sie ihn in den Befehl eingeben oder indem Sie ein Objekt angeben, das den Inhalt enthält. Probe Windows - File discovery (filebaseddiscovery.ps1) MID Server-Skript CollectConnectionsAndProcessesInfo.ps1
Add-Member • NotePropertyName • NotePropertyValue • MemberType • Name • Wert	Ermöglicht das Hinzufügen von Eigenschaften und Methoden zu einer Instanz eines Windows PowerShell-Objekts. Beispielsweise können Sie ein NoteProperty-Mitglied hinzufügen, das eine Beschreibung des Objekts enthält, oder ein ScriptMethod-Mitglied, das ein Skript zum Ändern des Objekts ausführt. Probe Windows - File discovery (filebaseddiscovery.ps1) MID Server-Skript CollectConnectionsAndProcessesInfo.ps1
Add-Type • TypeDefinition • AssemblyName • MemberDefinition • Name • Namespace • PassThru	Fügt in Ihrer Windows PowerShell-Sitzung eine Microsoft .NET Framework-Klasse hinzu. Sie können dann das Cmdlet „New-Object“ verwenden, um Objekte zu instanziieren und diese Objekte wie jedes andere .NET Framework-Objekt zu verwenden. Wenn Sie Ihrem Windows PowerShell-Profil den Befehl Add-Type hinzufügen, ist die Klasse in allen Windows PowerShell-Sitzungen verfügbar. Probes • Windows - MSSQL (sqlinfo.ps1) • Windows - Azure (is.azure.ps1) MID Server-Skript • Credentials.psm1 • RegistryAPI.psm1 • LaunchProc.psm1
Compare-Object • Eigenschaft • PassThru	Vergleicht zwei Objektsätze. Ein Objektsatz ist der Referenzsatz, der andere Satz ist der Differenzsatz. Das Ergebnis des Vergleichs gibt an, ob ein Eigenschaftswert nur im Objekt aus dem Referenzsatz oder, wenn der Parameter IncludeEqual angegeben ist, in beiden Objekten vorkommt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	MID Server-Skript DiagnosticsUtil.psm1
ConvertTo-SecureString • Zeichenfolge • AsPlainText • Erzwingen	Konvertiert verschlüsselte Standardzeichenfolgen in sichere Zeichenfolgen. Es kann auch Nur-Text in sichere Zeichenfolgen konvertieren. Es wird mit ConvertFrom-SecureString und Read-Host verwendet. Die von dem Cmdlet erstellte sichere Zeichenfolge kann mit Cmdlets oder Funktionen verwendet werden, die einen Parameter vom Typ SecureString erfordern. Probes Windows - Storage 2012 - PS (storage.2012.ps1) MID Server-Skript Credentials.psm1
ConvertTo-Json	Konvertiert ein beliebiges Objekt in eine Zeichenfolge im JSON-Format (JavaScript Object Notation). Eigenschaften werden in Feldnamen sowie Feldwerte in Eigenschaftswerte konvertiert, und Methoden werden entfernt. MID Server-Skript CollectConnectionsAndProcessesInfo.ps1
Copy-Item • Pfad • Ziel • Erzwingen • Recurse • PassThru	Kopiert ein Element von einem Speicherort an einen anderen Speicherort im selben Namespace. Beispielsweise kann eine Datei in einen Ordner kopiert werden, jedoch nicht auf ein Zertifikatlaufwerk. MID Server-Skript • ADMELauncherWMI.psm1 • ExecuteRemote.psm1 • LaunchProc.psm1 • NmapInstallation.ps1
ForEach-Objekt: Prozess	Führt einen Vorgang für jedes Element in einer Sammlung von Eingabeobjekten durch. Die Eingabeobjekte können an das Cmdlet weitergeleitet oder mithilfe des InputObject-Parameters angegeben werden. Probes • Windows - JBoss Find web.xml List (indwebxml.ps1) • Windows - MSSQL (sqlinfo.ps1) MID Server-Skript • CollectConnectionsAndProcessesInfo.ps1 • DiagnosticsUtil.psm1 • PSScript.ps1
Format-List	Formatiert die Ausgabe eines Befehls als Liste von Eigenschaften, in denen jede Eigenschaft in einer separaten Zeile angezeigt wird. Mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	Format-List können Sie alle oder ausgewählte Eigenschaften eines Objekts als Liste formatieren und anzeigen. MID Server-Skript RegistryAPI.psm1
Get-ChildItem • Pfad • Datei • Recurse • Filter • Verzeichnis • Einbeziehen	Ruft die Elemente an einem oder mehreren angegebenen Speicherorten ab. Wenn das Element ein Container ist, werden die Elemente innerhalb des Containers, sogenannte untergeordnete Elemente, abgerufen. Mit dem Parameter Recurse können Sie Elemente in allen untergeordneten Containern abrufen. MID Server-Skript • CollectConnectionsAndProcessesInfo.ps1 • DiagnosticsUtil.psm1 • ExecuteRemote.psm1 • LaunchProc.psm1 • NmapInstallation.ps1 • PSScript.ps1 • RegistryAPI.psm1
Get-Content • Roh • Pfad	Ruft den Inhalt von Elementen am durch den Pfad angegebenen Speicherort ab, zum Beispiel den Text in einer Datei. Dabei wird der Inhalt Zeile für Zeile gelesen, und es wird eine Sammlung von Objekten zurückgegeben, von denen jedes eine Inhaltszeile repräsentiert. Probes Windows - ADM Enhanced MID Server-Skript • ADMELauncherWMI.psm1 • ADMELauncherWinRM.psm1 • ScriptAPI.psm1
Get-Date: Uformat	Ruft ein DateTime-Objekt ab, das das aktuelle Datum oder ein von Ihnen angegebenes Datum darstellt. Datum und Uhrzeit können in verschiedenen Windows- und UNIX-Formaten formatiert werden. Mit Get-Date können Sie eine Datums- oder Uhrzeitzeichenfolge generieren und diese Zeichenfolge dann an andere Cmdlets oder Programme senden. Probes Windows - File Discovery (filebaseddiscovery.ps1) MID Server-Skript • DiagnosticsUtil.psm1 • LaunchProc.psm1
Get-Item	Ruft das Element am angegebenen Speicherort ab. Der Inhalt des Elements wird nicht am Speicherort abgerufen, es sei denn, Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	verwenden ein Platzhalterzeichen (*), um den gesamten Inhalt des Elements anzufordern. Probes Windows - ADM Enhanced MID Server-Skript • ExecuteRemote.psm1 • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1
Get-ItemProperty • Pfad • Name • ErrorAction	Ruft die Eigenschaften der angegebenen Elemente ab. Beispielsweise können Sie mit diesem Cmdlet den Wert der Eigenschaft LastAccessTime eines Dateiobjekts abrufen. Sie können dieses Cmdlet auch zum Anzeigen von Registrierungseinträgen und deren Werten verwenden. MID Server-Skript • RegistryAPI.psm1 • ScriptAPI.psm1 • NmapInstallation.psm1
Get-Member: MemberType	Ruft die Mitglieder, Eigenschaften und Methoden von Objekten ab. Verwenden Sie zum Festlegen des Objekts den Parameter InputObject, oder leiten Sie ein Objekt an Get-Member weiter. Verwenden Sie zum Abrufen von Informationen über statische Mitglieder (die Mitglieder der Klasse, nicht der Instanz) den Parameter Static. Wenn Sie nur bestimmte Typen von Mitgliedern abrufen möchten, zum Beispiel NoteProperties, verwenden Sie den Parameter MemberType. Probes Windows - ADM Enhanced MID Server-Skript CollectConnectionsAndProcessesInfo.ps1
Get-Process • ID • ErrorVariable (alias EV) • PSProvider	Ruft die Prozesse auf einem lokalen Computer oder Remotecomputer ab. Ohne Parameter ruft dieses Cmdlet alle Prozesse auf dem lokalen Computer ab. Sie können einen bestimmten Prozess auch anhand des Prozessnamens oder der Prozess-ID (PID) angeben oder ein Prozessobjekt über die Pipeline an dieses Cmdlet übergeben. Probes Windows - File Discovery (filebaseddiscovery.ps1) MID Server-Skript • CollectConnectionsAndProcessesInfo.ps1 • Get-PEB.psm1
Get-PSDrive	Ruft die Laufwerke in der aktuellen Sitzung ab. Sie können ein bestimmtes Laufwerk oder alle Laufwerke in der Sitzung abrufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
• Name • ErrorAction • PSProvider	Probes Windows - ADM Enhanced MID Server-Skript • ADMELauncherWMI.psm1 • Credentials.psm1
Get-PSSession	Ruft die von Benutzern verwalteten Windows PowerShell-Sitzungen (PSSessions) auf lokalen und Remotecomputern ab MID Server-Skript Credentials.psm1
Get-Variable: Name	Ruft die Windows PowerShell-Variablen in der aktuellen Konsole ab. Sie können nur die Werte der Variablen abrufen, indem Sie den Parameter ValueOnly angeben, und Sie können die zurückgegebenen Variablen nach Namen filtern. MID Server-Skript • ExecuteRemote.psm1 • PSScript.ps1 • DiagnosticsUtil.psm1
Get-WmiObject • ComputerName • Filter • Anmeldeinformationen • Identitätswechsel • Authentifizierung • ErrorAction (alias EA) • Liste • Namespace • Klasse	Ruft Instanzen von WMI-Klassen (Windows Management Instrumentation) oder Informationen über die verfügbaren WMI-Klassen ab. Um einen Remotecomputer anzugeben, verwenden Sie den Parameter ComputerName. Wenn der Parameter List angegeben ist, ruft das Cmdlet Informationen über die in einem angegebenen Namespace verfügbaren WMI-Klassen ab. Wenn der Parameter Query angegeben ist, führt das Cmdlet eine WQL-Anweisung (WMI Query Language) aus. Probes • Windows - MSSQL (sqlinfo.ps1) • Windows - Storage 2008 - PS (storage.ps1) MID Server-Skript • ExecuteRemote.psm1 • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1
Get-WSManInstance: ResourceURI	Ruft eine Instanz einer Verwaltungsressource ab, die durch einen Ressourcen-URI (Uniform Resource Identifier) angegeben ist. Die abgerufenen Informationen können ein komplexer XML-Informationssatz (ein Objekt) oder ein einfacher Wert sein. MID Server-Skript ScriptAPI.psm1
Gruppenobjekt: NoElement	Zeigt Objekte in Gruppen basierend auf dem Wert einer angegebenen Eigenschaft an. Group-Object gibt eine Tabelle mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	einer Zeile für jeden Eigenschaftswert und einer Spalte zurück, in der die Anzahl der Elemente mit diesem Wert angezeigt wird. MID Server-Skript RegistryAPI.psm1
Import-Module • Name • DisableNameChecking • Global	Fügt der aktuellen Sitzung mindestens ein Modul hinzu. Die von Ihnen importierten Module müssen auf dem lokalen Computer oder einem Remotecomputer installiert sein. Probes Windows - Storage 2012 - PS (storage.2012.ps1) MID Server-Skript • Credentials.psm1 • PSScript.ps1
Invoke-Command • Sitzung • ScriptBlock • ErrorAction • ErrorVariable • ArgumentList (Alias ist „args“) • FilePath	Führt Befehle auf einem lokalen Computer oder Remotecomputer aus und gibt die gesamte Ausgabe der Befehle zurück, einschließlich Fehler. Mit einem einzigen Befehl Invoke-Command können Sie Befehle auf mehreren Computern ausführen. Probes Windows - Storage 2012 - PS (storage.2012.ps1) MID Server-Skript • ADMELauncherWinRM.psm1 • Credentials.psm1 • ExecuteRemote.psm1 • LaunchProc.psm1 • Get-PEB.psm1 • WMIFetch.psm1
Invoke-Expression	Wertet oder führt eine angegebene Zeichenfolge als Befehl aus und gibt die Ergebnisse des Ausdrucks oder Befehls zurück. Ohne Invoke-Expression würde eine an die Befehlszeile übermittelte Zeichenfolge unverändert zurückgegeben (als Echo-Zeichenfolge wiederholt). MID Server-Skript • NmapInstallation.ps1 • ScriptAPI.psm1
Invoke-WmiMethod • Name • ComputerName • Argumentlist • Anmeldeinformationen • ErrorAction	Ruft die Methoden von WMI-Objekten (Windows Management Instrumentation) auf MID Server-Skript • LaunchProc.psm1 • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
Messobjekt: Summe	Berechnet die Eigenschaftswerte bestimmter Objekttypen. Measure-Object führt abhängig von den Parametern im Befehl drei Arten von Messungen durch. MID Server-Skript CollectConnectionsAndProcessesInfo.ps1
New-Item • ItemType • Pfad • Erzwingen • ErrorAction	Erstellt ein neues Element und legt dessen Wert fest. Welche Elementtypen erstellt werden können, hängt vom Speicherort des Elements ab. Beispielsweise erstellt New-Item im Dateisystem Dateien und Ordner. In der Registrierung erstellt New-Item hingegen Registrierungsschlüssel und -einträge. MID Server-Skript • CollectConnectionsAndProcessesInfo.ps1 • ExecuteRemote.psm1 • LaunchProc.psm1 • NmapInstallation.ps1 • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1
New-Object • TypeName • Eigenschaft • ArgumentList	Erstellt eine Instanz eines Microsoft .NET Framework- oder COM-Objekts Probes • Windows - AWS Relationship (AWS_InstanceID.ps1) • Windows - Azure (is.azure.ps1) • Windows - MSSQL (sqlinfo.ps1) • Windows - File Discovery (filebaseddiscovery.ps1) • Windows - Storage 2012 - PS (storage.2012.ps1) MID Server-Skript • ADMELauncherWMI.psm1 • CollectConnectionsAndProcessesInfo.ps1 • Credentials.psm1 • Get-PEB.psm1 • LaunchProc.psm1 • WMIFetch.psm1 XMLUtil.psm1 • ExecuteRemote.psm1
New-PSDrive • PSProvider • Stamm • ErrorAction • Anmeldeinformationen	Erstellt temporäre und persistente Laufwerke, die einem Speicherort in einem Datenspeicher wie einem Netzlaufwerk, einem Verzeichnis auf einem lokalen Computer oder einem Registrierungsschlüssel zugeordnet sind, sowie persistente, in Windows zugeordnete Netzlaufwerke, die einem Speicherort im Dateisystem auf einem Remotecomputer zugeordnet sind. MID Server-Skript

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
• Name • Bereich	• ADMELauncherWMI.psm1 • ScriptAPI.psm1
New-Variable • Namer • Wert • Erzwingen	Erstellt eine neue Variable in Windows PowerShell. Sie können der Variablen während der Erstellung einen Wert zuweisen oder den Wert nach der Erstellung zuweisen oder ändern. MID Server-Skript PSScript.ps1
New-PSSession • Anmeldeinformationen • SessionOption	Erstellt eine Windows PowerShell-Sitzung (PSSession) auf einem lokalen Computer oder Remotecomputer. Beim Erstellen einer PSSession stellt Windows PowerShell eine dauerhafte Verbindung zu einem Remotecomputer her. MID Server-Skript PSRemoteSession.psm1
New-PSSessionOption	Erstellt ein Objekt, das erweiterte Optionen für eine von Benutzern verwaltete Sitzung enthält. Sie können das Objekt als Wert des Parameters SessionOption von Cmdlets verwenden, die eine PSSession erstellen, zum Beispiel New-PSSession, Enter-PSSession und Invoke-Command. MID Server-Skript PSRemoteSession.psm1
New-Timespan • Start • Ende	Erstellt ein Zeitspannenobjekt, das ein Intervall darstellt. Sie können diesen Befehl für die Addition oder Subtraktion von Zeit bei einem DateTime-Objekt verwenden. Probes Windows - File Discovery (filebaseddiscovery.ps1)
Ausgehende Datei: Dateipfad	Sendet die Ausgabe an eine Datei. Sie können diesen Operator anstelle von > verwenden, wenn Sie die zugehörigen Parameter verwenden müssen. Probes Windows - File Discovery (filebaseddiscovery.ps1)
Out-Null	Sendet die Ausgabe an NULL, wodurch sie effektiv gelöscht wird MID Server-Skript Get-PEB.psm1
Out-String	Konvertiert die von Windows PowerShell verwalteten Objekte in ein Array von Zeichenfolgen. Standardmäßig akkumuliert Out-String die Zeichenfolgen und gibt sie als einzelne Zeichenfolge zurück. Sie können den Parameter stream jedoch auch dazu verwenden, Out-String anzuweisen, jeweils eine Zeichenfolge zurückzugeben. Mit diesem Cmdlet können Sie die Zeichenfolgenausgabe durchsuchen und sie wie in herkömmlichen Shells bearbeiten, wenn die Objektbearbeitung weniger praktisch ist. MID Server-Skript Get-PEB.psm1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
Receive-Job	Ruft die Ergebnisse von Windows PowerShell-Hintergrundaufträgen ab, zum Beispiel solchen, die mit dem Cmdlet Start-Job oder dem Parameter AsJob eines beliebigen Cmdlet gestartet wurden. Sie können die Ergebnisse aller Aufträge abrufen oder Aufträge anhand von Name, ID, Instanz-ID, Computername, Speicherort bzw. Sitzung oder durch Übermittlung eines Auftragsobjekts identifizieren. MID Server-Skript LaunchProc.psm1
Remove-Item • Recurse • Pfad • Erzwingen	Löscht mindestens ein Element. Da es von vielen Anbietern unterstützt wird, kann es viele verschiedene Elementtypen löschen, einschließlich Dateien, Ordner, Registrierungsschlüssel, Variablen, Aliase und Funktionen. MID Server-Skript • ExecuteRemote.psm1 • NmapInstallation.ps1 • LaunchProc.psm1 • CollectConnectionsAndProcessesInfo.ps1
Remove-Job	Löscht Windows PowerShell-Hintergrundaufträge. Sie können Aufträge starten, indem Sie Start-Job oder den Parameter AsJob eines beliebigen Cmdlet verwenden. Sie können dieses Cmdlet zum Löschen aller Aufträge oder zum Löschen von Aufträgen basierend auf Name, ID, Instanz-ID, Befehl oder Status bzw. durch Übergabe eines Auftragsobjekts an Remove-Job verwenden. Ohne Parameter oder Parameterwerte hat Remove-Job keine Auswirkungen. MID Server-Skript LaunchProc.psm1
Remove-PSDrive: Name	Löscht temporäre Windows PowerShell-Laufwerke, die mit dem Cmdlet New-PSDrive erstellt wurden MID Server-Skript • ADMELauncherWMI.psm1 • ScriptAPI.psm1
Remove-PSSession: Sitzung	Schließt Windows PowerShell-Sitzungen (PSSessions) in der aktuellen Sitzung. Das Cmdlet beendet alle Befehle, die in PSSessions ausgeführt werden, beendet die PSSession und gibt die Ressourcen frei, die von der PSSession verwendet wurden. Wenn die PSSession mit einem Remotecomputer verbunden ist, schließt dieses Cmdlet auch die Verbindung zwischen dem lokalen Computer und dem Remotecomputer. Probes Windows - Storage 2012 - PS (storage.2012.ps1) MID Server-Skript Credentials.psm1
Remove-Variable	Löscht eine Variable und ihren Wert aus dem Bereich, in dem sie definiert ist, zum Beispiel in der aktuellen Sitzung. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
• Name • Wert	dieses Cmdlet nicht verwenden, um Variablen zu löschen, die als Konstanten festgelegt oder systemspezifisch sind. MID Server-Skript PSScript.ps1
Rename-Item • Pfad • NewName	Ändert den Namen eines angegebenen Elements. Dieses Cmdlet wirkt sich nicht auf den Inhalt des Elements aus, das umbenannt wird. Sie können Rename-Item nicht zum Verschieben eines Elements verwenden, beispielsweise durch Angabe eines Pfads zusammen mit dem neuen Namen. Um ein Element zu verschieben und umzubenennen, verwenden Sie das Cmdlet Move-Item. Probes Windows - File Discovery (filebaseddiscovery.ps1)
Select-Object • ExpandProperty (Alias Expand) • Eigenschaft • ExcludeProperty	Dient zur Auswahl bestimmter Eigenschaften eines Objekts oder Objektsatzes. Mit dem Cmdlet lassen sich außerdem spezifische Objekte, eine bestimmte Anzahl von Objekten oder Objekte an einer bestimmten Position in einem Array auswählen. Alias ist „Select“. Probes Windows - MSSQL (sqlinfo.ps1) MID Server-Skript • CollectConnectionsAndProcessesInfo.ps1 • RegistryAPI.psm1
Select-String • Muster • NotMatch	Sucht nach Text und Textmustern in Eingabezeichenfolgen und Dateien. Sie können es wie Grep in UNIX und Findstr in Windows verwenden. Sie können Select-String oder den entsprechenden Alias sls eingeben. MID Server-Skript CollectConnectionsAndProcessesInfo.ps1
Select-XML • Xpath • Inhalt • Namespace	Ermöglicht die Verwendung von XPath-Abfragen zur Suche nach Text in XML-Zeichenfolgen und -Dokumenten. Geben Sie eine XPath-Abfrage ein, und verwenden Sie den Parameter Content, Path oder Xml, um die zu durchsuchende XML-Datei anzugeben. MID Server-Skript ScriptAPI.psm1
Set-Content • Pfad • Wert • Erzwingen • Codierung	Schreibt oder ersetzt den Inhalt im angegebenen Element, zum Beispiel einer Datei. Sie können den Inhalt in den Befehl eingeben oder Inhalt über die Pipeline an Set-Content senden. MID Server-Skript • ADMELauncherWinRM.psm1 • CollectConnectionsAndProcessesInfo.ps1 • ExecuteRemote.psm1
Standort festlegen: Pfad	Legt den Arbeitsort auf einen angegebenen Speicherort fest: ein Verzeichnis, Unterverzeichnis, Registrierungsspeicherort oder beliebiger Anbieterpfad.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	MID Server-Skript Credentials.psm1
Set-StrictMode: Version	Konfiguriert den strikten Modus für den aktuellen Umfang und alle untergeordneten Bereiche und aktiviert bzw. deaktiviert ihn. Im strikten Modus generiert Windows PowerShell einen Abschlussfehler, wenn der Inhalt eines Ausdrucks, Skripts oder Skriptblocks gegen grundlegende bewährte Codierungsregeln verstößt. MID Server-Skript Get-PEB.psm1
Set-Variable • Name • Wert • Option • Bereich	Weist einer angegebenen Variablen einen Wert zu oder ändert den aktuellen Wert. Wenn die Variable nicht vorhanden ist, wird sie durch das Cmdlet erstellt. MID Server-Skript • PSScript.ps1 • CollectConnectionsAndProcessesInfo.ps1 • ExecuteRemote.psm1
Sortierobjekt: Eigenschaft	Sortiert Objekte in aufsteigender oder absteigender Reihenfolge basierend auf den Werten der Eigenschaften des Objekts. Sie können eine einzelne Eigenschaft oder mehrere Eigenschaften (für eine Sortierung mit mehreren Schlüsseln) angeben und eine Sortierung auswählen, bei der die Groß-/Kleinschreibung berücksichtigt bzw. nicht berücksichtigt wird. Sie können Sort-Object auch anweisen, nur die Objekte mit einem eindeutigen Wert für eine bestimmte Eigenschaft anzuzeigen. Probes Windows - MSSQL (sqlinfo.ps1) MID Server-Skript DiagnosticsUtil.psm1
Split-Path • Blatt • Pfad • Übergeordnet	Gibt nur den angegebenen Teil eines Pfads zurück, zum Beispiel den übergeordneten Ordner, einen Unterordner oder einen Dateinamen. Das Cmdlet kann auch Elemente abrufen, auf die der geteilte Pfad verweist, und feststellen, ob der Pfad relativ oder absolut ist. Probes • Windows - Weblogic - Find (findconfig.ps1) • Windows - Storage 2012 - PS (storage.2012.ps1) MID Server-Skript • Credentials.psm1 • LaunchProc.psm1 • PSScript.ps1 • ExecuteRemote.psm1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
Start-Sleep • S (Alias für Sekunden) • M (Alias für Millisekunden)	Hält die Aktivität für den angegebenen Zeitraum in einem Skript oder einer Sitzung an. Sie können es verwenden, während Sie auf den Abschluss eines Vorgangs warten oder eine Pause einlegen, bevor Sie den Vorgang wiederholen. Probes Windows - Active Connections Multiple (WMI_ActiveConnections.ps1) MID Server-Skript • CollectConnectionsAndProcessesInfo.ps1 • LaunchProc.psm1 • NmapInstallation.ps1
Stop-Job	Beendet gerade laufende Hintergrundaufträge der Windows PowerShell. Sie können dieses Cmdlet zum Anhalten aller Aufträge oder zum Anhalten bestimmter Aufträge basierend auf Name, ID, Instanz-ID oder Status bzw. durch Übergabe eines Auftragsobjekts an Stop-Job verwenden. MID Server-Skript LaunchProc.psm1
Test-Path • Pfad • PathType	Bestimmt, ob alle Elemente des Pfads vorhanden sind. Gibt $True zurück, wenn alle Elemente vorhanden sind, und $False, wenn nicht alle da sind. Kann auch bestimmen, ob die Pfadsyntax gültig ist und ob der Pfad zu einem Container, einem Terminal oder einem Blattelement führt MID Server-Skript • ExecuteRemote.psm1 • LaunchProc.psm1 • NmapInstallation.ps1 • PSScript.ps1 • RegistryAPI.psm1 • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1 • CollectConnectionsAndProcessesInfo.ps1
Test-WSMan • Computer • Port	Sendet eine Identifizierungsanforderung, die bestimmt, ob der WinRM-Service auf einem lokalen Computer oder Remotecomputer ausgeführt wird. Wenn der Service auf dem getesteten Computer ausgeführt wird, zeigt das Cmdlet das Identitätsschema von WS-Management, die Protokollversion, den Produktanbieter und die Produktversion des getesteten Service an. MID Server-Skript ScriptAPI.psm1
Where-Object	Wählt Objekte mit bestimmten Eigenschaftswerten aus der Sammlung von Objekten aus, die an sie übergeben werden. Beispielsweise sind mit dem Cmdlet Where-Object folgende Auswahlvorgänge möglich: Dateien, die nach einem bestimmten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	Datum erstellt wurden, Ereignisse mit einer bestimmten ID oder Computer mit einer bestimmten Version von Windows. MID Server-Skript • CollectConnectionsAndProcessesInfo.ps1 • DiagnosticsUtil.psm1 • WMIFetch.psm1
Write-Error • Nachricht • Kategorie	Deklariert einen nicht endenden Fehler. Standardmäßig werden Fehler im Fehlerstream zusammen mit der Ausgabe an das anzuzeigende Hostprogramm gesendet. Probes • Windows - MySQL Configuration (mysqlconfig.ps1ps1) • Windows - MySQL Version (mysqlinfo.ps1) • Oracle - Instance Pfile (oraclepfile.ps1) • Oracle - Instance Version (oracleversion.ps1) • Windows - MSSQL (sqlinfo.ps1) MID Server-Skript • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1 • ExecuteRemote.psm1 • LaunchProc.psm1 • NmapInstallation.ps1
Write-Host: NoNewLine	Schreibt benutzerdefinierte Ausgaben an einen Host. Sie können die Farbe des Texts mithilfe des Parameters ForegroundColor und die Hintergrundfarbe mithilfe des Parameters BackgroundColor angeben. Mit dem Parameter Separator können Sie eine Zeichenfolge angeben, die zum Trennen von angezeigten Objekten verwendet wird. Das jeweilige Ergebnis hängt von dem Programm ab, das Windows PowerShell hostet. Probes • Windows - Network ARP Table (arpTable.ps1) • Windows - Weblogic - Find (findconfig.ps1) • Windows - JBoss Get (findjbossservicexml.ps1) • Windows - WebSphere - Web Services () • Windows - JBoss Find (findwebxml.ps1) • Windows - Weblogic - Get () • Windows - WebSphere - Cell (getcellxml.ps1) • Windows - WebSphere - Web Applications (getserverindexxml.ps1) • Oracle - Instance PFile (oraclepfile.ps1) • Oracle - Instance Version (oracleversion.ps1)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cmdlet/Parameter	Beschreibung
	• Windows - MSSQL (sqlinfo.ps1) • Windows - Storage 2012 - PS (storage.2012.ps1) • Windows - Storage 2008 - PS (storage.ps1) • Windows - Active Connections Multiple (WMI_ActiveConnections.ps1) MID Server-Skript • ADMELauncherWinRM.psm1 • ADMELauncherWMI.psm1 • PSScript.ps1 • RegistryAPI.psm1 • ScriptAPI.psm1 • WMIFetch.psm1 • DiagnosticsUtil.psm1 • NmapInstallation.ps1
Write-Output	Sendet die angegebenen Objekte an den nächsten Befehl in der Pipeline. Wenn dies der letzte Befehl in der Pipeline ist, werden die Objekte in der Konsole angezeigt. Probes • Windows - Azure (is.azure.ps1) • ExecuteRemote (testExecuteRemote.ps1) • Windows - File Discovery (filebaseddiscovery.ps1) MID Server-Skript Get-PEB.psm1
Ausführlich schreiben: Nachricht	Schreibt Text in den ausführlichen Nachrichtenstrom in Windows PowerShell. Normalerweise wird der ausführliche Nachrichtenstrom verwendet, um Informationen über die Befehlsverarbeitung bereitzustellen, die für das Debugging eines Befehls verwendet wird. MID Server-Skript • Get-PEB.psm1 • LaunchProc.psm1 • ExecuteRemote.psm1

MID Server-Parameter für PowerShell

Parameter steuern das Verhalten eines bestimmten MID-Servers und haben eine niedrigere Priorität als die MID-Server-Eigenschaften.

Die folgenden Parameter sind optional.

Hinweis: Nachdem Sie die Einstellung für einen Parameter geändert haben, müssen Sie den MID-Server-Service neu starten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
mid.powershell_api.session_pool.max_size	Gibt die maximale Anzahl von Sitzungen an, die im Sitzungspool zulässig sind. **Hinweis:** Das Einstellen oder Ändern dieses Parameters erfordert einen Neustart des MID Servers. • Typ: Ganzzahl • Standardwert: 25
mid.powershell_api.session_pool.target.max_size	Gibt die maximale Anzahl von Sitzungen an, die im Pool pro Zielhost zulässig sind. **Hinweis:** Das Einstellen oder Ändern dieses Parameters erfordert einen Neustart des MID Servers. • Typ: Ganzzahl • Standardwert: 3
mid.powershell_api.winrm.use_ssl	Erfordert die Verwendung von SSL-Zertifikaten für HTTPS-Verbindungen mit WinRM. • Typ: wahr | falsch • Standardwert: false
mid.powershell_api.winrm.additional_pssesion_options	Steuert die erweiterten Optionen für eine PSSession. Weitere Informationen zu erweiterten Optionen für eine PSSession finden Sie unter https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/new-pssessionoption?view=powershell-6 .
mid.powershell_api.winrm.remote_https_port	Konfiguriert den Port für das Verbinden zu Windows-Servern mit PowerShell über HTTPS. • Typ: Ganzzahl • Standardwert: 5986

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
mid.powershell_api.winrm.remote_port	Konfiguriert den Port für das Verbinden zu Windows-Servern mit PowerShell über HTTP. • Typ: Ganzzahl • Standardwert: 5985
mid.powershell_api.winrm.skip_ssl_cert_check	Überspringt die Prüfung für das SSL-Zertifikat, wenn WinRM für HTTPS-Verbindungen verwendet wird. • Typ: wahr | falsch • Standardwert: false
mid.powershell_api.winrm.skip_ssl_cert_check_options	Überspringt spezifische Prüfungen für SSL-Zertifikate, wenn WinRM für HTTPS-Verbindungen verwendet wird. Konfigurieren Sie MID-Server, um Prüfungen für Zertfifikate aus einer Certification Authority (CA) zu überspringen, aus dem Common Name (CN), der den mit dem Zertifikat verknüpften Host festlegt, und für widerrufene Zertifikate. • Typ: Zeichenfolge • Standardwert: -SkipCACheck -SkipCNCheck -SkipRevocationCheck
mid.powershell.use_credentials	Legt die Anmeldeinformationen fest, die Discovery mit PowerShell verwendet werden sollen. Die Einstellung *wahr* lässt MID-Server Proben ausführen mit den Windows Anmeldeinformationen aus der entsprechenden Tabelle. Um Proben mit den Anmeldeinformationen des Benutzers für den Service MID-Server auszuführen, stellen Sie diesen Parameter auf *falsch* ein. • Typ: true | false • Standardwert: true
mid.use_powershell	Aktiviert oder deaktiviert PowerShell für Discovery. Starten Sie MID-Server neu, nachdem Sie den Wert geändert haben. Wenn PowerShell nicht installiert ist oder die installierte Version niedriger

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	als Version 2.0 ist, wird Discovery zur Verwendung von WMIRunner zurückgesetzt. • Typ: true | false • Standardwert: true
mid.powershell.path	Ermöglicht es einem Administrator, auf eine bestimmte PowerShell auf einem MID-Server zu verweisen, wenn mehr als eine PowerShell installiert ist. Geben Sie den Pfad zum Ordner an, das die ausführbare PowerShell-Datei enthält, zum Beispiel `C:\mypowershell` oder `C:\mypowershell \`. ServiceNow hängt automatisch die Zeichenfolge „powershell.exe“ an den Pfad an. Konfigurieren Sie diesen Parameter, wenn sowohl 32-Bit- als auch 64-Bit-PowerShells auf demselben MID-Server aktiv sind und die richtige PowerShell für den Kontext gestartet werden muss. 64-Bit Windows verwendet die Dateisystemumleitung und der MID-Server wird als 32-Bit-Anwendung ausgeführt. Wenn ein Pfad in %WinDir%\System32 festgelegt werden soll, leitet Windows automatisch auf %WinDir %\SysWOW64 um. Geben Sie den Pfad als %WinDir%\Sysnative an, um eine Umleitung zu vermeiden. Legen Sie statt C:\WINDOWS \system32\WindowsPowerShell \v1.0\ zum Beispiel C:\WINDOWS \sysnative\WindowsPowerShell \v1.0\ fest. **Hinweis:** Bei einer 64-Bit-Version von Windows XP kann ein MicrosoftMicrosoft Azure Event Hubs-Hotfix erforderlich sein, um diese Funktion zu aktivieren. Um Anwendungen zu finden, die auf einem 64-Bit-Windows-Computer ausgeführt werden, muss MID-Server auf einem 64-Bit-Windows-Host-Computer ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	• Typ: Zeichenfolge (Pfad) • Standardwert: keiner
mid.powershell.enforce_utf8	Aktivieren Sie diesen Parameter, um Befehle auf einem Windows-Zielsystem zu zwingen, die UTF-8-codierte Ausgabe zurückzugeben. Bei Deaktivierung kann das Zielsystem seine Standardcodierung verwenden. Dieser Parameter ist nur gültig, wenn PowerShell aktiviert ist. Das Festlegen dieses Werts auf „false“ kann zu falschen Werten in der CMDB führen, wenn von einem Probe Nicht-ASCII-Zeichen zurückgegeben werden. • Typ: true | false • Standardwert: wahr
mid.powershell_api.idle_session_timeout	Gibt den Wert für den Timeout von PowerShell-Sitzungen im Leerlauf in Sekunden an. **Hinweis:** Das Einstellen oder Ändern dieses Parameters erfordert einen Neustart des MID-Server. • Typ: Ganzzahl • Standardwert: 60
mid.powershell.command.parameter_passing	Aktivieren Sie diesen Parameter, um die Übergabe von PowerShell-Parametern von der Befehlszeile aus zuzulassen. • Typ: wahr | falsch • Standardwert: false
mid.powershell.command.script.parameter_passing	Aktivieren Sie diesen Parameter, um die Übergabe von PowerShell-Skripts von der Befehlszeile aus zuzulassen. • Typ: wahr | falsch • Standardwert: falsch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
mid.windows.management_protocol	Ermöglicht Administratoren die Auswahl des für die Geräte- und Prozessklassifizierung verwendeten Windows-Verwaltungsprotokolls. Verfügbare Optionen: • WMI • WinRM • Typ: Zeichenfolge • Standardwert: WMI
mid.windows.probe_timeout	Legt das Timeout-Intervall für alle Windows-Probes auf einem bestimmten MID Server fest. Dieser Wert wird von den Werten überschrieben, die für einzelne Probes mit dem Probe-Parameter „wmi_timeout“ konfiguriert wurden. • Typ: Ganzzahl • Standardwert: 600

Application Dependency Mapping (ADM) für Discovery

Application Dependency Mapping (ADM) erkennt CIs durch die Erkennung von TCP-Verbindungen zwischen Geräten.

Wenn die ADM-Erkennung aktiviert ist, führt Discovery während der Erkundungsphase stets die ADM-Probes aus, um den TCP-Datenverkehr in Ihrem Netzwerk zu erkennen. Mithilfe dieser TCP-Verbindungen kann Discovery zusätzliche CIs finden und Beziehungen zwischen ihnen herstellen.

IPv6 wird für ADM unterstützt.

Hinweis: ADM bietet derzeit keine Unterstützung für mehrere Sprachen. Wenn die zurückgegebenen Werte nicht in Englisch vorliegen, können die zurückgegebenen Daten nicht richtig analysiert werden, und die Erkennung schlägt fehl.

Standardmäßige und erweiterte ADM-Erkennung

Standardmäßige ADM-Erkennung

Löst eine ADM-Probe aus, die mithilfe der Befehle `netstat` und `lsof` einen einzelnen Snapshot von TCP-Verbindungen auf Zielcomputern erstellt. Es werden jedoch keine neuen TCP-Verbindungen erkannt, die zwischen diesen 24-Stunden-Intervallen auftreten.

Die standardmäßige ADM-Erkennung ist standardmäßig aktiviert.

Erweiterte ADM-Erkennung (ADME)

Löst eine erweiterte ADM-Probe aus, die ein Skript auf Hostcomputern installiert, auf denen Discovery reguläre Muster basierend auf aktiven TCP-Verbindungen erstellt. Sie können eine Reihe von Eigenschaften und Probe-Parametern verwenden, die mehrere Aspekte der erweiterten ADM-Erkennung steuern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die ADME-Erkennung ist standardmäßig nicht aktiviert.

Service-Mapping verwendet die ADM-Probes für die datenverkehrsbasierende Erkennung. Weitere Informationen finden Sie unter Erkennung auf Basis von Predictive Intelligence.

Anforderungen

Sowohl die standardmäßige als auch die erweiterte ADM-Erkennung unterstützen die folgenden Betriebssysteme:

- Windows
- Unix
- Solaris (Auf Solaris-Computern ist erweitertes ADM in globalen Zonen verfügbar. Für lokale Zonen ist nur Standard-ADM verfügbar.)
- AIX
- HP-UX

Zur Verwendung des WMI-Protokolls ist Version 3.0 von PowerShell erforderlich.

Hinweis:

Wenn Sie die Ausführungsrichtlinie des Windows-Servers auf RemoteSigned oder AllSigned festlegen, kann ADME PowerShell-Skripts ausführen. Sie müssen das ServiceNow-Zertifikat zu den vertrauenswürdigen Herausgebern importieren, damit die Skripts ordnungsgemäß ausgeführt werden.

TCP-Nachverfolgungsdatei für erweitertes ADM

Beim ersten Start der erweiterten Probe durch Discovery werden keine TCP-Informationen erfasst. Stattdessen stellt die erweiterte Probe nur die TCP-Nachverfolgungsdatei bereit, in der Informationen über die erkannten TCP-Verbindungen gespeichert werden. Nach der erneuten Ausführung von Discovery übermittelt die erweiterte Probe den Inhalt der TCP-Nachverfolgungsdatei über den MID Server zurück an die Instanz. Die Informationen werden in der CMDB gespeichert.

Die TCP-Nachverfolgungsdatei wird standardmäßig an folgenden Speicherorten gespeichert:

- Windows: `admin$\temp\{Ihr_Instanzname}`. Während der Überwachung von TCP-Verbindungen werden die Informationen im Arbeitsspeicher abgelegt und später in der Datei gespeichert.
- Linux: `/tmp/{Ihr_Instanzname}`.

Sie können den Speicherort und andere Aspekte der Nachverfolgungsdatei mit ADM-Eigenschaften ändern.

Wenn Sie erweitertes ADM deaktivieren, bereinigt Discovery die Ordner im Hostdateisystem, wenn Discovery das nächste Mal ausgeführt wird. Nur die TCP-Nachverfolgungsdatei verbleibt.

Anforderungen für erweitertes ADM auf Linux-Computern

Ändern Sie die Datei sudoers, sodass die folgenden Befehle einbezogen werden:

Windows

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Unterstützte Dienstprogramme: netstat
- Erforderliche sudoer-Befehle: Keine
- Zusätzliche Anforderungen: Keine

AIX

- Unterstützte Dienstprogramme:
  - netstat
  - lsof (wenn netstat nicht funktioniert)
- Erforderliche sudoer-Befehle:
  - `Cmnd_Alias ADME_CMDS=/usr/bin/netstat -Aan, /usr/sbin/lsof -iTCP -n -P`
  - `discoUser ALL=(root)NOPASSWD:ADME_CMDS`
  - `Defaults:discoUser ! requiretty`
- Zusätzliche Anforderungen: Keine

Solaris

- Unterstützte Dienstprogramme:
  - netstat (für Solaris Version 11.2)
  - lsof (für Solaris-Versionen vor 11.2)
- Erforderliche sudoer-Befehle:
  - `Cmnd_Alias ADME_CMDS = /usr/bin/netstat,/opt/csw/bin/lsof -iTCP -n -P -zglobal`
  - `discoUser ALL=(root) NOPASSWD:ADME_CMDS`
  - `Defaults!ADME_CMDS !requiretty`
  - `Cmnd_Alias ADME_PS = /usr/ucb/ps`
  - `discoUser ALL=(root) NOPASSWD:ADME_PS`
  - `Disco ALL=(root) /usr/bin/pfiles`
  - `Disco ALL=(root) /usr/bin/pgrep`
  - `Defaults!ADME_PS !requiretty`

  Hinweis: Sie müssen **-zglobal** hinzufügen, damit lsof ausgeführt wird.

- Zusätzliche Anforderungen: Fügen Sie den lsof-Pfad dem sicheren Pfad hinzu. Beispiel: Wenn der Pfad zu lsof `/opt/csw/bin` lautet, muss der sichere Pfad `secure_path = /usr/bin:/usr/sbin:/bin:/sbin:/opt/csw/bin` lauten.

  Hinweis: Die Befehle mit `PS` gelten sowohl für Standard-ADM als auch für erweitertes ADM.

HP UX

- Unterstützte Dienstprogramme: lsof
- Erforderliche sudoer-Befehle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `Cmnd_Alias ADME_CMDS = /usr/local/bin/lsof -iTCP -n -P`
- `discoUser ALL=(root) NOPASSWD:ADME_CMDS`
- `Defaults!ADME_CMDS !requiretty`

Hinweis: Netstat wird nicht unterstützt.

- Zusätzliche Anforderungen: Keine

Centos und Ubuntu

- Unterstützte Dienstprogramme: Keine
- Erforderliche sudoer-Befehle:
  - `Cmnd_Alias ADME_CMDS = /usr/sbin/lsof -iTCP -n -P, /usr/bin/netstat -antp, /sbin/ss -tlnp, /sbin/ss -tenp`
  - `discoUser ALL=(root) NOPASSWD:ADME_CMDS`
  - `Defaults!ADME_CMDS !requiretty`
- Zusätzliche Anforderungen: Keine

Beachten Sie in Bezug auf die sudo-Befehle Folgendes:

- `ADME_CMDS` ist eine Variable, die auf eine Liste von Befehlen verweist.
- `/usr/bin/` ist das Verzeichnis, in dem sich lsof und netstat befinden.
- `discoUser` ist ein Benutzer, der über Root-Zugriff verfügen muss.

erweitertes ADMeinrichten und verwenden

Führen Sie die folgenden Schritte aus, um erweitertes ADM einzurichten und zu verwenden:

1. Aktivieren Sie erweitertes ADM mit der Discovery-Eigenschaft glide.discovery.enable_adme.
2. Bestimmen Sie das Basisverzeichnis, in dem die TCP-Nachverfolgungsdatei auf den Hostcomputern abgelegt wird. Wenn Sie den Speicherort ändern möchten, geben Sie ihn in den folgenden Discovery-Eigenschaften an:
   - `glide.discovery.adme.base_dir_unix`
   - `mid.powershell.target_base_dir`
3. Führen Sie basierend auf den Betriebssystemen der Hostcomputer eine der folgenden Aktionen aus:
   - Linux: Ändern Sie die Datei sudoers, damit die erforderlichen Befehle einbezogen werden:
   - Windows: Legen Sie den Parameter `mid.windows.management_protocol` auf dem MID Server fest, um WinRM oder WMI zu verwenden. Dieser Parameter legt das Protokoll fest, das Ihr MID Server für die Kommunikation mit Windows-Remotehosts verwendet.
4. Erstellen Sie einen Zeitplan, und führen Sie Discovery aus.
5. Zeigen Sie die Ergebnisse in den TCP-Tabellen an.
6. Steuern Sie optional die Größe der TCP-Nachverfolgungsdatei und die Nutzlast mithilfe von Parametern für die erweiterten ADM-Probes. Unter Erkennung von TCP-Verbindungen finden Sie die Namen der Probes und Parameter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter und Eigenschaften für ADM-Erkennung konfigurieren

Mithilfe von Eigenschaften können Sie die ADM-Erkennung aktivieren oder deaktivieren und den Speicherort der TCP-Nachverfolgungsdatei für erweitertes ADM festlegen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Sie können auch die Größe der TCP-Nachverfolgungsdatei und die Nutzlast mithilfe von Parametern für die erweiterten ADM-Probes steuern. Unter Erkennung von TCP-Verbindungen finden Sie die Namen der Probes und Parameter.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Discovery** um die Systemeigenschaften festzulegen.
2. Navigieren zu **Discovery-Definition** > **Probes** um die Probe-Parameter festzulegen.
3. Konfigurieren Sie die folgenden Eigenschaften und Probe-Parameter.
   Weitere Informationen finden Sie im Wissensartikel KB0822767 .

ADM-Eigenschaften und Probe-Parameter

Probe Parameter	Systemeigenschaft	Beschreibung
	glide.discovery.enable_adme	ADME: Aktivieren S erweiterte ADM-So „Ja“ wird die erwe Probe ausgelöst ur bei Bedarf auf die zurück. ◦ **Typ**: true | false ◦ **Standardwert**: fa
	glide.discovery.application_mapping	Aktivieren Sie die Anwendungszuord Wenn diese Eigens „true“ festgelegt is Erkennungen die re ADM-Sonde währe Erkundungsphase Discovery einen Se **Wichtig:** Dur Deaktivieren d Eigenschaft wi Erstellung von zwischen Anw deaktiviert, ab die ADM-Probe -Sensoren dea die Prozessklas wird nicht verh

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe Parameter	Systemeigenschaft	Beschreibung
		◦ **Typ**: true | false ◦ **Standardwert**: tru
sampling_interval	glide.discovery.adme.sampling_interval	ADME - Abtastinter Wie oft werden Pro Verbindungsdaten erfasst? Muss mind Sekunden betrage ◦ **Typ**: integer ◦ **Standardwert**: 12
base_dir	glide.discovery.adme.base_dir_unix	ADME – Unix-Basisv Ein vorhandenes V den UNIX-Zielcomp als Arbeitsbereich werden sollen. Mus absoluter Pfad zum sein. Die UNIX- und Anmeldeinformatio Sie für die Verbindu verwenden, müsse diesen Ordner zugr ◦ **Typ**: Zeichenfolg ◦ **Standardwert**: /t
powershell_param_base_dir	mid.powershell.target_base_dir	PowerShell – Zielbo Eine Netzwerkfreig Ziel-Windows-Com als Arbeitsbereich werden sollen. We Verzeichnis ändern auch um einen fre Netzwerkordner ha ◦ **Typ**: Zeichenfolg ◦ **Standardwert**: ac
aggregation_interval (Unix) powershell_param_aggregation_interval (Windows)	glide.discovery.adme.aggregation_interval	ADME – Aggregati (Sek): Wie oft (in Se sofortige Daten in zusammengefasst Es muss mindesten Sekunden betrage muss ein Vielfache Abtastintervalls sei ◦ **Typ**: integer ◦ **Standardwert**: 36
rolling_window_size (Unix)	glide.discovery.adme.rolling_window_size	ADME - Rollfende F Wie viele kürzlich a

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Probe Parameter	Systemeigenschaft	Beschreibung
powershell_param_rolling_window_size (Windows)		Blöcke sollen gesp werden? Ein aggre Block besteht aus ADME-Aggregatio und den ADME-Abtastintervallabt die neuesten Blöck beibehalten. ◦ **Typ**: Ganzzahl ◦ **Standardwert**: 24
max_total_samples (Unix) powershell_param_max_total_samples (Windows)	glide.discovery.adme.max_total_samples	ADME – Maximale Samples: Die Anza Skript genommene Die Ausführung de wird nach Abschlu Probenanzahl bee ◦ **Typ**: Ganzzahl ◦ **Standardwert**: 10

4. Klicken Sie auf **Speichern**.

Discovery-Verhalten

Discovery-Verhalten bestimmen die von Shazzam gestarteten Probes und die MID Server, von denen diese Probes gestartet werden.

Im Gegensatz zu einem Scan, der von einem einzelnen MID Server in einem bestimmten IP-Adressbereich durchgeführt wird, kann ein Verhalten mehreren MID Servern in demselben IP-Adresssegment oder in verschiedenen Netzwerksegmenten unterschiedliche Aufgaben zuweisen. Verhalten sind in Erkennungszeitplänen für Erkennungen verfügbar, in denen Konfigurationselemente (CI) in der CMDB aktualisiert werden.

Verhalten können in den folgenden Szenarien verwendet werden:

- Lastenausgleich: Ein Verhalten ermöglicht den Lastenausgleich in Systemen, die mehrere MID Server verwenden, die in einer oder mehreren Domänen bereitgestellt werden.
- Verschiedene Protokolle in mehreren Domänen: Konfigurieren Sie einen MID Server für die Suche nach allen Protokollen in einer Domäne und einem anderen MID Server, um einen WMI-Scan in einer zweiten Domäne durchzuführen.
- Zugriffssteuerungslisten (ACLs): Discovery kann SNMP-Geräte scannen, die durch eine ACL geschützt sind, wenn der MID Server-Hostcomputer Zugriff über diese ACL erhält. Verwenden Sie ein Verhalten, um einen MID Server zum Scannen von durch eine ACL geschützten Geräten zu konfigurieren.
- Geräte, die zwei Protokolle ausführen: Auf einigen Geräten werden möglicherweise zwei Protokolle gleichzeitig ausgeführt. Das häufigste Beispiel für zwei auf einem Gerät ausgeführte Protokolle sind die Protokolle SSH und SNMP. Ein Verhalten kann steuern, welches der beiden Protokolle für bestimmte Geräte untersucht wird. Das Verhalten verhindert dann die Erkundung des jeweils anderen Protokolls.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verhalten ermöglichen zudem die effiziente Discovery von SSH- und SNMP-Geräten sowie WMI-Geräten, die mit mehreren MID Servern in mehreren Windows-Domänen ausgeführt werden.

Beispiel: Eine Organisation verfügt über zwei Windows-Domänen und verschiedene UNIX-Computer und SNMP-Geräte in ihrem Netzwerk. Die Herausforderung besteht darin, alle Geräte effizient und ohne doppelten Aufwand zu erkennen. Jede Domäne enthält einen MID-Server Windows, mit dem die IP-Adressen der beiden im Zeitplan Discovery angegebenen Domänen sowie die SSH- und SNMP-Geräte gescannt werden. Es wird ein Verhalten benötigt, das die Arbeit angemessen aufteilt, um zu vermeiden, dass etwas zweimal gescannt wird. In diesem Beispiel wird davon ausgegangen, dass sich beide Domänen an demselben geografischen Standort befinden und dass ein einzelner Zeitplan ausreicht.

Hinweis: Die bevorzugte Methode für die Ausführung von Discovery über mehrere Windows-Domänen hinweg besteht in der Verwendung von PowerShell. Damit kann sich ein einzelner MID Server auf Computern in verschiedenen Domänen mit für die Instanz gespeicherten Anmeldeinformationen authentifizieren.

Discovery-Verhalten erstellen

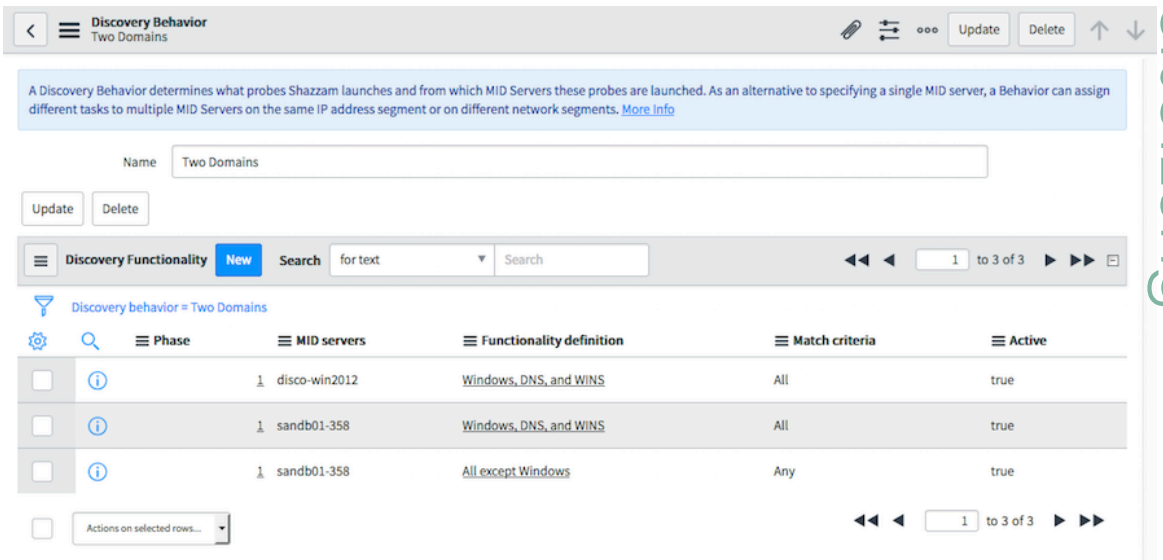
Erstellen Sie ein Discovery-Verhalten, um festzulegen, welche Probes von Shazzam gestartet werden und welcher MID Server verwendet wird.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **Verhalten** und klicken Sie auf **Neu**.
2. Geben Sie einen Namen ein.
3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.



4. Klicken Sie in der zugehörigen Liste „Discovery-Funktionalität“ auf **Neu**.
   Discovery Die Funktionalität definiert, was jeder MID-Server in diesem Verhalten tun muss, insbesondere welche Protokolle erkannt werden sollen.
5. Füllen Sie die Formularfelder folgendermaßen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Phase	Geben Sie eine ganze Zahl ein, die eine beliebige Phase darstellt. Die Phase wird verwendet, um eine oder mehrere Funktionalitäten zu gruppieren. Alle Funktionalitäten innerhalb einer bestimmten Phase werden gemeinsam ausgeführt, und alle Phasen werden in numerischer Reihenfolge ausgeführt. Alle Funktionalitäten in einem Verhalten können dieselbe Phase aufweisen. Die Shazzam-Probe wird einmal für jede Phase in einem Verhalten ausgeführt, weswegen eine geringere Anzahl von Phasen wünschenswert ist. Führen Sie mehrere Verhaltensphasen nur aus, wenn Geräte im Netzwerk mehrere Protokolle wie SSH und SNMP ausführen. In diesem Beispiel legen Sie eine Phase für den SSH-Scan und eine weitere Phase für den SNMP-Scan fest.
Aktiv	Lassen Sie diese Option ausgewählt, um die Discovery-Funktionalität anzuwenden.
Funktionalitätsdefinitionen	Klicken Sie auf das Suchsymbol, und wählen Sie dann eine vorkonfigurierte Funktionalität aus, die das Protokoll oder die Liste der von jedem MID Server gescannten Protokolle definiert.
Kriterien anpassen	Definieren Sie hier Kriterien für MID Server unter Windows.
MID Server	Wählen Sie mindestens einen MID Server aus, um diese Funktionalität für die folgenden Discovery-Typen auszuführen: ◦ IP-Scan ◦ CI-Scan Discovery gleicht die Last automatisch aus, wenn mehrere MID Server ausgewählt werden.

6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
7. Um Kriterien hinzuzufügen, die erfüllt sein müssen, damit die Funktionalität ausgelöst wird, klicken Sie in der zugehörigen Liste „Funktionalitätskriterien“ auf **Neu**, füllen die Formularfelder aus und klicken dann auf **Senden**.

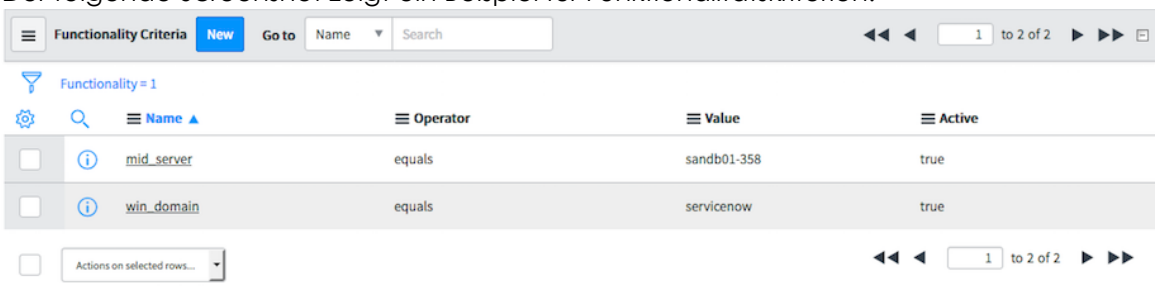
Feld	Eingabewert
Name	Der Name im Kriterium entspricht der Variablen, die die folgenden Informationen übergibt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	◦ `mid_server`: Der MID Server, der die Ergebnisse der Shazzam-Probe verarbeitet ◦ `win_domain`: Die Windows-Domäne des Zielgeräts
Operator	Wählen Sie einen logischen Operator aus.
Wert	Geben Sie den tatsächlichen Namen des MID Servers (`mid_server`) oder der Domäne (`win_domain`) ein, der/die für dieses Kriterium an Discovery übergeben werden soll. Dieses Feld kann auch den Wert `mid_domain` enthalten, der die Windows-Domäne des MID Servers definiert, der die Shazzam-Ergebnisse verarbeitet.

Hinweis: Funktionalitätskriterien sind nur für MID Server unter Windows erforderlich, und das auch nur, wenn das Verhalten Discovery domänenübergreifend steuert. Wenn die Instanz die Shazzam-Probe für eine Discovery startet, in der ein Verhalten mehrere MID Server zum Scannen mehrerer Domänen definiert, bestimmen die Funktionalitätskriterien, welcher MID Server die Ergebnisse der Probe verarbeitet.

Der folgende Screenshot zeigt ein Beispiel für Funktionalitätskriterien.



Nächste Maßnahme

Horizontale Erkennung planen vom Typ **Konfigurationselement**, und wählen Sie **Verhalten verwenden** für die MID-Server-Auswahlmethode aus.

Lastenausgleichsverhalten einrichten

Wenn mehrere MID Server so konfiguriert sind, dass sie dasselbe Protokoll scannen, können Benutzer ein Lastenausgleichsverhalten einrichten, um die Arbeit zwischen den MID Servern automatisch auszugleichen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Verhalten ermöglichen einen Lastenausgleich, wenn mehrere MID Server so konfiguriert sind, dass sie dasselbe Protokoll scannen. Beispiel: Eine Organisation hat 50 Remotestandorte, deren Größe zwischen 10 und mehreren Hundert Geräten variiert. Alle Außenstellen sind Teil derselben Windows-Domäne, die von einem zentralen Standort aus verwaltet wird. An diesem zentralen Standort sind drei MID Server installiert: zwei zum Scannen aller Windows-Geräte und einer zum Scannen der verbleibenden Geräte. Da sich einige der Zweigstellen in anderen Zeitzonen befinden, müssen für jede Zeitzone unterschiedliche Zeitpläne zur Ausführung von Discovery außerhalb der Spitzenzeiten erstellt werden. Für alle Zeitpläne kann dasselbe Verhalten verwendet werden, das automatisch zu einem Lastenausgleich der beiden Windows MID Server führt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie einen Verhaltensdatensatz.

   a. Erstellen Sie einen neuen Discovery-Verhaltensdatensatz, und geben Sie ihm einen beschreibenden Namen wie *LoadBalanced*.

   b. Klicken Sie mit der rechten Maustaste in die Headerleiste, und wählen Sie im Kontextmenü **Speichern** aus.

      Diese Aktion speichert den Datensatz und erstellt im Formular die zugehörige Liste „Discovery-Funktionalität“.

2. Definieren Sie die Windows-Funktionalität.

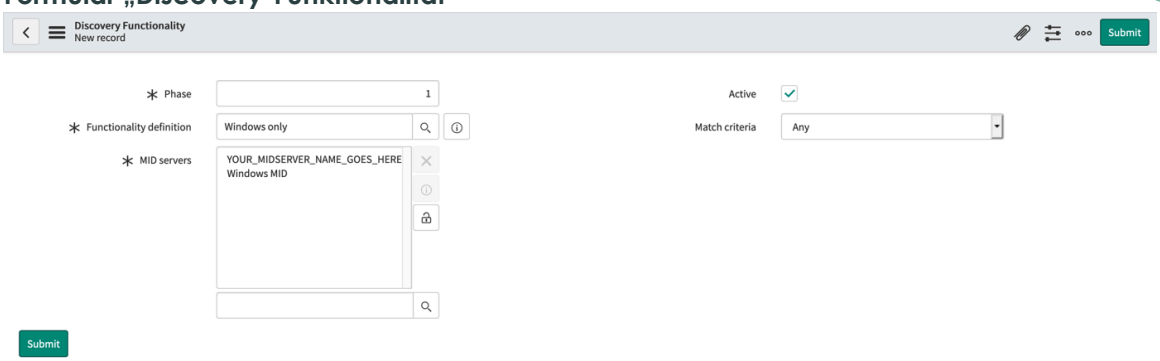
   a. Klicken Sie in der zugehörigen Liste „Discovery-Funktionalität“ auf **Neu**.

   b. Erstellen Sie mithilfe der im Folgenden beschriebenen Felder einen neuen Datensatz.

   c. Klicken Sie mit der rechten Maustaste in die Headerleiste, und wählen Sie im Kontextmenü **Speichern** aus.

Feld	Eingabewert
Phase	Geben Sie Phasennummer `1` in dieses Feld ein.
Funktionalität	Wählen Sie in der Liste *Windows only (WMI) (Nur Windows (WMI))* aus. Diese Funktionalität definiert das Protokoll, das gescannt wird. Da Sie WMI zum Scannen ausgewählt haben, müssen Sie Windows MID Server für diese Funktionalität auswählen.
MID Server	Sie wählen die beiden MID Server aus, die sich die Last für die WMI-Probes teilen sollen. Durch die Eingabe mehrerer MID Server in dieses Feld wird Discovery angewiesen, die Last automatisch zwischen diesen Servern auszugleichen. Wenn für jeden Server eine separate Funktionalität erstellt wird, würde kein Lastenausgleich erfolgen.
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Übernehmen Sie die Standardkriterien von *Beliebig*.

Formular „Discovery-Funktionalität“



3. Erstellen Sie Funktionalitätskriterien.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die gesamte Windows-Funktionalität erfordert Kriterien zum Identifizieren der Windows-Domäne und zum Definieren von speziellem Verhalten für die genannten MID Server.

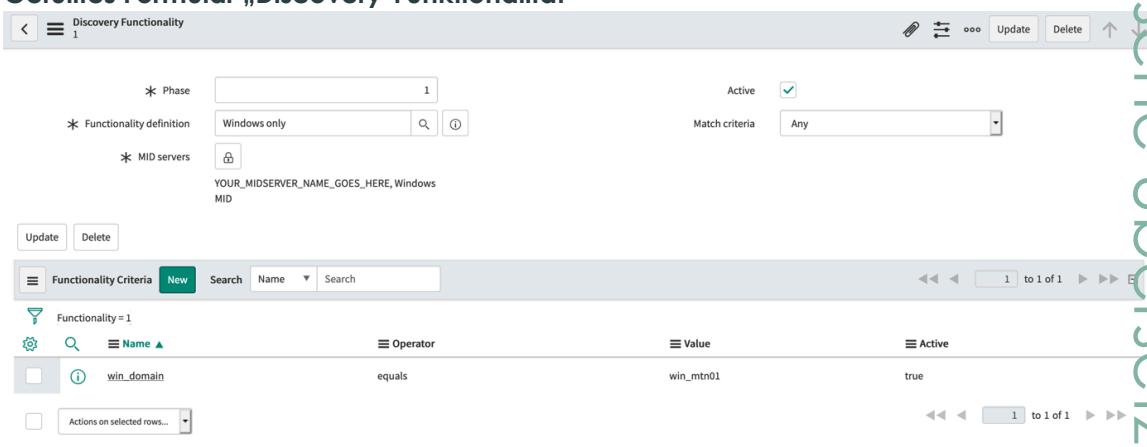
a. Klicken Sie in der zugehörigen Liste auf **Neu**.

b. Geben Sie die folgenden Werte ein:

Feld	Eingabewert
Name	Geben Sie `win_domain` als Namen für die Windows-Domäne ein, die Discovery mit den definierten MID Servern scannt.
Operator	Wählen Sie für dieses Kriterium *ist gleich* als Operator aus.
Wert	Dies ist der Name der Windows-Domäne, die diese MID Server nach Geräten scannen.
Aktiv	Stellen Sie sicher, dass Sie die Kriterien aktivieren, indem Sie dieses Kontrollkästchen (*true*) aktivieren.

Die festgelegten Kriterien werden im Formular „Discovery-Funktionalität“ für die Windows MID Server angezeigt.

Gefülltes Formular „Discovery-Funktionalität“



4. Definieren Sie die Funktionalität für die restlichen Scans.

Erstellen Sie einen zweiten Datensatz zum Scannen nach allen verbleibenden Protokollen (SSH, SNMP usw.) mit den folgenden Einstellungen:

Feld	Eingabewert
Phase	Geben Sie Phasennummer `1` in dieses Feld ein. Diese Phase wird gleichzeitig mit den WMI-Scans und mit derselben Shazzam-Probe ausgeführt. Aus Effizienzgründen verwenden Sie dieselbe Phasennummer, da Sie wissen, dass keines der Geräte in den Ziel-IP-Bereichen mehrere Protokolle (zum Beispiel SSH und SNMP) ausführt. Wenn Geräte mehrere Protokolle ausführen, würden Sie eine zweite oder gar dritte Phase angeben, um zuerst das richtige Protokoll für jedes Gerät zu erkennen.

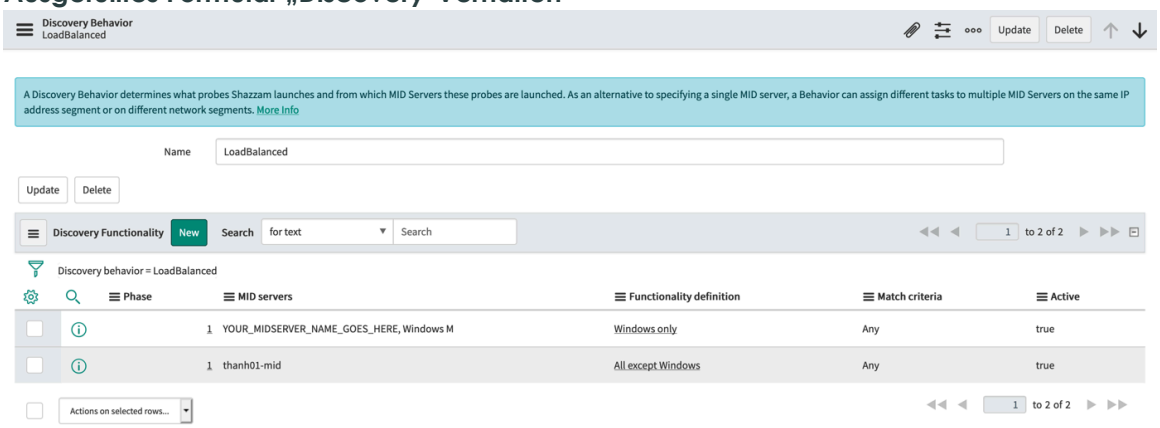
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Funktionalität	Wählen Sie in der Liste *All except Windows (no WMI) (Alle außer Windows (kein WMI))* aus. Diese Funktionalität veranlasst den MID Server, alle verbleibenden Protokolle zu scannen, nachdem Discovery die WMI-Scans ausgeführt hat.
MID Server	Geben Sie den Namen des MID Servers ein, der nach allen anderen Geräten scannt. Wenn Sie den automatischen Lastenausgleich verwenden möchten, können Sie diesem Feld einen zusätzlichen MID Server hinzufügen.

Das ausgefüllte Formular „Discovery-Verhalten“ sieht wie folgt aus. Für diesen MID Server müssen keine Funktionalitätskriterien erstellt werden.

Ausgefülltes Formular „Discovery-Verhalten“



5. Erstellen Sie einen Erkennungszeitplan für jede Zeitzone, und benennen Sie das soeben erstellte Verhalten.

   a. Navigieren zu **Discovery** > **Discovery-Zeitpläne** und klicken Sie in der Datensatzliste auf **Neu**.

   b. Wählen Sie im Feld **Erkennen** den Typ *Konfigurationselemente* aus.
   Daraufhin wird das Feld „Verhalten“ angezeigt.

   c. Klicken Sie auf das Lupensymbol, und wählen Sie das zu verwendende Verhalten aus.
   In diesem Beispiel wird *LoadBalanced* ausgewählt.

   d. Wählen Sie den entsprechenden Zeitpunkt zum Ausführen von Discovery für diesen Standort aus.

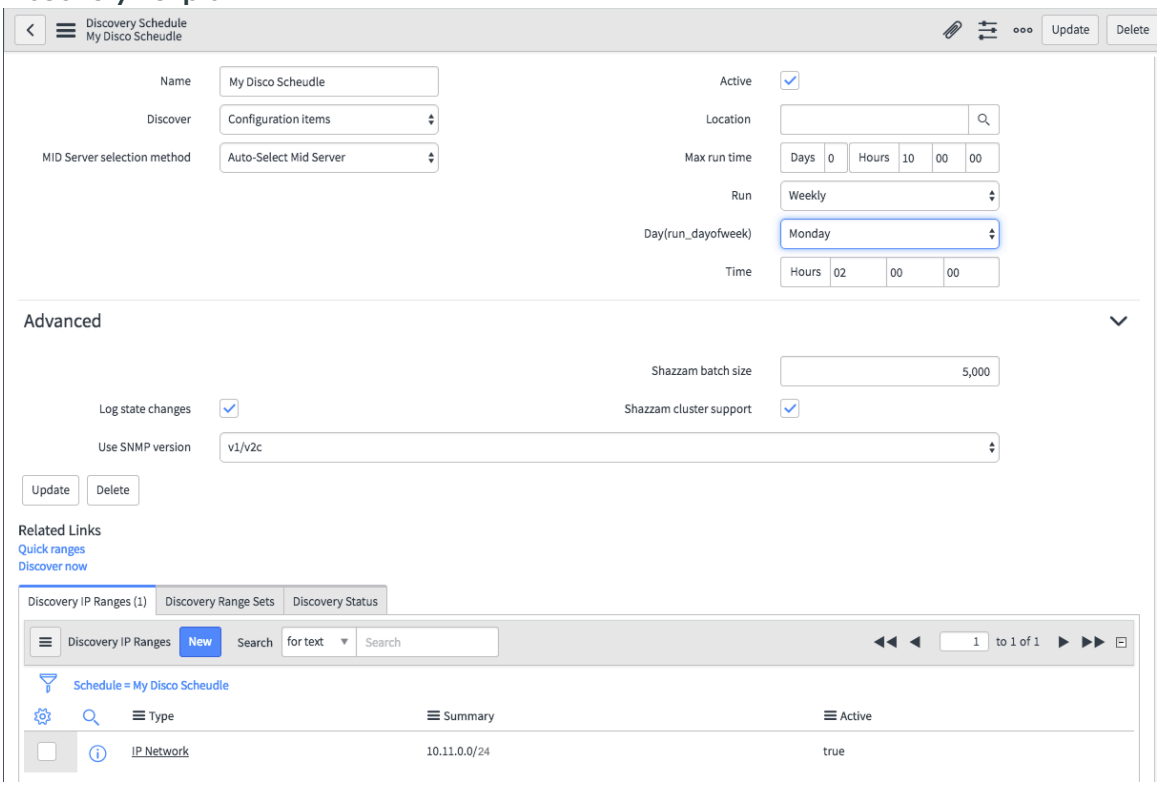
   e. Klicken Sie auf **Kurzbereiche**, und definieren Sie die IP-Adressbereiche, Netzwerke und Listen, die für diesen Standort durchsucht werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Speichern Sie den Datensatz.

g. Erstellen Sie zusätzliche Zeitpläne für jede Zeitzone oder Region im Netzwerk, und wählen Sie dasselbe Verhalten aus.

Discovery Zeitplan



Beispiele für Funktionalitäten eines Discovery-Verhaltens

Dieses Beispiel für ein Discovery-Verhalten erfordert drei Funktionalitäten für das Verhalten.

Für dieses Verhalten erstellen Sie die folgenden drei Funktionalitäten: einen MID Server zum Scannen von Domäne A nur für Windows-Geräte, eine zweite Funktionalität für denselben MID Server zum Scannen nach allen SSH- und SNMP-Geräten und eine dritte Funktionalität, die einen zweiten MID Server benennt, der Domäne B nach Windows-Geräten scannt. Die Begründung hierfür lautet wie folgt:

- Ein MID Server unter Windows kann nur Windows-Computer in der Windows-Domäne erkennen, der er angehört. Dies liegt einzig und allein an der Funktionsweise der Windows-Authentifizierung. Aus diesem Grund wird eine WMI-Funktionalität für jede Domäne benötigt.
- Ein MID Server kann unter Windows mit den richtigen Anmeldeinformationen SSH- und SNMP-Geräte überall erkennen. WMI-, SSH- und SNMP-Funktionalitäten können jedoch nicht über Windows-Domänen kombiniert werden. Das liegt daran, dass die Funktionalitätskriterien für WMI-Scans die Discovery auf eine bestimmte Domäne beschränken. Aus diesem Grund erfordern die SSH- und die SNMP-Erkennung jeweils eine eigene Funktionalität.
- Jeder Computer soll nur einmal gescannt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionalität 1: WMI-Scan auf Domäne A

Sie konfigurieren einen MID Server zum Scannen nach dem WMI-Protokoll auf Domäne A. WMI-Scans authentifizieren sich auf Windows-Computern mit den Domänenanmeldeinformationen des MID Server-Computers unter Windows. MID Server können unter Windows nicht außerhalb ihrer eigenen Domänen nach dem WMI-Protokoll suchen.

Erstellen Sie die erste Funktionalität mit den folgenden Werten:

Feld	Eingabewert
Phase	Geben Sie Phasennummer **1** in dieses Feld ein. Alle Funktionalitäten in diesem Beispiel verwenden dieselbe Phasennummer, weswegen eine einzelne Shazzam-Probe für alle Funktionalitäten in dieser Phase gestartet wird. Eine einzelne Phase stellt, wenn möglich, die effizienteste Verwendung der Shazzam-Probe dar.
Funktionalität	Wählen Sie in der Liste **Windows, DNS und WINS** aus. Diese Funktionalität definiert das WMI-Protokoll, das gescannt wird, und löst die Domäne auf. Da Sie sich dafür entschieden haben, nach WMI zu scannen, müssen Sie für diese Funktionalität einen Windows-MID Server auswählen.
MID Server	Wählen Sie einen Windows-MID Server aus Domäne A aus, in diesem Fall **sandb01-358**.
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Ändern Sie die Kriterien in **Alle**.

Funktionalitätskriterien erstellen

Alle Windows-Funktionalitäten erfordern Kriterien zum Identifizieren der Domäne und des MID Servers. In diesem Beispiel werden zwei Kriterien für diese Funktionalität erstellt. Klicken Sie zum Erstellen von Funktionalitätskriterien in der zugehörigen Liste auf **Neu**, und geben Sie die folgenden Werte für den MID Server ein, der den WMI-Scan in Domäne A durchführt:

Feld	Eingabewert
Name	Erstellen Sie die folgenden Kriterien: • Geben Sie `mid_server` als Namen für den MID Server ein, der die WMI-Scans in Domäne A ausführt. • Geben Sie `win_domain` als Namen für die Windows-Domäne ein, die von Discovery mit dem definierten MID Server gescannt wird.
Operator	Wählen Sie für dieses Kriterium **ist gleich** als Operator aus.
Wert	• Geben Sie für den Wert *mid_server* den Namen des MID Servers ein, der Domäne A auf Windows-Geräte scannt. • Geben Sie für den Wert *win_domain* den Namen der Domäne A ein, die dieser MID Server nach Windows-Geräten scannt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Aktiv	Stellen Sie sicher, dass Sie die Kriterien aktivieren, indem Sie dieses Kontrollkästchen (true) aktivieren.

Die festgelegten Kriterien werden im Formular „Discovery-Funktionalität“ für dieses Verhalten angezeigt.

Funktionalität 2: SSH und SNMP

Sie möchten in Ihrem Netzwerk nach UNIX-Computern und -Netzwerkgeräten scannen, diese aber Geräte nicht zweimal klassifizieren. Einer Ihrer MID Server ist so konfiguriert, dass er SSH und SNMP mit einer anderen Funktionalität klassifiziert, als für WMI-Scans verwendet wird. Sie müssen keine Kriterien für Nicht-WMI-Funktionalität erstellen.

Erstellen Sie die zweite Funktionalität mit den folgenden Werten:

Feld	Eingabewert
Phase	Geben Sie Phasennummer `1` in dieses Feld ein. Alle Funktionalitäten in diesem Beispiel verwenden dieselbe Phasennummer, weswegen eine einzelne Shazzam-Probe für alle Funktionalitäten in dieser Phase gestartet wird. Eine einzelne Phase stellt, wenn möglich, die effizienteste Verwendung der Shazzam-Probe dar.
Funktionalität	Wählen Sie in der Liste **All except Windows (no WMI) (Alle außer Windows (kein WMI))** aus. Diese Funktionalität scannt nur nach den Protokollen SSH und SNMP.
MID Server	Wählen Sie den MID Server aus Domäne A aus, in diesem Fall **sandb01-358**.
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Übernehmen Sie die Standardkriterien von *Beliebig*. Für Nicht-WMI-Funktionalitäten werden keine Kriterien verwendet.

Funktionalität 3: WMI-Scan auf Domäne B

Damit müssen Sie nur noch eine Funktionalität für die WMI-Scans in Domäne B erstellen. Aufgrund des Windows-Authentifizierungsmechanismus müssen Sie einen Windows-MID Server zum Scannen von Domäne B konfigurieren, der ein Mitglied dieser Domäne ist.

Erstellen Sie die dritte Funktionalität mit den folgenden Werten:

Feld	Eingabewert
Phase	Geben Sie Phasennummer `1` in dieses Feld ein. Alle Funktionalitäten in diesem Beispiel verwenden dieselbe Phasennummer, weswegen eine einzelne Shazzam-Probe für alle Funktionalitäten in dieser Phase gestartet wird. Eine einzelne Phase stellt, wenn möglich, die effizienteste Verwendung der Shazzam-Probe dar.
Funktionalität	Wählen Sie in der Liste **Windows, DNS und WINS** aus. Diese Funktionalität definiert das WMI-Protokoll, das gescannt wird, und löst die Domäne auf. Da Sie sich dafür entschieden haben, nach WMI zu scannen, müssen Sie für diese Funktionalität einen Windows-MID Server auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
MID Server	Wählen Sie einen Windows-MID Server aus Domäne B aus, in diesem Fall **disco-win2003**.
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Ändern Sie die Kriterien in *Alle*.

Funktionalitätskriterien erstellen

Alle Windows-Funktionalitäten erfordern Kriterien zum Identifizieren der Windows-Domäne und des MID Servers. In diesem Beispiel werden zwei Kriterien für diese Funktionalität erstellt. Klicken Sie zum Erstellen von Funktionalitätskriterien in der zugehörigen Liste auf **Neu**, und geben Sie die folgenden Werte für den MID Server ein, der den WMI-Scan in Domäne B durchführt:

Feld	Eingabewert
Name	Erstellen Sie die folgenden Kriterien: • Geben Sie `mid_server` als Namen für den MID Server ein, der die WMI-Scans in Domäne B ausführt. • Geben Sie `win_domain` als Namen für die Windows-Domäne ein, die von Discovery mit dem definierten MID Server gescannt wird.
Operator	Wählen Sie für dieses Kriterium **ist gleich** als Operator aus.
Wert	• Geben Sie für den Wert *mid_server* den Namen des MID Servers ein, der Domäne B auf Windows-Geräte scannt. • Geben Sie für den Wert *win_domain* den Namen der Domäne B ein, die dieser MID Server nach Windows-Geräten scannt.
Aktiv	Stellen Sie sicher, dass Sie die Kriterien aktivieren, indem Sie dieses Kontrollkästchen (true) aktivieren.

Die festgelegten Kriterien werden im Formular „Discovery-Funktionalität“ für dieses Verhalten angezeigt.

Beispiel für Discovery-Verhalten: Auf ACL-geschütztes SNMP-Gerät zugreifen

Greifen Sie mit dem Verhalten Discovery auf ein durch eine ACL geschütztes SNMP-Gerät zu.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Eine bestimmte Art von Zugriffssteuerungsliste (ACL) auf einem SNMP-Gerät kann verhindern, dass Discovery dieses Gerät identifiziert. Diese Liste definiert Hostcomputer anhand von IP-Adressen, die zum Ausführen von Agents auf SNMP-Geräten zugelassen sind. In diesem Beispiel sollen alle Geräte in einem IP-Bereich klassifiziert, identifiziert und aktualisiert werden, einschließlich der durch eine ACL geschützten SNMP-Geräte. Dazu müssen ein MID Server mit Zugriff auf die geschützten SNMP-Geräte installiert und ein Verhalten erstellt werden, mit dem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

nach allen Protokollen gescannt werden kann, sodass alle Geräte gefunden werden und keine zusätzliche Arbeit anfällt.

Prozedur

1. Installieren Sie einen MID Server auf einem von der ACL zugelassenen Host.

   Zum Scannen der SNMP-Geräte in einem durch eine ACL geschützten Netzwerk muss ein MID Server auf einem Hostcomputer installiert werden, für den anhand der IP-Adresse in der ACL angegeben ist, dass er über Zugriff auf die SNMP-Geräte verfügt. Da dieser MID Server nur SNMP-Geräte scannt, kann er auf jedem unterstützten Betriebssystem installiert werden. Der andere MID Server, der zur Erkennung von WMI und SSH konfiguriert ist, kann auf jedem Windows-Host installiert werden, für den die angegebenen IP-Bereiche sichtbar sind.

2. Installieren Sie zusätzliche MID Server, wenn Sie eine dieser Funktionen für den Lastenausgleich konfigurieren möchten.
3. Erstellen Sie einen Verhaltensdatensatz.

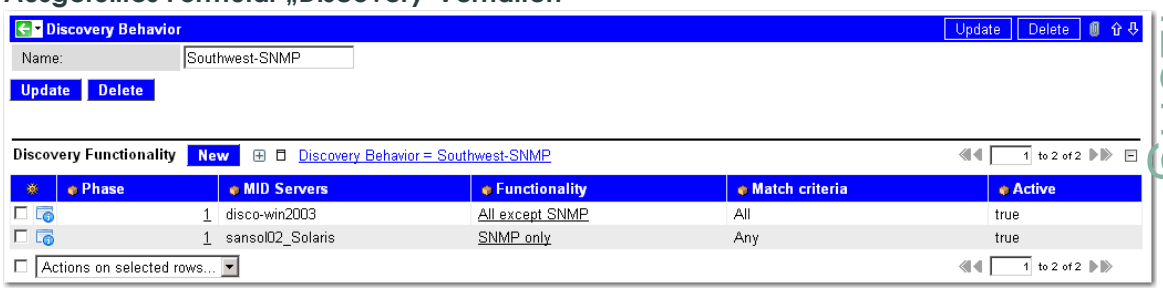
   a. Erstellen Sie einen neuen Discovery-Verhaltensdatensatz, und geben Sie ihm einen beschreibenden Namen wie *Southwest-SNMP*.

   b. Klicken Sie mit der rechten Maustaste in die Headerleiste, und wählen Sie im Kontextmenü **Speichern** aus.
   Diese Aktion speichert den Datensatz und erstellt im Formular die zugehörige Liste „Discovery-Funktionalität“.

   c. Um dieses Verhalten abzuschließen (wie in Abbildung 1 gezeigt), müssen Sie Funktionalitäten mit den MID Servern erstellen, die Sie zu diesem Zweck installiert haben.

   Für die Funktionalität, die nach dem WMI-Protokoll scannt, müssen Sie Kriterien definieren, die die Windows-Domäne und den verwendeten MID Server angeben. Da diese Discovery auf einer Windows-Domäne ausgeführt wird, können Sie eine Funktionalität für WMI und SSH (**All except SNMP (Alle außer SNMP)**) mit demselben MID Server konfigurieren.

Ausgefülltes Formular „Discovery-Verhalten“



4. Definieren Sie die Funktionalitäten.
   Erstellen Sie für dieses Verhalten zwei Funktionalitäten: eine für SNMP auf dem MID Server, der auf dem in der ACL angegebenen Host installiert ist, und eine weitere für WMI und SSH auf einem zweiten MID Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

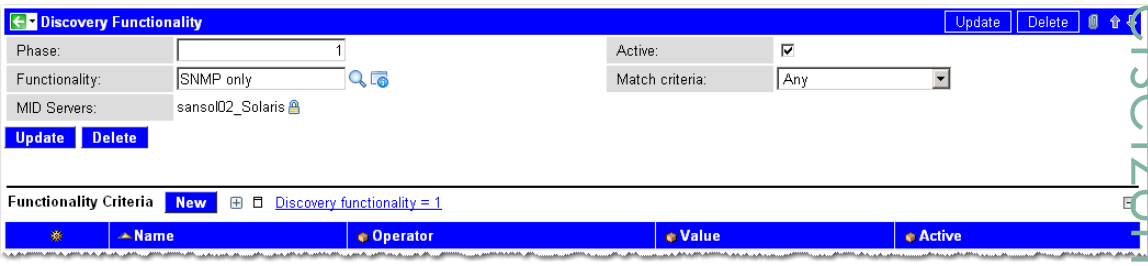
a. Klicken Sie in der zugehörigen Liste „Discovery-Funktionalität“ auf **Neu**, um Funktionalitäten hinzuzufügen.

b. **Hinweis:** Konfigurieren Sie den auf dem berechtigten Hostcomputer installierten MID Server so, dass er nur nach dem SNMP-Protokoll scannt.

Erstellen Sie die erste Funktionalität mit den folgenden Werten:

Feld	Eingabewert
Phase	Geben Sie Phasennummer `1` in dieses Feld ein. Beide Funktionalitäten in diesem Beispiel verwenden dieselbe Phasennummer, weswegen eine einzelne Shazzam-Probe für alle Funktionalitäten in dieser Phase gestartet wird. Eine einzelne Phase stellt, wenn möglich, die effizienteste Verwendung der Shazzam-Probe dar.
Funktionalität	Wählen Sie in der Liste *Nur SNMP* aus. Diese Funktionalität definiert das Protokoll, das gescannt wird.
MID Server	Wählen Sie einen MID Server (*sansol02_Solaris*) aus, der auf einem Solaris-Host installiert ist und dem durch die ACL Zugriff auf die SNMP-Geräte gewährt wird. Wenn Discovery einen automatischen Lastenausgleich für diese Funktionalität ausführen soll, können Sie mehrere MID Server auswählen.
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Übernehmen Sie die Standardkriterien von *Beliebig*. Für SNMP-Funktionalitäten werden keine Kriterien verwendet.

Nur nach SNMP scannen



c. **Hinweis:** In der zweiten Funktionalität scannt Discovery Ihre Domäne nach den Protokollen WMI und SSH. Da WMI eines der Protokolle ist, muss der MID Server für diese Funktionalität auf einem Windows-Computer installiert sein und über Kriterien verfügen.

Erstellen Sie die zweite Funktionalität mit den folgenden Werten:

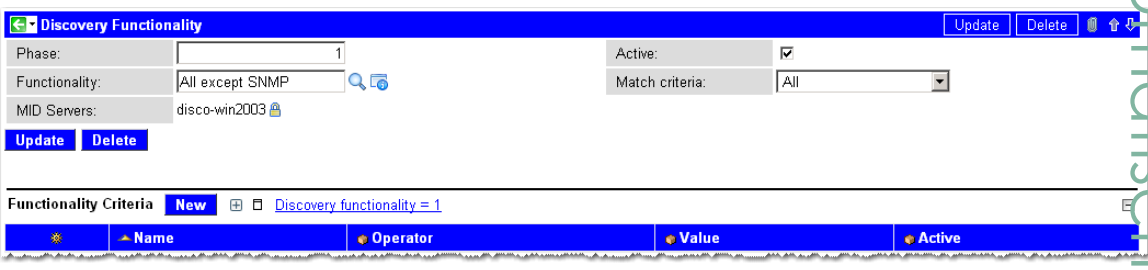
Feld	Eingabewert
Phase	Geben Sie Phasennummer `1` in dieses Feld ein. Alle Funktionalitäten in diesem Beispiel verwenden dieselbe Phasennummer, weswegen eine einzelne Shazzam-Probe für alle Protokoll-Scans gestartet wird. Eine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
	einzelne Phase stellt, wenn möglich, die effizienteste Verwendung der Shazzam-Probe dar.
Funktionalität	Wählen Sie in der Liste *All except SNMP (Alle außer SNMP)* aus. Diese Funktionalität definiert die Protokolle, nach denen gescannt wird. Da WMI eines der ausgewählten Protokolle ist, müssen Sie einen Windows-MID Server für diese Funktionalität verwenden.
MID Server	Wählen Sie einen Windows-MID Server in Ihrer Domäne aus. In diesem Fall wählen Sie *disco-win2003* aus. Wenn Discovery einen automatischen Lastenausgleich für diese Funktionalität ausführen soll, können Sie mehrere MID Server auswählen.
Aktiv	Stellen Sie sicher, dass dieses Kontrollkästchen aktiviert ist, um dieses Verhalten zu aktivieren.
Kriterien anpassen	Ändern Sie die Kriterien in *Alle*.

Nach allen außer SNMP scannen



d. **Hinweis:** Funktionalitäten, die nach WMI scannen, erfordern Kriterien zum Identifizieren der Domäne und des MID Servers. In diesem Beispiel werden zwei Kriterien für diese Funktionalität erstellt.

Um Funktionalitätskriterien für einen WMI-Scan zu erstellen, klicken Sie in der zugehörigen Liste auf **Neu**.

e. Geben Sie die folgenden Werte für den MID Server ein, der den WMI-Scan in unserer Domäne durchführt:

Feld	Eingabewert
Name	Erstellen Sie die folgenden Kriterien: ▪ Geben Sie `mid_server` als Namen für den MID Server ein, der die WMI-Scans ausführt. ▪ Geben Sie `win_domain` als Namen für die Windows-Domäne ein, die von Discovery mit dem definierten MID Server gescannt wird.
Operator	Wählen Sie für dieses Kriterium *ist gleich* als Operator aus.
Wert	▪ Geben Sie für den Wert *mid_server* den Namen des MID Servers ein, der Domäne B auf Windows-Geräte scannt. ▪ Geben Sie für den Wert *win_domain* den Namen Ihrer Windows-Domäne ein.

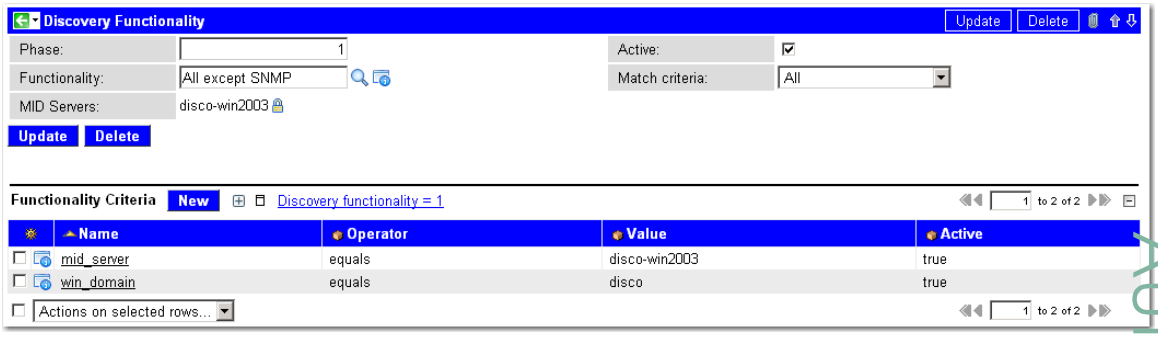
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Aktiv	Stellen Sie sicher, dass Sie die Kriterien aktivieren, indem Sie dieses Kontrollkästchen (*true*) aktivieren.

Die festgelegten Kriterien werden wie folgt im Formular „Discovery-Funktionalität“ für dieses Verhalten angezeigt.

Funktionalitätskriterien für WMI-Scans



5. Erstellen Sie den Zeitplan.

a. Erstellen Sie einen Discovery-Zeitplan, und benennen Sie das soeben erstellte Verhalten.

b. Navigieren zu **Discovery** > **Discovery-Zeitpläne** und klicken Sie in der Datensatzliste auf **Neu**.

c. Wählen Sie im Feld **Erkennen** den Modus *Konfigurationselemente* aus.
Diese Aktion zeigt das Feld **Verhalten** an.

d. Klicken Sie auf das Lupensymbol, und wählen Sie das zu verwendende Verhalten aus.
Wählen Sie in diesem Beispiel *Southwest-SNMP* aus.

e. Wählen Sie den entsprechenden Zeitpunkt zum Ausführen von Discovery für diesen Standort aus.

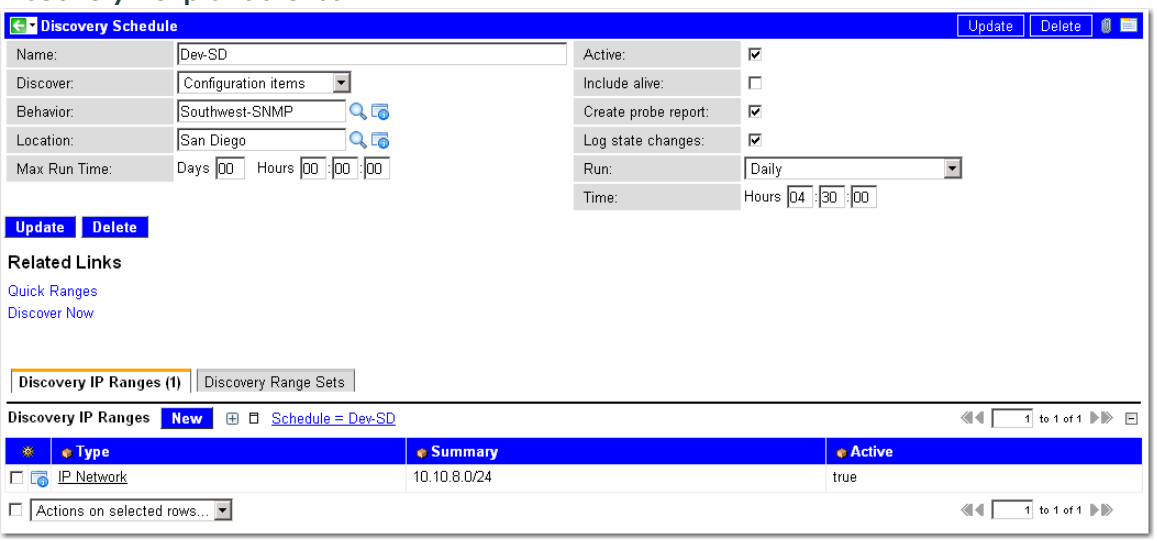
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Klicken Sie auf **Kurzbereiche**, und definieren Sie die IP-Adressbereiche, Netzwerke und Listen, die für diese Domäne gescannt werden sollen.

g. Speichern Sie den Datensatz.

Discovery-Zeitplandatensatz



CI-Löschstrategien für Mustererkennung

Wenn Sie eine Erkennung mit einem Muster durchführen, können Sie auswählen, was mit CIs geschehen soll, die in der CMDB vorhanden sind, aber von Discovery nicht mehr erkannt werden.

Hinweis: Löschstrategien sind nur mit Mustern verfügbar, nicht mit Probes/Sensoren.

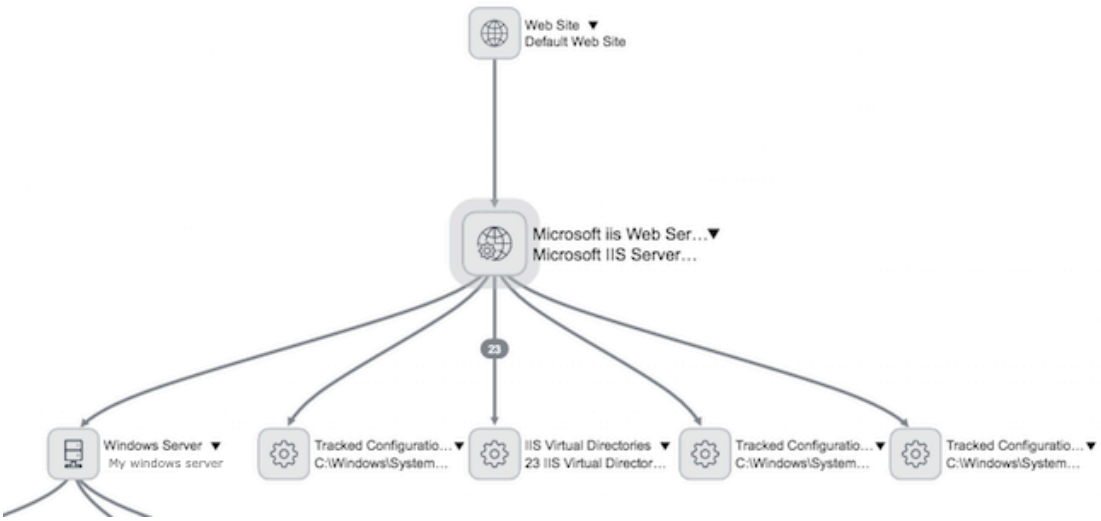
Wenn Sie ein Muster zum Durchführen der Erkennung verwenden, identifizieren Sie einen CI-Typ. Dabei handelt es sich um das Haupt-CI, das Sie suchen, zum Beispiel einen IIS-Webserver oder Tomcat-Server. Discovery kann auch zugehörige CIs erkennen und die CMDB entsprechend füllen. Beispielsweise kann Discovery nach der Erkennung eines IIS-Servers mit dem Muster „IIS“ auch die zugehörigen CIs finden:

- Den Windows-Computer, der den Webserver hostet
- Die Konfigurationsdateien für den IIS-Server
- Die Website, die der IIS-Server hostet

Die Abhängigkeitszuordnung zum Haupt-CI zeigt auch die zugehörigen CIs an, wie in der folgenden Grafik dargestellt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

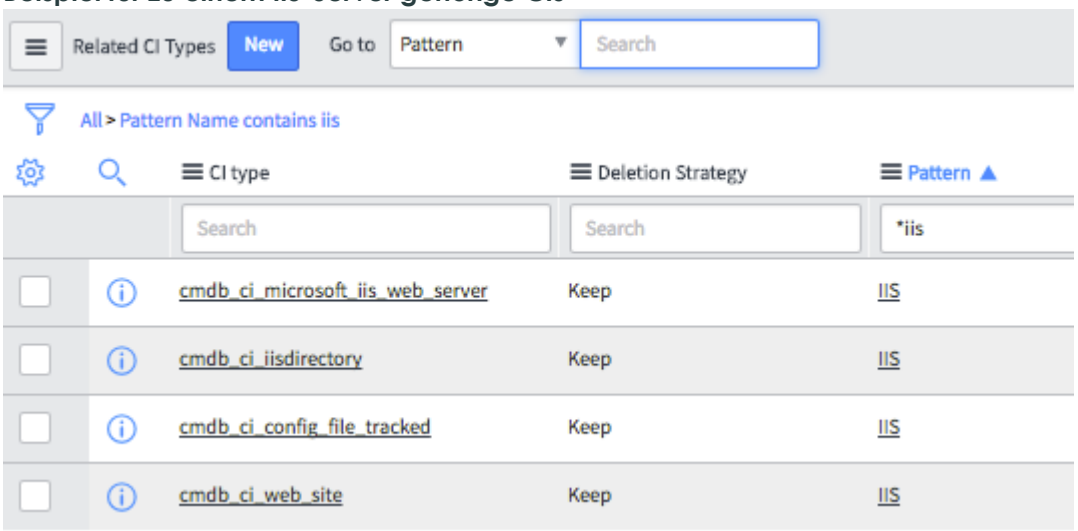
Beispiel für ein Haupt-CI des IIS-Servers und die zugehörigen CIs



Nachdem Sie das Haupt-CI und die zugehörigen CIs zum ersten Mal mit einem Muster erkannt haben, fügt Discovery der Tabelle „Zugehörige CI-Typen“ [sa_ci_to_pattern] für jede Beziehung zwischen dem Haupt-CI und einem zugehörigen CI-Typ einen Eintrag hinzu. In diesen Datensätzen bestimmen Sie die Löschungsstrategie für jedes zugehörige CI anhand des Typs, zu dem es gehört. Außer für AWS- und Azure-Cloud-Datenbanken können Sie keine Löschungsstrategie für das Haupt-CI festlegen.

Sie können eine Liste der Beziehungen anzeigen, wie in der folgenden Abbildung dargestellt:

Beispiel für zu einem IIS-Server gehörige CIs



Die Löschungsstrategie für zugehörige CIs wird wirksam, wenn die beiden folgenden Bedingungen zutreffen:

- Nachdem Sie Discovery mit dem Muster erneut ausgeführt haben
- Discovery erkennt das Haupt-CI erfolgreich, aber nicht das zugehörige CI.

Für die Löschungsstrategie sind die folgenden Optionen verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
Behalten	Behält den Konfigurationsdatei-CI-Datensatz bei und nimmt keine weiteren Änderungen am Datensatz vor. Diese Option ist die Standardeinstellung.
Löschen	Löscht den Konfigurationsdatei-CI-Datensatz aus der CMDB und die Beziehung zum Haupt-CI.
Als abwesend markieren	Markiert das Feld **Status** [install_status] des Konfigurationsdatei-CI-Datensatzes als **Abwesend** - dies bedeutet, dass Discovery die verfolgte Konfigurationsdatei nicht finden kann. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen. **Hinweis:** Es gibt zwei Tabellen, deren CIs gelöscht werden, wenn sie als abwesend markiert sind: „cmdb_ci_network_adapter“ und „cmdb_ci_ip_address“.
Beziehungen löschen	Löscht nur die CI-Beziehungen zwischen dem zugehörigen CI und dem Haupt-CI.
Als deaktiviert markieren	Markiert das Feld **Status** [install_status] des CI-Datensatzes der Konfigurationsdatei als **Deaktiviert**, was bedeutet, dass Discovery diese Konfigurationsdatei nicht mehr verwendet. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen.

Hinweis: Löschstrategien sind nicht für zugehörige Einträge verfügbar, bei denen es sich um Regeln handelt, die auf zugehörigen CIs basieren. Weitere Informationen finden Sie unter .

Löschungsstrategie festlegen

Legen Sie eine Löschungsstrategie fest, wenn Sie Aktionen für ein zugehöriges CI durchführen möchten, das Discovery über die Mustererkennung nicht mehr finden kann. Sie können das Haupt-CI nur löschen, wenn es sich dabei um eine AWS- oder Azure-Cloud-Datenbank handelt.

Vorbereitungen

- Erforderliche Rolle: cloud_admin, service_mapping_admin oder admin
- CIs: Ein Haupt-CI und zugehörige CIs, die im Erkennungsprozess bei der Mustererkennung erkannt wurden

Warum und wann dieser Vorgang ausgeführt wird

Sie können Löschungsstrategien für alle erkannten CIs festlegen, einschließlich Konfigurationsdatei-CIs. Für nachverfolgte Konfigurationsdateien greifen Sie jedoch auf eine andere Weise auf die Löschungsstrategie zu als der in diesem Thema beschriebenen. Anweisungen dazu finden Sie unter Löschungsstrategie für nachverfolgte Konfigurationsdateien festlegen.

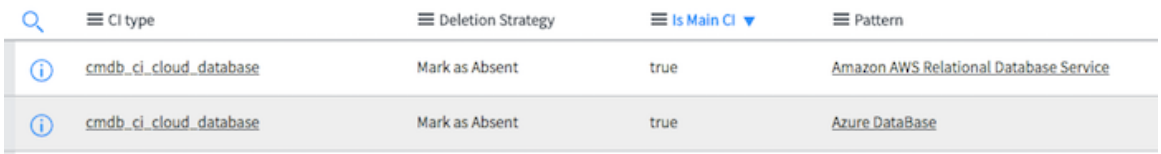
Prozedur

1. Öffnen Sie die Liste der zugehörigen CI-Typen, indem Sie `sa_ci_to_pattern.list` im Anwendungsfilter eingeben.
2. Filtern Sie die Liste, um den CI-Typ zu finden, der durch die Mustererkennung einem Haupt-CI zugehörig ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie eine Löschungsstrategie für eine Cloud-Datenbank festlegen möchten, durchsuchen Sie die Liste nach dem CI-Typ *cmdb_ci_cloud_database*.

Beachten Sie, dass für die CI-Typen *cmdb_ci_cloud_database* der Wert **Ist-Haupt-CI** auf **true** festgelegt ist. Das gibt an, dass Sie eine Löschungsstrategie für AWS- und Azure-Datenbanken festlegen können, selbst wenn es sich dabei um das Haupt-CI handelt, das durch die Cloud-Erkennung erkannt wird.



CI type	Deletion Strategy	Is Main CI	Pattern
cmdb_ci_cloud_database	Mark as Absent	true	Amazon AWS Relational Database Service
cmdb_ci_cloud_database	Mark as Absent	true	Azure DataBase

3. Doppelklicken Sie in der Listenansicht auf den Wert im entsprechenden Feld in der Spalte **Löschungsstrategie**.
4. Wählen Sie einen neuen Wert aus:

Wert	Beschreibung
Behalten	Behält den Konfigurationsdatei-CI-Datensatz bei und nimmt keine weiteren Änderungen am Datensatz vor. Diese Option ist die Standardeinstellung.
Löschen	Löscht den Konfigurationsdatei-CI-Datensatz aus der CMDB und die Beziehung zum Haupt-CI.
Als abwesend markieren	Markiert das Feld **Status** [install_status] des Konfigurationsdatei-CI-Datensatzes als **Abwesend** - dies bedeutet, dass Discovery die verfolgte Konfigurationsdatei nicht finden kann. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen. **Hinweis:** Es gibt zwei Tabellen, deren CIs gelöscht werden, wenn sie als abwesend markiert sind: „cmdb_ci_network_adapter“ und „cmdb_ci_ip_address“.
Beziehungen löschen	Löscht nur die CI-Beziehungen zwischen dem zugehörigen CI und dem Haupt-CI.
Als deaktiviert markieren	Markiert das Feld **Status** [install_status] des CI-Datensatzes der Konfigurationsdatei als **Deaktiviert**, was bedeutet, dass Discovery diese Konfigurationsdatei nicht mehr verwendet. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen.

Konfigurationsdateien nachverfolgen

Bei der horizontalen Erkennung können Konfigurationsdateien, die zu bestimmten Anwendungen gehören, erkannt und der CMDB hinzugefügt werden. Sie können die Änderungen an diesen Dateien nachverfolgen, indem Sie sie mit vorherigen Versionen vergleichen.

Warnung: Konfigurationsdateien enthalten sensible Systeminformationen. Um nicht autorisierten Zugriff zu verhindern, stellen Sie sicher, dass in der Tabelle „Nachverfolgte Konfigurationsdatei“ [cmdb_ci_config_file_tracked] Zugriffssteuerungslisten (ACL) platziert sind. Erlauben Sie nur autorisierten Benutzern, diese Tabelle anzuzeigen, oder deaktivieren Sie die Einstellung **Inhalt speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten zum Nachverfolgen der Konfigurationsdatei

CI-Typ

Alle Anwendungen und Hosts in Ihrer Organisation müssen über einen entsprechenden Typ von Konfigurationselement bzw. Configuration Item (CI) verfügen, der dafür erforderlich ist, dass diese Anwendungen und Hosts richtig erkannt und verarbeitet werden.In einem Basissystem sind für viele CI-Typen Konfigurationsdateipfade vorgegeben. Sie können neue Definitionen für die Nachverfolgung von Konfigurationsdateien hinzufügen oder ändern. Siehe Nachverfolgung von Changes in Konfigurationsdateien ändern für Anweisungen.

Muster

Die Nachverfolgung der Konfigurationsdatei ist für Muster verfügbar, die Anwendungen erkennen. Für das Muster können Sie Definitionen zur Dateinachverfolgung erstellen, die den CI-Typ angeben, zu dem das Anwendungs-CI gehört, sowie den Pfad der Konfigurationsdatei. Geben Sie so viele Definitionen für die Nachverfolgung von Dateien an wie nötig. Sie können auch angeben, ob Sie den Inhalt von Konfigurationsdateien speichern möchten, damit Sie den Inhalt verschiedener Versionen anzeigen und vergleichen können.

Hinweis:

Die Nachverfolgung der Konfigurationsdatei ist nicht für Erkennungen verfügbar, die mit traditionellen Probes und Sensoren durchgeführt werden.

Die Klassifizierung, die das Muster auslöst, muss die Probe „Horizontal Pattern“ angeben, der wiederum das Muster angeben muss. Wenn Sie ein Upgrade Ihrer Instanz auf die aktuelle Version durchführen, sind nicht alle Klassifizierer so konfiguriert, dass sie für die Erkennung standardmäßig Muster verwenden.

CMDB

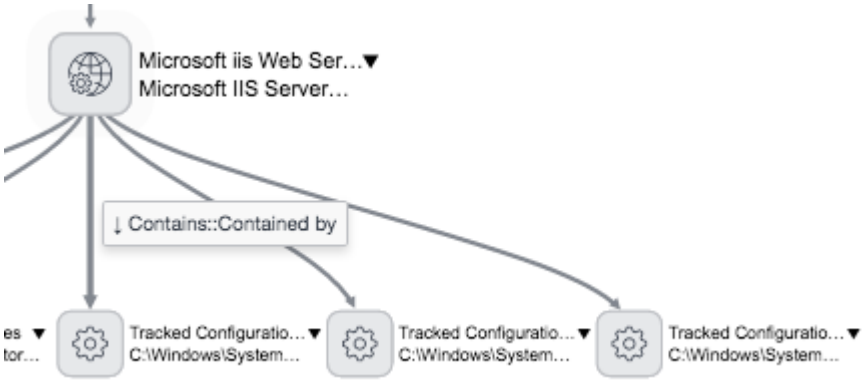
Alle Konfigurationsdateien werden als CI in der Tabelle „Nachverfolgte Konfigurationsdatei“ [cmdb_ci_config_file_tracked] gespeichert. Wenn Sie das Speichern des Inhalts aktivieren, enthalten diese CI-Datensätze den Inhalt der Konfigurationsdateien, einschließlich vorheriger Versionen. Im CI-Datensatz der Konfigurationsdatei können Sie verschiedene Versionen vergleichen.

Abhängigkeits- und Anwendungsservice-Zuordnungen

Sowohl Abhängigkeitsübersichten als auch für Servicezuordnungen zeigen nachverfolgte Konfigurationsdateien an. Die Beziehung zwischen einer Konfigurationsdatei und ihrem Host ist eine Beziehung vom Typ „Enthält“. Die Anwendung enthält die Konfigurationsdatei.

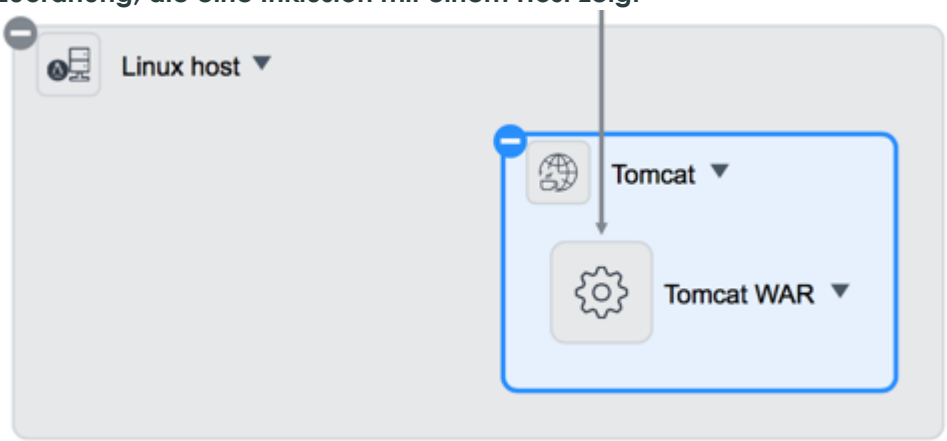
Dieser IIS-Webserver enthält beispielsweise drei nachverfolgte Konfigurationsdateien:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Manchmal organisieren Sie CI-Typen als Haupt-CI-Typ und seine zugehörigen CI-Typen. In einer Serviceinstanzzuordnung zeigt Service-Mapping Änderungen an Konfigurationsdateien der zugehörigen CIs für die Haupt-CIs in Einschlüssen an. Bei Inklusionen behandelt das System auf einem Server gehostete Anwendungen als unabhängige Objekte. Die Tomcat-WAR-CI wird beispielsweise getrennt von ihrem Host, den Tomcat-CIs, angezeigt. In diesem Fall zeigt Service-Mapping Änderungen an Konfigurationsdateien von Tomcat WAR an, wenn Sie Tomcat auswählen. Zusätzlich zeigt Service-Mapping Änderungen an Konfigurationsdateien des Hardware-Servers an, der Inklusionen hostet. In diesem Beispiel handelt es sich um einen Linux-Server:

Zuordnung, die eine Inklusion mit einem Host zeigt



Löschungsstrategie

Sie können angeben, was Sie mit den CI-Datensätzen nachverfolgter Konfigurationsdateien tun möchten, wenn sie bei der Erkennung nicht mehr erkannt werden. Sie können den CI-Datensatz der Konfigurationsdatei beibehalten, automatisch löschen, nur die CI-Beziehungen löschen oder als abwesend markieren.

Erkennungsmuster, die die Nachverfolgung von Konfigurationsdateien standardmäßig unterstützen

Die folgenden Muster bieten standardmäßig Definitionen von nachverfolgten Dateien:

Klassifizierung	Muster	CI-Typ	Dateipfad der nachverfolgten Datei
Apache-Server	Apache On Unix	Apache-Webserver [cmdb_ci_apache_web_server]	`$config_file`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassifizierung	Muster	CI-Typ	Dateipfad der nachverfolgten Datei
	Apache On Windows		
MySQL-Server	MySQL server On Windows and Linux	MySQL-Instanz [cmdb_ci_db_mysql_instance]	`$config_file`
Microsoft IIS Server	IIS	Microsoft IIS-Webserver [cmdb_ci_microsoft_iis_we	`EVAL(javascript: var rtrn = '';var winDir = CTX.getCommandManager().shellCommand("echo %WinDir%", false, null, null, CTX);rtrn = winDir.trim() + '\\System32\\Inetsrv\\Config\\*.config';)`
		Virtuelles IIS-Verzeichnis [cmdb_ci_iisdirectory]	`$install_directory + "\*.config"`
TIBCO BusinessWorks und EMS	ActiveMatrix BusinessWorks	ActiveMatrix Business Works [cmdb_ci_appl_tibco_matrix]	`$config_file`
	Enterprise Message Service	Tibco Enterprise Message Service [cmdb_ci_appl_tibco_message]	`$config_file`
Oracle	Oracle DB on Windows	Oracle-Instanz [cmdb_ci_db_ora_instance	`$install_directory + "\network\admin\*.ora"`
		Oracle-Instanz [cmdb_ci_db_ora_instance	`$install_directory + "\dbs\*.ora"`
	Oracle DB on Unix	Oracle-Instanz [cmdb_ci_db_ora_instance	`$install_directory + "/dbs/*.ora"`
		Oracle-Instanz [cmdb_ci_db_ora_instance	`$install_directory + "/network/admin/*.ora"`
Tomcat	Tomcat	Tomcat [cmdb_ci_app_server_tom	`$install_directory + "/conf/server.xml"`
		Tomcat WAR [cmdb_ci_app_server_tom	`$install_directory + "/WEB-INF/web.xml"`
WMB	WMB On Unix	IBM WebSphere Message Broker [cmdb_ci_appl_ibm_wmb]	`$install_directory + "/*/etc/config/*/*.prop"`
	WMB On Windows	IBM WebSphere Message Broker [cmdb_ci_appl_ibm_wmb]	`$install_directory + "\*\etc\config\*\*.prop"`
WMQ	WMQ On Windows	IBM MQ Manager (früher IBM WebSphere MQ) [cmdb_ci_appl_ibm_wmq]	`$install_directory + "\*\config\*"`
	WMQ On Windows	IBM MQ-Manager [cmdb_ci_appl_ibm_wmq]	`$install_directory + "/bin/*.sh"`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibung

1. Aktivieren Sie die Nachverfolgung von Konfigurationsdateien, indem Sie die Discovery-Eigenschaft `glide.discovery.enable_file_tracking` auf „true“ setzen.

   Sie können auch andere Eigenschaften konfigurieren, um die Größe und Anzahl der nachverfolgten Konfigurationsdateien, das Zeitfenster, in dem Änderungen an Konfigurationsdateien für eine bestimmte Version nachverfolgt werden, und die Anzahl der zulässigen Änderungen an einer Konfigurationsdatei während dieses Zeitfensters zu steuern. Details siehe Discovery-Eigenschaften.

2. Führen Sie die folgenden Schritte aus, um den unbefugten Zugriff auf sensible Informationen aus Konfigurationsdateien zu verhindern:

   a. Stellen Sie sicher, dass in der Tabelle „Nachverfolgte Konfigurationsdatei“ [cmdb_ci_config_file_tracked] Zugriffssteuerungsregeln (ACL) platziert sind. Erlauben Sie nur autorisierten Benutzern, diese Tabelle anzuzeigen, oder deaktivieren Sie die Einstellung **Inhalt speichern**.

   b. Stellen Sie sicher, dass die Rolle tracked_file_reader, die den Zugriff auf Konfigurationsdateidaten steuert, den richtigen Benutzern und Benutzergruppen zugewiesen ist. Standardmäßig enthält die Rolle itil die Rolle tracked_file_reader, die allen Benutzern mit der Rolle itil Zugriff auf Informationen in Konfigurationsdateien gewährt.

3. Stellen Sie sicher, dass die Probe „Horizontal Discovery“ für den Klassifizierer der zu erkennenden Software aktiviert ist. Falls nicht, können Sie sie aktivieren, das Muster angeben und dann die anderen Probes deaktivieren. Anweisungen dazu finden Sie unter Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen.
4. Fügen Sie Definitionen von nachverfolgten Dateien hinzu, oder ändern Sie sie, um den CI-Typ oder Dateipfad zu ändern.
5. Definieren Sie die Löschungsstrategie für nachverfolgte Dateien, um festzulegen, was mit den CI-Datensätzen der nachverfolgten Konfigurationsdateien geschehen soll, wenn sie bei der Mustererkennung nicht mehr zu finden sind.
6. Führen Sie eine horizontale Erkennung auf den Hosts aus, auf denen die Anwendungen ausgeführt werden, die Sie mit Mustern erkennen möchten. Öffnen Sie den CI-Datensatz der Anwendung, und überprüfen Sie die zugehörige Liste „Nachverfolgte Konfigurationsdateien“.
7. Vergleichen Sie zwei Versionen von nachverfolgten CI-Konfigurationsdateien, um die tatsächlich vorgenommenen Änderungen anzuzeigen.

Nachverfolgung von Changes in Konfigurationsdateien ändern

Konfigurieren Sie das System so, dass Informationen über Changes in Konfigurationsdateien gesammelt werden, die zu einem Configuration Item (CI) gehören. Service-Mapping verwendet diese Informationen, um Benutzer über Änderungen an CI-Konfigurationsdateien zu informieren und die tatsächlichen Änderungen an Konfigurationsdateien direkt in den Serviceinstanzzuordnungen anzuzeigen.

Vorbereitungen

Erforderliche Rolle: cloud_admin, service_mapping_admin oder admin
Um die Nachverfolgung von Konfigurationsdateien für ein CI zu aktivieren, für das das System Dateien nachverfolgt, konfigurieren Sie die Klassifizierung für den CI-Typ, zu dem dieses CI gehört:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für CI-Typen, die Anwendungen darstellen, können Sie für das relevante Muster eine Discovery-Prozessklassifizierung erstellen. Fügen Sie in der Spalte **Probe** die Probe Horizontal Pattern hinzu, und geben Sie Ihr Muster anschließend in der Spalte **Muster** an.
- Führen Sie für CI-Typen, die SNMP-Geräte darstellen, die Konfiguration gemäß der Beschreibung in Discovery-CI-Klassifizierung erstellen durch.

Hinweis: CI-Klassifizierungen für Hosts müssen nicht erstellt werden, da diese Klassifizierungen im Basissystem enthalten sind.

Warum und wann dieser Vorgang ausgeführt wird

Das System verfolgt Konfigurationsdateien als Teil des horizontalen Erkennungsprozesses eines CI, zu dem diese Dateien gehören. Konfigurationsdateien enthalten CI-Einstellungen und -Parameter. Service-Mapping nutzt diese Informationen, um Benutzer über Änderungen an CI-Konfigurationsdateien zu informieren und die tatsächlichen Änderungen an Konfigurationsdateien direkt in den Zuordnungen für Service anzuzeigen. Informationen darüber, wie das System Konfigurationsdateien nachverfolgt und wie es Informationen zu diesen Dateien speichert und aktualisiert, finden Sie unter Konfigurationsdateien nachverfolgen.

Für CI-Typen mit Prozessklassifizierern, die Muster auslösen, verfolgt das System Konfigurationsdateien nach. Die Muster enthalten Definitionen für nachverfolgte Dateien. Dies beinhaltet den CI-Typ, zu dem die Anwendung gehört, und den Pfad der Konfigurationsdatei. Mehrere Muster, zum Beispiel das Muster „IIS“, stellen Definitionen für nachverfolgte Dateien standardmäßig bereit. Sie können diese Standarddefinitionen verwenden oder für jedes Muster, das von einem Prozessklassifizierer ausgelöst wird, eigene erstellen.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**.
2. Klicken Sie auf das Muster für das relevante CI.

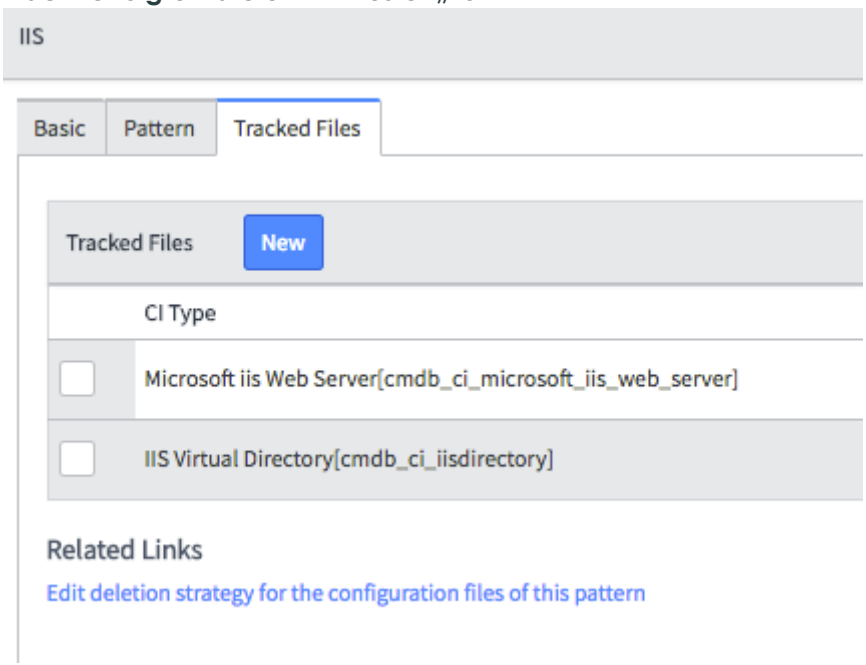
   Wichtig: Durch die Aktivierung der Nachverfolgung von Konfigurationsdateien wird der Inhalt eines Musters nicht geändert.

3. Klicken Sie auf die Registerkarte **Nachverfolgte Dateien**.
   Für Erkennungsmuster, die die Nachverfolgung von Konfigurationsdateien unterstützen, wird standardmäßig mindestens eine Definition für nachverfolgte Dateien angezeigt.

   Wenn die Registerkarte „Nachverfolgte Dateien“ nicht angezeigt wird, stellen Sie sicher, dass das Muster als Prozessklassifizierer angegeben ist. Anweisungen dazu finden Sie unter Probe „Horizontal Pattern“ einem Klassifizierer hinzufügen.

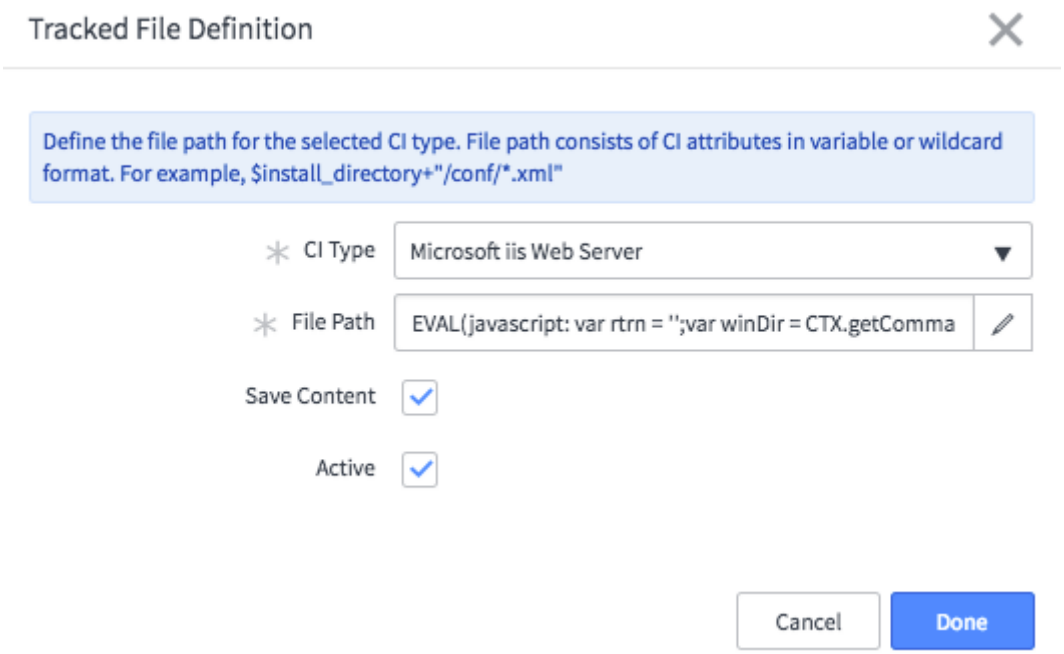
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachverfolgte Dateien im Muster „IIS“



4. Klicken Sie auf **Bearbeiten**, um eine vorhandene Definition hinzuzufügen, oder klicken Sie auf **Neu**, um eine neue zu erstellen.
5. Füllen Sie die Formularfelder aus, oder ändern Sie sie (siehe Tabelle):

Beispiel für eine Definition für nachverfolgte Dateien für die Erkennung von IIS-Servern



Feld	Beschreibung
CI-Typ	Wählen Sie entweder den primären oder den zugehörigen CI-Typ aus, zu dem die Konfigurationsdatei gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

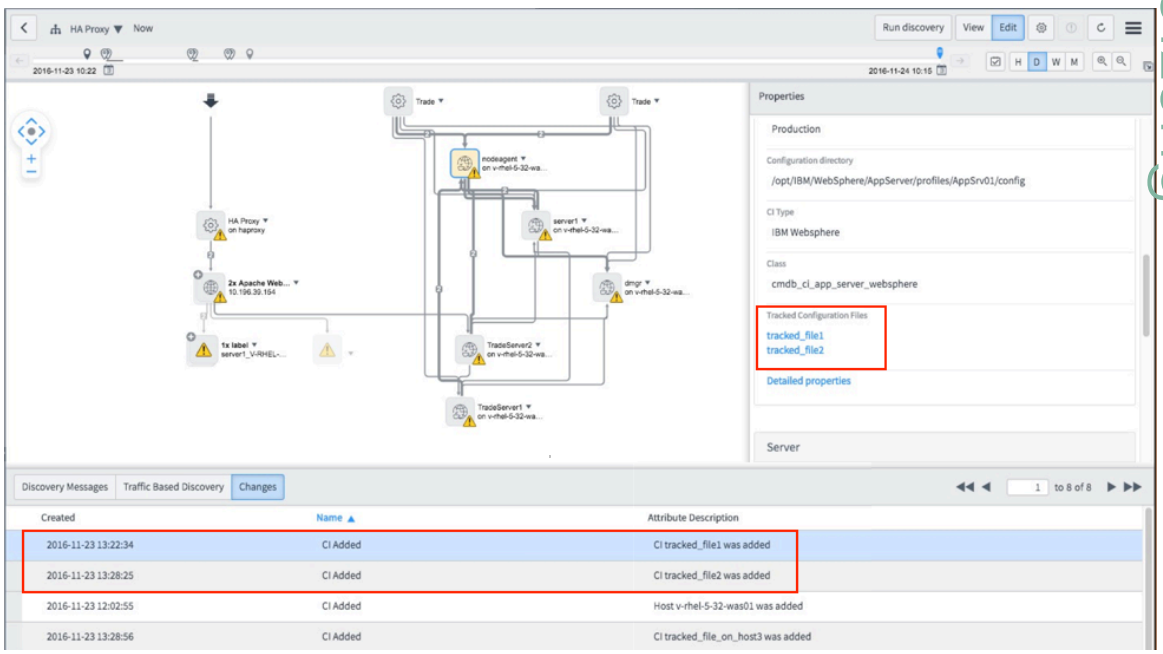
Feld	Beschreibung
Dateipfad	Definieren Sie den Pfad der zu überwachenden Konfigurationsdatei. Sie können Mustervariablen und Platzhalterzeichen verwenden. Zum Beispiel für den folgenden Pfad: <den Ordner mit dem Parameter "Installationsverzeichnis"> / conf / <beliebige XML-Datei>, geben Sie $ Installationsverzeichnis + "/ conf / *. Xml" ein.
Inhalt speichern	Aktivieren Sie dieses Kontrollkästchen, um diese Datei für die Anzeige und den direkten Vergleich mit der ServiceNow-Instanz verfügbar zu machen.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um die Nachverfolgung dieser Konfigurationsdatei zu aktivieren.

6. Klicken Sie auf **Erledigt**.
7. Legen Sie gegebenenfalls die Löschungsstrategie für nachverfolgte Dateien fest (siehe Beschreibung in Löschungsstrategie für nachverfolgte Konfigurationsdateien festlegen).

Nächste Maßnahme

Führen Sie eine Erkennung auf den Hosts aus, auf denen die Anwendungen ausgeführt werden, die Sie mit Mustern erkennen möchten, öffnen Sie den CI-Datensatz der Anwendung, und überprüfen Sie die zugehörige Liste „Nachverfolgte Konfigurationsdateien“. Wenn Sie Service-Mapping verwenden, vergewissern Sie sich, dass die Komponente begonnen hat, Informationen über Änderungen an Konfigurationsdateien zu erfassen:

1. Navigieren Sie zur Zuordnung des für Service, die die CIs enthält.
2. Vergewissern Sie sich, dass auf der Registerkarte „Changes“ die Liste einen Datensatz der von Ihnen vorgenommenen Änderungen enthält. Zum Beispiel, dass die Konfigurationsdatei hinzugefügt, geändert oder gelöscht wurde.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Versionen von CI-Konfigurationsdateien vergleichen

Sie können zwei Versionen von nachverfolgten CI-Konfigurationsdateien vergleichen, um die tatsächlich an ihnen durchgeführten Änderungen zu sehen.

Vorbereitungen

Erforderliche Rolle: Administrator

Wenn Discovery und Service-Mapping eine zu verfolgende Konfigurationsdatei nicht wie gewünscht nachverfolgen, führen Sie die erweiterte Konfiguration wie in Nachverfolgung von Changes in Konfigurationsdateien ändern beschrieben durch.

Warum und wann dieser Vorgang ausgeführt wird

Discovery und Service-Mapping überprüfen die Konfigurationsdateien während der horizontalen Erkennung mithilfe von Mustern auf Changes. Wenn eine Konfigurationsdatei geändert wird, speichert das System die Version der Datei. Sie können den Zeitstempel verwenden, um zwischen Versionen zu unterscheiden.

Änderungen an Konfigurationsdateien sind CIs zugeordnet, zu denen diese Dateien gehören. Karten zeigen Konfigurationsdateiänderungen als Änderungen an zugehörigen CIs an.

Prozedur

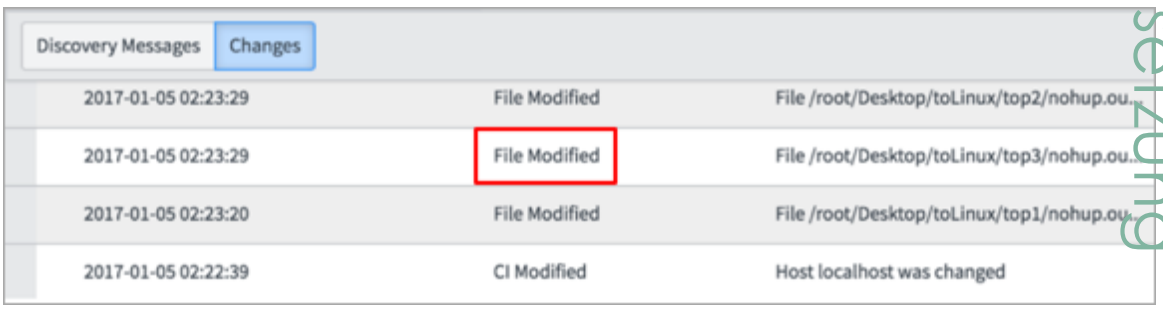
1. So vergleichen Sie die neueste und die vorherige Version der CI-Konfigurationsdatei aus Service-Mapping:

   a. Navigieren zu **Alle** > **Service-Mapping** > **Services** > **Business-Services**.

   b. Klicken Sie neben dem erforderlichen Business Service auf **Karte anzeigen**.

   c. Suchen Sie auf der Registerkarte **Changes** nach dem Change-Datensatz für die geänderte CI-Konfigurationsdatei.

   Wichtig: Der Name des Change muss **Datei geändert** lauten.

   d. Klicken Sie mit der rechten Maustaste auf den Change-Datensatz für die geänderte CI-Konfigurationsdatei, und wählen Sie **Change in nachverfolgten Dateiinhalten anzeigen** aus.
   Die Registerkarte „Vergleich nachverfolgter Konfigurationsdateien“ wird geöffnet und zeigt die neuesten und die vorherigen Versionen der Konfigurationsdatei an.

   e. Fahren Sie mit 3 fort.

2. So vergleichen Sie zwei beliebige Versionen der CI-Konfigurationsdatei aus der Liste der Versionen von Discovery aus:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Navigieren zu **Alle** > **Discovery** > **Nachverfolgte Konfigurationsdateien** und sortieren oder filtern Sie die Liste nach Kriterien wie **„Zugehöriges CI“** oder **„Host“**.
- Öffnen Sie im Konfigurationsmodul einen CI-Datensatz für den CI-Typ, zu dem die Konfigurationsdatei gehört. Um beispielsweise einen Tomcat-Server zu finden, navigieren Sie zu **Alle** > **Konfiguration** > **Anwendungsserver** > **Tomcat**, und wählen Sie dann den gewünschten Tomcat-Server aus. Die Liste der Konfigurationsdateien wird in der zugehörigen Liste der nachverfolgten Konfigurationsdateien angezeigt.

a. Wählen Sie eine Konfigurationsdatei aus der Liste aus.
Der Datensatz der nachverfolgten Konfigurationsdatei enthält folgende Angaben:

Feld	Beschreibung
Dateiname	Name und Dateipfad der Datei
Dateigröße	Dateigröße
Zuletzt geändert	Datum, an dem die Datei zuletzt geändert wurde
Dateiinhalt	Inhalt der Datei, wenn Sie die Option zum Speichern des Inhalts in der Dateiverfolgungsdefinition ausgewählt haben.

b. Klicken Sie in der zugehörigen Liste **Inhaltsversionen** auf eine der Versionen in der zugehörigen Liste **Aktualisierungszeit**.
Dieselben Informationen über die Konfigurationsdatei werden zusammen mit der Aktualisierungszeit angezeigt.

c. Klicken Sie auf **Vergleichen**.
Die Registerkarte „Vergleich nachverfolgter Konfigurationsdateien“ wird geöffnet und zeigt die Versionen der Konfigurationsdatei an, die Sie ausgewählt haben.

3. Überprüfen Sie die tatsächlichen Änderungen.

Hervorhebungsfarben geben die Art der Änderung an:

- Lila - Aktualisierte Linie
- Pink - Neue Linie
- Grau - Zeile gelöscht

4. Navigieren Sie mit den Pfeilen in der oberen rechten Ecke zwischen den Änderungen.

Löschungsstrategie für nachverfolgte Konfigurationsdateien festlegen

Sie können angeben, was Sie mit den CI-Datensätzen nachverfolgter Konfigurationsdateien tun möchten, wenn sie bei der Mustererkennung nicht mehr erkannt werden.

Vorbereitungen

- Erforderliche Rolle: discovery_admin, service_mapping_admin oder admin
- Ein Muster, das nachverfolgte Konfigurationsdateien angibt

Warum und wann dieser Vorgang ausgeführt wird

Sie können Löschungsstrategien für alle erkannten CIs festlegen, nicht nur Konfigurationsdatei-CIs. Für Standard-CIs greifen Sie jedoch auf eine andere Weise auf die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Löschungsstrategie zu als für Konfigurationsdatei-CIs. Siehe Löschungsstrategie festlegen für Anweisungen.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster** und öffnen Sie das gewünschte Muster.
2. Klicken Sie auf die Registerkarte **Nachverfolgte Dateien**.
3. Klicken Sie unter **Zugehörige Links** auf **Löschstrategie für die Konfigurationsdateien dieses Musters bearbeiten**.
   Die Liste „Zugehörige CI-Typen“ wird mit gefilterten Datensätzen in der Tabelle „Zugehöriger CI-Typ“ [sa_ci_to_pattern] angezeigt. Der Filter zeigt nur Datensätze mit dem CI-Typ „Nachverfolgte Konfigurationsdateien“ [cmdb_ci_config_file_tracked] an. Das ist die Tabelle, in der das System Konfigurationsdatei-CIs speichert.
4. Doppelklicken Sie in der Listenansicht auf den Wert im entsprechenden Feld in der Spalte **Löschungsstrategie** für die nachverfolgte Konfigurationsdatei.
5. Wählen Sie einen neuen Wert aus:

Wert	Beschreibung
Behalten	Behält den Konfigurationsdatei-CI-Datensatz bei und nimmt keine weiteren Änderungen am Datensatz vor. Diese Option ist die Standardeinstellung.
Löschen	Löscht den Konfigurationsdatei-CI-Datensatz aus der CMDB und die Beziehung zum Haupt-CI.
Als abwesend markieren	Markiert das Feld **Status** [install_status] des Konfigurationsdatei-CI-Datensatzes als **Abwesend** - dies bedeutet, dass Discovery die verfolgte Konfigurationsdatei nicht finden kann. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen. **Hinweis:** Es gibt zwei Tabellen, deren CIs gelöscht werden, wenn sie als abwesend markiert sind: „cmdb_ci_network_adapter“ und „cmdb_ci_ip_address“.
Beziehungen löschen	Löscht nur die CI-Beziehungen zwischen dem zugehörigen CI und dem Haupt-CI.
Als deaktiviert markieren	Markiert das Feld **Status** [install_status] des CI-Datensatzes der Konfigurationsdatei als **Deaktiviert**, was bedeutet, dass Discovery diese Konfigurationsdatei nicht mehr verwendet. Dieser Status weist das System nicht an, das tatsächliche CI oder die Beziehung zu löschen.

Zugehörige Informationen

CI-Löschstrategien für Mustererkennung

Löschungsstrategie festlegen

Quellennamen der Discovery-Ergebnisse ändern

Sie haben die Möglichkeit, den Quellennamen der Ergebnisse einer Erkennung zu ändern. Das kann hilfreich sein, wenn Discovery in Ihrem Netzwerk zusammen mit einem anderen Erkennungsprodukt ausgeführt wird und Sie benutzerdefinierte Bezeichner verwenden möchten.

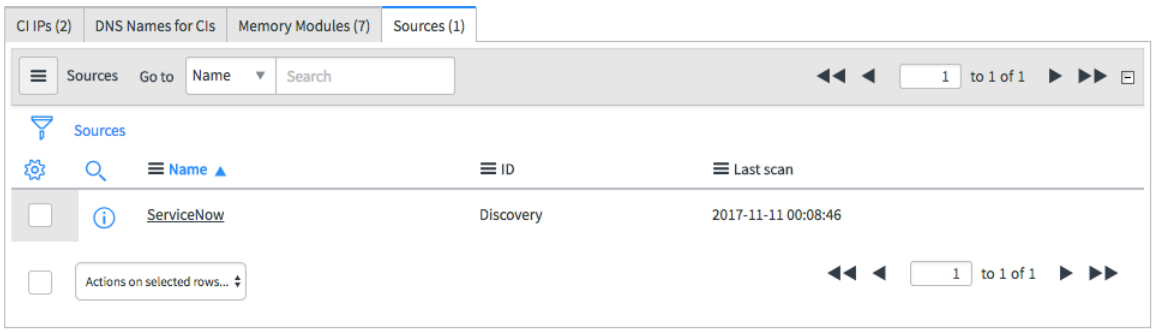
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
In der Tabelle „Quelle“ [sys_object_source] werden Informationen gespeichert, die die Quelle einer Erkennung, die ID dieser Quelle sowie Datum und Uhrzeit des letzten Scans identifizieren.

Um diese Informationen anzuzeigen, konfigurieren Sie ein CI-Formular, und fügen Sie die zugehörige Liste **Quellen** hinzu. Diese Tabelle wird automatisch gefüllt, wenn das Plugin Discovery aktiviert ist.

Quellenliste



So migrieren Sie Ihre Discovery-Quelle zu ServiceNow:

Prozedur
1. Aktualisieren Sie die Systemeigenschaft *glide.discovery.source_name* auf den Wert ServiceNow.
2. Bearbeiten Sie den Wörterbucheintrag für die Tabelle „Konfigurationselement“ [cmdb_ci].
3. Aktualisieren Sie die Auswahlliste für die Spalte *discovery_source*, sodass nur der Wert ServiceNow für ein Erkennungsprodukt vorhanden ist.
4. Öffnen Sie eine Liste für die Tabelle „Konfigurationselement“ [cmdb_ci], und filtern Sie sie nach einem Feldwert *Discovery-Quelle*, den Sie ändern möchten.
5. Verwenden Sie die Option *Alle aktualisieren*, um den Wert in ServiceNowzu ändern.
6. Öffnen Sie eine Liste für die Tabelle „Quelle“ [sys_object_source], und filtern Sie sie nach dem Feldwert des Namens, den Sie ändern möchten.
7. Verwenden Sie die Option *Alle aktualisieren*, um den Wert in ServiceNowzu ändern.

Plugin „Discovery API“

Das Plugin „Discovery API“ bietet APIs für bereichsbezogene Anwendungen und wird geladen, wenn das Plugin „Discovery“ aktiviert wird.

Details zu diesen Discovery API-Methoden finden Sie unter ServiceNow® Developer Site. Sie werden hier nach Klasse aufgelistet.

Hinweis: Java API-Methoden können nicht angepasst werden.

DiscoveryAPI - Scoped

Die Methoden in dieser Klasse starten eine Schnellerkennung einer einzelnen IPv4-Adresse und geben Zusammenfassungen zuvor gestarteter Discovery-Status für ein einzelnes CI oder für alle gescannten CIs zurück. Ein MID Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird basierend auf der angegebenen IP-Adresse oder der angegebenen Anwendung automatisch ausgewählt.

- *discoverIpAddress()*: Erkennt eine einzelne IPv4-Adresse
- *reportCiIpAddressStatus()*: Gibt eine Zusammenfassung des Discovery-Status eines Konfigurationselements anhand des spezifischen Status sys_id und der IPv4-Adresse zurück
- *reportCiStatus()*: Gibt eine Zusammenfassung eines CI-Discovery-Status anhand eines spezifischen Discovery-Status sys_id zurück

ReportCiStatusOutputJS

Die Methoden sind Getter, die bestimmte Objekteigenschaften für die DiscoveryAPI-Methode *reportCiIpAddressStatus* zurückgeben und die Informationen dann in eine JSON-Zeichenfolge konvertieren.

- *getCiOperationStatus()*: Wird verwendet, um den Status des gescannten CI zurückzugeben
- *getCmdbCI()*: Wird verwendet, um den Wert im Feld cmdb_ci aus der Tabelle discovery_device_history für das gescannte CI zurückzugeben
- *getDiscoveryState()*: Wird verwendet, um den Wert aus dem Feld **Status** in der Tabelle „Discovery-Status“ [discovery_status] zurückzugeben
- *getIpAddress()*: Wird verwendet, um den Wert aus dem Feld „Quelle“ in der Tabelle discovery_device_history für das gescannte CI zurückzugeben
- *getIssues()*: Wird verwendet, um den Wert aus dem Feld „Probleme“ in der Tabelle discovery_device_history für das gescannte CI zurückzugeben
- *getIssuesLink()*: Wird verwendet, um den Wert aus dem Feld issues_link in der Tabelle discovery_device_history für das gescannte CI zurückzugeben.
- *toJson()*: Wird verwendet, um das Objekt *ReportCiStatusOutputJS* zu serialisieren.

Filter für laufende Prozesse

Filtern Sie alle Prozesse mit Kombinationen aus Name und Schlüsselparametern, bevor Sie zur Instanz zurückkehren. Standardmäßig können Sie Betriebssystemprozesse filtern. Das Filtern von Prozessen hilft, die Anzahl der in der Datenbank erstellten, aktualisierten oder gelöschten Datensätze zu reduzieren, was die Gesamtleistung der Datenbank verbessern kann.

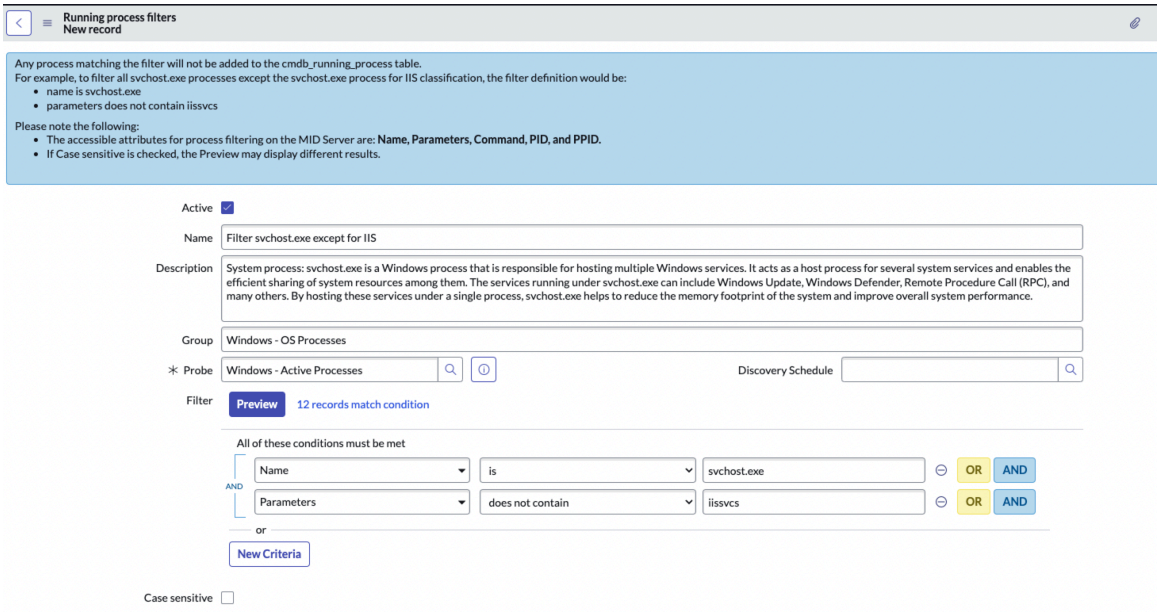
Vorbereitungen
Erforderliche Rolle: discovery_admin, admin

Warum und wann dieser Vorgang ausgeführt wird
Um dem Filter Prozesse hinzuzufügen, müssen Sie Konfigurationen mit dem Filterdatensatz „Laufender Prozess“ [running_process_filter] einrichten. Diese Datensätze stellen sicher, dass die Tabelle „Laufender Prozess“ [cmdb_running_process] nicht von gefilterten Prozessen gefüllt wird.

Prozedur

1. Navigieren Sie zu running_process_filter.list.
2. Klicken Sie auf **Neu**, um einen neuen Datensatz zu erstellen.
   Das Formular und seine Beschreibungen werden weiter unten erläutert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
Aktiv	Aktivieren Sie das Kontrollkästchen zum Ein- oder Ausschließen.
Name	Name für den Datensatz.
Beschreibung	Kurze Beschreibung des Datensatzes.
Gruppe	Ein Name für den Konfigurationstyp. Filter für laufende Prozesse können nach Belieben gruppiert werden, um die Identifizierung und Auswahl in der Tabelle zu erleichtern.
Probe	Pflichtfeld. Welche Probe diesen Filter verwendet. Häufig Linux oder Windows aktive Prozesse oder ADM erweitert. Wenn die Probe ausgeführt wird, sendet die Instanz die running_process_filter-Datensätze als Probe-Parameter. Das Probe verwendet dies dann, um die Ergebnisse zu filtern, bevor die Informationen an die Instanz zurückgesendet werden.
Discovery-Zeitplan	Sie können den Filter auf einen bestimmten Zeitplan Discovery anwenden. Wenn Sie dieses Feld verlassen, gilt es für alle Zeitpläne, auch für Schnell Discovery.
Filter	Prozesse, die dem Filter entsprechen, werden nicht der Tabelle „cmdb_running_process“ hinzugefügt. Wenn Sie beispielsweise alle svchost.exe-Prozesse mit Ausnahme des svchost.exe-Prozesses für die IIS-Klassifizierung filtern möchten, lautet die Filterdefinition:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Name ist svchost.exe ◦ Parameter enthält nicht iissvcs Informationen zum Festlegen von Filterbedingungen finden Sie unter: Bedingungsgenerator
Groß-/Kleinschreibung beachten	Gilt für das Feld Filter. Wenn „Groß-/Kleinschreibung beachten“ aktiviert ist, ruft der Filter möglicherweise mehr oder weniger Informationen ab, als Sie möchten. Standardmäßig ist deaktiviert.
OOB-Filter	Es stehen die Filter Linux und Windows zur Auswahl. Unter Sofort einsatzbereite Prozessfilter finden Sie weitere Details.

3. Geben Sie die Details ein, und klicken Sie auf **Senden**.

Sofort einsatzbereite Prozessfilter

Es gibt eine Vielzahl von sofort einsatzbereiten Prozessfiltern Linux und Windows, die aktiviert sind und zum Filtern von Prozessen verwendet werden.

Linux sofort einsatzbereite Filter

Name	Beschreibung
dhclient	dhclient ist ein Systemprozess in Linux, der für die dynamische Konfiguration von Netzwerkschnittstellen mithilfe des Dynamic Host Configuration Protocol (DHCP) verantwortlich ist. Er kommuniziert mit einem DHCP-Server, um Netzwerkkonfigurationsinformationen wie IP-Adresse, Subnetzmaske, Standard-Gateway und DNS-Server zu erhalten. dhclient wird häufig in Umgebungen verwendet, in denen Netzwerkadressen dynamisch zugewiesen werden, z. B. in Heimnetzwerken und Netzwerken kleiner Unternehmen.
Crond	Crond ist ein Systemservice in Linux, der das Planungsdienstprogramm cron unterstützt. Es ist für die Ausführung geplanter Aufgaben zu bestimmten Zeiten und Intervallen verantwortlich. Crond wird häufig zur Automatisierung von Systemwartungsaufgaben wie Sicherungen und Protokollrotation sowie zum Ausführen anwenderdefinierter Skripts und Anwendungen zu bestimmten Zeiten verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
Schlaf	Der Ruheprozess ist ein Befehl, mit dem die Ausführung eines Shell-Skripts oder Befehls für eine bestimmte Zeit angehalten wird. Dies ist eine einfache Möglichkeit, die Ausführung eines Skripts oder Befehls um eine bestimmte Dauer zu verzögern.
agentty	agentty ist ein Systemservice in Linux, der Anmeldesitzungen für die virtuelle Konsole verwaltet. Er stellt eine Terminalschnittstelle bereit, über die sich Benutzer beim System anmelden und auf die Befehlszeilenschnittstelle zugreifen können. agentty ist für die Initialisierung des Terminals, das Anzeigen der Anmeldeaufforderung und die Authentifizierung der Anmeldeinformationen des Benutzers verantwortlich.
dbus-daemon	dbus-daemon ist ein Systemservice in Linux, der das D-Bus-Nachrichtenbussystem implementiert. Ermöglicht die Kommunikation zwischen Anwendungen und Systemservices auf demselben Host oder in einem Netzwerk. „dbus-daemon“ verwaltet den Nachrichtenbus und sendet Nachrichten zwischen Anwendungen und Services, sodass diese Daten austauschen und voneinander Services anfordern können.
rsyslogd	rsyslogd ist ein Systemservice in Linux, der Systemprotokolle verwaltet und zentralisierte Protokollierungsfunktionen bereitstellt. Es handelt sich um ein leistungsstarkes und flexibles Protokollierungssystem, mit dem Administratoren Protokollnachrichten konfigurieren und verwalten können, die von verschiedenen Anwendungen und Services in einem System oder in einem Netzwerk generiert werden. rsyslogd bietet erweiterte Funktionen wie Protokollfilterung, Protokollweiterleitung und Protokollrotation und unterstützt verschiedene Ausgabeformate und -ziele, einschließlich Dateien, Datenbanken und Remote-Syslog-Server. rsyslogd wird häufig in Serverumgebungen verwendet und kann mithilfe einer Konfigurationsdatei oder einer grafischen Benutzeroberfläche konfiguriert werden.
geprüft	auditd ist ein Systemservice in Linux, der ein Audit-Framework für die Nachverfolgung sicherheitsrelevanter Ereignisse im System

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	bereitstellt. Er sammelt und protokolliert vom Kernel und den Userspace-Anwendungen generierte Sicherheitsereignisse, die für forensische Analysen, Compliance-Überwachung und Angriffserkennung verwendet werden können. auditd kann so konfiguriert werden, dass basierend auf vordefinierten Regeln oder Richtlinien Warnungen generiert oder andere Aktionen ausgeführt werden.
irqbalance	irqbalance ist ein Systemservice in Linux, der Unterbrechungsanforderungen (IRQs) auf die Prozessoren in einem Multicore-System verteilt, um die Leistung zu verbessern und die Latenz zu reduzieren. Es erkennt und überwacht die IRQ-Aktivität und verteilt IRQs an den am wenigsten ausgelasteten Prozessor. Dadurch werden Verarbeitungsengpässe reduziert und die Reaktionsfähigkeit des Systems verbessert. irqbalance wird häufig in leistungsstarken Computing-Umgebungen und anderen Systemen mit hoher Interrupt-Aktivität verwendet.
systemd-journal	systemd-journal ist ein Systemservice in Linux, der ein zentralisiertes Protokollierungssystem für System- und Anwendungsprotokolle bereitstellt. Es wurde entwickelt, um Protokolldaten auf strukturierte und effiziente Weise zu sammeln und zu speichern, und ermöglicht das erweiterte Abfragen und Filtern von Protokolldaten. systemd-journal bietet eine einheitliche Schnittstelle für den Zugriff auf und die Verwaltung von Protokollen in verschiedenen Linux -Verteilungen und kann mithilfe einer Konfigurationsdatei oder einer Befehlszeilenschnittstelle konfiguriert werden. Es wird häufig in Server- und Desktopumgebungen verwendet, um System- und Anwendungsprobleme zu überwachen und zu beheben.
abrtd	abrtd ist ein Systemprozess, der auf Systemen Linux von ausgeführt wird und dafür verantwortlich ist, Anwendungsabstürze zu erkennen und dem Systemadministrator zu melden. Der Prozess sammelt Informationen über die abgestürzte Anwendung, z. B. Core-Dumps, und speichert sie in einem Bericht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
atd	atd ist ein Systemservice in Linux, der die Planung einmaliger Aufgaben ermöglicht, die zu einem bestimmten Zeitpunkt und Datum ausgeführt werden sollen. Dies ist nützlich für die Ausführung von Aufgaben, die zu einem bestimmten Zeitpunkt ausgeführt werden müssen, oder für die Automatisierung von Aufgaben, die einmal in der Zukunft ausgeführt werden müssen.
lvmeta	lvmetad ist ein Systemservice in Linux, der Metadaten-Caching für Logical Volume Management (LVM) bereitstellt. Metadateninformationen zu LVM-Volumes und -Geräten werden zwischengespeichert, was die Leistung von LVM-Vorgängen verbessern und die Zeit zum Scannen und Initialisieren von LVM-Geräten reduzieren kann. lvmetad wird häufig in Systemen verwendet, die stark von LVM abhängig sind, z. B. Virtualisierungsumgebungen und Speicherserver.
polkitd	polkitd ist ein Systemservice in Linux, der ein Autorisierungs-Framework für die Steuerung des Zugriffs auf privilegierte Aktionen und Ressourcen bereitstellt. Sie ermöglicht nicht privilegierten Benutzern das Ausführen bestimmter Aufgaben oder den Zugriff auf bestimmte Ressourcen, die erweiterte Berechtigungen erfordern, z. B. das Installieren von Software oder das Konfigurieren von Netzwerkeinstellungen, indem sie sie dazu auffordert, sich mit ihrem Passwort oder auf andere Weise zu authentifizieren. polkitd bietet eine Richtlinien-Engine, die von Administratoren konfiguriert werden kann, um differenzierte Zugriffssteuerungen für bestimmte Benutzer, Gruppen oder Anwendungen zu definieren.
ACID	accid ist ein Systemservice in Linux, der auf ACPI-Ereignisse (Advanced Configuration and Power Interface) lauscht, die von der Hardware generiert werden, und das Betriebssystem benachrichtigt. Es ist verantwortlich für die Verwaltung von Leistungsereignissen, z. B. das Drücken von Netzschaltern, und das Ausführen anwenderdefinierter Aktionen als Reaktion darauf.
Anacron	anacron ist ein Systemservice in Linux, der die Planung von regelmäßigen Aufgaben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	ermöglicht, ähnlich wie Cron, jedoch mit der zusätzlichen Möglichkeit, sicherzustellen, dass verpasste Aufgaben ausgeführt werden, wenn das System das nächste Mal verfügbar wird. Dies ist nützlich für die Ausführung regelmäßiger Aufgaben, die aufgrund von Systemausfällen oder Inaktivität des Benutzers verzögert werden können.
(sd-pam)	sd-pam ist ein Systemservice in Linux, der Unterstützung für das PAM-Framework (Pluggable Authentication Modules) bietet. Er ist für die Verarbeitung von Anforderungen zur Anwenderauthentifizierung und -autorisierung von verschiedenen Systemservices und -anwendungen verantwortlich.
NetworkManager	NetworkManager ist ein Systemservice in Linux, der die Netzwerkkonnektivität für Desktops, Laptops und andere Geräte verwaltet. Es bietet eine einheitliche Schnittstelle zum Konfigurieren und Verwalten von kabelgebundenen, drahtlosen, mobilen Breitband- und anderen Netzwerkverbindungen und verwaltet die IP-Adressierung, die DNS-Konfiguration und andere Netzwerkeinstellungen. NetworkManager wird häufig in Desktopumgebungen und grafischen Benutzeroberflächen verwendet und kann über eine grafische Benutzeroberfläche oder eine Befehlszeilenschnittstelle konfiguriert werden.
hcid	hcid ist ein Systemservice in Linux, der Unterstützung für Bluetooth-Konnektivität bietet. Er ist für die Verwaltung von Bluetooth-Geräten, -Verbindungen und -Services im System verantwortlich. hcid bietet eine Schnittstelle für Anwendungen und Systemservices zur Interaktion mit Bluetooth-Geräten und wird zum Konfigurieren und Verwalten von Bluetooth-Einstellungen verwendet, z. B. Gerätekoppelung, Authentifizierung und Autorisierung.
ausgeblendet	hidd ist ein Systemprozess in Linux, der Unterstützung für Bluetooth Human Interface Devices (HID) wie Tastaturen und Computermäuse bietet. Er ist für die Verwaltung von Bluetooth-Verbindungen und die Bereitstellung einer gemeinsamen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	Schnittstelle für die Kommunikation zwischen HID-Geräten und dem System verantwortlich. hidd wird häufig in Desktop-Umgebungen verwendet, um die Verwendung drahtloser Eingabegeräte mit dem System zu ermöglichen.
iscsid	iscsid ist ein Systemprozess in Linux, der Unterstützung für das iSCSI-Protokoll bietet, das für den Zugriff auf Speichergeräte über ein Netzwerk verwendet wird. Er ist für die Erkennung von iSCSI-Zielen, das Einrichten und Verwalten von iSCSI-Sitzungen und den Zugriff auf iSCSI-Geräte so geeignet, als wären sie lokal verbundene Speicher. iscsid wird häufig in Virtualisierungsumgebungen und anderen Systemen verwendet, die Remotezugriff auf Speicherressourcen erfordern.
klogd	klogd ist ein Systemprozess in Linux, der für die Protokollierung von Kernel-Nachrichten im Systemprotokoll verantwortlich ist. Überwacht den Protokollpuffer des Kernels auf neue Nachrichten und schreibt sie in die Systemprotokolldatei oder sendet sie an einen Remote-Protokollierungsserver. klogd wird häufig zur Behebung von Kernelproblemen und zur Überwachung der Systemaktivität sowie zum Sammeln von Diagnoseinformationen für Systemadministratoren und -entwickler verwendet.
mingetty tty1	mingetty tty ist ein Systemprozess in Linux, der eine Terminal-Anmeldeaufforderung für eine virtuelle Konsole bereitstellt. Er ist für die Initialisierung des Terminalgeräts, das Anzeigen der Anmeldeaufforderung und das Akzeptieren der Anmeldeinformationen für die Anwender verantwortlich. mingetty tty wird für jede virtuelle Konsole in einem Linux -System verwendet und kann für Systemadministrations- und Debugging-Aufgaben sowie zum Ausführen von konsolenbasierten Anwendungen verwendet werden.
ModemManager	ModemManager ist ein Systemservice in Linux, der mobiles Breitband (GSM/CDMA/UMTS/LTE) und andere Modemverbindungen verwaltet. Es bietet eine einheitliche Schnittstelle zum Konfigurieren und Verwalten von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	Modemgeräten, zum Herstellen von Verbindungen mit dem Internet oder anderen Netzwerken und zum Überwachen der Modemaktivität. ModemManager wird häufig auf Laptops, Tablets und anderen Mobilgeräten verwendet, die eine drahtlose Netzwerkverbindung erfordern.
pcscd	pcscd ist ein Systemservice in Linux, der Unterstützung für Smartcard-Lesegeräte und Smartcards bietet. Anwendungen können über den Schnittstellenstandard PC/SC (Personal Computer/Smart Card) auf Smart Cards und deren Inhalt zugreifen. pcscd bietet eine einheitliche Schnittstelle für den Zugriff auf verschiedene Arten von Smartcard-Lesegeräten. Sie kann von Anwendungen wie Webbrowsern, E-Mail-Clients und Authentifizierungssystemen verwendet werden, die Smartcard-Unterstützung erfordern.
macht-profiles-daemon	„power-profiles-daemon“ ist ein Systemservice in Linux, der Leistungsprofile und Energieverwaltungseinstellungen für Laptops und andere Mobilgeräte verwaltet. Sie bietet eine einheitliche Schnittstelle zum Konfigurieren und Verwalten von Energiesparfunktionen wie Bildschirmhelligkeit, CPU-Frequenzskalierung und Anhalt-Modi, basierend auf Anwendereinstellungen und Systemnutzungsmustern. „power-profiles-daemon“ wird häufig in Desktopumgebungen und grafischen Anwenderoberflächen verwendet und kann über eine grafische Anwenderoberfläche oder eine Befehlszeilenschnittstelle konfiguriert werden.
Pulsaudio	Pulseaudio ist ein Systemservice in Linux, der Audiogeräte, Streams und Anwendungen verwaltet. Er bietet eine einheitliche Audioschnittstelle für Eingabe- und Ausgabeaudiostreams und unterstützt erweiterte Funktionen wie Lautstärkeregelung, Mischung und Audioeffekte. Pulseaudio wird häufig in Desktop-Umgebungen und grafischen Anwenderoberflächen verwendet und kann über eine grafische Anwenderoberfläche oder eine Befehlszeilenschnittstelle konfiguriert werden. Er unterstützt eine Vielzahl von Audiohardware- und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	-softwarekonfigurationen, einschließlich mehrerer Audiogeräte und Netzwerk-Audiostreaming.
chronyd	chronyd ist ein Systemservice in Linux, der für die Synchronisierung der Systemuhr mit einer Referenzzeitquelle verantwortlich ist. Es implementiert das Network Time Protocol (NTP) und kann zur Synchronisierung der Systemuhr mit einer Vielzahl von Zeitquellen verwendet werden, einschließlich GPS-Uhren und Atomuhren. chronyd wird häufig in Umgebungen verwendet, in denen eine genaue Zeitsynchronisierung wichtig ist, z. B. beim Finanzhandel oder in der wissenschaftlichen Forschung.
rtkit-daemon	rtkit-daemon ist ein Systemservice in Linux, der Echtzeitplanung und Prioritätsverwaltung für Audioanwendungen und andere zeitkritische Anwendungen bietet. Es soll sicherstellen, dass diese Anwendungen Zugriff auf die CPU und andere Systemressourcen erhalten, die sie benötigen, um ordnungsgemäß zu funktionieren und Audiostörungen, Latenz oder andere Leistungsprobleme zu vermeiden. rtkit-daemon nutzt die Echtzeitfähigkeiten Linux und bietet eine einfache Schnittstelle für Anwendungen, um Echtzeitplanung und -priorität anzufordern. Es wird häufig in Desktop-Umgebungen und Audioanwendungen verwendet und kann mithilfe einer Konfigurationsdatei oder einer grafischen Benutzeroberfläche konfiguriert werden.
sssd	sssd ist ein Systemservice in Linux, der eine zentralisierte Authentifizierung, Identitäts- und Zugriffsverwaltung für eine Vielzahl von Services und Anwendungen bietet. Es wurde entwickelt, um die Verwaltung von Benutzeraccounts und Anmeldeinformationen in großen Umgebungen mit mehreren Domänen zu vereinfachen, und bietet eine einheitliche Schnittstelle für Authentifizierung, Autorisierung und Identitätsauflösung. sssd unterstützt eine Vielzahl von Identitätsquellen, einschließlich lokaler Dateien, LDAP-Verzeichnisse und Active Directory-Domänen, und bietet erweiterte Funktionen wie Offline-Authentifizierung, Caching und Failover. Wird häufig in

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	Unternehmensumgebungen verwendet und kann mithilfe einer Konfigurationsdatei oder einer grafischen Benutzeroberfläche konfiguriert werden.
sssd_kcm	sssd_kcm ist ein Systemservice in Linux, der einen Kerberos-Anmeldeinformations-Cache-Manager für den System Security Services Daemon (SSSD) bereitstellt. Es wurde entwickelt, um die Sicherheit und Leistung der Kerberos-basierten Authentifizierung und Autorisierung zu verbessern, indem Kerberos-Anmeldeinformationen und -Tickets lokal zwischengespeichert und eine einheitliche Schnittstelle für den Zugriff bereitgestellt werden. sssd_kcm wird häufig in Unternehmensumgebungen verwendet, die für die zentrale Authentifizierung und Zugriffssteuerung auf Kerberos angewiesen sind, und kann mithilfe einer Konfigurationsdatei oder einer grafischen Benutzeroberfläche konfiguriert werden.
systemd-hostnamed	systemd-hostnamed ist ein Systemservice in Linux, der die Konfiguration des Hostnamens und der DNS-Auflösung bereitstellt. Es soll die Konfiguration von netzwerkbezogenen Einstellungen wie Hostname, Domänenname und DNS-Server vereinfachen. systemd-hostnamed bietet eine einheitliche Schnittstelle zum Konfigurieren dieser Einstellungen für verschiedene Linux -Verteilungen und kann mithilfe einer Konfigurationsdatei oder einer Befehlszeilenschnittstelle konfiguriert werden. Es wird häufig in Server- und Desktopumgebungen verwendet, um Netzwerkeinstellungen während des Systemstarts oder zur Laufzeit zu konfigurieren.
systemd-timesyncd	systemd-timesyncd ist ein Systemservice in Linux, der die Zeitsynchronisierung für die Systemuhr bereitstellt. Es synchronisiert die Systemuhr über das Netzwerk mit einem Remote-Zeitserver und kann so konfiguriert werden, dass aus Redundanzgründen mehrere Zeitquellen verwendet werden. systemd-timesyncd wird häufig in Server- und Desktopumgebungen verwendet, um eine genaue Zeitmessung für verschiedene System- und Anwendungsfunktionen sicherzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
hald	hald ist ein Systemservice in Linux, der für das Erkennen und Verarbeiten von Hardware-Ereignissen verantwortlich ist, z. B. das Einfügen und Entfernen von Speichergeräten und anderen Hardwarekomponenten. Es bietet eine gemeinsame Schnittstelle für Anwendungen und Systemservices für die Interaktion mit der Hardware und wird zum Konfigurieren und Verwalten von Systemressourcen verwendet, z. B. Eingabegeräte und Speichervolumes. hald wird häufig in Desktopumgebungen verwendet, um Plug-and-Play-Funktionen für Hardwaregeräte bereitzustellen.
xfs	xfs ist ein leistungsstarkes Journaling-Dateisystem für Linux, das für Skalierbarkeit und große Dateien optimiert ist. Sie wurde ursprünglich von Silicon Grafiken, Inc. für die Verwendung in deren IRIX-Betriebssystem entwickelt und später auf Linuxportiert. xfs unterstützt Funktionen wie Snapshots, Online-Größenänderung und erweiterte Dateiberechtigungen. Er wird häufig in den Bereichen High Performance Computing, Medien und Unterhaltung sowie in anderen Branchen verwendet, in denen der Umgang mit großen Dateien und Datensätzen von entscheidender Bedeutung ist.
audispd	audispd ist ein Systemservice in Linux, der für die Verarbeitung von Audit-Ereignissen verantwortlich ist, die vom Auditing-Subsystem des Kernels generiert werden. Es ist Teil des Audit-Frameworks und wird verwendet, um die sichere Protokollierung von Systemereignissen zu Audit- und forensischen Zwecken bereitzustellen. audispd kann so konfiguriert werden, dass Audit-Ereignisse an verschiedene Ziele gesendet werden, z. B. an Syslog oder einen zentralen Protokollserver.
automount	automount ist ein Systemservice in Linux, der das automatische Bereitstellen von Dateisystemen bereitstellt, wenn Benutzer oder Anwendungen auf sie zugreifen. Sie ermöglicht das Bereitstellen von Dateisystemen bei Bedarf und reduziert so den Zeitaufwand und den Aufwand für unnötige Dateisystemressourcen. Automount ist besonders in Umgebungen mit einer großen Anzahl von Netzwerkdateisystemen oder Wechselspeichergeräten nützlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
avahi-daemon: chroot-Helfer	avahi-daemon ist ein Systemservice in Linux, der das Zeroconf-Protokoll für die Service-Discovery in lokalen Netzwerken implementiert. Die Chroot-Hilfe ist eine Komponente von avahi-daemon. Sie ist für die Einrichtung einer chroot-Umgebung für den Service verantwortlich. Dies erhöht die Sicherheit, indem der Zugriff von avahi-daemon auf das System eingeschränkt wird.

Windows sofort einsatzbereite Filter

Name	Beschreibung
Systemleerer Prozess	Im Betriebssystem Windows ist „System-Leerlaufprozess“ nicht wirklich ein Prozess, sondern eine System-Leerlaufaufgabe, die ausgeführt wird, wenn die CPU nichts anderes zu tun hat. Er stellt den Prozentsatz der Zeit dar, in der sich die CPU im Leerlauf befindet und für andere Prozesse verfügbar ist. Daher ist es eine wichtige Systemkomponente, die die aktuelle CPU-Auslastung anzeigt, wenn keine anderen Prozesse ausgeführt werden.
svchost.exe	„svchost.exe“ ist ein Windows -Prozess, der für das Hosten mehrerer Windows -Services verantwortlich ist. Es fungiert als Hostprozess für mehrere Systemservices und ermöglicht die effiziente gemeinsame Nutzung von Systemressourcen. Die unter „svchost.exe“ ausgeführten Services können Windows Update, Windows Defender, Remote Procedure Call (RPC) und viele andere sein. Durch das Hosten dieser Services in einem einzigen Prozess trägt svchost.exe dazu bei, den Speicherbedarf des Systems zu reduzieren und die allgemeine Systemleistung zu verbessern.
wmiprvse.exe	wmiPrvSE.exe ist ein Windows -Systemprozess, der Verwaltungsinformationen und -steuerung über das Windows Management Instrumentation (WMI)-Framework bereitstellt. Es wird als Service im Hintergrund ausgeführt und ermöglicht Anwendungen und Skripts den Zugriff auf Systemverwaltungsinformationen, die Ausführung von Verwaltungsaufgaben und die Überwachung der Systemleistung. „WmiPrvSE.exe“ kann sowohl im lokalen als auch im Remotemodus ausgeführt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	werden und zur Verwaltung einer Vielzahl von Systemressourcen verwendet werden, einschließlich Hardware, Software und Netzwerkkomponenten. Es ist eine wichtige Komponente des Betriebssystems Windows und wird in der Regel von Systemadministratoren und IT-Experten verwendet.
conhost.exe	„conhost.exe“ ist ein Prozess Windows, der als Host für Konsolenanwendungen dient. Es wurde in Windows 7 eingeführt und ist für die Verwaltung der Eingabeaufforderungsfenster und anderer konsolenbasierter Anwendungen verantwortlich. conhost.exe bietet verbesserte Kompatibilitäts- und Sicherheitsfunktionen im Vergleich zu seinem Vorgänger, dem csrss.exe-Prozess, der in älteren Versionen von Windowsfür den gleichen Zweck verwendet wurde.
WUDFHost.exe	WUDFHost.exe ist ein Windows User-Mode-Treiber-Framework(UMDF)-Hostprozess, der Benutzermodus-Treiber verwaltet, die im Kontext von Windows Driver Foundation (WDF) ausgeführt werden. Es bietet ein Framework für die Entwicklung und Ausführung von Treibern im Benutzermodus anstelle des Kernelmodus und verbessert die Stabilität und Zuverlässigkeit des Systems. WUDFHost.exe wird für Plug-and-Play-Geräte und andere treiberbasierte Hardwarekomponenten verwendet. Er wird im Hintergrund ausgeführt und verbraucht normalerweise wenige Systemressourcen.
LogonUI.exe	LogonUI.exe ist ein Windows -Systemprozess, der den Anmeldebildschirm für Windows und die Anwenderauthentifizierung verwaltet. Wenn ein Benutzer versucht, sich bei einem Computer Windows anzumelden, zeigt LogonUI.exe den Anmeldebildschirm an und fordert den Benutzer auf, die Anmeldeinformationen einzugeben. Sobald die Anmeldeinformationen des Benutzers eingegeben wurden, überprüft LogonUI.exe sie und gewährt dem Benutzer Zugriff auf das System. LogonUI.exe ist eine wesentliche Komponente des Betriebssystems Windows und darf nicht beendet oder deaktiviert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
csrss.exe	Der Prozess csrss.exe ist eine wichtige Komponente des Betriebssystems Windows. Sie ist für die Verarbeitung bestimmter Funktionen im Zusammenhang mit der grafischen Benutzeroberfläche (GUI) verantwortlich, z. B. für die Verwaltung von Fenstern und Konsolen. Um die Stabilität und Sicherheit des Betriebssystems zu gewährleisten, wird der Prozess in einer separaten Sitzung von der Sitzung des Benutzers ausgeführt. Es handelt sich um einen wichtigen Systemprozess, der nur dann beendet werden sollte, wenn ein bestimmter und gültiger Grund vorliegt.
dllhost.exe	dllhost.exe ist ein Windows -Systemprozess, der für die Ausführung und Verwaltung von Komponenten des Komponentenobjektmodells (COM, Component Object Model) verantwortlich ist. com-Komponenten sind wiederverwendbare Softwaremodule, auf die andere Programme zugreifen können. Sie werden häufig verwendet, um die prozessübergreifende Kommunikation zwischen verschiedenen Anwendungen zu erleichtern. Der Prozess „dllhost.exe“ hostet diese com-Komponenten und stellt deren ordnungsgemäße Ausführung und Verwaltung sicher. Es wird häufig von einer Vielzahl von Windows -Anwendungen und -Services verwendet.
Fontdrvhost.exe	Fontdrvhost.exe ist ein Windows -Systemprozess, der die Installation, Entfernung und Aufzählung von Schriftartendateien verwaltet. Sie ist für das Laden und Rendern von Schriftarten in Anwendungen verantwortlich, die den Schriftart-Cache-Service Windows verwenden. „Fontdrvhost.exe“ wird im Hintergrund ausgeführt und hat keine sichtbare Schnittstelle. Dies ist wichtig für die Verwaltung der Schriftartenbibliothek des Systems und dafür, dass Anwendungen bei Bedarf Schriftarten zur Verfügung stehen.
wlanext.exe	wlanext.exe ist ein Windows -Systemprozess, der Unterstützung für WLAN-Konfigurationen und -Vorgänge bietet. Er ist für die Verwaltung der Adapter für drahtlose Netzwerke und die Implementierung der Funktionalität des automatischen WLAN-Konfigurationsservice verantwortlich, der die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	automatische Konfiguration von drahtlosen Netzwerken ermöglicht und das WPS-Protokoll (Wi-FiProtected Setup) unterstützt. Der Prozess wird im Hintergrund ausgeführt und kann über die Serviceskonsole oder die Eingabeaufforderung verwaltet werden.
winlogon.exe	„winlogon.exe“ ist ein Systemprozess in Windows, der die An- und Abmeldung von Benutzersitzungen verwaltet. Er ist für die Authentifizierung von Anwendern und das Laden ihres Anwenderprofils bei der Anmeldung sowie für das Schließen geöffneter Anwendungen und das Speichern von Anwenderdaten verantwortlich, wenn sich ein Anwender abmeldet oder das System heruntergefahren wird. „Winlogon.exe“ wird als Dienst im Hintergrund ausgeführt und ist für das ordnungsgemäße Funktionieren des Betriebssystems Windows von entscheidender Bedeutung.
unsecapp.exe	unsecapp.exe ist ein Windows -Systemprozess, der mit dem Distributed Component Object Model (DCOM) zusammenhängt. Es wird im Hintergrund ausgeführt und fungiert als Vermittler zwischen einer Client- und einer Serveranwendung, die über DCOM kommunizieren. Wenn ein Client eine Anforderung über DCOM an einen Server sendet, ist „unsecapp.exe“ dafür verantwortlich, die Sicherheitsaspekte der Kommunikation zu behandeln und sicherzustellen, dass die Anforderung autorisiert wird. Es handelt sich um einen rechtmäßigen Systemprozess, der sich normalerweise im Ordner „C:\Windows \System32“ befindet.
w3wp.exe	„w3wp.exe“ ist ein Prozess Windows vom Typ , der für den Prozess Windows „ Prozessaktivierung – Service-Worker-Prozess“ steht. Sie wird vom Webserver von Internet Information Services (IIS) zum Hosten und Verwalten von ASP.NET-Webanwendungen verwendet. w3wp.exe ermöglicht die gleichzeitige Ausführung mehrerer Webanwendungen auf demselben Server und bietet für jede Anwendung eine sichere, isolierte Umgebung. Es handelt sich um eine kritische Komponente des IIS-Servers, die häufig genau überwacht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	wird, um die Stabilität und Leistung von Webanwendungen sicherzustellen.
dwm.exe	„dwm.exe“ ist ein Windows -Systemprozess, der für Desktop Windows Manager steht. Sie ist für die Verwaltung von grafischen Effekten im Betriebssystem Windows verantwortlich, z. B. transparente Fenster und Fensteranimationen. Der Prozess ist auch für das Rendern des Desktops, das Verwalten von Fenstern und das Bereitstellen von visuellen Effekten wie z. B. Azure Glass verantwortlich. Es wurde mit Windows Vista eingeführt und ist seitdem in allen nachfolgenden Versionen von Windowsenthalten.
lsass.exe	„lsass.exe“ ist ein kritischer Systemprozess in Windows, der Authentifizierungs- und sicherheitsbezogene Funktionen wie lokale und Remote-Anmeldung, Passwortänderungen und die Durchsetzung von Sicherheitsrichtlinien verarbeitet. Es handelt sich um eine Kernkomponente des Betriebssystems Windows und wird für das ordnungsgemäße Funktionieren des Systems benötigt.
System	System ist kein Windows -Prozess im herkömmlichen Sinne. Stattdessen bezieht er sich auf eine Sammlung von Prozessen und Services, die für das Funktionieren des Betriebssystems von entscheidender Bedeutung sind. Diese Prozesse und Services sind für die Verwaltung von Hardwareressourcen, die Verarbeitung von Systemereignissen und die Bereitstellung wichtiger Funktionen wie Speicherverwaltung, Prozessplanung und Sicherheit verantwortlich. Mit anderen Worten: System ist der Kern des Betriebssystems Windows.
smss.exe	smss.exe (Session Manager Subsystem) ist ein kritischer Systemprozess in Windows, der für das Starten von Benutzermodusanwendungen während des Systemstarts verantwortlich ist. Außerdem erstellt es System-Threads, initialisiert systemweite Datenstrukturen und verarbeitet Anforderungen zum Herunterfahren und Neustarten des Systems. Dies ist einer der ersten Prozesse, die während des Startvorgangs Windows gestartet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
services.exe	„services.exe“ ist ein Systemprozess in Windows, der für die Verwaltung von Systemservices verantwortlich ist, einschließlich des Startens und Stoppens von Services und der Steuerung der Konfigurationseinstellungen. Es wird im Hintergrund ausgeführt und bietet wichtige Funktionen für das Betriebssystem.
wininit.exe	„wininit.exe“ ist ein Systemprozess in Windows, der während des Startvorgangs des Betriebssystems ausgeführt wird. Die Hauptfunktion besteht darin, kritische Systemservices und -prozesse zu initialisieren, die für den ordnungsgemäßen Betrieb des Systems erforderlich sind. Er ist für die Ausführung der Startsequenz Windows verantwortlich, einschließlich des Starts des Sitzungsmanager-Prozesses (smss.exe).
spoolsv.exe	spoolsv.exe ist ein Systemserviceprozess in Windows, der den Druckprozess verwaltet. Es ist für das Einreihen und Spoolen von Druckaufträgen in die Warteschlange, für die Kommunikation mit dem Drucker und dafür verantwortlich, dass jeder Auftrag ordnungsgemäß gedruckt wird. Der Prozess wird im Hintergrund ausgeführt und ist entscheidend für das ordnungsgemäße Funktionieren des Druck-Subsystems in Windows. Wenn beim Prozess „spoolsv.exe“ Fehler auftreten, kann dies zu Druckproblemen und Fehlern führen.
taskhostw.exe	taskhostw.exe ist ein Windows -Systemprozess, der als Host für verschiedene Hintergrundaufgaben dient, die auf dem System ausgeführt werden. Es verwaltet und führt Aufgaben wie Aktualisierungen Windows, Wartungsaufgaben und anwenderdefinierte Aufgaben aus. Es handelt sich um einen kritischen Systemprozess, dessen Beendigung zu Systeminstabilität führen kann.
SearchProtocolHost.exe	SearchProtocolHost.exe ist ein Prozess Windows, der für die Indizierung und Durchführung von Suchvorgängen im System verantwortlich ist. Er ist Teil des Suchservice Windows, mit dem Benutzer schnell nach Dateien und Ordnern auf ihrem Computer suchen können. Der Prozess SearchProtocolHost.exe wird im Hintergrund ausgeführt und indiziert Dateien und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	Ordner basierend auf anwenderdefinierten Suchkriterien. Wenn eine Suchabfrage ausgeführt wird, wird der Prozess aktiviert und ruft die relevanten Suchergebnisse ab.
SearchIndexer.exe	SearchIndexer.exe ist ein Windows -Systemprozess, der Dateien und Ordner auf lokalen und Netzwerklaufwerken indiziert, um eine schnellere Suche zu ermöglichen. Es wird im Hintergrund ausgeführt und indiziert kontinuierlich neue oder geänderte Dateien, um eine aktuelle Indexdatenbank zu pflegen. Der Prozess ist für die Suchfunktionalität Windows von von entscheidender Bedeutung und kann unter den meisten Windows -Betriebssystemen gefunden werden.
Explorer.exe	Explorer.exe ist ein Kernprozess in Betriebssystemen Windows, der für die Bereitstellung der Benutzeroberflächen-, Desktop- und Dateiverwaltungsfunktionen verantwortlich ist. Er wird allgemein als Windows Explorer oder Datei-Explorer bezeichnet und ermöglicht Benutzern das Navigieren und Verwalten von Dateien, Ordnern und Anwendungen auf ihrem Computer.
SearchFilterHost.exe	„SearchFilterHost.exe“ ist ein Windows -Systemprozess für die Indizierung und Suche von Dateien auf dem Computer. Es handelt sich um eine Komponente des Suchservice MicrosoftMicrosoft Azure Event Hubs Windows, mit dem Benutzer schnell nach Dateien und Dokumenten auf ihrem Computer suchen können. Der Prozess wird im Hintergrund ausgeführt und kann während der Indizierung von Dateien eine erhebliche Menge von Systemressourcen verbrauchen.
SCNotification.exe	SCNotification.exe ist ein Windows -Systemprozess, der dafür verantwortlich ist, dem Benutzer Systembenachrichtigungen wie Warnungen und Nachrichten anzuzeigen. Es ist Teil des Prozesses Windows Shell Experience Host (ShellExperienceHost.exe), der die Anwenderoberfläche für das Startmenü, die Taskleiste und das Aktionscenter in Windows 10 verwaltet.
sihost.exe	„sihost.exe“ ist ein Systemprozess in Windows, der für das Starten des Startmenüs und die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows sofort einsatzbereite Filter (Fortsetzung)

Name	Beschreibung
	Verarbeitung der zugehörigen Interaktionen verantwortlich ist. Es ist ein wesentlicher Bestandteil der -Benutzeroberfläche und stellt eine grafische Oberfläche für die Interaktion mit dem System bereit.
MonitoringHost.exe	MonitoringHost.exe ist ein rechtmäßiger Systemprozess, der Teil des Betriebssystems Windows ist. Es wird von der Windows Error Reporting-Infrastruktur (WER) verwendet, um Telemetrie- und Diagnosedaten zu sammeln und an MicrosoftMicrosoft Azure Event Hubszu senden und dann die Stabilität und Leistung von Windowszu verbessern.

Discovery-Ressourcennutzung

Typische Transaktionen unter Windows und Unix generieren je nach erkanntem Element unterschiedliche Mengen von Netzwerkverkehr.

Diese Tabelle zeigt den Bandbreitenverbrauch nach Betriebssystem für jedes Datenflusssegment einer typischen Erkennung mit Probes und Mustern. Die Geräte verwenden Probes, während die Anwendungen Muster verwenden. Außerdem wird der Bandbreitenvergleich zwischen einer ersten Erkennung für dreischichtige Anwendungen und alle nachfolgenden Erkennungen dargestellt, bei denen keine Hardwaredaten erfasst werden. Damit wird die Gesamtdatenübertragung für jede einmal erkannte Geräteklasse in Megabyte gemessen.

Hinweis: Diese Messungen wurden mit grundlegenden Betriebskonfigurationen durchgeführt. Die Ergebnisse Ihres lokalen Systems können abweichen.

Discovery-Bandbreitendiagramm

Device Type	MID > Instance	Instance>MID	Mid >Target	Target >MID	Total
Windows 2016	0.104966	0.101271	0.77739	2.364353	3.34798
Windows 2012	0.126327	0.07928	1.177146	3.707051	5.089804
Windows 2008	0.141816	0.104674	1.032673	3.594784	4.873947
Windows 10	0.091466	0.075601	0.642313	2.221103	3.030483
Linux CentOS	0.164232	0.111376	0.148742	0.690117	1.114467
Mac OSX	0.103707	0.068302	0.021681	0.461365	0.655055
HP-UX	0.120358	0.106676	0.042669	0.101149	0.370852
Solaris	0.130551	0.099414	0.060243	0.346605	0.636813
Cisco UCS switch	0.029665	0.027465	0.094918	0.097444	0.249492
F5 load balancer	0.043935	0.03689	0.017179	0.012132	0.110136
A10 load balancer	0.046631	0.032266	0.018313	0.03182	0.12903
EMC Storage	0.4776	0.373828	1.215954	4.741926	6.809308
Three-tier application - initial Discovery	0.712829	0.678862	7.084678	9.430181	17.90655
F5 load balancer				0.017179	0.012132
Apache on Linux				0.540161	1.107108
Websphere on Linux				0.729403	1.165112
Oracle on Windows				5.797935	7.145829
Three-tier application - subsequent Discovery	0.150882	0.107409	2.536535	0.560122	3.354948
F5 load balancer				0.001347	0.012132
Apache on Linux				0.136366	0.079392
Websphere on Linux				0.341042	0.11365
Oracle on Windows				2.05778	0.354948

Diese Tabelle zeigt die Erkennung verschiedener Betriebssystemtypen, die Muster nutzen. Dieser misst (in Megabyte) die Gesamtmenge der erstellten Daten und die Gesamtmenge der Daten in nachfolgenden Scans für jedes Gerät.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Bandbreitenmuster

Device		Mid > Instance	Instance > Mid	Mid > Target	Target > Mid	Total
Linux	Create	0.39	0.486	0.098	0.273	1.247
	Update	0.382	0.499	0.093	0.264	1.238
Windows Server	Create	0.289	0.316	5.628	8.508	14.741
	Update	0.273	0.306	5.621	8.458	14.658
Solaris	Create	1.222	1.4	0.383	0.917	3.922
	Update	1.24	1.42	0.399	0.675	3.734
HPUX	Create	0.176	0.222	0.063	0.13	0.591
	Update	0.178	0.247	0.062	0.128	0.615
Citrix Netscalar	Create	0.424	1.919	0.019	0.042	2.404
	Update	0.355	0.619	0.016	0.041	1.031
F5	Create	0.087	0.135	0.026	0.047	0.295
	Update	0.132	0.171	0.026	0.047	0.376
L3 Switch	Create	0.172	0.125	0.282	0.478	1.057
	Update	0.178	0.126	0.282	0.479	1.065

Monitoring von Erkennungen und Problemlösung

Erfahren Sie, wie Sie den Fortschritt Ihrer Erkennungen überwachen und das System konfigurieren, um Leistungsmetriken zu aggregieren, die wichtig für Sie sind. Hier finden Sie Beschreibungen der angezeigten Fehlermeldungen sowie mögliche Schritte zur Lösung von Problemen. Die Hi-Knowledge Base enthält mehrere Artikel, die Sie bei der Behandlung von Problemen mit Erkennungen unterstützen.

MID Server-Übersicht	

Discovery-Homepage

Öffnen Sie den Discovery-Manager, um Zeitpläne für IP-basierte und cloudbasierte Erkennungen zu erstellen oder zu bearbeiten. Zeigen Sie die von Ihren Zeitplänen erkannten CIs und Cloud-Ressourcen an, und verfolgen Sie dann alle aufgetretenen Fehler nach.

Discovery-Dashboard

Überwachen Sie laufende Discovery-Vorgänge, und verwalten Sie Berichte, die die Datenbank abfragen. Zeigen Sie Zusammenfassungen über Discovery-Status, erkannte Geräte, Zeitleisten und Fehler an.

Leitfaden zur Discovery-Fehlerbehebung

Lesen Sie den Leitfaden zur Discovery-Fehlerbehebung in der Knowledge Base, wenn bei Ihnen Unregelmäßigkeiten auftreten, etwa wenn Discovery den erkannten Host nicht klassifizieren kann oder wenn die Shazzam-Probe bestimmte Gerätetypen nicht findet.

KB0657528: Problembehandlung hinsichtlich Anmeldeinformationen und Berechtigungen für Discovery, Service-Mapping und Orchestration

Discovery-Probleme können durch falsch konfigurierte oder fehlende Anmeldeinformationen verursacht werden. Erfahren Sie, wie Sie fehlende Anmeldeinformationen oder Berechtigungen identifizieren und konfigurieren.

Discovery-Fehlermeldungen

Zeigen Sie die Liste der allgemeinen Fehlermeldungen und möglichen Lösungen an.

Leistungsmetriken zu Erkennungen

Zeigen Sie Leistungsmetriken zu Probe-/Muster- und Sensorverarbeitungszeiten an. Sie können Rollup-Daten verwenden, um die Leistung bestimmter

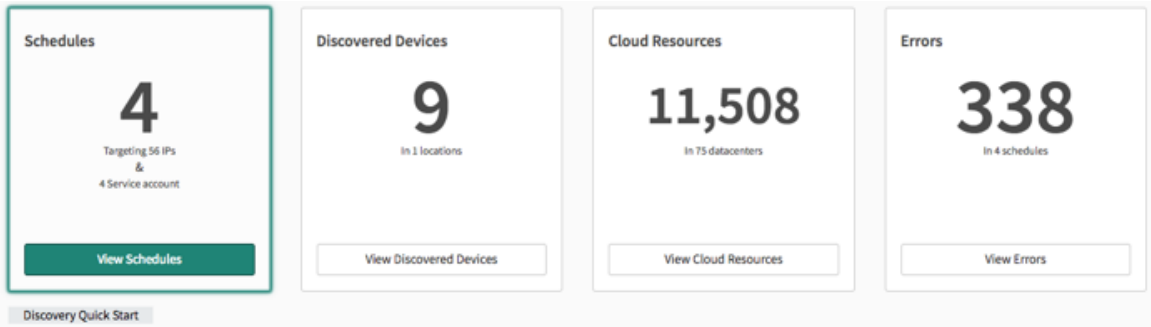
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennungen zu überwachen oder um die Leistung zwischen Versionen nach einem Upgrade zu vergleichen.

Discovery-Homepage

Auf der Seite Discovery-Startseite finden Sie eine Zusammenfassung der Erkennungen, die durch Cloud- und Nicht-Cloud-Zeitpläne ausgelöst worden sind. Sie können alle Fehler anzeigen, die während einer Discovery aufgetreten sind, und Vorschläge zur Fehlerkorrektur einsehen. Verwenden Sie die Ansicht „Homepage“, um die für die in einem Cloud-Zeitplan ausgewählten Servicekonten erkannten Cloud-Ressourcen zu untersuchen.

Um die Seite Discovery-Startseite zu öffnen, navigieren Sie zu **Discovery** > **Startseite**. Auf der Homepage werden Discovery-Summen für die folgenden Kategorien angezeigt. Klicken Sie auf eine Kachel, um Details zu dieser Kategorie anzuzeigen.

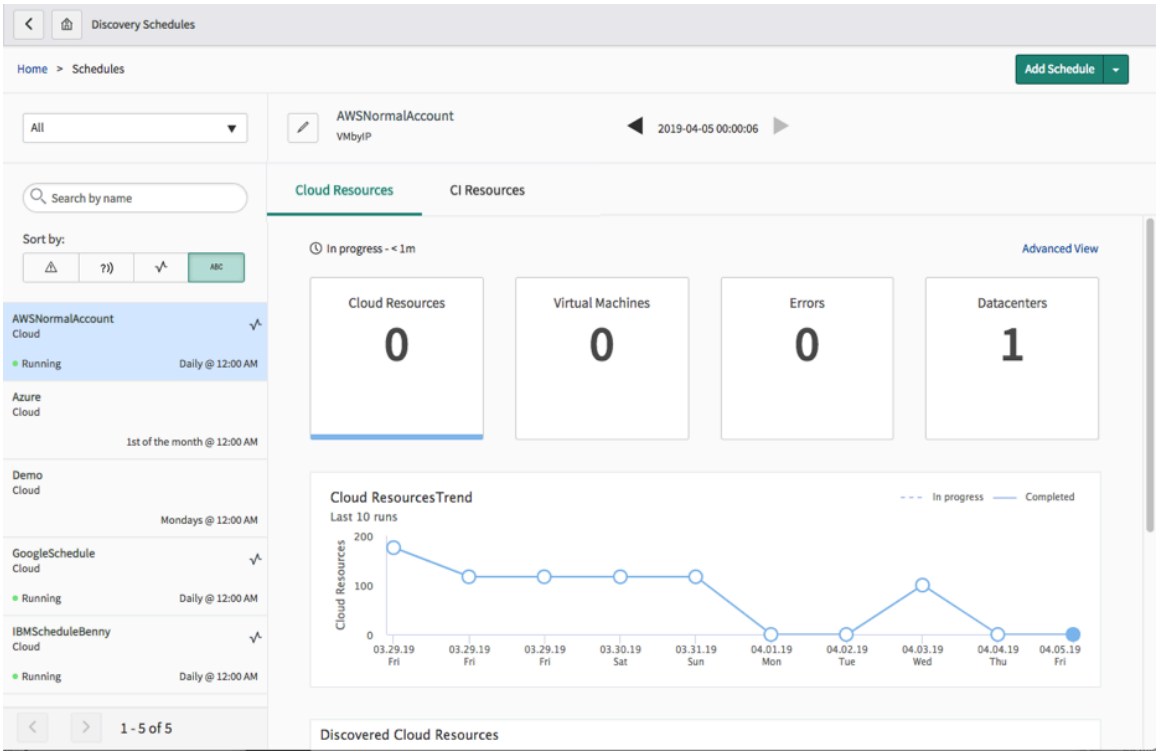


Element	Beschreibung
Zeitpläne	Die Anzahl der Discovery-Zeitpläne, die zur Erkennung von Cloud-Ressourcen und virtuellen Computern (IP-Adressen) konfiguriert sind. Klicken Sie auf **Zeitpläne anzeigen**, um die CI-Zeitplanansicht zu öffnen, in der spezifische Informationen über die einzelnen CI-Zeitpläne separat angezeigt werden. Zeigen Sie die Ergebnisse Ihrer Cloud- oder IP-Adresszeitpläne an, und erstellen Sie neue Zeitpläne.
Erkannte Geräte	Die Gesamtanzahl der erkannten Geräte-CIs. Geräte umfassen alle CIs in Tabellen, die die Tabelle „Hardware“ [cmdb_ci_hardware] erweitern, zum Beispiel „Computer“ [cmdb_ci_computer] und „Cisco-UCS-Zubehör“ [cmdb_ci_ucs_equipment].
Cloud-Ressourcen	Die Gesamtanzahl der für die ausgewählten Servicekonten erkannten Ressourcen (virtuellen Computer). Unter Erkennung von virtuellen Maschinen aktivieren finden Sie Details zum Einrichten von Discovery für Ihre Cloud-Ressourcen. Klicken Sie auf **Cloudressourcen anzeigen**, um eine Liste der erkannten Cloud-Ressourcen nach Typ zu öffnen.
Fehler	Die Gesamtanzahl der während der Erkennung aufgetretenen, nicht gelösten Fehler. Klicken Sie auf **Fehler anzeigen**, um einen Drilldown zu bestimmten Fehlertypen durchzuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Zeitpläne anzeigen

In der Zeitplanansicht werden Details zu jedem Zeitplan angezeigt, der für den ausgewählten Filter ausgeführt wurde. Standardmäßig sind in der Liste alle Erkennungszeitpläne in alphabetischer Reihenfolge aufgeführt, unabhängig vom aktuellen Ausführungsstatus.

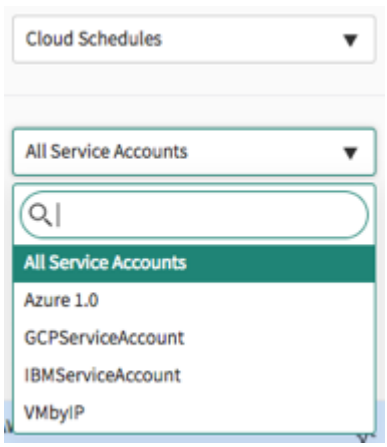


Verwenden Sie die folgenden Steuerelemente, um Discovery-Ergebnisse nach Zeitplänen zu filtern:

Zeitplanfilter

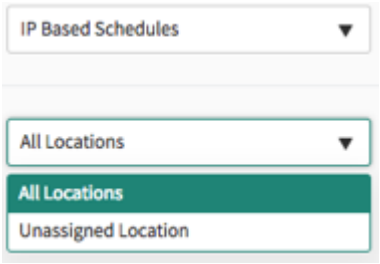
Folgende Filter sind zur Auswahl verfügbar:

- **Alle**: Ergebnisse aller Erkennungszeitpläne, die ausgeführt wurden. Das ist der Standardfilter.
- **Cloud-Zeitpläne**: Ergebnisse aller Cloud-Erkennungszeitpläne, die ausgeführt wurden. Wenn Sie diesen Filter auswählen, wird ein zweiter Filter eingeblendet, mit dem Sie Cloud-Zeitpläne nach **Servicekonto** anzeigen können.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **IP-basierte Zeitpläne**: Ergebnisse aller Erkennungszeitpläne, die für Konfigurationselemente (CI) unter Verwendung von IP-Bereichen ausgeführt wurden. Wenn Sie diesen Filter auswählen, wird ein zweiter Filter angezeigt, mit dem Sie die CI-Zeitpläne nach einem bestimmten Standort oder allen Standorten anzeigen können.



Zeitplansortierer

Wählen Sie in der Zeitplanauswahl im linken Bereich von links nach rechts eines der folgenden Sortierkriterien aus:

- Fehler für alle aufgelisteten Zeitpläne
- Nicht identifizierte IP-Adressen
- Letzte Aktivität, durch die die derzeit zuerst ausgeführten Zeitpläne auflistet werden
- Alphabetische Liste der Zeitpläne

Zeitplanliste

Liste der verfügbaren Erkennungszeitpläne. Wählen Sie einen Zeitplan aus, um dessen Details anzuzeigen. Klicken Sie oben auf der Seite auf das Stiftsymbol, um den Zeitplan zu bearbeiten.

Datum-/Uhrzeitanzeige

Datum und Uhrzeit des Zeitpunkts, an dem der ausgewählte Zeitplan ausgeführt wurde

Zeitplanthemen

Kacheln, die die Kategorien für Erkennungsergebnisse für den ausgewählten Zeitplan anzeigen. Klicken Sie auf eine Kachel, um weitere Details dazu anzuzeigen.

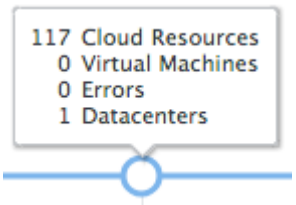
- **Cloud-Ressourcen**: Zeigt die Gesamtanzahl der für diesen Filter aktualisierten oder erstellten CIs an
- **Virtuelle Computer**: Zeigt die Gesamtanzahl der mit dem ausgewählten Zeitplan erkannten virtuellen Computer an
- **Fehler**: Zeigt die Gesamtanzahl der Fehler an, die beim Ausführen des ausgewählten Zeitplans aufgetreten sind
- **Datacenter**: Zeigt die Anzahl der Rechenzentren an, die bei der Erstellung des Erkennungszeitplans ausgewählt wurden

Trenddiagramm für Cloud-Ressourcen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dies ist ein Trenddiagramm für den ausgewählten Zeitplan. Jeder Kreis im Diagramm stellt eine bestimmte Discovery-Ausführung dar.

Platzieren Sie den Cursor auf einem beliebigen Kreis, um eine Zusammenfassung dieser Erkennung anzuzeigen.



Klicken Sie auf einen Kreis, um die Werte zu filtern, die in den Discovery-Themen angezeigt werden. Die Ergebnisse füllen die entsprechenden Kacheln über dem Diagramm.

Fehler nach Kategorie

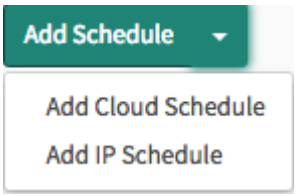
Dies sind die Kategoriekacheln für die während der Erkennung aufgetretenen Fehler für den ausgewählten Zeitplan. Klicken Sie auf eine Kachel, um die Fehler in dieser Kategorie anzuzeigen und empfohlene Aktionen zur Fehlerkorrektur anzuzeigen. Weitere Einzelheiten erhalten Sie unter Discovery-Fehlermeldungen.

Erkannte Cloud-Ressourcen

Aufgliederung der für den ausgewählten Zeitplan erkannten Cloud-Ressourcen, dargestellt in einem horizontalen Balkendiagramm

Zeitpläne hinzufügen

Typen der hinzufügbaren Zeitpläne



Erweiterte Ansicht

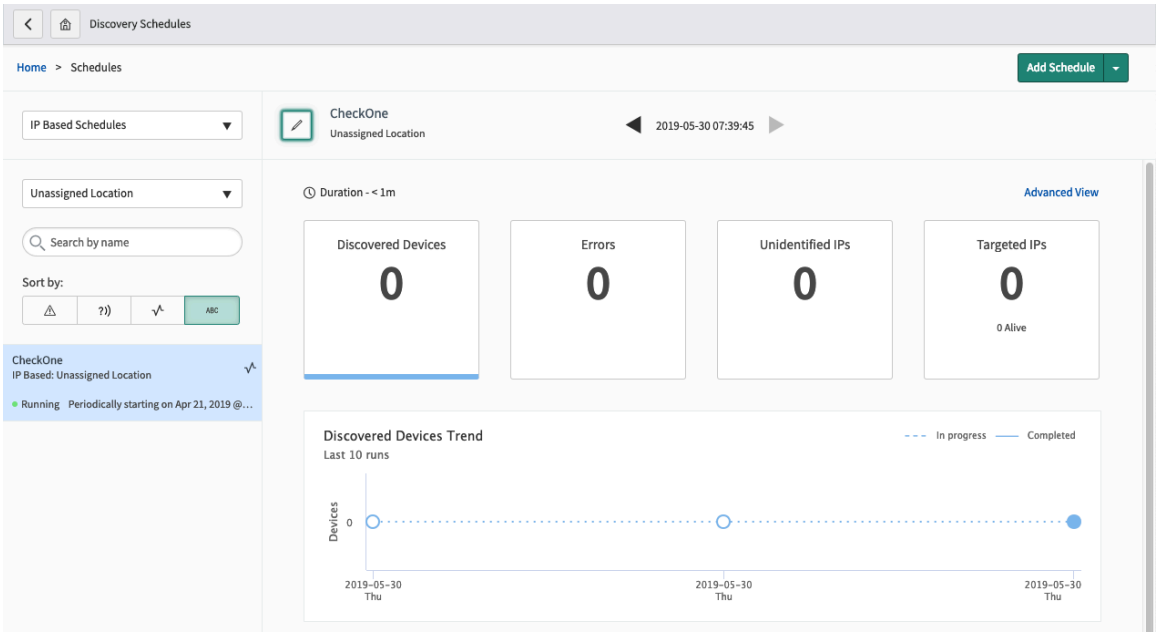
Zeigt den Discovery-Statusdatensatz für den ausgewählten Zeitplan an. Über diesen Link können Sie die Ergebnisse des Zeitplans in der ECC-Warteschlange und im Discovery-Protokoll überprüfen.

IP-basierte Zeitpläne anzeigen

Wählen Sie zum Anzeigen der Ergebnisse von IP-Bereichserkennungen im primären Filter die Option **IP-basierte Zeitpläne** aus. Verwenden Sie das eingeblendete sekundäre Feld, um die Suchergebnisse nach **Standort** zu filtern. Daraufhin zeigen die Kacheln die Ergebniskategorien für den ausgewählten IP-basierten Zeitplan an. Klicken Sie auf eine Kachel, um weitere Details dazu anzuzeigen.

- **Erkannte Geräte**: Gesamtanzahl der vom IP-basierten Zeitplan erkannten virtuellen Computer, einschließlich Ziel-IP-Adressen und nicht identifizierter IP-Adressen
- **Fehler**: Zeigt die Gesamtanzahl der Fehler an, die beim Ausführen des ausgewählten IP-basierten Zeitplans aufgetreten sind
- **Nicht identifizierte IPs**: Anzahl der nicht identifizierten CIs, die vom IP-basierten Zeitplan erkannt wurden
- **Ziel-IP-Adressen**: Anzahl der gefundenen CIs, die im IP-basierten Zeitplan konfiguriert waren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Fehler im CI-Erkennungszeitplan beheben

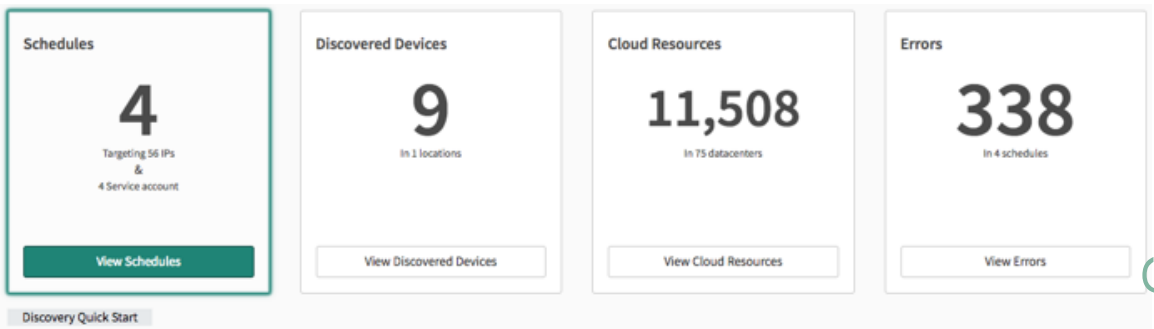
Auf der ServiceNow-Homepage können Sie die während einer Erkennung aufgetretenen Discovery-Fehler anzeigen und erhalten Vorschläge zur Lösung dieser Fehler. Sie können die Fehler für alle Zeitpläne oder für einen einzelnen Zeitplan anzeigen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**.
   Die Zusammenfassungsseite für alle Zeitpläne wird angezeigt.



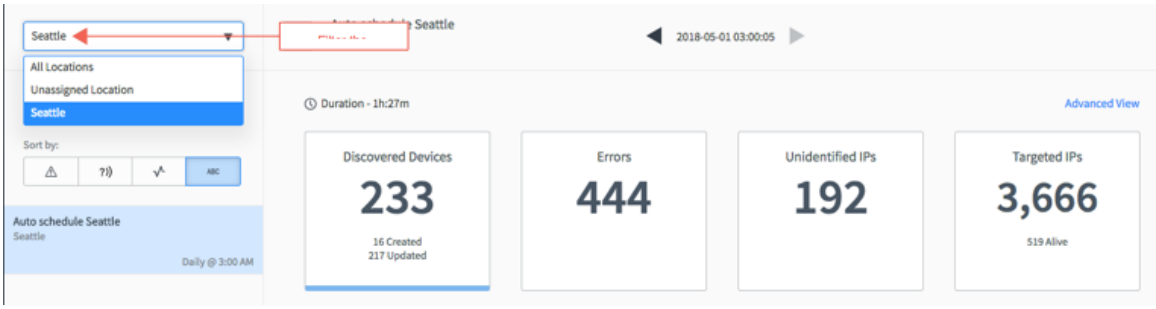
2. Zeigen Sie die Fehler mit einer der folgenden Methoden an:
   - Klicken Sie auf die Kachel **Fehler**, um die Fehler nach Kategorie für alle CI-Erkennungszeitpläne anzuzeigen.
   - Klicken Sie auf die Kachel **Zeitpläne**, um die Fehler für einen einzelnen Zeitplan anzuzeigen.

     a. Wählen Sie auf dem Zusammenfassungsbildschirm den Zeitplan aus, den Sie auf Fehler untersuchen möchten.

     Wenn Sie über zahlreiche Zeitpläne verfügen, können Sie sie über die Dropdown-Liste „Standort“ nach dem Standort oder über das Feld **Nach Namen suchen** nach dem Zeitplannamen filtern.

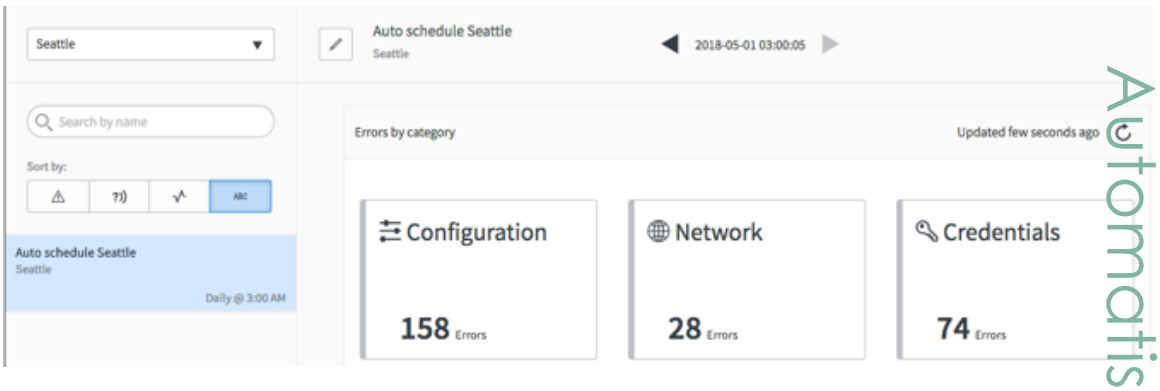
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



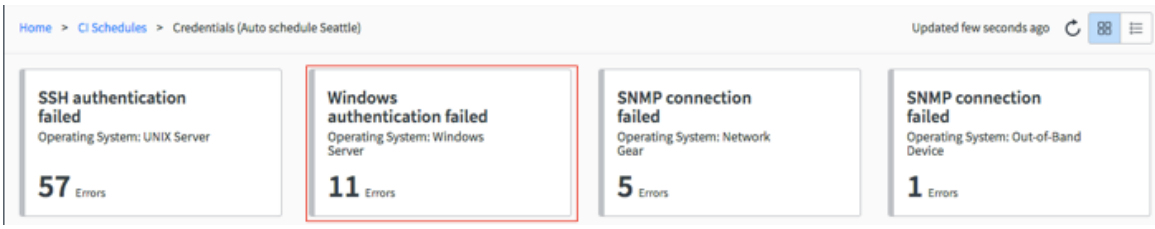
b. Nachdem Sie den Zeitplan ausgewählt haben, klicken Sie auf die Kachel **Fehler**.

c. Scrollen Sie nach unten, um die Fehler nach Kategorie anzuzeigen.



3. Klicken Sie auf eine Kategoriekachel, um die spezifischen Fehlercodes anzuzeigen, die in dieser Kategorie aufgetreten sind.

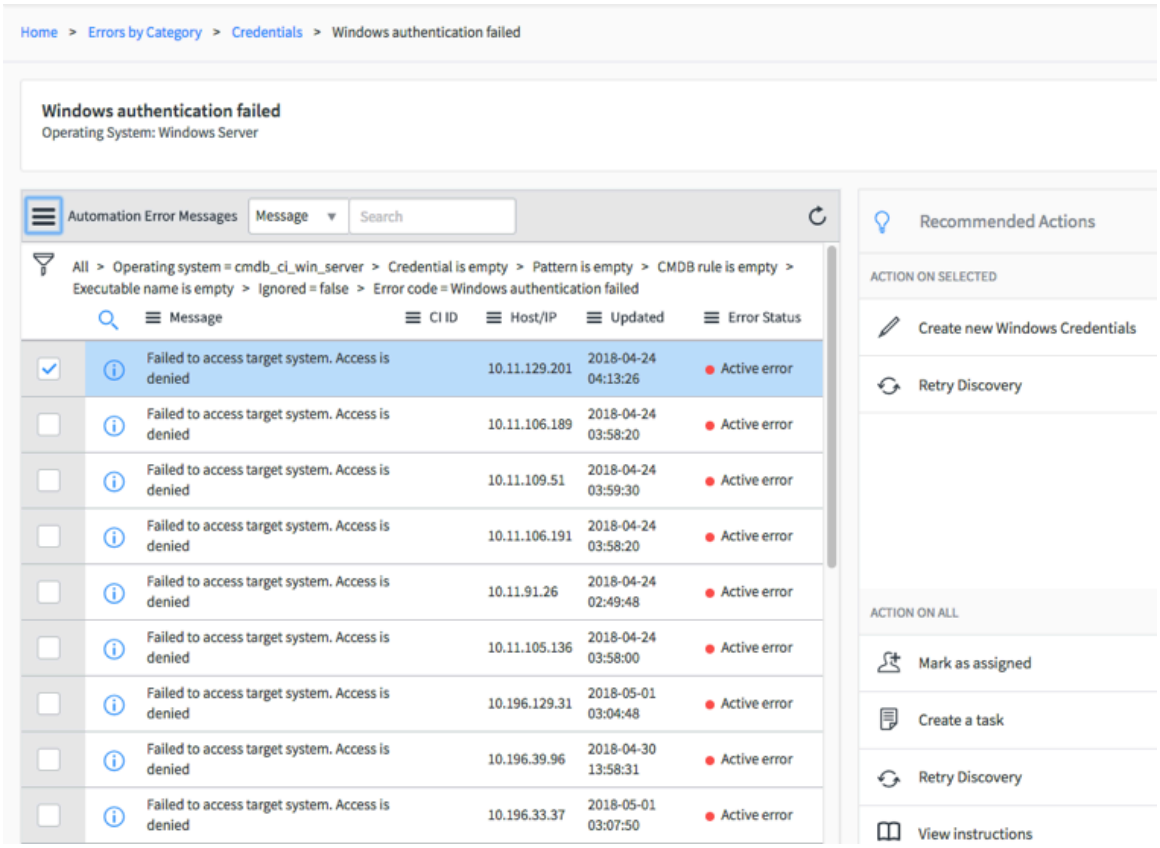
4. Klicken Sie auf die Kachel für den Fehlercode, den Sie untersuchen möchten.



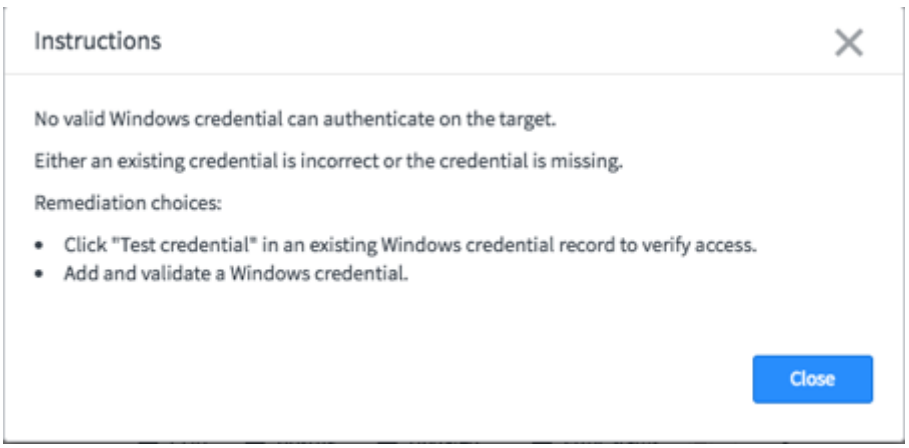
Die Liste zeigt alle Vorkommen dieses Fehlercodes an, entweder für einen einzelnen CI-Zeitplan oder für alle Zeitpläne, und zwar abhängig vom Pfad, den Sie zum Anzeigen der Fehler ausgewählt haben. Die Liste zeigt die IP-Adresse jeder Instanz an, bei der der Fehler aufgetreten ist, und den Fehlerstatus **Aktiver Fehler**. Der Bereich **Recommended Actions** auf der rechten Seite enthält die empfohlene Aktion für den ausgewählten Fehler. Der Bereich **AKTION FÜR ALLE** enthält Vorgänge, die Sie für alle Fehler in der Liste ausführen können.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

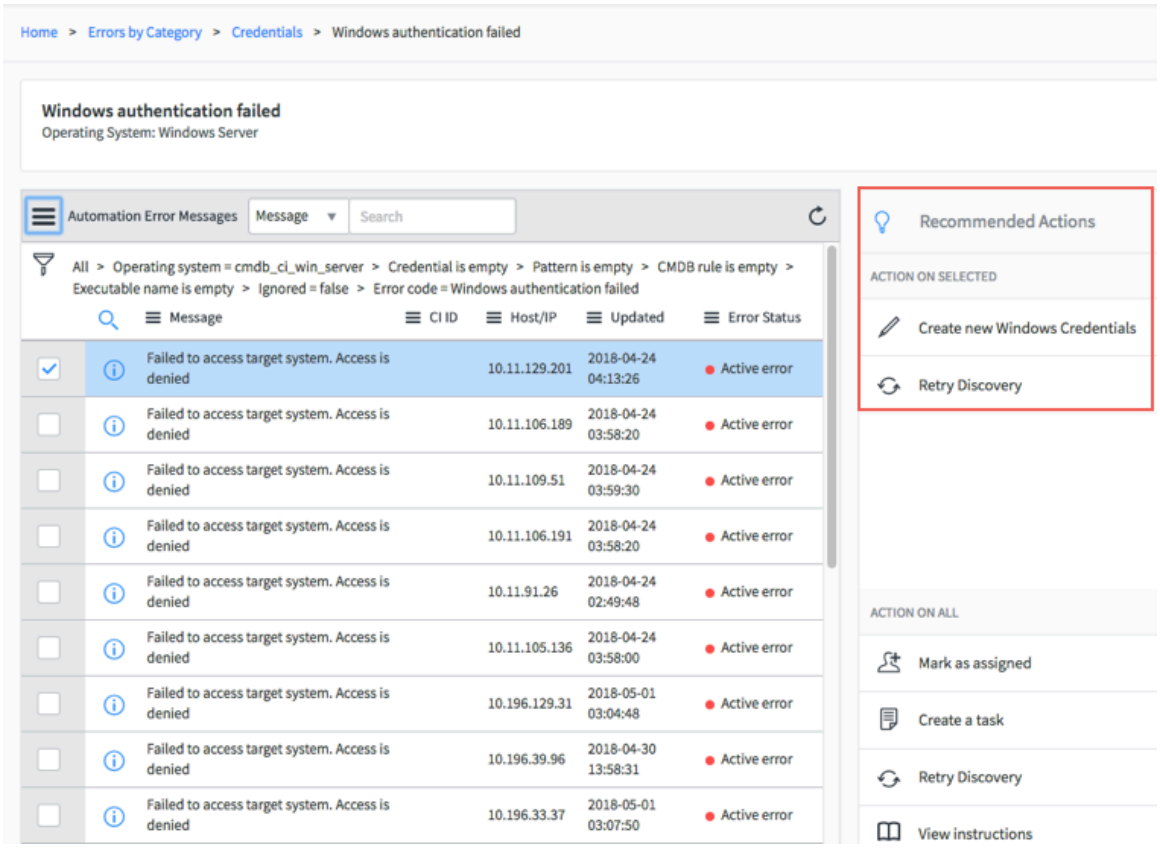


5. Klicken Sie auf **Anweisungen anzeigen**, um Details und Vorschläge zur Fehlerkorrektur für den Fehlercode anzuzeigen.

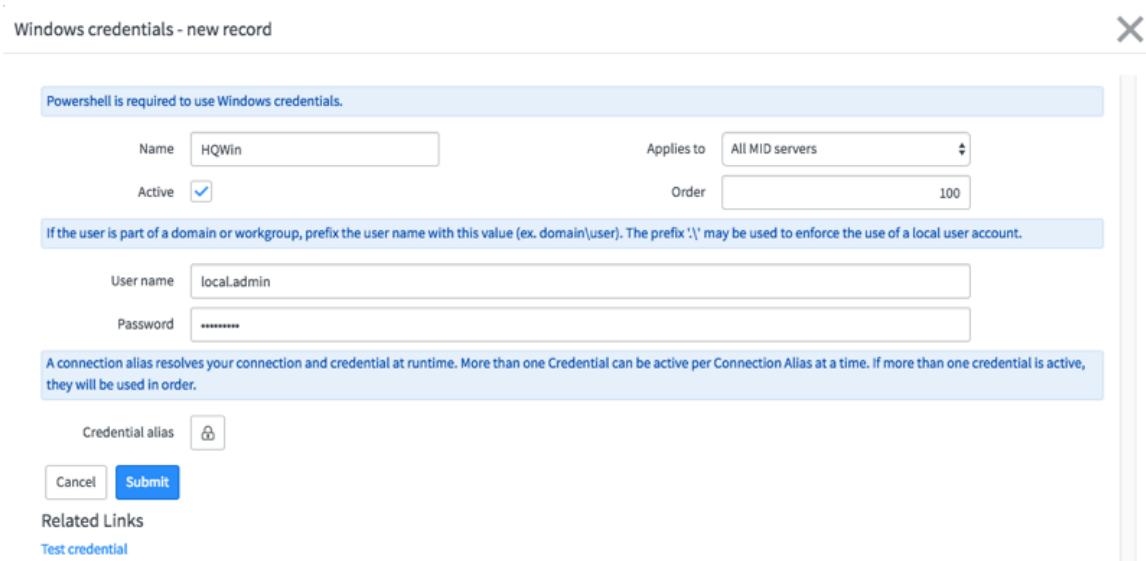


6. Um mit der Arbeit zu beginnen, aktivieren Sie entweder das Kontrollkästchen neben einem Fehler, um diesen Fehler zu beheben, oder wählen Sie eine Aktion für **ALLE** aus, um diesen Fehlercode für alle Instanzen dieses Fehlers zu beheben.
In diesem Beispiel empfiehlt das System, zur Behebung dieses Fehlercodes neue Windows-Anmeldeinformationen zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Schließen Sie die vorgeschlagenen Aufgaben zur Fehlerkorrektur ab, bevor Sie die Erkennung erneut versuchen.
In diesem Beispiel wird über den Link **Neue Windows-Anmeldeinformationen erstellen** ein Formular zum Erstellen und Testen neuer Windows-Anmeldeinformationen geöffnet.



8. Nachdem Sie alle empfohlenen Aufgaben abgeschlossen haben, klicken Sie auf **Discovery wiederholen**.
Eine mögliche Vorgehensweise besteht darin, die Discovery für **ALLE** Instanzen nach dem Erstellen der Anmeldeinformationen zu wiederholen. Möglicherweise stellen die neuen Anmeldeinformationen die Lösung des Problems für alle Instanzen dar, bei denen dieser Fehlercode auftritt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Überprüfen Sie die Spalte **Fehlerstatus**, um die Ergebnisse Ihrer Maßnahmen zur Fehlerkorrektur anzuzeigen.
   Einzelne Wiederholungsversuche werden schnell abgeschlossen. Neuversuche für eine große Anzahl von IP-Adressen können mehrere Minuten dauern.

   Fehler können einen der folgenden Status aufweisen:

   - **Aktiver Fehler**: Der Fehler ist nicht gelöst. Das ist der Standardstatus aller neuen Fehler.
   - **Gelöst**: Der Fehler ist behoben. Für die empfohlenen Aktionen wird Fehler erfolgreich gelöst angezeigt.
   - **Zugewiesen**: Zur Behebung dieses Fehlers ist eine Aufgabe zugewiesen. Klicken Sie auf **Eine Aufgabe erstellen**, um einen Benutzer für alle aktiven Fehler einer Aufgabe zuzuweisen. Zugewiesene Fehler gelten als **Aktive Fehler**, für die noch Aktionen ausgeführt werden können.
   - **Ausstehende Erkennung**: Es wird darauf gewartet, dass die Erkennung gestartet wird, nachdem Sie die Aktion **Discovery wiederholen** für alle Fehler ausgeführt haben.
   - **In Erkennung**: Die Erkennung ist derzeit aktiv.

Zugehörige Informationen

Discovery-Status

Protokolle für horizontale Erkennung prüfen

ECC-Warteschlange für Discovery

Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen

Discovery-Dashboard

Das Discovery-Dashboard ist der zentrale Ort für Benutzer von Discovery, um laufende Discovery-Vorgänge zu überwachen. Das Dashboard enthält Berichte, die Anfragen in der Datenbank stellen und die Ergebnisse anzeigen.

Dashboards sind die Startseiten für Produkte in der Instanz. Das Discovery-Dashboard bietet Zusammenfassungsinformationen für Discovery bezüglich Status, Geräte, Anwendungen und Zeitleiste. Außerdem werden Discovery-Fehler und Lösungsvorschläge angezeigt.

Hinweis: Alle Daten im Dashboard sind domänengetrennt und zeigen nur Daten an, die aus der Domäne gesammelt wurden, die im MID-Server-Benutzerkonto für den verwendeten Discovery-Zeitplan angegeben ist.

Um das Discovery-Dashboard anzuzeigen, navigieren Sie zu **Discovery** > **Dashboard**.

Funktionen des Discovery-Dashboard

Das Discovery-Dashboard zeigt Folgendes an:

- Den aktuellen Fortschritt (Status) der aktiv ausgeführten Discovery-Zeitpläne
- Neu erkannte Geräte und Anwendungen nach Zeitpunkt der Erkennung
- Vorhandene von Discovery nicht aktualisierte Geräte und Anwendungen
- Fehler, die während eines ausgeführten Discovery-Zeitplans aufgetreten sind.
- Berechtigungsnachweise, die von einem Discovery-Zeitplan entweder nicht benötigt oder nicht verwendet wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Berichte zum Dashboard hinzufügen

Ab dem Madrid-Release werden Anzeigen in Dashboards nicht mehr unterstützt und wurden durch Widgets ersetzt. In vorhandenen Dashboards können Sie Discovery-Anzeigen weiterhin verwenden. Sie können Ihren Dashboards jedoch keine alten Discovery-Anzeigen hinzufügen. Wenn Sie Berichtsfunktionen benötigen, die im aktuellen Dashboard nicht verfügbar sind, müssen Sie mithilfe von Widgets eigene Berichte erstellen.

Komponenten des Discovery-Dashboard

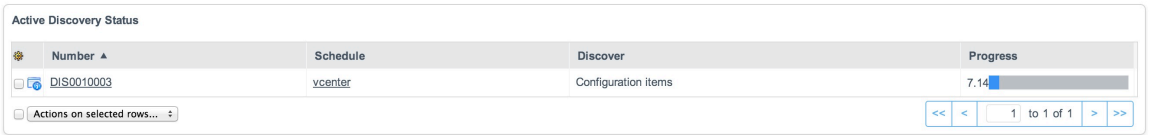
Sie können die Berichte im Dashboard anpassen, sodass für Ihre Umgebung wichtige Statistiken angezeigt werden.

Statusbericht der aktiven Discovery

Der Statusbericht von „Aktiv Discovery “ zeigt den Fortschritt eines aktiv ausgeführten Discoveryan. Die angezeigten Informationen werden aus dem Statusmodul Discovery abgerufen. Das Feld **Fortschritt** des Statusdatensatzes gibt den Fertigstellungsgrad des Zeitplans Discovery an. Der Prozentsatz der Fertigstellung wird basierend auf vorherigen Läufen desselben Discovery-Zeitplans berechnet. Das Fortschrittsfeld ist in den folgenden Fällen leer:

- Wenn Sie DiscoverNow verwenden
- Wenn Sie Discovery von einem Configuration Item (CI) aus verwenden
- Während der ersten Ausführung eines Zeitplans Discovery

Statusbericht der aktiven Discovery

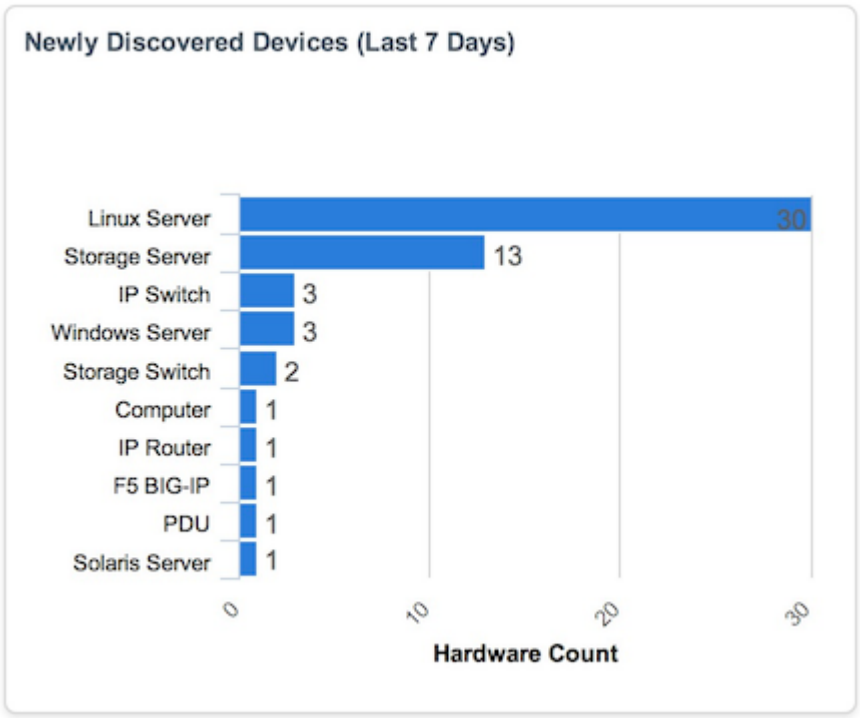


Bericht „Neu erkannte Geräte“

Der Bericht „Neu erkannte Geräte“ zeigt die Anzahl der Geräte an, die die Anwendung Discovery in den letzten sieben Tagen identifiziert hat, gruppiert nach der Klasse des Geräts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

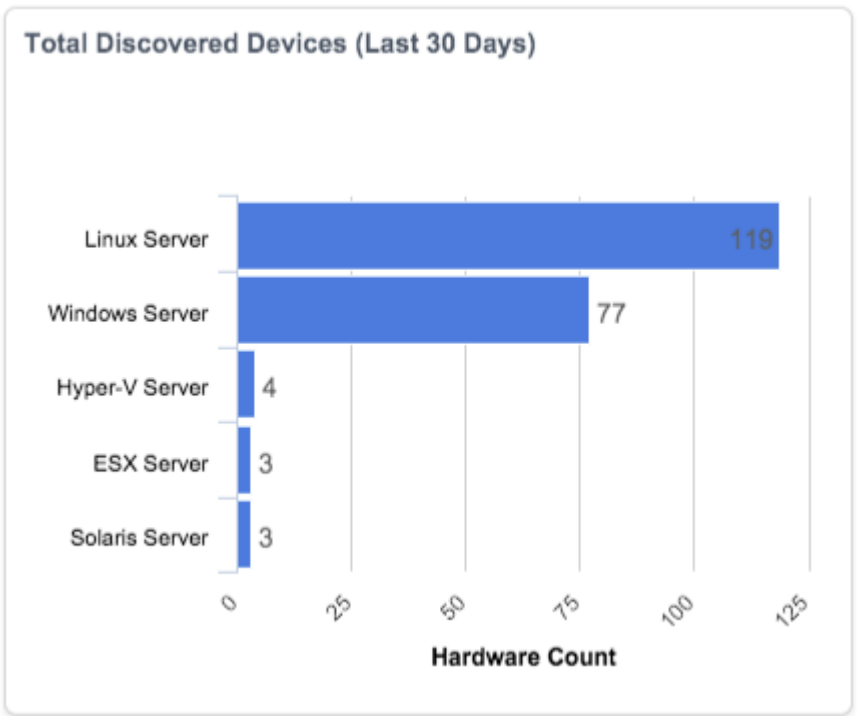
Bericht „Neu erkannte Geräte“



Bericht „Insgesamt erkannte Geräte“

Der Bericht „Insgesamt erkannte Geräte“ zeigt die Gesamtanzahl der Geräte an, die die Anwendung Discovery in den letzten 30 Tagen identifiziert hat, gruppiert nach der Klasse des Geräts.

Bericht „Insgesamt erkannte Geräte“

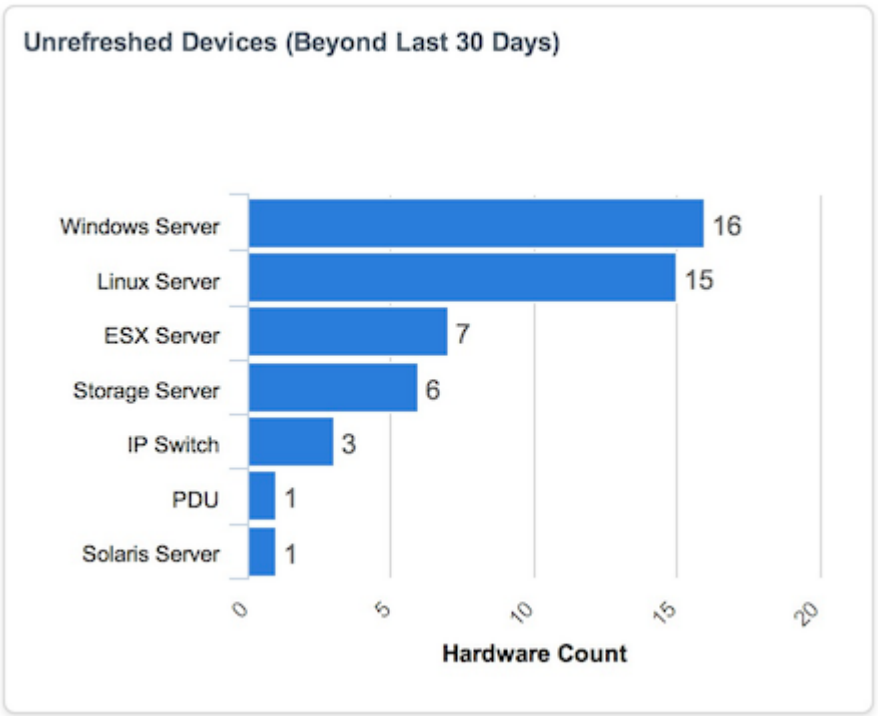


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bericht zu nicht aktualisierten Geräten

Im Bericht „Nicht aktualisierte Geräte“ werden Geräte angezeigt, die bis vor einem Jahr erkannt wurden, in den letzten 30 Tagen jedoch nicht identifiziert wurden, gruppiert nach der Klasse des Geräts.

Bericht zu nicht aktualisierten Geräten

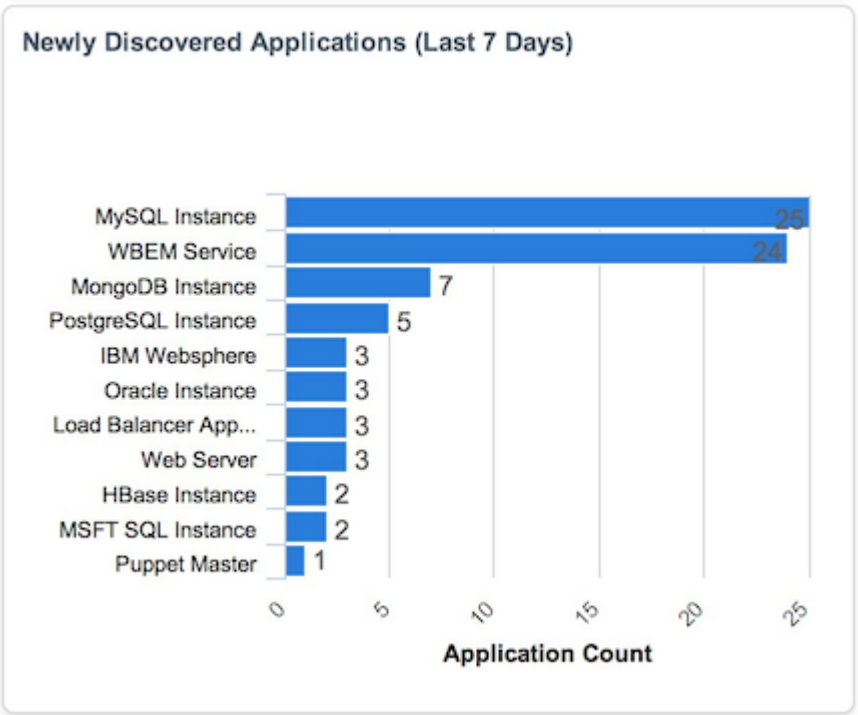


Bericht über neu erkannte Anwendungen

Der Bericht „Erkannte neue Anwendungen“ zeigt die Anzahl der neuen Anwendungen an, die von der Anwendung Discovery in den letzten sieben Tagen identifiziert wurden, gruppiert nach der Klasse der Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

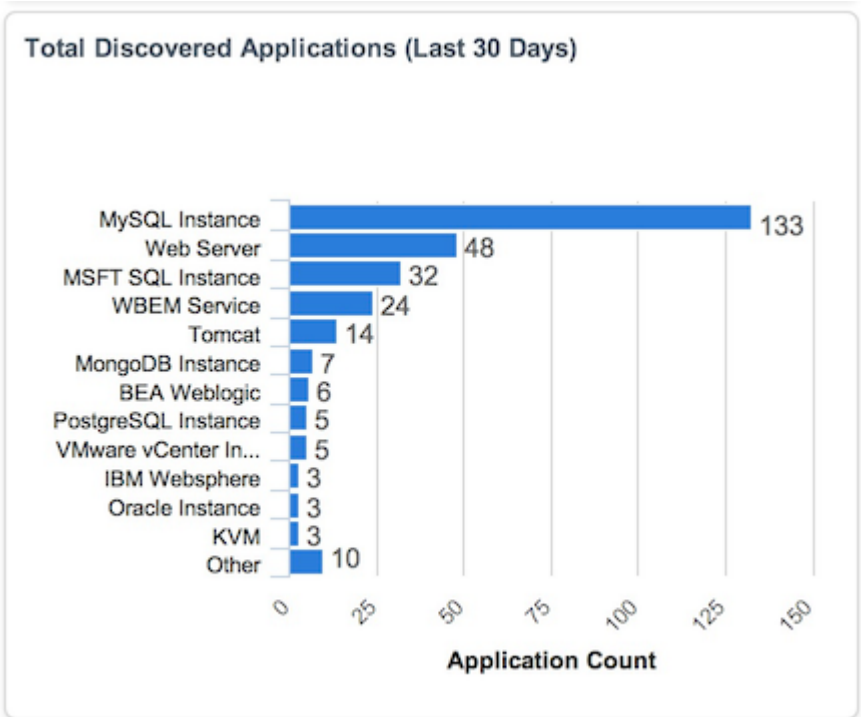
Bericht über neu erkannte Anwendungen



Bericht über insgesamt erkannte Anwendungen

Der Bericht „Insgesamt erkannte Anwendungen“ zeigt die Gesamtanzahl der Anwendungen an, die die Anwendung Discovery in den letzten 30 Tagen identifiziert hat, gruppiert nach der Klasse der Anwendung.

Bericht über insgesamt erkannte Anwendungen

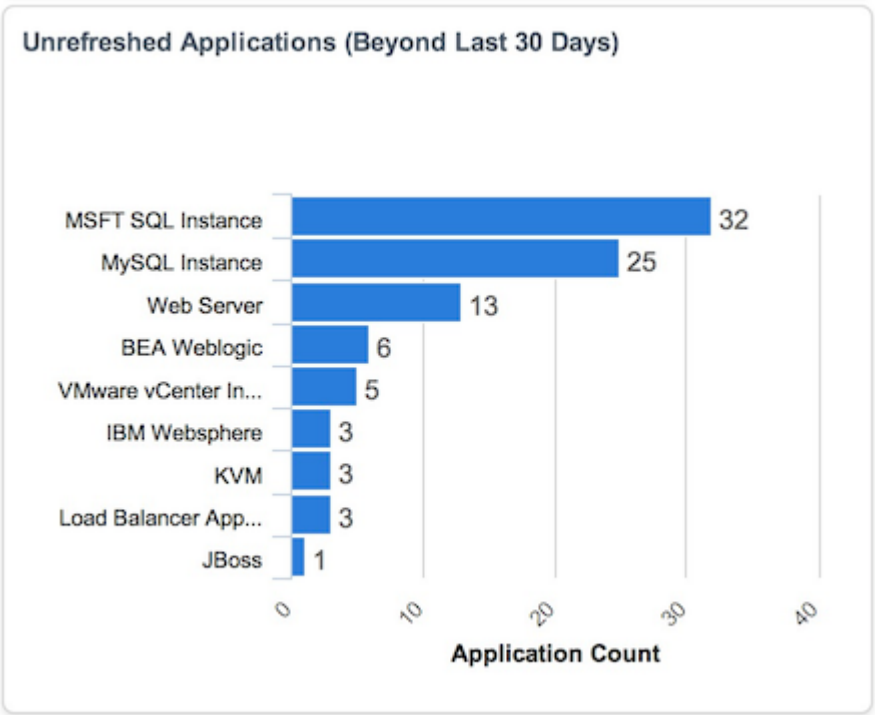


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bericht zu nicht aktualisierten Anwendungen

Im Bericht „Nicht aktualisierte Anwendungen“ werden Anwendungen angezeigt, die bis vor einem Jahr erkannt wurden, in den letzten 30 Tagen jedoch nicht identifiziert wurden, gruppiert nach der Klasse der Anwendung.

Bericht zu nicht aktualisierten Anwendungen



Fehlerbericht der aktiven Discovery

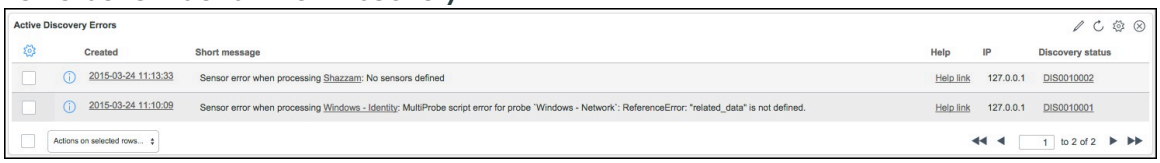
Der Bericht Aktive Discovery Fehler listet die Fehler auf, die von den einzelnen aktiven Discoverygeneriert werden. Die Fehler für einen bestimmten Discovery werden überschrieben, wenn dieser Discovery erneut ausgeführt wird. Dieser Bericht enthält folgende Daten:

Fehlerberichtsdaten der aktiven Discovery

Spalte	Beschreibung
Erstellt	Zeitstempel der Fehlermeldung.
Kurznachricht	Inhalt der Fehlermeldung, die während des Discovery-Laufs generiert wurde.
Hilfe	Link zu einem Vorschlag, wie der Fehler behoben werden kann. In einigen Fällen ist der Link spezifisch für den Fehler. In anderen Fällen verweist der Link auf eine allgemeine Seite, die eine Lösung für häufige Fehler enthält.
IP	IP-Adresse des Assets, auf dem der Fehler entdeckt wurde.
Discovery-Status	Discovery-Statusnummer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlerbericht der aktiven Discovery

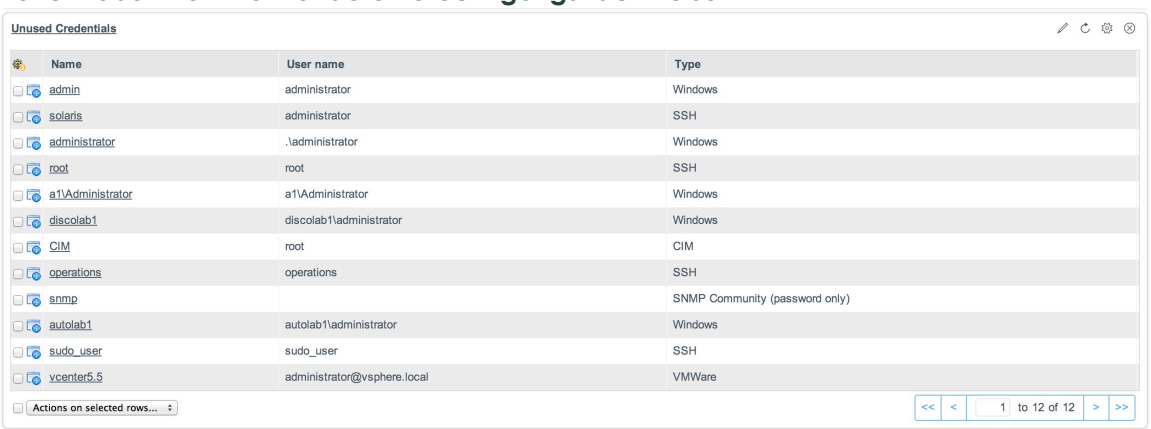


Bericht über nicht verwendete Berechtigungsnachweise

Im Bericht „Nicht verwendete Anmeldeinformationen“ werden die Anmeldeinformationen aufgelistet, die derzeit nicht von den Anwendungen Discovery oder Orchestration verwendet werden.

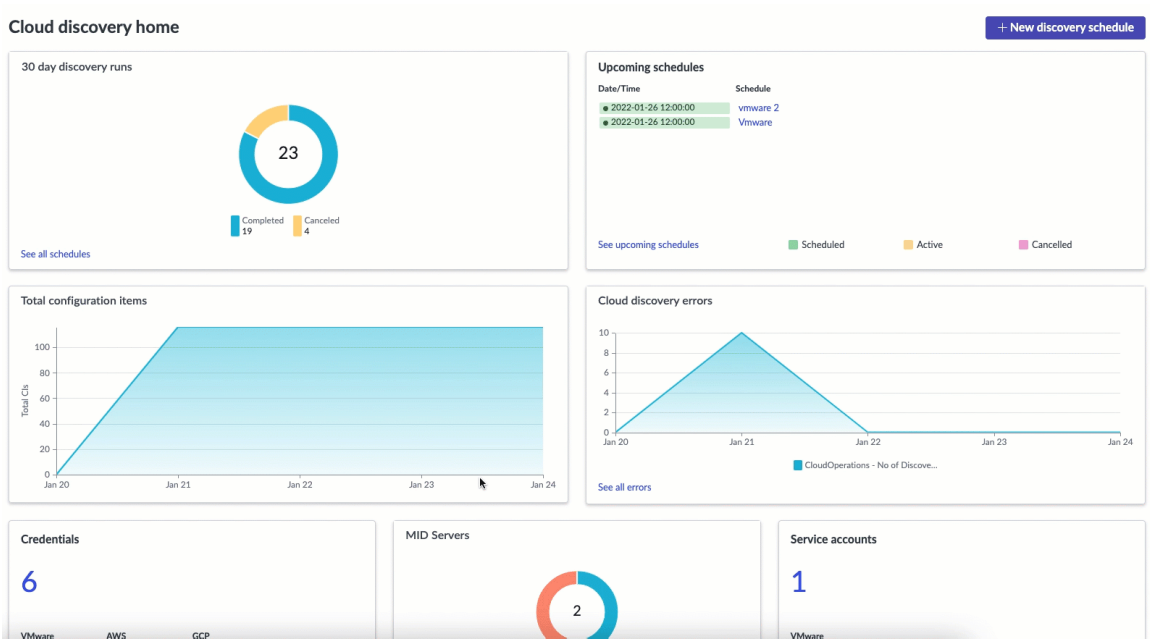
Hinweis: Dies kann Anmeldeinformationen für eine Erkennung einschließen, die geplant, aber nicht zum ersten Mal ausgeführt wurde.

Bericht über nicht verwendete Berechtigungsnachweise



Cloud-Discovery Homepage in Arbeitsbereich für Cloud-Vorgänge

Die Cloud-Discovery-Homepage bietet eine Zusammenfassung der Discovery-Vorgänge, die durch einen Discovery-Zeitplan ausgelöst wurden. Sie können die Anzahl der im Laufe der Zeit erkannten CIs und aufgetretenen Fehler anzeigen. Außerdem können Sie einen beliebigen Dashboard-Bericht auswählen, um zusätzliche Informationen anzuzeigen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Now Platform-Rollen

sn_cloud_ops_ws.cloud_ops_admin

Rufen Sie die Homepage Cloud-Discovery auf

Um das Dashboard zu öffnen, wechseln Sie zu: **Cloud-Discovery-Arbeitsbereich** > **Cloud-Discovery** > **Dashboard**.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
sn_cloud_ops_ws.cloud_ops_admin	Der sn_cloud_ops_ws.cloud_ops_admin kann die folgenden Informationen im Cloud-Discovery-Dashboard überprüfen: • 30-tägige Discovery-Ausführungen • Bevorstehende Zeitpläne • Total configuration items (Gesamte Konfigurationselemente) • Cloud-Discovery-Fehler • Anmeldeinformationen • MID Servers • Servicekonto • Cloud-VMs nach Rechenzentrum

Indikatoren

Anmeldeinformationen

Dieser Indikator zeigt die Gesamtanzahl der im System definierten Anmeldeinformationen und ihre Aufgliederung nach Cloud-Anbieter an.

Wählen Sie die unter einem beliebigen Anmeldeinformationstyp angegebene Nummer aus, um eine gefilterte Liste der übereinstimmenden Anmeldeinformationen anzuzeigen.

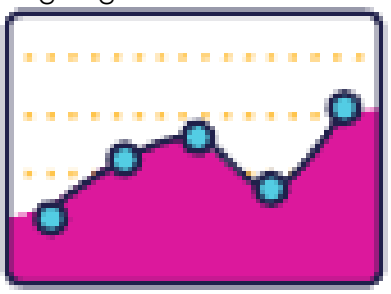
Servicekonten

Dieser Indikator zeigt die Gesamtanzahl der im System definierten Servicekonten und ihre Aufgliederung nach Cloud-Anbieter an.

Wählen Sie die unter einem beliebigen Cloud-Provider angegebene Nummer aus, um eine gefilterte Liste der übereinstimmenden Servicekonten anzuzeigen.

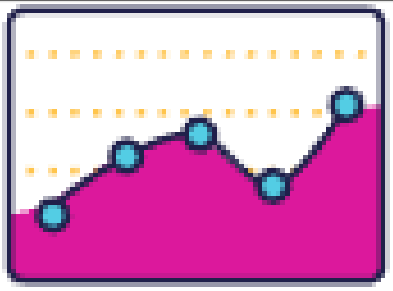
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Discovery-Ausführungen für 30 Tage	Ringdiagramm 	discovery_status	In diesem Beric werden Anzahl Status der Disc Ausführungen i letzten 30 Tage angezeigt. Von Discovery werd folgenden Statu Bericht angeze • Aktiv • Abgebroche • Abgeschlosse Wählen Sie den aus, um die List aller Erkennung anzuzeigen.
Bevorstehende Zeitpläne	Liste	discovery_schedule	In diesem Beric werden Informa über bis zu ach bevorstehende geplante Erken angezeigt. Wählen Sie eine Zeitplan aus, ur Details anzuzeig
Total configuration items (Gesamte Konfigurationselemente)	Linien- und Flächendiagramm	cmdb_ci	In diesem Beric die Anzahl der der Zeit erkannt angezeigt. Wählen Sie den aus, um die List bisher erkannte Konfigurationse anzuzeigen. Sie können einen beliebigen CI-D auswählen, um Informationen z und den zugeh Daten aus meh Quellen anzuze falls verfügbar.
Cloud-Discovery-Fehler	Linien- und Flächendiagramm	discovery_log	In diesem Beric die Anzahl der

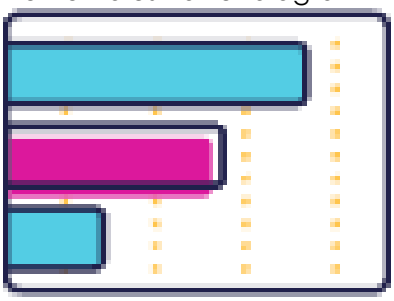
Automatisch übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Discovery-Fehle Zeitverlauf ang Wählen Sie den aus, um die List Cloud-Discover im Discovery-Pr anzuzeigen. Alt können Sie auf Informationen z indem Sie zu na **Diagnose** > **Dis** **Protokoll**.
Anmeldeinformationen	Indikator	discovery_credential	In diesem Beric die Gesamtanz im System defin Anmeldeinform und ihre Aufglie nach Cloud Pro angezeigt. Wählen Sie die einem beliebig Anmeldeinform angegebene Nummer aus, u gefilterte Liste d übereinstimmen Anmeldeinform anzuzeigen.
MID Server verwenden	Ringdiagramm 	ecc_agent	In diesem Beric die Gesamtanz MID Servers und Status angezeig
Servicekonto	Indikator	cmdb_ci_cloud_service_account	In diesem Beric die Gesamtanz im System defin Servicekonten u ihre Aufgliederu nach Cloud Pro angezeigt. Wählen Sie die einem beliebig

Automatisch übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Cloud-Provider angegebene Nummer aus, u gefilterte Liste d übereinstimmer Servicekonten anzuzeigen.
Cloud-VMs nach Rechenzentrum	Horizontales Balkendiagramm 	sn_disco_cd_vm_analytics	In diesem Beric wird die Anzahl pro Rechenzen erkannten VMs angezeigt. Von Cloud-Disc wird dieser Beri nur für Microsof Azure-, Amazon Services (AWS)- vCenter-Reche angezeigt.

Cloud-Discovery Zeitpläne-Dashboard in Arbeitsbereich für Cloud-Vorgänge

Das Zeitplan-Dashboard von Cloud-Discovery zeigt Informationen zur ausgewählten Discovery-Ausführung an.

Erforderliche Now Platform-Rollen

sn_cloud_ops_ws.cloud_ops_admin

Greifen Sie auf das Zeitplan-Dashboard Cloud-Discovery zu

Um das Dashboard zu öffnen, wechseln Sie zu: **Cloud-Discovery-Arbeitsbereich** > **Cloud-Discovery** > **Zeitpläne**.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
sn_cloud_ops_ws.cloud_ops_admin	• Zeigen Sie die Ressourcenanzahl aus den letzten Discovery-Ausführungen an. • Zeigen Sie die für die letzten Discovery-Ausführungen benötigte Zeit an. • Zeigen Sie die Liste der neu erkannten CIs an. • Zeigen Sie die Liste der CIs an, die gegenüber der vorherigen Discovery-Ausführung fehlen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender	Dashboard-Verwendung
	• Zeigen Sie die Anzahl der während der ausgewählten Discovery-Ausführung erkannten CIs an. • Zeigen Sie die Anzahl von Erkennungsfehlern an, die während der ausgewählten Discovery-Ausführung aufgetreten sind.

Indikatoren

Gesamtzahl der Ressourcen

Der Indikator zeigt die Gesamtanzahl der während der ausgewählten Discovery-Ausführung erkannten Configuration Items (CI) an.

Neu erkannt

Der Indikator zeigt die Anzahl der neuen CIs an, die während der ausgewählten Discovery-Ausführung erkannt wurden.

Abwesend vom letzten

Der Indikator zeigt die Anzahl der in der ausgewählten Discovery-Ausführung fehlenden CIs an. Das heißt, CIs wurden während der vorherigen Discovery-Ausführung erkannt, fehlen jedoch in der ausgewählten Discovery-Ausführung.

Fehler

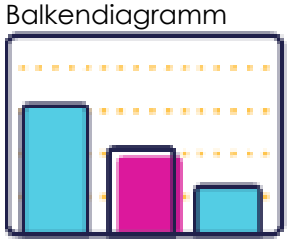
Der Indikator zeigt die Anzahl von Erkennungsfehlern, die während der ausgewählten Discovery-Ausführung aufgetreten sind.

Dauer

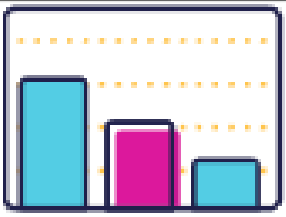
Der Indikator zeigt die Zeit an, die zum Abschließen der ausgewählten Discovery-Ausführung benötigt wurde.

Hinweis: Cloud-Discovery berechnet die Indikatoren **Neu erkannt** und **Abwesend vom letzten** nur für die musterbasierten Erkennungen.

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Ressourcenanzahl laut letzten Discovery-Ausführungen	Balkendiagramm 	discovery_cloud_results	In diesem Bericht wird die Anzahl der CIs angezeigt, die während der letzten 10 Ausführungen des ausgewählten Discovery-Zeitplans erkannt wurden.
Zeit für letzte Discovery-Ausführungen	Balkendiagramm	discovery_status	In diesem Bericht wird die Zeit angezeigt, die die letzten 10 Ausführungen des ausgewählten Discovery-Zeitplans

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			bis zum Abschluss benötigt haben. Dieser Bericht umfasst sowohl abgeschlossene als auch abgebrochene Discovery-Durchläufe.

Filter

Name	Typ	Beschreibung
Zeitplanfilter	Auswahlbasierter Filter	Standardmäßig sind in der Liste alle Cloud-Discovery-Zeitpläne in alphabetischer Reihenfolge aufgeführt, unabhängig vom aktuellen Ausführungsstatus. Verwenden Sie den Zeitplanfilter, um die Cloud-Discovery-Zeitpläne zu filtern. Sie können die Zeitpläne nach Cloud-Provider, Zeitplanname oder beidem filtern. Sie können die gefilterte Liste auch nach einem der folgenden Kriterien sortieren: • **Alphabetisch**: Sortieren Sie die Zeitplannamen alphabetisch. • **Fehler**: Sortieren Sie nach der Anzahl der während der Erkennung aufgetretenen Fehler. • **Discovery wird ausgeführt**: Sortieren Sie nach Status der Erkennung. Wählen Sie nach dem Filtern des Zeitplans die Discovery-Ausführung aus der Dropdown-Liste „Bericht“ aus, um ihre Daten im Zeitplan-Dashboard anzuzeigen, das auf der Registerkarte **Ergebnisse** angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Typ	Beschreibung
		Hinweis: Nur die letzten 10 Discovery-Ausführungen werden in der Dropdown-Liste „Bericht“ angezeigt.

Leistungsmetriken zu Erkennungen

Diese Discovery-Erweiterung sammelt Leistungsmetriken über die Probe-/Muster- und Sensorverarbeitungszeit und aggregiert diese Daten über die Zeit. Sie können Rollup-Daten verwenden, um die Leistung bestimmter Erkennungen zu überwachen oder um die Leistung zwischen Versionen nach einem Upgrade zu vergleichen.

Metriken

Discovery stellt die folgenden einzelnen Leistungsmetriken bereit:

- Probe-Verarbeitungszeit und Musterverarbeitungszeit
- Sensorverarbeitungszeit
- Verarbeitungszeit der Identification and Reconciliation Engine (IRE) für Discovery-Muster. Diese Verarbeitungszeit ist bereits in der Sensorverarbeitungszeit enthalten, wird hier jedoch isoliert, um mehr Einblicke in Identifizierung und Abgleich von Musternutzlasten zu erhalten.

Discovery kann einzelne Metriken für diese Attribute zusammenfassen:

- Builds/Versionen
- Discovery-Status
- Ziel-IP-Adresse

Metrikzusammenfassungen auslösen

Metrik-Rollups werden wie folgt gestartet:

- **Nach Build zusammengefasst**: Implementiert durch die reguläre Aufgabe **Aggregate Discovery Probe And Sensor Metrics By Build (Metriken für Discovery-Probes und -Sensoren nach Build zusammenfassen)**. Diese Aufgabe wird um 02:00 Uhr Ortszeit ausgeführt.
- **Nach Status zusammengefasst**: Implementiert durch die Skriptaktion **Rollup Probe/Sensor Metrics by Status (Rollup-Probe-/Sensormetriken nach Status)**, die durch die registrierten Ereignisse **discovery.complete** und **discovery.cancelled** ausgelöst wird
- **Nach Ziel zusammengefasst**: Implementiert durch die Skriptaktion **Rollup Probe/Sensor Metrics by Target (Rollup-Probe-/Sensormetriken nach Ziel)**, die durch das registrierte Ereignis **discovery.device.complete** ausgelöst wird

Hinweis: Wenn die Discovery-Ausführung abgebrochen wird, bevor sie abgeschlossen ist, kann Discovery die Zusammenfassungstabelle der IP-Zielmetriken nicht aktualisieren. Das liegt daran, dass das Ereignis *`discovery.device.complete`*, das die Zusammenfassung auslöst, nicht ausgeführt wird. IP-Zieldaten für eine unterbrochene Erkennung werden erfasst, wenn nachfolgende Erkennungen erfolgreich auf dem Ziel ausgeführt werden. Das Abbrechen der Discovery-Ausführung wirkt sich nicht auf die Zusammenfassung anderer Metriken aus, die anders ausgelöst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabellen

Discovery-Leistungsmetrikdaten werden in den folgenden Tabellen gespeichert:

Tabelle	Beschreibung
Probe- und Sensormetriken (einzeln) [discovery_perf_metric_probe_sensor]	Speichert die einzelnen Leistungsmetriken für Probe-/Muster-, Sensor- und IRE-Verarbeitungszeiten
Probe- und Sensormetriken (Zusammenfassung) [discovery_perf_metric_probe_sensor_rollup]	Dies ist die Basistabelle der Metrikzusammenfassung. Darin werden keine Daten gespeichert. Die drei Rollup-Tabellen „Nach Build“, „Nach Status“ und „Nach Ziel“ erweitern allesamt diese Tabelle.
Probe- und Sensormetriken (nach Build zusammengefasst) [discovery_perf_metric_probe_sensor_rollup_by_build]	Speichert die zusammengefassten Leistungsmetriken für Probes/Muster, Sensoren und IRE nach Build und Version
Probe- und Sensormetriken (nach Status zusammengefasst) [discovery_perf_metric_probe_sensor_rollup_by_status]	Speichert die zusammengefassten Leistungsmetriken für Probes/Muster, Sensoren und IRE nach Discovery-Status
Probe- und Sensormetriken (nach Ziel zusammengefasst) [discovery_perf_metric_probe_sensor_rollup_by_target]	Speichert die zusammengefassten Leistungsmetriken für Probes/Muster, Sensoren und IRE nach IP-Adresse

Discovery-Eigenschaften

Die Eigenschaften von Leistungsmetriken steuern, ob eine Zusammenfassung erfolgt, aber nicht, welche Daten in der Zusammenfassung enthalten sind. Status- und IP-Zieldaten werden wie folgt erfasst:

- Rollups für Status enthalten immer neue Daten. Discovery erfasst während der Erkennung kontinuierlich Daten für alle Probes und Sensoren für diesen Discovery-Status und speichert sie in der Tabelle „Probe- und Sensormetriken (einzeln)“ [discovery_perf_metric_probe_sensor]. Die Zusammenfassung fasst alle Probe-Daten und Sensordaten für diesen bestimmten Status zusammen, nachdem die Ereignisse *`discovery.cancel`* und *`discovery.complete`* für diesen Status ausgelöst wurden, jedoch nur, wenn die Zusammenfügungseigenschaft für Status-Rollups aktiviert ist.
- Discovery erfasst kontinuierlich Daten für IP-Ziele und speichert sie in der Tabelle „Probe- und Sensormetriken (einzeln)“ [discovery_perf_metric_probe_sensor]. Die Zusammenfassung führt für alle vorhandenen IP-Zieldaten einen Rollup durch, nachdem die Eigenschaft *`glide.discovery.perf.metrics.rollup_by_target`* aktiviert wurde, und erstellt Datensätze in der Tabelle „Probe- und Sensormetriken (nach Ziel zusammengefasst)“ [discovery_perf_metric_probe_sensor_rollup_by_target].

Die folgenden Eigenschaften steuern die Erfassung von Metriken für Probes und Sensoren:

Eigenschaft	Beschreibung
glide.discovery.perf.metrics.enable_collection	Aktiviert die Erfassung von Leistungsmetriken • **Typ**: true | false • **Standard**: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
glide.discovery.perf.metrics.rollup_by_build	Aktiviert die Erfassung einzelner Discovery-Leistungsmetriken in einer Zusammenfassungstabelle, die nach Build gruppiert ist • **Typ**: true | false • **Standard**: true
glide.discovery.perf.metrics.rollup_by_status	Aktiviert die Erfassung einzelner Discovery-Leistungsmetriken in einer Zusammenfassungstabelle, die nach Status gruppiert ist • **Typ**: true | false • **Standardwert:** false
glide.discovery.perf.metrics.rollup_by_target	Aktiviert die Erfassung einzelner Discovery-Leistungsmetriken in einer Zusammenfassungstabelle, die nach Ziel-IP-Adresse gruppiert ist. Standardmäßig erfasst Discovery kontinuierlich einzelne IP-Adressmetriken, auch wenn die Zusammenfassung nach Ziel-IP deaktiviert ist. Wenn Sie die Zusammenfassung für IP-Ziele aktivieren, schließt Discovery alle Zielmetriken in die Zusammenfassungstabelle ein. • **Typ**: true | false • **Standardwert:** false

Discovery-Leistungsmetriken für Probes, Sensoren und Muster anzeigen

Standardmäßig verfolgt Discovery die Leistung einzelner Probes, Sensoren und Muster durch Messung der Verarbeitungszeit. Bei Verwendung von Mustern misst Discovery die Verarbeitungszeit der Identification and Reconciliation Engine (IRE).

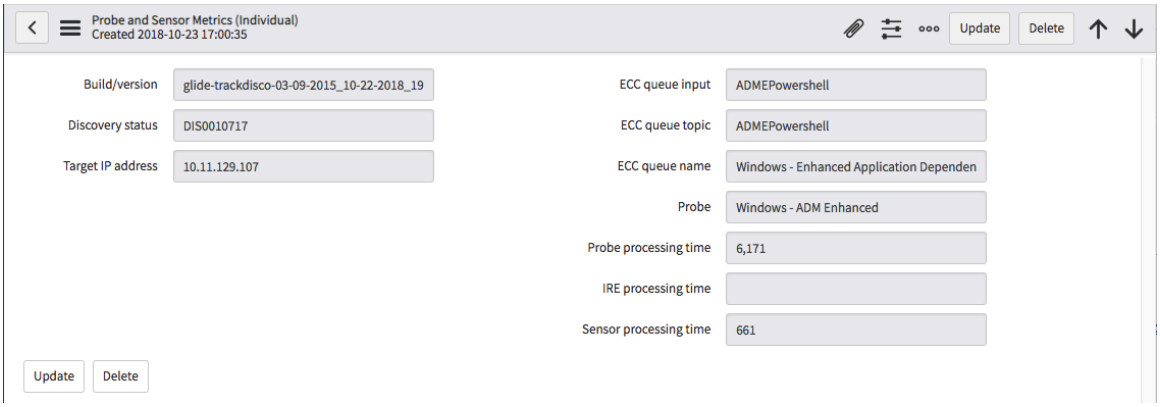
Vorbereitungen

Erforderliche Rolle: discovery_admin, admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery – Performance-Metriken** > **Probe/Sensor (Einzeln)**.
2. Sortieren Sie die Liste nach dem Discovery-Status, um die Liste der Probes und Muster anzuzeigen, die in einer bestimmten Erkennung ausgeführt wurden.
3. Sie können die Metriken für jede Probe, jeden Sensor oder jedes Muster in der Liste anzeigen oder den Datensatz öffnen.
   Alle Metrikdaten für Probes und Sensoren sind schreibgeschützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Das Formular „Probe- und Sensormetriken (einzeln)“ enthält folgende Felder:

Feldbezeichnung	Feldname	Beschreibung
Build/Version	build_version	Build, in dem die Erkennung ausgeführt wurde
Discovery-Status	discovery_status	ID-Nummer des Discovery-Status, von dem die Metriken erfasst wurden
Ziel-IP-Adresse	target_ip	IP-Adresse des Ziels für diese Erkennung
Eingabe für ECC-Warteschlange	ecc_queue_input	Identifiziert einen bestimmten ECC-Eingabedatensatz in der ECC-Warteschlangentabelle
ECC-Warteschlangenthema*	ecc_queue_topic	Identifiziert die Java-Klasse auf dem MID Server, der die Probe ausführt
ECC-Warteschlangenname*	ecc_queue_name	Identifiziert die Probe/ das Muster, deren/ dessen Leistung durch diese Zusammenfassung ausgewertet wurde
Probe*	probe	Name der für diese Erkennung verwendeten Probe
Probe-Verarbeitungszeit	probe_time	Interaktionszeit des MID Servers mit dem Ziel, einschließlich Erstellung der Nutzlast, die an die Instanz zurückgesendet wird. Die Zeit wird in Millisekunden angegeben.
IRE-Verarbeitungszeit	ire_time	Zeit, die für die Verarbeitung der Musternutzlast für die Instanz durch die Identification and Reconciliation Engine (IRE)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbezeichnung	Feldname	Beschreibung
		erforderlich ist. Die IRE-Zeit ist nützlich, da sie den Teil der vom Muster verwendeten Sensorzeit anzeigt. Die Zeit wird in Millisekunden angegeben.
Sensorverarbeitungszeit	sensor_time	Zeit, die der Sensor zur Verarbeitung der Nutzlast für die Instanz für eine Erkennung benötigt hat. Die Zeit wird in Millisekunden angegeben.

*Wird zur eindeutigen Identifizierung einer Probe/eines Musters und des zugehörigen Sensors beim Erfassen von Metriken für eine Erkennung verwendet

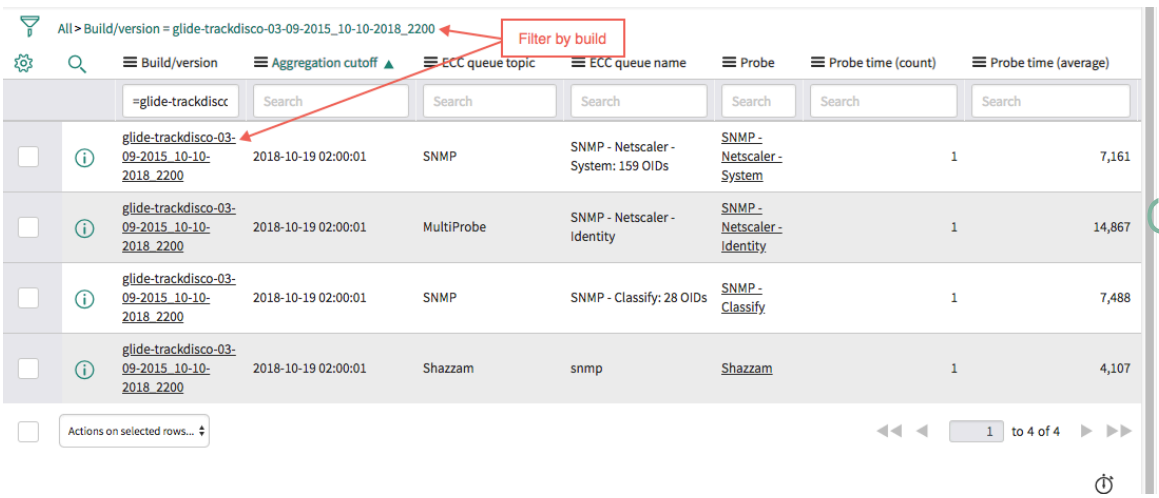
Nach Build zusammengefasste Discovery-Leistungsmetriken anzeigen

Verwenden Sie die Rollup-Daten nach Build, um sicherzustellen, dass die Verarbeitungszeiten für Discovery-Komponenten für Erkennungen in einem 24-Stunden-Zeitraum konsistent bleiben. Zeigen Sie zusammengefasste Build-Daten vor und nach einem Upgrade an, um die Leistung der alten und der neuen Version zu vergleichen. Alle zusammengefassten Leistungsdaten sind schreibgeschützt.

Vorbereitungen
Erforderliche Rolle: discovery_admin, admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery – Performance-Metriken** > **Probe/Sensor (Rollup nach Build)**.
2. Sortieren Sie die Liste nach **Build/Version**.



3. Filtern Sie nach einem bestimmten Build, um die zusammengefassten Verarbeitungszeiten für die Probes und Muster anzuzeigen, die eine Erkennung für diesen Build durchgeführt haben.
4. Öffnen Sie einen Datensatz, um die Statistiken für Probes/Muster für den ausgewählten Build anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Formular zeigt zusätzliche Felder an, die in der Liste nicht sichtbar sind. Rollup-Berechnungen beziehen sich auf einen 24-Stunden-Zeitraum und beginnen jede Nacht um 02:00 Uhr.

5. Beschreibungen zusätzlicher Metriken, die im Formular für Rollups nach Build angezeigt werden, finden Sie in der Tabelle mit Daten zu Leistungszusammenfassungen.

Nach Status zusammengefasste Discovery-Leistungsmetriken anzeigen

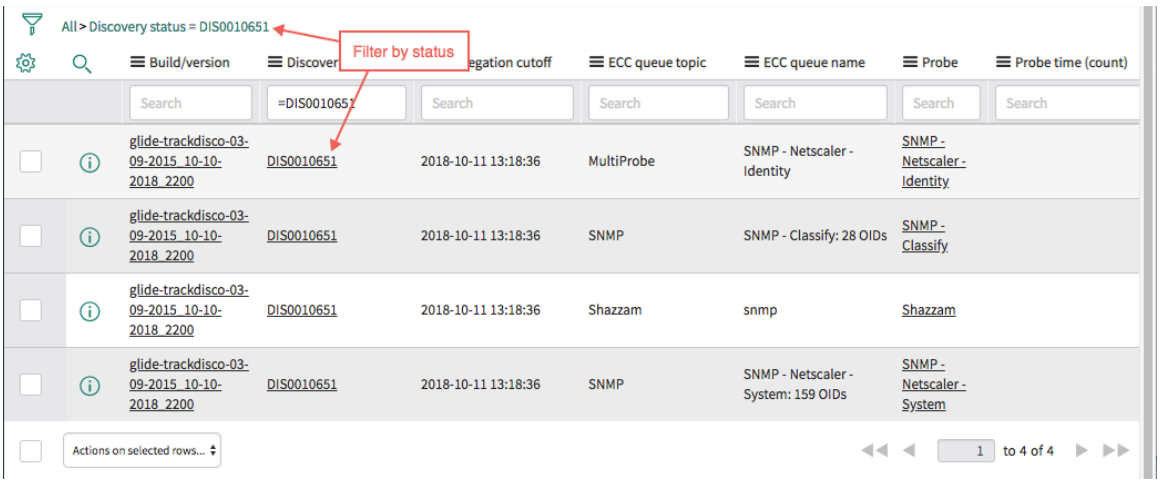
Verwenden Sie die Rollup-Daten nach Status, um sicherzustellen, dass die Verarbeitungszeiten für Probes, Muster und Sensoren für eine bestimmte Erkennung konsistent bleiben. Alle zusammengefassten Leistungsdaten sind schreibgeschützt.

Vorbereitungen
Erforderliche Rolle: discovery_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery – Performance-Metriken** > **Probe/Sensor (Rollup nach Status)**.
2. Sortieren Sie die Liste nach **Discovery-Status**, um die zusammengefassten Verarbeitungszeiten für die Probes und Muster anzuzeigen, die in einer bestimmten Erkennung ausgeführt wurden.



3. Filtern Sie nach einem bestimmten Status, um für in diesem Status ausgeführte Probes und Muster verfügbare Metriken anzuzeigen.
4. Öffnen Sie einen Datensatz, um die Statistiken für Probes/Muster für den ausgewählten Status anzuzeigen.
   Das Formular zeigt zusätzliche Felder an, die in der Liste nicht sichtbar sind. Rollups werden nur für den Status „Abgeschlossen“ oder „Abgebrochen“ erstellt.
5. Beschreibungen zusätzlicher Metriken, die im Formular für Rollups nach Status angezeigt werden, finden Sie in der Tabelle mit Daten zu Leistungszusammenfassungen.

Nach IP-Adresse zusammengefasste Discovery-Leistungsmetriken anzeigen

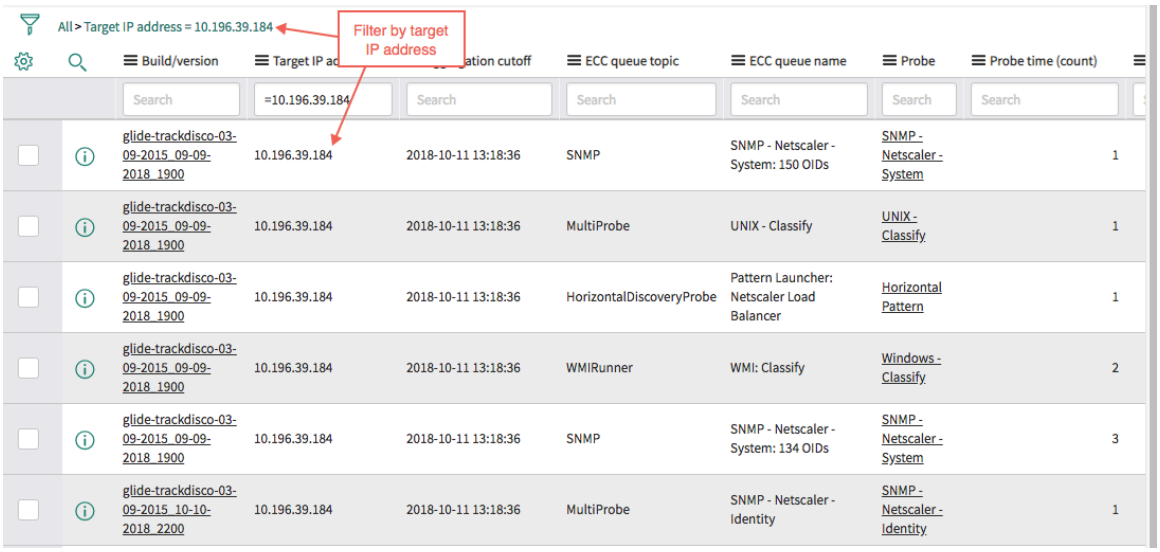
Verwenden Sie die Rollup-Daten nach Ziel, um sicherzustellen, dass die Verarbeitungszeiten für Probes, Muster und Sensoren für jede Erkennung einer bestimmten IP-Adresse konsistent bleiben. Alle zusammengefassten Leistungsdaten sind schreibgeschützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: discovery_admin, admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Discovery – Performance-Metriken** > **Probe/Sensor (Rollup nach Ziel)**.
2. Sortieren Sie die Liste nach **Ziel-IP-Adresse**.



3. Filtern Sie nach einer bestimmten IP-Adresse, um die zusammengefassten Verarbeitungszeiten für die Probes und Muster anzuzeigen, die eine Erkennung für diese IP-Adresse durchgeführt haben.
4. Öffnen Sie einen Datensatz, um die Statistiken für die/das ausgewählte Probe/Muster für die spezifische IP-Adresse anzuzeigen.
   Das Formular zeigt zusätzliche Felder an, die in der Liste nicht sichtbar sind. Rollups werden durchgeführt, nachdem IP Discovery erfolgreich abgeschlossen wurde.
5. Beschreibungen zusätzlicher Metriken, die im Formular für Rollups nach Ziel angezeigt werden, finden Sie in der Tabelle mit Daten zu Leistungszusammenfassungen.

Zusammengefasste Daten für Discovery-Leistungsmetriken

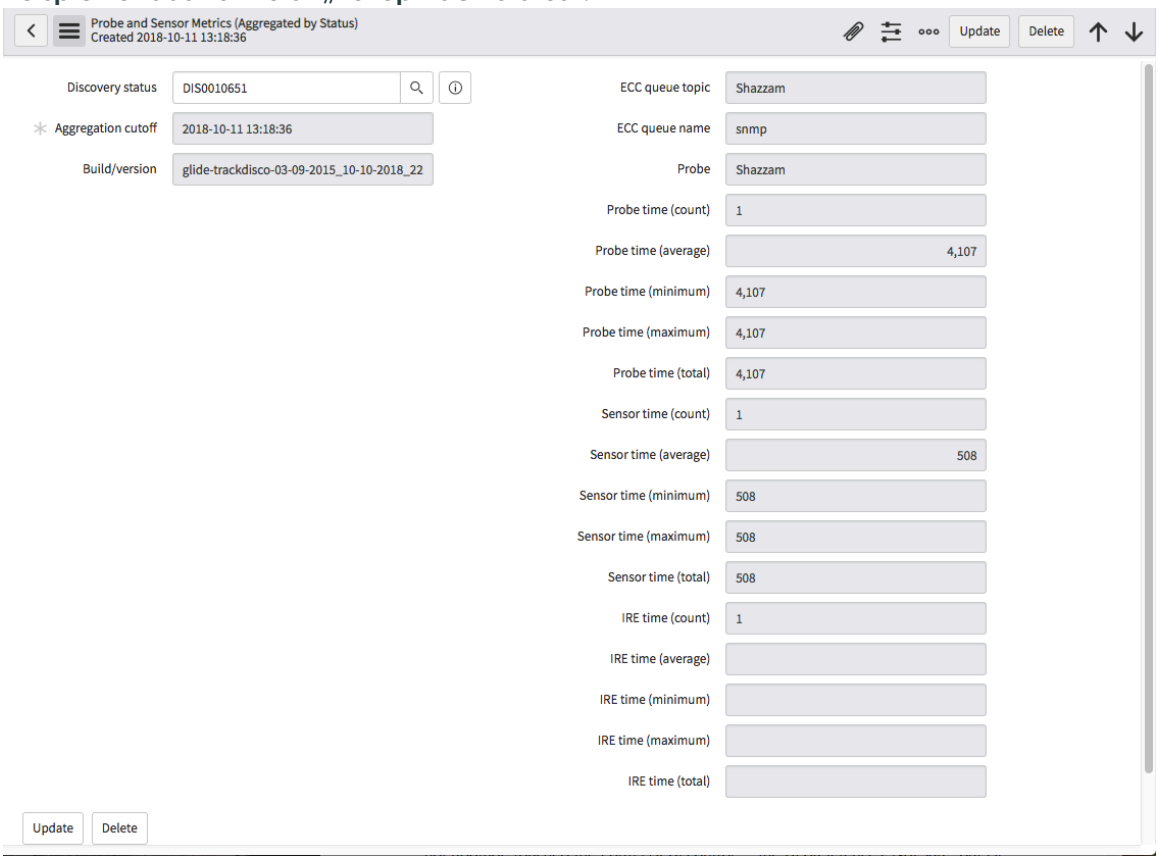
Discovery-Leistungsmetriken können bei jeder Discovery-Ausführung Daten für Probes, Muster und Sensoren zusammentragen. Discovery berechnet die Verarbeitungszeiten und erhöht die Anzahl der Ausführungen einer Komponente für jedes Rollup-Profil: Status, Ziel oder Build. Alle zusammengefassten Leistungsdaten sind schreibgeschützt.

Beispiel für Rollup-Formular

Dies ist ein Beispiel für einen Zusammenfassungsdatensatz für Metriken über Probes und Sensoren. Die hier angezeigten Metrikfelder werden für jede Zusammenfassung verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für das Formular „Rollup nach Status“.



Zusammengefasste Daten für Leistungs-Framework

Sofern nicht anders angegeben, gelten diese Felder für alle Zusammenfassungsdatensätze.

Feldbezeichnung	Feldname	Beschreibung
Build/Version	build_version	Der Name des Build, der auf der Instanz ausgeführt wird. Dieser Name identifiziert Version, Patch-Ebene und Release-Datum von ServiceNow Platform.
Discovery-Status	discovery_status	ID-Nummer des Discovery-Statusdatensatzes für diese Zusammenfassung **Hinweis:** Dieses Feld wird nur im Formular für Rollups nach Status angezeigt.
Ziel-IP-Adresse	target_ip_address	IP-Adresse des Ziels für diese Erkennung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbezeichnung	Feldname	Beschreibung
		Hinweis: Dieses Feld wird nur im Formular für Rollups nach Ziel angezeigt.
Ende der Zusammenfassung	aggregation_cutoff	Der Endzeitpunkt variiert je nach Rollup-Profil. • **Nach Build**: Standardmäßig täglich um 02:00 Uhr • **Nach Status**: Abschlusszeit der letzten Zusammenfassung für diesen Discovery-Status, der möglicherweise ausgeführt wurde, als **discovery.complete** oder **discovery.cancelled** für diesen Status ausgeführt wurde • **Nach Ziel**: Abschlusszeit der letzten Zusammenfassung für diese Ziel-IP-Adresse, die möglicherweise ausgeführt wurde, als **discovery.device.complete** für diese IP-Adresse ausgeführt wurde
ECC-Warteschlangenthema*	ecc_queue_topic	Identifiziert die Java-Klasse auf dem MID Server, der die Probe ausführt
ECC-Warteschlangenname*	ecc_queue_name	Identifiziert die Probe/ das Muster, deren/ dessen Leistung durch diese Zusammenfassung ausgewertet wurde
Probe*	probe	Name der für diese Erkennung verwendeten Probe
Probe-Zeit (Anzahl)	probe_time_count	Anzahl der Ausführungen einer Probe für ein bestimmtes Rollup-Profil
Probe-Zeit (Durchschnitt)	probe_time_average	Durchschnittliche Zeit, die eine Probe benötigt hat, um Daten zu einem Ziel zu sammeln und die Nutzlast für ein bestimmtes Rollup-Profil zu formatieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbezeichnung	Feldname	Beschreibung
Probe-Zeit (Minimum)	probe_time_min	Minimale Zeit, die eine Probe benötigt hat, um Daten zu einem Ziel zu sammeln und die Nutzlast für ein bestimmtes Rollup-Profil zu formatieren
Probe-Zeit (Maximum)	probe_time_max	Maximale Zeit, die eine Probe benötigt hat, um Daten zu einem Ziel zu sammeln und die Nutzlast für ein bestimmtes Rollup-Profil zu formatieren
Probe-Zeit (gesamt)	probe_time_total	Gesamtzeit, die eine Probe benötigt hat, um Daten zu einem Ziel zu sammeln und die Nutzlast für ein bestimmtes Rollup-Profil zu formatieren
Sensorzeit (Anzahl)	sensor_time_count	Anzahl der Verarbeitungen von Nutzlasten durch einen Sensor für ein bestimmtes Rollup-Profil
Sensorzeit (Durchschnitt)	sensor_time_average	Durchschnittliche Zeit, die ein Sensor für die Verarbeitung von Nutzlasten auf der Instanz für ein bestimmtes Rollup-Profil benötigt hat
Sensorzeit (Minimum)	sensor_time_min	Minimale Zeit, die ein Sensor für die Verarbeitung von Nutzlasten auf der Instanz für ein bestimmtes Rollup-Profil benötigt hat
Sensorzeit (Maximum)	sensor_time_max	Maximale Zeit, die ein Sensor für die Verarbeitung von Nutzlasten auf der Instanz für ein bestimmtes Rollup-Profil benötigt hat
Sensorzeit (gesamt)	sensor_time_total	Gesamtzeit, die ein Sensor für die Verarbeitung von Nutzlasten auf der Instanz für ein bestimmtes Rollup-Profil benötigt hat
IRE-Zeit (Anzahl)	ire_time_count	Anzahl der Verarbeitungen der Nutzlast eines Musters durch die Identification and Reconciliation Engine (IRE) für ein bestimmtes Rollup-Profil
IRE-Zeit (Durchschnitt)	ire_time_average	Durchschnittliche Zeit, die die IRE für die Verarbeitung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbezeichnung	Feldname	Beschreibung
		der Nutzlast eines Musters für ein bestimmtes Rollup-Profil benötigt hat
IRE-Zeit (Minimum)	ire_time_min	Minimale Zeit, die die IRE für die Verarbeitung der Nutzlast eines Musters für ein bestimmtes Rollup-Profil benötigt hat
IRE-Zeit (Maximum)	ire_time_max	Maximale Zeit, die die IRE für die Verarbeitung der Nutzlast eines Musters für ein bestimmtes Rollup-Profil benötigt hat
IRE-Zeit (gesamt)	ire_time_total	Gesamtzeit, die die IRE für die Verarbeitung der Nutzlast eines Musters für ein bestimmtes Rollup-Profil benötigt hat

* Zusammen identifizieren diese Werte eindeutig ein für eine Erkennung verwendetes Probe/Sensor-Paar (eine „Probe-Ausführung“).

Discovery-Fehlermeldungen

Im System werden Fehlermeldungen und Warnungen dokumentiert, damit Benutzer Probleme erkennen und Maßnahmen ergreifen können, um diese zu beheben.

Allgemeine Fehlermeldungen

Eingabe-/Ausgabefehler

- CONNECTION_FAILED
- CONNECTION_TIMEOUT
- CONNECTION_REFUSED
- CONNECTION_CIPHER_UNSUPPORTED
- CONNECTION_PROTOCOL_UNSUPPORTED
- CONNECTION_LOST
- INVALID_CONNECTION_PARAMETER
- FILE_NOT_FOUND
- IO_ERROR

Authentifizierungsfehler

- NO_CREDENTIALS
- AUTHENTICATION_FAILED
- INVALID_CREDENTIALS_TYPE

SSH-Fehler

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- SSH_SHELL_UNSUPPORTED
- SSH_SCRIPT_TRANSFER_FAILED
- SSH_INVALID_SESSION

Windows-Fehler

POWER_SHELL_VERSION_UNSUPPORTED

Befehlsfehler

- COMMAND_TIMEOUT
- INVALID_COMMAND
- COMMAND_FILTER_ERROR
- COMMAND_PARSER_ERROR
- COMMAND_KEY_MAPPER_ERROR
- COMMAND_VALUE_NORMALIZER_ERROR
- TERMINAL_SESSION_LOST_ERROR
- TERMINAL_SESSION_ENVIRONMENT_MODIFICATION_ERROR

Generische Komponentenfehler

- INVALID_COMPONENT
- INVALID_COMPONENT_PARAMETER
- INVALID_OPERATION

Allgemeine Fehlermeldungen

Nachricht: org.xml.sax.SAXParseException: The entity name must immediately follow the '&' in the entity reference

Eine Version dieser Nachricht wird angezeigt, wenn Sie Sonderzeichen in einem Passwort verwendet haben, das in einer XML-Datei gespeichert ist.

Nachricht: Identified, ignored extra IP

Diese Nachricht kann am Ende der Klassifizierungsphase von Discovery angezeigt werden, wenn eine Ziel-IP-Adresse zu einem Gerät gehört, das gleichzeitig erkannt wird.

Beispiel: Ein Windows-Server verfügt über zwei NIC-Karten mit zwei IP-Adressen. Beide IP-Adressen liegen im selben Erkennungszeitplan innerhalb des Zielbereichs von Discovery. Diese Nachricht wird generiert, um darauf hinzuweisen, dass die zweite IP-Adresse ignoriert wird, da dasselbe CI innerhalb einer Discovery-Ausführung nicht zweimal aktualisiert werden soll.

Diese Nachricht ist eine zu erwartende Warnung. Es ist keine Aktion erforderlich.

Nachricht: Authentication failures

Der Erkennungsprozess konnte das CI nicht erkennen, da die Erkennungsanwendung nicht authentifiziert werden konnte. Um diesen Fehler zu beheben, fügen Sie der Tabelle „Discovery-Anmeldeinformationen“ die Anmeldeinformationen dieses Computers hinzu.

Nachricht: Identified, not updating CI, now finished

Keine Übereinstimmung mit einem der CI-Bezeichner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachricht: The impersonation of user failed

Diese Nachricht stammt aus der PowerShell. Überprüfen Sie, ob die Domäne zusammen mit dem Benutzernamen in den Anmeldeinformationen angegeben ist.

Nachricht: Connection failed to WMI service. Error: Permission denied

Diese Nachricht stammt aus WMI. Überprüfen Sie, ob der MID-Server-Service mit den richtigen Anmeldeinformationen ausgeführt wird und Zugriff auf das Zielgerät hat.

Um dies zu überprüfen, führen Sie auf dem MID-Server-Host in der Eingabeaufforderung den folgenden Befehl aus:

```
wmic /node:target /user:user /password:password path
 win32_operatingsystem
target = IP address of target device
user = user account used by the mid server service
password = password used by the mid server service
```

Nachricht: Connection failed to WMI service. Error: The remote server machine does not exist or is unavailable

Diese Nachricht stammt aus WMI. Überprüfen Sie, ob das MID-Server-Servicekonto Zugriff auf den Zielcomputer hat. Überprüfen Sie, ob als MID-Server-Servicekonto ein Domänenadministratorkonto verwendet wird. Überprüfen Sie, ob vorhandene Firewalls für die Verbindung geöffnet sind. Um dies zu überprüfen, führen Sie auf dem MID-Server-Host in der Eingabeaufforderung den folgenden Befehl aus:

Führen Sie ihn aus für runner_type = WMI:

```
wmic /node:"<target>" /user:"<user>" /password:"<password>"
 path win32_operatingsystem
From within a Powershell console on the mid server host,
 execute for runner_type=Powershell:
gwmi win32_operatingsystem -computer <ip> -credential
 '<username>'
```

Nachricht: Provider is not capable of the attempted operation

Das WMI-Repository wurde beschädigt. Durch Befolgen der Anweisungen im Artikel „WMI: Repository Corruption, or Not?“ (WMI: Beschädigung des Repository: ja oder nein?) auf der Microsoft TechNet-Website lässt sich das Problem beheben.

Nachricht: The result file can't be fetched because it doesn't exist

PRB581515 - Powershell does not work when customer has locked down write rights to admin share (Powershell funktioniert nicht, wenn der Kunde Schreibrechte für Administratorfreigabe gesperrt hat)

Nachricht: Please run sneep as root to ensure correct serial number from fserial data source

Damit die Probe „Solaris - Serial Number“ ordnungsgemäß funktioniert, muss das Oracle-Befehlszeilentool **Sneep** installiert sein. Es gibt eine bekannte Einschränkung bei Fujitsu PRIMEPOWER-Geräten. Um diese Einschränkung zu umgehen, führen Sie die Solaris-Erkennung mit Root-Anmeldeinformationen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Fehlermeldungen für Sensoren

Nachricht: The multisensor will not process because its major version = X while probe_name responding script's major version = Y

Fehlermeldungen dieser Art weisen darauf hin, dass die Hauptversion nicht übereinstimmt.

Nachricht: The multisensor will not process because its responding script's major version = X while its referenced probe probe_name major version = Y

Fehlermeldungen dieser Art weisen darauf hin, dass die Hauptversion nicht übereinstimmt.

Nachricht: sensor_name sensor's major version = X while its related probe's major version = Y

Fehlermeldungen dieser Art weisen darauf hin, dass bei den Versionen von Probe und Sensor ein schwerwiegender Versionskonflikt besteht und der Sensor die Verarbeitung anhält, bis diese Bedingung behoben ist.

Message: sensor_name multisensor's minor version = X while probe_name responding script's minor version = Y

Fehlermeldungen dieser Art weisen darauf hin, dass die Nebenversion nicht übereinstimmt.

Nachricht: sensor_name multisensor's responding script's minor version = X while its referenced probe probe_name minor version = Y

Fehlermeldungen dieser Art weisen darauf hin, dass die Nebenversion nicht übereinstimmt.

Nachricht: sensor_name sensor's minor version = X while its related probe's minor version = Y

Fehlermeldungen dieser Art weisen darauf hin, dass bei den Versionen von Probe und Sensor ein geringfügiger Versionskonflikt besteht Die Verarbeitung wird fortgesetzt, Sie sollten diesen Zustand allerdings beheben.

Nachricht: Message: Sensor error when processing . . . : No sensors defined

Jede aktive Probe sucht nach einem entsprechenden Sensor, um die von der Probe erfassten Daten zu verarbeiten. Die Nachricht „No sensors defined (Keine Sensoren definiert)“ gibt an, dass der entsprechende Sensor für die Probe fehlt oder inaktiv ist.

Nachricht: Message: Sensor error when processing . . . : typeError: . . .

Diese type-Fehlermeldung weist darauf hin, dass der Sensor einen der wichtigsten Fehlerkonstruktoren in JavaScript besitzt.

Nachricht: Message: Sensor error when processing ...: Exception while processing sensor: XML Parse Problem: ![CDATA]

Dieser XML-Analysefehler tritt auf, wenn der Discovery-Sensor die Nutzlast der ECC-Eingabewarteschlange nicht analysieren kann. Die Nutzlast ist nicht gemäß XML-Spezifikationen formatiert. Mögliche Lösungen:

- Verwenden Sie für problematische Zeichen Maskierungszeichen. Ändern Sie beispielsweise **<** in **&lt** und **&** in **&amp**.
- Verwenden Sie Maskierungszeichen für ganze Textblöcke mit CDATA-Abschnitten oder Codierungsdeklarationen am Anfang des Texts.
- Entfernen Sie alle Leerzeichen (Leerzeichen, Tabulatorzeichen, Zeilenumbrüche) vor XML-Deklarationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachricht: Message: Sensor error when processing Linux - Network ARP Tables: Exception while running probe post processing script: No XML data

Das System zeigt den Fehler „No XML data (Keine XML-Daten)“ an, wenn der XML-Sensorprozessor in der Probe-Ausgabe nicht die erwarteten XML-Daten findet. Während der Sensorverarbeitung versucht Discovery, die Probe-Ergebnisse abzurufen, die Probe-Ausgabe ist jedoch leer. Prüfen Sie, ob die Probe die richtige Ausgabe für die Verarbeitung durch den Sensor zurückgibt.

Nachricht: Message: Sensor error when processing Shazzam: Exception while running probe post processing script: Probe not found: null

Der Fehler „Probe not found (Probe nicht gefunden)“ tritt auf, wenn der Sensorprozessor den vermeintlich mit dem Sensor verknüpften Probe-Datensatz nicht findet. Während der Sensorverarbeitung ruft Discovery den Probe-Datensatz aus dem Probe-Cache ab und speichert ihn zur späteren Referenz. Der Fehler „Probe not found (Probe nicht gefunden)“ tritt auf, wenn die sys_id der Probe nicht gefunden werden kann oder wenn ein Problem mit dem Probe-Cache vorliegt.

Weitere Informationen finden Sie unter Nach Ursache für Fehler „Probe not found (Probe nicht gefunden)“ suchen.

Suche nach der Ursache einer Sensorfehlermeldung

Verwenden Sie dieses Verfahren, um einen Discovery-Sensorfehler zu identifizieren.

Vorbereitungen

Erforderliche Rolle: admin oder sn_cloud_ops_ws.cloud_ops_admin

Warum und wann dieser Vorgang ausgeführt wird

Für diesen Prozess müssen Sie Folgendes identifizieren:

- Den Fehler
- Den Namen des Sensors, bei dem der Fehler aufgetreten ist
- Den Datumsstempel des Fehlers
- Den zugeordneten Stack Trace des Fehlers

Prozedur

1. Führen Sie je nach verwendeter Anwendung eine der folgenden Aktionen aus:
   - Um das **Discovery-Protokoll** in Arbeitsbereich für Cloud-Vorgängeanzuzeigen, navigieren Sie zu **Cloud-Discovery-Arbeitsbereich** > **Cloud-Discovery** > **Discovery-Protokoll**.
   - Um das **Discovery-Protokoll** in Discoveryanzuzeigen, navigieren Sie zu **Alle** > **Discovery** > **Discovery-Protokoll**.
2. Um den Fehler zu finden, filtern Sie nach dem **Ebenennamen** des **Fehlers**.
   Wenn Sie Discovery verwenden, können Sie auch den Fehler und den Datumsstempel im Fehlerbericht anzeigen. Der Bericht ist im Discovery-Dashboard verfügbar.
3. Beachten Sie das Feld **Erstellt** im Fehlerdatensatz.
   Dieser Zeitstempel wird verwendet, um den richtigen Stack Trace zu finden.
4. Beachten Sie das Feld **Kurznachricht** im Fehlerdatensatz.
   Dieses Feld zeigt den Namen des Sensors, bei dem der Fehler aufgetreten ist.
5. Um den Stack Trace zu finden, navigieren Sie zu **Systemprotokolle** > **Fehler**.
6. Suchen Sie nach dem Datum und der Uhrzeit, die dem Wert im Feld **Erstellt** des Fehlerdatensatzes im Discovery-Protokoll entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Das Feld **Nachricht** dieses Eintrags enthält den vollständigen Stack Trace des Fehlers. Der Stack Trace enthält die Fehlermeldung, die sys_id des Skripts und die Nummer der Zeile, in der der Fehler aufgetreten ist.
8. Nachdem Sie die Fehlerdetails ermittelt haben, können Sie die JavaScript-Datei reparieren.

Ursache der Fehlermeldung „No Sensor Defined (Kein Sensor definiert)“ identifizieren

Jede aktive Probe sucht nach einem entsprechenden Sensor, um die von der Probe erfassten Daten zu verarbeiten. Die Nachricht „No Sensors Defined (Keine Sensoren definiert)“ gibt an, dass der entsprechende Sensor für die Probe fehlt oder inaktiv ist.

Vorbereitungen
Erforderliche Rolle: admin oder sn_cloud_ops_ws.cloud_ops_admin

Warum und wann dieser Vorgang ausgeführt wird
Um die Ursache für diesen Fehler zu finden, identifizieren Sie das Feld **Kurznachricht** des Fehlerdatensatzes. Dieses Feld zeigt den Namen der Probe an, für die der Sensor fehlt.

Prozedur
1. Führen Sie je nach verwendeter Anwendung eine der folgenden Aktionen aus:
   - Um die Ursache des Fehlers mithilfe von Arbeitsbereich für Cloud-Vorgängezu identifizieren, navigieren Sie zu **Cloud-Discovery-Arbeitsbereich** > **Cloud-Discovery** > **Diagnose** > **Discovery-Protokoll**.
   - Um die Ursache des Fehlers mithilfe von Discoveryzu identifizieren, navigieren Sie zu **Alle** > **Discovery** > **Ausgabe und Artefakte** > **Discovery-Protokoll**.
2. Filtern Sie nach dem **Ebenennamen** des **Fehlers**.
   Wenn Sie Discovery verwenden, finden Sie den Fehlerbericht auch im Discovery-Dashboard.
3. Beachten Sie das Feld **Kurznachricht** im Fehlerdatensatz.
   Dieses Feld zeigt den Namen des Sensors an. In diesem Beispiel ist der Sensorfehler aufgetreten, als die Shazzam-Probe das Vorhandensein des Shazzam-Sensors überprüft hat.

Ursache einer Sensorfehlermeldung beheben

Zum Beheben einer Discovery-Sensorfehlermeldung müssen Sie die JavaScript-Datei korrigieren, die den Code enthält, der den Fehler generiert hat.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
So korrigieren Sie die JavaScript-Datei:

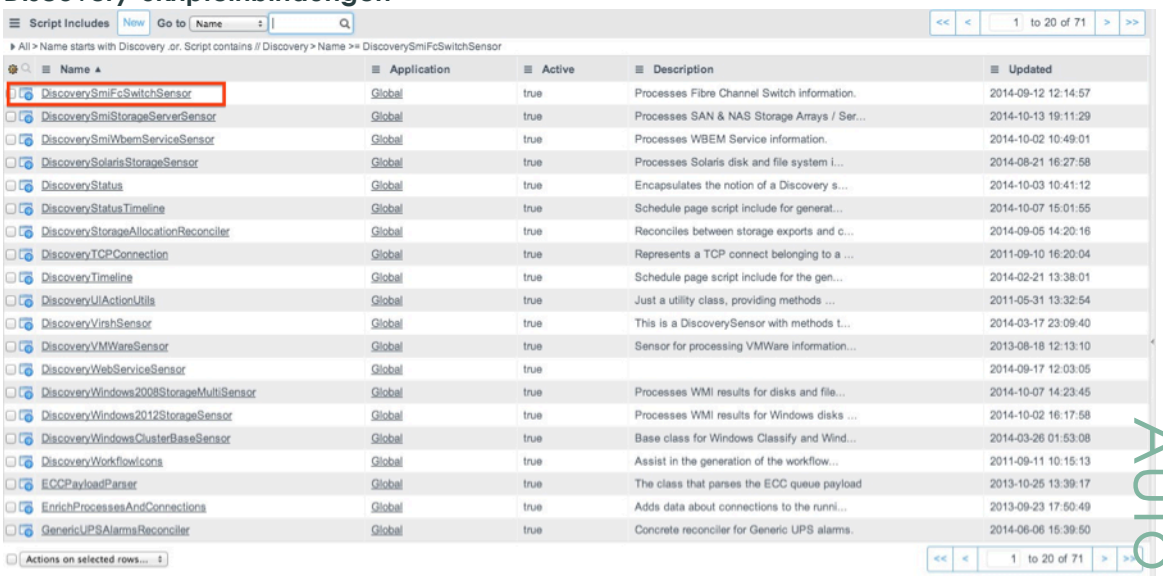
Prozedur
1. Navigieren Sie in Discovery zu dem Modul, in dem der Fehler aufgetreten ist.

   In diesem Beispiel navigieren Sie zu **Discovery-Definition** > **Skripteinbindungen**.
2. Korrigieren Sie den Fehler.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. In diesem Beispiel suchen Sie nach DiscoverySmiFcSwitchSensor im Feld **Name**.

Discovery-Skripteinbindungen



b. Klicken Sie auf den Link, um zur Detailseite für diese Skripteinbindung zu wechseln.

c. Ändern Sie das JavaScript-Skript auf dieser Seite, um den angegebenen Fehler zu beheben.

d. Klicken Sie auf **Aktualisieren**.

Nach Ursache für Fehler „Probe not found (Probe nicht gefunden)“ suchen

Überprüfen Sie die korrekte sys_id der Probe, die dem Parameter *probe* in der Nutzlast des Datensatzes für die ECC-Warteschlangeneingabe zugeordnet ist.

Vorbereitungen

Erforderliche Rolle: discovery_admin, admin

Prozedur

1. Notieren Sie sich die sys_id der Probe, die in der Nutzlast der ECC-Warteschlange angezeigt wird.

Nutzlastbeispiel für ECC-Warteschlange

```
▼<parameters>
   <parameter name="port" value="22"/>
   <parameter name="probe" value="10e0eebd0a0a0b4f61f46a5027df7fb6"/>
   <parameter name="priority" value="0"/>
   <parameter name="use_class" value="discovery_classy_unix"/>
```

2. Navigieren zu **Discovery-Definition** > **Probes** und öffnen Sie den Datensatz für die Probe, die Sie überprüfen möchten.
3. Klicken Sie mit der rechten Maustaste auf den Header des Datensatzes.
4. Wählen Sie im Kontextmenü **sys_id kopieren**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befolgen Sie die Anweisungen des Browsers, um die sys_id zu kopieren, falls die Sicherheitsmaßnahmen des Browsers diese Funktion einschränken.

5. Vergleichen Sie diesen Wert mit der sys_id der Probe aus der Nutzlast.
   Wenn die sys_id des Probe-Datensatzes nicht mit dem Wert in der Nutzlast übereinstimmt, versuchen Sie, die Ursache für den falschen Wert zu ermitteln.

Cloud-Discovery-Fehler in Arbeitsbereich für Cloud-Vorgänge beheben

Zeigen Sie die während der Erkennung aufgetretenen Cloud-Discovery-Fehler an und beheben Sie sie. Sie können die Fehler für alle Cloud-Discovery-Ausführungen oder eine einzelne Cloud-Discovery-Ausführung anzeigen.

Vorbereitungen

Erforderliche Rolle: sn_cloud_ops_ws.cloud_ops_admin

Prozedur

1. Navigieren zu **Cloud-Discovery-Arbeitsbereich** > **Cloud-Discovery**.
2. Wählen Sie **Fehler** aus.
   Die Registerkarte **Status** des Moduls „Zeitpläne“ zeigt die Liste der Fehler für die ausgewählte Discovery-Ausführung an.
3. Wählen Sie eine Kategoriekachel aus, um die spezifischen Fehlercodes anzuzeigen, die in dieser Kategorie aufgetreten sind.
4. Wählen Sie die Kachel für den Fehlercode aus, den Sie untersuchen möchten.
   In der Liste werden alle Vorkommen dieses Fehlercodes für alle Cloud-Discovery-Zeitpläne angezeigt. Die Liste zeigt die Fehlermeldung, die ID des Configuration Item (CI), die IP-Adresse jeder Instanz, bei der der Fehler aufgetreten ist, und den Fehlerstatus an.
5. Führen Sie eine der folgenden Aktionen aus:
   - Wählen Sie die spezifischen Fehler aus und wählen Sie dann die entsprechende Aktion im Abschnitt **Selected errors** (Ausgewählte Fehler) aus.
   - Wählen Sie die entsprechende Aktion im Abschnitt **Alle Fehler** aus.

     Von Cloud-Discovery wird die ausgewählte Aktion auf alle Fehler in der Liste angewendet.

Verfügbare Aktionen

Aktion	Beschreibung
Aufgabe erstellen	Sie können eine Fehleraufgabe erstellen und einem Benutzer zur Lösung zuweisen. Zugewiesene Fehler gelten als **Aktive Fehler**, für die noch Aktionen ausgeführt werden können. Cloud-Discovery zeigt die Nummer der Fehleraufgabe auf der Fehlercode-Kachel an.
Erkennung wiederholen	Cloud-Discovery versucht erneut eine IP-basierte Erkennung. Wenn Sie **Discovery wiederholen** auswählen, wird diese Aktion von Cloud-Discovery für alle aktiven Fehler ausgeführt, die in der Liste verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Beschreibung
	Sie können die Erkennung nur wiederholen, wenn das Plugin „ServiceNow® IP-based Discovery“ (com.snc.discovery.ip_based) in der Instanz installiert und aktiviert ist.
Ignorieren	Cloud-Discovery ignoriert den Fehler.

6. Überprüfen Sie die Spalte **Fehlerstatus**, um die Ergebnisse der Fehlerkorrektur anzuzeigen. Einzelne Wiederholungsversuche werden schnell abgeschlossen. Neuversuche für eine große Anzahl von IP-Adressen können mehrere Minuten dauern.

   Fehler können einen der folgenden Status aufweisen:

   - **Aktiver Fehler**: Der Fehler ist nicht gelöst. Das ist der Standardstatus aller neuen Fehler.
   - **Gelöst**: Der Fehler ist behoben.
   - **Zugewiesen**: Zur Behebung dieses Fehlers ist eine Aufgabe zugewiesen.
   - **Ausstehende Erkennung**: Es wird darauf gewartet, dass Discovery gestartet wird, nachdem Sie die Aktion **Discovery wiederholen** für alle Fehler ausgeführt haben.
   - **In Erkennung**: Discovery ist derzeit aktiv.

Discovery Platform Analytics and Reporting-Lösungen

Platform Analytics and Reporting-Lösungen enthalten vorkonfigurierte Dashboards. Diese Dashboards enthalten Visualisierungen handlungsrelevanter Daten, mit denen Sie Ihre Geschäftsprozesse und -praktiken optimieren können.

Platform Analytics and Reporting-Lösungen

Platform Analytics Datenvisualisierungen verwenden Performance Analytics Indikatordaten, um Daten im Zeitverlauf anzuzeigen, sodass Sie Ihre Geschäftsprozesse analysieren und Verbesserungsbereiche identifizieren können. Mit Platform Analytics and Reporting-Lösungen können Sie mit einem minimalen Setup den Mehrwert von Performance Analytics für Ihre Anwendung nutzen. Sie können auch jederzeit eigene Objekte erstellen.

Wichtig: Richten Sie Platform Analytics and Reporting-Lösungen in einer Instanz außerhalb der Produktion ein, und testen Sie die Lösung, bevor Sie sie in der Produktion aktivieren.

Um das Lösungs-Plugin für Discovery zu aktivieren, kann ein Administrator zu navigieren **Systemdefinitionen** > **Plugins** und aktivieren Sie das Performance Analytics - Inhaltspaket - Discovery-Plugin.

Zugehörige Informationen

Platform Analytics and Reporting-Lösungen

Performance Analytics-Abonnement aktivieren

Discovery – Referenz

Referenzthemen enthalten zusätzliche Informationen zu Discovery-Listen und -Formularen.

Formular „Aufgaben zur Befehlsvalidierung“ für die musterbasierte Discovery

Das Formular**„Aufgaben zur Befehlsvalidierung“** zeigt die Felder an, die Sie ausfüllen müssen, wenn Sie eine Aufgabe zum Testen eines Musterbefehls erstellen oder ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu **Aufgaben zur Befehlsvalidierung**finden Sie unter Validiert Befehle, die in der musterbasierten Discovery verwendet werden.

Feld	Beschreibung
Nummer	Die Aufgabennummer wird automatisch vom System erstellt.
Methode für MID Server-Auswahl	Wählen Sie die relevante Methode aus: • **Spezifischer MID Server**: Zum Definieren des MID Servers für diesen Test. • **Automatische MID Server-Auswahl**: Zur Verwendung eines MID Servers, der dem IP-Bereich oder IP-Netzwerk zugewiesen wurde, den/das Sie für den Test verwenden möchten. Wählen Sie diese Methode nur aus, wenn Sie einen MID-Server mit IP-Bereichen konfiguriert haben oder als Standard-MID-Server für Discovery. • **Try All Eligible MID Servers** (Alle berechtigten MID Server testen): Zur Verwendung eines beliebigen MID Servers, der für den IP-Bereich oder das IP-Netzwerk verfügbar ist, den/das Sie für den Test verwenden möchten. Wählen Sie diese Methode nur aus, wenn Sie einen MID-Server mit IP-Bereichen konfiguriert haben oder als Standard-MID-Server für Discovery.
MID Server	Name des MID-Servers. Dieses Feld wird nur angezeigt, wenn unter **Methoden für MID Server-Auswahl** die Option **Spezifischer MID Server** ausgewählt ist.
Alle Musterbefehle validieren	Das Kontrollkästchen zum gleichzeitigen Validieren aller von einem bestimmten Muster verwendeten Befehle.
Betriebssystemklasse	CI-Klasse, die die Server darstellt, auf denen Sie diese Validierungsaufgabe ausführen.
Befehlstyp	Befehlstyp, der von der Art des Servers abhängt: • **Shell-Befehl** • **WMI-Abfrage** • **SNMP-Abfrage** (tabellarisch und skalar) • **SNMP-Walk** • **HTTP GET** (für Anmeldeinformationen für Standardauthentifizierung, nicht für Token)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dieses Feld ist nur verfügbar, wenn **AI-Musterbefehle validieren** nicht ausgewählt ist.
IP-Adressen	Beliebige Kombination von IPv4-Adressen, IP-Bereichen oder IP-Netzwerken. Beispiel: • `10.196.39.12, 10.196.39.12`: Kommagetrennte IP-Adressen für eine Liste eigenständiger Adressen. • `1.1.1.1-1.1.1.100`: Durch Bindestriche getrennte IP-Adressen für einen IP-Bereich. • `1.1.1.1/28`: Schrägstrichschreibweise für ein IP-Netzwerk. **Hinweis:** Vergewissern Sie sich, dass Sie die Skripteinbindung ParseIPRanges installiert haben, wenn Sie einen IP-Bereich oder ein IP-Netzwerk verwenden möchten. Weitere Informationen finden Sie unter KB1123625: Tool zur Befehlsvalidierung .
Befehle	Die Befehle, für die Sie die Anmeldeinformationen testen möchten. Normalerweise handelt es sich dabei um einen Befehl, der vom Discovery-Prozess nicht ausgeführt werden konnte. Beispiel: **/api/v1/pods?limit=50** oder **sudo dmidecode**. Sie können nur Befehle aus der Liste der verfügbaren Befehle auswählen. Dieses Feld ist nur verfügbar, wenn **„Alle Musterbefehle validieren“** nicht ausgewählt ist.
Muster	Der Name des Musters, für das Sie die Befehle validieren möchten. Dieses Feld ist nur verfügbar, wenn **AI-Musterbefehle validieren** nicht ausgewählt ist.

Zugehörige Informationen

Befehlsliste für Befehle, die für die musterbasierte Discovery verwendet werden

Befehlsliste für Befehle, die für die musterbasierte Discovery verwendet werden

Die **Befehlsliste** enthält alle Befehle, die von den Mustern der Infrastruktur- oder Anwendungstypen verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften der Befehlsliste

Attribut	Beschreibung
Anwendbare Betriebssystemklasse	Der Befehl soll für diese Betriebssystemklasse ausgeführt werden.
CI-Typ	Das Muster, das diesen Befehl enthält, ist diesem CI-Typ zugewiesen. **Hinweis:** Einige ServiceNow-Anwendungen bezeichnen CI-Typen als CI-Klassen.
Befehl	Der Discovery-Befehl.
Befehlstyp	Der Typ des Befehls: • **Shell-Befehl** • **WMI-Abfrage** • **SNMP-Abfrage** (tabellarisch und skalar) • **SNMP-Walk** • **HTTP GET** (für Anmeldeinformationen für Standardauthentifizierung, nicht für Token)
Ist Failover-Schritt	Dieser Befehl wird in einem Failover-Schritt innerhalb eines Musters verwendet.
Veraltet	Dieses Feld dient zur internen Verwendung.
Muster	Der Befehl ist Teil dieses Discovery-Musters.
Schrittname	Der Name des Schritts, der diesen Befehl enthält.
Domäne	Der Befehl wird für das Erkennen von CIs in dieser Domäne validiert. Dieses Feld gilt für domänengetrennte Umgebungen.

Details zu Discovery-Protokollen

Discovery-Protokolle enthalten Informationen zum horizontalen Discovery-Prozess basierend auf Probes und Mustern.

Zugehörige Liste „Discovery-Protokoll“

Die zugehörige Liste „Discovery-Protokoll“ enthält Informationen zur horizontalen Erkennung basierend auf Probes.

Das Discovery-Protokoll enthält die folgenden Informationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Erstellt	Zeitstempel der Discovery Aktivität. Jeder Zeitstempel definiert die ungefähre Zeit der Aktivität. Mehrere Discovery Ereignisse können in zufälliger Reihenfolge innerhalb einer Sekunde auftreten.
Ebene	Klassifiziert die Aktivität in eine der folgenden Ebenen für die allgemeine Sortierung: • Fehler • Informationen • Warnung
Kurznachricht	Informative Nachricht, in der das Ergebnis der Aktivität oder der Discovery-Fortschritt angezeigt wird. Suchen Sie hier nach dem Ergebnis eines Klassifizierungs-Tests oder nach einem Authentifizierungsfehler.
Eingabe für ECC-Warteschlange	Der zugehörige Eingabedatensatz aus der ECC-Queue für diese Ermittlung. Sie können diese Datensätze auch in der verwandten Liste **ECC-Queue** anzeigen.
CI	Benennt ein Gerät, für das in der CMDB ein übereinstimmendes CI gefunden wurde. Wählen Sie den Link, um den CI-Datensatz für das Gerät anzuzeigen.
Quelle	Benennt die bestimmte Aktivität, z. B. die Shazzam-Sonde oder eine UNIX-Klassifizierungs-Sonde.
Gerät	Listet die IP-Adresse des erkannten CI auf. Alle durch die IP-Adresse identifizierten Geräte werden im Protokoll angezeigt, auch wenn sie alle Einladungen zur Kommunikation abgelehnt haben. Jede Portaktivität von einem Gerät speichert sie in das Protokoll, auch wenn alle nachfolgenden Versuche zur Identifizierung fehlschlagen. Wählen Sie die IP-Adresse des Geräts aus, um die Ereignisse anzuzeigen, die der Erkennung dieses Geräts zugeordnet sind.

Horizontales Discovery-Protokoll

Das Fenster „Horizontales Discovery-Protokoll“ enthält Informationen zur musterbasierten horizontalen Erkennung.

Discovery-Protokollelement	Beschreibung
Pre Pattern Execution	Aktionen, die vor dem Start des Musters ausgeführt wurden
Selecting Pattern for Execution	Das Muster, das für die Erkennung ausgeführt wurde
{Identification Section name}	Zeigt die Ergebnisse der Vorgänge im Muster an. Erweitern Sie den Namen, um die einzelnen Vorgänge anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Protokollelement	Beschreibung
Pre Payload Processing Scripts	Die Ergebnisse der Skripts, die ausgeführt wurden, bevor die Nutzlast empfangen wurde
Payload Processing	Details zur Nutzlast und ihrer Verarbeitung. Suchen Sie nach Fehlern, die möglicherweise bei verschiedenen Aktivitäten aufgetreten sind, zum Beispiel beim Ausführen von Identifizierungsregeln und Aktualisierungen der CMDB.
Post Payload Processing Scripts	Die Ergebnisse der Skripts, die ausgeführt wurden, nachdem die Nutzlast empfangen wurde

Cloud-Discovery Formularreferenz für Service-Account

Das Cloud-Discovery-Formular „Servicekonto“ zeigt detaillierte Informationen zum ausgewählten Cloud-Provider an. Das Servicekontoformular Cloud-Discovery ist im Arbeitsbereich für Cloud-Vorgängeverfügbar.

Amazon Web Services (AWS) – Servicekonto-Felder

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen.
Account-ID	12-stellige IAM-Kontonummer (Identity and Access Management)
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die AWS-Erkennung erstellt haben. Wenn der Account ein Mitgliedsaccount einer AWS-Organisation ist und Sie den zugeordneten Verwaltungsaccount mit Anmeldeinformationen konfiguriert haben, lassen Sie dieses Feld leer. Um in Now Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit Anmeldeinformationen für AWS finden Sie unter Zugriff auf AWS-Konten mit permanenten AWS-Anmeldeinformationen konfigurieren.
URL	URL des Rechenzentrums.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon Web Services (AWS) – Servicekonto-Felder (Fortsetzung)

Feld	Beschreibung
	Füllen Sie dieses Feld nur für die Regionen-Accounts AWS GovCloud (US) und AWS China aus.
Name der Zugriffsrolle	Name der IAM-Rolle, die für den vertrauende Account erstellt wurde.
Select account for access (Konto für Zugriff auswählen)	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, die keine permanenten AWS-Anmeldeinformationen verwenden und für den Zugriff IAM-Rollen ausnutzen.

Felder des Microsoft Azure-Servicekontos

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Microsoft Azure-Abonnements
Subscription ID (Abonnement-ID)/ Management group ID (Verwaltungsgruppen-ID)	Microsoft Azure-Abonnement-ID
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die Microsoft Azure-Erkennung erstellt haben. Um in Now Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars „Azure-Service-Prinzipal“ finden Sie unter Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern.
URL	Lassen Sie dieses Feld leer.
Ereignisse abrufen	Option, um in der Now Platform das Sammeln von Informationen über Ressourcen-Changes aus der Microsoft Azure-Cloud zu aktivieren. Die Now Platform verwendet die Informationen über Ressourcen-Changes zur Aktualisierung der Configuration Management Database (CMDB). Weitere Informationen zu den unterstützten Azure-Ressourcentypen finden Sie unter Azure Verarbeitung von Changes. Wenn Sie das Kontrollkästchen Ereignisse abrufen für eine Verwaltungsgruppe aktivieren, aktiviert Now Platform die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder des Microsoft Azure-Servicekontos (Fortsetzung)

Feld	Beschreibung
	Verarbeitung von Changes Azure für alle Abonnements in der Verwaltungsgruppe.

Felder des Google Cloud Platform-Servicekontos

Feld	Beschreibung
Service-Account	Projekt-ID des Google Cloud Platform (GCP)-Projekts, dessen Ressourcen Sie erkennen möchten. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Projekt-ID des Google Cloud Platform (GCP)-Projekts.
Project ID (Projekt-ID)/ Folder ID (Ordner-ID)	Projekt-ID des Google-Projekts
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die GCP-Erkennung erstellt haben. Um in Now Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit API-Anmeldeinformationen für Google finden Sie unter Erkennung von Google Cloud Platform.
Ereignisse abrufen	Option zum Aktivieren der eventgesteuerten ServiceNow®-Erkennung zum Sammeln von Events für die in den Google-Projekt-LDCs gehosteten Ressourcentypen.

Felder des IBM-Servicekontos

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Servicekontos
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die IBM-Erkennung erstellt haben. Um in Now Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder des IBM-Servicekontos (Fortsetzung)

Feld	Beschreibung
	indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit Anmeldeinformationen für IBM finden Sie unter Erkennung von IBM-Clouds.
Account-ID	IBM-Software-Anwendernummer, die in der Instanz für den Zugriff auf die IBM Cloud-Konsole verwendet werden soll

Oracle Cloud Infrastructure – Servicekonto-Felder

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Servicekontos
Account-ID	OCI-Compartment-ID
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die Erkennung der Oracle Cloud Infrastructure (OCI) erstellt haben. Um in Now Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit API-Anmeldeinformationen für Oracle finden Sie unter Daten gesammelt für Oracle Cloud-Discovery.
Rechenzentrums-URL	Rechenzentrumswert. Beispiel: `https://$service.ap-mumbai-1.oraclecloud.com`

OpenStack – Servicekonto-Felder

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Servicekontos
OpenStack account ID (OpenStack-Konto-ID)	Projekt-ID des OpenStack-Projekts, das erkannt werden soll

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OpenStack – Servicekonto-Felder (Fortsetzung)

Feld	Beschreibung
Account credentials (Kontoanmeldeinformationen)	Name der Anmeldeinformationen, die Sie für die OpenStack-Discovery erstellt haben Um in Now Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit Anmeldeinformationen für OpenStack finden Sie unter OpenStack-Ressourcenerkennung.
Cloud URL	OpenStack-Identitätsservice-Endpunkt. Beispiel: https://<openstack dns>:<port>.

Red Hat Virtualization (RHV) – Servicekonto-Felder

Feld	Beschreibung
Servicekonto	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen. Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Servicekontos
Manager URL	Konto-ID, zu der diese Anmeldeinformationen gehören. Geben Sie die API-URL der RHV-M-Instanz an, einschließlich des Ports. Beispiel: https://my-manager-instance.com:443
Manager credentials (Manager-Anmeldeinformationen)	Name der Anmeldeinformationen, die Sie für die RHV-Discovery erstellt haben Um in Now Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit Anmeldeinformationen für RHV finden Sie unter Red Hat Virtualisierung-Erkennung.

Felder des VMware-Servicekontos

Feld	Beschreibung
Service-Account	Name des Serviceaccounts, dessen Ressourcen erkannt werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder des VMware-Servicekontos (Fortsetzung)

Feld	Beschreibung
	Dieses Feld wird nur angezeigt, wenn die Option „Vorhandener Serviceaccount“ ausgewählt ist.
Name	Name des Servicekontos
UUID	Universeller eindeutiger Bezeichner (Universal Unique Identifier, UUID) der Instanz. So greifen Sie auf die UUID zu: **1.** Öffnen Sie den Browser für verwaltete Objekte (Managed Object Browser, MOB) für vCenter. **2.** Auswahlvorgang **Inhalt** > **Über**. **3.** Fügen Sie den Wert der Instanz-UUID-Eigenschaft in dieses Feld ein.
Anmeldeinformationen	Name der Anmeldeinformationen, die Sie für die VMware-Erkennung erstellt haben. Um in Now Platform Anmeldeinformationen hinzuzufügen, wählen Sie das Symbol „Neue Anmeldeinformationen hinzufügen“ ( ), und füllen Sie die Felder aus. Bei Bedarf können Sie vorhandene Anmeldeinformationen auswählen und dann bearbeiten, indem Sie das Symbol „Anmeldeinformationen bearbeiten“ ( ) wählen. Eine Beschreibung der Felder des Formulars mit Anmeldeinformationen für VMware finden Sie unter VMware-Anmeldeinformationen .
URL	Vollständige vCenter-URL

Erstellen Sie eine neue Formularreferenz für den Discovery-Zeitplan

Das Formular zum Erstellen eines neuen Discovery-Zeitplans zeigt Informationen zum Zeitplan und zum Ziel-Cloud-Anbieter an. Das Formular Neuen Discovery-Zeitplan erstellen ist in Arbeitsbereich für Cloud-Vorgängeverfügbar.

Anweisungen zu diesem Verfahren finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge.

Anbieterformular auswählen

Feld	Beschreibung
Name des Discovery-Zeitplans	Name des Discovery-Zeitplans.
Cloud-Anbieter	Name des Cloud-Anbieters, der die zu erkennenden Ressourcen hostet.
MID-Auswahltypen	MID-Server oder MID-Cluster, den Sie zum Erkennen der Cloud-Ressourcen verwenden möchten. Die folgenden Optionen sind verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anbieterformular auswählen (Fortsetzung)

Feld	Beschreibung
	• MID-Server automatisch auswählen: Discovery verwendet automatisch einen geeigneten MID-Server. • Spezifischer MID-Server-Cluster: Discovery verwendet den im Feld „MID-Cluster“ angegebenen MID-Cluster. • Spezifischer MID-Server: Discovery verwendet den im MID-Server-Feld angegebenen MID-Server. Wenn der ausgewählte MID-Server Teil eines MID-Clusters ist, werden die Aufträge gleichmäßig auf alle MID Servers dieses Clusters verteilt. Dieses Feld wird nur angezeigt, wenn einer der folgenden Werte im Feld „Cloud-Anbieter“ ausgewählt ist: • AWS • Azure • Google
MID-Cluster	MID-Cluster, die Sie mit dem Cloud-Discovery-Zeitplan verwenden möchten. Dieses Feld wird nur angezeigt, wenn im Feld „MID-Auswahltypen“ der Wert „Spezifischer MID-Server-Cluster“ ausgewählt ist.
Discovery ohne Anmeldeinformationen	Option zur Verwendung der Discovery ohne Anmeldeinformationen. Um die MID Servers anzuzeigen und zu filtern, die eine IAM-Rolle annehmen können, um die Cloud-Ressourcen zu erkennen, schieben Sie den Schalter **Discovery ohne Anmeldeinformationen** nach rechts.
MID Servers	MID Servers, die Sie mit dem Cloud-Discovery-Zeitplan verwenden möchten. Dieses Feld wird nur angezeigt, wenn im Feld „MID-Auswahltypen“ der Wert „Spezifischer MID-Server“ ausgewählt ist.

Cloud-Discovery-Referenz

Referenzthemen enthalten zusätzliche Informationen zu den in Cloud-Discoveryverwendeten Listen, Formularen und Cloud-Einstellungen.

Referenz des Formulars „Einstellungen bearbeiten“.

Das Formular „Einstellungen bearbeiten“ zeigt Informationen zu den Amazon Web Services -Einstellungen (AWS) an, die zum Aufzeichnen und Übermitteln der Ereignisse AWS an den lauschenden Endpunkt verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Einstellungen bearbeiten“.

Feld	Beschreibung
Allgemeine Einstellungen	
Zu erfassende Ressourcentypen	Ressourcentypen, für die Sie die Konfigurationsänderung aufzeichnen möchten. Geben Sie auch an, ob Sie die Konfigurationsänderung für globale Ressourcen aufzeichnen möchten, z. B. AWS AMI-Ressourcen. Weitere Informationen finden Sie unter dem Thema Auswählen der AWS Config-Ressourcen in der AWS -Dokumentation.
Aufbewahrungszeitraum für Daten	(Optional) Aufbewahrungsrichtlinie für die aufgezeichneten Ereignisse.
AWS Konfigurationsrolle	Eine AWS-Rolle, die auf die folgenden Services und Ressourcen zugreifen kann: • Simple Notification Service (SNS) • AWS-Konfigurationsservice • Ressourcentypen, für die Sie die Konfigurationsänderung nachverfolgen möchten
Liefermethode	
AWS S3-Bucket	Ein AWS S3-Bucket zum Speichern der aufgezeichneten Ereignisse Erstellen Sie einen AWS S3-Bucket, oder wählen Sie einen vorhandenen AWS S3-Bucket aus, auf den Sie Zugriff haben.
Konfigurationsänderungen und Benachrichtigungen an ein Amazon -SNS-Thema streamen	Option zum Veröffentlichen der Ereignisbenachrichtigungen im SNS-Thema.
Amazon SNS-Thema	Amazon SNS-Thema, in dem der Konfigurationsservice AWS die Ereignisse veröffentlichen soll. 1. Wählen Sie die Option **Thema aus Ihrem Account auswählen** aus. 2. Wählen Sie in der Dropdown-Liste „SNS-Themenname“ das in Schritt 3 erstellte SNS-Thema [Amazon aus.

Discovery-CLI-Befehle

Eine Liste der Befehle, die für die Befehlszeilenschnittstelle Discovery (CLI) in der Anwendung Musterdesigner Erweiterungen verfügbar sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Discovery-Einblicke

Ruft Details zu Ihren Discovery-Konfigurationen und -Mustern ab. Die Details umfassen Informationen zu anwenderdefinierten Mustern, Instanzdetails und Plugin-Details.

Befehlsgruppe

Übergeordnete Gruppe: Discovery

Erforderliche Rollen

discovery_admin

Wenn Sie einen mit Discoveryverbundenen Service verwenden, müssen Sie über die erforderlichen Rollen für diesen Service verfügen.

Befehlsstruktur

```
snc discovery discovery-insights
```

Beispiel

Rufen Sie Details zu Ihren Discovery-Konfigurationen und -Mustern ab, indem Sie den folgenden Befehl ausführen:

```
snc discovery discovery-insights
```

Der Befehl gibt ein Objekt JSON (Standardformat) zurück, das die Informationen in der folgenden Tabelle enthält.

Vom Befehl „discovery-insights“ zurückgegebene JSON-Objekte

Objekt	Details
`anwenderdefinierte Muster`	• `PatternName`: Name des anwenderdefinierten Mustersz. • `Quelle`: Speicherort, an dem die anwenderdefinierten Changes enthalten sind (z. B. Standard)
`instanceDetails`	• `buildDate`: Datum des Instanzerstellung (Format: MM-TT-JJJJ_HHMM) • `buildName`: Name des Instanz-Builds
`pluginDetails`	Plugins, die zur Discovery-Konfiguration gehören oder zum Ausführen CLIvon erforderlich sind.

Rückgabewert

```
✔ Discovery diagnostics successfully completed.
{
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
   "customizedPattern": [
      {
         "patternName": "A10",
         "source": "Default"
      },
      {
         "patternName": ".NET Application",
         "source": "Default"
      }
   ],
   "instanceDetails": {
      "buildDate": "09-16-2023_2010",
      "buildName": "utah-p0"
   },
   "pluginDetails": {
      "CMDB CI Class Models": "1.48",
      "Discovery and Service Mapping Patterns": "1.8.0",
      "Pattern Designer Enhancements": "3.1.0",
      "Visibility Content": "6.13.0"
   }
}
```

„get-discovery-credentials“

Ruft die Liste der Discovery-Anmeldeinformationen ab.

Befehlsgruppe

Übergeordnete Gruppe: Discovery

Erforderliche Rollen

discovery_admin

Wenn Sie einen mit Discoveryverbundenen Service verwenden, müssen Sie über die erforderlichen Rollen für diesen Service verfügen.

Befehlsstruktur

```
snc discovery get-discovery-credentials [arguments]
```

Argument:

`--testableonly`: Enthält nur Anmeldeinformationen, die getestet werden können. Mögliche Werte: true oder false.

Beispiele

Rufen Sie eine Liste der Discovery-Anmeldeinformationen ab, indem Sie den folgenden Befehl ausführen:

```
snc discovery get-discovery-credentials
```

Listen Sie nur testbare Discovery-Anmeldeinformationen auf, indem Sie den Befehl mit dem folgenden Argument ausführen:

```
snc discovery get-discovery-credentials --testableonly="true"
```

Rückgabewert

```
✔ Get only testable credentials [ssh, snmpv3, snmp,
 ssh_private_key, windows, vmware, jdbc, jms]: true
✔ Discovery credentials details retrieved
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
{
   "credentials": [
      {
         "active": true,
         "name": "shCred",
         "type": "ssh",
         "updated": "2023-10-16 10:57:27"
      },
      {
         "active": true,
         "name": "WindowsCred",
         "type": "windows",
         "updated": "2023-10-10 12:18:17"
      },
      {
         "active": true,
         "name": "Azure",
         "type": "azure",
         "updated": "2022-10-19 05:57:21"
      },
      {
         "active": true,
         "name": "public",
         "type": "snmp",
         "updated": "2023-09-28 07:40:35"
      },
      {
         "active": true,
         "name": "Windows MID Server Service Account",
         "type": "windows",
         "updated": "2023-10-16 10:57:23"
      },
      …
   ]
}
```


get-discovery-logs

Ruft Discovery-Protokolle mit flexiblen Optionen ab, einschließlich:

- Statusfilterung
- Geräteeinschluss
- Protokolle der ECC-Warteschlangen (External Communication Channel).
- Musterprotokolle
- Auswahlmöglichkeiten für Ausgabeformate

Befehlsgruppe

Übergeordnete Gruppe: Discovery

Erforderliche Rollen

discovery_admin

Wenn Sie einen mit Discoveryverbundenen Service verwenden, müssen Sie über die erforderlichen Rollen für diesen Service verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehlsstruktur

```
snc discovery get-discovery-logs [arguments]
```

Argumente

Argumente für den Befehl „get-discovery-logs“.

Argument	Beschreibung
`--status-id`	Discovery-Statusnummer, nach der Protokolle gefiltert werden sollen.
`--devices`	Enthält gerätespezifische Protokolle. Mögliche Werte: true oder false.
`--ecc-queue-logs`	Enthält zugehörige ECC-Warteschlangenprotokolle. Mögliche Werte: true oder false.
`--pattern-logs`	Enthält Musterausführungsprotokolle. Mögliche Werte: true oder false.
`--pattern-log-level`	Maximaler Schweregrad für die Filterung von Musterprotokollen. Verfügbare Optionen: • DEBUG: Enthält nur DEBUG-Protokollnachrichten (Standard) • FEHLER: Enthält FEHLER- und DEBUG-Nachrichten • WARN: Enthält WARN-, ERROR- und DEBUG-Nachrichten • INFO: Schließt alle Nachrichten ein
`--log-limit`	Maximale Anzahl der zurückzugebenden Protokolldatensätze liegt zwischen 1 und 100 (Standard: 100). Gilt nur für ECC-Warteschlangen und Musterprotokolle.
`--Ausgabeformat`	Ausgabeformat für die Protokolle. Unterstützte Formate sind JSON (Standardformat) oder Tabelle.

Beispiele

Rufen Sie Discovery-Protokolle ab, indem Sie den folgenden Befehl ausführen:

```
snc discovery get-discovery-logs [options]
```

Passen Sie den Protokollabruf an, indem Sie die Argumente entweder einzeln oder als einzelnen Befehl einfügen.

- So führen Sie den Befehl mit einem Argument nach dem anderen aus:

```
snc discovery get-discovery-logs
Discovery status number: DIS0010013
Include Devices: true
Include ECC Queue logs: true
Include pattern execution logs: true
Pattern max log level (INFO, WARN, ERROR, DEBUG): DEBUG
Maximum number of log records to return: 100
Output format [supported: json(default), table]: json
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- So führen Sie den Befehl als einzelnen Befehl aus:

```
snc discovery get-discovery-logs --status-id="DIS0010013"
 --ecc-queue-logs="true" --devices="true"
 --pattern-logs="true" --output-format="json"
```

Wenn die maximale Anzahl der zurückzugebenden Protokolldatensätze hoch ist, sollten Sie ein Tabellenausgabeformat verwenden.

Rückgabewert


```
✔ Discovery Status details retrieved
{
   "Devices": [
      {
         "CMDBCI": "",
         "ClassificationProbe": "Windows - Classify",
         "Completed": "4",
         "CompletedActivity": "Updated CI",
         "Created": "2023-10-17 09:25:33",
         "CurrentActivity": null,
         "Issues": "0",
         "ScanStatus": "Completed 4",
         "Started": "4",
         "Status": "DIS0010136"
      }
   ],
   "DiscoveryLogs": [
      {
         "CI": "",
         "Created": "2023-10-17 09:25:24",
         "Device": "",
         "ECCQueueInput": "",
         "Level": "0",
         "Message": "Discovery started",
         "Source": "Discovery",
         "Status": "DIS0010136"
      },
      {
         "CI": "",
         "Created": "2023-10-17 09:26:49",
         "Device": "192.168.1.100",
         "ECCQueueInput": "HorizontalDiscoveryProbe",
         "Level": "0",
         "Message": "Exploring CI Pattern, Pattern name:
 Windows OS - Servers",
         "Source": "DiscoverySensor",
         "Status": "DIS0010136"
      },
      {
         "CI": "",
         "Created": "2023-10-17 09:27:01",
         "Device": "192.168.1.100",
         "ECCQueueInput": "",
         "Level": "0",
         "Message": "Discovery completed",
         "Source": "Discovery",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "Status": "DIS0010136"
         }
      ],
      "DiscoveryStatus": [
         {
            "Completed": "5",
            "Created": "2023-10-17 09:25:24",
            "Description": "Discover Now",
            "Discover": "CIs",
            "Duration": "1970-01-01 00:01:37",
            "Number": "DIS0010136",
            "Schedule": "WinServer",
            "Started": "5",
            "State": "Completed",
            "Updated": "2023-10-17 09:27:08"
         }
      ],
…
}
```

get-midserver

Ruft detaillierte Informationen zu MID Serversab, einschließlich Status- und Validierungsdetails. Optional können Sie Problemprotokolle MID Servers in die Ausgabe aufnehmen.

Befehlsgruppe

Übergeordnete Gruppe: Discovery

Erforderliche Rollen

discovery_admin

Wenn Sie einen mit Discoveryverbundenen Service verwenden, müssen Sie über die erforderlichen Rollen für diesen Service verfügen.

Befehlsstruktur

```
snc discovery get-midservers [arguments]
```

Argument

`--include-issues`: Schließt Problemprotokolle mit jedem MID-Serverein. Mögliche Werte: „true“ oder „false“ (Standard: true).

Beispiel

Rufen Sie Details zu MID Servers ab, indem Sie den folgenden Befehl ausführen:

```
snc discovery get-midservers
```

Rufen Sie eine Liste von MID Servers und die zugehörigen Problemprotokolle ab, indem Sie den Befehl mit dem folgenden Argument ausführen:

```
snc discovery get-midservers --include-issues=true
```

Rückgabewert

```
✔ MID Server details were fetched successfully.
{
   "mid_servers": [
      {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        "home_directory":
 "C:\\Users\\admin\\Desktop\\midInstallationFolder\\agent",
        "host_name": "LocalLab",
        "host_os_version": "10.0.xxxx",
        "ip_address": "192.168.0.1",
        "issues": [],
        "last_refreshed": "2023-10-01 00:00:00",
        "name": "WindowsMidServer",
        "started": "2023-10-01 00:01:01",
        "status": "Up",
        "sys_id": "cb8d1625c3fdb110c72691477d01312e",
        "unresolved_issues": "0",
        "validated": "true",
        "validated_at": "2023-10-01 00:01:01"
     }
   ]
}
```

get-pattern-commands

Ruft eine umfassende Liste von Befehlen ab, die einem angegebenen Discovery-Muster zugeordnet sind, identifiziert durch seinen Namen oder seine sys_id.

Befehlsgruppe

Übergeordnete Gruppe: Discovery

Erforderliche Rollen

discovery_admin

Wenn Sie einen mit Discoveryverbundenen Service verwenden, müssen Sie über die erforderlichen Rollen für diesen Service verfügen.

Befehlsstruktur

```
snc discovery get-pattern-commands [arguments]
```

Argument

`--pattern`: Musternname oder sys_id

Beispiele

Rufen Sie eine Liste von Befehlen ab, die dem angegebenen Muster zugeordnet sind, indem Sie den Befehl entweder mit dem Musternamen oder der sys_id ausführen.

- Führen Sie den Befehl aus, indem Sie den Musternamen `Windows OS - Server`eingeben:

  ```
  snc discovery get-pattern-commands --pattern="Windows OS -
   Servers"
  ```

- Führen Sie den Befehl aus, indem Sie das Muster sys_id `670e55a4db702200c06776231f961942`eingeben:

  ```
  snc discovery get-pattern-commands
   --pattern="670e55a4db702200c06776231f961942"
  ```

Rückgabewert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
✔ Commands fetched successfully.
[
   {
      "Command": "\"\\root\\CIMV2\" \"SELECT
 Caption,IPAddress,MACAddress,DHCPEnabled,Index,InterfaceIndex,
IPEnabled FROM Win32_NetworkAdapterConfiguration\"",
      "Command Type": "wmi",
      "sys_id": "2e677c4ec3adb1106618b10ad0013185"
   },
   {
      "Command": "\"\\root\\CIMV2\" \"SELECT
 Index,InterfaceIndex,Name,Manufacturer,NetConnectionID FROM
 Win32_NetworkAdapter\"",
      "Command Type": "wmi",
      "sys_id": "6a677c4ec3adb1106618b10ad0013185"
   },
   {
      "Command": "powershell -command \\Get-NetRoute
 -AddressFamily IPv6\\",
      "Command Type": "shell",
      "sys_id": "a6677c4ec3adb1106618b10ad0013185"
   },
   {
      "Command": "\"\\root\\CIMV2\" \"SELECT
 Destination,Mask,NextHop, InterfaceIndex FROM
 Win32_IP4RouteTable\"",
      "Command Type": "wmi",
      "sys_id": "e2677c4ec3adb1106618b10ad0013185"
   },
   {
      "Command": "\"\\root\\CIMV2\" \"SELECT DefaultIPGateway
 FROM Win32_NetworkAdapterConfiguration\"",
      "Command Type": "wmi",
      "sys_id": "e6677c4ec3adb1106618b10ad00131ab"
   },
…
]
```

get-patterns

Ruft eine umfassende Liste der verfügbaren Discovery-Muster ab.

Befehlsgruppe

Übergeordnete Gruppe: Discovery

Erforderliche Rollen

discovery_admin

Wenn Sie einen mit Discoveryverbundenen Service verwenden, müssen Sie über die erforderlichen Rollen für diesen Service verfügen.

Befehlsstruktur

```
snc discovery get-patterns
```

Beispiel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rufen Sie eine Liste der verfügbaren Discovery-Muster ab, indem Sie den folgenden Befehl ausführen:

```
snc discovery get-patterns
```

Rückgabewert

```
✔ Details of Discovery Patterns successfully retrieved.
[
   {
      "active": true,
      "ci_type": "cmdb_ci_appl_dot_net",
      "name": ".NET Application",
      "pattern_type": "1 - Application"
   },
   {
      "active": true,
      "ci_type": "cmdb_ci_lb_service",
      "name": "A10",
      "pattern_type": "1 - Application"
   },
   {
      "active": true,
      "ci_type": "cmdb_ci_lb_a10",
      "name": "A10 Load Balancer",
      "pattern_type": "3 - Infrastructure"
   },
   {
      "active": true,
      "ci_type": "cmdb_ci_lb_a10",
      "name": "A10 Load Balancer SSH",
      "pattern_type": "3 - Infrastructure"
   },
   {
      "active": true,
      "ci_type": "cmdb_ci_appl_generic",
      "name": "A10 SSH Hosting Formatting",
      "pattern_type": "2 - Shared library"
   },
   …
]
```

midserver-action

Führt verschiedene Aktionen für MID Serversaus, z. B. Anhalten, Fortsetzen oder Neustarten.

Befehlsgruppe

Übergeordnete Gruppe: Discovery

Erforderliche Rollen

discovery_admin

Wenn Sie einen mit Discoveryverbundenen Service verwenden, müssen Sie über die erforderlichen Rollen für diesen Service verfügen.

Befehlsstruktur

```
snc discovery midserver-action [arguments]
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Argumente

Argumente für den Befehl „midserver-action“.

Argument	Beschreibung
`-m` oder `--mid-server`	Name oder sys_id des MID-Server
`-a` oder `--action`	Aktion, die für MID-Serverausgeführt werden soll. Verfügbare Optionen: • für ungültig erklären • resume • Stoppen • pause • autoUpgrade • Upgrade • restart • „file_discovery_refresh“ • GRAB_logs • validieren

Beispiel

Führen Sie eine -Aktion für MID-Server mit dem folgenden Befehl aus:

```
snc discovery midserver-action [options]
```

Starten Sie MID-Server `WinMidServer` neu, indem Sie den folgenden Befehl ausführen:

```
snc discovery midserver-action --mid-server="WinMidServer"
 --action="restart"
```

Rückgabewert

```
✔ Successfully submitted mid-server action
{
   "Action": "restart",
   "MidServer": "cb8d1625c3fdb110c72691477d01312e",
   "Output": "Mid server restart in-progress."
}

✔ Mid server action executed successfully
restart executed successfully.
```

Schnell-Discovery

Führt eine Schnell-Discovery für ein angegebenes Configuration Item (CI) oder eine angegebene IP-Adresse aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die Anzahl der Rückrufversuche den Höchstwert überschreitet, erhalten Sie möglicherweise die folgende Fehlermeldung:

```
✗ Discovery Failed.
{
"CurrentActivity": "",
"DiscoveryStatus": {},
"State": "Active"
}
```

Die Meldung gibt an, dass die Anzahl der Rückrufwiederholungen überschritten wurde, die Erkennung jedoch fehlgeschlagen ist, aber weiterhin im Hintergrund ausgeführt wird. Überprüfen Sie die Discovery-Protokolle, indem Sie entweder den Befehl `snc discovery get-discovery-logs` ausführen oder die Instanz ServiceNow® auf Aktualisierungen des Discovery-Status überprüfen.

Befehlsgruppe

Übergeordnete Gruppe: Discovery

Erforderliche Rollen

discovery_admin

Wenn Sie einen mit Discoveryverbundenen Service verwenden, müssen Sie über die erforderlichen Rollen für diesen Service verfügen.

Befehlsstruktur

```
snc discovery quick-discovery [arguments]
```

Argumente

Argumente für die Befehls-Schnell-Discovery

Argument	Beschreibung
`--type`	Ziel-Hosttyp: entweder IP oder CI.
`--target`	Details des Zielhosts. • IP: IP-Adresse • CI: Die verfügbaren Optionen sind: ◦ Name ◦ Sys_id ◦ Seriennummer
`--error-logs-only`	Enthält nur Fehlerprotokolle. Mögliche Werte: „true“ oder „false“ (Standard: true).

Beispiele

Führen Sie eine Schnell-Discovery für eine Zielentität anhand eines angegebenen Kriteriums aus.

```
snc discovery quick-discovery
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Führen Sie eine Schnell-Discovery für die IP-Adresse `192.168.1.100` aus, indem Sie den folgenden Befehl und das folgende Argument ausführen:

```
snc discovery quick-discovery --type="ip"
 --target="192.168.1.100"
```

- Führen Sie eine Schnell-Discovery für das angegebene CI aus, indem Sie den Befehl mit dem Namen, sys_id oder der Seriennummer ausführen.
  - Geben Sie Folgendes ein, um eine Schnell-Discovery für den CI-Namen `eCommerce001`auszuführen:

```
snc discovery quick-discovery --type="ci"
 --target="ecommerce001"
```

  - Um eine Schnell-Discovery für das CI sys_id `d0e8761137201000deeabfc8bcbe5da7`auszuführen, geben Sie Folgendes ein:

```
snc discovery quick-discovery --type="ci"
 --target="d0e8761137201000deeabfc8bcbe5da7"
```

  - Um eine Schnell-Discovery für die CI-Seriennummer `L3BB911`auszuführen, geben Sie Folgendes ein:

```
snc discovery quick-discovery --type="ci" --target="L3BB911"
```

Rückgabewert

```
snc discovery quick-discovery --type="ip"
 --target="192.168.1.100"
✔ Discovery job submitted
Status Number: DIS0010054
✔ Discovery is complete
{
   "DiscoveryLogs": [],
   "DiscoveryStatus": [
      {
         "Completed": "5",
         "Created": "2023-10-17 10:59:52",
         "Description": "Discover CI",
         "Discover": "CIs",
         "Duration": "1970-01-01 00:01:41",
         "Number": DIS0010054,
         "Schedule": "",
         "Started": "5",
         "State": "Completed",
         "Updated": "2023-10-17 11:02:06"
      }
   ],
   "State": "Completed"
}
```

run-command

Führt Befehle auf Remotegeräten mit den angegebenen Anmeldeinformationen, Zielen und MID Serversaus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehlsgruppe

Übergeordnete Gruppe: Discovery

Erforderliche Rollen

discovery_admin

Wenn Sie einen mit Discoveryverbundenen Service verwenden, müssen Sie über die erforderlichen Rollen für diesen Service verfügen.

Befehlsstruktur

```
snc discovery run-command [arguments]
```

Argumente

Argumente für den Befehl „run-command“.

Argument	Beschreibung
`--Befehl`	Auszuführender Befehl
`--command-type`	Auszuführender Vorgangstyp.
`--credential`	Anmeldeinformationen, die zum Ausführen des Befehls verwendet werden.
`--midserver`	Name von MID-Server, der für die Kommunikation mit dem Ziel verwendet wird.
`--os-server`	CI-Klasse, die das Serverbetriebssystem darstellt, unter dem die Befehle ausgeführt werden sollen. Geben Sie beispielsweise *`cmdb_ci_linux_server`* für den Server Linux ein.
`--target`	Host-IP-Adresse, auf der Sie den Befehl ausführen möchten.

Beispiel

Führen Sie den folgenden Befehl aus, damit die Abfrage von Windows Management Instrumentation (`WMI`) das System auffordert, die Eigenschaften *`UUID`* und *`IdentifyingNumber`* aus der Klasse *`Win32_ComputerSystemProduct`* im Namespace `\root\CIMV2` abzurufen:

```
snc discovery run-command --command="\"\\root\\CIMV2\" \"SELECT
 UUID,IdentifyingNumber FROM Win32_ComputerSystemProduct\""
 --command-type="wmi" --credential="WinCred"
 --midserver="WinMidServer" --os-server="cmdb_ci_win_server"
 --target="192.168.1.1"
```

Rückgabewert

```
✔ The command is sent for execution.
{
"eccQueueOutputSysId": "9a3c55a3c33db910c72691477d0131cd"
}

✔ Command Executed Successfully...
{
"result": {
"IdentifyingNumber": "VMware-00 00 00 00 00 00 00 00-00 00 00
 00 00 00 00 00",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"Name": "VMware Virtual Platform",
"Object Reference": null,
"UUID": "61410042-XXXX-XXXX-XXXX-XXXXXXXXXXXX",
"Version": "None",
"__CLASS": "Win32_ComputerSystemProduct",
"internal_classname": "Win32_ComputerSystemProduct",
"internal_namespace": "root/cimv2"
}
}
```

Test-Discovery-Anmeldeinformationen

Validiert die Discovery-Anmeldeinformationen anhand eines angegebenen Zielsystems mithilfe eines festgelegten MID-Server. Der Befehl überprüft nur die Bereitschaft der Anmeldeinformationen für Netzwerk-Discovery-Aufgaben. Die Konfiguration der Discovery-Anmeldeinformationen oder des Zielsystems wird dadurch nicht geändert oder beeinflusst.

Wichtig:

Dieser Befehl erfordert, dass eine bestimmte XML-Datei in die Liste „Modulzugriffsrichtlinie“ importiert wurde. Weitere Informationen finden Sie im Artikel Discovery CLI [KB1553142] in der Now Support Knowledge Base.

Befehlsgruppe

Übergeordnete Gruppe: Discovery

Erforderliche Rollen

discovery_admin

Wenn Sie einen mit Discoveryverbundenen Service verwenden, müssen Sie über die erforderlichen Rollen für diesen Service verfügen.

Befehlsstruktur

```
snc discovery test-discovery-credential [arguments]
```

Argumente

Argumente für „test-discovery-credential“.

Argument	Beschreibung
`--dbname`	Name der Datenbank, für die diese Anmeldeinformationen getestet werden sollen.
`--dbtype`	Typ der Datenbank, für die diese Anmeldeinformationen getestet werden sollen. Verfügbare Optionen: • MSSQL: für Microsoft SQL Server • MySQL • Oracle
`--icf`	Name der JNDI-Klasse (Java Benennungs- und Verzeichnisschnittstelle), die zum Erstellen des InitialContext verwendet wird. Der Name der JNDI-Klasse muss zuerst den Paketnamen und dann den Klassennamen enthalten. Um beispielsweise eine Verbindung zur Klasse

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Argumente für „test-discovery-credential“. (Fortsetzung)

Argument	Beschreibung
	ActiveMQ JNDI herzustellen, geben Sie Folgendes ein: `org.apache.activemq.jndi.ActiveMQInitialContextFactory`.
`--midserver`	Name von MID-Server, der für diesen Test verwendet werden soll. Zum Testen Windows der -Anmeldeinformationen müssen Sie Windows MID-Serververwenden.
`--name`	Name des Berechtigungsnachweises
`--port`	Port des Ziels, der für diesen Test verwendet werden soll. Das System füllt dieses Feld vorab mit dem Standardport für den ausgewählten Anmeldeinformationstyp aus.
`--target`	Zielhost, auf dem diese Anmeldeinformationen ausgeführt werden. Dieser Wert muss für alle Anmeldeinformationstypen außer VMwareeine IP-Adresse sein, für die der Wert die Host-URL sein kann.

Beispiel

Testen Sie die Discovery-Anmeldeinformationen `WinCred` für MID-Server `WinMidServer`, indem Sie den folgenden Befehl ausführen:

```
snc discovery test-discovery-credential --name="WinCred"
 --target="192.168.1.1" --midserver="WinMidServer"
```

Der Befehl gibt eine Erfolgsmeldung zurück, wenn die folgenden Bedingungen erfüllt sind:

- Die Anmeldeinformationen sind gültig
- Die Verbindung zum Zielsystem wurde erfolgreich hergestellt
- Der angegebene MID-Server ist betriebsbereit

Wenn diese Bedingungen nicht erfüllt sind, wird eine Fehlermeldung angezeigt, in der die Probleme beschrieben werden.

Rückgabewert

```
✔ Discovery credentials tested successfully
Credential Test Id [ecc-sys-id]:
 "2b36e40ec3727990c72691477d0131c6"
✔ The credential test is complete
{
   "output": "Test Succeeded"
}
```

Weitere Informationen zu Discovery CLIfinden Sie im Artikel Discovery-CLI [KB1553142] in der Now Support Knowledge Base.

Vorschlagsformular für Fingerabdrücke der Anwendung

Wenn Sie Vorschläge basierend auf Anwendungsfingerabdrücken anzeigen, überprüfen Sie die Informationen im Vorschlagsformular für Anwendungsfingerabdrücke.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten des Vorschlagsfingerabdruckformulars der Anwendung

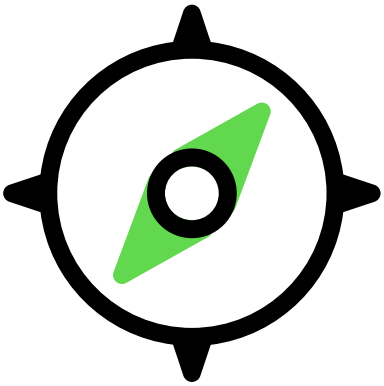
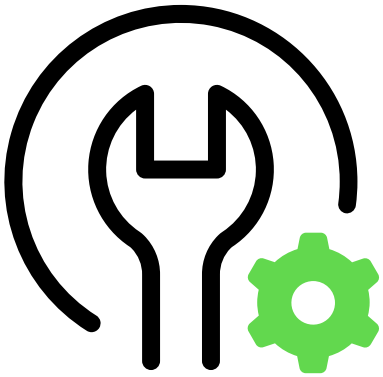
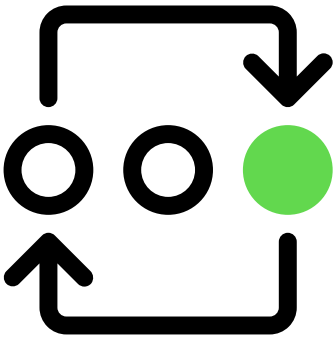
Feld	Beschreibung
Discovery-Mustername	Der Name des Musters.
Vorgeschlagene CMDB CI-Klasse	Der Name der CMDB-CI-Klasse. Dieses Feld ist bereits ausgefüllt, aber als Administrator können Sie es bei Bedarf ändern.
Vorgeschlagene Klassifiziererregel	Der Name des Prozesses, der mit der Aktion „Ignorieren“ von der Discovery ausgeschlossen wurde.
Genauigkeitsprozent	Ein Prozentsatz, basierend auf einem Validierungsalgorithmus, der die Qualität der Vorhersage überprüft. Wählen Sie Vorschläge mit höherer Genauigkeit aus. Sie können dieses Feld nicht ändern.
Vorgeschlagener Gruppenname	Der Name ITOM-Transparenz, der für den Vorschlag generiert wird. Dieses Feld ist bereits ausgefüllt, Sie können es jedoch bei Bedarf ändern.
Prozessanzahl	Die Anzahl der erkannten Prozesse, auf denen dieser Vorschlag basiert
Erweiterter Gruppenname	Die 10 wichtigsten Stichwörter, die weitere Informationen zum Prozess liefern. Predictive Intelligence extrahiert diese Stichwörter aus dem Prozess. Dieses Feld ist bereits ausgefüllt und kann nicht geändert werden.

Zertifikatsbestand-Management

Mit Zertifikatsbestand-Managementkönnen Sie alle TLS-Zertifikate erkennen, den Bestand darin durchführen und proaktiv verwalten. Zertifikatsbestand-Management unterstützt IPv6 und bietet damit eine umfassende Abdeckung für Ihre Zertifikatverwaltungsanforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Verwalten	Zertifikatsbestand-Management – Referenz
Zertifikatsbestand-Management	Zertifikatsbestand-Management	
		
Nutzen Sie Zertifikatsbestand-Management, um -Zertifikate zu erstellen und zu verwalten	Erfahren Sie, wie Sie einrichten Zertifikatsbestand-Management	Machen Sie sich mit Dashboards, Tabellen, Mustern und Begriffen vertraut

Problembehandlung und Hilfe

- Was ist Zertifikatverwaltung?
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Zertifikatsbestand-Management erkunden

Zertifikatsbestand-Management dient als zentralisierte und automatisierte Lösung für die Bewältigung der Komplexitäten der Zertifikatverwaltung. Sie erhöht die Sicherheit, stellt die Compliance sicher und bietet einen optimierten Ansatz für die Verwaltung des Lebenszyklus digitaler Zertifikate in einer Organisation.

Zertifikatsbestand-Management – Übersicht

Zertifikatsbestand-Management ist eine zentralisierte und automatisierte Lösung zur Optimierung der Nachverfolgung und Verwaltung digitaler Zertifikate in einer IT-Infrastruktur. Durch die Automatisierung der Discovery-, Bestands- und Überwachungsprozesse ermöglicht Zertifikatsbestand-Management Unternehmen die Pflege eines umfassenden Datensatzes von Zertifikaten, einschließlich wichtiger Details wie Ablaufdaten und Aussteller.

Das System erleichtert die Nachverfolgung in Echtzeit, automatisiert Routineaufgaben wie Verlängerungen und unterstützt die Anpassung an spezifische Unternehmensanforderungen. Mit Funktionen zur Integration in vorhandene CI-basierte Zeitpläne Discovery und Unterstützung für IPv6 bietet Zertifikatsbestand-Management Flexibilität und Effizienz bei der Verwaltung des gesamten Lebenszyklus von -Zertifikaten. Die rollenbasierte Zugriffssteuerung gewährleistet eine sichere und maßgeschneiderte Nutzung, während Warnungen und Benachrichtigungen Administratoren über kritische Ereignisse auf dem Laufenden halten und

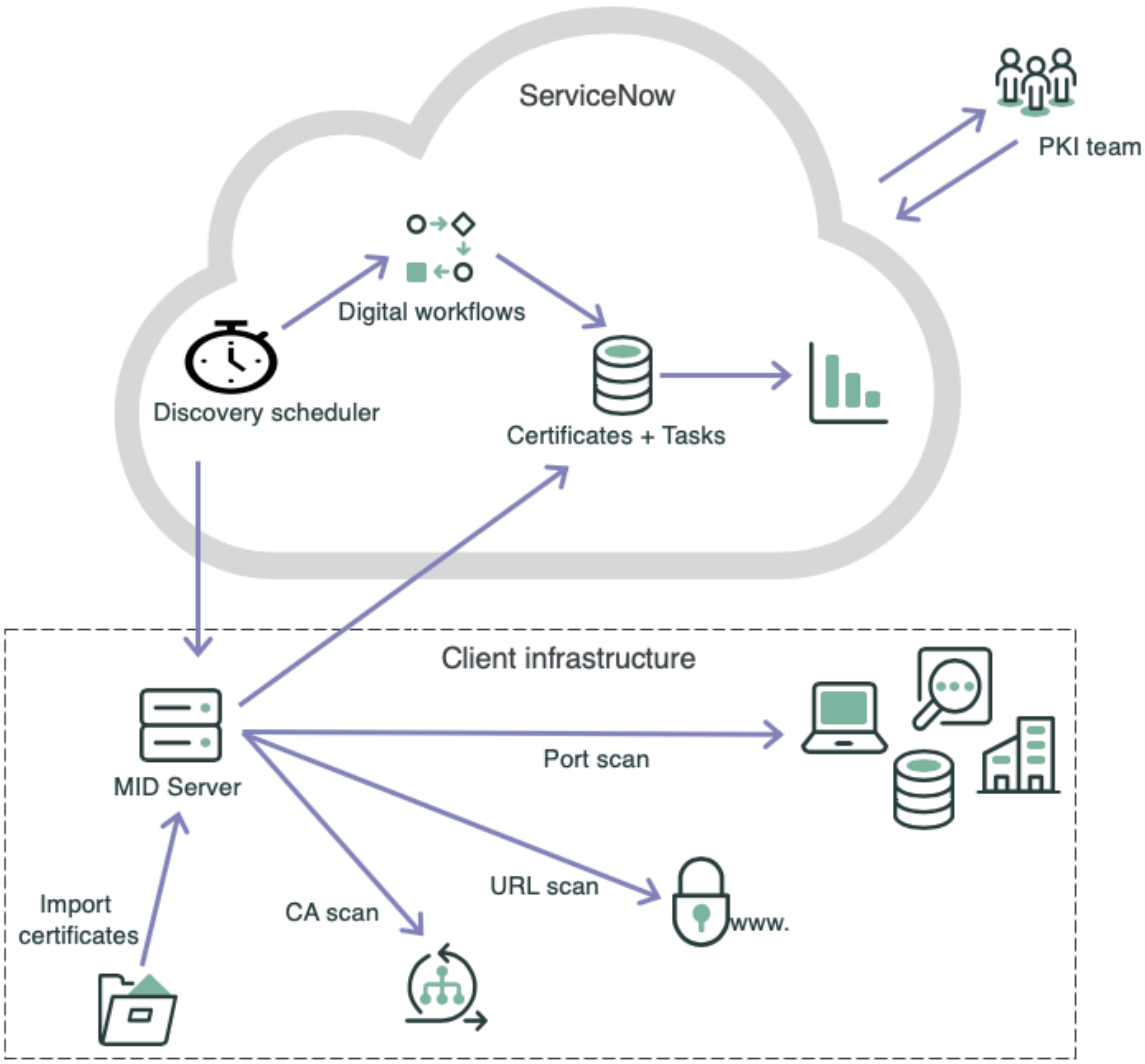
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

so zu erhöhter Sicherheit, Compliance und betrieblicher Effizienz bei der Zertifikatverwaltung beitragen.

Zertifikatsbestand-Management – Workflow

Zertifikatsbestand-Management optimiert den Prozess des Scannens von Zertifikaten durch die automatische Erkennung der Zertifikate an bestimmten Ports über Ihre etablierten, auf Configuration Items (CI) basierenden Zeitpläne Discovery. Darüber hinaus bieten Zertifikatsbestand-Management Benutzern die Flexibilität, neue Discovery -Zeitpläne zu generieren, die auf das Scannen einzelner URLs zugeschnitten sind. Dieser dynamische Ansatz gewährleistet eine robuste und anpassungsfähige Methode zum Erkennen und Verwalten von Zertifikaten und trägt zu einer sicheren und gut organisierten IT-Infrastruktur bei.

Prozessflussdiagramm



Weitere Informationen zur Funktionsweise von Zertifikatsbestand-Management finden Sie unter Prozess-Flow in Zertifikatsbestand-Management.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management – Vorteile

Vorteil	Funktion	Anwender
Verwaltung von TLS-Zertifikaten durch Verwaltung eines zentralen Bestands, Priorisierung von Zertifikaten und Nutzung von Verlängerungs-Workflows, um kostspielige Ausfälle zu vermeiden und eine sichere Umgebung zu gewährleisten.	Zertifikatsbestand-Management konfigurieren	Zertifikatadministrator [sn_disco_certmgmt.pki_admin]
Automatisierte Funktionen zur Optimierung der Nachverfolgung, um die manuelle Überwachung einer großen Anzahl von Zertifikaten zu verhindern. Verfolgen Sie einen proaktiven Ansatz, indem Sie sich über bevorstehende Ablaufdaten informieren, und tragen Sie so zu einer gut verwalteten und sicheren Zertifikatumgebung bei.	Zertifikatsbestand-Management verwenden	Zertifikatanwender [sn_disco_certmgmt.pki_user]
Eine sichere und konforme Zertifikatumgebung wird durch die Überwachung, Genehmigung, Validierung und Autorisierung der erforderlichen Aktionen im Zusammenhang mit Zertifikataufgaben und -Flows aufrechterhalten. Dieser umfassende Ansatz stellt sicher, dass Zertifikatverlängerungsaufgaben und Incidents für abgelaufene Zertifikate angemessen behandelt werden, und trägt zu einem robusten Sicherheits-Framework bei.	Zertifizierungsaufgaben genehmigen	Zertifikatgenehmiger pki_approver

Prozess-Flow in Zertifikatsbestand-Management

Zertifikatsbestand-Management ermöglicht Discovery die automatische Suche nach Zertifikaten an bestimmten Ports über Ihre vorhandenen CI-basierten Zeitpläne Discovery. Darüber hinaus können Sie neue Discovery-Zeitpläne zum Scannen einzelner URLs erstellen.

Funktionsweise von Zertifikatsbestand-Management

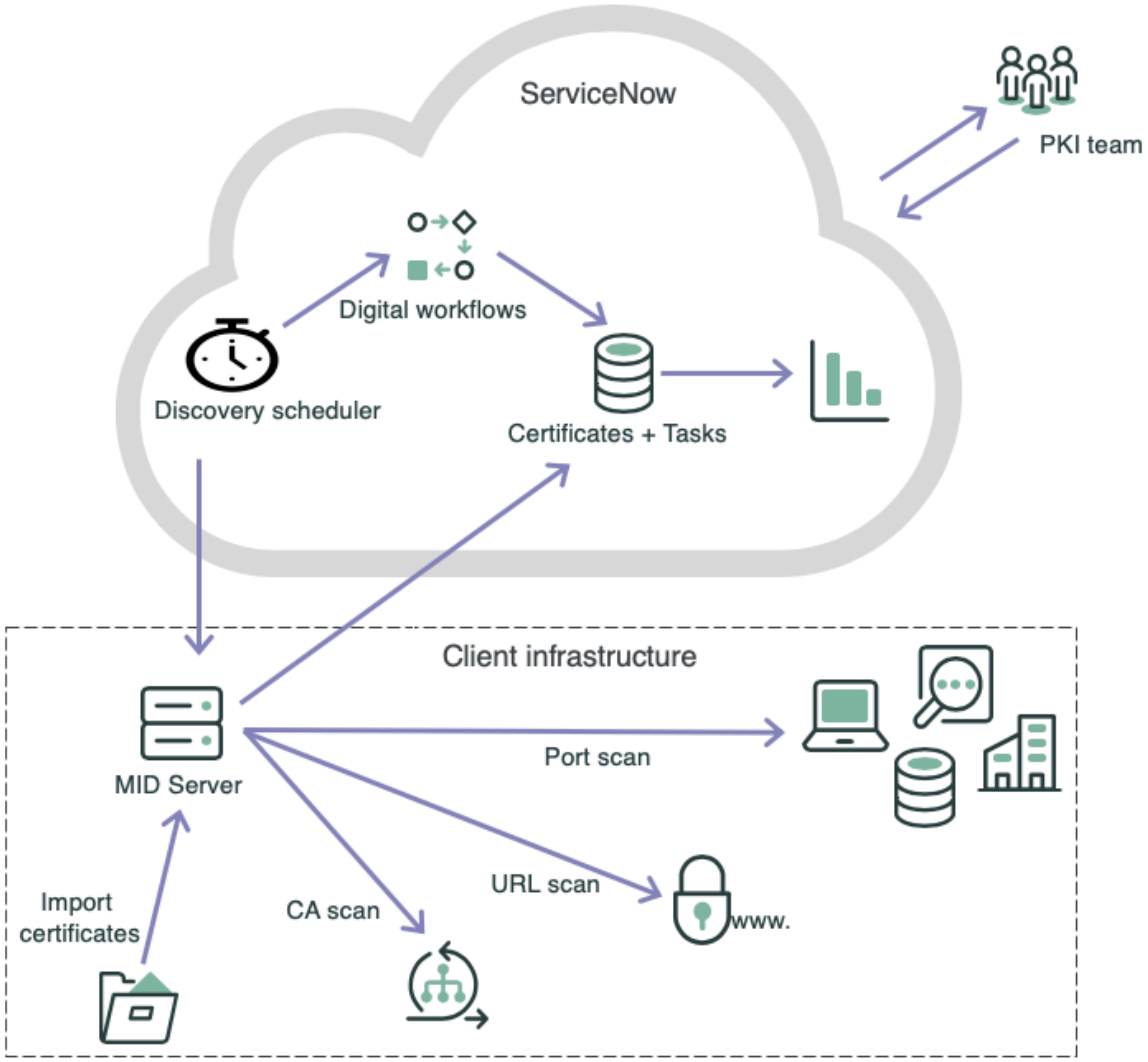
In Version 1.1.7 von Zertifikatsbestand-Management können Sie auch nach Zertifizierungsstellen suchen und Zertifikate aus Dateien importieren.

Mit dem Yokohama-Release können Sie Version 1.2.0 von Zertifikatsbestand-Management herunterladen. Sie können in der Tabelle „HTTP(S)-Endpunkt“ [cmdb_ci_endpoint_http] verwendete Zertifikate erkennen und in einem Massenvorgang eine Liste von SSL-Zertifikaten importieren. Sie können Ereignisse und Warnungen für ablaufende und abgelaufene Zertifikate erstellen und sich in Slack über ablaufende und abgelaufene Zertifikate benachrichtigen lassen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozessflussdiagramm



Der Prozess-Flow Zertifikatsbestand-Management ist in zwei verschiedene Phasen unterteilt:

- Phase vor der Discovery: Das erste Segment des Prozesses hängt von der Quelle der Zertifikat-Discovery ab. Diese Phase konzentriert sich auf Aktionen, die zum Identifizieren von Zertifikaten aus verschiedenen Quellen innerhalb der IT-Infrastruktur erforderlich sind.
- Phase nach der Discovery: Diese Phase umfasst nachfolgende Aktionen, die ausgeführt werden, nachdem die Zertifikate erfolgreich erkannt wurden. Sie umfasst Prozesse wie Katalogisierung, Nachverfolgung und Verwaltung von Zertifikaten, um eine sichere und effiziente Integration in das System zu gewährleisten.

Phase vor der Discovery

Die Phase vor der Erkennung umfasst vorbereitende Schritte, z. B. das Definieren von Scan-Parametern und das Konfigurieren von Anmeldeinformationen, um eine reibungslose Initiierung des Zertifikat-Discovery-Prozesses zu gewährleisten.

Discovery über Ports

Die Port-Probe [tls_ssl_certs] scannt automatisch 14 standardmäßig vorautorisierte Ports. Die Port-Probe [tls_ssl_certs] scannt automatisch 14 standardmäßig vorautorisierte Ports.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Typische Ports für SSL: 443, 8443, 9443, 636 (ldaps), 993 (imaps), 995 (popssl), 989, 990
- StartTLS-Ports: 25 (smtp), 110, 143, 389, 21, 587 (smtp)

Im Rahmen des CI-Prozesses Discovery während Shazzam verwendet der MID-Server Scanner, um Zertifikatketteninformationen von der IP-Portnummer zu erfassen und verschiedene Attribute zu erfassen, einschließlich der Zertifikathierarchie. MID-Server wandelt diese Zertifikate dann in eine XML-Nutzlast um und gibt sie für die -Instanz frei. Der Shazzam-Sensor erkennt wiederum den Eintrag in der ECC-Warteschlange und fügt einen neuen Datensatz in die Tabelle „Erkanntes Zertifikat“ [sn_disco_certmgmt_certificate_history] ein.

Die folgenden Felder werden aus der XML-Nutzlast abgerufen und im Java-Code der Shazzam-TLS-Port-Probe für erkannte Zertifikate überprüft: Certificate ID, Revocation_status, Subject, Issuer, Sans/, is_self_signed, is_ca, valid_from, valid_to, signature_algorithm,fingerabdruck_algorithm, key_size, serial_number und version.

Discovery über URL

Die Tabelle „Zertifikat-URL“ [sn_disco_certmgmt_cert_url] enthält eine Liste von URLs, die Ziele der Zertifikaterkennung darstellen. Jeder Datensatz enthält auch einen optionalen Verweis auf die Tabelle „Eindeutiges Zertifikat“ [cmdb_ci_certificate], um anzugeben, welches Zertifikat mit der angegebenen URL-Definition verknüpft ist. Die erforderlichen Parameter aus dem Zeitplan Discovery werden kombiniert, um den Status Discovery zu erstellen und zu initialisieren. Die Probe [CertificateDiscoveryFromURLScan] erkennt die Zertifikatkette für jede der URLs im Batch und gibt eine XML-Nutzlast aus, die die Zertifikatkette für jedes Zertifikat enthält. Er fügt auch einen neuen Datensatz in die Tabelle „Erkanntes Zertifikat“ [sn_disco_certmgmt_certificate_history] ein.

Discovery über Importzertifikate (Version 1.1.7, Zertifikatbestand und -verwaltung)

Die Importzertifikate werden über das Muster „SSL-Zertifikat importieren“ erkannt, das auf den folgenden Parametern basiert.

- Hostname/IP, auf dem/der die Zertifikate gehostet werden
- Ordner, in dem sich die Zertifikate befinden
- TLS_keepOriginalCertificate: Wenn Sie diesen Parameter auf „wahr“ setzen, kann dies zu einer erhöhten Nutzlast und möglicherweise zu Problemen mit unzureichendem Arbeitsspeicher führen.
- Mid_temp_folder: Der temporäre Ordner unter MID-Server, in den die Dateien vorübergehend kopiert werden.

Hinweis: Die Option zur automatischen Auswahl MID-Server wird für MID-Kombinationen aus Windows und Linux NICHT unterstützt. Wenn der MID-Server zum Speichern der ursprünglichen Zertifikatdateien verwendet wird, müssen Hostname/IP leer oder localhost sein, und der spezifische MID-Server für den Discovery-Zeitplan muss ausgewählt sein.

Discovery über CA-Berechtigung (Version 1.1.7 Certificate Inventory and Management)

Sobald die Anmeldeinformationen für das Zertifikatsbestand-Management-System entweder mit der Zertifizierungsstelle GoDindi, DigiCert, Entrust oder Sectigo eingerichtet wurden und der Zeitplan Discovery ausgeführt wird, führt das spezifische CA-Muster REST-API-Aufrufe an (GoDdie, DigiCert, Entrust oder Sectigo) aus und sammelt ruft die Liste der Zertifikate

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ab und speichert sie in den Tabellen [cmdb_ci_certificate], [certificate_domain] und [sys_attachment].

„ca_api_url“ und „ca_api_version“ sind optionale Parameter. Wenn diese Parameter innerhalb von Musterparametern leer gelassen werden, werden Standardwerte verwendet. Die Standardwerte umfassen:

- DigiCert – Zertifikatverwaltung (ca_api_version = v2, ca_api_url = https://www.digicert.com/services/)
- Entrust – Zertifikatverwaltung (ca_api_version = v2, ca_api_url = https://api.entrust.net/enterprise/)
- GoDdies Zertifizierungsverwaltung (ca_api_version = v1, ca_api_url = https://api.goddie.com/)
- Sectigo – Zertifikatverwaltung (ca_api_version = v1, ca_api_url = https://cert-manager.com/api/ssl/)

Die Argumente für die Muster GoDdy, DigiCert, Entrust und Sectigo lauten wie folgt. Ab Version 1.2.0 können Sie Sectigo und Entrust Certificate Authorities (CAs) scannen.

- Start_offset: Die Offset-Position zum Lesen von Zertifikaten von CA-Behörden mit einem Standardwert von 0.
- Limit: Die Anzahl der Zertifikate, die ab start_offset gelesen werden sollen, mit einem Standardwert von 1500.
- CredentialAlias: Der Name des Anmeldeinformationsalias oder Tags, der mit den CA-Anmeldeinformationen verknüpft ist und in der Konfiguration des serverlosen Ausführungsmusters hinzugefügt wurde.

  Wenn der Parameter TLS_keepOriginalCertificate auf „true“ festgelegt ist, wird die Zertifikatdatei an das Zertifikat-CI angehängt. Dies kann die Nutzlast erhöhen, was möglicherweise zu Problemen mit unzureichendem Arbeitsspeicher führt.

- IncludeCertStatus: Ein Parameter zum Angeben zusätzlich zu den Standardwerten zu erkennender zusätzlicher Zertifikatstatus.

Zertifikatstatus nach Zertifizierungsstellen

Zertifizierungsstelle	Standardstatus erkannt
Sectigo	◦ Ausgegeben ◦ Abgelaufen
DigiCert und GoDdies	◦ Aktiv ◦ Abgelaufen ◦ Widerrufen ◦ Abgebrochen
Entrust	◦ Aktiv ◦ Abgelaufen ◦ Widerrufen

Sie können mehrere Zertifikatstatus angeben, indem Sie die einzelnen Status durch Kommas trennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Das Feld **„Status“** in der Tabelle „Eindeutiges Zertifikat“ [cmdb_ci_certificate] gibt den Lebenszyklusstatus des Zertifikats an, nicht den Rohstatus aus der API. Wenn die API Status wie „Ausgestellt“, „Gültig“, „Abgelaufen“ oder „Abgebrochen“ zurückgibt, werden sie in der Tabelle „Eindeutiges Zertifikat“ [cmdb_ci_certificate] als „ausgestellt“ gespeichert.

Sobald die Phase vor der Discovery abgeschlossen ist, fahren Sie mit der Phase nach der Discoveryfort.

Phase nach der Discovery

Nach der Discovery-Phase verwaltet das System TLS-Zertifikate und bietet Flexibilität für manuelle und automatisierte Anforderungsoptionen für verschiedene zertifikatsbezogene Aufgaben und Prozesse.

Die von der Zertifizierungsstelle und dem Stamm signierten TLS-Zertifikatketten füllen die Tabellen „Eindeutiges Zertifikat“ [cmdb_ci_certificate] und „Installiertes Zertifikat“ [sn_disco_certmgmt_cmdb_installed_certificate]. Anschließend überprüft eine regelmäßige Aufgabe die Tabelle „Eindeutiges Zertifikat“ auf ablaufende und abgelaufene Zertifikate und initiiert die Erstellung und Zuweisung von Zertifikataufgaben und Incidents.

Sie haben die Möglichkeit, manuell neue Zertifikate anzufordern und vorhandene Zertifikate zu verlängern. Weitere Informationen finden Sie unter Manueller Flow für Zertifikatanforderungen.

In Version 1.3.8 wurde die Möglichkeit eingeführt, Anforderungen für neue, verlängerte oder widerrufene Zertifikate zu automatisieren. Weitere Informationen finden Sie unter Automatisierte Zertifikatverwaltung für TLS-Zertifikate.

Zur Optimierung der Systemleistung entfernt eine Tabellenbereinigung nach einer angegebenen Anzahl von Tagen automatisch alte Zertifikatdatensätze aus diesen beiden Tabellen:

- Tabelle „Erkanntes Zertifikat“ [sn_disco_certmgmt_certificate_history]: älter als 30 Tage
- Tabelle „Installiertes Zertifikat“ [sn_disco_certmgmt_cmdb_installed_certificate]: älter als 90 Tage

Hinweis: Sie können verschiedene Verhaltensweisen in Bezug auf Zertifikatsbestand-Management je nach Bedarf mithilfe bestimmter Zertifikateigenschaften umschalten (siehe Discovery-Eigenschaften und Systemeigenschaften) .

Zertifikatsbestand-Management Rollen und Zuständigkeiten

Dedizierte Benutzer mit spezialisierten Rollen werden zugewiesen, um die Überwachung und Nachverfolgung von Anforderungen für neue und verlängerte Zertifikate zu optimieren.

Das Dashboard Zertifikatsbestand-Management und die Zertifikatkonfigurationseinstellungen werden je nach zugewiesenen Rollen aktiviert oder deaktiviert.

Rolle	Verantwortlichkeiten
Zertifikatadministrator [sn_disco_certmgmt.pki_admin]	Der Headless-Benutzer (ein Account, der nicht an einen bestimmten Benutzer gebunden ist) ist im Basissystem enthalten und mit der Rolle *sn_disco_certmgmt.pki_admin* ausgestattet. Es fungiert als Anrufer für automatisch generierte Verlängerungsaufgaben für Zertifikate und Incidents. Um diesen Anwender anzupassen, passen Sie die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Verantwortlichkeiten
	Anwender-ID mithilfe der Discovery-Eigenschaft an: *glide.discovery.certs.cert_admin_user_id*, anstatt sie als standardmäßigen monitorlosen Anwender zu belassen. Diese Rolle ist für die Änderung nicht standardmäßiger Attribute im ursprünglichen Zertifikatdatensatz verantwortlich und kann Attribute wie Status, Status, „Zugewiesen an“, Zuweisungsgruppe, Verlängerungsnachverfolgung und Servicetyp ändern. Die inhärenten Attribute des Zertifikats bleiben unverändert. Der Standardstatus für erkannte Zertifikate ist „Installiert“, aber diese Rolle kann ihn manuell an andere Status wie „Ausgestellt“, „Installiert“, „Widerrufen“ und „Deaktiviert“ anpassen. Darüber hinaus können Benutzer mit dieser Rolle verschiedene Dashboards anzeigen und verfügen über Lese-/Schreibzugriff auf Zertifikate und Zertifikataufgaben, die dem Zertifikat Discoveryzugeordnet sind. **Hinweis:** • Die Rolle sn_disco_certmgmt.pki_admin enthält die Rolle sn_disco_certmgmt.pki_user. • Alle Benutzer mit der Rolle pki_admin können dem Genehmigerfeld im Zertifikatanforderungsformular hinzugefügt werden. Benutzern mit der Rolle pki_admin sollte die Rolle approved_admin manuell zugewiesen werden, um Anforderungen aus dem Zertifikataufgabenformular zu genehmigen oder abzulehnen. Dieser Genehmiger muss sich nicht anmelden, um die Aufgabe zu genehmigen. In einem Zertifikataufgabenformular oder einer zugehörigen Liste kann der Systemadministrator oder ein Benutzer mit der Rolle approved_admin oder pki_admin mehrere Genehmiger hinzufügen oder den vorhandenen Genehmiger bearbeiten. • Die Rolle approver_user ist erforderlich, wenn der Benutzer eine Anforderung genehmigen möchte, indem er sich anmeldet. Ohne die Rolle approver_user kann ein Benutzer nicht zu **Meine Genehmigungen** navigieren, um die Anforderungen zu genehmigen.
Zertifikatanwender [sn_disco_certmgmt.pki_user]	Diese Rolle ist für die Überwachung der Zertifikat-Discovery verantwortlich und erhält die Möglichkeit, auf verschiedene Dashboards zuzugreifen. Außerdem verfügt sie über Lese-/Schreibberechtigungen für Zertifikate und zugehörige Zertifikataufgaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Verantwortlichkeiten
Zertifikatgenehmiger [sn_disco_certmgmt.pki_approver]	Ein Anwender mit dieser Rolle (normaler Anwender) ist für Zertifikatanforderungen verantwortlich und kann Zertifikatanforderungen über das Formular Servicekatalog initiieren.
Anfordernde Person des Zertifikats [sn_disco_certmgmt.certificate_requester]	Diese Rolle ist für die Übermittlung von Zertifikatanforderungen verantwortlich und kann Zertifikate von Servicekataloganfordern und verlängern.

Zertifikatsbestand-Management konfigurieren

Erstellen Sie einen optimierten Prozess, um Einblicke in das Zertifikatbestandsmanagement zu erhalten, der wichtige Aspekte wie Zertifikat-Discovery, Massen-Upload-Funktionalität, Wartung von Zertifikatkettenbeziehungen, Konfiguration von Anmeldeinformationsbezeichnern, Anpassung des Systems, Erstellung von Neu-/Verlängerungsanforderungen, Archivierungsaufgaben und Automatisierung abdeckt von TLS-Zertifikatverwaltung, Integration mit Ereignismanagement, Slack-Benachrichtigungen für Warnungen und Nutzung von cert-Manager für eine effiziente Zertifikatgenerierung.

Konfiguration – Übersicht

Bevor Sie Zertifikatsbestand-Managementverwenden, müssen Sie die erforderlichen Plugins einrichten, die Aktivierung sicherstellen, Ihre Instanz auf die neueste Version aktualisieren und die Anwendung Zertifikatsbestand-Management von ServiceNow Storeherunterladen. Weitere Einzelheiten finden Sie unter Erste Schritte mit Zertifikatsbestand-Management.

Nachdem die Voraussetzungen erfüllt sind, können Sie mit den folgenden Aufgaben fortfahren.

Zertifikatsbestand-Management Aufgaben

Aufgabe	Beschreibung
Transparenz von TLS-Zertifikaten	Richten Sie ein effizientes Certificate Inventory Management-System ein, indem Sie die Zertifikat-Discovery konfigurieren, Massen-Uploads von Zertifikaten ermöglichen, Kettenbeziehungen verwalten, sicheren Zugriff konfigurieren und das System an die spezifischen Organisationsanforderungen anpassen.
Manueller Flow für Zertifikatanforderungen	Ermöglichen Sie die Erstellung neuer Zertifikatanforderungen oder Zertifikatverlängerungen im System unter Einhaltung definierter Richtlinien. Implementieren Sie einen Prozess zur Archivierung abgeschlossener Zertifikataufgaben und zur Verwaltung eines Verlaufsdatensatzes für Audit- und Compliance-Zwecke.
Automatisierte Zertifikatverwaltung für TLS-Zertifikate	Richten Sie Automatisierungsprozesse ein, um TLS-Zertifikate nach Bedarf zu verwalten,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management Aufgaben (Fortsetzung)

Aufgabe	Beschreibung
	einschließlich Verlängerung, Aktualisierung und Sperrung.
Zertifikatintegrationen und -benachrichtigungen	Stellen Sie eine Integration zwischen Event Management-Systemen und Certificate Inventory Management her, um Echtzeitüberwachung und Reaktion auf zertifikatsbezogene Ereignisse zu ermöglichen. Konfigurieren Sie Benachrichtigungen, die an Slack-Kanäle gesendet werden, um Stakeholder über kritische Zertifikatereignisse und Änderungen auf dem Laufenden zu halten.
Zertifikatgenerierung über Zertifikat-Manager-Integration	Verwenden Sie den Zertifikatmanager oder ein ähnliches Tool, um den Zertifikatgenerierungsprozess zu automatisieren und eine effiziente und sichere Ausstellung basierend auf vordefinierten Richtlinien sicherzustellen.

Erste Schritte mit Zertifikatsbestand-Management

Bevor Sie sich mit den Funktionen Zertifikatsbestand-Management von vertraut machen, müssen Sie die erforderlichen Anforderungen erfüllen, indem Sie das Plugin „“ installieren und aktivieren, Ihre Instanz aktualisieren und die Anwendung von ServiceNow Storeabrufen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Hinweis: Im ServiceNow Store werden regelmäßig neue Anwendungen und Updates für die von ServiceNow erstellten Anwendungen veröffentlicht. Wenn Sie bereits über die Anwendung verfügen, können Sie die neueste Version herunterladen, um Ihre bestehende Experience mit unseren Produkten zu verbessern. Da bei jeder Veröffentlichung einer Anwendung im Store neue Funktionen verfügbar sind oder Funktionen erweitert wurden, werden die in einem bestimmten Release verfügbaren Inhalte und Features in der Dokumentation mit der Versionsnummer angegeben.

Prozedur

1. Stellen Sie sicher, dass die folgenden Plugins installiert und aktiviert sind.
   - ITOM-Transparenz Plugin „“ [com.snc.itom.vis.license]
   - Plugin Discovery [com.snc.discovery]
   - Configuration Management for Scoped Apps (CMDB) [com.snc.cmdb.scoped]
2. Vergewissern Sie sich, dass Ihr System auf Yokohama oder höher aktualisiert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während des Upgrade-Prozesses wird das Plugin Zertifikatsbestand-Management [com.sn_disco_certmgmt] automatisch installiert, wenn die Plugins ITOM-Transparenz [com.snc.itom.vis.license] und Discovery [com.snc.discovery] bereits installiert sind.

3. Laden Sie die Anwendung Zertifikatsbestand-Management von ServiceNow Storeherunter.

Ergebnisse
Sie sind bereit für die ersten Schritte mit Zertifikatsbestand-Management.

Hinweis: MID-Server benötigt je nach Anwendungsfall Zugriff auf die folgenden Endpunkte:

- Entrust: Zertifikat-URL erkennen: `https://api.entrust.net/enterprise/`
- URL zum Herunterladen des Entrust-Stammzertifikats: `https://web.entrust.com/root-certificates/`
- DigiCert: `https://www.digicert.com/services/`
- Sectigo: `https://cert-manager.com/api/ssl/`
- GoDaddy: `https://api.godaddy.com/`

Transparenz von TLS-Zertifikaten

Die Anwendung Zertifikatsbestand-Management ermöglicht Discovery die automatische Suche nach Zertifikaten an bestimmten Ports über Ihre vorhandenen CI-basierten Discovery-Zeitpläne. Darüber hinaus können Sie Discovery-Zeitpläne zum Scannen einzelner URLs erstellen.

Im ServiceNow Store werden regelmäßig neue Anwendungen und Updates für die von ServiceNow erstellten Anwendungen veröffentlicht. Wenn Sie bereits über die Anwendung verfügen, können Sie die neueste Version herunterladen, um Ihre bestehende Experience mit unseren Produkten zu verbessern. Da bei jeder Veröffentlichung einer Anwendung im Store neue Funktionen verfügbar sind oder Funktionen erweitert wurden, werden die in einem bestimmten Release verfügbaren Inhalte und Features in der Dokumentation mit der Versionsnummer angegeben.

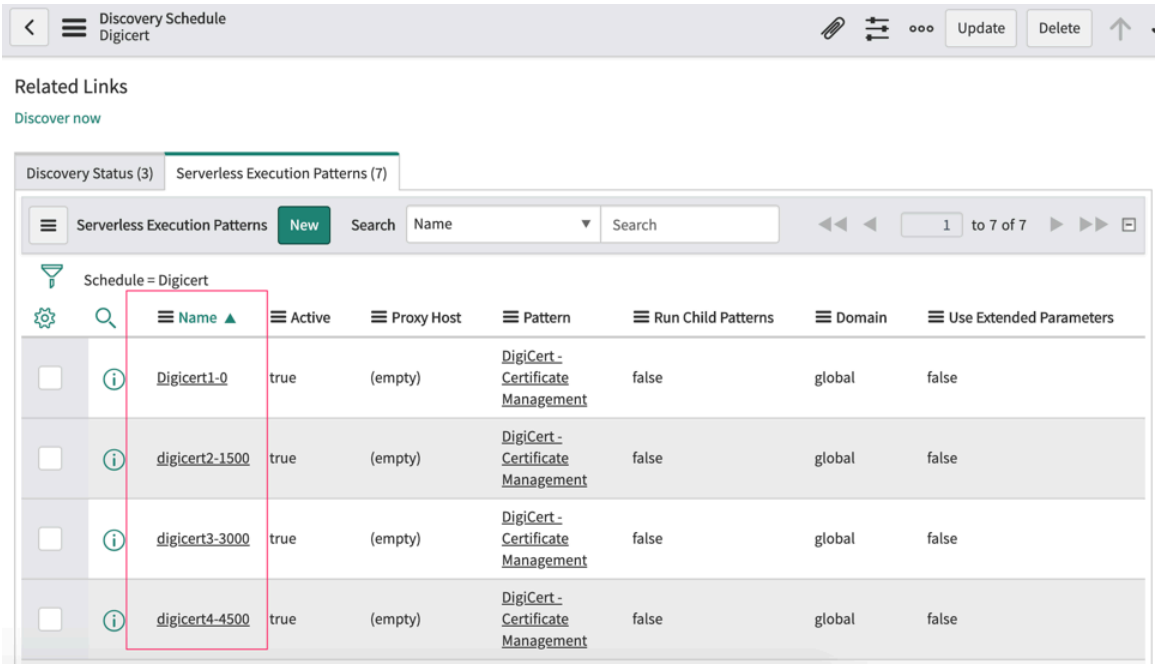
In Zertifikatsbestand-Management Version 1.1.7 können Sie eine Liste importierter Zertifikate hinzufügen und nach Zertifikaten von Ihrer Zertifizierungsstelle (CA) wie GoDaddy und DigiCert suchen. In Version 1.2.0 können Sie auch nach den CAs Sectigo und Entrust scannen.

In Version 1.3.8 von Zertifikatsbestand-Management wurden in der Anwendung vorhandene Zertifizierungsstellenmuster für DigiCert erweitert, um die folgenden Felder als Teil der Zertifikatserkennung der CA-Vertrauensstellung zu erfassen. Alle diese Felder werden in der Tabelle „Zertifikatverlängerungen“ [sn_disco_certmgmt_certificate_extension] gespeichert.

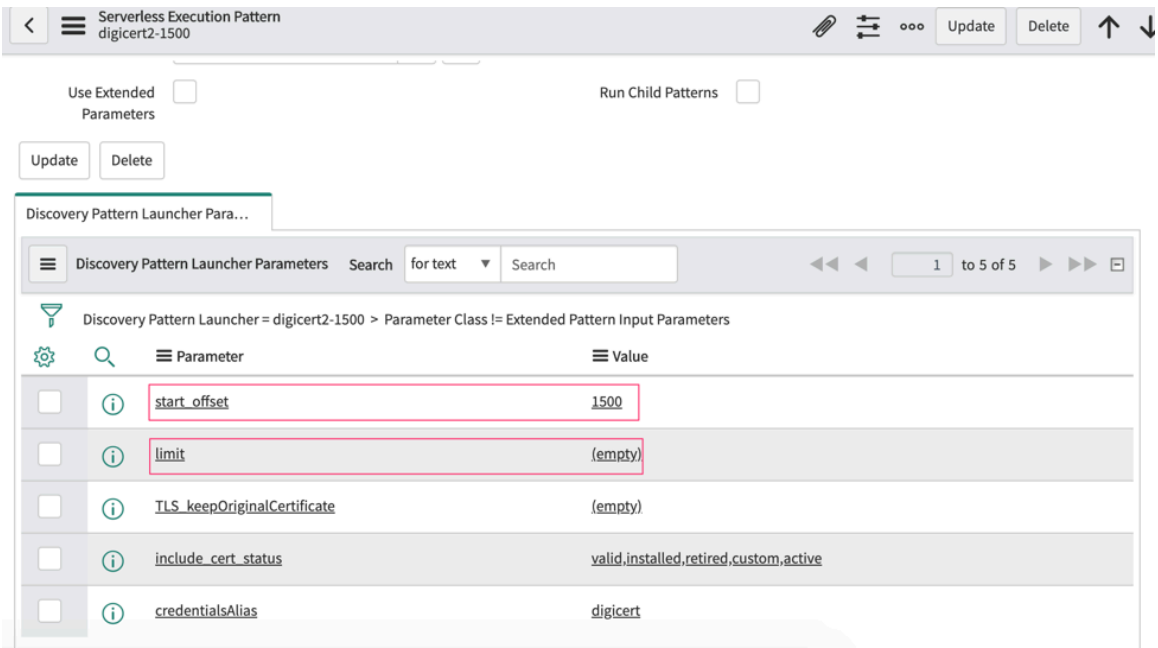
- Zertifikat-ID
- Auftrags-ID
- Fingerabdruck
- Seriennummer
- Zertifikatstatus

Um Zertifikate zu importieren oder die Vertrauensstellung einer Zertifizierungsstelle mit mehr als 1500 Zertifikaten zu erkennen, erstellen Sie einen Erkennungszeitplan mit mehreren konfigurierten serverlosen Mustern. Jede Musterausführung unterstützt die Erkennung von maximal 1500 Zertifikaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Zum Erkennen aller Zertifikate müssen „limit“ (Standardwert: 1500) und „start_offset“ (Standardwert: 0) entsprechend konfiguriert werden. Um beispielsweise bis zu 6.000 Zertifikate abzurufen, fügen Sie vier serverlose Muster mit start_offset 0, 1500, 3000 und 4500 hinzu. Die Parameter „start_offset“ and „limit“ werden wie dargestellt konfiguriert.



Wenn über Port-Scans ausführen

Wenn die TLS-Port-Probe [tls_ssl_certs] aktiviert ist, scannt Discovery automatisch 14 vorautorisierte Ports als Teil Ihrer vorhandenen CI-Zeitpläne Discovery.

Vorbereitungen

Erforderliche Rolle: admin oder discovery_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Aktivieren Sie die Port-Probe „TLS“ [tls_ssl_certs].
   a. Navigieren zu **Discovery-Definition** > **Anschlussprobes**.
   b. Öffnen Sie **tls_ssl_certs**.
   c. Um die Probe zu aktivieren, aktivieren Sie das Kontrollkästchen **Aktiv**.
      Standardmäßig ist das Kontrollkästchen für Neuinstallationen deaktiviert.
   d. Speichern Sie die Änderungen.
2. Fügen Sie einen IP-Service hinzu, um die Port-Probe „TLS“ zu konfigurieren.
   a. Navigieren zu **Discovery-Definition** > **IP-Services**.
   b. Erstellen Sie einen neuen IP-Service mit einem Port.
3. Konfigurieren Sie die Port-Probe „TLS“.
   Bearbeiten Sie die Port-Probe-Definition, um bis zu 138 zusätzliche Ports hinzuzufügen oder vorhandene zu entfernen.
   a. Navigieren zu **Discovery-Definition** > **Anschlussprobes**.
   b. Öffnen Sie **tls_ssl_certs**.
   c. Entsperren Sie das Feld **Ausgelöst durch Services**, indem Sie das Sperrsymbol daneben wählen.
   d. Entfernen Sie alle Ports aus der Liste, oder fügen Sie zusätzliche aus dem Suchbereich hinzu.
   e. Speichern Sie die Änderungen.

Ergebnisse
Ihre vorhandenen Discovery-Zeitpläne sollten an den angegebenen Ports dann automatisch nach Zertifikaten scannen.

Zertifikaterkennung über individuelle URL-Scans ausführen

Um die Zertifikat-Discovery über URL-Scans zu initiieren, müssen Sie einzelne URLs manuell einfügen und einen neuen Zeitplan für das Zertifikat Discovery konfigurieren.

Vorbereitungen
Erforderliche Rolle: admin oder discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Nur die Zertifikate, die während URL-Scans auf dem Server verfügbar sind, können erkannt werden. Um die verfügbaren Zertifikate zu bestätigen, verwenden Sie den folgenden Befehl:

```
openedsl s_client -showcerts -connect<URL> :<PORT>
```

Prozedur

1. Navigieren zu **Alle** > **Zertifikatverwaltung** > **Quell-URLs für Zertifikat-Discovery**.
2. Um der Tabelle einzelne URLs hinzuzufügen, wählen Sie **Neu**aus.
   Stellen Sie sicher, dass Sie genaue Ergebnisse erhalten, indem Sie URLs im folgenden Format eingeben: schema://host:port. Der Port ist optional, und Standardwerte werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verwendet, wenn keine angegeben sind. Beispiele: https://www.servicenow.com oder https://servicenow.com:443, ldaps://myldap.com oder ldaps://myldap.com:636.

3. Erstellen Sie einen Discovery-Zeitplan mit den folgenden Feldern.
   Weitere Informationen zum Einrichten von Discovery -Zeitplänen finden Sie unter Horizontal-Discovery planen.

   a. Wählen Sie **Discovery**: **Zertifikate**.

   b. Wählen Sie **Typ der Zertifikaterkennung**:**URL-Zertifikaterkennung** aus.

      Behalten Sie die Batchgröße unverändert, es sei denn, es gibt eine spezifische Empfehlung, sie zu ändern.

4. Um andere URLs hinzuzufügen oder zu löschen, wählen Sie auf der Registerkarte **Zertifikat-URLsdie Option Bearbeiten**aus.
5. Wählen Sie **Absenden**.
6. Aktivieren Sie das Kontrollkästchen, um URLs aus der Tabelle „HTTP(s)-Endpunkt“ [cmdb_ci_endpoint_http] in den Discovery-Prozess einzubeziehen.

Ergebnisse

Wenn Ihr Discovery-Zeitplan ausgeführt wird, wird in den angegebenen URLs automatisch nach Zertifikaten gescannt, und alle URLs werden aus der Tabelle cmdb_ci_endpoint_http abgerufen. Anschließend wird eine Zuordnung zwischen der URL und dem Zeitplan in *sn_disco_certmgmt_cert_url_sched_m2m* erstellt.

Wenn Service-Mapping aktiviert ist, wird standardmäßig eine Beziehung zwischen dem HTTP-Endpunkt und der Anwendung erstellt, wenn ein Eintrag in cmdb_ci_endpoint_http erstellt wird. Beispielsweise wird die Anwendung Amazon automatisch mit amazon.com verknüpft.

Die Beziehung lautet: cmdb_ci_endpoint_http[übergeordnet] --> [Endpunkt implementieren in::Endpunkt implementieren von] --> cmdb_ci_appl[untergeordnet].

Wenn die obige Beziehung vorhanden ist, erstellt die URL-Zertifikaterkennung eine zusätzliche Beziehung zwischen dem Zertifikat und der Anwendung. Diese Beziehung lautet: cmdb_ci_appl[übergeordnet] --> [Verwendet::Verwendet von] --> cmdb_ci_certificate[untergeordnet].

Hinweis: URL-Discovery-Zeitpläne generieren keine Server Configuration Items (CIs).

Massen-Upload von Zertifikaten verwenden

Ab Zertifikatsbestand-Management Version 1.2.0 haben Sie die Möglichkeit zum effizienten Massenimport von SSL-Zertifikaten, sodass Sie bis zu 5000 Zertifikate in einer einzigen XLSX-Datei hochladen können, um Zeit und Ressourcen zu sparen.

Vorbereitungen

Erforderliche Rolle: pki_user oder pki_admin

Dem Standardadministrator sind die Rollen pki_user und pki_admin zugewiesen. Anwender mit den folgenden Rollen haben Zugriff auf den Massen-Upload von Zertifikaten.

- sn_disco_certmgmt.pki_user
- sn_disco_certmgmt.pki_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatverwaltung** > **Massen-Upload von Zertifikaten durchführen**.
2. Wählen Sie auf der Seite „Massen-Upload“ den Link **Vorlagendatei herunterladen** (.xlsx), um die Datei „`sample_cmdb_ci_certificate.xlsx`“ herunterzuladen.
3. Öffnen Sie die heruntergeladene Datei `sample_cmdb_ci_certificate.xlsx`.
4. Sehen Sie sich die Beispielwerte in den Spalten an, und fügen Sie die Eigenschaften des SSL-Zertifikats den entsprechenden Spalten hinzu.

   Jeder Eintrag in der Excel-Tabelle entspricht einem CI-Zertifikat. Stellen Sie sicher, dass die folgenden Pflichtspalten ausgefüllt sind.

   - root_issuer
   - issuer
   - subject_common_name
   - issuer_common_name
   - fingerprint
   - issuer_distinguished_name
   - subject_distinguished_name
   - fingerprint_algorithm
   - valid_to: Darf nicht kleiner als valid_fom sein. In Millisekunden. Beispiel: 1586789478000 stellt den 13. April 2020, 14:51:18 Uhr dar.
   - valid_from: In Millisekunden. Beispiel: 1586789478000 stellt den 13. April 2020, 14:51:18 Uhr dar.
   - signature_algorithm
   - key_size
   - Zustand: ausgegeben, installiert, widerrufen, deaktiviert oder sonstige

   Hinweis: Um die Kettenbeziehung des Zertifikats aufrechtzuerhalten, muss jedes Zertifikat den Fingerabdruck seines Stammzertifikats in der Spalte **„root_issuer“** und den Fingerabdruck seines Ausstellers in der Spalte „ **Aussteller“** enthalten. Bei selbstsignierten Zertifikaten müssen **„root_issuer“** und **„issuser“** den Wert des Fingerabdrucks des Zertifikats aufweisen.

5. Speichern Sie die Datei `sample_cmdb_ci_certificate.xlsx`.
6. Navigieren zu **Zertifikatverwaltung** > **Massen-Upload von Zertifikaten durchführen**.
7. Wählen Sie **Datei durchsuchen** und dann die vollständige Datei `sample_cmdb_ci_certificate.xlsx` aus.
8. Wählen Sie **Hochladen** aus.

Ergebnisse

Wenn beim Upload Fehler auftreten, werden eine Warnmeldung und ein Link zu den Fehlerprotokollen angezeigt. Nur Benutzer mit der Administratorrolle können diese Protokolle anzeigen. Fehler können auftreten, wenn ein Pflichtfeld leer gelassen wird oder wenn ein valid_from-Epochenwert größer als valid_to ist.

Nachdem die Datei erfolgreich hochgeladen wurde, wird eine Erfolgsmeldung mit einem Umleitungslink *View All* angezeigt. Sie können eine Liste der Zertifikate anzeigen, die der Tabelle „Eindeutiges Zertifikat“ [cmdb_ci_certificate] hinzugefügt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikaterkennung über Zertifikatdateiimport ausführen

In Zertifikatsbestand-Management Version 1.1.7 können Sie Zertifikate erkennen, indem Sie Zertifikatdateien mithilfe der musterbasierten Discovery in das System importieren.

Vorbereitungen

Stellen Sie sicher, dass „TLS_keepOriginalCertificate“ auf „falsch“ festgelegt ist.

Stellen Sie sicher, dass das Zertifikat in einem der folgenden Formate vorliegt: .cert, .pem, .txt, .der.

Erforderliche Rolle: admin oder discovery_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Importzertifikate werden mithilfe des Musters „SSL-Zertifikat importieren“ erkannt, das auf den folgenden Parametern basiert:

- Server: Hostname oder IP-Adresse, unter der die Zertifikate gehostet werden. Wenn Sie aus MID-Serverimportieren, geben Sie „localhost“ an, und lassen Sie „temp_certificate_folder“ leer.
- server_certificate_folder: Ordnerpfad auf dem Server, der die Zertifikate enthält.
- Parameter „TLS_keepOriginalCertificate“: Auf „falsch“ setzen, um potenzielle Probleme aufgrund von unzureichendem Arbeitsspeicher aufgrund der erhöhten Nutzlast zu vermeiden.
- temp_certificate_folder: Temporärer Ordner unter MID-Server, in den Dateien kopiert werden.

Prozedur

1. Erstellen Sie einen Discovery-Zeitplan mit den folgenden Feldern.
   Weitere Informationen zum Einrichten von Discovery -Zeitplänen finden Sie unter Horizontal-Discovery planen.
   a. Wählen Sie **Discovery**: **Zertifikate importieren** aus.
   b. Wählen Sie **Typ der Zertifikaterkennung**: **Zertifikate importieren** aus.
   c. Wählen Sie **Methode für MID Server-Auswahl**: **Spezifischer MID Server** aus.
   d. **MID-Server**auswählen: Wählen Sie den gewünschten MID-Server aus.
   e. Fügen Sie die Anmeldeinformationen für den Hostcomputer Windows oder Linux hinzu, auf dem sich die Zertifikate befinden.
   f. Füllen Sie alle anderen erforderlichen Felder aus.
   g. Wählen Sie **Speichern**.
2. Um das Muster „SSL-Zertifikat importieren“ hinzuzufügen, wählen Sie auf der Registerkarte **Muster für Ausführung ohne Server** die **Option Neu**aus.

Ergebnisse

Wenn Ihr Discovery-Zeitplan ausgeführt wird, werden Ihre Dateien automatisch gescannt.

Zertifikatkettenbeziehungen über Zertifikatimport verwalten

Die Verwaltung von Zertifikatkettenbeziehungen über Zertifikatimport stellt die Integrität und Sicherheit digitaler Zertifikate sicher und validiert ihre Authentizität in einem System.

Zur Verwaltung von Zertifikatkettenbeziehungen wird als Erweiterung der Branchenstandard .txt verwendet. Zertifikatkettenbeziehungen werden nicht mit anderen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateierweiterungen verwaltet. Die erwartete Reihenfolge von Zertifikaten in einer TXT-Zertifikatkettendatei lautet: Serverzertifikat, Zwischenzertifikat und Stammzertifikat.

Anwendungsfälle:

- Wenn zwei oder mehr Zertifikate gefunden werden, die Formate wie .cert und .pem aufweisen, wird nur das erste Zertifikat berücksichtigt. Die anderen Zertifikate werden nicht verarbeitet, und es werden keine Zertifikatkettenbeziehungen verwaltet.
- Wenn eine TXT-Erweiterung vorhanden ist, die nur ein Zertifikat enthält, wird sie als Serverzertifikat betrachtet, und es werden keine Zertifikatbeziehungen verwaltet.
- Wenn eine TXT-Erweiterung vorhanden ist, die zwei Zertifikate enthält, wird das erste Zertifikat als Serverzertifikat und das zweite Zertifikat als Stammzertifikat betrachtet (keine Zwischenzertifikate).

Hinweis: Die Beziehung der Zertifikatkette hängt von der letzten Ausführung der URL-/IP-Discovery ab. Durch das Importieren einer Datei ohne Zertifikatkettenbeziehungen werden alle vorhandenen Kettenbeziehungen unterbrochen, die demselben Zertifikat (Fingerabdruck) zugeordnet sind.

Bezeichner für Anmeldeinformationen für Anmeldeinformationstyp Zertifikatverwaltung konfigurieren

Stellen Sie die eindeutige Identifizierung und eine effektive Verwaltung von Anmeldeinformationen sicher, indem Sie den Anmeldeinformationsbezeichner für Zertifikatsbestand-Managementkonfigurieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Um die Unterstützung von Anmeldeinformationen für externe Speicher für die TLS-Zertifikat-Discovery von CA-Typen wie GoDdies, DigiCert und Sectigo zu aktivieren, richten Sie den Anmeldeinformationsbezeichner innerhalb der Instanz für den entsprechenden Anmeldeinformationstyp für die Zertifikatverwaltung ein.

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**.
2. Wählen Sie **Neu**.
3. Wählen Sie einen Anmeldeinformationstyp mit der Bezeichnung **Anmeldeinformationen für Zertifikatverwaltung**aus.
4. Aktivieren Sie im Anmeldeinformationsformular das Kontrollkästchen **Externer Anmeldeinformationsspeicher**.
5. Füllen Sie die Felder **Anmeldeinformationsalias** und **Nachweis-ID** aus.
   Stellen Sie sicher, dass die Anmeldeinformations-ID und Arg_ID in der Datei „Resolver für Anmeldeinformationen“ übereinstimmen.
6. Wählen Sie **Absenden**.

Führen Sie die Zertifikat-Discovery über die Abfrage der Zertifizierungsstelle aus

Die Ausführung einer Zertifikat-Discovery über eine Zertifizierungsstellenabfrage ermöglicht die systematische Identifizierung und den Import von TLS-Zertifikaten von bestimmten Zertifizierungsstellen und gewährleistet so eine umfassende Nachverfolgung, Verwaltung und Sicherheit des Zertifikatbestands. Erkennen Sie TLS-Zertifikate von Zertifizierungsstellen (CA) mit Zertifikatsbestand-Managementund verwenden Sie Muster für verschiedene Zertifizierungsstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: pki_admin oder discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Bei der Zertifikat-Discovery verwendet das Muster der Zertifizierungsstellen (Certific Authorities, CA) bestimmte API-Elemente. Der Anwender, der den Anmeldeinformationen für die Instanz hinzugefügt wird, benötigt Berechtigungen für diese Abfragen. Weitere Informationen zum Muster von Zertifizierungsstellen (Certificate Authorities, CA) und den zugehörigen API-Elementen finden Sie unter API-Elemente und Berechtigungen für Muster von Zertifizierungsstellen.

Prozedur
1. Generieren Sie bei Bedarf einen Alias für Anmeldeinformationen.
   Weitere Informationen hierzu finden Sie unter Aliasse für Anmeldeinformationen für Discovery . Erstellen Sie für neue Anmeldeinformationen einen neuen Anmeldeinformationsalias. Falls mehrere Anmeldeinformationen denselben Alias verwenden, priorisiert Discovery die Anmeldeinformationen und initiiert den Prozess.
2. Erstellen Sie einen neuen Anmeldeinformationstyp, der für die Zertifizierungsstelle (Certificate Authority, CA) spezifisch ist.

   a. Navigieren zu **Discovery** > **Anmeldeinformationen** Wählen Sie dann **Neu**aus.

   b. Wählen Sie **Anmeldeinformationen für Zertifikatverwaltung** aus.

   c. Um die **Liste „Alias für Anmeldeinformationen“**zu entsperren, wählen Sie das Sperrsymbol. Der Alias wird den Anmeldeinformationen zugeordnet.

   d. Wählen Sie **Typ angeben**: **Anmeldeinformationen** aus.

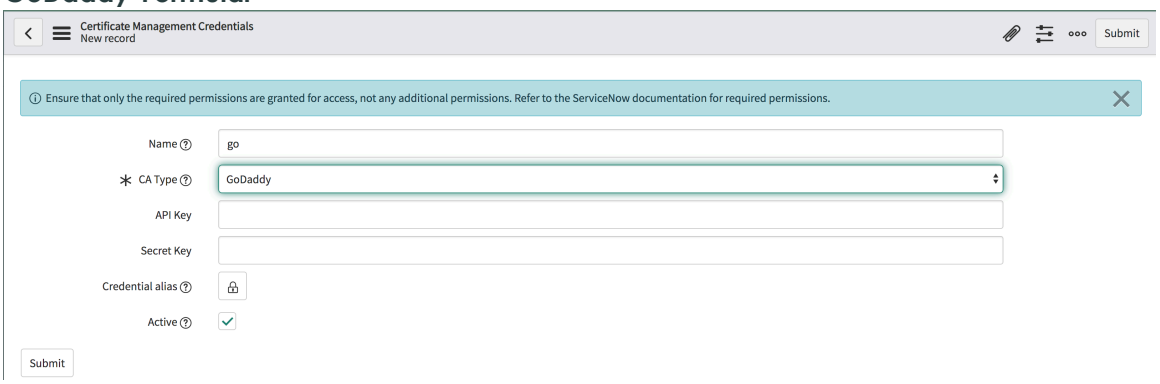
   e. Wählen Sie **CA-Typ**aus.
   Die verfügbaren CA-Typen sind: GoDdies, Digicert, Entrust oder Sectigo.

   f. Füllen Sie die Felder für den ausgewählten CA-Typ aus.

   Jede Zertifizierungsstelle (Certificate Authority, CA) erfordert bestimmte Formularfeldeinträge. Weitere Informationen finden Sie unter API-Schlüssel-Anmeldeinformationen .

   Sehen Sie sich die folgenden Beispiele für Formulare für die einzelnen Zertifizierungsstellen an.

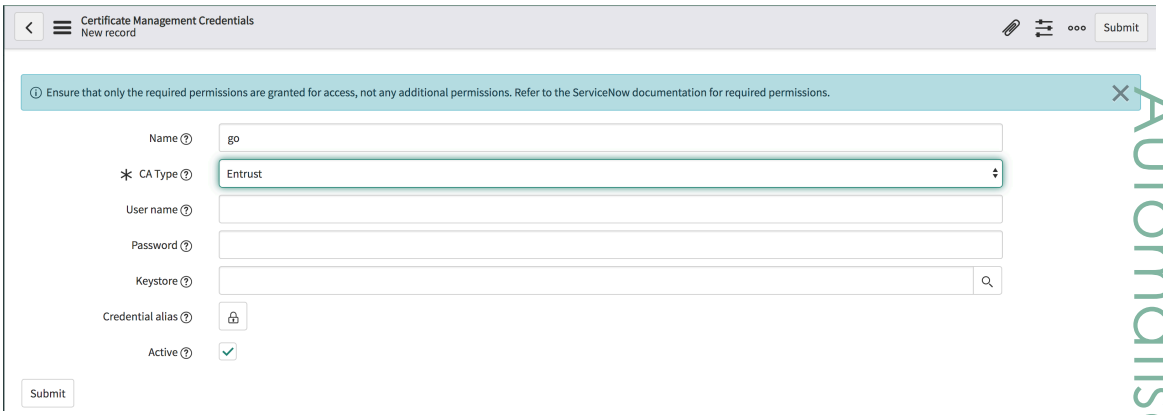
GoDaddy-Formular



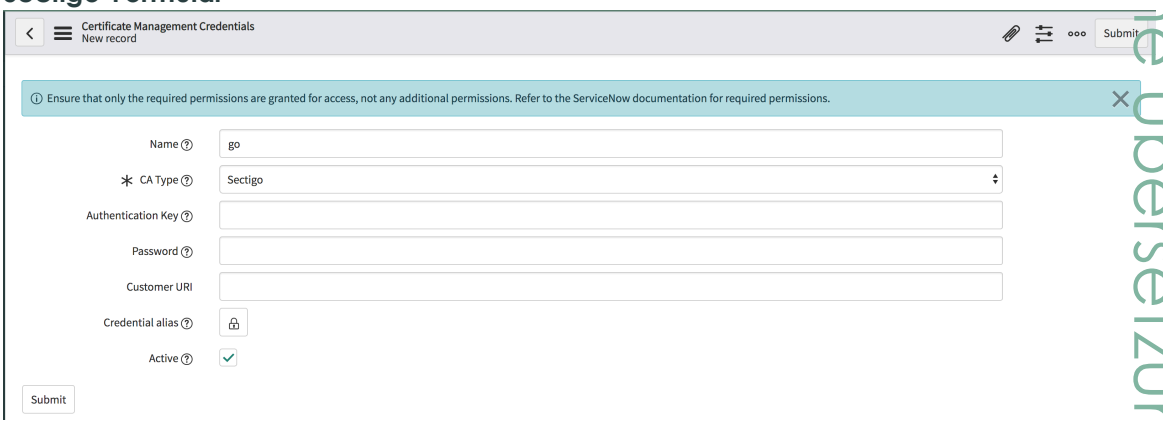
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DigiCert-Formular

Entrust-Formular



Sectigo-Formular



Automatische Übersetzung

3. Erstellen Sie einen Discovery-Zeitplan mit den folgenden Feldern.
   Weitere Informationen zum Einrichten von Discovery -Zeitplänen finden Sie unter Horizontal-Discovery planen.
   a. Wählen Sie **Discovery**: **Zertifikate**.
   b. Wählen Sie **Typ der Zertifikaterkennung**: **CA Trust Discovery (Erkennung der CA-Vertrauensstellung)** aus.
   c. Wählen Sie **Methode für MID Server-Auswahl**: **Automatische Auswahl** oder **Spezifischer MID Server** aus.
   d. Füllen Sie alle anderen erforderlichen Felder aus.
   e. Wählen Sie **Speichern**.
4. Um das benötigte CA-Muster hinzuzufügen, wählen Sie auf der Registerkarte **Muster für serverlose Ausführung** die **Option Neu**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie die Option **Zertifikatstatus einschließen** aktivieren, können Sie mehrere Zertifikatstatus angeben, indem Sie sie durch Kommas trennen.

5. Wählen Sie **Absenden**.

Ergebnisse
Wenn Ihr Discovery-Zeitplan ausgeführt wird, werden Ihre Dateien automatisch gescannt.

Zertifikatsbestand-Management anpassen

Passen Sie verschiedene Aspekte in Zertifikatsbestand-Management mithilfe von Discovery -Eigenschaften an, um die Lösung an Ihre spezifischen Anforderungen anzupassen und die Verwaltung von TLS-Zertifikaten insgesamt zu verbessern.

Vorbereitungen
Erforderliche Rolle: admin oder discovery_admin

Prozedur

Um Discovery-Eigenschaftenzu bearbeiten, navigieren Sie zu **Alle** > **Discovery-Definition** > **Eigenschaften**.

- glide.discovery.certs.cert_admin_user_id
- glide.discovery.certs.days_before_expiration_to_create_renewal_task
- glide.discovery.certs.en_incident_creation_for_expired_certipts
- glide.discovery.certs.enable_renewal_task_creation_for_discovered_certipts
- glide.discovery.certs.slack_channel_id

Manueller Flow für Zertifikatanforderungen

Zertifikatanforderungen und Incidents werden automatisch erstellt, wenn ablaufende Zertifikate und abgelaufene Zertifikate erkannt werden. Anforderungen und Incidents zur Zertifikatverlängerung werden automatisch erstellt, wenn Zertifikate bald ablaufen oder abgelaufen sind. Sie können Anforderungen auch manuell mit Servicekatalogerstellen.

Eine regelmäßige Aufgabe untersucht die Tabelle „Eindeutige Zertifikate“ [cmdb_ci_certificate] täglich und löst Aufgaben für das Verlängerungszertifikat aus, wenn ein Zertifikat abgelaufen ist oder sich dem Ablauf nähert.

Wichtige Überlegungen zur Verlängerung von Zertifikaten:

- Aufgaben für Zertifikatverlängerungen werden 60 Tage vor Ablauf automatisch generiert. Um den Zeitrahmen zu ändern, aktualisieren Sie die Eigenschaft Discovery: *glide.discovery.certs.days_before_expiration_to_create_renewal_task*.
- Zertifikataufgaben werden automatisch mit Priorität 3 – Mittel zugewiesen. Ändern Sie die Priorität, indem Sie die Aufgabe bei Bedarf öffnen.
- Wenn für das aktuelle Zertifikat bereits eine Zertifikataufgabe vorhanden ist, werden keine zusätzlichen Aufgaben erstellt.
- Bei Aufgaben und Incidents zur Zertifikatverlängerung werden verschiedene Felder basierend auf dem Zertifikat-CI automatisch vorab ausgefüllt.
- Wenn ein Zertifikat abläuft und nicht ersetzt wird, wird ein neuer Incident erstellt. Für jedes abgelaufene Zertifikat wird jedoch nur ein Incident generiert.
- Um die Liste der Zertifikat-Incidents anzuzeigen, navigieren Sie zu **Service Desk** > **Incidents**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Zertifikatanforderungen erstellen

Erstellen Sie neue Zertifikatanforderungen manuell über Servicekatalog, um eine personalisierte und effiziente Beschaffung von Zertifikaten zu ermöglichen und mehr Flexibilität und Kontrolle zu bieten.

Vorbereitungen

Stellen Sie sicher, dass der Zertifikatverwaltungskatalog aktiviert ist.

Erforderliche Rolle: pki_admin

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Zertifikatverwaltung**.
2. Wählen Sie **Neues Zertifikat anfordern aus**.
3. Geben Sie die erforderlichen Informationen für die folgenden Pflichtfelder an.
   - **Zertifikatsignaturanforderung**
   - **Zertifizierungsstelle**
   - **Zertifikattyp**
   - **Gültigkeitszeitraum**
   - **Genehmiger**
4. Geben Sie nach Bedarf zusätzliche Details in das Formular ein, oder wählen Sie zusätzliche Details aus.
5. Wählen Sie **Absenden**.

Ergebnisse

Die Zertifikataufgabe wird generiert und zur Genehmigung übermittelt. Das Feld „Genehmigung“ ist für pki_user schreibgeschützt und kann für pki_admin bearbeitet werden.

Anforderung zur Verlängerung von Zertifikaten erstellen

Initiieren Sie Verlängerungsanforderungen für Zertifikate manuell mit Servicekatalog, um zusätzliche Flexibilität und Kontrolle zu bieten.

Vorbereitungen

Stellen Sie sicher, dass der Zertifikatverwaltungskatalog aktiviert ist.

Erforderliche Rolle: pki_admin

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Zertifikatverwaltung**.
2. Wählen Sie **Zertifikat verlängern aus**.
3. Wählen Sie ein Zertifikat-CI aus.
4. Geben Sie die erforderlichen Informationen für die folgenden Pflichtfelder an.
   - **Zertifikatsignaturanforderung**
   - **Angefordert für**
   - **Genehmiger**
5. Geben Sie nach Bedarf zusätzliche Details in das Formular ein, oder wählen Sie zusätzliche Details aus.
6. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Die Zertifikataufgabe wird generiert und zur Genehmigung übermittelt. Das Feld „Genehmigung“ ist für pki_user schreibgeschützt und kann für pki_admin bearbeitet werden.

Hinweis: Der Benachrichtigungsprozess für die Zertifikatverlängerung unterstützt ausschließlich den manuellen Flow und beinhaltet keine automatisierte Zertifikatverwaltung. Für CSR-Informationen müssen Sie die automatisierte Zertifikatverwaltung verwenden.

Wenn bei der Überwachung des Status eines Zertifikatauftrags ein Konfigurationsproblem auftritt, kann die Aufgabe im Status „In Arbeit“ hängen bleiben. Für die Lösung solcher Probleme ist der PKI-Administrator verantwortlich. Wenn beispielsweise MID-Server während der geplanten Aufgabe zur Nachverfolgung des Status der Zertifikatbestellung ausfällt, wartet das System auf die nächste geplante Aufgabe, anstatt einen Fehler zu protokollieren. Wenn MID-Server vor dem nachfolgenden Auftrag wieder aufgerufen wird, wird der Zertifikatabruf entsprechend fortgesetzt.

Zertifikataufgaben archivieren

In Version 1.1.7 Zertifikatsbestand-Managementführt das Plugin „Data Archiver“ [com.glide.uxdb] tägliche Vorgänge aus, um Daten, die nicht mehr benötigt werden, aus primären Tabellen in einen festgelegten Satz von Archivtabellen zu übertragen.

Vorbereitungen
Erforderliche Rolle: pki_user oder pki_admin

Warum und wann dieser Vorgang ausgeführt wird
Zertifikatsbestand-Management prüft und archiviert aktiv Zertifikataufgaben, die älter als ein Jahr sind. Dazu muss das entsprechende Plugin aktiviert sein, damit die geplanten Archivierungsaufgaben ausgeführt werden können. Es ist wichtig zu beachten, dass die Archivierungsregel für Zertifikataufgaben, die in der Anwendung Zertifikatsbestand-Management enthalten ist, standardmäßig deaktiviert ist.

Prozedur

1. Aktivieren Sie **die Regel für Zertifikataufgaben**.
2. Navigieren zu **Archivregeln** > **Zertifikataufgabenarchiv**.
3. Aktivieren Sie die Checkbox **Aktiv**.

Ergebnisse
Bei der Aktivierung archiviert diese Regel Daten aus der Tabelle „Zertifikataufgabe“ [sn_disco_certmgmt_certificate_task] unter den folgenden Bedingungen:

- Status „Geschlossen - vollständig“
- Die letzte Aktualisierung erfolgte vor mehr als zwölf Monaten

Automatisierte Zertifikatverwaltung für TLS-Zertifikate

In Zertifikatsbestand-Management Version 1.3.8 wird eine neue Funktion eingeführt, die die Automatisierung des Anforderungs-Flows für neue, verlängerte oder widerrufende Zertifikate ermöglicht.

Zertifikatsbestand-Management bietet die Möglichkeit, Zertifikate automatisch von Zertifizierungsstellen abzurufen, ohne dass ein manuelles Eingreifen des PKI-Teams erforderlich ist. In Version 2.1.0 unterstützt diese Funktion DigiCert und Entrust CA Gateway für nahtlose automatische Erfüllungs-Flows mit der Einschränkung, dass nur OV DigiCert-Zertifikate angefordert werden können. Darüber hinaus führt Version 2.3.2 Unterstützung für Microsoft

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CA ein. Weitere Informationen finden Sie in der jeweiligen Anbieterdokumentation. Für automatisierte Flows mit DigiCert oder Entrust CA Gateway in Certificate Inventory and Management benötigen Sie Berechtigungen zum Anfordern, Verlängern und Widerrufen von Zertifikaten.

Der CA-Benutzer MicrosoftMicrosoft Azure Event Hubs benötigt die folgenden Berechtigungen:

Microsoft Gateway-Benutzerberechtigungen

Berechtigung	Aktion
CredSSP auf CA, Zwischenserver und MID-Server	Richten Sie CredSSP für CA, den Zwischenserver und MID-Serverein. Schritte zur Konfiguration von CredSSP finden Sie in der Now Support Knowledge Base, die im KB-Artikel KB1632624 dokumentiert ist.
Mitgliedschaft in Unternehmensadministratoren	Stellen Sie sicher, dass der Benutzer Mitglied in der Gruppe „Enterprise-Administratoren“ ist.
Sicherheitsgruppeneinschluss für Vorlage	Stellen Sie sicher, dass der Benutzer in der Sicherheitsgruppe der Vorlage enthalten ist.
Bestimmte Berechtigungen in CA	Erteilen Sie folgenden Benutzerberechtigungen: Lesen, Zertifikate ausstellen und verwalten, CA verwalten und Zertifikate in der CA anfordern.

Automatisierte Flows für die Zertifikatverwaltung verwenden

Die automatisierte Zertifikatverwaltung in Zertifikatbestand und -management optimiert TLS-Zertifikatprozesse und bietet Vorteile wie höhere Effizienz, weniger manuelle Eingriffe und höhere Sicherheit. Die Automatisierung der Zertifikatverwaltung stellt eine rechtzeitige Verlängerung sicher, minimiert das Risiko abgelaufener Zertifikate und bietet einen systematischen Ansatz für die Verwaltung des Lebenszyklus von TLS-Zertifikaten.

Vorbereitungen

Erforderliche Rolle: pki_admin oder admin

Um den automatisierten Flow der Zertifizierungsstelle MicrosoftMicrosoft Azure Event Hubs zu verwenden, müssen Sie das Plugin **„ServiceNow IntegrationHub Action Step – PowerShell“** installieren und über ein Integration Hub-Abonnement verfügen. Weitere Informationen finden Sie unter IntegrationHub Nutzung und Abonnement .

Prozedur

1. Legen Sie die Systemeigenschaft *sn_disco_certmgmt.cert_task_default_approval_group* auf den Standardnamen der Genehmigungsgruppe fest.
   Der Name der Genehmigungsgruppe ist die Standardgruppe, die verwendet wird, wenn die Zertifikatanforderung in den manuellen Modus wechselt, z. B. wenn keine übereinstimmende Richtlinie oder mehr als zwei übereinstimmende Richtlinien vorhanden sind. Sie können mehrere durch Kommata getrennte Genehmigungsgruppen hinzufügen. Die erste Gruppe in der Liste, die zur Aufgabendomäne gehört, wird für die Genehmigung verwendet. Wenn keine domänenspezifische Gruppe gefunden wird, wird der erste Name in der globalen Domänenliste verwendet.
2. Um den Gültigkeitszeitraum des Zertifikatauftrags festzulegen, aktualisieren Sie die Systemeigenschaft *sn_disco_certmgmt.default_cert_order_validity_period*.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Standardwert lautet 730 Tage (2 Jahre).

3. Richten Sie die Weiterleitungsrichtlinie für jede Zertifizierungsstelle ein (z. B. DigiCert, Entrust CA Gateway oder MicrosoftMicrosoft Azure Event Hubs CA).
   Sie können mehrere Routing-Richtlinien für eine einzelne CA definieren, um verschiedene Konten zum Abrufen von Zertifikaten zu verwenden. Für MicrosoftMicrosoft Azure Event Hubs CA können Sie dann entweder:
   - Fügen Sie die IP des CA-Servers im Feld „ca_host_ip“ der Weiterleitungsrichtlinie hinzu, ODER
   - Fügen Sie die IP eines Zwischenservers im Feld „ca_host_ip“ der Weiterleitungsrichtlinie hinzu. Der Zwischenserver kann ein beliebiger Windows -Server sein, der sich in derselben Domäne wie der CA-Server MicrosoftMicrosoft Azure Event Hubs befindet und Zugriff auf die in PowerShell verfügbaren Befehle vom Typ „certutil“ und „certreq“ hat.

     Wenn ein Zwischenserver verwendet wird, führt der MID-Server ein PowerShell-Skript auf dem Zwischenserver mit Invoke-Command aus, das wiederum Remote Procedure Call (RPC) verwendet, um die Befehle certutil und certreq auf dem CA Server auszuführen.

4. Erstellen Sie die Zertifikatanmeldeinformationen, und ordnen Sie diese dem Anmeldeinformationsalias zu.
   Alle Anmeldeinformationen sollten einem eindeutigen Anmeldeinformationsalias zugeordnet werden. Weitere Informationen finden Sie unter Anmeldeinformationsalias für Discovery .
5. Stellen Sie sicher, dass sich die Informationen zum Zertifikat und zur Zertifikat-URL in den Tabellen „Zertifizierungsstelle“ [sn_disco_certmgmt_ca] und „Zertifizierungsstellen-API-URL“ [sn_disco_certmgmt_ca_api_url] befinden.
   Die Standard-URL für DigiCert enthält alle Validierungstyp-URLs. Sie können bei Bedarf zusätzliche URLs hinzufügen.
6. Stellen Sie sicher, dass sich die Informationen zum Zertifikat und zur Zertifikat-URL in den Tabellen „Zertifizierungsstelle“ [sn_disco_certmgmt_ca] und „Zertifizierungsstellen-API-URL“ [sn_disco_certmgmt_ca_api_url] befinden.
   Die Standard-URL für DigiCert und Entrust CA Gateway enthält alle Validierungstyp-URLs. Sie können bei Bedarf zusätzliche URLs hinzufügen.
7. Stellen Sie sicher, dass sich die Informationen zum Zertifikat und zur Zertifikat-URL in den Tabellen „Zertifizierungsstelle“ [sn_disco_certmgmt_ca] und „Zertifizierungsstellen-API-URL“ [sn_disco_certmgmt_ca_api_url] befinden.
   Die Standard-URL für DigiCert und Entrust CA Gateway enthält alle Validierungstyp-URLs. Sie können bei Bedarf zusätzliche URLs hinzufügen.
8. Legen Sie die Aufgabenpriorität fest.

   Basierend auf der Aufgabenpriorität werden die Priorität und der Typ der Change-Anforderungen zugeordnet. Die Change-Anforderung hat die gleiche Priorität wie die Aufgabenpriorität mit Ausnahme von P5 (die Change-Anforderung hat kein P5, daher wird sie in diesem Fall P4 zugeordnet).

   Um den Typ der Change-Anforderungen zu ändern, muss die Change-Management-Eigenschaft *com.snc.change_management.change_model.type_compatibility* auf „true“ festgelegt werden. Der Standardwert ist „Falsch“.

   a. Legen Sie die Aufgabe fest, und ändern Sie bei Bedarf die Systemeigenschaft *sn_disco_certmgmt.default_cert_task_priority*, um die Prioritäten für Neu- und Verlängerungsaufgaben zu konfigurieren.
      Die Priorität ist standardmäßig P3. Die möglichen Werte sind 1, 2, 3, 4, 5. Wenn der Wert 1 ist, wird die Priorität auf P1 festgelegt usw. Wenn ein ungültiger Wert angegeben ist, wird die Priorität auf den Standardwert P3 zurückgesetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Legen Sie die Aufgabe fest, und ändern Sie bei Bedarf die Systemeigenschaft *sn_disco_certmgmt.default_revoke_cert_task_priority*, um Prioritäten für Aufgaben beim Widerrufen zu konfigurieren.
Die Priorität ist standardmäßig P1. Die möglichen Werte sind 1, 2, 3, 4, 5. Wenn der Wert 1 ist, wird die Priorität auf P1 festgelegt usw. Wenn ein ungültiger Wert angegeben ist, wird die Priorität auf den Standardwert P1 zurückgesetzt.

9. Wahlweise: Installieren Sie das Plugin „Integrations-Hub“ [com.glide.hub.integrations].

(Optional) Das Plugin [com.glide.hub.integrations] ist nicht erforderlich, um das DigiCert-Zertifikat anzufordern und den Status der Zertifikatbestellung zu verfolgen. Wenn der Kunde jedoch die Zertifikat-Subflow-Aktionen debuggen oder seinen eigenen Anpassungsflow für DigiCert hinzufügen möchte, muss er dieses Plugin installieren.

Das Plugin [com.glide.hub.integrations] ist nicht erforderlich, um das DigiCert- oder das Entrust CA Gateway-Zertifikat anzufordern und den Status der Zertifikatbestellung zu verfolgen. Wenn der Kunde jedoch die Zertifikat-Subflow-Aktionen debuggen oder seinen eigenen Anpassungs-Flow für DigiCert oder Entrust CA Gateway hinzufügen möchte, muss er dieses Plugin installieren.

Das Plugin [com.glide.hub.integrations] ist nicht erforderlich, um das DigiCert- oder das Entrust CA Gateway-Zertifikat anzufordern und den Status der Zertifikatbestellung zu verfolgen. Wenn der Kunde jedoch die Subflow-Aktionen des Zertifikats debuggen oder einen eigenen Anpassungs-Flow für DigiCert, Entrust CA Gateway oder MicrosoftMicrosoft Azure Event Hubs CA hinzufügen möchte, muss er dieses Plugin installieren.

Routing-Richtlinien für die automatisierte Zertifikatverwaltung einrichten

Richten Sie eine Weiterleitungsrichtlinie ein, um eine automatisierte Zertifikatverwaltung in Certificate Inventory and Management einzurichten. Dies beinhaltet das Erstellen einer Richtlinie basierend auf Faktoren wie Zertifizierungsstelle (Certificate Authority, CA), Umgebung und anderen Funktionen, um eine effiziente TLS-Zertifikatverwaltung sicherzustellen.

Vorbereitungen
Erforderliche Rolle: pki_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird
Doppelte Zertifikatanforderungen sind nicht zulässig. Sie können diese Einstellung jedoch überschreiben, indem Sie das Kontrollkästchen „Allow duplicate requests“ (Duplizierte Anforderungen zulassen) aktivieren. Eine Zertifikatanforderung gilt als Duplikat, wenn eine weitere Zertifikataufgabe mit demselben Domänennamen vorhanden ist, die noch ausgeführt wird. Genehmigungen werden derzeit nur in der Genehmigungs-Experience des Erfüllers unterstützt.

Die Routing-Richtlinie entscheidet, welche Zertifizierungsstelle für Zertifikatvorgänge kontaktiert werden muss. Sie enthält die Attribute für die Zertifizierungsstelle, deren URL, Anmeldeinformationen, Genehmigungsgruppe, Zuweisungsgruppe und CSR. Die Routing-Richtlinie löst den Flow zum Anfordern von Zertifikaten für bestimmte Zertifizierungsstellen aus.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatverwaltung** > **Richtlinien für Zertifikatweiterleitung**.

2. Wählen Sie **Neu**, und füllen Sie die erforderlichen Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während Anforderungen für neue Zertifikate und die Erneuerung von Zertifikaten automatisiert werden können, bevorzugen viele PKI-Teams eine persönliche Validierung vor der Erfüllung. Wenn ja, aktivieren Sie das Kontrollkästchen **Genehmigung erforderlich**.

Hinweis:

Organisation, Organisationseinheit, Ort, Bundesland, Land und E-Mail akzeptieren kommagetrennte Werte. * wird als beliebig betrachtet. Der allgemeine Antragstellername und der alternative Antragstellername werden mit einem regulären Ausdruck unterstützt. Für das RegEx-Format gelten die folgenden Einschränkungen:

- Sie darf keine Kommas enthalten.
- Es darf nicht mit einem Schrägstrich (/) beginnen und enden. * entspricht jeder Domäne

3. Die folgenden CSR-Attribute stimmen mit den Einträgen in der Tabelle „Routing-Richtlinie“ [sn_disco_certmgmt_routing_policy] überein:
   - Organisation
   - Organisationseinheit
   - Ort
   - Status
   - Land
   - E-Mail
   - Umgebung
   - Zertifikatzweck (intern/extern)
   - Allgemeiner Antragstellername
   - Alternativer Antragstellername

   Hinweis: Für Entrust CA Gateway gibt es auch diese Felder: „Bezeichner der Zertifizierungsstelle“, „Zertifikatprofil“ und „Zertifikatformat“. Verwenden Sie für MicrosoftMicrosoft Azure Event Hubs CA auch diese Felder: Zertifizierungsstelle, CA-Vorlagenname, CA-Host-IP, Anmeldeinformationen und CSR-Attribute.

4. Die folgenden Optionen können auftreten.

Option	Bezeichnung
Wenn eine einzelne Routing-Richtlinie übereinstimmt	Überprüfen Sie die folgenden Bedingungen: ◦ Validieren Sie den allgemeinen Antragstellernamen mit dem Muster des regulären Ausdrucks, das in der Tabelle „Routing-Richtlinie“, dem Domänennamen oder * angegeben ist. ◦ Überprüfen Sie, ob der Gültigkeitszeitraum der Zertifikatanforderung den maximalen Gültigkeitszeitraum in der Tabelle „Routing-Richtlinie“ nicht überschreitet. ◦ Prüfen Sie auf die Kennzeichnung für zulässige duplizierte Zertifikatanforderungen in der Tabelle „Routing-Richtlinie“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Wenn mehrere Routing-Richtlinien in Frage kommen	Die Aufgabe wird der Standardgenehmigergruppe zugewiesen.
Wenn keine Routing-Richtlinie gefunden wurde	Die Aufgabe wird der Standardgenehmigergruppe zugewiesen.
Wenn eine einzelne Richtlinie übereinstimmt und die Kennzeichnung „Genehmigung erforderlich“ auf „true“ gesetzt ist	Die Aufgabe wird der Aufgabengenehmigungsgruppe zugewiesen, die in der Routing-Richtlinie definiert ist.

Ergebnisse
Die Genehmigungsgruppe ist der Routing-Richtlinie zugewiesen und enthält die Rolle pki_approver und mindestens eines der aktiven Gruppenmitglieder, die in dieser Gruppe verfügbar sind. Wenn die Routing-Richtlinie eine manuelle Genehmigung erfordert, wird die Genehmigung von den Personen in der Genehmigungsgruppe angefordert.

Routing-Richtliniendetails

Weiterleitungsrichtlinien sind für die automatisierte Zertifikatverwaltung in TLS-Zertifikaten von entscheidender Bedeutung, da sie bestimmte Kriterien wie Zertifizierungsstelle und Umgebung definieren und eine effiziente Behandlung verschiedener Szenarien während des Zertifikatlebenszyklus ermöglichen.

Es gibt drei verschiedene Szenarien zur Funktionsweise von Routing-Richtlinien für die automatisierten Zertifikatverwaltung für TLS-Zertifikate.

- Szenario 1: Eine einzelne Routing-Richtlinie stimmt überein, und eine manuelle Genehmigung ist erforderlich. Der Genehmiger kann die Aufgabendetails überprüfen und die Zertifikatanforderung genehmigen. Nach der Genehmigung wird der automatisierte Flow ausgelöst.
- Szenario 2: Keine Routing-Richtlinie stimmt überein ODER es sind mehrere Routing-Richtlinien vorhanden, die übereinstimmen. Der Genehmiger kann die Aufgabendetails überprüfen und „Weiterleitungsrichtlinie wählen und genehmigen“ auswählen. Der Genehmiger muss die Weiterleitungsrichtlinie manuell auswählen. Die aktualisierte Routing-Richtlinie wird dann angezeigt. Der Genehmiger wählt die Routing-Richtlinie aus, die dann den automatisierten Flow auslöst.
- Szenario 3: Eine einzelne Routing-Richtlinie stimmt überein, eine manuelle Genehmigung ist nicht erforderlich, und die Kennzeichnung „Genehmigung erforderlich“ ist inaktiv. Dadurch wird der automatische Flow ausgelöst.

Hinweis:

Wenn der Genehmiger die Zertifikatanforderungsaufgabe abgelehnt hat, wird die Aufgabe als „Fehlgeschlagen“ markiert. Eine einzige Genehmigung reicht aus, um den Fortschritt des automatisierten Flows auszulösen.

Neue Zertifikate mit der automatisierten Zertifikatverwaltung anfordern

Fordern Sie ein neues Zertifikat an, und rufen Sie die Zertifikate für eine Anwendung mithilfe der automatisierten Zertifikatverwaltung automatisch ab. Zertifikatsbestand-Management Version 2.1.0 bietet Unterstützung für die Anforderung von Zertifikaten von DigiCert und Entrust CA Gateway. Version 2.3.2 unterstützt auch MicrosoftMicrosoft Azure Event Hubs CA.

Vorbereitungen
Stellen Sie sicher, dass der Zertifikatverwaltungskatalog aktiviert ist und eine Weiterleitungsrichtlinie erstellt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nur für DigiCert: Sie benötigen den API-Schlüssel von DigiCert, wobei die Domäne bereits von DigiCert validiert wurde. Wenn Sie eine Zertifikatanforderung mit einer neuen Domäne übermitteln, die nicht von DigiCert validiert wurde, wird die Anforderung als Ausstehend angezeigt, der automatisierte Flow kann die Zertifikatinformationen nicht abrufen, und die Anforderung wird als Fehlgeschlagen markiert.

Erforderliche Rolle: Zertifikatanforderer, PKI-Administrator, PKI-Anwender oder Administrator

Zertifikatanforderer sind Benutzer, die nicht über die Rolle „PKI-Administrator“ oder „PKI-Benutzer“ verfügen.

Hinweis: Genehmigungen werden derzeit nur in der Genehmigungs-Experience des Erfüllers unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Zertifikatverwaltung**.
2. Wählen Sie **Neues Zertifikat anfordern – Automatisierter Flow aus**.
3. Geben Sie Details für die folgenden Pflichtfelder an: **CSR** und **Gültigkeitszeitraum**.
4. Füllen Sie das Formular aus, oder wählen Sie zusätzliche Informationen aus, und klicken Sie dann auf **Absenden**, um mit der Bestellung fortzufahren.

   Die Tabelle „Routing-Richtlinie“ [sn_disco_certmgmt_routing_policy] hilft beim Abrufen der Routing-Richtlinien-ID für die Zertifizierungsstelle. Wenn keine einzelne Routing-Richtlinien-ID zurückgegeben wird, muss der Genehmiger die Routing-Richtlinie auswählen und die Aufgabe genehmigen. Weitere Informationen finden Sie unter Zertifikataufgaben genehmigen.

   Dadurch wird eine neue Zertifikataufgabe erstellt, die dann den automatisierten Flow auslöst. Wenn in der Routing-Richtlinie das Feld „Genehmigung erforderlich“ aktiviert wurde, muss die Aufgabe genehmigt werden, bevor der automatisierte Flow beginnt.

Ergebnisse

- Sobald die Anforderung übermittelt wurde, sendet der automatisierte Flow die Anforderung an die Zertifizierungsstelle, um das Zertifikat zu erhalten.

  Hinweis: PowerShell-Schritt wird für MicrosoftMicrosoft Azure Event Hubs CA verwendet. Dies erfordert das Plugin: com.glide.hub.action_step.powershell.

- Ein Datensatz wird in der Tabelle „Zertifikaterweiterung“ [sn_disco_certmgmt_certificate_extension] erstellt, sobald das Zertifikat erfolgreich abgerufen wurde.
- Alle 30 Minuten wird die regelmäßige Aufgabe „DigiCert − Status der Zertifikatbestellung verfolgen“ ausgeführt, und der Status wird überprüft.

  Hinweis: Es gibt keine geplanten Aufgaben für Entrust CA Gateway und MicrosoftMicrosoft Azure Event Hubs CA.

- Wenn das Zertifikat verfügbar ist, wird es an die Zertifikataufgabe angehängt.
- Die Zertifikataufgabe wird dann als „Abgeschlossen“ markiert und eine Change-Anforderung wird erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn mehrere Aufgaben für dieselbe CSR erstellt werden und „Allow Duplication“ (Duplizierung zulassen) in der Routing-Richtlinie nicht aktiviert ist, schlägt die Aufgabe fehl.
- Wenn der Gültigkeitszeitraum den Gültigkeitszeitraum der übereinstimmenden Routing-Richtlinie überschreitet, schlägt die Aufgabe fehl.

Generiert automatisch eine Zertifikatsignaturanforderung

Sie können eine Zertifikatsignaturanforderung (Certificate Signing Request, CSR) für die Instanz generieren, indem Sie die erforderlichen Informationen im Katalogformular angeben.

Das manuelle Erstellen einer CSR kann ein umständlicher und fehleranfälliger Prozess sein. Die automatische CSR-Generierung kann in den Formularen **„Neues Zertifikat anfordern“** und **„Neues Zertifikat anfordern (automatisiert)“** aktiviert werden. Diese Funktion ist standardmäßig aus Sicherheitsgründen deaktiviert.

Um die automatische CSR-Generierung zu aktivieren, legen Sie die Systemeigenschaft **sn_disco_certmgmt.enable_csr_generation** auf „wahr“ fest. Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Sobald die Option **Möchten Sie CSR generieren?** Im Zertifikatanforderungsformular wird das Kontrollkästchen „“ angezeigt. Durch Aktivieren des Kontrollkästchens werden die erforderlichen Eingabefelder zum Generieren der CSR aktiviert. Geben Sie die erforderlichen Informationen ein, und wählen Sie **Generieren**aus. Die Eingabedaten werden validiert, und die CSR wird entsprechend formatiert.

Die Zertifikatsignaturanforderung wird im Feld **Zertifikatsignaturanforderung (Certificate Signing Request, CSR)** generiert, und ein privater Schlüssel wird im Feld **Privater Schlüssel** generiert. Wählen Sie den **Download-** Link aus, um den privaten Schlüssel zur späteren Verwendung zu speichern. Standardmäßig beträgt die Größe des privaten Schlüssels 2048, kann jedoch mit der Systemeigenschaft **sn_disco_certmgmt.private_key_size**geändert werden. Weitere Informationen finden Sie unter Discovery-Eigenschaften.

Wenn Sie **Absenden**auswählen, fordert das Formular Sie mit einer Warnung zum Herunterladen und Speichern des privaten Schlüssels auf. Aus Sicherheitsgründen speichert ServiceNow keine privaten Schlüssel. Daher muss der private Schlüssel gespeichert werden, bevor Sie das Formular verlassen, da er sonst verloren geht.

Zertifizierungsaufgaben genehmigen

Manchmal müssen Sie eine Zertifikataufgabe manuell genehmigen, um die Gültigkeit und Sicherheit von TLS-Zertifikaten sicherzustellen.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Genehmigung für eine Routing-Richtlinie angefordert wird, wählen Sie die erstellte Routing-Richtlinie aus. Genehmigungen werden derzeit nur in der Genehmigungs-Experience des Erfüllers unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Selfservice** > **Meine Genehmigung**.
2. Öffnen Sie die automatisch erstellte Genehmigungsaufgabe.
3. Überprüfen Sie die neuen Zertifikatdetails, und wählen Sie **Weiterleitungsrichtlinie wählen und genehmigen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

1. Der automatisierte Flow zum Anfordern eines neuen Zertifikats wird initiiert.
2. Sie können die Zertifikataufgabe öffnen, indem Sie zu navigieren **Zertifikatverwaltung** > **Aufgabe „Neues Zertifikat“**.
3. Stellen Sie sicher, dass der automatisierte Flow ausgelöst wird.
4. Wenn die Zertifizierungsstelle die Zertifikatanforderung genehmigt, werden sowohl die Auftrags-ID als auch die Zertifikat-ID für das neu angeforderte Zertifikat abgerufen. Wenn die Zertifizierungsstelle nicht genehmigt, wird nur die Auftrags-ID abgerufen.

Hinweis: Für Entrust CA Gateway werden die Zertifikatseriennummer und die Registrierungs-ID abgerufen.

Zertifikate mithilfe der automatisierten Zertifikatverwaltung erneuern

Fordern Sie die Verlängerung eines Zertifikats an, und rufen Sie das Zertifikat für eine Anwendung automatisch ab, um sichere und unterbrechungsfreie Services durch Verlängerung des Gültigkeitszeitraums des Zertifikats zu gewährleisten und potenzielle Serviceunterbrechungen aufgrund abgelaufener Zertifikate zu verhindern.

Vorbereitungen

Stellen Sie sicher, dass der Zertifikatverwaltungskatalog aktiviert ist und eine Weiterleitungsrichtlinie erstellt wurde.

Erforderliche Rolle: PKI-Administrator, Administrator, Zertifikatbesitzer oder Benutzer, die Teil der Zertifikatbesitzer-Gruppe sind.

Zertifikatbesitzer und Zertifikatbesitzer-Gruppe enthalten die Rolle „Zertifikatanforderer“ (minimale Rolle).

Hinweis: Genehmigungen werden derzeit nur in der Genehmigungs-Experience des Erfüllers unterstützt.

Warum und wann dieser Vorgang ausgeführt wird

Entrust CA Gateway-Zertifikate können derzeit nicht verlängert werden. Um ein vorhandenes Zertifikat zu verlängern, fordern Sie ein neues Zertifikat mit denselben Details wie das ursprüngliche Zertifikat an. Derzeit ist keine Renew-API für Entrust CA Gateway- und MicrosoftMicrosoft Azure Event Hubs CA-Zertifikate verfügbar. Während einer Verlängerungsanforderung wird intern ein neues Zertifikat mit denselben Attributen wie das ausgewählte Zertifikat generiert.

Für die Verlängerung eines vorhandenen Zertifikats ist eine CSR obligatorisch. Die anfordernde Person kann eine vorhandene CSR (falls verfügbar) oder eine neue CSR verwenden. Wenn Sie eine vorhandene CSR verwenden möchten, verwenden Sie dieselbe CSR, um ein neues Zertifikat von der CA anzufordern. Wenn Felder mit Vault- und Java-APIs eingegeben werden, wird die CSR generiert.

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Zertifikatverwaltung**.
2. Klicken Sie auf **Zertifikat verlängern – Automatisierter Flow**.
3. Geben Sie Details für die folgenden Pflichtfelder an: **CSR** und **Gültigkeitszeitraum**.
4. Füllen Sie das Formular aus, oder wählen Sie zusätzliche Informationen aus, und klicken Sie dann auf **Absenden**, um mit der Bestellung fortzufahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

1. Die Tabelle „Routing-Richtlinie“ [sn_disco_certmgmt_routing_policy] hilft beim Abrufen der Routing-Richtlinien-ID für die Zertifizierungsstelle.
   - Wenn keine Übereinstimmung mit einer einzelnen Routing-Richtlinie erzielt wird, muss der Genehmiger die Zertifizierungsstelle auswählen und den Flow auslösen.
   - Wenn die CSR einen anderen Domänennamen als den ausgegebenen Zertifikatdomänennamen enthält, fordert die Aufgabe die Genehmigung an.
   - Wenn eine einzelne Routing-Richtlinie übereinstimmt, aber in der Tabelle „Zertifikaterweiterung“ [sn_disco_certmgmt_certificate_extension] keine Verlängerungszertifikatinformationen verfügbar sind, muss die Aufgabe genehmigt werden.
   - Zertifikate können nicht erneuert werden, wenn Zertifizierungsstelle und Bestell-ID oder Fingerabdruckdetails für das Zertifikat in der Tabelle „Zertifikaterweiterung“ [sn_disco_certmgmt_certificate_extension] fehlen. Erkennen Sie das Zertifikat über die Abfrage der Zertifizierungsstelle, um die erforderlichen Details in die Zertifikaterweiterungstabelle aufzunehmen. Wählen Sie nach Discovery die Routing-Richtlinie aus, und genehmigen Sie die Aufgabe.
2. Dadurch wird eine Aufgabe für das bestellte Zertifikat erstellt, die den Flow zur Anforderung des Verlängerungszertifikats auslöst.
3. Sobald die Anforderung übermittelt wurde, sendet der automatisierte Flow die Anforderung an die Zertifizierungsstelle, um das Zertifikat zu erhalten.

   Hinweis: PowerShell-Schritt wird für MicrosoftMicrosoft Azure Event Hubs CA verwendet. Dies erfordert das Plugin: com.glide.hub.action_step.powershell.

4. Die Auftrags-ID wird dann in den Tabellen „Zertifikataufgabe“ [sn_disco_certmgmt_certificate_task] und „Zertifikaterweiterung“ [sn_disco_certmgmt_certificate_extension] gespeichert.

   Hinweis: Für Entrust CA Gateway werden die Zertifikatseriennummer und die Registrierungs-ID abgerufen. Die Seriennummer wird in der Tabelle „Zertifikatverlängerung“ [sn_disco_certmgmt_certificate_extension] gespeichert.

5. Alle 30 Minuten wird die geplante Aufgabe „DigiCert − Status der Zertifikatbestellung verfolgen“ ausgeführt und der Status wird überprüft.

Hinweis:

Das System ruft Details zum ausgewählten Zertifikat aus der Tabelle „Zertifikaterweiterung“ [sn_disco_certmgmt_certificate_extension] ab und fordert die Zertifizierungsstelle auf, das Zertifikat zu verlängern. Zertifikate können nicht erneuert werden, wenn Zertifizierungsstelle, Bestell-ID oder Fingerabdruck in dieser Tabelle fehlen. Wenn die zusätzlichen Details für die Verlängerung des Zertifikats aus irgendeinem Grund fehlen, protokolliert das System eine Meldung und schlägt vor, was zu tun ist. In diesem Fall müssen Sie die Erkennung für das Zertifikat mithilfe der CA-basierten Erkennung durchführen. Weitere Informationen finden Sie unter Führen Sie eine Zertifikat-Discovery über eine Zertifizierungsstellenabfrage aus, um diese Details in die Zertifikaterweiterungstabelle aufzunehmen.

Zertifikate mithilfe der automatisierten Zertifikatverwaltung widerrufen

Fordern Sie einen Widerruf des Zertifikat für eine Anwendung an. Der Widerruf erfordert keine Genehmigung, wenn die Bestell-ID und die Zertifikat-ID in der Zertifikaterweiterungstabelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vorhanden sind. Wenn Bestell-ID und Zertifizierungs-ID nicht in der Zertifikaterweiterungstabelle vorhanden sind, fordert die Aufgabe die Genehmigung an.

Vorbereitungen

Stellen Sie sicher, dass der Zertifikatverwaltungskatalog aktiviert ist und eine Weiterleitungsrichtlinie erstellt wurde.

Erforderliche Rolle: pki_admin oder admin

Hinweis: Genehmigungen werden derzeit nur in der Genehmigungs-Experience des Erfüllers unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Servicekatalog** > **Zertifikatverwaltung**.
2. Wählen Sie **Zertifikat widerrufen – Automatisierter Flow aus**.
3. Fügen Sie das ausgestellte Zertifikat ein, das Sie widerrufen möchten (z. B. www.undefined.com).
   Mehrere Zertifikate können zum Widerrufen ausgewählt werden.
4. Geben Sie einen ausreichenden Grund für den Widerruf des Zertifikats an.
   Für MicrosoftMicrosoft Azure Event Hubs CA muss der Grund ein ganzzahliger Wert sein. Wenn ein anderer Wert angegeben wird, wird der Standardwert 0 verwendet, was bedeutet, dass er nicht angegeben ist.
5. Um den Widerrufauftrag zu erteilen, wählen Sie **Absenden**aus.
6. Wählen Sie im Bestätigungs-Popup **OK**aus.

Ergebnisse

1. Wenn Sie einen Widerruf anfordern, wird automatisch eine Aufgabe wird erstellt.
   - Wenn die Bestell-ID und die Zertifikat-ID in der Zertifikaterweiterungstabelle [sn_disco_certmgmt_certificate_extension] vorhanden sind, erfordert der Widerruf keine Genehmigung.
   - Wenn die Bestell-ID und die Zertifikat-ID nicht in der Zertifikaterweiterungstabelle [sn_disco_certmgmt_certificate_extension] vorhanden sind, fordert die Aufgabe eine Genehmigung an.
   - Wenn die Seriennummer für Entrust CA Gateway nicht in der Tabelle „Zertifikatverlängerung“ [sn_disco_certmgmt_certificate_extension] vorhanden ist, wird von der Aufgabe eine Genehmigung angefordert.
2. Sobald das PKI-Team die Genehmigung erteilt hat, erfolgt die Zuordnung zwischen dem Zertifikat und der Zertifizierungsstelle basierend auf der ausgewählten Routing-Richtlinie.
3. Dadurch wird der Widerrufvorgang für die ausgewählte Zertifizierungsstelle ausgelöst, die die Zertifizierungsstellen-APIs verwendet.
4. Details werden in der Zertifikaterweiterungstabelle gespeichert.
5. Alle 30 Minuten wird die regelmäßige Aufgabe „DigiCert − Status der Zertifikatbestellung verfolgen“ ausgeführt, und der Status wird überprüft.

   Hinweis: Es gibt keine geplanten Aufgaben für Entrust CA Gateway und MicrosoftMicrosoft Azure Event Hubs CA.

6. Der Status des Zertifikats wird dann als widerrufen markiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Zertifikate können nicht widerrufen werden, wenn die Details der Zertifizierungsstelle oder die Zertifizierungs-ID in der Tabelle „Zertifikatverlängerung“ [sn_disco_certmgmt_certificate_extension] fehlen. Für Entrust CA Gateway können Zertifikate nicht widerrufen werden, wenn die Seriennummer fehlt. Erkennen Sie das Zertifikat über die Abfrage der Zertifizierungsstelle, um die erforderlichen Details in die Zertifikaterweiterungstabelle aufzunehmen. Anschließend wählt Discovery die Routing-Richtlinie aus und genehmigen die Aufgabe.

Widerrufen Sie die Anforderung der Zertifikat-API. Wenn „skip_approval“ „true“ ist, wird der Widerrufsprozess schneller abgeschlossen. Wenn „skip_approval“ auf „false“ festgelegt ist, wird der Widerrufsprozess abgeschlossen, sobald der DigiCert- oder Entrust CA Gateway-Administrator die Anforderung zum Widerrufen genehmigt oder abgelehnt hat. Um den Genehmigungsschritt zu überspringen, muss der API-Schlüssel über Administratorrechte verfügen.

Zertifikatintegrationen und -benachrichtigungen

Ab Version 1.2.0 ist Zertifikatsbestand-Management nahtlos in Ereignismanagementintegriert und bietet eine einheitliche Lösung für optimierte Abläufe. Diese Integration ermöglicht die Generierung von Ereignissen und Benachrichtigungen mit der zusätzlichen Funktion, Warnungen an Slack zu senden. Dadurch werden die Kommunikations- und Warnungsmechanismen im System Zertifikatsbestand-Management verbessert.

Ereignismanagement mit Zertifikatsbestand-Management integrieren

Ab Zertifikatsbestand-Management Version 1.2.0 und höher kann Ereignismanagement Ereignisse und Warnungen für ablaufende und abgelaufene Zertifikate erstellen und so die Überwachungsfunktionen des Systems verbessern.

Vorbereitungen

Stellen Sie sicher, dass die Store-Anwendung Ereignismanagement installiert ist.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die Integration nutzt die Funktion Flow Designer, um Ereignisse zu initiieren. Sie nutzt einen bereits vorhandenen täglichen Zeitplan Discovery, der abgelaufene oder ablaufende Zertifikate identifiziert und einen Subflow aktiviert. Bei der Aktivierung des Subflows wird die Installation der Store-Anwendung Ereignismanagement überprüft. Wenn die Anwendung installiert ist, generiert der Subflow ein Ereignis für ablaufende oder abgelaufene Zertifikate.

Prozedur

1. Um alle generierten Warnungen oder Ereignisse anzuzeigen, navigieren Sie zu **Alle** > **Ereignismanagement** > **Alle Warnungen** oder **Alle** > **Ereignismanagement** > **Alle Ereignisse**.
2. Um bestimmte Zertifikatereignisse auszuschließen und Warnungsauslöser zu verhindern, navigieren Sie zu **Ereignismanagement** > **Regeln** > **Ereignisregeln** und führen Sie die folgenden Schritte aus.
   a. Wählen Sie die Regel **Abgelaufenes Zertifikat/Ablaufende Ereignisse** aus.
   b. Wählen Sie die Registerkarte **Ereignisfilter**.
   c. Wählen Sie **Events ignorieren, die diesem Filter entsprechen** aus.
   d. Fügen Sie nach Bedarf weitere erforderliche Details hinzu.
   e. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatbenachrichtigungen in Slack erhalten

Richten Sie in Version 1.2.0 von Zertifikatsbestand-ManagementBenachrichtigungen für Slack ein, um über ablaufende und abgelaufene Zertifikate informiert zu werden. Erhalten Sie detaillierte Warnungen mit praktischen URL-Links für zusätzliche Informationen.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Eine regelmäßige Aufgabe in Zertifikatsbestand-Management überprüft regelmäßig die Ablaufdaten von Zertifikaten, die im Feld valid_to der Tabelle cmdb_ci_certificate gespeichert sind. Wenn Zertifikate abgelaufen sind oder sich dem Ablauf nähern, initiiert die Aufgabe den Subflow Slack-Nachricht verarbeiten, der anschließend Benachrichtigungen an den festgelegten Kanal Slack sendet.

Prozedur

1. Richten Sie Slack-Spoke ein .
2. Erstellen Sie einen Slack-Bot , und fügen Sie ihn einem Slack-Kanal hinzu.
3. Konfigurieren Sie die standardmäßigen Slack-Anmeldeinformationen .
4. Konfigurieren Sie anwenderdefinierte Slack-Anmeldeinformationen .

   Wenn Ihre Slack -Spoke-Version 1.2.0 ist, können Sie den nächsten Schritt zum Abrufen der Kanal-ID umgehen.

5. Rufen Sie die ID für Ihren Slack -Kanal ab.
   a. Wechseln Sie zu **Slack**.
   b. Klicken Sie mit der rechten Maustaste auf den Kanal.
   c. Auswahlvorgang **Weitere Optionen** > **Link kopieren**.
   d. Kopieren Sie die folgende Zeichenfolge über den bereitgestellten Link<archive/> .
6. Konfigurieren Sie die Eigenschaft Slack Kanal-ID.
   a. Navigieren zu **Discovery** > **Eigenschaften**.
   b. Geben Sie einen Wert in die Eigenschaft Slack Kanal-ID *glide.discovery.certs.slack_channel_id*ein.
7. Wählen Sie **Speichern**.

Ergebnisse
Benachrichtigungen werden an den Kanal Slack weitergeleitet, der in den Eigenschaften Discovery von angegeben ist. Wenn einem Benutzer ein Zertifikat zugewiesen ist und die konfigurierte E-Mail-Adresse mit der E-Mail-Adresse Slack übereinstimmt, wird der Benutzer in der Nachricht Slack gekennzeichnet. Die geplante Aufgabe Slack wird wöchentlich ausgeführt. Sie können ihre Häufigkeit anpassen, indem Sie die Einstellungen für die geplante Aufgabe „Zertifikatbenachrichtigung“ ändern.

Zertifikatgenerierung über Zertifikat-Manager-Integration

Fordern Sie ein Zertifikat über Kubernetes cert-manager mit dem ServiceNow Externen Aussteller (sn-external-issuer) an, und speichern Sie das Zertifikat und die zugehörigen Informationen sicher im Cluster Kubernetes als Geheimnis. In Kubernetesist ein Geheimnis ein Objekt, mit dem Sie vertrauliche Informationen wie Passwörter, API-Schlüssel und Zertifikate speichern und verwalten können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Erstellen eines externen Ausstellers finden Sie unter Erstellen und Bereitstellen eines externen Ausstellers für die Zertifikatverwaltung [KB1435392] .

Bereitstellungsanforderungen

- Stellen Sie „cert-manager“ in Ihrer Umgebung Kubernetes bereit. Aktualisieren Sie **die Datei „manager.yaml“** mit Instanz-URL, Zertifikatbesitzergruppe, Zertifikatbesitzer, Umgebung und Verlängerungsnachverfolgung.
- Stellen Sie den externen Aussteller ServiceNow (sn-external-issuer) in Ihrer Umgebung Kubernetes bereit. Erstellen Sie ein Kubernetes Geheimnis *`clusterissuer-servicenow-credentials`* mit dem Instanzanwendernamen und dem Passwort, um sicherzustellen, dass der Benutzer über die zum Anfordern eines -Zertifikats erforderlichen Rollen verfügt.

ServiceNow Externer Aussteller (sn-external-issuer)

- Externe Aussteller erweitern die Zertifikatmanager-Funktionalität, um Zertifikate über nicht zum Kern gehörende APIs und Services auszustellen.
- Der ServiceNow Externe Aussteller ist eine ServiceNow-spezifische Implementierung eines externen Ausstellers.
- Wenn eine neue Zertifikataufgabe erstellt wird, werden deren Zertifikatanforderungs-UID und Zertifikataufgaben-Sys-ID im lokalen JSON-Cache und in der Tabelle mit der Zertifikatanforderungs-UID zur Aufgabenzuordnung in der Instanz gespeichert.
- Der ServiceNow Externe Aussteller fragt die Instanz ab, um den Status der -Zertifikataufgabe zu überwachen.
- Wenn sich die Zertifikataufgabe im Status **„In Arbeit“** befindet, werden die Zertifikatanforderungs-UID und die Zertifikataufgaben-Sys-ID der Tabelle „UID-Zuordnung des externen Ausstellers“ in der Instanz und dem lokalen JSON-Cache hinzugefügt. Während dieser Zeit versucht der Zertifikatmanager automatisch, das Zertifikat anzufordern.
- Bei Erhalt einer Zertifikatanforderung sucht der Zertifikatmanager im lokalen JSON-Cache nach einer übereinstimmenden Aufgabe. Wenn der Wert gefunden wird, wird die gleiche Aufgabe abgefragt. Andernfalls wird die Instanz nach Datensätzen aus der Tabelle „UID-Zuordnung des externen Ausstellers“ abgefragt und der lokale JSON-Cache gefüllt.
- Sobald die Aufgabe als abgeschlossen markiert und das Zertifikat generiert wurde, sendet der externe Aussteller ServiceNow eine weitere Anforderung an die Instanz, lädt den Zertifikatanhang herunter und aktualisiert die Zertifikatressource und das entsprechende Geheimnis in Kubernetes.

Externer Aussteller von ServiceNow wird in bereitgestellt Kubernetes

Die Bereitstellung des externen Ausstellers von ServiceNow in Kubernetes umfasst die folgenden Schritte:

1. Rufen Sie auf der Downloadseite der ServiceNow-Instanz das ZIP-Paket „Helm Chart“ oder „YAML“ ab.
2. Passen Sie die Dateien `„manager.yaml“` oder `„values.yaml“` nach Bedarf für Ihren spezifischen Anwendungsfall an. Diese Dateien können wichtige Informationen wie die Instanz-URL und die Zertifikatbesitzergruppe enthalten.
3. Erstellen Sie ein Kubernetes -Geheimnis mit dem Namen `clusterissuer-servicenow-credentials` mit dem Anwendernamen und Passwort der Instanz.

   Beispielbefehl:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie ein Kubernetes -Geheimnis mit dem Namen `clusterissuer-servicenow-credentials` mit dem Anwendernamen und Passwort der Instanz. Beispielbefehl:

```
kubectl create secret generic clusterissuer-servicenow-credentials
              --from-literal=user=<user_name>
 --from-literal=password=<password> -n
           system
```

- Stellen Sie sicher, dass der Benutzer über die erforderlichen Rollen zum Anfordern von -Zertifikaten verfügt.

4. Führen Sie die folgenden Befehle für die Bereitstellung aus.

```
kubectl create ns system
kubectl apply -f crd
kubectl apply -f rbac
kubectl apply -f issuers
kubectl apply -f manager/manager.yaml
```

5. (Optional) Passen Sie alle zusätzlichen Konfigurationen in den Dateien an Ihre spezifischen Anforderungen an.
6. Stellen Sie sicher, dass die Bereitstellung erfolgreich ist und der externe Aussteller von ServiceNow betriebsbereit ist.

Flow zum Anfordern eines neuen Zertifikats

Übermitteln Sie nach der Bereitstellung eine Zertifikatressource mit den folgenden Informationen in einer Datei namens `certification_clusterisuer.yaml`.

- IssuerRef: clusterissuer-servicenow
- Aussteller: Aussteller-servicenow
- Art: ClusterIssuer
- IssuerRef: servicenow-issuer.servicenow.com

Hier ist ein Beispiel für eine Zertifikatressource:

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
name: certificate-by-clusterissuer
spec:
commonName: certificate-by-clusterissuer.servicenow.com
secretName: certificate-by-clusterissuer
dnsNames:
- servicenow.com
- foo.servicenow.com
issuerRef:
name: clusterissuer-servicenow
group: servicenow-issuer.servicenow.com
kind: ClusterIssuer
```

Wenden Sie die Zertifikatressource mit `kubectl anwenden -f Certificate_clusterissuer.yaml an`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management verwenden

Zertifikatsbestand-Management ist ein leistungsstarkes Tool für die zentrale Nachverfolgung und effiziente Verwaltung digitaler Zertifikate, das Sicherheits-Compliance und optimierte Abläufe sicherstellt.

Zertifikatsbestand-Management – Referenz

Referenzthemen enthalten zusätzliche Informationen zum Dashboard Zertifikatsbestand-Management und zu den zugehörigen Komponenten, einschließlich Tabellen, Mustern und Begriffen.

Zertifikatsbestand-Management Tabellen

Zertifikatsbestand-Management -Tabellen bieten ein zentralisiertes System zum Nachverfolgen und Verwalten digitaler Zertifikate. Sie erfassen wichtige Details, einschließlich erkannter Zertifikate, Installationsorte, Verlaufsdaten und zugehöriger Aufgaben wie Verlängerungen und Anforderungen. Dieses Framework gewährleistet eine effiziente Zertifikatverwaltung und unterstützt Sicherheit, Compliance und optimiert den Betrieb.

Zertifikatsbestand-Management Tabellen

Tabelle	Beschreibung
Eindeutiges Zertifikat [cmdb_ci_certificate]	Discovery füllt diese Tabelle mit einem Datensatz für jedes eindeutige Zertifikat, das für die Zertifikatverwaltung erkannt wurde. Die Fingerabdruckspalte ist für jedes Serverzertifikat eindeutig. **Hinweis:** Sie können die gesamte Zertifikatkette auch über die zugehörige Liste in der Tabelle „Eindeutiges Zertifikat“ anzeigen.
Installiertes Zertifikat [sn_disco_certmt_cmdb_installed_certificate]	Discovery füllt diese Tabelle mit allen erkannten Zertifikaten und zeigt alle Speicherorte an, an denen Zertifikate installiert sind. Sie enthält keinen Verweis auf das Server-CI, und IRE wird nicht durchlaufen. Alle Beziehungen mit dem verwalteten Zertifikat werden in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] gespeichert. Die Beziehungen können für Server, Anwendungen und Business Services sein.
Erkanntes Zertifikat [sn_disco_certmgmt_certificate_history]	Erkannte Zertifikate werden zuerst als Teil des Shazzam- und URL-Erkennungssensors in dieser Tabelle gespeichert und zeigen die XML-Nutzlast aller Zertifikate mit dieser Adresse an.
Zertifikatdomäne [Zertifikatdomäne]	Speichert eine oder mehrere Domänen für den alternativen Antragstellernamen.
Zertifikataufgabe [sn_disco_certmgmt_certificate_task]	Speichert alle Aufgaben zur Zertifikatverlängerung und zur Anforderung neuer Zertifikate.
Zertifikat-URL [sn_disco_certmgmt_cert_url]	Enthält eine Liste von URLs nach Zeile für das Ziel für die Zertifikat-Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management Tabellen (Fortsetzung)

Tabelle	Beschreibung
Anmeldeinformationen für die Zertifikatverwaltung [sn_disco_certmgmt_certificate_management_credential] (Version 1.1.7, Zertifikatbestand und -verwaltung)	Speichert die CA-Typen einschließlich GoDdies und DigiCert. Andere werden basierend auf dem Skript certificate_authority gefüllt. Nur discovery_admin kann andere CA-Anmeldeinformationen erstellen. Für zukünftige Releases ist die Unterstützung von externen Anmeldeinformationen vorgesehen.
Geplante Zertifikat-URL [sn_discovery_cert_url_sched_m2m]	Verknüpft die URLs zur Erkennung von [discovery_cert_url] mit einem bestimmten Discovery-Zeitplan [discovery_schedule].
Zertifizierungsstelle [sn_disco_certmgmt_ca] (Version 1.3.8 Certificate Inventory and Management)	Enthält den Namen der Zertifizierungsstelle und die Basis-URL der REST API.
Zertifizierungsstellen-API-URL [sn_disco_certmgmt_ca_api_url] (Version 1.3.8 Certificate Inventory and Management)	Enthält die Referenz der Zertifizierungsstelle, die Endpunkt-URL der REST API und den Typ der Zertifikatvalidierung.
Routing-Richtlinie [sn_disco_certmgmt_routing_policy] (Version 1.3.8 Certificate Inventory and Management)	Entscheidet, welche Zertifizierungsstelle für Zertifikatvorgänge kontaktiert werden muss. Diese Tabelle enthält die Attribute für die Zertifizierungsstelle, deren URL, Anmeldeinformationen, Genehmigungsgruppe, Zuweisungsgruppe und CSR.
Automatisierte Zertifikataufgabe [sn_disco_certmgmt_task] (Version 1.3.8 Certificate Inventory and Management)	Enthält alle automatisierten Zertifikatanforderungsaufgaben (neu, verlängern und widerrufen).
Neue Zertifikataufgaben [sn_disco_certmgmt_new_task] (Version 1.3.8 Certificate Inventory and Management)	Erweitert von sn_disco_certmgmt_task und enthält Aufgaben zur Anforderung neuer Zertifikate.
Aufgaben „Zertifikat verlängern“ [sn_disco_certmgmt_renew_task] (Version 1.3.8 Certificate Inventory and Management)	Erweitert von sn_disco_certmgmt_task und enthält Aufgaben zur Anforderung eines verlängerten Zertifikats.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management Tabellen (Fortsetzung)

Tabelle	Beschreibung
Aufgaben „Zertifikat widerrufen“ [sn_disco_certmgmt_revoke_task] (Version 1.3.8 Certificate Inventory and Management)	Erweitert von „sn_disco_certmgmt_task“ und enthält Aufgaben zum Widerrufen von Zertifikatanforderungen.
Zertifikatverlängerungen [sn_disco_certmgmt_certificate_extension] (Version 1.3.8 Certificate Inventory and Management)	Speichert Informationen für alle Serverzertifikate.

Zertifikatsbestand-Management-Muster

Zertifikatbestandsmuster optimieren die Verwaltung digitaler Zertifikate, sorgen für mehr Sicherheit, Compliance und eine effiziente Lebenszykluskontrolle und reduzieren das Risiko von Schwachstellen. Verwalten Sie den Zertifikatbestand mit optimierten Mustern effizient.

Zertifikatsbestand-Management Muster und Beschreibungen

Muster	Beschreibung
GoDdies – Certificate Management-Muster (Version 1.1.7 Certificate Inventory and Management)	Teil der Anwendung „Certificate Inventory and Management“ Ermöglicht den Import von Zertifikaten und die Suche nach Zertifikaten der Zertifizierungsstelle (CA) GoDaddy
DigiCert – Certificate Management Pattern (Version 1.1.7 Certificate Inventory and Management)	Teil der Anwendung „Certificate Inventory and Management“ Ermöglicht den Import von Zertifikaten und die Suche nach Zertifikaten der Zertifizierungsstelle (CA) DigiCert
Entrust – Zertifikatverwaltungsmuster (Version 1.2.0, Zertifikatbestand und -verwaltung)	Teil der Anwendung „Certificate Inventory and Management“ Ermöglicht den Import von Zertifikaten und die Suche nach Zertifikaten der Zertifizierungsstelle (CA) Entrust
Sectigo – Zertifikatverwaltungsmuster (Version 1.2.0, Zertifikatbestand und -verwaltung)	Teil der Anwendung „Certificate Inventory and Management“ Ermöglicht den Import von Zertifikaten und die Suche nach Zertifikaten der Zertifizierungsstelle (CA) Sectigo
Importieren Sie das SSL-Zertifikatmuster Version 1.1.7 Certificate Inventory and Management.	Ermöglicht die Erkennung von Zertifikaten durch den Import von Zertifikaten aus Dateien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsbestand-Management Muster und Beschreibungen (Fortsetzung)

Muster	Beschreibung
Muster**für Amazon AWS – Certificate Manager** und **Amazon AWS – Tags für Zertifikat-Tags sammeln**. Zertifikatsbestand-Management, mindestens 3.4.0. Muster für Discovery und Service-Mapping, mindestens 1.12.0.	Erkennt Zertifikate im Rahmen der AWS Cloud-Discovery.
Muster**für Google Cloud Platform (GCP) – Zertifikatmanager-Zertifikate** und **Google Cloud Platform (GCP) – Muster für klassische Zertifikate**. Zertifikatsbestand-Management, mindestens 3.4.0. Muster für Discovery und Service-Mapping, mindestens 1.12.0.	Erkennt Zertifikate im Rahmen der GCP Cloud-Discovery.
Azure – Key Vault-Zertifikatmuster. Zertifikatsbestand-Management, mindestens 3.4.0. Muster für Discovery und Service-Mapping, mindestens 1.12.0.	Erkennt Zertifikate im Rahmen der Azure Cloud-Discovery.

AWS Discovery des Zertifikat-Managers

Cloud-Discovery verwendet Muster, um Zertifikatdaten zu erkennen, die vom Amazon AWS Cloud Certificate Manager (ACM) verwaltet werden. Zum Erkennen dieser Daten müssen Muster für Discovery und Service-Mapping und Zertifikatsbestand-Managementinstalliert und aktualisiert werden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüft die Konfiguration eines AWS -Accounts

Weitere Informationen finden Sie unter Cloud-Discovery erkunden

Überprüfen Sie die Installation der Plugins

Zertifikatsbestand-Management (sn_disco_certmgmt) mindestens 3.4.0

Muster für Discovery und Service-Mapping (sn_itom_pattern) mindestens 1.12.0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass Cloud-Discovery berechtigt ist, AWSzu erkennen.

Führen Sie die folgenden Befehle mit AWS der CLI aus, um die Berechtigungen und Richtlinien zu überprüfen, die an Ihre aktive IAM-Rolle angehängt sind:

- Zertifikate auflisten

```
AWS_PAGER = „" AWS ACM-Liste der Zertifikate - Region<region>
```

- Beschreiben Sie die Zertifikate

```
AWS_PAGER = „" AWSACM-Beschreibung-Zertifikat --Zertifikat-
Arnarn:Aws:ACM:<region> :<accout_id> :Zertifikat/
<certificate_id>
```

- Ruft Zertifikate ab

```
AWS_PAGER = ''awsacm get-certificate --certificate-
arnarn:aws:acm:<region> :<account_id> :Zertifikat/
<certificate_id>
```

- Tags abrufen

```
AWS_PAGER = „" awsresourcegroupstaggingapi get-resources --
tags-pro-seite 100 --resource-type-filters „acm:certificate"
```

Legen Sie die Konfiguration der Systemeigenschaft fest

Wenn die Systemeigenschaft *sn_itom_pattern.issuer_certificate_search_by_idn* auf **false**festgelegt ist, verwendet Discovery die Fingerabdrücke des Zertifikats, um Aussteller und Stammaussteller zu finden.

Verifizieren Sie die Anforderungen für MID-Server .

MID-Server muss entweder die Fähigkeit „ALL" oder „AWS" aufweisen.

Überprüfen Sie die Konfiguration des Zeitplans Cloud-Discovery .

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Das Muster **„Amazon AWS – Certificate Manager"** und die gemeinsame Bibliothek **„Amazon AWS – Zertifikat-Tags sammeln"** unterstützen die Discovery der folgenden Tabellen und Felder.

Feld	Beschreibung
Eindeutige Zertifikate [cmdb_ci_certificate]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Hostname/Domäne, der bzw. die dem Zertifikat zugeordnet ist. Beispiel: **.service-now.com*
Fingerabdruck	Hashwert des Zertifikats Beispiel: *d708c8583c78c176d5df1a4f01aac746294 e390a03038f280b0d8*
Fingerabdruck-Algorithmus	Der Algorithmus, der zum Hashing des Zertifikats verwendet wird. Beispiel: Dis Fingerabdrücke mit dem SHA-256-Algorithmus. Der ausgefüllte Wert lautet d
Seriennummer	Seriennummer des Zertifikats Beispiel: *70 d8 c9 52 77 1c 2d 54 97 00 b5 e8 c1 73*
Allgemeiner Antragstellername	Hostname/Domäne, der bzw. die dem Zertifikat zugeordnet ist. Beispiel: **.s*
Eindeutiger Antragstellername	Der eindeutige Name der Entität, für die das Zertifikat ausgestellt wird. Der Distinguished Name des Antragstellers besteht aus Folgendem • Allgemeiner Name (CN). • Organisation (O) – Die Organisation, die die Domäne besitzt,, für die das Z wird. • Organisationseinheit (OU) – Die Organisationseinheit, die die Domäne bes Zertifikat ausgestellt wird.
Allgemeiner Ausstellername	Allgemeiner Name des Zertifikatausstellers. Beispiel: Zertifizierungsstelle von E
Eindeutiger Name des Ausstellers	Der eindeutige Name des Zertifikatausstellers. Der Distinguished Name des Ausstellers besteht aus Folgendem • Common Name (CN) – die Behörde, die das Zertifikat ausgestellt hat. Beis *Zertifizierungsstelle von Entrust*. • Organisation (O) – Die Organisation, die das Zertifikat ausgestellt hat. Beisp *Inc.* • Organisationseinheit (OE): Einheit, die über die gesetzlichen Rechte zum A Zertifikats verfügt.
Verlängerungsnachverfolgung	Gibt an, ob Aufgaben mit Priorität 1 oder Priorität 3 für ablaufende Zertifikat sollen Discovery legt **die Verlängerungsnachverfolgung** auf *Priorität3* fest, wen Systemeigenschaft *glide.discovery.certs.enable_renewal_task_creation_for_discov* auf **true** festgelegt ist.
Gültig ab	Das Zertifikat ist ab diesem Datum (UTC) gültig. Beispiel: *2023-09-25 10:43*

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Gültig bis	Das Ablaufdatum des Zertifikats (UTC). Beispiel: 2024-09-24 10:43:03
Antragstellerorganisation	Die Organisation (O), für die das Zertifikat ausgestellt wurde.
Antragsteller-Organisationseinheit	Die Organisationseinheit (OE), für die das Zertifikat ausgestellt wird.
Antragstellerland	Das Land (C) der Organisation, für die das Zertifikat ausgestellt wurde. Wird Buchstaben bestehenden Ländercode ausgefüllt.
Antragstellerstatus	Die Region, das Bundesland oder der Kanton der Organisation, für die das Z wurde. Wird mit einem Code aus zwei Buchstaben ausgefüllt.
Antragsteller-Ort	Stadt, Standort (L) der Organisation, für die das Zertifikat ausgestellt wurde.
E-Mail-Adresse des Antragstellers	Die E-Mail-Adresse der Organisation, für die das Zertifikat ausgestellt wurde.
Bearbeiter	Ein Verweis auf die Entität, die das Zertifikat signiert und ausgestellt hat. Die verfügbar, wenn das ausgegebene Zertifikat Teil derselben Nutzlast ist.
Stammaussteller	Ein Verweis auf das Stammzertifikat. Die Referenz ist verfügbar, wenn das au Teil derselben Nutzlast ist.
Alternativer Antragstellername	Der Name des Zertifikatdomänendatensatzes.

CI-Beziehungen

Das Muster **„Amazon AWS – Certificate Manager“** und die gemeinsame Bibliothek **„Amazon AWS – Zertifikat-Tags sammeln“** unterstützen die Discovery der folgenden Beziehungen:

CI	Beziehung	CI
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Schlüsselwert [cmdb_key_value]	Referenz	Eindeutiges Zertifikat [cmdb_ci_certificate]

GCP Discovery des Zertifikat-Managers

Cloud-Discovery verwendet Muster, um Zertifikatdaten zu erkennen, die vom Zertifikatmanager GCP verwaltet werden. Zum Erkennen dieser Daten müssen Muster für Discovery und Service-Mapping und Zertifikatsbestand-Managementinstalliert und aktualisiert werden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Überprüft die Konfiguration eines GCP -Accounts

Weitere Informationen finden Sie unter Cloud-Discovery erkunden

Überprüfen Sie die Installation der Plugins

Zertifikatsbestand-Management (sn_disco_certmgmt), mindestens 3.4.0

Muster für Discovery und Service-Mapping (sn_itom_pattern), mindestens 1.12.0

Überprüfen Sie die Konfiguration der Systemeigenschaft

Wenn die Systemeigenschaft *sn_itom_pattern.issuer_certificate_search_by_idn* auf **False**festgelegt ist, verwendet Discovery die Fingerabdrücke des Zertifikats, um Aussteller und Stammaussteller zu finden.

Verifizieren Sie die Anforderungen für MID-Server .

MID-Server muss entweder die Fähigkeit **„ALL“** oder die Fähigkeit **„GCP“** aufweisen.

Überprüfen Sie die Konfiguration des Zeitplans Cloud-Discovery .

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die Muster **„Google Cloud Platform (GCP) – Certificate Manager Certificates“** und **„Google Cloud Platform (GCP) – Classic Certificates“** unterstützen die Discovery der folgenden Tabellen und Felder.

Feld	Beschreibung
Eindeutige Zertifikate [cmdb_ci_certificate]	
Name	Hostname/Domäne, der bzw. die dem Zertifikat zugeordnet ist. Beispiel: **.service-now.com*
Seriennummer	Seriennummer des Zertifikats Beispiel: *70 d8 c9 52 77 1c 2d 54 97 00 b5 e8 c1 73*
Allgemeiner Antragstellername	Hostname/Domäne, der bzw. die dem Zertifikat zugeordnet ist. Beispiel: **.*
Eindeutiger Antragstellername	Der eindeutige Name der Entität, für die das Zertifikat ausgestellt wird. Der Distinguished Name des Antragstellers besteht aus Folgendem

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Allgemeiner Name (CN). • Organisation (O): Die Organisation, die die Domäne besitzt, für die das Ze wird. • Organisationseinheit (OU) – Die Organisationseinheit, die die Domäne bes Zertifikat ausgestellt wird.
Allgemeiner Ausstellername	Allgemeiner Name des Zertifikatausstellers. Beispiel: Zertifizierungsstelle von E
Eindeutiger Name des Ausstellers	Der eindeutige Name des Zertifikatausstellers. Der Distinguished Name des Ausstellers besteht aus Folgendem • Common Name (CN) – die Behörde, die das Zertifikat ausgestellt hat. Beis *Zertifizierungsstelle von Entrust*. • Organisation (O) – Die Organisation, die das Zertifikat ausgestellt hat. Beisp *Inc.* • Organisationseinheit (OE): Einheit, die über die gesetzlichen Rechte zum A Zertifikats verfügt.
Verlängerungsnachverfolgung	Gibt an, ob Aufgaben mit Priorität 1 oder Priorität 3 für ablaufende Zertifikat sollen Discovery legt **die Verlängerungsnachverfolgung** auf *Prioritäts*fest, wen Systemeigenschaft *glide.discovery.certs.enable_renewal_task_creation_for_discov* auf **true**festgelegt ist.
Gültig ab	Das Zertifikat ist ab diesem Datum (UTC) gültig. Beispiel: *2023-09-25 10:43*
Gültig bis	Das Ablaufdatum des Zertifikats (UTC). Beispiel: 2024-09-24 10:43:03
Antragstellerorganisation	Die Organisation (O), für die das Zertifikat ausgestellt wurde.
Antragsteller-Organisationseinheit	Die Organisationseinheit (OE), für die das Zertifikat ausgestellt wird.
Antragstellerland	Das Land (C) der Organisation, für die das Zertifikat ausgestellt wurde. Wird Buchstaben bestehenden Ländercode ausgefüllt.
Antragstellerstatus	Die Region, das Bundesland oder der Kanton der Organisation, für die das Z wurde. Wird mit einem Code aus zwei Buchstaben ausgefüllt.
Antragsteller-Ort	Stadt, Standort (L) der Organisation, für die das Zertifikat ausgestellt wurde.
E-Mail-Adresse des Antragstellers	Die E-Mail-Adresse der Organisation, für die das Zertifikat ausgestellt wurde.
Bearbeiter	Ein Verweis auf die Entität, die das Zertifikat signiert und ausgestellt hat. Die verfügbar, wenn das ausgegebene Zertifikat Teil derselben Nutzlast ist.
Stammaussteller	Ein Verweis auf das Stammzertifikat. Die Referenz ist verfügbar, wenn das au Teil derselben Nutzlast ist.
Alternativer Antragstellername	Der Name des Zertifikatdomänendatensatzes.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Die Muster **„Google Cloud Platform (GCP) – Certificate Manager Certificates“** und **„Google Cloud Platform (GCP) – Classic Certificates“** unterstützen die Discovery der folgenden Beziehungen:

CI	Beziehung	CI
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	Google-Rechenzentrum [cmdb_ci_google_datacenter]
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Schlüsselwert [cmdb_key_value]	Referenz	Eindeutiges Zertifikat [cmdb_ci_certificate]

Azure Discovery des Key Vault-Zertifikats

Cloud-Discovery verwendet Muster, um die Key Vault-Zertifikate von Azure zu erkennen. Zum Erkennen dieser Daten müssen Muster für Discovery und Service-Mapping und Zertifikatsbestand-Managementinstalliert und aktualisiert werden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Überprüft die Konfiguration eines Azure -Accounts

Weitere Informationen finden Sie unter Cloud-Discovery erkunden

Überprüfen Sie die Installation der Plugins

Zertifikatsbestand-Management (sn_disco_certmgmt), mindestens 3.4.0

Muster für Discovery und Service-Mapping (sn_itom_pattern), mindestens 1.12.0

Überprüfen Sie die Konfiguration der Systemeigenschaft

Stellen Sie sicher, dass *sn_itom_pattern.issuer_certificate_search_by_idn* auf **„Wahr“** festgelegt ist, um Discovery so zu konfigurieren, dass Aussteller nur anhand des eindeutigen Namens des Ausstellers gesucht werden. Discovery kann den Fingerabdruck nicht für jedes Zertifikat in der Kette berechnen, da PFX-Datensätze für Schlüsselwertzertifikate keine Zertifikatketten enthalten.

Verifizieren Sie die Anforderungen für MID-Server .

MID-Server muss entweder die Fähigkeit **„ALL“** oder **„Azure“** aufweisen.

Überprüfen Sie die Konfiguration des Zeitplans Cloud-Discovery .

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Das Muster **„Azure – Key Vault-Zertifikate“** unterstützt die Discovery der folgenden Tabellen und Felder.

Feld	Beschreibung
Eindeutige Zertifikate [cmdb_ci_certificate]	
Name	Hostname/Domäne, der bzw. die dem Zertifikat zugeordnet ist. Beispiel: *`*.service-now.com`*
Seriennummer	Seriennummer des Zertifikats Beispiel: *`70 d8 c9 52 77 1c 2d 54 97 00 b5 e8 c1 73`*
Allgemeiner Antragstellername	Hostname/Domäne, der bzw. die dem Zertifikat zugeordnet ist. Beispiel: *`*.s`*
Eindeutiger Antragstellername	Der eindeutige Name der Entität, für die das Zertifikat ausgestellt wird. Der Distinguished Name des Antragstellers besteht aus Folgendem • Allgemeiner Name (CN). • Organisation (O): Die Organisation, die die Domäne besitzt, für die das Ze wird. • Organisationseinheit (OU) – Die Organisationseinheit, die die Domäne bes Zertifikat ausgestellt wird.
Allgemeiner Ausstellername	Allgemeiner Name des Zertifikatausstellers. Beispiel: Zertifizierungsstelle von E
Eindeutiger Name des Ausstellers	Der eindeutige Name des Zertifikatausstellers. Der Distinguished Name des Ausstellers besteht aus Folgendem • Common Name (CN) – die Behörde, die das Zertifikat ausgestellt hat. Beis *`Zertifizierungsstelle von Entrust`*. • Organisation (O) – Die Organisation, die das Zertifikat ausgestellt hat. Beisp *`Inc.`* • Organisationseinheit (OE): Einheit, die über die gesetzlichen Rechte zum A Zertifikats verfügt.
Verlängerungsnachverfolgung	Gibt an, ob Aufgaben mit Priorität 1 oder Priorität 3 für ablaufende Zertifikat sollen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Discovery legt **die Verlängerungsnachverfolgung** auf *Priorität3* fest, wen Systemeigenschaft *glide.discovery.certs.enable_renewal_task_creation_for_discov* auf **true** festgelegt ist.
Gültig ab	Das Zertifikat ist ab diesem Datum (UTC) gültig. Beispiel: *2023-09-25 10:43*
Gültig bis	Das Ablaufdatum des Zertifikats (UTC). Beispiel: 2024-09-24 10:43:03
Antragstellerorganisation	Die Organisation (O), für die das Zertifikat ausgestellt wurde.
Antragsteller-Organisationseinheit	Die Organisationseinheit (OE), für die das Zertifikat ausgestellt wird.
Antragstellerland	Das Land (C) der Organisation, für die das Zertifikat ausgestellt wurde. Wird Buchstaben bestehenden Ländercode ausgefüllt.
Antragstellerstatus	Die Region, das Bundesland oder der Kanton der Organisation, für die das Z wurde. Wird mit einem Code aus zwei Buchstaben ausgefüllt.
Antragsteller-Ort	Stadt, Standort (L) der Organisation, für die das Zertifikat ausgestellt wurde.
E-Mail-Adresse des Antragstellers	Die E-Mail-Adresse der Organisation, für die das Zertifikat ausgestellt wurde.
Bearbeiter	Ein Verweis auf die Entität, die das Zertifikat signiert und ausgestellt hat. Die verfügbar, wenn das ausgegebene Zertifikat Teil derselben Nutzlast ist.
Stammaussteller	Ein Verweis auf das Stammzertifikat. Die Referenz ist verfügbar, wenn das au Teil derselben Nutzlast ist.
Alternativer Antragstellername	Der Name des Zertifikatdomänendatensatzes.

CI-Beziehungen

Das Muster **„Azure – Key Vault-Zertifikate“** unterstützt die Discovery der folgenden Beziehungen:

CI	Beziehung	CI
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Eindeutiges Zertifikat [cmdb_ci_certificate]	Hostet::Gehostet auf	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Schlüsselwert [cmdb_key_value]	Referenz	Eindeutiges Zertifikat [cmdb_ci_certificate]

Discovery von Java KeyStore und Windows-Zertifikatspeicher .

Discovery verwendet den Erweiterungsabschnitt **„Zertifikate sammeln“** der Muster für **Linux Server** und **Windows – Server,** um Zertifikate zu erkennen, die im Java KeyStore oder im Windows Zertifikatspeicher gespeichert sind. Zum Erkennen der Zertifikatinformationen müssen Muster für Discovery und Service-Mapping und Zertifikatsbestand-Managementinstalliert und aktualisiert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Stellen Sie sicher, dass die folgenden Plugins auf dem neuesten Stand sind

- Muster für Discovery und Service-Mapping (sn_itom_pattern), mindestens 1.12.0
- Zertifikatsbestand-Management (sn_disco_certmgmt), mindestens 3.4.0

Stellen Sie sicher, dass für das Muster aktiviert ist

Die Mustererweiterung **„Zertifikate sammeln“** ist standardmäßig deaktiviert. Überprüfen Sie in der Liste **„Discovery-Muster“**, ob für die Erweiterung „ **Zertifikate sammeln** “ das Feld **Aktiv** auf **true**festgelegt ist.

Überprüfen Sie die Konfiguration der Java KeyStore-Anmeldeinformationen

Wählen Sie im Modul **Discovery-Anmeldeinformationen** die **Option jks-Anmeldeinformationen**aus. Stellen Sie sicher, dass Sie die Discovery-IP-Affinität konfiguriert haben. Fügen Sie im Feld **Typ**,`java_keystore`ein. Weitere Informationen finden Sie unter Erste Schritte mit Anmeldeinformationen

Überprüfen Sie die Konfiguration des Zeitplans Discovery.

Weitere Informationen finden Sie unter Erkennungen im Netzwerk ausführen

Von Discovery während der horizontalen Erkennung erfasste Daten

Der Abschnitt mit der Erweiterung **„Zertifikate sammeln“** der Muster **Linux Server** und **Windows OS – Server** unterstützt die Discovery der folgenden Tabellen und Felder.

Feld	Beschreibung
Eindeutige Zertifikate [cmdb_ci_certificate]	
Fingerabdruck [fingerprint]	Die Fingerabdrucknummer des Zertifikats.
Seriennummer [serial_number]	Seriennummer des Zertifikats
Signaturalgorithmus [signature_algorithm]	Der Signaturalgorithmus des Zertifikats.
Fingerabdruck-Algorithmus [fingerprint_algorithm]	Der Fingerabdruckalgorithmus des Zertifikats.
Distinguished Name des Ausstellers [issuer_distinguished_name]	Der eindeutige Name des Zertifikatausstellers. Der Distinguished Name des Ausstellers besteht aus Folgendem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Common Name (CN) – die Behörde, die das Zertifikat ausgestellt hat. Beispiel: *Zertifizierungsstelle von Entrust*. • Organisation (O) – Die Organisation, die das Zertifikat ausgestellt hat. Beispiel: *„Entrust", Inc.* • Organisationseinheit (OE): Einheit, die über die gesetzlichen Rechte zum Ausstellen des Zertifikats verfügt.
Distinguished Name des Antragstellers [subject_distinguished_name]	Der eindeutige Name der Entität, für die das Zertifikat ausgestellt wird. Der Distinguished Name des Antragstellers besteht aus Folgendem • Allgemeiner Name (CN). • Organisation (O): Die Organisation, die die Domäne besitzt, für die das Zertifikat ausgestellt wird. • Organisationseinheit (OU) – Die Organisationseinheit, die die Domäne besitzt, für die das Zertifikat ausgestellt wird.
Allgemeiner Antragstellername [subject_common_name]	Hostname oder Domäne, der bzw. die dem Zertifikat zugeordnet ist.
Antragstellerland [subject_country]	Das Land (C) der Organisation, für die das Zertifikat ausgestellt wurde. Wird mit einem aus zwei Buchstaben bestehenden Ländercode ausgefüllt.
Antragstellerstatus [subject_state]	Die Region, das Bundesland oder der Kanton der Organisation, für die das Zertifikat ausgestellt wurde. Diese Daten werden mit einem Code aus zwei Buchstaben ausgefüllt.
Antragstellerort [subject_locality]	Stadt, Standort (L) der Organisation, für die das Zertifikat ausgestellt wurde.
Antragsteller-Organisationseinheit [subject_organizational_unit]	Die Organisationseinheit (OE), für die das Zertifikat ausgestellt wird.
Antragstellerorganisation [subject_organization]	Die Organisation (O), für die das Zertifikat ausgestellt wurde.
Betreff-E-Mail [subject_email]	Die E-Mail-Adresse der Organisation, für die das Zertifikat ausgestellt wurde.
Gültig ab [valid_from]	Das Zertifikat ist ab diesem Datum gültig (Wird in Ihrer Zeitzone angezeigt.). Beispiel: *2023-09-25 10:43:03*
Gültig bis [valid_to]	Das Ablaufdatum des Zertifikats (Wird in Ihrer Zeitzone angezeigt.). Beispiel: 2024-09-24 10:43:03
Status [state]	Wenn Discovery das Zertifikat sammelt, zeigt das Feld **„installiert“**an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Alternativer Antragstellername [subject_alternative_name]	Eine Liste von Verweisen auf alternative Hostnamen, die vom Server verwendet werden.
Aussteller [issuser]	In diesem Feld befindet sich ein Verweis auf den Zertifikatdatensatz. Der Aussteller ist die Entität, die das Zertifikat signiert und ausgestellt hat. Die Referenz ist verfügbar, wenn das ausgegebene Zertifikat Teil derselben Nutzlast ist.
Installiertes Zertifikat [sn_disco_certmgmt_cmdb_installed_certificate]	
Discovery-Methode [discovery_method]	Wenn dieses installierte Zertifikat von einem Muster erkannt wurde, zeigt das Feld **Muster**an.
Quelle [source]	Die IP-Adresse des Host-Servers, auf dem Discovery ausgeführt wird.
Server [Server]	Der Java-basierte Webserver oder Windows -basierte Webserver, der das Zertifikat in Java-KeyStores auf dem Hostcomputer speichert.
Stammaussteller [root_issuer]	Ein Verweis auf den Stammzertifikatdatensatz. Die Referenz ist verfügbar, wenn das ausgegebene Zertifikat Teil derselben Nutzlast ist.

Zertifikatsbestand-Management Begriffe

Das Glossar für das Zertifikatsbestandsmanagement enthält eine Reihe von präzisen Definitionen und Erklärungen für Begriffe, die sich auf die Nachverfolgung, Speicherung und Verwaltung digitaler Zertifikate in einer IT-Umgebung beziehen.

Zertifizierungsstelle (CA)

: Entität, die ein digitales Zertifikat ausstellt

Zertifikatfingerabdruck

: Enthält die eindeutigen Informationen des Zertifikats, zum Beispiel Metadaten

Erkennungsmethode - CA (Zertifikatsbestand-Management Version 1.1.7)

: TLS-Zertifikate, die zu dieser Kategorie der Erkennungsmethode gehören, werden von einer Zertifizierungsstelle wie GoDaddy und DigiCert erkannt.

Erkennungsmethode - Zertifikatimport (Zertifikatsbestand-Management Version 1.1.7)

: TLS-Zertifikate, die zu dieser Kategorie der Erkennungsmethode gehören, werden erkannt, indem die Dateien mithilfe der musterbasierten Erkennung in das System importiert werden.

Erkennungsmethode - Port

: TLS-Zertifikate, die zu dieser Kategorie der Erkennungsmethode gehören, werden an Listener-Ports von Remoteservern erkannt.

Erkennungsmethode - URL

: TLS-Zertifikate, die zu dieser Kategorie der Erkennungsmethode gehören, werden aus URLs erkannt.

Externes Zertifikat

: Gibt an, dass das digitale Zertifikat entweder von der Stamm- oder Zwischenzertifizierungsstelle signiert ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Internes Zertifikat oder selbstsigniert

Gibt an, dass das digitale Zertifikat von derselben Entität signiert ist, deren Identität es zertifiziert. Zum Beispiel sind interne oder selbstsignierte Zertifikate nicht von Stamm- oder Zwischen-CAs signiert.

Transport Layer Security (TLS)

Nachfolgeprotokoll zu SSL. TLS ist eine verbesserte Version von SSL. Es funktioniert ähnlich wie SSL und verwendet eine Verschlüsselung, um die Übertragung von Daten und Informationen zu schützen.

Trust-Manager

Validiert das TLS-Zertifikat

Truststore

Repository zum Speichern von CA-Zertifikaten

Eindeutige und installierte Zertifikate im Vergleich

Eindeutig: Jede eindeutige Instanz bzw. jeder eindeutige Fingerabdruck eines Zertifikats

Installiert: Zeigt an, wo jedes erkannte Zertifikat installiert ist

API-Elemente und Berechtigungen für Muster von Zertifizierungsstellen

Erkunden Sie die API-Muster-Elemente und Berechtigungen von Zertifizierungsstellen (Certificate Authorities, CA), um umfassende Einblicke in die zugehörigen Funktionalitäten und Autorisierungsanforderungen zu erhalten.

API-Elemente und -Berechtigungen

Zertifizierungsstellen	API-Element
GoDaddy	• * / v1 / Zertifikate • * /v1/certificates/{certificate_id}/download
DigiCert	• * /services/v2/order/certificate • * /services/v2/certificate/{certificate_id}/chain
Entrust	• * / v2/certificates • * / v2/certificates/{certificate_id}
Sectigo	• * /cert-manager/api/ssl/v1 • * /cert-manager/api/ssl/v1/collect/{certificate_id}/pem

In Zertifikatsbestand-Management Version 1.1.7 stehen folgende Muster zur Verfügung:

- GoDaddy
- DigitCert

In Zertifikatsbestand-Management Version 1.2.0 stehen folgende Muster zur Verfügung:

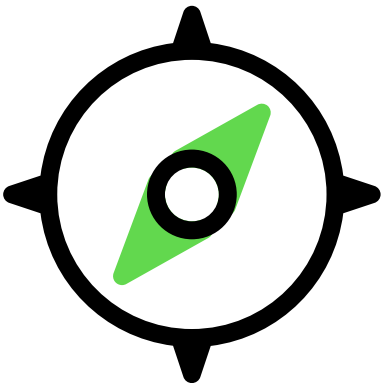
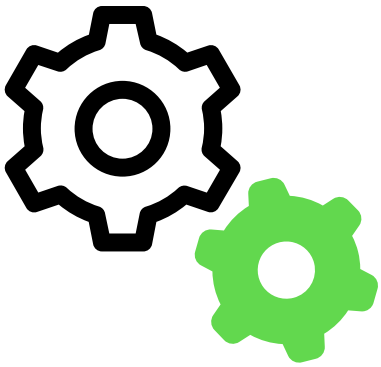
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Entrust
- Sectigo

Umgebung für die automatisierte Zertifikatverwaltung

Automated Certificate Management Environment (ACME) ist ein Protokoll zur Automatisierung der Verwaltung von SSL/TLS-Zertifikaten.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Erfahren Sie mehr über ACME und die damit verbundenen Vorteile.	Richten Sie ein, und konfigurieren Sie ACME.	Verwenden Sie ACME, um die Interaktion zwischen einer -Zertifizierungsstelle und einem Server zu automatisieren.

ACME erkunden

Die Automated Certificate Management Environment (ACME) ist ein Kommunikationsprotokoll, das die Interaktion zwischen einer Zertifizierungsstelle (Certificate Authority, CA) und einem Server automatisiert. Optimiert die Prozesse des Anforderns, Erneuerns und Widerrufens von SSL/TLS-Zertifikaten.

Übersicht überACME

ACME verwendet Nachrichten im JSON-Format, die über eine sichere HTTPS-Verbindung übertragen werden. Diese Kommunikation ermöglicht eine automatisierte Verwaltung des Zertifikatlebenszyklus, wodurch manuelle Eingriffe und das Fehlerrisiko reduziert werden.

ACME ist ein weit verbreiteter Standard, der von Administratoren der Public Key-Infrastruktur, Brancheninhabern, Anwendern der Zertifikatverwaltung, Administratoren, Kontoinhabern und Teammanagern verwendet wird.

ACME -Vorteile

Beim Anfordern, Verlängern oder Widerrufen von SSL/TLS-Zertifikaten bietet ACME erhebliche Vorteile:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Es automatisiert Aufgaben im Zusammenhang mit der Zertifikatverwaltung und reduziert so den Verwaltungsaufwand für IT-Teams.
- Dadurch wird verifiziert, ob die Zertifikate gültig und aktuell sind.
- Es macht manuelle Aufgaben für die Zertifikatverwaltung überflüssig, wodurch die Gesamtkosten reduziert werden.

Konfigurieren von ACME

Die Konfiguration der Automated Certificate Management Environment (ACME) hilft bei der automatischen Konfiguration der SSL/TLS-Zertifikate für Webserver, erhöht die Sicherheit und vereinfacht die Administration.

Erstellen Sie die Anmeldeinformationen für die ACME-Zertifizierungsstelle

Erstellen Sie ACME-Anmeldeinformationen auf der Website oder API der ACME-Zertifizierungsstelle, die von Ihrer ACME-Client-Software für die Interaktion mit der ACME-Zertifizierungsstelle (CA) verwendet werden sollen, um Zertifikate anzufordern, zu verlängern oder zu widerrufen.

Vorbereitungen

Erforderliche Rolle: pki_admin oder admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Anmeldeinformationen**.
2. Wählen Sie **Neu**.
3. Im Feld **Welche Art von Anmeldeinformationen möchten Sie erstellen?** Wählen Sie auf der Seite **Anmeldeinformationen für Zertifikatverwaltung**aus.
4. Füllen Sie die Felder des Formulars aus.

Formular für Anmeldeinformationen für die Zertifikatverwaltung

Feld	Beschreibung
Name	Name für die Anmeldeinformation
Anmeldeinformationsalias	Anmeldeinformationsalias, der mit den CA-Anmeldeinformationen verknüpft wird.
CA-Typ	Typ der Zertifizierungsstelle (z. B. Let's Encrypt oder Entrust).
ACME	Option zum Aktivieren des ACME-Flows für den Entrust CA-Typ. **Hinweis:** Für den CA-Typ **Let's Encrypt**ist diese Option standardmäßig ausgewählt.
Privater Schlüssel	Erstellen Sie einen beliebigen privaten Schlüssel, oder generieren Sie ein Konto mit „Let's Encrypt“ oder „Entrust“, und geben Sie einen privaten Schlüssel mit dem Schlüsseltyp „RSA“ oder „ECDSA“ an.
Tastentyp	Verschlüsselungsalgorithmus für den privaten Schlüssel (z. B. RSA oder ECDSA).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schlüssel-ID	Wird für die Account-Bindung verwendet und von der Zertifizierungsstelle bereitgestellt. **Hinweis:** Anwendbar für CA-**Typentrust**.
MAC-Schlüssel	Wird für die Account-Bindung verwendet und von der Zertifizierungsstelle bereitgestellt. **Hinweis:** Anwendbar für CA-**Typentrust**.

5. Wählen Sie **Aktualisieren**.

Richten Sie die Weiterleitungsrichtlinie für ACME ein

Richten Sie eine Weiterleitungsrichtlinie ein, um eine Automated Certificate Management Environment (ACME) einzurichten. Dabei wird eine Richtlinie basierend auf Faktoren wie Zertifizierungsstelle (Certificate Authority, CA), Umgebung und anderen Funktionen erstellt, um eine effiziente SSL/TLS-Zertifikatverwaltung sicherzustellen.

Vorbereitungen
Erforderliche Rolle: pki_admin, flow_designer, action_designer oder admin

Warum und wann dieser Vorgang ausgeführt wird
Doppelte Zertifikatanforderungen sind nicht zulässig. Sie können diese Einstellung jedoch überschreiben, indem Sie das Kontrollkästchen „Allow duplicate requests“ (Duplizierte Anforderungen zulassen) aktivieren. Eine Zertifikatanforderung gilt als Duplikat, wenn eine andere Zertifikataufgabe mit demselben Domänennamen noch ausgeführt wird.

Die Routing-Richtlinie entscheidet, welche Zertifizierungsstelle für Zertifikatvorgänge kontaktiert werden muss. Sie enthält die Attribute für die Zertifizierungsstelle, deren URL, Anmeldeinformationen, Genehmigungsgruppe, Zuweisungsgruppe und CSR. Die Routing-Richtlinie löst den Flow zum Anfordern von Zertifikaten für bestimmte Zertifizierungsstellen aus.

Prozedur

1. Navigieren zu **Alle** > **Zertifikatverwaltung** > **Richtlinien für Zertifikatweiterleitung**.
2. Wählen Sie **Neu**.
3. Füllen Sie im Formular **„Zertifikatweiterleitungsrichtlinie“** die Felder aus.

   Eine Beschreibung der Feldwerte finden Sie unter Formular „Certificate Routing Policy“ (Richtlinie für Zertifikatweiterleitung)..
4. Wählen Sie **Aktualisieren**.

Formular „Certificate Routing Policy“ (Richtlinie für Zertifikatweiterleitung).

Füllen Sie das Formular für die Zertifikatweiterleitungsrichtlinie aus, um die Weiterleitungsrichtlinie für ACME einzurichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für die Zertifikatweiterleitung

Feld	Beschreibung
Name	Name der Weiterleitungsrichtlinie.
Zertifizierungsstelle	CA, die zum Erstellen eines neuen Zertifikats oder zum Verlängern oder Widerrufen von Zertifikaten verwendet wird. Die unterstützten CAs basierend auf Ihren Anmeldeinformationen sind: • Lassen Sie uns verschlüsseln • Entrust
Zuweisungsgruppe	Gruppe, der eine manuelle Zertifikataufgabe zugewiesen ist.
DNS-Abfrageaktion	Flow Designer-Option zum automatischen Auflösen von DNS-Abfragen (z. B. Basisskript – **ACME DNS-Abfrage – GoDdy**). **Hinweis:** Sie können auch eine neue Aktion erstellen, die dem Basisskript ähnelt, um jeden anderen DNS-Anbieter zu unterstützen. Die Rolle „flow_designer“ oder „action_designer“ ist für diese Aktion erforderlich. Wenn **„Keine“** ausgewählt ist, werden die neuen oder verlängerten Zertifikate über den manuellen Flow der DNS-Abfrage von ACME durchgeführt.
Anmeldeinformationsalias	Mit den CA-Anmeldeinformationen verknüpfter Anmeldeinformationsalias.
Zweck des Zertifikats	Gibt an, ob die Zertifikatanforderung für einen internen oder externen Zweck erfolgt.
Aufgabengenehmigungsgruppe	Gruppe, der die Aufgabengenehmigung zugewiesen ist.
DNS-Aufgabenzuweisungsgruppe	Gruppe, der die DNS-Abfrage für diese Aufgabe zugewiesen ist.
MID-Server	MID-Server für Zertifikataktionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für die Zertifikatweiterleitung (Fortsetzung)

Feld	Beschreibung
Hinweis: Die Felder **Organisation**, **Organisationseinheit**, **Ort**, **Bundesland**, **Land**und **E-Mail-Adresse** akzeptieren durch Kommas getrennte Werte. Die Felder **Allgemeiner Antragstellername** und **Alternativer Antragstellername** akzeptieren reguläre Ausdrücke. Das Format des regulären Ausdrucks weist die folgenden Einschränkungen auf: • Darf keine Kommas enthalten. • Darf nicht mit einem Schrägstrich (/) beginnen oder enden.	

Verwenden von ACME

Verwenden Sie die Automated Certificate Management Environment (ACME), um SSL/TLS-Zertifikate anzufordern, zu verlängern oder zu widerrufen.

ACME bietet zwei Optionen:

- Manueller Flow der DNS-Abfrage von ACME

  Der Benutzer, der die DNS-Abfragen selbst durchführt.

- Automatisierter ACME-Flow der DNS-Abfrage

  Die in der Weiterleitungsrichtlinie ausgewählte DNS-Abfrageaktion fügt den DNS-Abfragedatensatz automatisch den DNS-Datensätzen der Domäne hinzu.

Führen Sie die folgenden Aufgaben aus, um mit der Verwendung von ACME zu beginnen:

- Fordern Sie ein neues Zertifikat mit dem manuellen ACME-Flow der DNS-Abfrage an
- Fordern Sie ein neues Zertifikat mit dem automatisierten ACME-Flow der DNS-Abfrage an
- Verlängern Sie das Zertifikat mit dem manuellen ACME-Flow der DNS-Abfrage
- Verlängern Sie das Zertifikat mit dem automatisierten ACME-Flow der DNS-Abfrage
- Widerrufen Sie das Zertifikat mit dem automatisierten ACME-Flow

Fordern Sie ein neues Zertifikat mit dem manuellen ACME-Flow der DNS-Abfrage an

Fordern Sie ein neues Zertifikat an, und rufen Sie die Zertifikate für eine Anwendung automatisch mit dem manuellen Flow der DNS-Abfrage von ACME ab.

Vorbereitungen

- Der Zertifikatverwaltungskatalog muss aktiviert sein.
- Es muss eine Weiterleitungsrichtlinie ohne DNS-Abfrageaktion vorhanden sein.

Erforderliche Rolle: Zertifikatanforderer, PKI-Administrator, PKI-Benutzer oder Administrator

Hinweis:

Die anfordernde Person des Zertifikats ist ein Anwender, der nicht über die Rolle „PKI-Administrator“ oder „PKI-Anwender“ verfügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Greifen Sie auf den automatisierten Flow zur Zertifikatanforderung zu.
   a. Navigieren zu **Alle** > **Servicekatalog**.
   b. Wählen Sie **Zertifikatverwaltung**aus.
   c. Wählen Sie **Automatisierter Flow**aus.
2. Wählen Sie **Neues Zertifikat anfordern (automatisiert)**aus.
3. Füllen Sie die Felder des Formulars aus.

Neues Zertifikat

Feld	Beschreibung
Zweck des Zertifikats	Gibt an, ob die Anforderung für ein internes oder ein externes Zertifikat gilt. Wählen Sie für CAs (z. B. Let's Encrypt) die **Option Extern**aus.
Zertifikatsignaturanforderung (CSR, Certificate Signing Request)	Zertifikatsignaturanforderung, die die Zertifikatinformationen enthält.
Gültigkeitszeitraum für Zertifikat (in Tagen)	Anzahl der Tage, die das Zertifikat gültig ist. Für „Let's Encrypt“ beträgt die maximale Gültigkeitsdauer 90 Tage.
Zertifikat-Besitzergruppe	Gruppe, für die die Zertifikataufgaben generiert werden.
Zertifikat-Besitzer	Name oder Rolle der Person, die Besitzer des Zertifikats sein wird.

Die folgenden CSR-Attribute werden basierend auf den Zertifikatinformationen von CSR abgeglichen und automatisch ausgefüllt:

- Allgemeiner Antragstellername
- Alternativer Antragstellername
- Organisation
- Organisationseinheit
- Ort/Stadt
- Provinz
- Land
- E-Mail-Adresse

4. Wählen Sie **Absenden**.
   Sobald die Anforderung übermittelt wurde, wird eine Aufgabe erstellt und eine Aktivität zugewiesen, mit der Sie die DNS-Abfrage abschließen und als abgeschlossen markieren können.
5. Wählen Sie auf der Seite **„Neue Zertifikataufgabe“** im Feld **DNS-Aufgabe** den Datensatz aus.
6. Fügen Sie auf der Seite **„DNS-Aufgabe“** einen DNS TXT-Datensatz für die angehängte DNS-Abfrage hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Kopieren Sie im Bereich **„DNS-Abfragen“** den DNS-Wert.

b. Wechseln Sie im Webbrowser zur Domäne, und fügen Sie den DNS-Wert als TXT-Datensatz hinzu.
Die Domäne kann beispielsweise sein **godaddy.com** > **thedisconow.com**.

c. Füllen Sie die anderen Pflichtfelder aus.

d. Wählen Sie **Speichern**.

Hinweis: Die meisten DNS-Updates werden innerhalb einer Stunde wirksam, die Aktualisierung kann jedoch bis zu 48 Stunden dauern.

7. Ändern Sie auf der Seite **„DNS-Aufgabe“** den Status des Datensatzes in **Abgeschlossen**.
8. Wahlweise: Überprüfen Sie, ob der DNS-Datensatz erfolgreich verbreitet wurde.
Um zu überprüfen, ob die Weitergabe erfolgreich war, verwenden Sie den Befehl *dig*.
9. Wählen Sie **Speichern**.

Ergebnisse

- Sobald die DNS-Abfrage abgeschlossen ist, sendet der automatisierte Flow die Anforderung an die Zertifizierungsstelle, um das Zertifikat zu erhalten.
- Das Zertifikat wird an die Aufgabe Neues Zertifikat angehängt.
- Der Status der Zertifikataufgabe ändert sich in Abgeschlossen.

Fordern Sie ein neues Zertifikat mit dem automatisierten ACME-Flow der DNS-Abfrage an

Fordern Sie ein neues Zertifikat an, und rufen Sie die Zertifikate für eine Anwendung mithilfe eines automatisierten Flows der DNS-Abfrage (Automated Certificate Management Environment, ACME) automatisch ab.

Vorbereitungen

Stellen Sie sicher, dass Anmeldeinformationen eingerichtet wurden.

Hinweis: Die GoDdies-Anmeldeinformationen werden mit dem Basissystem auf der Seite „Anmeldeinformationen“ bereitgestellt.

Der Zertifikatverwaltungskatalog wurde aktiviert.

Eine Weiterleitungsrichtlinie mit einer DNS-Abfrageaktion ist vorhanden.

Erforderliche Rolle: Zertifikatanforderer, PKI-Administrator, PKI-Benutzer, flow_designer, action_designer oder admin

Hinweis:

Eine anfordernde Person für das Zertifikat ist ein Anwender, der nicht über die Rolle „PKI-Administrator“ oder „PKI-Anwender“ verfügt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Greifen Sie auf den automatisierten Flow zu.
   a. Navigieren zu **Alle** > **Servicekatalog**.
   b. Wählen Sie **Zertifikatverwaltung**aus.
   c. Wählen Sie **Automatisierter Flow**aus.
2. Wählen Sie **Neues Zertifikat anfordern (automatisiert)**aus.
3. Füllen Sie die Felder des Formulars aus.

Formular „Neues Zertifikat“.

Feld	Beschreibung
Zweck des Zertifikats	Gibt an, ob die Anforderung für ein internes oder ein externes Zertifikat gilt. Wählen Sie für CAs wie Let's Encrypt die **Option Extern**aus.
Zertifikatsignaturanforderung (CSR, Certificate Signing Request)	Zertifikatsignaturanforderung, die Zertifikatinformationen enthält.
Gültigkeitszeitraum für Zertifikat (in Tagen)	Anzahl der Tage, die das Zertifikat gültig ist. Für „Let's Encrypt“ beträgt die maximale Gültigkeitsdauer 90 Tage.
Zertifikat-Besitzergruppe	Gruppe, für die die Zertifikataufgaben generiert werden.
Zertifikat-Besitzer	Name oder Rolle der Person, die Besitzer des Zertifikats sein wird.

Die folgenden CSR-Attribute werden basierend auf den Zertifikatinformationen von CSR abgeglichen und automatisch ausgefüllt:

- Allgemeiner Antragstellername
- Alternativer Antragstellername
- Organisation
- Organisationseinheit
- Ort/Stadt
- Provinz
- Land
- E-Mail-Adresse

4. Wählen Sie **Absenden**.
   Sobald die Anforderung übermittelt wurde, wird eine Aufgabe zum Abschließen der DNS-Abfrage erstellt. Die Aufgabe wird automatisch abgeschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

- Sobald die Weitergabe des DNS-Datensatzes nach zwei Minuten abgeschlossen ist, wird die DNS-Abfrage automatisch abgeschlossen, und der automatisierte Flow sendet eine Anforderung an die Zertifizierungsstelle, um das Zertifikat abzurufen.

  Administratoren können diese Dauer ändern, indem sie die Systemeigenschaft *sn_disco_certmgmt.wait_time_for_dns_record_propagation* ändern.

- Das Zertifikat wird an die Aufgabe Neues Zertifikat angehängt.
- Der Status der Anforderungszertifikataufgabe ändert sich in Abgeschlossen.

Verlängern Sie das Zertifikat mit dem manuellen ACME-Flow der DNS-Abfrage

Anforderung zum Verlängern des Zertifikats und zum automatischen Abrufen der Zertifikate für eine Anwendung mithilfe des manuellen ACME-Flows der DNS-Abfrage.

Vorbereitungen

- Der Zertifikatverwaltungskatalog muss aktiviert sein.
- Es muss eine Weiterleitungsrichtlinie ohne DNS-Abfrageaktion vorhanden sein.

Erforderliche Rolle: Zertifikatanforderer, PKI-Administrator, PKI-Benutzer oder Administrator

Hinweis:

Die anfordernde Person des Zertifikats ist ein Anwender, der nicht über die Rolle „PKI-Administrator“ oder „PKI-Anwender“ verfügt.

Prozedur

1. Greifen Sie auf den automatisierten Flow zur Zertifikatanforderung zu.
   a. Navigieren zu **Alle** > **Servicekatalog**.
   b. Wählen Sie **Zertifikatverwaltung**aus.
   c. Wählen Sie **Automatisierter Flow**aus.
2. Wählen Sie **Zertifikat verlängern (automatisiert)**aus.
3. Füllen Sie die Felder des Formulars aus.

Zertifikat verlängern

Feld	Beschreibung
Ausgestelltes Zertifikat	Zu verlängerndes Zertifikat.
Zweck des Zertifikats	Fordern Sie ein internes oder externes Zertifikat an. Wählen Sie für CAs (z. B. Let's Encrypt) die **Option Extern**aus.
Zertifikatsignaturanforderung (CSR, Certificate Signing Request)	Zertifikatsignaturanforderung, die Zertifikatinformationen enthält.
Gültigkeitszeitraum für Zertifikat (in Tagen)	Anzahl der Tage, die das Zertifikat gültig ist. Für „Let's Encrypt“ beträgt die maximale Gültigkeitsdauer 90 Tage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zertifikat-Besitzergruppe	Gruppe, für die die Zertifikataufgaben generiert werden.
Zertifikat-Besitzer	Name oder Rolle der Person, die Besitzer des Zertifikats sein wird.

Die folgenden CSR-Attribute werden basierend auf den Zertifikatinformationen von CSR abgeglichen und automatisch ausgefüllt:

- Allgemeiner Antragstellername
- Alternativer Antragstellername
- Organisation
- Organisationseinheit
- Ort/Stadt
- Provinz
- Land
- E-Mail-Adresse

4. Wählen Sie **Absenden**.
   Sobald die Anforderung übermittelt wurde, wird eine Aufgabe erstellt und eine Aktivität zugewiesen, mit der Sie die DNS-Abfrage abschließen und als abgeschlossen markieren können.
5. Wählen Sie auf der Seite **„Neue Zertifikataufgabe“** im Feld **DNS-Aufgabe** den Datensatz aus.
6. Fügen Sie auf der Seite **„DNS-Aufgabe“** einen DNS TXT-Datensatz für die angehängte DNS-Abfrage hinzu.

   a. Kopieren Sie im Bereich **„DNS-Abfragen“** den DNS-Wert.

   b. Wechseln Sie im Webbrowser zur Domäne, und fügen Sie den DNS-Wert als TXT-Datensatz hinzu.
   Die Domäne kann beispielsweise sein **godaddy.com** > **thedisconow.com**.

   c. Füllen Sie die anderen Pflichtfelder aus.

   d. Wählen Sie **Speichern**.

   Hinweis: Die meisten DNS-Updates werden innerhalb einer Stunde wirksam, die Aktualisierung kann jedoch bis zu 48 Stunden dauern.

7. Ändern Sie auf der Seite **„DNS-Aufgabe“** den Status des Datensatzes in **Abgeschlossen**.
8. Wahlweise: Überprüfen Sie, ob der DNS-Datensatz erfolgreich verbreitet wurde.
   Um zu überprüfen, ob die Weitergabe erfolgreich war, verwenden Sie den Befehl *dig*.
9. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

- Sobald die DNS-Abfrage abgeschlossen ist, sendet der automatisierte Flow die Anforderung an die Zertifizierungsstelle, um das Zertifikat zu erhalten.
- Das Zertifikat wird an die Aufgabe Neues Zertifikat angehängt.
- Der Status der Zertifikataufgabe ändert sich in Abgeschlossen.

Verlängern Sie das Zertifikat mit dem automatisierten ACME-Flow der DNS-Abfrage

Fordert die Verlängerung des Zertifikats und den automatischen Abruf der Zertifikate für eine Anwendung mithilfe eines automatisierten Flows der DNS-Abfrage (Automated Certificate Management Environment, ACME) an.

Vorbereitungen

Stellen Sie sicher, dass Anmeldeinformationen eingerichtet wurden.

Hinweis: Die GoDdies-Anmeldeinformationen werden mit dem Basissystem auf der Seite „Anmeldeinformationen“ bereitgestellt.

Der Zertifikatverwaltungskatalog wurde aktiviert.

Eine Weiterleitungsrichtlinie mit einer DNS-Abfrageaktion ist vorhanden.

Erforderliche Rolle: Zertifikatanforderer, PKI-Administrator, PKI-Benutzer, flow_designer, action_designer oder admin

Hinweis:

Eine anfordernde Person für das Zertifikat ist ein Anwender, der nicht über die Rolle „PKI-Administrator“ oder „PKI-Anwender“ verfügt.

Prozedur

1. Greifen Sie auf den automatisierten Flow zur Zertifikatverlängerung zu.
   a. Navigieren zu **Alle** > **Servicekatalog**.
   b. Wählen Sie **Zertifikatverwaltung**aus.
   c. Wählen Sie **Automatisierter Flow**aus.
2. Wählen Sie **Zertifikat verlängern (automatisiert)**aus.
3. Füllen Sie die Felder des Formulars aus.

Zertifikat verlängern

Feld	Beschreibung
Ausgestelltes Zertifikat	Zu verlängerndes Zertifikat.
Zweck des Zertifikats	Fordern Sie ein internes oder externes Zertifikat an. Wählen Sie für CAs (z. B. Let's Encrypt) die **Option Extern**aus.
Zertifikatsignaturanforderung (CSR, Certificate Signing Request)	Zertifikatsignaturanforderung, die Zertifikatinformationen enthält.
Gültigkeitszeitraum für Zertifikat (in Tagen)	Anzahl der Tage, die das Zertifikat gültig ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Für „Let's Encrypt“ beträgt die maximale Gültigkeitsdauer 90 Tage.
Zertifikat-Besitzergruppe	Gruppe, für die die Zertifikataufgaben generiert werden.
Zertifikat-Besitzer	Name oder Rolle der Person, die Besitzer des Zertifikats sein wird.

Die folgenden CSR-Attribute werden basierend auf den Zertifikatinformationen von CSR abgeglichen und automatisch ausgefüllt:

- Allgemeiner Antragstellername
- Alternativer Antragstellername
- Organisation
- Organisationseinheit
- Ort/Stadt
- Provinz
- Land
- E-Mail-Adresse

4. Wählen Sie **Absenden**.
Sobald die Anforderung übermittelt wurde, wird eine Aufgabe zum Abschließen der DNS-Abfrage erstellt. Die Aufgabe wird automatisch abgeschlossen.

Ergebnisse

- Sobald die Weitergabe des DNS-Datensatzes nach zwei Minuten abgeschlossen ist, wird die DNS-Abfrage automatisch abgeschlossen, und der automatisierte Flow sendet eine Anforderung an die Zertifizierungsstelle, um das Zertifikat abzurufen.

  Administratoren können diese Dauer ändern, indem sie die Systemeigenschaft *sn_disco_certmgmt.wait_time_for_dns_record_propagation* ändern.

- Das Zertifikat wird an die Aufgabe Neues Zertifikat angehängt.
- Der Status der Anforderungszertifikataufgabe ändert sich in Abgeschlossen.

Widerrufen Sie das Zertifikat mit dem automatisierten ACME-Flow

Fordern Sie einen Widerruf des Zertifikat für eine Anwendung an.

Vorbereitungen

Stellen Sie sicher, dass der Zertifikatverwaltungskatalog aktiviert ist und eine Weiterleitungsrichtlinie erstellt wurde.

Erforderliche Rolle: pki_admin oder admin

Prozedur

1. Greifen Sie auf den automatisierten Flow zur Zertifikatanforderung zu.
   a. Navigieren zu **Alle** > **Servicekatalog**.
   b. Wählen Sie **Zertifikatverwaltung**aus.
   c. Wählen Sie **Automatisierter Flow**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie **Zertifikat widerrufen (automatisiert)**aus.
3. Entsperren Sie das Feld **Ausgestelltes Zertifikat**.
4. Wählen Sie das Symbol „Nachschlagen mit Liste“ ( ) und anschließend das Zertifikat, das Sie widerrufen möchten.
   Sie können mehr als ein Zertifikat auswählen.
5. Geben Sie einen ausreichenden Grund für den Widerruf des Zertifikats an.
6. Platzieren Sie den Widerrufauftrag, indem Sie **Absenden**wählen.
7. Wählen Sie im Bestätigungsdialogfeld **OK**aus.

Ergebnisse
Es wird automatisch eine Aufgabe erstellt, die den Sperrvorgang auslöst. Sobald der Vorgang abgeschlossen ist, ändert sich der Status des Zertifikats in Widerrufen.

Service-Mapping

Die Anwendung ServiceNow® Service-Mapping erkennt alle Anwendungsservices in Ihrer Organisation und erstellt eine umfassende Zuordnung aller in diesen Anwendungsservices verwendeten Geräte, Anwendungen und Konfigurationsprofile.

Service-Mapping ist als separates Abonnement erhältlich und erfordert eine Aktivierung durch Service-Mapping-Personal.

Mit serviceorientierten Vorgängen Kontrolle gewinnen

Service-Mapping ermöglicht IT-Abteilungen von Unternehmen, Organisationen und Cloud-Unternehmen, die Platform-as-a-Service bereitstellen, die Erstellung einer serviceorientierten Ansicht der Infrastruktur.

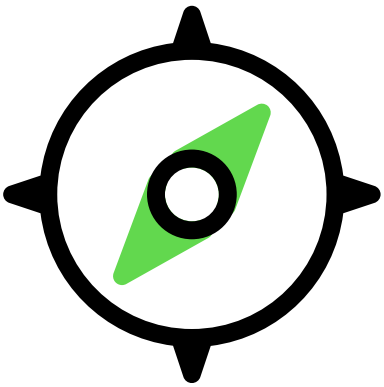
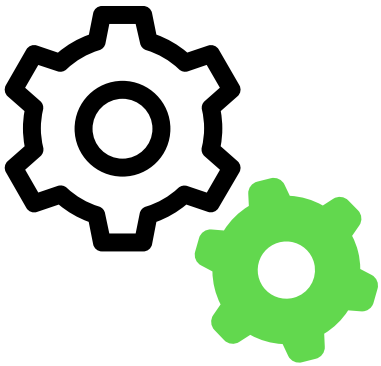
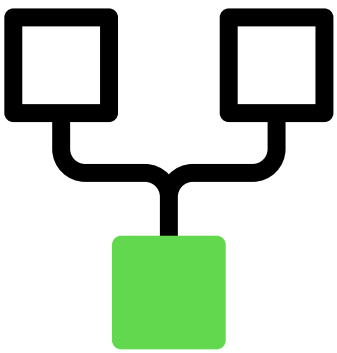
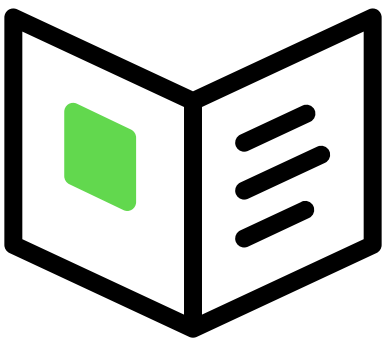
Amortisierungszeit schnell erreichen

Verkürzen Sie den Zuordnungsprozess, und optimieren Sie die Genauigkeit mit sofort einsatzbereiten Optionen. Mit Service-Mapping werden verschiedene Methoden zum Sammeln von Informationen über Konfigurationselemente (Configuration Items, CIs) und über deren Organisation in Anwendungsservices bereitgestellt. Die folgenden Zuordnungsmethoden sind verfügbar: musterbasiert, tagbasiert, datenverkehrsbasiert und erkennungsbasiert auf Basis von Predictive Intelligence.

Multi-Cloud-Strategie umsetzen

Ordnen Sie Services mit hoher Genauigkeit über dynamische cloudbasierte Provider hinweg zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen  Erfahren Sie mehr über die verschiedenen Methoden zur Zuordnung von Anwendungsservices.	Konfigurieren  Planen und konfigurieren Sie Ihre Implementierung.	
Verwenden  Überprüfen Sie die Zuordnung von Anwendungsservices für Analyse und Wartung.	Referenz  Rufen Sie Details zu -Komponenten wie Rollen, Tabellen und Eigenschaften ab.	

Service-Mapping erkunden

Service-Mapping erkennt alle Serviceinstanzen in Ihrer Organisation und erstellt eine umfassende Zuordnung aller Geräte, Anwendungen und Konfigurationsprofile, die in diesen Serviceinstanzen verwendet werden.

Video: Übersicht über Service Mapping

Dieses Video bietet einen Überblick über Service-Mapping auf der Seite Now Platform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping – Benutzer

Service-Mapping ermöglicht IT-Abteilungen von Unternehmen, Organisationen und Cloud-Unternehmen, die Platform-as-a-Service bereitstellen, die Erstellung einer serviceorientierten Ansicht der Infrastruktur.

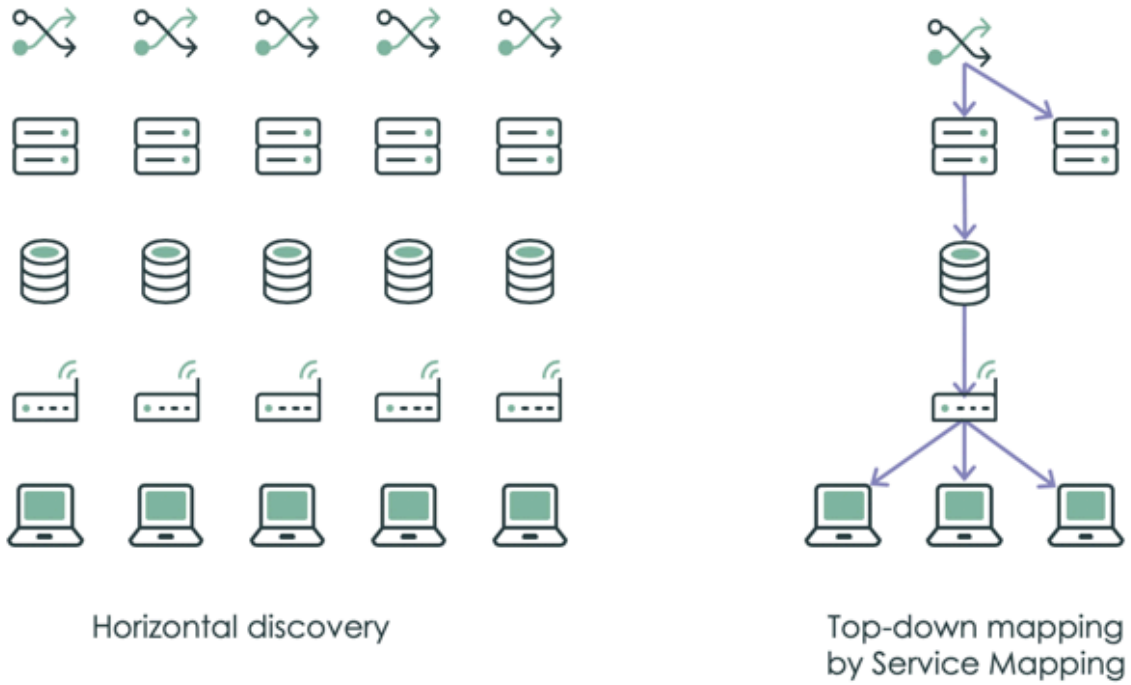
Wie verwenden Sie Service-Mapping?

Eine Serviceinstanz stellt eine Reihe verbundener Anwendungen und Hosts dar, die zur Bereitstellung eines Service für eine Organisation konfiguriert sind. Serviceinstanzen können intern sein, wie ein E-Mail-System einer Organisation, oder auf Kunden ausgerichtet sein, wie die Website einer Organisation. Zum Erstellen von Finanzberichten über eine webbasierte Anwendung sind beispielsweise Computer, Webserver, Anwendungsserver, Datenbanken, Middleware und Netzwerkinfrastruktur erforderlich. Diese Anwendungen und Hosts sind alle so konfiguriert, dass sie den Dienst der Finanzberichterstattung anbieten.

Normalerweise erstellen und verwalten IT-Abteilungen einen Bestand, der Geräte und Anwendungen als eigenständige, unabhängige Objekte behandelt. Verbindungen zwischen Geräten und Anwendungen werden nicht berücksichtigt. Dies wird in der Regel als horizontale Erkennung bezeichnet. Die größte Herausforderung von IT-Abteilungen wird durch diese Methode nicht bewältigt, die darin besteht, die Verbindungen und Abhängigkeiten zwischen den einzelnen Objekten zu verstehen.

Service-Mapping Ordnet Abhängigkeiten basierend auf einer Verbindung zwischen Geräten und Anwendungen zu. Diese Methode wird als Zuordnung von oben nach unten bezeichnet. Mithilfe der Top Down-Zuordnung können Sie sofort die Auswirkungen eines problematischen Objekts auf den Rest des Serviceinstanzbetriebs erkennen.

Vergleich der Ergebnisse der horizontalen Zuordnung und der Zuordnung von oben nach unten



Serviceinstanz-Zuordnungen zeigen Infrastrukturobjekte und semantische Verbindungen zwischen ihnen. Service-Mapping generiert für Service-Zuordnungen regelmäßig neu, um sie aktuell und relevant zu halten. Alle fehlerhaften Objekte werden zusammen mit den betroffenen Geräten und Anwendungen angezeigt und geben so einen Überblick über den für Service-Status.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie funktioniert Service-Mapping?

Service-Mapping kann unterschiedliche Methoden zum Erstellen von Anwendungsservices bereitstellen. Die Hauptmethode von Service-Mapping zum Erkennen und Zuordnen von Geräten und Anwendungen ist die Verwendung von Mustern. Ein Muster ist eine Folge von Vorgängen, die zum Erkennen der Attribute von Geräten und Anwendungen und deren ausgehenden Verbindungen dienen. Wenn Ihre Organisation Tags für die Asset-Verwaltung verwendet, können die Tags zum Zuordnen von Serviceinstanzen verwendet werden. Service-Mapping kann Geräte und Anwendungen auch durch Verfolgen der Datenverkehrsverbindungen zwischen ihnen erkennen. Diese Methode wird als datenverkehrsbasierte Zuordnung bezeichnet. Weitere Informationen finden Sie unter Richtige Methode zur Erkennung und Zuordnung von Anwendungsservices auswählen.

Was Sie wissen müssen, bevor Sie beginnen

Sie können Service-Mapping nur verwenden, wenn das Produkt Discovery aktiviert und eingerichtet ist.

Sie müssen Benutzer definieren und Anmeldeinformationen konfigurieren, um Service-Mapping und Discovery Zugriff auf Anwendungen und Geräte in Ihrem Unternehmensnetzwerk zu ermöglichen. Weitere Informationen finden Sie unter Service-Mapping konfigurieren.

Service-Mapping auf Now Platform

Service-Mapping ist auf Discovery und MID-Server, angewiesen, um Geräte und Anwendungen zu erkennen. Service-Mapping nutzt Ergebnisse der horizontalen Erkennung von Discovery. MID-Server erleichtert die Kommunikation zwischen Service-Mapping und erkannten Geräten und Anwendungen.

Von Service-Mapping gesammelte und organisierte Daten sind in Ereignismanagement, Abhängigkeitsansichten und Anwendungs-Portfoliomanagement (APM) sichtbar. Mit Ereignismanagement können Sie Events anzeigen, um Aktionen zur Wiederherstellung der Anwendungsservices Ihrer Organisation durchzuführen. Abhängigkeitsansichten zeigt Beziehungen zwischen Geräten und Anwendungen im Kontext der Anwendungsservices an, zu denen sie gehören. Wenn Service-Mapping in APM integriert ist, bietet es Informationen zu Komponenten, aus denen eine Geschäftsanwendung besteht, und hilft APM-Benutzern, die Leistung von Geschäftsanwendungen zu überwachen.

Service-Mapping unterstützt Domänentrennung. Wenn in Ihrer Now Platform Domänentrennung eingesetzt wird, können Administratoren und Benutzer nur Anwendungsservices sehen und verwalten, die zu ihrer eigenen Domäne gehören.

Eine Liste der Service-Mapping Plugin-Abhängigkeiten finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Transparenz.

Zugehörige Informationen

- Anwendungsservices
- Ereignismanagement
- Abhängigkeitsansichten

Richtige Methode zur Erkennung und Zuordnung von Anwendungsservices auswählen

Service-Mapping stellt verschiedene Methoden zum Sammeln von Informationen über Konfigurationselemente (CIs) und zu deren Organisation in Anwendungsservices bereit. Die folgenden Zuordnungsmethoden sind verfügbar: musterbasiert, tagbasiert, datenverkehrsbasiert und erkennungsbasiert auf Basis von Predictive Intelligence. Erfahren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie mehr über die Zuordnungsmethoden, um die Methoden auszuwählen, die den Anforderungen Ihres Unternehmens am besten entsprechen.

Zuordnungsmethode	Beschreibung	Vorteile	Nachteile
Empfehlungen für automatisierte Services	Predictive Intelligence wertet Verbindungen zwischen Anwendungsfingerabdrücken, CIs und Prozessen aus und bewertet ihre Relevanz. Service-Mapping verwendet diese Informationen, um Verbindungen basierend auf Verbindungsregeln zu erstellen. Außerdem werden Verbindungsvorschläge für Server und Lastenausgleichsmodule generiert, damit Sie entscheiden können, welche Verbindungen den Serviceinstanzen hinzugefügt oder daraus entfernt werden sollen.	Auf Basis von Verbindungsregeln fügt Service-Mapping automatisch CI-Verbindungen und CIs hinzu, zu denen sie führen. Sie können die Standardverbindungsregeln ändern oder eigene erstellen, um diese Erkennungsmethode zu verbessern. Die Erkennung auf Basis von Predictive Intelligence ist für die Zuordnung mehrerer Anwendungsservices effektiv.	Wenn Sie die Erkennung auf Basis von Predictive Intelligence verwenden, um TCP-Verbindungen und -Prozesse zu identifizieren, stellen Sie sie in großen lokalen Bereitstellungen bereit. Predictive Intelligence ist eine ML-Lösung und erfordert Schulung. Um mit dieser Erkennungsmethode die besten Ergebnisse zu erzielen, müssen Sie die Erkennung wiederholt ausführen. Service-Mapping kann fälschlicherweise dynamische Verbindungen hinzufügen oder entfernen.
Musterbasierte Erkennung	Service-Mapping verwendet Muster zum Erkennen und Zuordnen von CIs. Ein Muster ist eine Folge von Befehlen, deren Zweck darin besteht, Attribute eines CI und seiner ausgehenden Verbindungen zu ermitteln. Ein typisches Service-Mapping-Muster besteht aus separaten Algorithmen zum Identifizieren von CIs und Ermitteln von CI-Verbindungen.	Die musterbasierte Discovery erstellt präzise und vollständige Serviceinstanzen, die zuverlässig eine serviceorientierte Sicht auf die IT-Infrastruktur Ihrer Organisation darstellen.	Die musterbasierte Zuordnung erfordert die Konfiguration von Anmeldeinformationen, Benutzern und Benutzerberechtigungen, damit Service-Mapping auf Anwendungen im privaten Netzwerk Ihrer Organisation zugreifen kann. Dieser Prozess kann zeitaufwändig und mühsam sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungsmethode	Beschreibung	Vorteile	Nachteile
Tagbasierte Erkennung	Wenn Ihre Organisation Tags für die Asset-Verwaltung verwendet, können die Tags zum Zuordnen von Serviceinstanzen verwendet werden. Discovery und Cloud Provisioning and Governance erkennen mit CIs verknüpfte Tags und füllen CMDB mit diesen Daten. Service-Mapping verwendet die Tag-bezogenen Daten aus CMDB zum Zuordnen von Services.	Tags eignen sich zur effektiven Zuordnung mehrerer Anwendungsservices.	Tagbasierte Serviceinstanzen enthalten möglicherweise keine relevanten CIs, wenn diesen CIs nicht die richtigen Tags zugewiesen sind.
Datenverkehrsbasierte Erkennung	Service-Mapping kann Konfigurationselemente (CIs) anhand ihrer datenverkehrsbasierten Verbindungen erkennen und zuordnen. Diese Methode wird als datenverkehrsbasierte Zuordnung bezeichnet und ergänzt die musterbasierte Zuordnung. Je nach Konfiguration variiert das Systemverhalten hinsichtlich der datenverkehrsbasierten Erkennung.	Die Verwendung der datenverkehrsbasierten Erkennung ist wie das Auswerfen eines feineren Netzes, mit dem von Service Mapping sogar die CIs gefunden werden, die mithilfe von Mustern nicht erkannt wurden.	Die datenverkehrsbasierte Erkennung führt zwar zu einer inklusiveren Zuordnung, kann aber auch zur Zuordnung vieler redundanter CIs führen, die den Betrieb des Anwendungsservice nicht beeinflussen. Dadurch kann ein Anwendungsservice durch irrelevante CIs unübersichtlich werden. Sie sollten die datenverkehrsbasierte Erkennung in der Anfangsphase der Erkennung eines Anwendungsservice verwenden und sie deaktivieren, sobald Erkennung und Feinabstimmung des Anwendungsservice abgeschlossen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping mit Agent Client Collector

Agent Client Collector ermöglicht die Erkennung und Zuordnung von Anwendungsservices, ohne dass Sie Anmeldeinformationen für MID-Servereinrichten müssen.

Mit Agent Client Collectorkönnen Sie sowohl von oben nach unten als auch auf maschinellem Lernen basierende Service-Mapping bereitstellen und profitieren von einem vereinfachten Ansatz für die Zuordnung von Anwendungsservices.

Informationen zum Konfigurieren von Service-Mapping für die Verwendung mit Agent Client Collectorfinden Sie unter Agent Client Collector zur Verwendung mit Service-Mappingkonfigurieren.

CMDB-basierte Zuordnung

Mit den in Configuration Management Database (CMDB)gespeicherten Daten können Sie eine Top Down-Discovery ausführen und die Anwendungsservices Ihres Unternehmens zuordnen, ohne auf ein MID-Serverzugreifen zu müssen.

Die Top Down-Discovery beginnt mit einer IP-Adresse und ruft den zugehörigen Host ab. Anschließend wird versucht, ein verfügbares MID-Serverzu finden. Wenn kein MID-Server verfügbar ist und die CMDB-basierte Zuordnung aktiv ist, wird sie initiiert. Diese Funktion überwacht den eingehenden Datenverkehr, um den Zielprozess zu ermitteln, der unter einer identifizierten IP-Adresse ausgeführt wird, und sucht nach einer damit verknüpften Anwendung. Die Anwendung wird dann als Knoten in der Servicezuordnung zugeordnet.

Wenn eine Anwendung nicht identifiziert wird, verwendet die CMDB-basierte Zuordnung die Logik von Application Dependency Mapping (ADM), um eine Anwendung zu klassifizieren und zu erstellen, die mit dem Zielprozess innerhalb von CMDBverknüpft ist.

Wenn ADM die Anwendung nicht klassifizieren kann, wird in der Tabelle „Anwendung“ [cmdb_ci_appl] in CMDBeine einfache Anwendung erstellt. Weitere Informationen finden Sie unter Application Dependency Mapping (ADM) für Discovery.

Informationen zur Konfiguration Service-Mapping von für die CMDB-basierte Zuordnung finden Sie unter Service-Mapping für die Verwendung mit Configuration Management Database (CMDB)konfigurieren.

Empfehlungen für automatisierte Services

Empfehlungen für automatisierte Services vereinfacht die Verarbeitung der Zuordnung von Anwendungsservices oder das Hinzufügen zu einem vorhandenen Service durch Bereitstellen von Anwendungsservice-Kandidaten mithilfe von maschinellem Lernen. Zugeordnete Services stellen wichtige Informationen bereit, mit denen Sie datengesteuerte Entscheidungen treffen, Services priorisieren und auf Situationen reagieren können.

Mithilfe von maschinellem Lernen (ML) identifiziert Service-Mapping schnell potenzielle Anwendungsfingerabdrücke basierend auf erkannten Prozessen. Es wertet die Beziehung zwischen diesen Fingerabdrücken und den Configuration Items (CIs) aus und stellt sinnvolle Verbindungen her. Diese Verbindungen werden verwendet, um eine Anwendungsservicezuordnung zu erstellen, eine visuelle Darstellung eines Service.

Empfehlungen für automatisierte Services vereinfacht den Zuordnungsprozess weiter, indem mithilfe der ML-Informationen Einstiegspunkte berechnet werden, die effizient ermitteln, wo mit der Zuordnung eines Anwendungsservice begonnen werden soll. Außerdem wird eine Liste mit Anwendungsservice-Candidates generiert. Jeder Candidate enthält einen Einstiegspunkt sowie einen Satz zuvor identifizierter Ressourcen, die in die Servicezuordnung aufgenommen werden sollen. Sie können dann einen Kandidaten auswählen, um einen neuen Anwendungsservice zu erstellen oder ihn einem vorhandenen Service hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Fingerabdrücke

Service-Fingerabdrücke ergänzt Empfehlungen für automatisierte Services durch die Identifizierung eindeutiger, klassifizierter Komponenten identifizierter Anwendungsservice-Kandidaten. Die Darstellung dieser Komponenten erleichtert die Auswahl des am besten geeigneten vorgeschlagenen Anwendungsservice. Sie können Komponenten einer Anwendung in Ihrer tatsächlichen Umgebung anzeigen, einschließlich Details wie Produkt, Produktkategorie, Herausgeber und Beschreibung. Verwenden Sie diese Informationen, um nach bestimmten Komponenten zu suchen, die Sie erkennen möchten, oder um fundierte Entscheidungen darüber zu treffen, welche Kandidaten in Anwendungsservices umgewandelt werden sollen.

Um Service-Fingerabdrückezu verwenden, müssen Sie ITOM Content Service aus dem ServiceNow® Store herunterladen und installieren und dann ITOM Content Serviceaktivieren. Weitere Informationen finden Sie unter ITOM Content Service.

Domain Separation mit Empfehlungen für automatisierte Services

Empfehlungen für automatisierte Services unterstützt Domain Separation ab Version 1.9.0. Für lokale Instanzen wird derzeit kein Support angeboten. Wenden Sie sich an das Produktmanagement, um weitere Informationen zu erhalten.

Zugehörige Informationen

Service-Mapping erkunden

Service-Mapping Arbeitsbereich

Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich

Anwendungsservices zuordnen basierend auf Empfehlungen für automatisierte Services

Erkennung auf Basis von Predictive Intelligence

Service-Mapping verwendet von Predictive Intelligence verarbeitete Daten, um Vorschläge für datenverkehrsbasierte Verbindungen zu generieren.

Mit Predictive Intelligence generierte Verbindungsvorschläge

Predictive Intelligence wertet Verbindungen zwischen Anwendungsfingerabdrücken, CIs und Prozessen aus und bewertet ihre Relevanz. Service-Mapping verwendet diese Informationen, um Verbindungen basierend auf Verbindungsregeln zu erstellen. Außerdem werden Verbindungsvorschläge für Server und Lastenausgleichsmodule generiert, damit Sie entscheiden können, welche Verbindungen den Serviceinstanzen hinzugefügt oder daraus entfernt werden sollen. Das Konfidenzniveau gibt die Wahrscheinlichkeit an, dass diese Verbindung Teil der Serviceinstanzen ist.

- **Hoch** – Es handelt sich wahrscheinlich um eine Verbindung zu einer internen Komponente, die nur von dieser Komponente oder Anwendung verwendet wird.
- **Mittel** – Es handelt sich wahrscheinlich um eine Verbindung zu einer Middleware-Komponente, die von mehreren Services verwendet wird, z. B. IBM MQ oder Oracle WebLogic Server.
- **Niedrig** – Es handelt sich wahrscheinlich um eine Verbindung zu einer Anwendung, die auf zahlreichen Servern im Unternehmen bereitgestellt wird, normalerweise zu Überwachungszwecken. Zum Beispiel Tivoli Enterprise Monitoring Agents oder MID-Server.
- **Sehr niedrig** – Es handelt sich wahrscheinlich um eine Verbindung zu einer zentralen Anwendung, die von der gesamten Organisation verwendet wird, z. B. Microsoft Active Directory oder Okta.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Discovery basierend auf Predictive Intelligence aktiviert ist, fügt Service-Mapping basierend auf Verbindungsregeln automatisch Verbindungen zu Serviceinstanzen hinzu. Service-Mapping generiert diese Vorschläge basierend auf datenverkehrsbezogenen Daten aus der Configuration Management Database (CMDB) und der Analyse von Anwendungsfingerabdrücken, CIs und Prozessen durch Predictive Intelligence.

Verbindungsregeln auf Basis von Verbindungsvorschlägen

Verbindungsvorschläge verbessern die mit Predictive Intelligence generierten Verbindungsvorschläge. Jede Regel enthält eine Bedingung, die einen Aspekt einer datenverkehrsbasierten Verbindung beschreibt. Die in Bedingungen verfügbaren Felder stammen aus der Tabelle „Verbindungsvorschlag“ [sa_ml_connection_suggestion], die bei einer Erkennung von oben nach unten (einer sog. Top-Down-Discovery) gefüllt wird. Sie können Ihre Regeln direkt auf Verbindungsvorschlägen basieren. Erstellen Sie beispielsweise eine Regel für jede Verbindung mit dem Konfidenzniveau „Hoch“. Wenn Sie wissen, welche CIs Teil der Serviceinstanzen sein müssen, können Sie alternativ Felder auswählen, die auf diese CIs verweisen.

Wenn Service-Mapping eine Verbindung basierend auf Verbindungsregeln hinzufügt, werden die folgenden Aktionen ausgeführt:

1. Die Verbindungsregel wird dem Verbindungsvorschlag zugeordnet.
2. Das Attribut für *Decision* für den Verbindungsvorschlag wird in `Durch Regel hinzugefügt` geändert.
3. Während der erneuten Erkennung von Services wird eine Ebene der tatsächlichen CI-Verbindungen zu relevanten Anwendungsservices hinzugefügt.

Jedes Mal, wenn Anwendungsservices neu erkannt werden, fügt Service-Mapping nur eine Ebene von CI-Verbindungen hinzu. Sie können die Häufigkeit in Ihren Erkennungszeitplänen ändern, um die Zuordnung der Anwendungsservices mithilfe von Verbindungsregeln abzuschließen.

Service-Mapping wertet nur aktive Verbindungsregeln und nur für Verbindungsvorschläge aus, die das Entscheidungsattribut „Unentschieden“ besitzen. Das System wendet die Regeln mit dem folgenden Algorithmus an:

1. Service-Mapping überprüft lokale Regeln auf eine CI-Verbindung. Wenn mehrere Regeln für dieselbe CI-Verbindung relevant sind, verwendet Service-Mapping zur Bestimmung der Reihenfolge das entsprechende Attribut und wertet die Regeln vom niedrigsten zum höchsten Reihenfolgewert aus. Standardmäßig überprüft Service-Mapping nur 20 lokale Regeln.
2. Wenn ein Verbindungsvorschlag mit der Verbindungsregelbedingung übereinstimmt, fügt Service-Mapping diese Verbindung dem entsprechenden Anwendungsservice hinzu.
3. Wenn Service-Mapping keine Übereinstimmung mit lokalen Regeln findet, beginnt das System, globale Regeln in aufsteigender Reihenfolge anhand des Reihenfolgeattributs auszuwerten und anzuwenden. Standardmäßig überprüft das System nur 20 globale Regeln.
4. Wenn ein Verbindungsvorschlag mit der Regelbedingung übereinstimmt, fügt das System ihn den entsprechenden Anwendungsservices hinzu. Wenn eine Regel so konfiguriert ist, dass vorgeschlagene Verbindungen von bestimmten Services ausgeschlossen werden, wendet das System diese Regel nicht auf diese Services an.
5. Jedes Mal, wenn Service-Mapping Anwendungsservices des manuellen oder erkannten Typs neu erkennt, validiert es hinzugefügte datenverkehrsbasierte Verbindungen automatisch anhand der aktiven Verbindungsregeln. Auf diese Weise stellt das System

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sicher, dass Anwendungsservices nur relevante Verbindungen basierend auf den aktuellen und aktiven Verbindungsregeln enthalten.

6. Wenn eine Regel nicht mehr gültig ist, ändert Service-Mapping das Entscheidungsattribut für den entsprechenden Verbindungsvorschlag in „Unentschieden“. Service-Mapping entfernt auch die Zuordnung zwischen der Verbindungsregel und dem Verbindungsvorschlag. Sofern Service-Mapping keine andere Verbindungsregel auf CI-Verbindungen anwenden kann, die irrelevant wurden, entfernt Service-Mapping sie aus den Anwendungsservices.

Bei Bedarf können Sie die Anzahl der lokalen oder globalen Verbindungsregeln ändern, die das System im Algorithmus verwendet (siehe Mit Service Mapping installierte Eigenschaften).

Erkennung auf Basis von Predictive Intelligence aktivieren

Die Erkennung auf Basis von Predictive Intelligence funktioniert auf Produktebene. Gesteuert wird diese Funktion mit der Eigenschaft *sa_ml.connection_suggestions.active*. Wenn die datenverkehrsbasierte Erkennung in Ihrer Bereitstellung vor Release Quebec aktiviert war und Sie damit mindestens einen Anwendungsservice erkannt haben, ist die Erkennung auf Basis von Predictive Intelligence standardmäßig deaktiviert.

Zugehörige Informationen

CIs für mehrere Anwendungsservices mithilfe von Verbindungsregeln hinzufügen

CIs für einzelne Anwendungsservices mithilfe von Verbindungsregeln hinzufügen

CIs für mehrere Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

CIs für einzelne Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

Musterbasierte Erkennung in Service-Mapping

Die musterbasierte Erkennung ist die Hauptmethode von Service-Mapping zum Sammeln von Daten über Geräte und Anwendungen, die in Anwendungsservices verwendet werden. Nachdem Service-Mapping Daten gesammelt hat, wird eine Zuordnung von Anwendungsservices erstellt und die erfassten Daten werden in CMDB gespeichert.

ServiceNow -Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Configuration Items (CIs) umfassen.

Service-Mapping verwendet Muster zum Erkennen und Zuordnen von CIs. Ein Muster ist eine Folge von Befehlen, deren Zweck darin besteht, Attribute eines CI und seiner ausgehenden Verbindungen zu ermitteln. Ein typisches Service-Mapping-Muster besteht aus zwei Arten von Algorithmen zum Identifizieren von CIs und Finden von CI-Verbindungen.

Der Ausgangspunkt eines Erkennungsprozesses ist ein Einstiegspunkt. Ein Einstiegspunkt ist ein Punkt, auf den Clients auf eine Serviceinstanz zugreifen. Um beispielsweise Ihre E-Mail-Serviceinstanz zuzuordnen, definieren Sie eine IP-Adresse oder einen Hostnamen des E-Mail-Servers als Einstiegspunkt. Der Erkennungs- und Zuordnungsprozess beginnt mit der horizontalen Erkennung durch Discovery, um den Host zu identifizieren. Nach Abschluss der Hosterkennung startet Service-Mapping die Discovery von oben nach unten, um auf diesem Host ausgeführte Anwendungen zu finden und zuzuordnen.

Service-Mapping verwendet MID Servers, um mit CIs in Ihrer Organisation zu kommunizieren. MID Servers befinden sich in Ihrem Unternehmensnetzwerk und Service-Mapping kann mit ihnen kommunizieren, ohne Firewalls zu überwinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

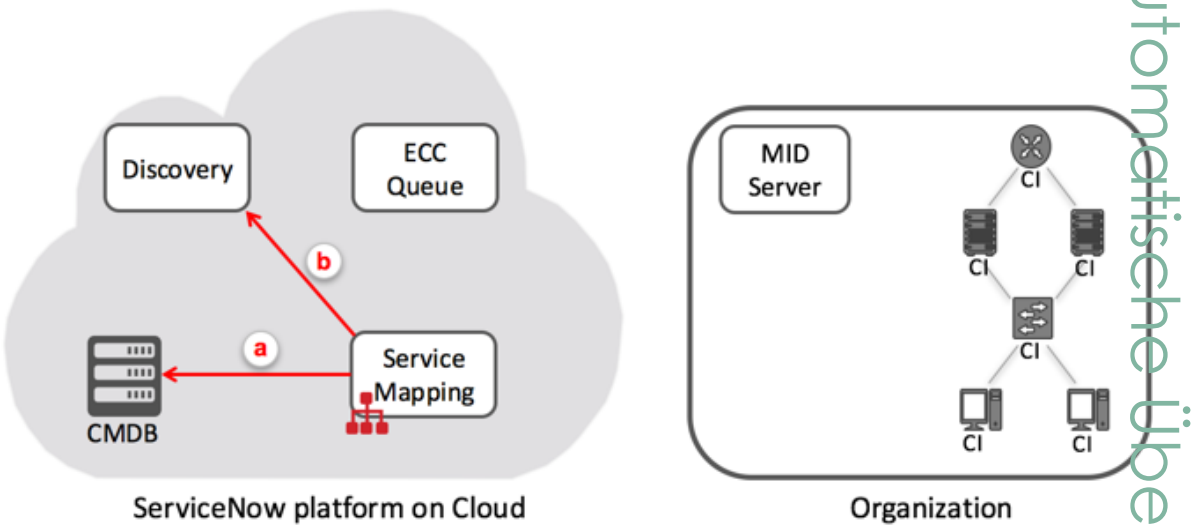
Hinweis: Mustervorgänge bieten derzeit keine Unterstützung mehrerer Sprachen. Wenn die Werte, die von Mustervorgängen zurückgegeben werden, nicht in Englisch vorliegen, können die zurückgegebenen Daten nicht richtig analysiert werden, und die Muster-Discovery schlägt fehl.

Der Erkennungs- und Zuordnungsprozess besteht aus den folgenden Interaktionen:

1. Ein Administrator definiert einen für Service mit einem Einstiegspunkt für ein Anwendungs-CI.

   Service-Mapping erstellt einen Datensatz für den neuen für Service in der Tabelle „Zugeordneter Anwendungsservice“ [cmdb_ci_service_discovered].

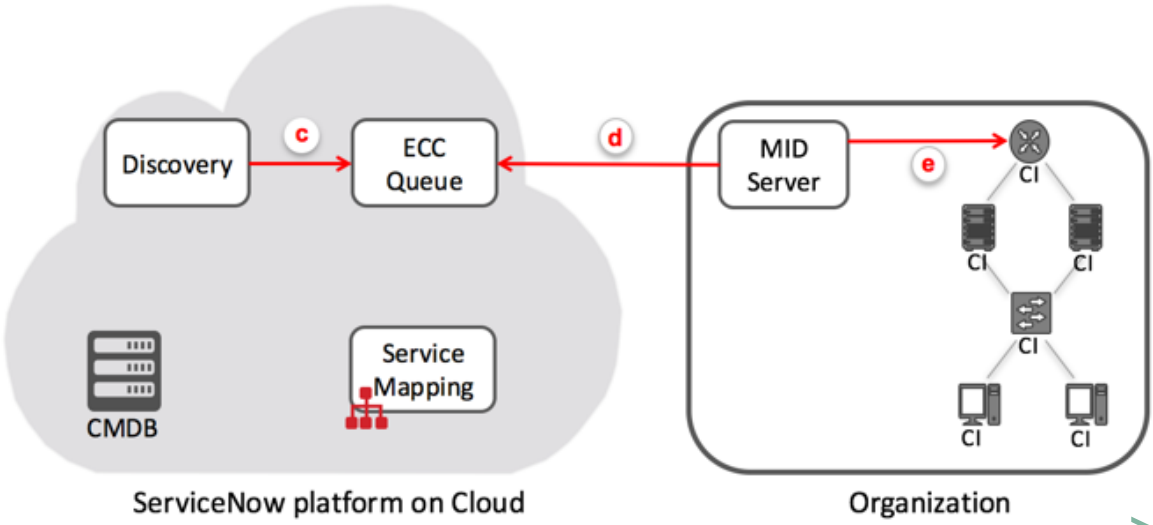
2. Das Gerät, auf dem die Anwendung gehostet wird, wird identifiziert.
   a. Service-Mapping prüft, ob das Gerät, das dieses Anwendungs-CI hostet, in der CMDB vorhanden ist .
   b. Wenn das Gerät, das diese Anwendungs-CI hostet, nicht vorhanden ist, löst Service-Mapping eine Discovery aus, um den Host zu erkennen.



   c. Discovery erstellt den ersten Satz von Probes für die Porterkennung (die sogenannten Shazzam-Probes) und platziert sie als Erkennungsanforderung in der ECC-Warteschlange (External Communication Channel).
   d. MID-Server Überprüft die ECC-Warteschlange und ruft die ihr zugewiesene Erkennungsanforderung ab.
   e. MID-Server führt die Probes für den Host aus und erkennt offene Ports.

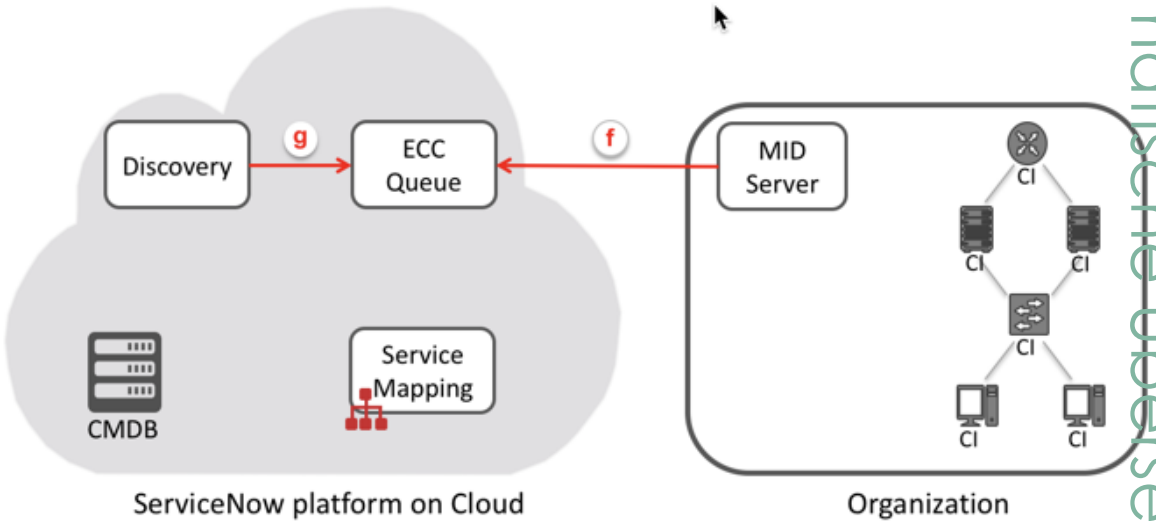
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



f. Der MID-Server übergibt Informationen über die Hostports an die ECC-Warteschlange.

g. Discovery prüft die ECC-Warteschlange und empfängt Informationen über die Hostports.

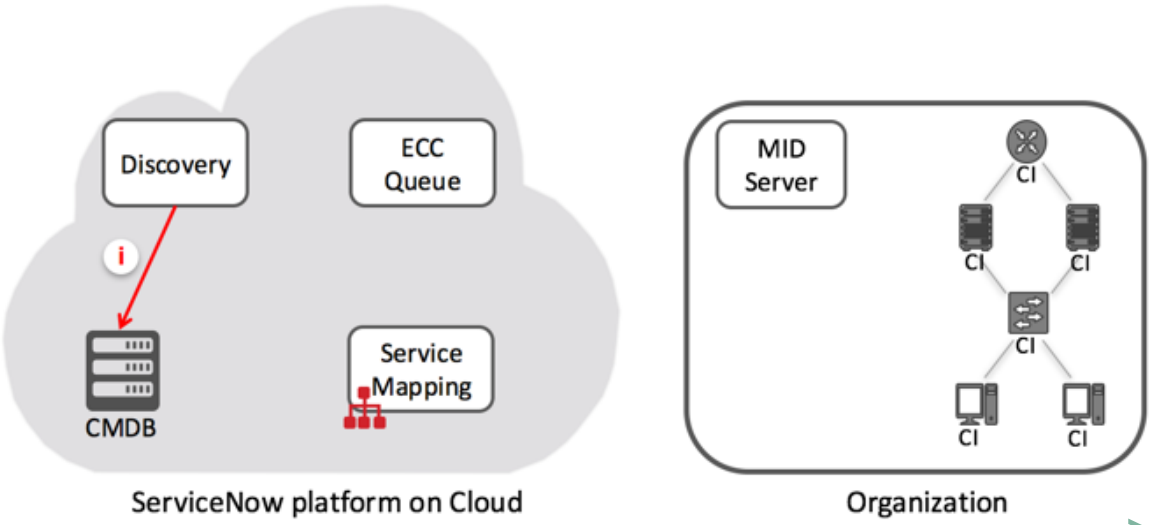


h. Diese Schritte werden für andere Probe-Typen wiederholt: Klassifizierung, Identifizierung und Erkundung.

i. Discovery fügt den Host der CMDB hinzu.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



j. Während der Hosterkennung mit Probes prüft Service-Mapping die ECC-Warteschlange, ob dieser Prozess abgeschlossen ist. Nach Abschluss der Hosterkennung überprüft Service-Mapping, ob dieser Host in der CMDB vorhanden ist.

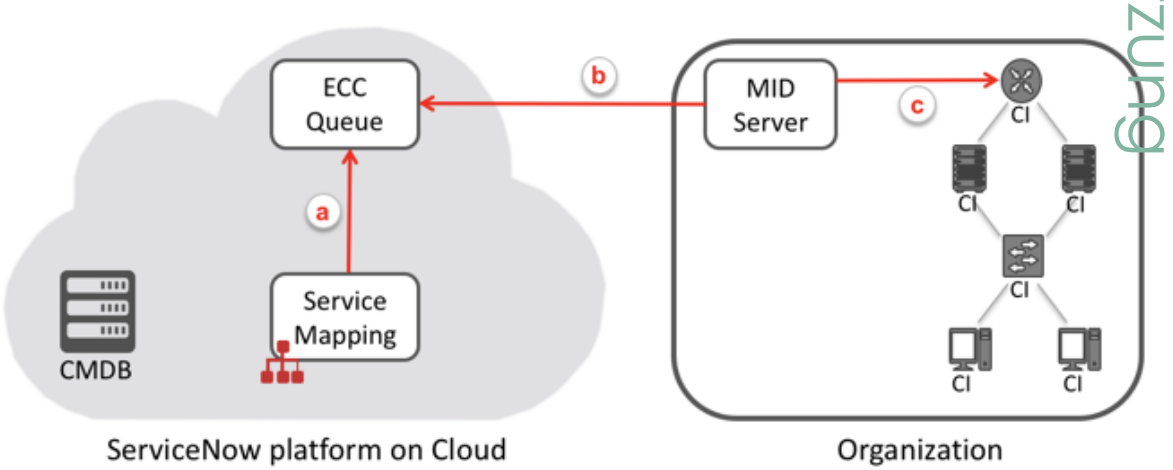
Hinweis: Eine detaillierte Beschreibung des Flow der horizontalen Erkennung finden Sie unter Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren.

3. Sobald der Host in CMDB gefunden wurde, erkennt Service-Mapping die auf diesem Host ausgeführte Anwendung.

a. Service-Mapping erstellt eine Anforderung zur Anwendungserkennung für die IP-Adresse des Einstiegspunkts. Anschließend wird die Anforderung in die ECC-Warteschlange geschrieben und der Anforderung ein MID-Server zugewiesen.

b. MID-Server überprüft die ECC-Warteschlange und ruft die ihr zugewiesene Erkennungsanforderung ab.

c. Der MID-Server beginnt mit der Ausführung von Identifizierungsabschnitten für die Muster, die dem Klassifizierer zugeordnet sind, um eine Übereinstimmung für den Einstiegspunkt zu finden. Wenn der Identifizierungsabschnitt mit dem Einstiegspunkt übereinstimmt, erkennt das Muster ein CI.



d. Der MID-Server beginnt mit der Ausführung von Konnektivitätsabschnitten für das Muster, um ausgehende Verbindungen des neu erkannten CI zu finden.

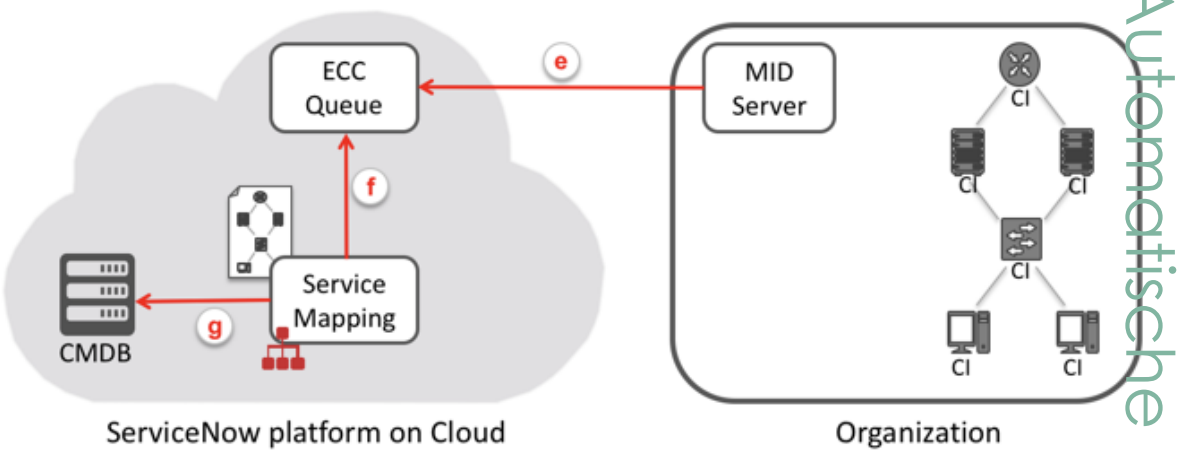
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Der MID-Server übergibt Informationen über das erkannte CI und seine Attribute und Verbindungen an die ECC-Warteschlange.

f. Service-Mapping überprüft die ECC-Warteschlange und erhält Informationen über das neu erkannte CI.

Wann auch immer Service-Mapping die ECC-Warteschlange prüft und Informationen zu einem ermittelten CI empfängt, prüft es diese Tabellen auf alle Daten zu ausgehenden Verbindungen, die sich auf das CI beziehen: die Tabellen cmdb_tcp und sa_flow_connection. Wenn diese beiden Tabellen eindeutige Daten enthalten, die von den Mustern nicht erkannt wurden, werden von Service-Mapping die Informationen zu den CI-Verbindungen erweitert, und die Informationen werden der Zuordnung hinzugefügt.

g. Service-Mapping schreibt die Informationen in die CMDB und fügt dieses CI der für Service-Zuordnung hinzu.



h. Service-Mapping erstellt die Erkennungsanforderungen für alle Anwendungen, mit denen das neu erkannte CI eine Verbindung herstellt. Die Zuordnung ist abgeschlossen, nachdem Service-Mapping ein CI zugeordnet hat, das entweder keine ausgehenden Verbindungen aufweist oder als Grenze markiert ist. Eine Grenze bewirkt, dass Service-Mapping die Erkennung ab diesem Punkt anhält und ausgehenden Verbindungen nicht folgt.

4. Das System führt regelmäßig eine Neuberechnung des Services durch, um die CMDB nach den neuesten CI-Änderungen abzufragen, Daten für Netzwerk- und Speicherpfade hinzuzufügen und CI-Auswirkungsregeln anzuwenden.

Zugehörige Informationen

ECC-Warteschlange für Discovery

Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren

Datenverkehrsbasierte Erkennung in Service-Mapping

Tag-basierte Erkennung in Service-Mapping

Wenn Ihre Organisation Tags für die Asset-Verwaltung verwendet, können die Tags zum Zuordnen von Serviceinstanzen verwendet werden.

Ein Tag ist eine Bezeichnung, die aus einem Schlüssel-Wert-Paar besteht. Ihre Organisation verwendet möglicherweise Tags, um Assets zu kategorisieren und um die Abfrage- und Berichtsfunktionen zu verbessern. Discovery und Cloud Provisioning and Governance können die von allen wichtigen Cloud-Anbietern und Container-Ökosystemen verwendeten Tags

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erkennen. Sobald die Tags erkannt wurden, können von Service-Mapping auf Grundlage dieser Tags Anwendungsservices erstellt werden. In der Regel verwenden Unternehmen Tags in virtualisierten, hyperkonvergenten oder Multi-Cloud-Infrastrukturen.

Beispiel für die Verwendung von Tags in der Organisationsinfrastruktur

Segment	Technologieanbieter	Getaggte Objekte
Cloud	Amazon Web Services (AWS), Azure, Google Cloud Platform (GCP), IBM Cloud Platform	IaaS-, PaaS-, FaaS-, CaaS-Ressourcen
Hyperkonvergent	Nutanix	Virtuelle Computer
Container	Kubernetes, Containerplattform OpenShift, AWS ECS	Container
Virtualisierung	VMware vCenter	Virtuelle Computer

Im Gegensatz zu anderen Zuordnungsmethoden ist es bei der tagbasierten Zuordnung nicht notwendig, Anmeldeinformationen zu konfigurieren oder Benutzern erweiterte Rechte zu gewähren. Sie können Tags effektiv verwenden, um mehrere Serviceinstanzen zuzuordnen.

Der Tag-basierte Erkennung- und Zuordnungsprozess besteht aus den folgenden Phasen:

1. Discovery und Cloud Provisioning and Governance erkennen Tags für Cloud- und Ressourcen-CIs und füllen dann die Daten für erkannte Tags in die Schlüsselwerttabelle [cmdb_key_value].
2. Der Administrator erstellt CI-Tag-Kategorien und definiert Tag-Schlüssel, die in den Kategorien enthalten sind. Tag-Kategorien enthalten Tags mit ähnlicher Verwendung, z. B. Tags, die sich auf verschiedene Arten von Umgebungen beziehen, wenn das Unternehmen die Tag-Werte „Produktion“ und „Staging“ verwendet.
3. Der Administrator erstellt eine Tag-basierte Servicefamilie und wählt Tag-Kategorien für die Zuordnung aus. Nur CIs, die Tag-Werte für die ausgewählten Tag-Kategorien erkannt haben, werden Teil der Anwendungsservices. Der Administrator kann die Kriterien einschränken, indem er zusätzlich zu den Tag-Kategorien noch Tag-Werte definiert. In diesem Fall nutzt Service-Mapping nur CIs mit übereinstimmenden Werten zum Erstellen von Anwendungsservices. CIs, denen mehrere Tags zugewiesen sind, können Teil mehrerer Services sein.

   Hinweis: Wenn Sie eine Servicefamilie zur Zuordnung von Services auf der Grundlage von Tags in einer domänengetrennten Umgebung erstellen, müssen Sie den entsprechenden Endknoten auswählen. Service-Mapping füllt tagbasierte Services auf der Grundlage dieser Servicefamilie nur mit CIs, die zu dem Endknoten gehören, zu der die Servicefamilie gehört.

4. Service-Mapping fragt CMDB nach CIs mit Tag-Werten ab, die den Tag-Definitionen für diese Tag-basierte Servicefamilie entsprechen.
5. Service-Mapping erstellt basierend auf den definierten Tags Servicekandidaten.

   Service-Mapping füllt tagbasierte Services auf der Grundlage dieser Servicefamilie nur mit CIs, die zu dem Endknoten gehören, zu der die Servicefamilie gehört.

6. Der Administrator wählt die zuzuordnenden Servicekandidaten aus und startet den Zuordnungsprozess.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Service-Mapping fügt der Tag-basierten Tabelle der Anwendungsservices [cmdb_ci_service_by_tags] neue Anwendungsservices hinzu.

   Wichtig: Tagbasierte Serviceinstanzen enthalten möglicherweise keine relevanten CIs, wenn diesen CIs nicht die richtigen Tags zugewiesen sind.

8. Service-Mapping ordnet Anwendungsservices zu, indem basierend auf CI-Beziehungen Verbindungen zwischen getaggten CIs erstellt werden. Die Tabelle „Durchsetzungsregeln für Anwendungsservices“ [svc_traversal_rules] enthält Informationen zum Erstellen von Tag-basierten Anwendungsservices.

   Hinweis: Service-Mapping enthält CIs, die Teil dieser Beziehungen sind, auch wenn diesen CIs keine Tags zugewiesen sind.

Sie können einzelne Tag-basierte Anwendungsservices mit dem Flow Gemeinsames Servicedatenmodell (CSDM) erstellen (siehe Anwendungsservices mithilfe von Tags ausfüllen) .

Zum Erstellen mehrerer Tag-basierter Services führen Sie das in Ordnen Sie Anwendungsservices mithilfe von Tags zu zu klassisch Service-Mapping beschriebene Verfahren aus.

Zugehörige Informationen

Konfiguration der Tag-basierten Discovery

Tag-Governance

Datenverkehrsbasierte Erkennung in Service-Mapping

Service-Mapping kann Konfigurationselemente (CIs) anhand ihrer datenverkehrsbasierten Verbindungen erkennen und zuordnen. Diese Methode wird als datenverkehrsbasierte Zuordnung bezeichnet und ergänzt die musterbasierte Zuordnung.

Datenverkehrsbasierte Zuordnung – Definition

Die Verwendung der Traffic-basierten Discovery ist wie das Auswerfen eines feineren Netzes, mit dem Service-Mapping sogar die CIs erkennen kann, die mithilfe von Mustern nicht erkannt wurden. Wenn ein CI zwei Verbindungen hat, wird die Traffic-basierte Verbindung nach der nächsten Top Down-Discovery geschlossen; alle manuellen oder musterbasierten Verbindungen bleiben bestehen.

Je nach Konfiguration variiert das Systemverhalten hinsichtlich der datenverkehrsbasierten Erkennung. Wenn die Discovery basierend auf Predictive Intelligence aktiviert ist, fügt Service-Mapping basierend auf Verbindungsregeln automatisch Verbindungen zu Serviceinstanzen hinzu. Service-Mapping generiert diese Vorschläge basierend auf datenverkehrsbezogenen Daten aus der Configuration Management Database (CMDB) und der Analyse von Anwendungsfingerabdrücken, CIs und Prozessen durch Predictive Intelligence.

Wenn Discovery-basierte Predictive Intelligence deaktiviert sind, fügt Service-Mapping automatisch datenverkehrsbasierte Verbindungen basierend auf den Daten CMDB zu Serviceinstanzen hinzu. Möglicherweise müssen Sie Verbindungen entfernen, die zu irrelevanten CIs führen, um Serviceinstanzen übersichtlicher zu gestalten. Wenn die Funktion für Verbindungsvorschläge deaktiviert ist, verwenden Sie die Traffic-basierte Discovery normalerweise in der Anfangsphase der Erkennung von Anwendungsservices. Deaktivieren Sie die datenverkehrsbasierte Erkennung, nachdem Sie die Erkennung und Feinabstimmung von Anwendungsservices abgeschlossen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die musterbasierte Discovery nach der datenverkehrsbasierten Discovery ausgeführt wird, können doppelte Verbindungen zwischen CIs entstehen. In diesem Fall entfernt das System die durch die Traffic-basierte Discovery erstellte Verbindung. Das System behält alle Verbindungen bei, die durch die Traffic-basierte Discovery erstellt wurden und nicht mithilfe von Mustern erkannt wurden.

Datenverkehrsbezogene Daten aus der CMDB

Im System werden Befehle und Netzwerk-Flow-Protokolle verwendet, um datenverkehrsbezogene Daten zu sammeln und in den CMDB-Tabellen zu speichern. Service-Mapping ruft diese Daten aus den Tabellen ab, um ein- und ausgehende CI-Verbindungen zu erkennen.

Tabellen, die Daten enthalten, die mit Traffic-basierten Methoden erfasst wurden

Tabelle	Quelle	**Benutzt von** Service-Mapping **zum**
Flow Connector [sa_flow_connection]	Netflow- und VPC-Protokolle	Erkennen Sie Abhängigkeiten, und fügen Sie Verbindungen während der Top Down-Discovery hinzu.
IP/Port und Statistiken für Flow-Services [sa_flow_service]	Netflow- und VPC-Protokolle	Entdecken Sie alle Services, die Ports überwachen. Im Basissystem verwendet Service-Mapping keine Daten aus dieser Tabelle.
Ablauf-Serverkommunikation [sa_flow_server_comm]	Netflow- und VPC-Protokolle	Entdecken Sie Services, die mit anderen Services kommunizieren. Im Basissystem verwendet Service-Mapping keine Daten aus dieser Tabelle.
TCP-Verbindung [cmdb_tcp]	netstat- und lsof-Befehle	Verbindungen bei der Top Down-Discovery erkennen.

In Basissystemen verwendet die Traffic-basierte Discovery nur TCP-Daten, die mithilfe der Befehle *netstat*, *ss* und *lsof* erfasst wurden. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung ausweiten, indem Sie Service-Mapping für die Datenerfassung mit Netflow- und VPC-Protokollen konfigurieren. Darüber hinaus hat Service-Mapping Zugriff auf die TCP-Verbindungsdaten, die vom verbesserten Application Dependency Mapping (ADM) erfasst werden. Discovery führt ADM als Teil der Horizontal-Discovery aus.

Datenverkehrsbasierte Erkennung im System aktivieren

Standardmäßig ist die datenverkehrsbasierte Erkennung mithilfe von Befehlen in Service-Mapping verfügbar, sodass diese Methode auf allen Ebenen verwendet werden kann. Sie können die datenverkehrsbasierte Erkennung auf verschiedenen Ebenen aktivieren, von der globalen bis zur spezifischsten:

Produktebene

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig ist die Traffic-basierte Discovery in Service-Mapping deaktiviert. Die Eigenschaft **„Verkehrsbasierte Discovery“** *[sa.traffic_based_discovery.active]* steuert die datenverkehrsbasierte Discovery auf Produktebene.

Wichtig: Sie können die Traffic-basierte Discovery nicht auf anderen Ebenen aktivieren, es sei denn, sie wird auf Produktebene aktiviert.

Die Funktion für Verbindungsvorschläge funktioniert auf Produktebene. Gesteuert wird diese Funktion mit der Eigenschaft *sa_ml.connection_suggestions.active*. Wenn in Ihrer -Bereitstellung vor Quebec die Traffic-basierte Discovery aktiviert war und Sie sie zum Erkennen mindestens eines Anwendungsservice verwendet haben, ist die Funktion für Verbindungsvorschläge standardmäßig deaktiviert.

Serviceinstanz Ebene

Sie können die Traffic-basierte Discovery für einen bestimmten aktivieren für Service. In diesem Fall verwendet Service-Mapping diese Methode für alle CIs, aus denen für Servicebesteht, es sei denn, die Traffic-basierte Discovery ist für einige CI-Typen oder bestimmte CIs deaktiviert.

CI-Typebene

Sie können in einer Erkennungsregel festlegen, dass ein bestimmter CI-Typ in der datenverkehrsbasierten Erkennung ein- oder ausgeschlossen wird. Diese Regel hat Vorrang vor der Einstellung, die Sie für für Service wählen.

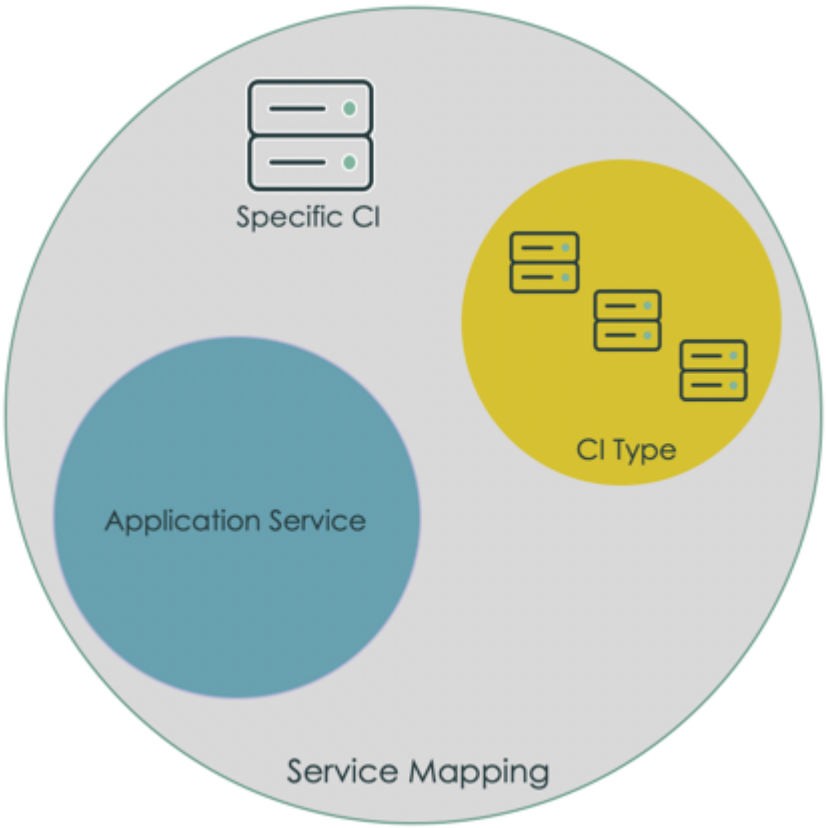
Spezifische CI-Ebene

Sie können in einer Erkennungsregel festlegen, dass ein bestimmtes CI in der datenverkehrsbasierten Erkennung ein- oder ausgeschlossen wird. Diese Regel hat Vorrang vor der Einstellung, die Sie für für Service wählen.

Regeln für bestimmte CIs haben Vorrang vor Regeln für CI-Typen. Wenn Sie beispielsweise keine Traffic-basierte Discovery auf Apache Tomcat-Servern verwenden möchten, können Sie eine Regel vom **CI-Typ** festlegen, die die Traffic-basierte Discovery für die Tomcat-Tabelle deaktiviert. Gleichzeitig können Sie eine Discovery-Regel erstellen, die die Traffic-basierte Discovery für einen bestimmten Tomcat-Server aktiviert. In diesem Fall verwendet Service-Mapping die Traffic-basierte Discovery unter allen Tomcat-Servern nur für diesen bestimmten Tomcat-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenverkehrsbasierte Erkennung auf verschiedenen Ebenen aktivieren



Zugehörige Informationen

- CIs für mehrere Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen
- CIs für einzelne Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen
- Application Dependency Mapping (ADM) für Discovery
- Nicht zu Anwendungsservices gehörende CIs entfernen
- Datenerfassung und -erkennung mit Netflow
- Datenerfassung und -erkennung mit VPC-Flow-Protokollen

Erkennung von Anwendungsservices in der Cloud mithilfe von Service-Mapping

Service-Mapping kann Anwendungsservices erkennen, die aus in der Cloud bereitgestellten Geräten und Anwendungen bestehen.

Es gibt zwei Arten von Cloud-Computing-Methoden, die Ihr Unternehmen verwenden kann: Infrastructure-as-a-Service (IaaS) und Platform-as-a-Service (PaaS). Service-Mapping erkennt Anwendungsservices basierend auf IaaS auf die gleiche Weise wie alle Anwendungsservices, die auf einer Infrastruktur innerhalb eines privaten Unternehmensnetzwerks basieren. Die Methode nutzt Discovery für die Suche nach Hosts, bevor Anwendungen und Verbindungen zwischen ihnen mithilfe von Mustern erkannt werden. Weitere Informationen zu diesem Discovery-Flow finden Sie unter Musterbasierte Erkennung in Service-Mapping.

Für die vollständige oder partielle Erkennung von Anwendungsservices auf Basis von PaaS wird ein anderes Paradigma benötigt. Anwendungen in solchen Bereitstellungen werden von Netzwerkgeräten in der Cloud gehostet. Um in einer solchen Bereitstellung einen Anwendungsservice zu erkennen, verwenden Sie Discovery und Service-Mapping wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie konfigurieren ein Servicekonto für die Cloud-Computing-Plattform, die den Anwendungsservice hostet. Service-Mapping und Discovery verwenden dieses Servicekonto zum Zugriff auf Geräte und Anwendungen auf dieser Plattform.
- Discovery führt die horizontale Erkennung mithilfe von Probes durch und findet die Infrastrukturgeräte in der Cloud.
- Discovery führt die horizontale Erkennung mithilfe von Mustern durch und findet in der Cloud gehostete Anwendungen und Services.
- Service-Mapping führt die Erkennung von oben nach unten durch, um Verbindungen zwischen Geräten und Anwendungen zu finden und die Zuordnung des Anwendungsservice zu erstellen.

Zugehörige Informationen

Cloud-Discovery erkunden

Service-Mapping-Flow

Erfahren Sie mehr über allgemeine Aufgaben, die Benutzer mit unterschiedlichen Rollen in Service-Mapping ausführen.

In Service-Mapping kooperieren Benutzer, um Anwendungsservices der Organisation zuzuordnen, zu überprüfen und zu überwachen.

Hinweis: Eine vollständige Liste der Rollen in Service-Mapping finden Sie unter Mit Service-Mapping installierte Komponenten.

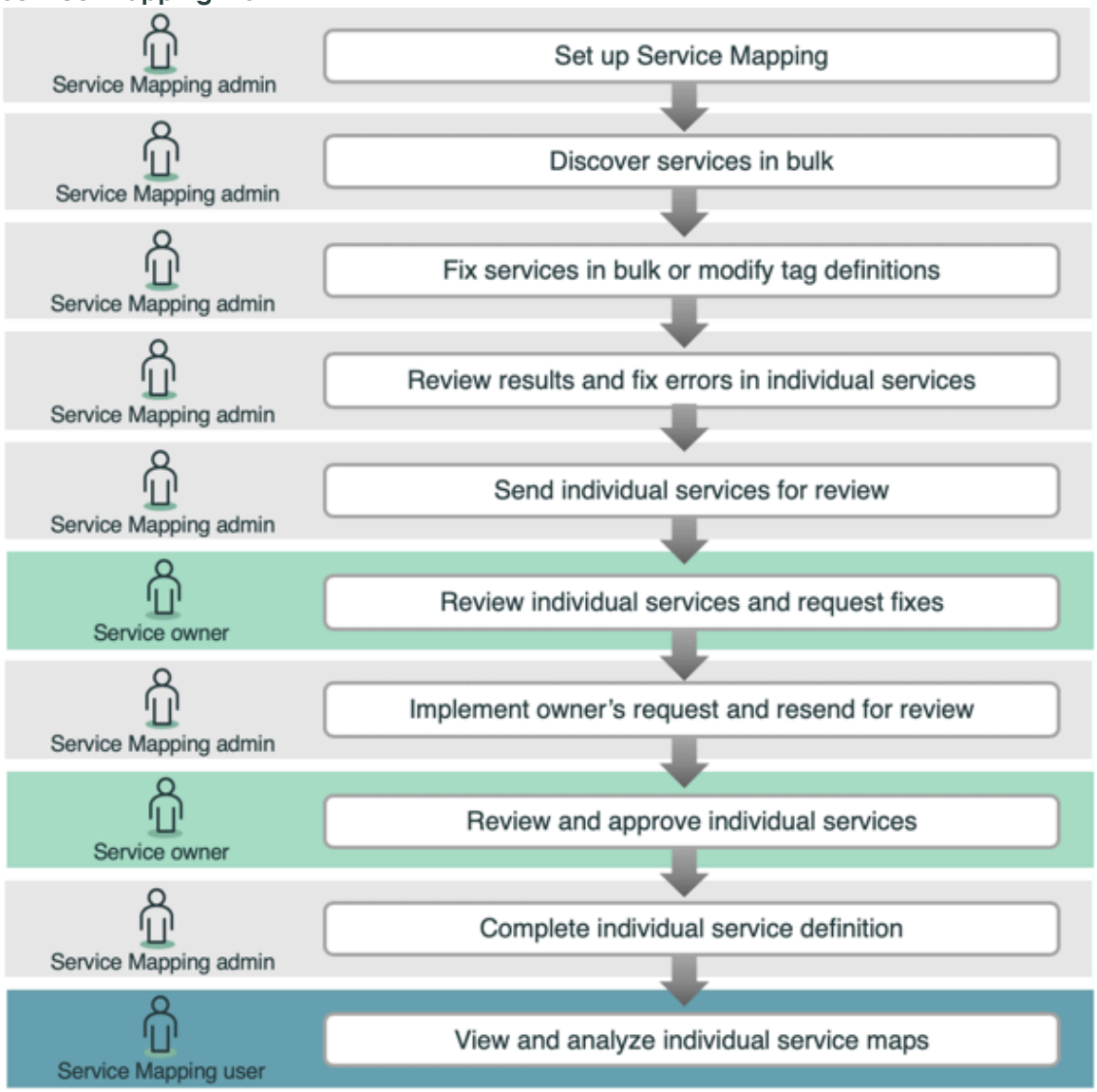
Ein typischer Service-Mapping-Workflow umfasst die folgenden Phasen:

1. Der Administrator führt grundlegende obligatorische Konfigurationen zum Einrichten von Service Mapping durch.
2. Der Administrator führt die Zuordnung von Anwendungsservices der Organisation als Massenvorgang aus. Darüber hinaus kann der Administrator einige Anwendungsservices einzeln zuordnen.
3. Der Administrator korrigiert Fehler in Anwendungsservices in einem Massenvorgang.
4. Der Administrator überprüft die Ergebnisse der ursprünglichen Zuordnung und behebt Fehler in einzelnen Anwendungsservices.
5. Der Administrator sendet die korrigierten Anwendungsservices zur Überprüfung an den Anwendungsservice-Eigentümer.
6. Der Besitzer der Serviceinstanz überprüft, ob die Serviceinstanzzuordnungen vollständig sind und alle wichtigen Komponenten, aus denen sie bestehen, korrekt dargestellt werden. Bei Bedarf hinterlässt der Besitzer Kommentare, die als Ablehnungsnachrichten bezeichnet werden, auf Serviceinstanzzuordnungen, die der Administrator Service-Mapping implementieren muss. Siehe Anwendungsservicezuordnungen prüfen.
7. Der Administrator nimmt auf Basis des Feedbacks des Anwendungsservice-Eigentümers eine Feinabstimmung der Anwendungsservice-Übersicht vor und sendet sie zur erneuten Überprüfung an den Eigentümer.
8. Wenn die überarbeiteten Serviceinstanzzuordnungen zufriedenstellend sind, genehmigt der Besitzer der Serviceinstanz sie. Wenn nicht, fordert der Verantwortliche weitere Fehlerkorrekturen an, die der Administrator umsetzen muss. Siehe Anwendungsservicezuordnungen prüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Der Administrator schließt die Definition der Anwendungsservices ab, indem er den Zugriff auf sie sowie einige erweiterte Attribute wie Kritikalität konfiguriert.
10. Nachdem die Definition des für Service abgeschlossen ist, kann der Service-Mapping-Benutzer die Anwendungsservices-Übersicht anzeigen.

Service-Mapping-Flow



Zusätzlich zu diesen Aufgaben kann es erforderlich sein, Muster anzupassen, die Service-Mapping verwendet, um Geräte und Anwendungen zu erkennen, die Anwendungsservices bilden. Anwender müssen über die Rolle pd_admin verfügen, um Muster anzupassen. Im Basissystem enthält die Rolle service_mapping_admin die pd_role. Das Anpassen von Mustern erfordert Grundkenntnisse in der Programmierung.

Zugehörige Informationen

Benutzerzugriff auf Anwendungsservices steuern

Service-Mapping konfigurieren

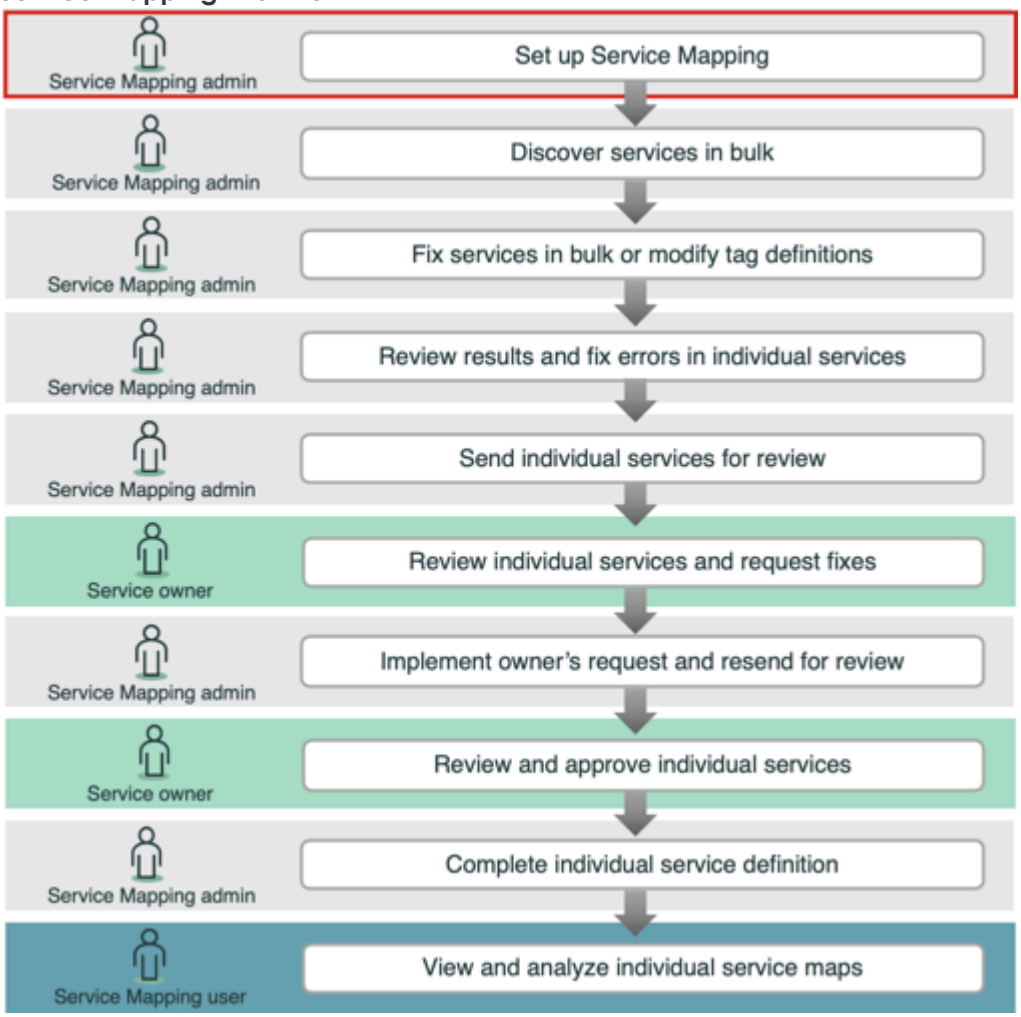
Der erste Schritt in Service-Mapping besteht darin, Rollen, Anmeldeinformationen und MID-Server-Verbindungen zu konfigurieren.

Das Einrichten von Service-Mapping ist die erste Phase im Workflow von Service-Mapping.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service Mapping-Workflow



Service-Mapping ist Teil von Now Platform und stellt einige der auf der gesamten Plattform genutzten Mechanismen und Funktionen bereit. Es gibt allerdings auch einige Konfigurationen, die nur für Service-Mapping gelten.

⚠ **Warnung:** Das Setup von Service-Mapping für den Advance Release unterscheidet sich von der Standardeinrichtung von Service-Mapping.

Führen Sie die folgenden Aufgaben exakt in der Reihenfolge aus, in der sie unten aufgeführt sind:

1. Service-Mapping anfordern.
2. Service-Mapping Plus installieren.
3. Installieren und konfigurieren Sie den MID-Server. MID Servers, die sich im privaten Netzwerk des Unternehmens befinden, erleichtern die Kommunikation zwischen Servern im Netzwerk und einigen ServiceNow-Anwendungen wie Service-Mapping und Discovery. Weitere Informationen finden Sie unter Konfiguration des MID Servers für Service-Mapping.
4. Vergewissern Sie sich, dass Discovery eingerichtet ist und die horizontale Erkennung wie erwartet ausführt.
5. Konfigurieren Sie die für die Hosterkennung erforderlichen Anmeldeinformationen.
6. Konfigurieren Sie die für Service-Mapping erforderlichen Anmeldeinformationen für den Zugriff auf Anwendungen im privaten Netzwerk Ihrer Organisation. Weitere Informationen finden Sie unter Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wenn das Netzwerk Ihrer Organisation Lastenausgleichsmodule enthält, die auf einem Linux-Host ausgeführt werden, erzeugen Sie ein Erkennungsverhalten für Lastenausgleichsmodule.
8. Ordnen Sie relevanten Benutzern die folgenden Service-Mapping-Rollen zu:

   service_mapping_admin

   Richtet die Service-Mapping-Anwendung ein. Ermöglicht die Zuordnung, Korrektur und Wartung von Serviceinstanzen. Führt auch eine erweiterte Konfiguration und Anpassung des Produkts durch. Weisen Sie diese Rolle Anwendungsadministratoren zu.

   service_mapping_user

   Zeigt Zuordnungen für funktionsfähige Serviceinstanzen an, um Change oder Migration zu planen und die Kontinuität und Verfügbarkeit von Services zu analysieren. Weisen Sie diese Rolle Anwendungsbenutzern zu.

   sm_app_owner

   Stellt Informationen bereit, die für die erfolgreiche Zuordnung einer Serviceinstanz erforderlich sind. Wenn ein Dienst zugeordnet ist, überprüft dieser Benutzer die Ergebnisse und genehmigt sie entweder oder schlägt Änderungen vor. Weisen Sie die Rolle sm_app_owner Benutzern zu, die Besitzer von Serviceinstanzen sind und mit der Infrastruktur und den Anwendungen vertraut sind, aus denen die Services bestehen.

9. Sicherstellen, dass Service-Mapping ordnungsgemäß eingerichtet ist.
10. Wenn Ihre Organisation über eine ServiceNow-Bereitstellung mit benutzerdefinierten Discovery- oder CMDB-Attributen verfügt, führen Sie die zusätzliche Konfiguration durch, die in KB0647574: Preparing customized ServiceNow deployments to work with Service Mapping (Vorbereitung benutzerdefinierter ServiceNow-Bereitstellungen zur Verwendung mit Service Mapping) beschrieben ist.

Zusätzlich zu den hier beschriebenen obligatorischen Setupkonfigurationen müssen Sie möglicherweise zusätzliche Konfigurationen durchführen, nachdem Sie den ersten Zuordnungsprozess abgeschlossen haben. Weitere Informationen finden Sie unter Erweiterte Konfiguration von Service Mapping.

Service-Mapping anfordern

Service-Mapping ist im Rahmen des ITOM-Transparenz-Abonnements verfügbar und erfordert eine Aktivierung durch ServiceNow-Personal.

Vorbereitungen

Erforderliche Rolle: keine

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktionsinstanz bzw. untergeordneten Produktionsinstanz Ihrer Organisation.

Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Erforderliche Rolle: admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Plugins werden automatisch aktiviert, wenn das Service-Mapping-Plugin (com.snc.service-mapping) aktiviert ist:

- Discovery (com.snc.discovery)

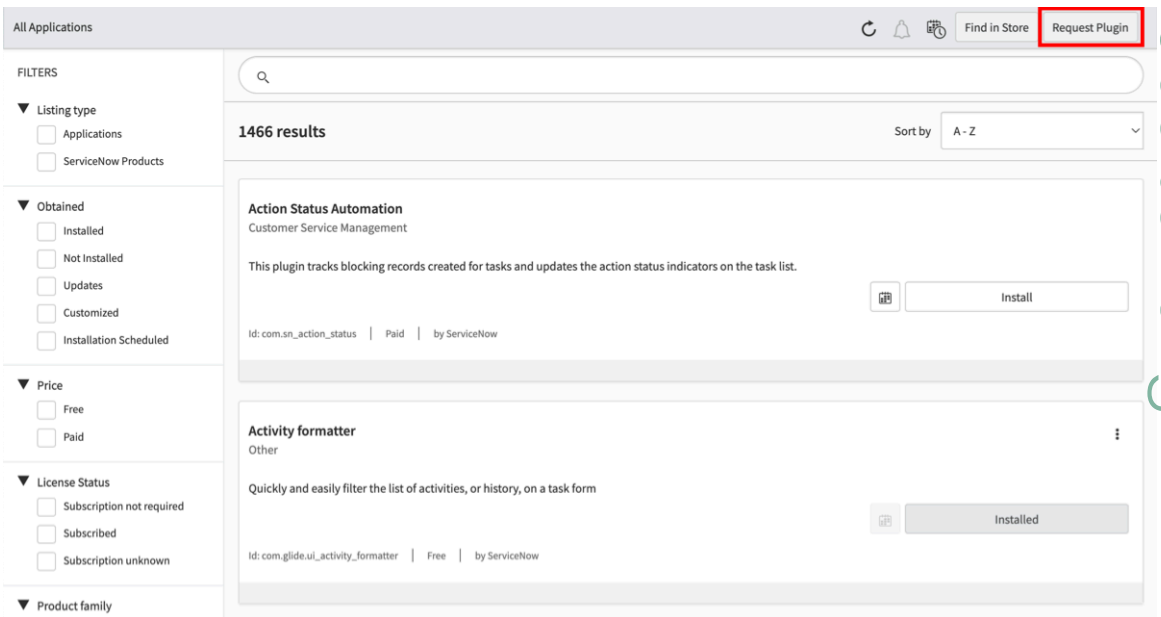
> **Hinweis:** Bei der erstmaligen Aktivierung des Plugins „Discovery“ im Release Yokohama installieren Sie zuerst das Plugin „Discovery“ (com.snc.discovery) und anschließend das Plugin „Muster für Discovery und Service-Mapping“ (com.sn_itom_pattern) in der Version 1.0.52, damit Cloud-Discovery funktioniert. Anschließend können Sie ein Upgrade auf Yokohama durchführen.

- Musterdesigner (com.snc.pattern.designer)
- Cloud Provisioning and Governance Core (com.snc.cloud.core)
- Performance Analytics – Content Pack – Service Mapping (com.snc.service-mapping.pa.content)
- Ereignismanagement und Service-Mapping Core (com.snc.service-watch)

> **Hinweis:** Das Plugin „Ereignismanagement und Service-Mapping Core“ (com.snc.service-watch) unterscheidet sich vom Plugin „Ereignismanagement“ (com.glideapp.itom.snac).

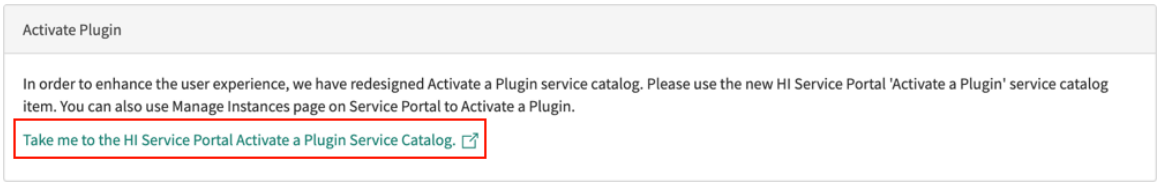
Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

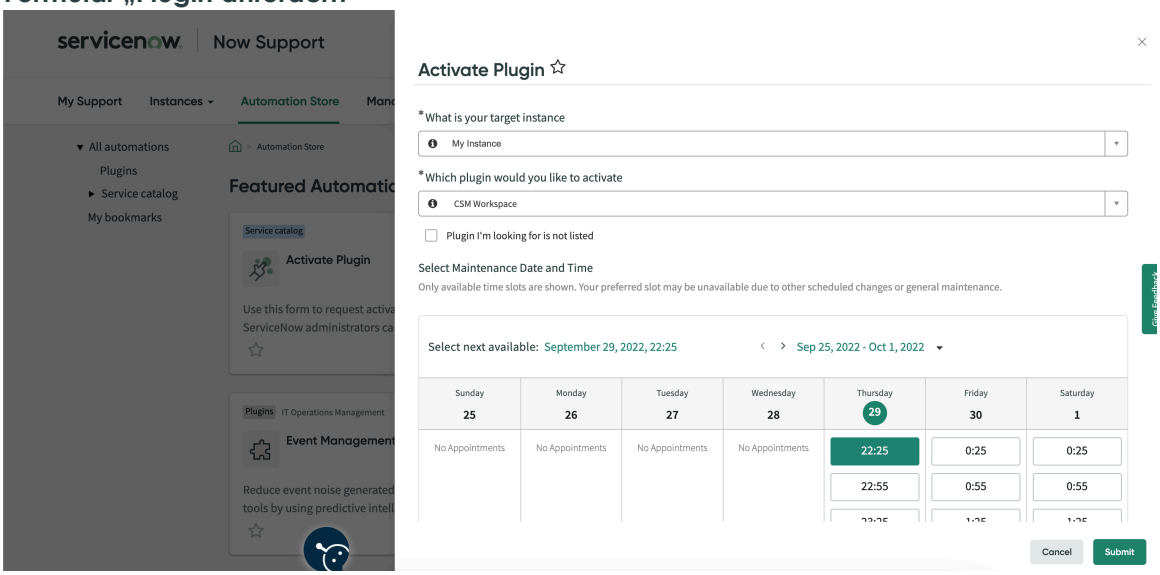
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-Artikel [KB0751715] in Now Support Knowledge Base.

Zugehörige Informationen

Für die Hosterkennung erforderliche Anmeldeinformationen

Service-Mapping Plus installieren

Mit der Administratorrolle können Sie die Anwendung Service Mapping Plus (sn_sm_scoped_app) installieren. Die Anwendung installiert die zugehörigen ServiceNow® Store-Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfen Sie die Anwendungsliste im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Service-Mapping Plus installiert:

- Regelmäßige Aufgaben
- Tabellen

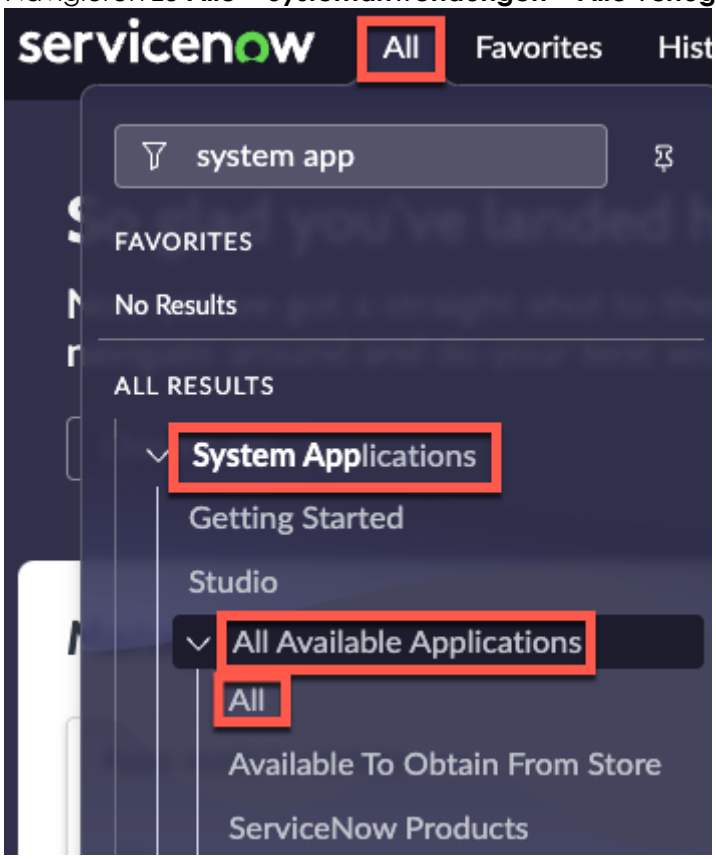
Weitere Informationen finden Sie unter Mit Service-Mapping Plus installierte Komponenten.

Eine Liste der Service-Mapping Plugin-Abhängigkeiten finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Transparenz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie die Anwendung Service Mapping Plus (sn_sm_scoped_app) mithilfe der Filterkriterien und der Suchleiste.

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Konfiguration des MID Servers für Service-Mapping

Konfigurieren Sie Service-Mapping und MID Servers so, dass sie gemeinsam funktionieren.

Was ist der MID-Server?

Der MID-Server (Management, Instrumentation, and Discovery) ist eine Java-Anwendung, die als Windows-Service oder UNIX-Daemon auf einem Server ausgeführt wird. MID Servers, die sich im privaten Netzwerk des Unternehmens befinden, erleichtern die Kommunikation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

zwischen Servern im Netzwerk und einigen ServiceNow-Anwendungen wie Service-Mapping und Discovery.

Hinweis: Wenn sowohl das Plugin „Service-Mapping“ (com.sn_itom_pattern) in der Instanz als auch ein Sprach-Plugin (z. B. Spanisch) aktiviert ist, stellen Sie sicher, dass die Sprache für den MID-Server im Benutzerdatensatz ebenfalls auf „English/None“ (Englisch/Keine) festgelegt ist.

MID-Server – Auswahlkriterien

Die meisten Umgebungen erfordern mehrere MID Servers, wobei Service-Mapping das relevante MID-Server für die Discovery verwendet. MID Servers haben die folgenden Auswahlkriterien, die Service-Mapping verwenden kann, um das relevante MID-Serverauszuwählen:

- Anwendung – legt fest, mit welcher Anwendung ein MID-Server arbeitet. Stellen Sie es auf Service-Mapping, um diesen MID-Server ausschließlich für Discovery-Anforderungen von Service-Mapping zu reservieren. Alternativ können Sie auf ALL setzen, damit alle ServiceNow-Anwendungen MID-Server verwenden können.

- Fähigkeit – Definiert die Netzwerkfähigkeit. Legen Sie für Service-Mappingdiesen Parameter auf ALL oder eine beliebige Kombination aus SSH, WMI, SNMP und Cloud Provisioning and Governance fest. Weitere Informationen finden Sie unter Fähigkeiten des MID-Servers konfigurieren .

- IP-Bereich – schränkt den Betrieb dieses MID-Server auf diesen IP-Bereich ein. Service-Mapping wählt diesen MID-Server nicht für eine Discovery-Anforderung, deren Endpunkt außerhalb dieses IP-Bereichs liegt. Siehe Konfigurieren eines IP-Adressbereichs für den MID Server .

  Hinweis: Informationen zur Umgehung der Konfiguration MID-Server basierend auf dem IP-Bereich finden Sie unter Optimieren Sie Service-Mapping mit MID-Affinität und Wiederverwendung von IPs.

Service-Mapping wählt einen MID-Server mit folgendem Algorithmus aus:

- Service-Mapping wählt den MID-Server aus, dessen Auswahlkriterien am besten mit den Parametern der Discovery-Anforderung übereinstimmen.
- Wenn es keine MID Servers mit übereinstimmenden Auswahlkriterien gibt, wählt Service-Mapping den Standard-MID-Server aus.
- Wenn es keine MID Servers mit übereinstimmenden Auswahlkriterien und keinen Standard-MID-Server gibt, kann Service-Mapping den Discovery-Prozess nicht starten.

Standardmäßig verwendet Service-Mapping diesen Algorithmus in allen Bereitstellungen, die von Istanbul oder Jakarta aktualisiert wurden, unterstützt jedoch sowohl neue als auch veraltete Algorithmen zur Auswahl eines MID-Servers. Weitere Informationen finden Sie unter MID Server-Auswahlalgorithmus wählen.

Standard-MID Servers für Service-Mapping

Zusätzlich zu den Auswahlkriterien können Sie einen der MID Servers als Standardserver konfigurieren, der Service-Mapping nutzt. Wenn es keine MID Servers gibt, deren Anwendung, Fähigkeit oder IP-Bereich geeignet ist, verwendet Service-Mapping den standardmäßigen MID-Server. Siehe Einen Standard-MID-Server für jede Anwendung konfigurieren .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PowerShell zur Erkennung nutzen

MID Servers können PowerShell für die direkte Kommunikation mit Windows-Servern verwenden, wobei sowohl WMI- als auch WinRM-Protokolle verwendet werden. Für Windows-Services, die das WinRM-Protokoll verwenden, richtet der PowerShell-Prozess eine sichere PSSession ein (PowerShell-Remoting-Sitzung) ein, bis MID-Server die Abfrage eines Windows-Servers beendet. Bei Windows-Servern, die das WMI-Protokoll verwenden, sendet der PowerShell-Prozess jeden PowerShell-Befehl mit Anmeldeinformationen.

Wenn Sie die MID Servers nicht für die Verwendung von PowerShell und PowerShell Remoting konfigurieren, verwenden die MID Servers WMI.

ServiceNow bietet jetzt Unterstützung für PowerShell 3.0 bis 5.1.

MID-Server-Erkennung ohne Anmeldeinformationen mit Nmap

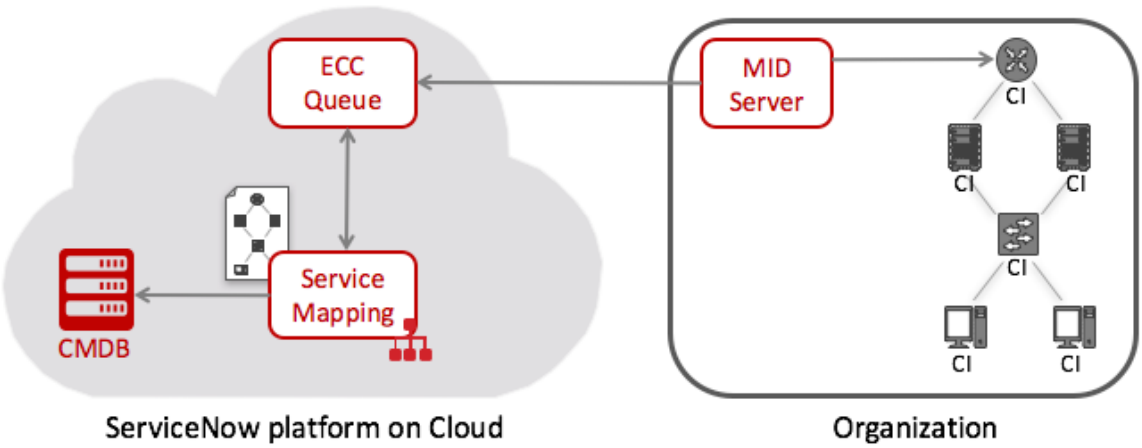
Wenn MID-Server nicht über ausreichende Anmeldeinformationen verfügt, um auf ein Gerät oder eine Anwendung zuzugreifen, kann sie Nmap-Befehle (Network Mapper) ausführen, um grundlegende Informationen ohne Verwendung von Anmeldeinformationen zu erfassen. Die Discovery ohne Anmeldeinformationen mit Nmap erfordert eine zusätzliche Konfiguration, wie in Nmap auf einem MID-Server installieren und deinstallieren beschrieben ist.

ServiceNow -Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Configuration Items (CIs) umfassen.

MID Servers platzieren

Die Anzahl der von Ihnen benötigten MID Servers hängt von den Anforderungen Ihres Unternehmens ab. Wenn Sie Geräte und Anwendungen in Ihrem privaten Netzwerk zuordnen möchten, platzieren Sie die MID Servers im privaten Netzwerk. Wenn Sie Geräte und Anwendungen in der DMZ zuordnen möchten, platzieren Sie die MID Servers sowohl in der DMZ als auch im privaten Netzwerk.

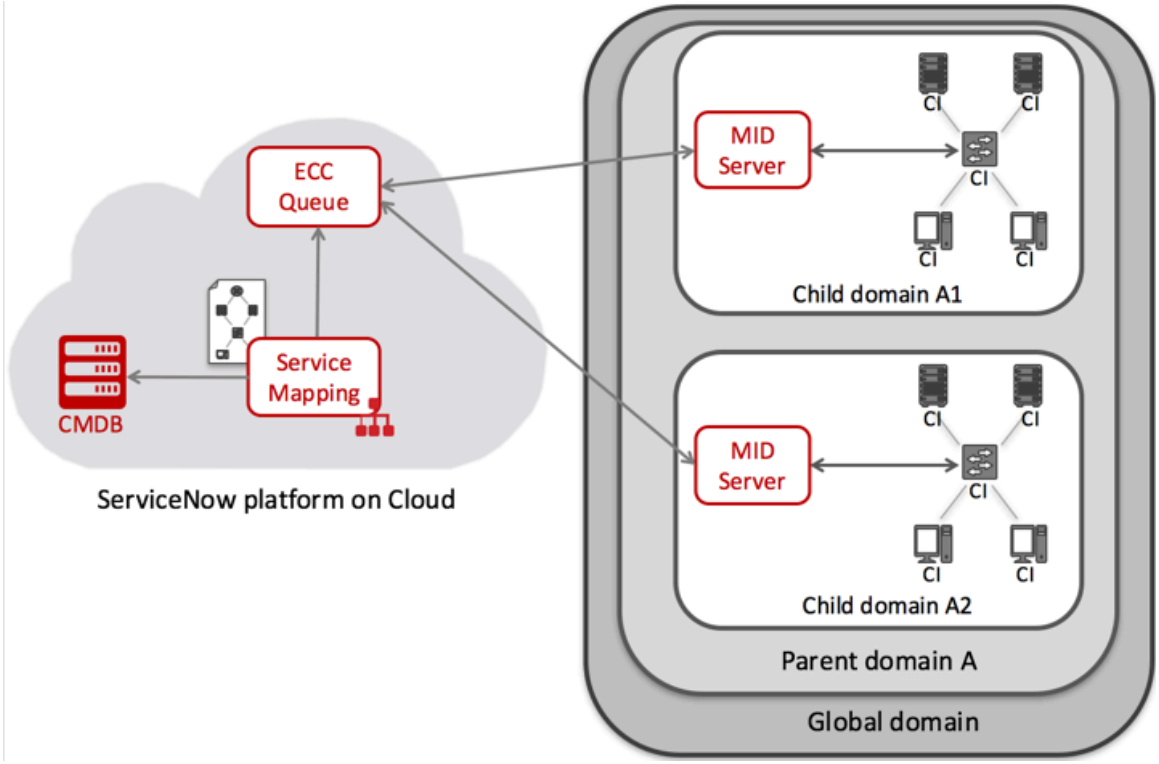
MID Servers im privaten Netzwerk platzieren



In Bereitstellungen, in denen die Domänentrennung aktiviert ist und Domänen so konfiguriert sind, dass sie eine Hierarchie bilden, müssen MID Servers auf der untersten Domänenebene, einer "Blattdomäne", platziert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID Servers in domänengetrennten Umgebungen platzieren



Sobald MID Servers MID Servers installiert ist, konfigurieren Sie sie für die Verwendung mit Service-Mapping, um die besten Discovery-Ergebnisse zu erzielen.

Zugehörige Informationen

- Musterbasierte Erkennung in Service-Mapping
- MID Server-Verbindungsvoraussetzungen
- Erkennung ohne Anmeldeinformationen mit Nmap
- Anwendungserkennung ohne Anmeldeinformationen
- Mehrere MID Server-Bereitstellungen
- MID Server-Installation
- MID-Server-Eigenschaften, die von Service-Mapping verwendet werden

MID Server-Auswahlalgorithmus wählen

Service-Mapping unterstützt die neuen und veralteten Algorithmen zur Auswahl eines MID-Servers für eine Erkennungsanforderung. Den zu aktivierenden Algorithmus können Sie je nach Anforderungen Ihres Unternehmens auswählen.

Vorbereitungen

Erforderliche Rolle: admin oder service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Service-Mapping wählt einen MID-Server mit folgendem Algorithmus aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Service-Mapping wählt den MID-Server aus, dessen Auswahlkriterien am besten mit den Parametern der Discovery-Anforderung übereinstimmen.
- Wenn es keine MID Servers mit übereinstimmenden Auswahlkriterien gibt, wählt Service-Mapping den Standard-MID-Server aus.
- Wenn es keine MID Servers mit übereinstimmenden Auswahlkriterien und keinen Standard-MID-Server gibt, kann Service-Mapping den Discovery-Prozess nicht starten.

Standardmäßig verwendet Service-Mapping diesen Algorithmus in allen Neuinstallationen und Bereitstellungen, die von Istanbul oder Jakarta upgegradet wurden.

In aktualisierten Bereitstellungen wählt Service-Mapping einen MID-Server mit einem veralteten Algorithmus:

- Service-Mappingwählt die MID-Server deren Anwendungskriterien auf *`ServiceMapping`* oder *`ALL`* eingestellt sind.
- Standardmäßig wählt Service-Mapping das MID-Server aus, dessen IP-Bereich mit der IP in der Discovery-Anforderung übereinstimmt.
- Wenn Service-Mapping keinen MID-Server mit dem übereinstimmenden IP-Bereich und der übereinstimmenden Anwendung finden kann, wird die Discovery-Anforderung dem Standard-MID-Server zugewiesen.
- Wenn es keinen Standard-MID-Server gibt und keine der MID Servers konfigurierte IP-Bereiche haben, verwendet Service-Mapping einen zufälligen MID-Server .
- Wenn es keinen Standard- MID-Server gibt und kein IP-Bereich stimmt mit der IP in der Discovery-Anforderung überein, kann Service-Mapping den Erkennungsprozess nicht starten.

Standardmäßig verwendet Service-Mapping den veralteten Algorithmus in allen Bereitstellungen, die auf Istanbul und früher upgegradet wurden.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Eigenschaften**.
2. So aktivieren Sie den neuen Algorithmus für Bereitstellungen, die auf Istanbul und früher upgegradet wurden:
   a. Deaktivieren Sie das Kontrollkästchen **Alten MID-Auswahlalgorithmus aktivieren**.
   b. Klicken Sie auf **Speichern**.
   c. Konfigurieren Sie die MID-Server-Auswahlkriterien (siehe Konfiguration des MID Servers für Service-Mapping).
3. So aktivieren Sie den veralteten Algorithmus für die Yokohama-Bereitstellung:
   a. Aktivieren Sie das Kontrollkästchen **Alten MID-Auswahlalgorithmus aktivieren**.
   b. Klicken Sie auf **Speichern**.
   c. Konfigurieren Sie die MID-Server-Auswahlkriterien (siehe MID-Server-Konfiguration für Service-Mapping in upgegradeten Bereitstellungen).

MID-Server-Konfiguration für Service-Mapping in upgegradeten Bereitstellungen

Für ServiceNow-Bereitstellungen, die von früheren Versionen auf Istanbul upgegradet wurden, verwendet Service-Mapping den veralteten Algorithmus, um den MID-Server für eine Erkennungsanforderung auszuwählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID Servers besitzen die folgenden Auswahlkriterien, anhand derer Service-Mapping in upgegradeten Bereitstellungen einen MID-Server für eine Erkennungsanforderung auswählt:

- Anwendung – legt fest, mit welcher Anwendung ein MID-Server arbeitet. Stellen Sie es auf Service-Mapping, um diesen MID-Server ausschließlich für Discovery-Anforderungen von Service-Mapping zu reservieren. Alternativ können Sie auf ALL setzen, damit alle ServiceNow-Anwendungen MID-Server verwenden können.

  In früheren Versionen konnten Sie MID Servers konfigurieren, um nur mit Service-Mapping über den Parameter *Capability* zu arbeiten. Wenn Sie bei dieser Konfiguration MID Servers hatten, wurde der Anwendungsparameter beim Upgrade auf Istanbul automatisch auf *ServiceMapping* gesetzt.

- IP-Bereich – schränkt den Betrieb dieses MID-Server auf diesen IP-Bereich ein. Service-Mapping wählt diesen MID-Server nicht für eine Discovery-Anforderung, deren Endpunkt außerhalb dieses IP-Bereichs liegt.

Zusätzlich zum IP-Bereich können Sie einen der MID Servers als Standardserver konfigurieren, der Service-Mapping nutzt. Betriebsinformationen finden Sie unter Standardmäßigen MID-Server in Service-Mapping für upgegradete Bereitstellungen konfigurieren.

In aktualisierten Bereitstellungen wählt Service-Mapping einen MID-Server mit einem veralteten Algorithmus:

- Service-Mappingwählt die MID-Server deren Anwendungskriterien auf *ServiceMapping* oder *ALL* eingestellt sind.
- Standardmäßig wählt Service-Mapping das MID-Server aus, dessen IP-Bereich mit der IP in der Discovery-Anforderung übereinstimmt.
- Wenn Service-Mapping keinen MID-Server mit dem übereinstimmenden IP-Bereich und der übereinstimmenden Anwendung finden kann, wird die Discovery-Anforderung dem Standard-MID-Server zugewiesen.
- Wenn es keinen Standard-MID-Server gibt und keine der MID Servers konfigurierte IP-Bereiche haben, verwendet Service-Mapping einen zufälligen MID-Server .
- Wenn es keinen Standard- MID-Server gibt und kein IP-Bereich stimmt mit der IP in der Discovery-Anforderung überein, kann Service-Mapping den Erkennungsprozess nicht starten.

Im neuen Algorithmus für die Auswahl von MID Servers wird ein zusätzliches Auswahlkriterium verwendet: Fähigkeit. Dadurch kann Service-Mapping ein Netzwerkprotokoll berücksichtigen. Informationen über aktualisierte Auswahlkriterien und den neuen Auswahlalgorithmus für den MID-Server finden Sie unter MID Server-Auswahlalgorithmus wählen.

Standardmäßig verwendet Service-Mapping in allen upgegradeten Bereitstellungen den veralteten Algorithmus, unterstützt jedoch sowohl neue als auch veraltete Algorithmen zur Auswahl eines MID-Servers. Bei Bedarf können Sie den neuen Auswahlalgorithmus MID-Server für Ihre upgegradete Bereitstellung aktivieren. Weitere Informationen finden Sie unter MID Server-Auswahlalgorithmus wählen.

Zugehörige Informationen

IP-Adressbereich für MID Server konfigurieren

Standardmäßigen MID-Server in Service-Mapping für upgegradete Bereitstellungen konfigurieren

In Bereitstellungen, die auf Istanbul oder früher upgegradet werden, verwendet Service-Mapping den standardmäßigen MID Server, wenn kein MID Server mit dem entsprechenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Bereich gefunden werden kann. Durch die Konfiguration eines standardmäßigen MID Servers wird der Erkennungsprozess verbessert.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin
Führen Sie dieses Verfahren nur für Bereitstellungen aus, die auf Istanbul oder früher upgegradet wurden. Führen Sie bei Neuinstallationen die Option Standard-MID-Server für jede Anwendung konfigurieren durch.

Stellen Sie sicher, dass Sie den Namen des MID Servers kennen, den Sie als Standard für Service-Mapping konfigurieren möchten.

Warum und wann dieser Vorgang ausgeführt wird

In aktualisierten Bereitstellungen wählt Service-Mapping einen MID-Server mit einem veralteten Algorithmus:

- Service-Mappingwählt die MID-Server deren Anwendungskriterien auf *`ServiceMapping`* oder *`ALL`* eingestellt sind.
- Standardmäßig wählt Service-Mapping das MID-Server aus, dessen IP-Bereich mit der IP in der Discovery-Anforderung übereinstimmt.
- Wenn Service-Mapping keinen MID-Server mit dem übereinstimmenden IP-Bereich und der übereinstimmenden Anwendung finden kann, wird die Discovery-Anforderung dem Standard-MID-Server zugewiesen.
- Wenn es keinen Standard-MID-Server gibt und keine der MID Servers konfigurierte IP-Bereiche haben, verwendet Service-Mapping einen zufälligen MID-Server .
- Wenn es keinen Standard- MID-Server gibt und kein IP-Bereich stimmt mit der IP in der Discovery-Anforderung überein, kann Service-Mapping den Erkennungsprozess nicht starten.

Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein, um zu den Systemeigenschaften zu navigieren.
2. Klicken Sie auf **Neu**.
3. Konfigurieren Sie die Werte für die neue Eigenschaft wie folgt:

Eigenschaft	Beschreibung
Name	Geben Sie `mid.server.sm_default` ein.
Beschreibung	Geben Sie eine Freitextbeschreibung für die Verwendung dieses MID Servers ein.
Typ	Wählen Sie **Zeichenfolge** aus.
Wert	Geben Sie den Namen des MID Servers ein, den Sie für Service-Mapping als Standard konfigurieren möchten.

4. Klicken Sie auf **Aktualisieren**.

Zugehörige Informationen

Konfiguration des MID Servers für Service-Mapping

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping

Informieren Sie sich über Anmeldeinformationen, Benutzer und Benutzerberechtigungen, die Sie konfigurieren müssen, damit Service-Mapping im privaten Netzwerk Ihrer Organisation Anwendungen erkennen und darauf zugreifen kann.

Konfigurieren Sie die relevanten Anforderungen für eine erfolgreiche Erkennung von oben nach unten:

Hostanmeldeinformationen

Service-Mapping nutzt Hostanmeldeinformationen, um auf Anwendungen zuzugreifen, die auf den entsprechenden Hosts ausgeführt werden. Normalerweise reichen Hostanmeldeinformationen für die Erkennung von oben nach unten aus. Um beispielsweise den HP Service Manager-Anwendungsserver zu erkennen, konfigurieren Sie nur Anmeldeinformationen (SSH-Anmeldeinformationen oder Windows-Anmeldeinformationen) für den Zugriff auf den Server, auf dem diese Anwendung gehostet wird.

Applicative-Anmeldeinformationen

Zur Erkennung mancher Anwendungen benötigt Service-Mapping neben den Anmeldeinformationen des Hosts, auf dem diese Anwendungen ausgeführt werden, noch weitere Anmeldeinformationen. Diese Art von Anmeldeinformationen wird in ServiceNow als Applicative-Anmeldeinformationen bezeichnet. Um beispielsweise ABAP SAP Central Services (ASCS) zu erkennen, konfigurieren Sie zusätzlich zu den Hostanmeldeinformationen auch Applicative-Anmeldeinformationen.

Erweiterte Rechte für Unix-basierte Hosts

Für auf MID Servers konfigurierte Unix-basierte Hosts müssen Sie für alle Unix-basierten Hosts in Ihrer Organisation einem Benutzer Anmeldeinformationen auf sudo-Ebene gewähren. Beispiel: Wenn der ASCS-Hostserver Unix-basiert ist, erteilen Sie einem Benutzer erweiterte Rechte, damit dieser für den Unix-basierten Server Discovery-Befehle ausführen kann.

SNMP-Community Anmeldeinformationen

Konfigurieren Sie die Berechtigungsnachweise für die SNMP-Community so, dass Service-Mapping und Discovery Netzwerkgeräte mit dem SNMP-Protokoll abfragen können. Konfigurieren Sie für Thunder ADC von A10 Networks beispielsweise SNMP-Community-Anmeldeinformationen.

Benutzer oder Benutzerberechtigungen

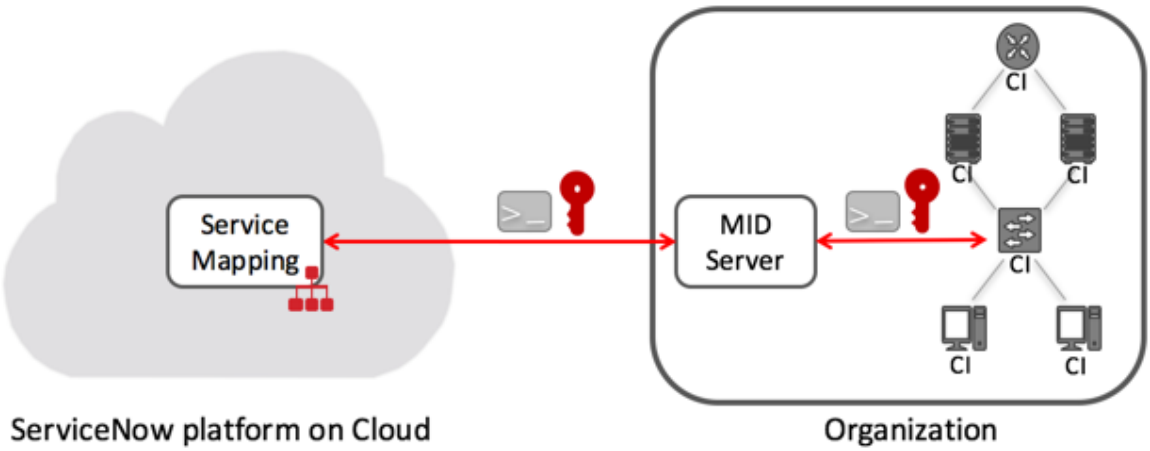
Möglicherweise müssen Sie zusätzliche Benutzer oder Benutzerberechtigungen angeben, um bestimmte Befehle auszuführen oder auf bestimmte Verzeichnisse zuzugreifen. Erteilen Sie für ASCS zum Beispiel einem Benutzer die Berechtigung zum Ausführen von SOAP in der RFC-Tabellenlesefunktion:

Now Platform bietet eine zentralisierte Möglichkeit zum Konfigurieren von Anmeldeinformationen für Discovery, Service-Mapping und andere Anwendungen. Sie können die Anmeldeinformationen für Hosts und Anwendungen nur einmal konfigurieren. Wenn Sie bereits hostbezogene Anmeldeinformationen für eine andere Anwendung konfiguriert haben, müssen Sie dies für Service-Mapping nicht noch einmal tun.

Sie können Anmeldeinformationen bestimmten MID Servers zuweisen oder allgemeine Anmeldeinformationen beibehalten, damit sie von allen MID Serversn verwendet werden können. MID Servers rufen Befehle und Anmeldeinformationen von der ServiceNow Instanz ab und wenden sie an, um CIs im privaten Unternehmensnetzwerk zu erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen MID-Servern zuweisen, damit diese auf CIs zugreifen können



Verwenden Sie die folgenden Richtlinien, um zu entscheiden, für welchen MID-Server Anmeldeinformationen erstellt werden:

- Wenn alle CIs des gleichen CI-Typs dieselben Anmeldeinformationen nutzen, müssen Sie keinen MID-Server für sie angeben. In diesem Fall werden sie standardmäßig für alle MID Servers verwendet.

  Hinweis: Die Angabe des MID-Servers beim Konfigurieren von Anmeldeinformationen ist optional.

- Wenn CIs desselben Typs und im gleichen Netzwerk unterschiedliche Anmeldeinformationen haben, konfigurieren Sie diese Anmeldeinformationen und definieren die Reihenfolge, in der Service-Mapping sie beim Verbindungsaufbau zu diesen CIs verwendet.

Zusätzlich zu den allgemeinen Anmeldeinformationen, die Sie für die MID Servers konfigurieren, müssen Sie auf allen Unix-basierten Hosts in Ihrer Organisation Anmeldeinformationen auf sudo-Ebene konfigurieren.

Wenn MID-Server nicht über ausreichende Anmeldeinformationen verfügt, um auf ein Gerät oder eine Anwendung zuzugreifen, kann sie Nmap-Befehle (Network Mapper) ausführen, um grundlegende Informationen ohne Verwendung von Anmeldeinformationen zu erfassen. Die Discovery ohne Anmeldeinformationen mit Nmap erfordert eine zusätzliche Konfiguration, wie in Nmap auf einem MID-Server installieren und deinstallieren beschrieben ist.

Überprüfen Sie die Liste der Anmeldeinformationen, die erforderlich sind, um Hosts und Anwendungen zu erkennen, die im Basissystem unterstützt werden.

Applikation	CI-Typ	Konfigurationsschritte
Betriebssystem AIX	AIX-Server [cmdb_ci_aix_server]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
IBM z/OS	IBM zOS server-Server [cmdb_ci_ibm_zos_server]	• Führen Sie den USS-Service an Port 22 des z/OS-Servers aus. • Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen . • Gewähren Sie dem Benutzer folgende Berechtigungen: ◦ Zum Schreiben in das /tmp-Verzeichnis ◦ Zum Anzeigen aller Benutzerprozesse ◦ Ausführen von REXX-Skripts.
		Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
		Gewähren Sie dem Benutzer folgende Berechtigungen: • Zum Schreiben in das /tmp-Verzeichnis • Zum Anzeigen aller Benutzerprozesse • Ausführen von REXX-Skripts.
Betriebssystem HP UX	HPUX-Server [cmdb_ci_hpux_server]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
Betriebssystem Linux	Linux-Server [cmdb_ci_linux_server]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
Betriebssystem Solaris	Solaris-Server [cmdb_ci_solaris_server]	Geben Sie Benutzern erweiterte Rechte, damit sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
Betriebssystem Windows	Windows Server [cmdb_ci_windows_server]	Konfigurieren Sie auf Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
		Geben Sie alle unter Für die Hosterkennung erforderliche Anmeldeinformationen beschriebenen erforderlichen Anmeldeinformationen und Berechtigungen an.
A10-Lastenausgleichsmodul	A10 Load Balancer [cmdb_ci_lb_a10]	Konfigurieren Sie die Applicative-Anmeldeinformationen .
		Konfigurieren Sie die SNMP-Anmeldeinformationen .
Windows Azure Active Directory Domain Services	Active Directory-Domänencontroller [cmdb_ci_ad_controller]	Konfigurieren Sie auf Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
AWS DynamoDB	Globale DynamoDB-Tabelle [cmdb_ci_dynamodb_global_table]	• Stellen Sie in der Konsole AWS einen Benutzer mit den folgenden Berechtigungen bereit: AmazonDynamoDBReadOnly-Zugriff und AWSLambdaInvocation-DynamoDB. • Konfigurieren Sie auf der Now Platform® die Anmeldeinformationen AWS mit einem geheimen Schlüssel und einem Zugriffsschlüssel.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
Amazon Web Services (AWS) – Elastic Load Balancing	Load Balancer-Service [cmdb_ci_lb_service]	Konfigurieren Sie die Amazon Web Services-Anmeldeinformationen.
		In Now Platform: Erstellen Sie ein Servicekonto. Setzen Sie die Konto-ID auf die in der AWS-Managementkonsole angezeigte Konto-ID für Amazon ELB.
Amazon Web Services (AWS) – API-Gateway		Konfigurieren Sie die Amazon Web Services-Anmeldeinformationen.
		In Now Platform: Erstellen Sie ein Servicekonto. Legen Sie die Konto-ID auf die Amazon-Konto-ID fest, zu der das API-Gateway gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
		Erteilen Sie einem Benutzer Berechtigungen zum Ausführen der apigateway:GET-Funktion nur für die GET-Aktion in API Gateway.
		Stellen Sie sicher, dass der MID-Server auf der virtuellen Maschine platziert wird, die Teil des zu erkennenden Servicekontos ist.
Amazon Web Services (AWS) – Elastic Compute Cloud (EC2)	Windows-Server [cmdb_ci_windows_server] oder Linux-Server [cmdb_ci_linux_server]	(Beim Hosting auf einem Unix-Server) konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
		In Now Platform: Erstellen Sie ein Servicekonto. Legen Sie die Konto-ID auf die Amazon-Konto-ID fest, zu der das API-Gateway

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
		Der MID-Server muss in der Amazon-Cloud platziert sein.
Amazon Web Services (AWS) – Relational Database Service (RDS)	Cloud-Datenbank [cmdb_ci_cloud_database]	Konfigurieren Sie die Amazon Web Services-Anmeldeinformationen.
		In Now Platform: Erstellen Sie ein Servicekonto. Legen Sie die Konto-ID auf die Amazon-Konto-ID fest, zu der RDS gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
		Der MID-Server muss in der Amazon-Cloud platziert sein.
Amazon Web Services (AWS) – Lambda	Cloud-Funktion [cmdb_ci_cloud_function]	Konfigurieren Sie die Amazon Web Services-Anmeldeinformationen.
		In Now Platform: Erstellen Sie ein Servicekonto. Legen Sie die Konto-ID auf die Amazon-Konto-ID fest, zu der AWS Lambda gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
		Stellen Sie sicher, dass der MID-Server auf der virtuellen Maschine platziert wird, die Teil des zu erkennenden Servicekontos ist.
		Gewähren Sie einem Benutzer die Berechtigung zum Ausführen der ListFunctions-API mit der Ressource: arn:aws:lambda:region:account-id: function:function-name. Gewähren Sie einem Benutzer die Berechtigung zum Ausführen der GetFunction-API mit der Ressource: „*“.
Apache Tomcat	Tomcat [cmdb_ci_app_server_tomcat]	Geben Sie dem Benutzer erweiterte Rechte, damit er

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Beim Hosting auf einem Unix-Server) konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows -Server) Konfigurieren Sie auf der Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Apache Tomcat WAR	Tomcat WAR [cmdb_ci_app_server_tomcat_war]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Beim Hosting auf UNIX) konfigurieren Sie auf der Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows -Server) Konfigurieren Sie auf der Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
Apache-Webserver	Apache-Webserver [cmdb_ci_apache_web_server]	(Unter UNIX) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		Erteilen Sie auf dem Server mit dem Apache-Webserver die Benutzerberechtigung zur Ausführung des folgenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Befehls: `$APACHEHOME/bin/httpd -V`.
		Stellen Sie auf dem Server mit dem Apache-Webserver sicher, dass die Datei $APACHEHOME/bin/envvar mit dem richtigen nativen Bibliothekspfad konfiguriert ist.
		(Beim Hosting auf UNIX) konfigurieren Sie auf der Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows -Server) Konfigurieren Sie auf der Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
App TNS-Dienst	[cmdb_ci_appl_ora_tns]	Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Beim Hosting auf einem Windows -Server) Konfigurieren Sie auf der Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
		(Beim Hosting auf Linux oder UNIX) konfigurieren Sie auf der Now Platformdie SSH-Anmeldeinformationen .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
F5 BIG-IP Global Traffic Manager (GTM) und F5 BIG-IP Local Traffic Manager (LTM)	Load Balancer-Service [cmdb_ci_lb_service]	• Konfigurieren Sie die SNMP-Anmeldeinformationen . **Hinweis:** Wenn Sie keine SSH-Anmeldeinformationen verwenden möchten, können Sie mit der REST API eine Verbindung zu F5-BIG-IP-Geräten herstellen. • (Optional) Wenn die Anmeldeinformationen für iRules oder SNMP-Community nicht ausreichen, um ausgehende Verbindungen zu ermitteln, konfigurieren Sie die SSH-Anmeldeinformationen auf Now Platform. Service-Mapping verwendet die SSH-Anmeldeinformationen zum Abrufen von Verbindungen, die nicht von CMDB stammen. Das Erkennen von Verbindungen mithilfe des SSH-Protokolls ist ein Failover-Mechanismus für die SNMP-basierte Discovery. • Um die Mitglieder des Lastenausgleichsmodul-Pools erfolgreich zu erkennen, navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties] und legen die Systemeigenschaft *sys_db_bigpipe.displayservicenames* auf **false** fest. • Benutzen Sie die Anmeldeinformationen zur Standardauthentifizierung für die Discovery über REST. • Geben Sie für die Horizontal-Discovery mit Discovery Berechtigungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		zum Ausführen der folgenden APIs an: ◦ `https://" get_attr {"managementIP"}"/mgmt/tm/sys/global-settings` ◦ `https://" get_attr {"managementIP"}"/mgmt/tm/sys/hardware` ◦ `https://"get_attr {"managementIP"}"/mgmt/tm/sys/failover` ◦ `https://"get_attr {"managementIP"}"/mgmt/tm/cloud/net/self` ◦ `https://"get_attr {"managementIP"}"/mgmt/tm/net/interface` ◦ `https://"get_attr {"managementIP"}"/mgmt/tm/net/self` ◦ `https://"get_attr {"managementIP"}"/mgmt/tm/net/vlan` ◦ `https://"get_attr {"managementIP"}"/mgmt/tm/ltm/pool` ◦ `https://"get_attr {"managementIP"}"/mgmt/tm/gtm/wideip` ◦ `https://"get_attr {"managementIP"}"/mgmt/tm/cm/traffic-group/` ◦ `https://"get_attr {"managementIP"}"/mgmt/tm/cm/device` Geben Sie für die Top Down-Discovery mit Service-Mapping Berechtigungen zum Ausführen der folgenden APIs an: ◦ `https://" get_attr {"managementIP"}"/mgmt/`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		tm/ltm/"get_attr {"irule"} ◦ https://" get_attr {"managementIP"}"/mgmt/tm/ltm/virtual/~Common~"get_attr {"vip_name"} ◦ https://" get_attr {"computer_system.managementIP"}"/mgmt/tm/ltm/pool/"get_attr {"pool_name"}"/members? • (Optional) Für die Top Down-Discovery mit Service-Mapping, konfigurieren Sie Applicative-Anmeldeinformationen . • (Optional) Für die Top Down-Discovery mit Service-Mapping, stellen Sie einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle bereit: ◦ Bigpipe-Befehle (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 9) ◦ Bigpipe- und Traffic Management Shell-Befehle (TMSH) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 10) ◦ TMSH-Befehle (Traffic Management Shell) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 11) ◦ Erweiterte Befehle für die Traffic Management Shell (TMSH) (für BIG-IP LTM F5 oder BIG-IP GTM F5 Version 10, 11 und 12) ◦ Der *show cm traffic-group - get command* für die Erkennung von F5 BIG-IP Device Service Clustering • (Optional) Für die Top Down-Discovery mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Service-Mapping , geben Sie dem Benutzer erhöhte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
BMC CTRL-M Enterprise Manager	Control-M [cmdb_ci_appl_controlm]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
		(Beim Hosting auf einem Linux- oder UNIX -Server) (Optional) Konfigurieren Sie auf der Now Platformdie SSH-Anmeldeinformationen .
BMC CTRL-M Gateway	Control-M [cmdb_ci_appl_controlm]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
		(Beim Hosting auf einem Linux- oder UNIX -Server) (Optional) Konfigurieren Sie auf der Now Platform, konfigurieren Sie cc.
BMC IT Asset Management (ITAM)	ITAM Asset Center [cmdb_ci_appl_itam]	Konfigurieren Sie auf der Seite Now Platformeinen BS-Benutzer Windows mit Berechtigungen für den Zugriff auf die ITAM-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Registry (siehe Windows-Anmeldeinformationen) .
CA Identity Manager-Bereitstellungsserver	CA Identity Manager-Bereitstellungsserver [cmdb_ci_appl_ca_id_man]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Cadebill Interconnect	Interconnect [cmdb_ci_inter_connect]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
Cadebill Interconnect-Instanz	Interconnect-Instanz [cmdb_ci_interconnect_instance]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
Cisco Application Control Engine ACE (unter Cisco CSM)	ACE [cmdb_ci_lb_ace]	Konfigurieren Sie unter Now Platformdie Applicative-Anmeldeinformationen .
		Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
		Konfigurieren Sie auf Now Platformdie SNMP-Community-Anmeldeinformationen wie in SNMP-Anmeldeinformationen beschrieben.
Cisco CallManager	Cisco CallManager [cmdb_ci_appl_cisco_call_man]	(Beim Hosting auf einem Server Linux oder UNIX) (Optional) Konfigurieren Sie auf der Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows -Server) Konfigurieren Sie auf der Now Platformeinen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben.
Cisco Global Site Selector (GSS)	Load Balancer-Service [cmdb_ci_lb_service]	Konfigurieren Sie die SNMP-Community-Anmeldeinformationen wie in SNMP-Anmeldeinformationen beschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen.
		Geben Sie einen Benutzer an, der zum Ausführen der Abfrage für die Domänenliste, die DNS-Regelausgabe und die VIP-Antwort berechtigt ist, um die ausgehenden Verbindungen von GSS abzurufen.
Citrix Delivery Controller	Delivery Controller [cmdb_ci_appl_delivery_controler]	• Konfigurieren Sie die Windows-Anmeldeinformationen, um auf den Hostcomputer zuzugreifen. • Stellen Sie sicher, dass PowerShell für Discovery auf Ihren MID Servern installiert ist. Für die für die Citrix-Discovery verwendeten Muster müssen PowerShell-Befehle ausgeführt werden können. • Für Betriebssystembenutzer müssen Sie „Get-XDSite“ ausführen. Der Citrix Studio-Administrator muss Berechtigungen erteilen. • (Optional) Für die Top Down-Discovery mit Service-Mapping installieren Sie auf dem Citrix Delivery Controller das Modul Citrix.Broker. • (Optional) Für die Top Down-Discovery mit Service-Mapping, erstellen Sie einen Benutzer mit Berechtigung zum Ausführen von PowerShell-Befehlen. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
Citrix-Nutzungssammler	Citrix Collector [cmdb_ci_appl_citrix_collector]	• Konfigurieren Sie die Applicative-Anmeldeinformationen . • Konfigurieren Sie einen Benutzer mit Berechtigungen zum Ausführen von PowerShell-Befehlen auf dem Citrix-Server. • (Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platformeinen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben. **Hinweis:** Um diese Anmeldeinformationen später für XenAPP zu verwenden, legen Sie das Attribut **Alias für Anmeldeinformationen** auf cmdb_ci_appl_citrix_xenapp fest. Um diese Anmeldeinformationen später für Citrix zu verwenden, legen Sie das Attribut **Alias für Anmeldeinformationen** auf cmdb_ci_appl_citrix_collector fest. • Gewähren Sie zum Erkennen von Epic die Berechtigung zum Ausführen des Befehls `afarm`. • Erteilen Sie einem Benutzer die Berechtigung zum Lesen und Abfragen des Citrix-Repository: ◦ Bei Versionen 4.5 und höher ein PowerShell-Skript vom XenApp-Server. ◦ Für Versionen vor 4.5 ein MicrosoftMicrosoft Azure

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Event Hubs Visual Basic Script (VBScript) vom Citrix-Präsentationsserver • (Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen . **Hinweis:** Um diese Anmeldeinformationen später für XenAPP zu verwenden, legen Sie das Attribut *Credential alias* auf cmdb_ci_appl_citrix_xenapp fest. Um diese Anmeldeinformationen später für Citrix zu verwenden, legen Sie das Attribut *Credential alias* auf cmdb_ci_appl_citrix_collector fest.
Citrix Presentation Server/ Citrix XenApp **Hinweis:** Citrix XenApp ist ab Release XenApp 5 der neue Name für Presentation Server.	Citrix XenAPP oder Presentation Server [cmdb_ci_appl_citrix_xenapp]	• Konfigurieren Sie auf der Now Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
Citrix Netscaler	Citrix Netscaler [cmdb_ci_lb_netscaler]	• Konfigurieren Sie die SNMP-Anmeldeinformationen . **Hinweis:** Sie haben auch die Möglichkeit SSH-Anmeldeinformationen zu verwenden. Wenn jedoch die Nutzlast der an die Instanz zurückgegebenen Daten groß ist, kann der Discovery-Prozess fehlschlagen. Verwenden Sie in diesem Fall stattdessen SNMP-Anmeldeinformationen. • (Optional) Gewähren Sie einem Benutzer den Lesezugriff auf die *NS.conf*-Konfigurationsdatei, wenn Sie keine SNMP- oder SSH-Anmeldeinformationen angeben möchten. • Benutzen Sie die Anmeldeinformationen zur Standardauthentifizierung für die Discovery über REST. Service-Mapping verwendet die SSH-Anmeldeinformationen zum Abrufen von Verbindungen, die nicht von CMDB stammen. Das Erkennen von Verbindungen mithilfe des SSH-Protokolls ist ein Failover-Mechanismus für die SNMP-basierte Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
Citrix NetScaler Global Server-Lastenausgleichsmodul	Load Balancer-Service [cmdb_ci_lb_service]	• Konfigurieren Sie die SNMP-Anmeldeinformationen . **Hinweis:** Sie haben auch die Möglichkeit SSH-Anmeldeinformationen zu verwenden. Wenn jedoch die Nutzlast der an die Instanz zurückgegebenen Daten groß ist, kann der Discovery-Prozess fehlschlagen. Verwenden Sie in diesem Fall stattdessen SNMP-Anmeldeinformationen. • (Optional) Gewähren Sie einem Benutzer den Lesezugriff auf die *NS.conf*-Konfigurationsdatei, wenn Sie keine SNMP- oder SSH-Anmeldeinformationen angeben möchten. • Benutzen Sie die Anmeldeinformationen zur Standardauthentifizierung für die Discovery über REST.
APK verbinden	Connect-It Service [cmdb_ci_appl_connectit]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platformeinen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben.
		(Beim Hosting auf einem Linux- oder Unix-Server) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
EMC Documentum	Documentum DocBase [cmdb_ci_appl_doc_docbroker]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Linux- oder Unix-Server) (Optional) Konfigurieren Sie auf der Now Platformdie SSH-Anmeldeinformationen .
Epic	epicd app server [cmdb_ci_epicd_app_server] epic agent [cmdb_ci_epic_agent] epic cache [cmdb_ci_epic_cache] epicd [cmdb_ci_endpoint_epicd]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Linux- oder Unix-Server) (Optional) Konfigurieren Sie auf der Now Platformdie SSH-Anmeldeinformationen .
FormEngine	Oracle Forms Engine [cmdb_ci_appl_ora_forms]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
Google Cloud Platform	Cloud-Servicekonto [cmdb_ci_cloud_service_account]	• Stellen Sie einen leseberechtigten Benutzer bereit, der zur Verwendung der folgenden API-Elemente berechtigt ist. • Konfigurieren Sie auf der Now Platform Google API-Anmeldeinformationen.
HAProxy	HAProxy Load Balancer [cmdb_ci_lb_haproxy]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Linux- oder Unix-Server) (Optional) Konfigurieren Sie auf der Now Platformdie SSH-Anmeldeinformationen .
HP Operations Manager	HP Operations Manager [cmdb_ci_appl_hp_operations]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
HP Service Manager-Anwendungsserver	HP Service Manager [cmdb_ci_appl_hp_service]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Linux- oder Unix-Server) (Optional) Konfigurieren Sie auf der Now Platformdie SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
HP Service Manager-Index	HP SM-Indexserver [cmdb_ci_appl_hp_index]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Linux- oder Unix-Server) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
HP Service Manager Knowledge Base	HP SM KnowledgeBase [cmdb_ci_appl_hp_sm_kb]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		auf der Now Platform SSH-Anmeldeinformationen .
HP Quality Center	HP Quality Center [cmdb_ci_appl_hp_qc]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
HP UCMDB	HP uCMDB [cmdb_ci_app_server_hp_ucmdb]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
IBM Cloud Platform	Cloud-Servicekonto [cmdb_ci_cloud_service_account]	Konfigurieren Sie auf der Now Platform die IBM-Anmeldeinformationen zum Zugriff auf das IBM-Konto.
IBM WebSphere Message Broker	IBM WebSphere Message Broker [cmdb_ci_appl_ibm_wmb]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie unter Now PlatformSSH-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle: • "source " + $directory + "/mqsiprofile" • "echo $MQSI_VERSION " • $directory + "/mqsireportbroker " + $name • $directory + "/mqsibrowse " + $name + " -t BROKERRESOURCES " Legen Sie das Attribut *Credential alias* auf [cmdb_ci_appl_ibm_wmb] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.
IBM CTRL-M Server	Control-M [cmdb_ci_appl_controlm]	(Unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Beim Hosting auf Windows) konfigurieren Sie auf der Now Platformdie Windows-Anmeldeinformationen .
IBM CICS Transaction Gateway CTG	IBM CTG [cmdb_ci_appl_ibm_ctg]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
IBM Customer Information Control System (CICS)	IBM CICS [cmdb_ci_appl_ibm_cics]	(Unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
IBM DB2	DB2-Instanz [cmdb_ci_db_db2_instance] **Hinweis:** Ab CMDB CI-Klassenmodelle Version 1.67.0 wurde die Bezeichnung in **DB2-Subsystem**umbenannt.	• (Unter Linux gehostet) Gewähren Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann. • (Beim Hosting auf Windows) konfigurieren Sie auf der Now Platformdie Windows-Anmeldeinformationen . Legen Sie das Tag-Attribut auf [cmdb_ci_db_db2_instance] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Optional) Um Verbindungen zu IBM DB2 zu erkennen, konfigurieren Sie SSH-Anmeldeinformationen für einen Benutzer, der berechtigt ist, die folgenden Befehle auszuführen: ◦ `db2 list tablespaces` ◦ "db2cmd /c /w /i db2 -tvf "+$ script_name • (Unter z/OS gehostet) Gewähren Sie dem Benutzer die folgenden Berechtigungen: ◦ Zum Schreiben in das /tmp-Verzeichnis ◦ Zum Anzeigen aller Benutzerprozesse ◦ Ausführen von REXX-Skripts. ◦ Einlesen des db2-Ordners. • (Unter z/OS gehostet) Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
IBM J2EE EAR	[cmdb_ci_app_server_ws_ear]	(Nur unter Linux) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf Windows) konfigurieren Sie auf der Now Platformdie Windows-Anmeldeinformationen .
Erkennung von IBM PowerHA Cluster (HACMP)	• Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group] • UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	Konfigurieren Sie einen UNIX-Benutzer mit Berechtigungen zum Ausführen aller in der offiziellen IBM-Dokumentation definierten Befehle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
	• UNIX-Clusterknoten [cmdb_ci_unix_cluster_node] • AIX-Server [cmdb_ci_aix_server] • UNIX-Cluster [cmdb_ci_unix_cluster] • Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	
IBM Tivoli Access Manager WebSEAL- oder IBM Security Access Manager(ISAM)-Appliance	Webseal [cmdb_ci_app_server_webseal]	(Nur für ISAM-Gerät) Konfigurieren Sie die Applicative-Anmeldeinformationen für den Benutzer, der berechtigt ist, die folgenden REST-Befehle auszuführen: • /reverseproxy – zum Abrufen von Daten über Reverse-Proxy und -Instanzen • /wga/reverseproxy/"+ ${junctionstable[].instance}+"/junctions – zum Abrufen von Verbindungen für jede Instanz • /wga/reverseproxy/ " + $instance_name + "/junctions?junctions_id=" + $junction_name – zum Abrufen von Weiterleitungs-URLs für die Einstiegspunktverbindung
		(Nur für ISAM-Appliance) Stellen Sie sicher, dass im System die cURL-Befehle für die Erkennung verwendet werden können: • Definieren Sie auf dem MID-Server, der für die Erkennung der ISAM-Appliance verwendet wird, die Variable PATH, die die Installation des cURL-Pakets für die entsprechenden MID-Server-Benutzer enthält. • Konfigurieren Sie Berechtigungen zum Ausführen der Datei

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		`curl.exe` für den entsprechenden MID-Server-Benutzer.
		(Beim Hosting auf Linux) Konfigurieren Sie auf der Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf Windows) konfigurieren Sie auf der Now Platformdie Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
IBM Virtualisierung und Hardware Management Console (HMC)	• HMC-Server • IBM-Frame • LPAR-Instanz (Logische Partition) Eine LPAR ist das Äquivalent zu einer virtuellen Maschine bei IBM. • LPAR-Ressource	• Stellen Sie sicher, dass die folgenden Anwendungen aktuell sind: ◦ Muster für Discovery und Service-Mapping ◦ CMDB CI-Klassenmodelle • Stellen Sie sicher, dass Sie für die folgenden HMC-Befehle berechtigt sind: ◦ `lssyscfg` ◦ `lshmc` ◦ `lshwres` • Vergewissern Sie sich, dass Sie für den folgenden AIX-Befehl (LPAR) berechtigt sind: `lparstat -i`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Hinweis: Der Befehl „`lparstat -i`" ist zusätzlich zu den für die AIX-Server-Discovery erforderlichen Befehlen erforderlich. Weitere Informationen zur AIX-Server-Discovery finden Sie unter Erkennung von AIX-Servern. Eine Liste der AIX-Befehle finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. • Konfigurieren Sie SSH-Anmeldeinformationen für Now Platform. Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .
IBM WebSphere Application Server	IBM Websphere [cmdb_ci_app_server_websphere]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf Windows) konfigurieren Sie auf der Now Platformdie Windows-Anmeldeinformationen .
		(Unter z/OS gehostet) Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
		(Unter z/OS gehostet) Gewähren Sie dem Benutzer die folgenden Berechtigungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		• Zum Schreiben in das /tmp-Verzeichnis • Zum Anzeigen aller Benutzerprozesse • Zum Ausführen von REXX-Skripts • Zum Ausführen von Befehlen mit oeconsol • Zur Ausführung des Befehls, mit dem Informationen über die WebSphere Application Server-Aufgabe abgerufen werden: `"oeconsol 'D OMVS,A=ALL' | grep "+ $taskname`. • Zum Lesen des Inhalts des WAS-Installationsordners und der Berechtigung zum Lesen von was.env.file, worin sich die Installationsvariablen befinden.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
IBM WebSphere DataPower	DataPower [cmdb_ci_app_server_datapower]	SNMP-Anmeldeinformationen SNMP-Anmeldeinformationen sind für die Verwendung der folgenden SNMP-Abfragen erforderlich: • Für die Horizontal-Discovery des Hostservers von DataPower [cmdb_ci_datapower_server]: ◦ 1.3.6.1.2.1.1.1 ◦ 1.3.6.1.2.1.1.5

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		◦ 1.3.6.1.2.1.4.20.1 ◦ 1.3.6.1.2.1.2.2.1 ◦ 1.3.6.1.4.1.14685.3.1.196.1 ◦ 1.3.6.1.4.1.14685.3.1.11.1 ◦ 1.3.6.1.4.1.14685.3.1.112.1 • Für die Top Down-Discovery des Hostservers für DataPower [cmdb_ci_datapower_server]: ◦ 1.3.6.1.2.1.1.1 ◦ 1.3.6.1.2.1.1.5 ◦ 1.3.6.1.4.1.14685.3.1.11.1 Applicative-Anmeldeinformationen Neben SNMP-Anmeldeinformationen sind zum Erkennen von DataPower-Anwendungsdomänen auch Applicative-Anmeldeinformationen erforderlich, auch als logische CIs bekannt. Darüber hinaus werden SNMP- und Applicative-Anmeldeinformationen für die Top Down-Discovery von Anwendungsbeziehungen (entsprechende DataPower-Anwendungsdomäne) verwendet. Benutzer mit Berechtigungen zum Ausführen von SOAP Damit eine Top Down-Discovery für den DataPower-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Webservice und die MQ-Verbindung ausgeführt werden kann, sind Berechtigungen zum Ausführen von SOAP-Abfragen erforderlich.
IBM WebSphere Message Broker-Flow	WMB Flow [cmdb_ci_appl_wmb]	(Auf Unix-Server) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		Stellen Sie einem Benutzer des IBM-Betriebssystems WebSphere Message Broker Berechtigungen zum Ausführen des WebSphere Message Broker-Service bereit.
		(Beim Hosting auf Windows) konfigurieren Sie auf der Now Platformdie Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie unter Now PlatformSSH-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle: • "source " + $directory + "/mqsiprofile" • "echo $MQSI_VERSION “ • $directory + "/mqsireportbroker " + $name • $directory + "/mqsibrowse " + $name + " -t BROKERRESOURCES “ Legen Sie das Attribut *Credential alias* auf [cmdb_ci_appl_ibm_wmb] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Anmeldeinformationen für dieses CI später in Mustern verwenden.
IBM WebSphere Message Broker	IBM WebSphere Message Broker [cmdb_ci_appl_ibm_wmb]	(Unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen. Legen Sie das Attribut *Credential alias* auf [cmdb_ci_appl_ibm_wmb] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen.
		Stellen Sie einem Benutzer des IBM-Betriebssystems WebSphere Message Broker Berechtigungen zum Ausführen des WebSphere Message Broker-Service bereit.
IBM MQ (früher IBM WebSphere MQ)	IBM MQ Manager (früher IBM WebSphere MQ) [cmdb_ci_appl_ibm_wmq]	(Unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		Konfigurieren Sie die Applicative-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle: • (Auf Windows-Server) "echo display QMSTATUS ALL | runmqsc -e " + $queue_manager – zum Abrufen des Status des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Warteschlangenmanagers (QM) • (Auf Windows-Server) "echo display QMGR ALL | runmqsc -e " + $queue_manager – for getting the complete information about QM. • (Auf Unix-Server) "echo \" display QMSTATUS ALL \" | runmqsc " + $queue_manager – zum Abrufen des Status des QM • (Auf Unix-Server) "echo \" display QMGR ALL \" | runmqsc " + $queue_manager – zum Abrufen von vollständigen Informationen über den QM • (Auf Unix-Server) "echo \" display queue(" + $entry_point.queue + ") \" | runmqsc " + $queue_manager – zum Abrufen von Informationen über die EP-Warteschlange
		(Beim Hosting auf Windows) konfigurieren Sie auf der Now Platformdie Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie SSH-Anmeldeinformationen . Legen Sie beim Konfigurieren der Anmeldeinformationen für das Betriebssystem das Attribut *Credential alias* auf cmdb_ci_appl_ibm_wmq fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden. (Optional) Um IBM MQ-Verbindungen zu finden, konfigurieren Sie SSH-Anmeldeinformationen für einen Benutzer mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Berechtigungen zum Ausführen der folgenden Befehle: • "echo \" display queue("+ $entry_point.queue +") \" | runmqsc "+ $queue_manager • "echo \" display QMSTATUS ALL \" | runmqsc "+ $queue_manager • echo \" display QMGR ALL \" | runmqsc "+ $queue_manager
		(Unter z/OS gehostet) Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
		(Unter z/OS gehostet) Gewähren Sie dem Benutzer die folgenden Berechtigungen: • Zum Schreiben in das /tmp-Verzeichnis • Zum Anzeigen aller Benutzerprozesse • Zum Ausführen von REXX-Skripts • Zum Ausführen von Befehlen mit oeconsol • Zur Ausführung von MQ-Befehlen
IBM MQ-Warteschlange (früher IBM WebSphere MQ-Warteschlange)	IBM MQ-Warteschlange (früher IBM WebSphere MQ-Warteschlange) [cmdb_ci_appl_ibm_wmq_queue]	(Auf Unix-Server) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		Konfigurieren Sie die Applicative-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		• dspmq – zum Abrufen von Informationen über den Warteschlangenmanager • "echo \" display queue(" + $entry_point.queue + ") \" | runmqsc " + $queue_manager – zum Abrufen von Informationen über die Warteschlange • "echo \" display clusqmgr(*) conname \" | runmqsc " + $queue_manager – zum Abrufen aller Zeilen des Warteschlangenmanagers (QM) des Clusters • "echo \" display qstatus(" + $entry_point.queue + ") TYPE(HANDLE) OPENTYPE(INPUT) CONNAME PID \" | runmqsc " + $queue_manager – zum Abrufen von Informationen über den Status der Warteschlange
		(Beim Hosting auf einem Unix-Server) konfigurieren Sie auf der Now PlatformSSH-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle: • dspmq echo \" display queue("+ $entry_point.queue +") \" | runmqsc "+ $queue_manager • (Optional) "echo \" display qcluster("+$rqmname +") \" | runmqsc "+ $queue_manager • (Optional) "echo \" dischl(*) CHLTYPE(SDR) CONNAME XMITQ WHERE(XMITQ EQ "+$xmit_name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		+")\" | runmqsc "+ $queue_manager • (Optional) "echo \" display clusqmgr(*) conname \" | runmqsc "+ $queue_manager • (Optional) "echo \" display qstatus("+ $entry_point.queue +") TYPE(HANDLE) OPENTYPE(INPUT) CONNAME PID \" | runmqsc "+ $queue_manager Legen Sie beim Konfigurieren der Anmeldeinformationen für das Betriebssystem das Attribut *Credential alias* auf cmdb_ci_appl_ibm_wmq fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.
		(Beim Hosting auf Windows) konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der folgenden Befehle: • dspmq echo \" display queue("+ $entry_point.queue +") \" | runmqsc "+ $queue_manager • (Optional) "echo \" display qcluster("+$rqmname +") \" | runmqsc "+ $queue_manager • (Optional) "echo \" dischl(*) CHLTYPE(SDR) CONNAME XMITQ WHERE(XMITQ EQ "+$xmit_name +")\" | runmqsc "+ $queue_manager • (Optional) "echo \" display clusqmgr(*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		conname \" | runmqsc "+ $queue_manager • (Optional) "echo \" display qstatus("+ $entry_point.queue +") TYPE(HANDLE) OPENTYPE(INPUT) CONNAME PID \" | runmqsc "+ $queue_manager Legen Sie beim Konfigurieren der Anmeldeinformationen für das Betriebssystem das Attribut *Credential alias* auf cmdb_ci_appl_ibm_wmq fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden..
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
IBM WebSphere Portal	WebSphere-Portal [cmdb_ci_appl_websphere_portal]	(Nur unter Linux) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Interconnect Web Service	Interconnect [cmdb_ci_inter_connect]	(Beim Hosting auf einem Unix-Server) Konfigurieren Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		auf der Now Platform SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
Jboss	JBoss [cmdb_ci_app_server_jboss]	Geben Sie Benutzern erweiterte Rechte, damit sie Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen können.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Jboss-Modul	Jboss-Modul [cmdb_ci_app_server_jb_module]	(Auf Unix-Server) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
JRun	JRun [cmdb_ci_app_server_jrun]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
JRun WAR Inc	JRun WAR [cmdb_ci_app_server_jrun_war]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
Microsoft Azure-Websites	Cloud-Webserver [cmdb_ci_cloud_webserver]	Fügen Sie in Now Platform einen Azure-Service-Prinzipal hinzu und richten Sie ein Cloud-Konto für Azure ein. Legen Sie für die Konto-ID den Azure-Service-Prinzipal fest, der in der Microsoft Azure-Konsole angezeigt wird.
Microsoft Azure-Lastenausgleichsmodul	Load Balancer-Service [cmdb_ci_lb_service]	Konfigurieren Sie auf der Now Platform einen Azure-Dienstprinzipal, und richten Sie ein Cloud-Konto für Azure ein. Legen Sie für die Konto-ID den Azure-Service-Prinzipal fest, der in der Microsoft Azure-Konsole angezeigt wird.
Microsoft Azure SQL-Datenbank	Cloud-Datenbankregel [cmdb_ci_cloud_database]	Fügen Sie in Now Platform einen Azure-Service-Prinzipal

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		hinzu und richten Sie ein Cloud-Konto für Azure ein. Legen Sie für die Konto-ID den Azure-Service-Prinzipal fest, der in der Microsoft Azure-Konsole angezeigt wird.
Microsoft Dynamic CRM	Dynamische CRM-Komponente [cmdb_ci_appl_ms_dynamic_crm]	Konfigurieren Sie auf Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft BizTalk Orchestration	BizTalk Orchestration [cmdb_ci_appl_biztalk_orch]	Konfigurieren Sie auf Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft BizTalk Server	BizTalk [cmdb_ci_appl_biztalk]	Konfigurieren Sie auf Now Platformeinen Domänenbenutzer für den Zugriff auf das Betriebssystem Windows wie in Windows-Anmeldeinformationen beschrieben.
Microsoft Exchange-Back-End-Server	ExchangeBackEndServer [cmdb_ci_exchange_backend]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
		Konfigurieren Sie die für die Hosterkennung erforderlichen Anmeldeinformationen für einen Windows-Server.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Hosts auf dem MID-Server konfigurieren .
Microsoft Exchange-Front-End-Server	ExchangeFrontEndServer [cmdb_ci_exchange_frontend]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
		Konfigurieren Sie die für die Hosterkennung erforderlichen Anmeldeinformationen für einen Windows-Server.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft FAST Search Server	Fast Search [cmdb_ci_appl_fastsearch]	Erstellen Sie einen Benutzer mit der Berechtigung zum Lesen der folgenden Dateien: • `install_directory +"\etc\VERSION.xml` • `und install_directory +"\etc\CSConfig.xml`
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft Exchange Hub Transport-Server Microsoft Exchange Postfach Microsoft Exchange CAS	ExchangeHub [cmdb_ci_exchange_hub] Exchange MailBox [cmdb_ci_exchange_mailbox] Exchange-Clientzugriffsserver [cmdb_ci_exchange_cas]	• Konfigurieren Sie auf der Now Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben. Verwenden Sie als Windows-Anmeldeinformationen Anwendername und Passwort des Microsoft Exchange Server-Administrators. Zum Beispiel Anwendername: local\administrator und Passwort: Are1300.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Hinweis: Wenn Sie Windows-Anmeldeinformationen für einen anderen Benutzer als den Microsoft Exchange Server-Administrator konfigurieren, verwendet Service-Mapping die Traffic-basierte Discovery, die zur Zuordnung aller Microsoft Exchange-Clients führt. • (Für Exchange CAS 2010 und 2013, 2016) Konfigurieren Sie auf der Now Platform Applicative-Anmeldeinformationen, indem Sie den CI-Typ auf „Exchange-Postfach“ einstellen. **Warnung:** Verwechseln Sie den CI-Typ der Exchange Mailbox nicht mit dem CI-Typ des Exchange Mailbox-Servers. Service-Mapping verwendet diese Applicative-Anmeldeinformationen für den Zugriff auf den Ordner „of/Servers/Servers.slab“ im Admin Center (EAC) Key Exchange. Service-Mapping verwendet auch die Applicative-Anmeldeinformationen, um die folgenden PowerShell-Befehle für MID Serversauszuführen: ◦ Get-ExchangeServer ◦ Get-ExchangeServer ◦ Get-Mailboxserver ◦ Get-ClusteredMailBoxServerStatus ◦ Get-ExchangeServer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		◦ Get-StorageGroup ◦ Get-MailboxDatabase • (Für Microsoft Exchange CAS 2010 und 2016) Installieren Sie das Microsoft.Exchange.Management.PowerSh Modul auf dem Windows Server, der Microsoft Exchange-CAS hostet. • (Für Microsoft Exchange CAS 2007) Installieren Sie das Microsoft.Exchange.Management.PowerSh Modul auf dem Windows Server, der Microsoft Exchange-CAS hostet. • (Für Microsoft Exchange CAS 2007, 2010) Laden Sie das rctrlx-Tool zum Ausführen von PowerShell-Befehlen auf Now Platform hoch, wie in Datei rctrlx.exe auf MID Servers hochladen beschrieben. • (Für Microsoft Exchange CAS 2007 und 2010) Statten Sie einen Exchange Mailbox-Betriebssystem-Benutzer mit den Rechten zum Ausführen von Exchange-Services unter Windows und der Berechtigung zum Abfragen des Exchange-Repositorys aus: Konfigurieren Sie auf der Now Platform die Windows-Anmeldeinformationen , indem Sie das Attribut *Credential alias* auf [cmdb_ci_exchange_mailbox] einstellen. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		WinRM-Hosts auf dem MID-Server konfigurieren . • Vergewissern Sie sich, dass Sie den Einstiegspunkt kennen, der zum Erkennen des Microsoft Exchange-Servers erforderlich ist. Verwenden Sie die URL für den Outlook-Webzugriff im folgenden Format: `http(s)://<hostname>:<port>/owa` Zum Beispiel `http(s)://myhost:<443>/owa`
Microsoft Identity Integration Server	IIFP [cmdb_ci_directory_iifp]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
Microsoft Internet Information Services (IIS)	Microsoft IIS-Webserver [cmdb_ci_microsoft_iis_web_server]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen . (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Virtuelles Verzeichnis für Microsoft Internet Information Services (IIS)	Virtuelles IIS-Verzeichnis [cmdb_ci_iisdirectory]	Konfigurieren Sie auf der Now Platform die folgenden Anmeldeinformationen: • Windows-Anmeldeinformationen • Applicative-Anmeldeinformationen Verifizieren Sie den Lesezugriff auf die folgenden Dateien: • `web.config`: Mögliche Speicherorte `$entry_point.path + „Web.config“` oder `$entry_point.path + „\Web.config“` • `maschine.config`: möglicher Speicherort `„dir \“C:\Windows\Microsoft.NET\“`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		• (Optional) Um ADO.NET-Verbindungen zu erkennen, legen Sie das Attribut *Credential alias* auf [cmdb_ci_iisdirectory] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Microsoft Message Queuing (MSMQ)	MSMQ [cmdb_ci_appl_msmq]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
Microsoft .NET Framework	.NET-Anwendung [cmdb_ci_appl_dot_net]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen . (Optional) Um ADO.NET-Verbindungen zu erkennen, legen Sie das Attribut *Credential alias* auf [cmdb_ci_iisdirectory] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.
		Erteilen Sie einem Betriebssystembenutzer des virtuellen IIS-Verzeichnisses Rechte zum Ausführen des IIS-Service unter Windows.
		Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
Microsoft SharePoint	SharePoint [cmdb_ci_appl_sharepoint]	Konfigurieren Sie auf der Now Platform die folgenden Anmeldeinformationen: • Windows-Anmeldeinformationen • Legen Sie das Attribut *Credential alias* auf [cmdb_ci_appl_sharepoint] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden. • Konfigurieren Sie den WMI-Abfragezugriff auf den SharePoint-Remoteserver. • (Optional) Um Windows SharePoint-Verbindungen zu erkennen, konfigurieren Sie Windows-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der http get-Anforderung an die URL der SharePoint-Zentraladministration.
		Erteilen Sie einem SharePoint-Betriebssystemsbenutzer Berechtigungen: • Zum Ausführen von SharePoint-Services unter Windows • Zum Anmelden bei der SharePoint-Verwaltungsseite
		Um zwei separate Anmeldeinformationen mit unterschiedlichen Berechtigungen zu verwenden, konfigurieren Sie die Anmeldeinformationen wie im Artikel Voraussetzungen für die Top Down-Discovery / Service Mapping-Discovery für SharePoint-System [KB0813083] im Artikel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Now Support Knowledge Basebeschrieben.
Microsoft SQL-Datenbank	MySQLClusterDataNode [cmdb_ci_db_mysql_clusternode]	Stellen Sie den/die folgenden Benutzer bereit: • Zur Erkennung von Microsoft BizTalk mithilfe von SQL-Abfragen einen Benutzer und Anmeldeinformationen für Microsoft BizTalk • Zur Erkennung von Lizenzierungsinformationen für Microsoft SQL Server einen Benutzer und Anmeldeinformationen zum Zugriff auf die Microsoft SQL-Datenbank Informationen zum Betrieb finden Sie in der Produktdokumentation.
		Anmeldeinformationen für die Host-Discovery wie in Windows-Anmeldeinformationen beschrieben.
		Konfigurieren Sie die Applicative-Anmeldeinformationen .
MongoDB	Mongo-Konfigurationsserver [cmdb_ci_appl_mongo_configserver]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
		Erteilen Sie einem Benutzer Berechtigungen zum Ausführen der unter Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern beschriebenen Mongo-Befehle.
MySQL Cluster MGM-Knoten	MySQLClusterMGMNode [cmdb_ci_db_mysql_clustermgmnode]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
Nginx	Nginx-Webserver [cmdb_ci_nginx_web_server]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
OpenText Documentum	Documentum DocBase [cmdb_ci_appl_doc_docbase]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
Oracle-Anwendungsserver	Oracle iAS [cmdb_ci_app_server_ora_ias]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
		(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
Oracle Advanced Queue-Warteschlange	Advanced Queue-Warteschlange [cmdb_ci_appl_ora_queue]	(Unter Unix) Konfigurieren Sie die Applicative-Anmeldeinformationen für Service Mapping.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
Oracle Clusterware	UNIX-Cluster [cmdb_ci_unix_cluster], UNIX-Clusterknoten [cmdb_ci_unix_cluster_node], UNIX-Clusterressource [cmdb_ci_unix_cluster_resource], virtuelle Cluster-IPs [cmdb_ci_cluster_vip]	Weitere Informationen finden Sie unter Oracle Discovery von Datenbanken.
Oracle Concurrent-Server	Oracle Concurrent Server [cmdb_ci_appl_ora_conc]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle-Datenbank	Oracle-Instanz [cmdb_ci_db_ora_instance]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platformeinen Domänenbenutzer für den Zugriff auf das

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben.
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle-Datenbank 12c	Oracle PDB-Instanz [cmdb_ci_db_ora_pdb_instance]	• Konfigurieren Sie Applicative-Anmeldeinformationen . • Für Windows konfigurieren Sie Windows-Anmeldeinformationen . • Für Unix konfigurieren Sie SSH-Anmeldeinformationen . • Konfigurieren Sie für die Oracle-Datenbank die Discovery von Oracle-Datenbanken. • Gewähren Sie einem Benutzer Berechtigungen zum Ausführen von Abfragen in den folgenden Tabellen: ◦ V$DATAFILE ◦ V$TEMPFILE ◦ V$LOG ◦ DBA_FREE_SPACE ◦ V$DATABASE ◦ V$PDBS ◦ V$PARAMETER
Queue für erweiterte Oracle-Datenbanken	Advanced Queue-Warteschlange [cmdb_ci_appl_ora_queue]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
		Stellen Sie einen Oracle-Instanzbenutzer mit Berechtigung zur Ausführung des Befehls sqlplus bereit (siehe Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern).
Oracle Discoverer Engine	Oracle Discoverer Engine [cmdb_ci_appl_ora_disc]	(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platformeinen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben.
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Discoverer-Anwenderoberfläche	Oracle Discoverer-UI [cmdb_ci_appl_ora_disc_ui]	(Unter Unix) Konfigurieren Sie die Applicative-Anmeldeinformationen für Service Mapping.
		Konfigurieren Sie auf der Now Platform einen Domänenbenutzer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben.
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Nur unter Unix) Geben Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle E-Business Suite	Oracle ESB [cmdb_ci_appl_ora_ebs]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		Konfigurieren Sie auf der Now Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben.
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Form-UI	Oracle Forms-UI [cmdb_ci_appl_ora_forms_ui]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platformeinen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		wie in Windows-Anmeldeinformationen beschrieben.
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Fulfillment-Server	Oracle Fulfillment Server [cmdb_ci_appl_ora_fs]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle GlassFish Server	GlassFish [cmdb_ci_appl_glassfish] GlassFish WAR [cmdb_ci_appl_glassfish_war]	• (Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen . • (Beim Hosting auf einem Linux- oder UNIX-Server) (Optional) Konfigurieren Sie in der Now Platform SSH-Anmeldeinformationen . • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle HTTP-Server	Oracle-HTTP-Server [cmdb_ci_appl_ora_http]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle iAS-Webmodul	Oracle iAS-Webmodul [cmdb_ci_app_server_ora_ias_wm]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
Oracle Metric-Client	Oracle Metric-Client [cmdb_ci_appl_ora_metric_client]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
Oracle Metric-Server	Oracle Metric-Server [cmdb_ci_appl_ora_metric_svr]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle MySQL-Server	MySQL-Instanz [cmdb_ci_db_mysql_instance]	Stellen Sie den/die folgenden Benutzer bereit: • Zur Erkennung von Microsoft BizTalk mithilfe von SQL-Abfragen einen Benutzer und Anmeldeinformationen für Microsoft BizTalk • Zur Erkennung von Lizenzierungsinformationen für Microsoft SQL Server einen Benutzer und Anmeldeinformationen zum Zugriff auf die Microsoft SQL-Datenbank
		Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Unter Linux gehostet) Gewähren Sie dem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Beim Hosting auf einem Linux-Server) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Net-Listener	Oracle Datenbank-Listener [cmdb_ci_db_ora_listener]	(Unter Linux gehostet) Konfigurieren Sie unter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Now Platformdie SSH-Anmeldeinformationen .
Oracle Notification Server	Oracle-Benachrichtigungsserver [cmdb_ci_appl_ora_notif_svr]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
Oracle OACORE-Server	Oracle OACORE-Server [cmdb_ci_appl_ora_oacore]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
Oracle OAFM-Server	Oracle OAFM-Server [cmdb_ci_appl_ora_oafm]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Unter Unix gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
Oracle PeopleSoft	Peoplesoft-Anwendungsserver [cmdb_ci_appl_peoplesoft]	(Unter Unix gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		Erteilen Sie einem Benutzer die Berechtigung zum Ausführen der unter Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern beschriebenen Befehle.
Oracle Prozessmanager	Oracle-Prozessmanager [cmdb_ci_appl_ora_pm]	(Wenn auf Unix gehostet wird) Konfigurieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Sie die Applicative-Anmeldeinformationen .
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Reports Server	Oracle-Berichtsserver [cmdb_ci_appl_ora_report]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle Tnslsnr-Engine	Oracle TNS-Listener-Engine [cmdb_ci_appl_ora_tnslsnr]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Unter Linux gehostet) Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
Oracle Tuxedo und Oracle Tuxedo-Portal	Tuxedo [cmdb_ci_appl_tuxedo] und Tuxedo-Portal [cmdb_ci_appl_tuxedo_portal]	• Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen . • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren . • (Wenn auf Unix gehostet wird) Geben Sie einem Benutzer die erweiterten Rechte zum Ausführen von Befehlen, die in Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern beschrieben werden.
Oracle WebLogic-Modul	Oracle iAS-Webmodul [cmdb_ci_app_server_ora_ias_wm]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
Oracle WebLogic-Server (Version 10.3)	Weblogic [cmdb_ci_app_server_weblogic]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Oracle WebLogic-On-Demand-Router-Lastenausgleichsmodul	Websphere ODR LB [cmdb_ci_app_server_ws_odr]	(Unter Unix) Konfigurieren Sie die Applicative-Anmeldeinformationen für Service Mapping.
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
Radware Alteon NG	Alteon Load Balancer [cmdb_ci_lb_alteon]	Konfigurieren Sie unter Now Platformdie SNMP-Anmeldeinformationen .
Radware AppDirector	Radware-Load Balancer [cmdb_ci_lb_radware]	Konfigurieren Sie unter Now Platformdie SNMP-Anmeldeinformationen .
Red Hat Cluster Suite	Virtuelle Cluster-IPs [cmdb_ci_cluster_vip] UNIX-Cluster [cmdb_ci_unix_cluster] UNIX-Clusterknoten [cmdb_ci_unix_cluster_node] UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
		Erteilen Sie einem Benutzer die Berechtigung zum Lesen dieser Dateien: • `/etc/cluster/cluster.conf` • `/etc/hosts`
		Erteilen Sie einem Benutzer erweiterte Rechte zur Ausführung dieses Befehls: `clustat -x`.
PostgreSQL-Datenbank	PostgreSQL-Instanz [cmdb_ci_db_postgresql_instance]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
		(Nur unter Unix) Geben Sie diesem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Pivotal RabbitMQ	RabbitMQ-Cluster [cmdb_ci_appl_rabbitmq_cluster]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
SAP Business Object XI Schedule	SAP BO BOXIScheduleRouter [cmdb_ci_appl_sap_bo_scheduler]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
SAP Crystal Management Server	SAP Business Objects CMS-Server [cmdb_ci_appl_sap_bo]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
SAP-Zentralinstanz/ SAP Central Services (SCS)/ SAP Development Infrastructure/ SAP Evaluated Receipt Settlement (ERS)/ SAP Java Connector/	SAP CI-Anwendung [cmdb_ci_appl_sap_ci] / SAP SCS-Anwendung [cmdb_ci_appl_sap_scs]/ SAP DI-Anwendung [cmdb_ci_appl_sap_di]/ SAP ERS-Anwendung [cmdb_ci_appl_sap_ers]/	• (Beim Hosting auf UNIX-Server) Konfigurieren Sie auf der Now Platform die Applicative-Anmeldeinformationen und SSH-Anmeldeinformationen . Die SSH-Anmeldeinformationen werden dazu verwendet,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
SAP NetWeaver-Dialoginstanz/ ABAP SAP Central Services (ASCS)	SAP JC-Anwendung [cmdb_ci_appl_sap_jc]/ SAP DI-Anwendung [cmdb_ci_appl_sap_di]/ SAP ASCS-Anwendung [cmdb_ci_appl_sap_ascs]	Verbindungen von der SAP-Zentralinstanz zu anderen Anwendungen und Geräten herzustellen. Gewähren Sie dem Benutzer außerdem erhöhte Rechte, damit er Befehle ausführen kann, die einen privilegierten Benutzer erfordern: Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern. • (Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform die Windows-Anmeldeinformationen, um Verbindungen von der SAP-Zentralinstanz zu anderen Anwendungen und Geräten herzustellen. • (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren. • (Optional für Discovery von oben nach unten durch Service-Mapping) Erteilen Sie einem Benutzer die Berechtigung zum Ausführen von SOAP in der RFC-Tabellenlesefunktion. • (Optional für Top Down-Discovery durch Service-Mapping) Wenn Ihre Organisation digitale SAP-Business-Services mithilfe von Webservices implementiert und Sie alle verbundenen Services zuordnen möchten, führen Sie die folgenden Aktionen aus: ◦ Konfigurieren Sie Applicative-Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der folgenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Befehle: CVERS, DBCONS und RFCONS. ◦ Stellen Sie sicher, dass Sie über die Webservice-URL verfügen. Informationen zum Erstellen von Webservices finden Sie unter https://blogs.sap.com/2012/10/24/how-to-create-web-services-abap-based/ .
SAP HANA-Datenbank	SAP HANA-Datenbank [cmdb_ci_appl_sap_hana_db]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
SAP Sybase DB	Sybase-Instanz [cmdb_ci_db_syb_instance]	(Wenn auf Unix gehostet wird) Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
		(Nur unter Unix) Geben Sie diesem Benutzer erweiterte Rechte, damit er Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern ausführen kann.
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
SQL Server Analysis Services (SSAS)	SQL Server Analysis Services [cmdb_ci_db_mssql_analysis]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
SQL Server Integration Services-Auftrag (SSIS)	SQL Server Integration Services-Auftrag [cmdb_ci_db_mssql_int_job]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
SQL Server Integration Services (SSIS)	SQL-Server-Integrationsservices [cmdb_ci_db_mssql_integration]	Konfigurieren Sie auf Now Platformdie Windows-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
SQL Server Reporting Services (SSRS)	SQL Server Reporting Services [cmdb_ci_db_mssql_reporting]	Erteilen Sie einem Benutzer des Betriebssystems SSRS Berechtigungen zum Ausführen des SSRS-Service.
		Konfigurieren Sie Anmeldeinformationen für einen Benutzer mit Berechtigungen zum Ausführen der http get-Anforderung für die Einstiegspunkt-URL.
		(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen . Legen Sie das Attribut *Credential alias* auf [cmdb_ci_db_mssql_reporting] fest. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.
		(Optional) Konfigurieren Sie zum Erkennen von Verbindungen zu Berichtsdatenquellen Anmeldeinformationen für einen Benutzer mit der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		Berechtigung zum Ausführen einer http post-Anforderung für die Einstiegspunkt-URL.
		Konfigurieren Sie die Applicative-Anmeldeinformationen .
		(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
Sun iPlanet Webserver	iPlanet Webserver [cmdb_ci_iplanet_web_server]	Konfigurieren Sie die Applicative-Anmeldeinformationen .
		Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
Sun Directory	Sun LDAP-Server [cmdb_ci_sun_ldap_dir_server]	Konfigurieren Sie die Applicative-Anmeldeinformationen .
		Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
Sun JES	JES [cmdb_ci_email_server_jes]	Konfigurieren Sie die Applicative-Anmeldeinformationen .
		Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
Symantec Enterprise Vault	Enterprise Vault [cmdb_ci_email_server_ent_vault]	Konfigurieren Sie auf Now Plattformdie Windows-Anmeldeinformationen .
TIBCO ActiveMatrix BusinessWorks/ TIBCO ActiveMatrix BusinessWorks-Prozess/ TIBCO EMS-Warteschlange/ TIBCO Enterprise Message Service (EMS)/	ActiveMatrix Business Works [cmdb_ci_appl_tibco_matrix]/ ActiveMatrix Business Works-Prozess [cmdb_ci_appl_tibco_matrix_proc]/ EMS-Warteschlange [cmdb_ci_appl_tibco_queue]/ Tibco Enterprise Message Service [cmdb_ci_appl_tibco_message]	• (Beim Hosting auf Unix) Konfigurieren Sie die Applicative-Anmeldeinformationen für Tibco EMS. • (Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen . • (Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Applikation	CI-Typ	Konfigurationsschritte
		• (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
TIBCO ActiveMatrix Adapter	Tibco-Adapter [cmdb_ci_appl_tibco_adapter]	(Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
		(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
Veritas Enterprise Vault	Enterprise Vault [cmdb_ci_email_server_ent_vault]	(Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .

Beheben von Problemen im Zusammenhang mit Anmeldeinformationen

Wenn Discovery-Probleme auftreten, die durch falsch konfigurierte oder fehlende Anmeldeinformationen verursacht werden, beheben Sie sie wie im KB-Artikel erläutert: Problembehandlung für Anmeldeinformationen und Berechtigungen bei Discovery, Service-Mapping, Orchestration

Für die Hosterkennung erforderliche Anmeldeinformationen

Es gibt Anmeldeinformationen und Berechtigungen, die Service-Mapping für die Erkennung von Hosts benötigt.

Vor der Erkennung von Anwendungen greift Service-Mapping auf Hosts zu, auf denen Anwendungen ausgeführt werden, und erkennt diese. Stellen Sie sicher, dass Sie alle erforderlichen Anmeldeinformationen angeben, um die Hosterkennung zu ermöglichen.

Now Platform bietet eine zentralisierte Möglichkeit zum Konfigurieren von Anmeldeinformationen für Discovery, Service-Mapping und andere Anwendungen. Sie können die Anmeldeinformationen für Hosts und Anwendungen nur einmal konfigurieren. Wenn Sie bereits hostbezogene Anmeldeinformationen für eine andere Anwendung konfiguriert haben, müssen Sie dies für Service-Mapping nicht noch einmal tun.

Für die Erkennung von Hosts unter UNIX oder Linux erforderliche Anmeldeinformationen

Discovery, Orchestration und IntegrationHub erkunden die Geräte UNIX und Linux mithilfe von SSH-Anmeldeinformationen, um Befehle über Secure Shell (SSH) auszuführen.

Um ausreichende Berechtigungen zu erteilen, konfigurieren Sie eine der folgenden UNIX- oder Linux-Anmeldeinformationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Nicht-Root-Benutzer und -Kennwort und Ausführung der ausgewählten Befehle als „root“ mithilfe des Dienstprogramms sudo
- Root-Benutzer und -Passwort

Informationen zu Befehlen, die Rechte auf Sudo-Ebene erfordern, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern und Befehle, die Root-Rechte erfordern, für Discovery und Orchestration .

Um mit Nicht-Root-Anmeldeinformationen auf Unix-basierte Hosts zuzugreifen, erteilen Sie Lesezugriff auf die folgenden Dateien und Verzeichnisse:

- /etc/*release
- /etc/bashrc
- /etc/profile
- /proc/cpuinfo
- /proc/vmware/sched/ncpus
- /var/log/dmesg
- APD-Verzeichnis

Für die Erkennung von Hosts auf Windows-Servern erforderliche Anmeldeinformationen

Um ausreichende Berechtigungen zu erteilen, konfigurieren Sie eine der folgenden Windows-Anmeldeinformationen:

- Ein Domänenbenutzer mit lokalem Administratorzugriff auf Windows-Zielhosts
- Einen Domänenadministrator

> **Hinweis:** Die Anmeldeinformationen für den Domänenadministrator benötigen Sie möglicherweise nur in einigen Fällen. Beispielsweise beim Erkennen von Domänencontrollern.

Konfigurieren Sie den MID-Server für die Verwendung von Windows-Anmeldeinformationen .

(Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

Beheben von Problemen im Zusammenhang mit Anmeldeinformationen

Wenn Discovery-Probleme auftreten, die durch falsch konfigurierte oder fehlende Anmeldeinformationen verursacht werden, beheben Sie sie wie im KB-Artikel erläutert: Problembehandlung für Anmeldeinformationen und Berechtigungen bei Discovery, Service-Mapping, Orchestration

Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern

Um Unix-basierte Hosts in Ihrer Organisation zu erkennen und zuzuordnen, nutzt Service-Mapping Befehle, für die erweiterte Rechte erforderlich sind. Konfigurieren Sie nicht nur die erforderlichen Anmeldeinformationen, sondern auch die Server in Ihrer Organisation, damit Service-Mapping diese Befehle mit erweiterten Rechten ausführen kann.

Sie führen diese Befehle nicht direkt aus. Service-Mapping verwendet Befehle, die erhöhte Rechte erfordern, als Teil der folgenden Prozesse:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Hosterkennung
- Prozessidentifikation am Port
- CIs anhand von Mustern entdecken

Einige dieser Befehle erfordern keine erweiterten Rechte, es sei denn, Verzeichnisse, auf die Service-Mapping zugreifen muss, sind geschützt. Weitere Informationen finden Sie unter Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern.

Betriebssystembefehle, die erweiterte Rechte erfordern

AIX-Befehle, die erweiterte Rechte erfordern

Befehl	Parameter	Beschreibung
cat	*file-name*	Zeigt den Dateiinhalt an
ls	*-F-1* *-lHF* *-w 1* *-1*	Listet den Verzeichnisinhalt auf
procwdx	*Process_id*	Ruft das Arbeitsverzeichnis eines Prozesses ab
rmsock	*Socketname tcpcp*	Sucht nach einem Prozess, der einen bestimmten Port abhört
lsof	*-Pnl +M -i*	Zeigt Dateien oder Verbindungen an, die mit dem Prozess verknüpft sind
lstat	Verschiedene Optionen	Ruft Informationen über einen Link ab
ps	*eww*	Ruft Umgebungsvariablen für den Prozess unter AIX ab

HP UX-Befehle, die erweiterte Rechte erfordern

Befehl	Parameter	Beschreibung
cat	*file-name*	Zeigt den Dateiinhalt an
ls	*-F-1* *-lHF* *-w 1* *-1*	Listet den Verzeichnisinhalt auf
pfiles	*Process_id*	Zeigt Dateien oder Verbindungen an, die mit dem Prozess verknüpft sind

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HP UX-Befehle, die erweiterte Rechte erfordern (Fortsetzung)

Befehl	Parameter	Beschreibung
lsof	*-Pnl +M -i*	Zeigt Dateien oder Verbindungen an, die mit dem Prozess verknüpft sind

Solaris-Befehle, die erweiterte Rechte erfordern

Befehl	Parameter	Beschreibung
cat	*File_name*	Zeigt den Dateiinhalt an
ls	*ls -F-1* *ls -1HF* *ls -w 1* *ls -1*	Listet den Verzeichnisinhalt auf
	e-l	Ruft Dateiattribute ab, die für die Entscheidung zum Zwischenspeichern von Dateien verwendet werden
pargs	*-e*	Ruft das ausführbare Verzeichnis ab.
pargs	*-a*	Ruft den Prozess ab.
lsof	*-Pnl +M -i*	Zeigt Dateien und Verbindungen an, die mit dem Prozess verknüpft sind.
netstat	*-anu*	Listet die offenen Ports auf Obligatorisch für Solaris Version 11.2 oder höher.
Ifconfig	*Ifconfig -a*	Zeigt Schnittstelleninformationen an (sudo zum Abrufen der MAC-Adressen erforderlich)
pwdx	*Process_id*	Ruft die Prozessinformationen ab
pargs	*-e process_id*	Ruft die Prozessinformationen ab
ps	*-eo user, pid, ppid, comm, args*	Ruft die Prozessliste ab
inetadm	*-l or without params*	Verarbeitet den Anwendungsfall mit dem inet-Daemon

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Befehle, die erweiterte Rechte erfordern

Befehle	Parameter	Beschreibung
cat	*File_name* *scsi* *tr '||n'* */proc* */proc/cpuinfo* *sys* *sys/hypervisor* *sys/hypervisor/compilation* *sys/hypervisor/compilation/compiled by*	Zeigt Informationen über den Inhalt der Datei an
cut	*-d* *-f1*	Zeigt die gesamte Ausgabe einer Datei an
dmidecode	*-t 17* *-s bios-vendor* *-t 1* *-t 2* *-t 3*	Zeigt Informationen zur Hardware des Linux-Servers in einem lesbaren Format an
lshw		Zeigt Informationen zur Hardware des Linux-Servers in einem lesbaren Format an
ls	*ls -F-1* *ls -1HF* *ls -w 1* *ls -1* *ls -l*	Listet den Verzeichnisinhalt auf
netstat	*-ltnup* *-ltnp* *-ntup*	Zeigt die offenen Netzwerkverbindungen an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Befehle, die erweiterte Rechte erfordern (Fortsetzung)

Befehle	Parameter	Beschreibung
	-an	
lsof **Hinweis:** Wird in einigen Fällen als Alternative zu netstat verwendet.	*-Pnl +M -i*	Zeigt Dateien und Verbindungen an, die mit dem Prozess verknüpft sind.
ss	*-ltnup* *-ntup* *-an*	Zeigt die offenen Netzwerkverbindungen an
stat	*--format="%Y"* *-L file_name*	Zeigt die Änderungszeit der Datei an
fdisk	*-l*	Zeigt alle Festplattenpartitionen an

Anwendungsbefehle, die erweiterte Rechte erfordern

Service-Mapping verwendet einige dieser Befehle in Mustern.

Apache-Webserver (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

Apache Tomcat (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an
netstat	Verschiedene Optionen	Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Tomcat (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
ss	Verschiedene Optionen	Listet die offenen Ports auf
find	*-name*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Apache Tomcat WAR (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt an
version.sh/version.bat	-	Ruft die Tomcat-Version ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf
ss	Verschiedene Optionen	Listet die offenen Ports auf
find	*-name*	Dieser Befehl wird in Verbindungsabschnitten des Musters zum Erkennen von Apache Tomcat-WAR-Verbindungen verwendet. Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

App TNS-Service (unter UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

BIG-IP Global Traffic Manager (GTM) F5 (unter F5 BIG-IP)

Befehl	Parameter	Beschreibung
ping	*-a -c 1 [url[1].host]*	Ruft die Host-IP ab

BMC CTRL-M Enterprise Manager (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf

BMC CTRL-M Gateway (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Dieser Befehl wird nur zum Erstellen von Verbindungen zum Control M-Server verwendet. Sucht nach Datei- und Ordnerpfaden

Citrix NetScaler (unter Citrix NetScaler)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
show	Verschiedene Optionen	Ruft die Netscaler-IP-Adresse ab.

EMC Documentum Broker (unter UNIX)

Befehl	Parameter	Beschreibung
find	Verschiedene Optionen	Sucht nach Verbindungen zu Docbase

FormEngine (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	(Nur unter Unix) Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

FormEngine (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	(Nur unter Unix) Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	(Nur unter Unix) Zeigt den Dateiinhalt an

IBM Customer Information Control System (CICS) (unter UNIX)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

IBM CTRL-M Server (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	(Nur für Unix) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Unix) Sucht nach Datei- und Ordnerpfaden

IBM CICS Transaction Gateway CTG (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	(Nur für Unix) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Extrahiert Zeichenfolgen aus der Ausgabe
cat	–	(Nur für Unix) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Zeigt den Dateiinhalt in der Ausgabe an
find	Verschiedene Optionen	(Nur für Unix) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Sucht nach

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM CICS Transaction Gateway CTG (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
		bestimmten Zeichenfolgen in Dateien und Ordnern

IBM DB2 (unter Linux)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
cat	–	Zeigt den Dateiinhalt in der Ausgabe an

IBM J2EE EAR (unter Linux)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
find	*-name*	Sucht nach Dateien und Ordnern im angegebenen Ordner

IBM WebSphere Application Server (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an
find	*-name* *-type*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere Portal (auf UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an
netstat	Verschiedene Optionen	Listet die offenen Ports auf
ss	Verschiedene Optionen	Listet die offenen Ports auf

IBM WebSphere Message Broker-Flow (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an
ps	*-ef*	Ruft die Prozessinformationen ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf
ss	Verschiedene Optionen	Listet die offenen Ports auf

IBM WebSphere Message Broker (unter UNIX)

Befehl	Parameter	Beschreibung
ps	*-ef*	Ruft die Prozessinformationen ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

IBM MQ (auf UNIX) – früher IBM WebSphere MQ

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM MQ-Warteschlange (auf UNIX) – früher IBM WebSphere MQ-Warteschlange

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

JBoss-Modul (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf

JBoss (unter UNIX und Windows)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	(Nur unter Unix) Listet Dateien und Ordner im angegebenen Ordner auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf

JRun (unter UNIX)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

JRun WAR Inc (unter UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JRun WAR Inc (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf

Microsoft Exchange-Clientzugriffsserver (CAS), Microsoft Exchange-Hub-Transport-Server, Microsoft Exchange-Postfach (unter Windows)

Befehl	Parameter	Beschreibung
Get-ExchangeServer	*-status -Identity "+ $hostname+"| export-clixml $env:TEMP |exchange_pwrshell_output.xml*	Extrahiert die Liste der Microsoft Exchange-Hosts und -Rollen
Get-ExchangeServer	*format-table -autosize -HideTableHeaders Name,Fqdn,IsMailboxServer*	Extrahiert die Liste der Microsoft Exchange-Hosts und -Rollen im Tabellenformat
Get-Mailboxserver	*format-list*	Extrahiert die Liste der Microsoft Exchange-Postfachserver
Get-ClusteredMailBoxServerStatus	*format-table -Property OperationalMachines*	Extrahiert Informationen über Microsoft Exchange-Postfachcluster
Get-ExchangeServer	*format-table -autosize -HideTableHeaders Name,Fqdn,IsHubTransportServer*	Extrahiert Informationen über Microsoft Exchange-Hub-Transport-Server
Get-StorageGroup	*-server "+$hname+" | select SystemFolderPath | Export-Csv out.csv -notype;cat out.csv*	Extrahiert Informationen über den Speicher und exportiert sie in eine Datei
Get-MailboxDatabase	*| select LogFolderPath | format-table -autosize -hideTableHeaders; Get-MailboxDatabase | select EdbFilePath| format-table -autosize -hideTableHeaders;Get-MailboxDatabase | select TemporaryDataFolderPath| format-table -autosize -hideTableHeaders*	Extrahiert Informationen über die Microsoft Exchange-Postfachdatenbank

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Server (unter Linux)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	(Nur unter Unix) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
ps	*--pid=[process.pid] --no-headers -o " %U : %p : %a"*	Ruft den Parameterwert „userid“ ab

MySQL-Cluster-MGM-Knoten (unter Linux)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
ps	*--pid=[process.pid] --no-headers -o " %U : %p : %a"*	(Nur unter Unix) Ruft den Parameterwert „userid“ ab

Nginx (unter UNIX)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
ps	*--pid=[process.pid] --no-headers -o " %U : %p : %a"*	Ruft den Parameterwert „userid“ ab
ls	*[IncludeTabletmp[].files]*	Dieser Befehl wird bei Bedarf zum Erstellen von HTTP-Verbindungen verwendet. Listet Dateien und Ordner im angegebenen Ordner auf
cat	*[IncludeTabletmp[].files]*	Dieser Befehl wird bei Bedarf zum Erstellen von HTTP-Verbindungen verwendet. Zeigt den Dateiinhalt an

Oracle E-Business Suite (auf UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle E-Business Suite (auf UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
Exportieren	–	Legt Variablen fest
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
sqlplus	Verschiedene Optionen	Erstellt die Verbindung zur Instanz Oracle.
awk	Verschiedene Optionen	Ändert die Ausgabe
netstat	Verschiedene Optionen	Ruft offene Ports ab

Oracle Advanced Queuing-Warteschlange (auf UNIX)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf.

Oracle Concurrent Server (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	(Nur für Unix) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
awk	Verschiedene Optionen	(Nur für Unix) Ändert die Ausgabe
ls	Verschiedene Optionen	(Nur für Unix) Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	(Nur für Unix) Zeigt den Dateiinhalt in der Ausgabe an
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle Discoverer Engine (unter UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Discoverer Engine (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
cat	–	Zeigt den Dateiinhalt an

Oracle Discoverer-Benutzeroberfläche (unter UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
cat	–	Zeigt den Dateiinhalt an

Oracle Form-Benutzeroberfläche (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

Oracle Fulfillment Server (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

Oracle HTTP Server (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Metric-Client (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

Oracle OACORE-Server (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

Oracle OAFM-Server (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

Oracle Database (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an
ps	*-ef*	Ruft die Prozessinformationen ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle iAS-Webmodul (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	(Nur für Unix) Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	(Nur für Unix) Zeigt den Dateiinhalt an
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf.

Oracle Prozessmanager (am UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

Oracle Berichtsserver (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

Oracle Tnslsnr Engine (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

Oracle WebLogic-Modul (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle WebLogic-Modul (auf UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an
find	*-name* *-type*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens

Oracle WebLogic Server (Version 10.3) (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

Oracle Lastenausgleichsmodul für bedarfsgesteuerten WebLogic-Router (auf UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt an

Oracle Tuxedo (am UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene	Listet Dateien und Ordner im vorgegebenen Ordner auf
cat	–	Zeigt den Dateiinhalt in der Ausgabe an
find	*-name*	Dieser Befehl wird nur zum Erstellen von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Tuxedo (am UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
		Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens
netstat	Verschiedene	Ruft offene Ports ab
ss	Verschiedene Optionen	Listet die offenen Ports auf
ps	*-ef*	(Nur für Unix) Ruft Prozessattribute ab

Oracle Tuxedo-Portal (unter UNIX)

Befehl	Parameter	Beschreibung
grep	Verschiedene	Extrahiert Zeichenfolgen aus der Ausgabe
ls	Verschiedene	Listet Dateien und Ordner im vorgegebenen Ordner auf
cat	-	Zeigt den Dateiinhalt in der Ausgabe an

PostgreSQL-Datenbank (unter UNIX)

Befehl	Parameter	Beschreibung
ls	*[IncludeTabletmp[].files]*	Dieser Befehl wird zum Erstellen von HTTP-Verbindungen verwendet. Listet Dateien und Ordner im angegebenen Ordner auf

Rabbit MQ (unter UNIX)

Befehl	Parameter	Beschreibung
ps - ef	*ps -ef | grep "+ $process.parentProcessId +" |egrep -v -e grep -e beam*	Ruft den übergeordneten Prozess ab

Red Hat Cluster Suite (unter Linux)

Befehl	Parameter	Beschreibung
clustat	*-x*	Zeigt die Clusterkonfiguration und den Status im XML-Format an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehle, für die ein privilegierter Benutzer erforderlich ist, um SAP-Anwendungen zu erkennen: ABAP, SAP Central Services (ASCS), SAP Control Instance, SAP Netweaver Dialog Instance, SAP Evaluated Receipt Settlement (ERS), SAP Java Cluster (SJC), SAP Central Services (SCS) (unter UNIX)

Befehl	Parameter	Beschreibung
pargs	*-e*	Ruft das ausführbare Verzeichnis ab.
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
ping	*-c 1*	Überprüft, ob der Host antwortet
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
lsof **Hinweis:** Wird in einigen Fällen als Alternative zu netstat verwendet.	*-Pnl +M -i*	Zeigt Dateien und Verbindungen an, die mit dem Prozess verknüpft sind.
CVERS	–	Ruft die Version der installierten SAP-Module ab
DBCONS	–	Ruft die Verbindungszeichenfolgen für SAP DB ab
RFCDES	–	Ruft die Verbindungszeichenfolge zu Systemen ab, die in SAP integriert sind
sapcontrol	*-function ABAPGetComponentList*	Ruft die sysid für SAP -Anwendungen und -Komponenten ab.

Sun Directory (unter Solaris)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf

Sun iPlanet Web Server (unter Solaris)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
netstat	Verschiedene Optionen	Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sun JES (unter Solaris)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

Sybase (unter UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

TIBCO ActiveMatrix Adapter (unter UNIX)

Befehl	Parameter	Beschreibung
cat	–	Zeigt den Dateiinhalt an
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf

TIBCO ActiveMatrix BusinessWorks (unter UNIX)

Befehl	Parameter	Beschreibung
hostname	–	Ruft den Hostnamen ab
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
cat	–	Zeigt den Dateiinhalt an
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf

TIBCO ActiveMatrix BusinessWorks-Prozess (unter UNIX)

Befehl	Parameter	Beschreibung
hostname	–	Ruft den Hostnamen ab
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
cat	–	Zeigt den Dateiinhalt an
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TIBCO ActiveMatrix BusinessWorks-Prozess (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
cut	Verschiedene Optionen	Teilt die Ausgabezeile auf

TIBCO EMS-Warteschlange (unter UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

TIBCO Enterprise Message Service (EMS) (unter UNIX)

Befehl	Parameter	Beschreibung
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

Zugehörige Informationen

Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern

Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern

Die meisten der von Service-Mapping für Erkennung und Zuordnung verwendeten Befehle erfordern keine erweiterten Rechte.

Überprüfen Sie diese Befehlsliste, um zu verstehen, wie Service-Mapping diese verwendet, und um sicherzustellen, dass die virtuelle Sicherheit Ihres Unternehmens nicht beeinträchtigt wird.

Sie führen diese Befehle nicht direkt aus. Service-Mapping verwendet Befehle, die erhöhte Rechte erfordern, als Teil der folgenden Prozesse:

- Hosterkennung
- Prozessidentifikation am Port
- CIs anhand von Mustern entdecken

Betriebssysteme

AIX-Befehle

Befehl	Parameter	Beschreibung
awk	Verschiedene Optionen	Analysiert die Zeichenfolge
istat	*file_name*	Ruft den Zeitpunkt der letzten Änderung der Datei ab
nslookup	*hostname*	Löst den DNS-Hostnamen auf
ping	*-c count ip/host*	Pingt den Host

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AIX-Befehle (Fortsetzung)

Befehl	Parameter	Beschreibung
arp -an	Verschiedene Optionen	Zeigt die ARP-Tabelle an
grep	Zu durchsuchende Zeichenfolge	Sucht eine Zeichenfolge in der vorherigen Befehlsausgabe
traceroute	*-n ip_address*	Zeigt die Layer-3-Netzwerkroute zum Zielhost an
netstat	*-an* *-Aan*	Zeigt offene Netzwerkverbindungen an
ps	*-eo user, pid, ppid, comm, args*	Ruft die Prozessliste ab
find	Verzeichnis und Parameter für die Suche	Sucht nach Dateien nach Name oder Typ

HP UX-Befehle

Befehl	Parameter	Beschreibung
ping	*-c count ip/host*	Pingt den Host
arp -an		Zeigt die ARP-Tabelle an
grep	Zu durchsuchende Zeichenfolge	Sucht eine Zeichenfolge in der vorherigen Befehlsausgabe
awk	Verschiedene Optionen	Analysiert die Zeichenfolge
traceroute	*-n ip_address*	Zeigt die Layer-3-Netzwerkroute zum Zielhost an
netstat	*-an*	Zeigt offene Netzwerkverbindungen an
ps	*-eo user, pid, ppid, comm, args*	Ruft die Prozessliste ab
find	Verzeichnis und Parameter für die Suche	Sucht nach Dateien nach Name oder Typ

IBM / z /OS

Befehle	Parameter	Beschreibung
sysvar	*SYSNAME*	Ruft den Systemnamen ab
hostname		Ruft den Gerätenamen ab
grep	Zu durchsuchende Zeichenfolge	Sucht nach einer Zeichenfolge in der Befehlsausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM / z /OS (Fortsetzung)

Befehle	Parameter	Beschreibung
hostname	–	Ruft den Hostnamen ab
netstat	*-g | awk '{if (NR>4) print |$1,|$3}'*	Ruft Netzwerkinformationen ab
netstat	*-r | awk '{if (NR>3) print |$1,|$2,|$5}'*	Ruft Gateway-Informationen ab
netstat	*-h | awk '{if (NR>4) print |$1}' | grep -v '127.0.0.1'*	Ruft ein IP-Array ab
netstat	*-R ALL | awk '{if (NR>1) print |$0}'*	Ruft Schnittstellen ab
netstat	*df -k | awk '{print |$1,|$2}' |sed -e s'/(//' | sed -e s'/)//' 2> /dev/null*	Ruft die Dateisysteminformationen ab
ps	–	Ruft die Prozessliste ab
ls	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
cat	*file-name*	Zeigt den Dateiinhalt an
cut	Verschiedene Optionen	Teilt die Ausgabe gemäß den eingegebenen Parametern auf
uname	*l, v, rm, s*	Ruft den Betriebssytemtyp ab

Linux

Befehle	Parameter	Beschreibung
nslookup	*hostname*	Löst den DNS-Hostnamen auf
ping	*-c count ip* *host*	Pingt den Host
arp	*-an/n*	Zeigt die ARP-Tabelle an
lp n	*-an/n*	Zeigt die ARP-Tabelle an
grep	Zu durchsuchende Zeichenfolge *-v* *hypervisor* *proc* *cpuinfo*	Sucht die Zeichenfolge in der vorherigen Befehlsausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux (Fortsetzung)

Befehle	Parameter	Beschreibung
	-i 'attached scsi' *var* *log* *dmesg* *'SCSI device'* *'Disk* *UUID*	
awk	Verschiedene Optionen	Analysiert die Zeichenfolge
netstat	*-an*	Zeigt offene Netzwerkverbindungen an
ss	*-an*	Zeigt offene Netzwerkverbindungen an
ps	*-eo user, pid, ppid, comm, args, wwwx*	Ruft die Prozessliste ab
egrep	Verschiedene Optionen	Durchsucht Text in der vorherigen Befehlsausgabe
find	Verzeichnis und Parameter für die Suche	Sucht nach Dateien nach Name oder Typ
traceroute	*-n ip_address*	Zeigt die Layer-3-Netzwerkroute zum Zielhost an
df	*-kP, echo*	Extrahiert die Informationen zum Dateisystem, einschließlich der Größe in KB
uptime	Verschiedene Optionen	Zeigt die aktuelle Uhrzeit, die Betriebsdauer des Systems, die Anzahl der aktuell angemeldeten Benutzer und Durchschnittswerte der Systemlast der letzten 1, 5 und 15 Minuten an
Datum	Verschiedene Optionen	Zeigt das Datum in der Zeitzone an, in der das Betriebssystem Linux konfiguriert ist
perl	*-e 'print time*	Öffnet die Perl-Shell und gibt die Zeit aus
command	*-v vxprint*	Dieser Befehl wird im Debug-Modus verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux (Fortsetzung)

Befehle	Parameter	Beschreibung
uname	*-a* *-r*	Zeigt Systeminformationen an
ipfconfig	*-a*	Zeigt die Konfiguration der Netzwerkschnittstelle an
ip	Weiterleitungsliste *-4 -o addr show* *-6 -o a* *r* Zu analysierende Zeichenfolge	Zeigt Informationen zur Netzwerkschnittstelle an, einschließlich der Weiterleitungstabelle
Route	*-n*	Zeigt die IP-Weiterleitungstabelle an
ip r		Zeigt die IP-Weiterleitungstabelle an
sed	*-n '2!p'*	Führt eine Funktion mit dem Streameditor SED aus
bash	*-c*	Führt den Befehl mit der UNIX-Shell oder der UNIX-Befehlssprache aus
waagent	*-version 2>/dev/null*	Zeigt die vom Microsoft Azure Linux-Agent extrahierten Informationen an

Solaris

Befehl	Parameter	Beschreibung
nslookup	*hostname*	Löst den DNS-Hostnamen auf
ping	*-c count ip/host*	Pingt den Host
arp	*-an*	Zeigt die ARP-Tabelle an
grep	Zu durchsuchende Zeichenfolge	Sucht die Zeichenfolge in der vorherigen Befehlsausgabe
awk	Verschiedene Optionen	Analysiert die Zeichenfolge
traceroute	*-n ip_address*	Zeigt die Layer-3-Netzwerkroute zum Zielhost an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Solaris (Fortsetzung)

Befehl	Parameter	Beschreibung
netstat	*-an*	Zeigt die offenen Netzwerkverbindungen an
zoneadm	*List*	Zeigt die Liste der Zonen an
egrep	Verschiedene Optionen	Durchsucht Text in der vorherigen Befehlsausgabe
find	Verzeichnis und Parameter	Sucht nach Dateien nach Name oder Typ

Windows WMI-Abfragen

Abfrage	Beschreibung
*Select * from Win32_ComputerSystem*	Ruft grundlegende Informationen zum Server wie die Seriennummer ab
Select LastModified from CIM_LogicalFile Where Name=...	Ruft den Zeitpunkt der letzten Änderung der Datei ab
Select AddressWidth from Win32_Processor	Ruft die Computerarchitektur ab (32 Bit oder 64 Bit)
*Select * From Win32_Process where (ProcessId = ?)*	Ruft die auf dem Computer ausgeführte Prozessliste ab
Select Name from CIM_LogicalDisk	Ruft die Dateisysteme auf dem Computer ab, zum Beispiel C: oder D :
Select FileName, Extension from CIM_Directory where Drive='drive' and Path='path'	Ruft die Liste der Dateien in einem bestimmten Verzeichnis ab

Windows-Befehle

Befehl	Parameter	Beschreibung
get_process_info.exe	*Process_id*	Extrahiert Informationen über die Prozesse mithilfe der von ServiceNow erstellten ausführbaren Datei
type	*File_name*	Zeigt den Inhalt der Textdatei an
nslookup	*Host_name*	DNS-Suche
arp	*-a*	Zeigt die ARP-Tabelle an
netstat	*-ano*	Zeigt die Netzwerkverbindungen an
findstr	Verschiedene Optionen	Sucht die Zeichenfolge in der vorherigen Befehlsausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Befehle (Fortsetzung)

Befehl	Parameter	Beschreibung
dir	*/q* */s /b*	Listet Dateien in den Verzeichnissen auf
paping	*--nocolor -c 1 -p* *port_num* *ip_address*	Dienstprogramm zum Ausführen von TCP-Ping für den angegebenen Host
ping	*-n 1* *ip_address/host*	Pingt den Host
tracert	*Ip_address*	Zeigt die Layer-3-Netzwerkroute zum Zielhost an

Anwendungen

A10-Lastenausgleichsmodule

Befehl	Parameter	Beschreibung
show partition	Verschiedene Optionen	Ruft die konfigurierte Partition ab
sh-run all-partitions	Verschiedene Optionen	Ruft Details wie Informationen über virtuelle Server, Ports, Servicegruppen und Poolmitglieder ab
show slb virtual-server all-partitions	Verschiedene Optionen	Ruft den Status des virtuellen Servers und Details zur Trefferanzahl ab

Befehle, die keinen privilegierten Benutzer für die Erkennung von ABAP SAP Central Services (ASCS) erfordern (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
msg_server	*-V*	Ruft die Version ab
ping	*-n 1*	(Nur für Windows) Überprüft, ob der Host antwortet
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Domänencontroller (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Ruft offene Ports ab
ss	Verschiedene Optionen	Listet die offenen Ports auf
hostname	–	Ruft den Hostnamen ab
dir	Verschiedene Optionen	Listet alle Dateien im angegebenen Ordner auf

Apache-Webserver (unter UNIX)

Befehl	Parameter	Beschreibung
httpd	*-V*	Ruft die Version ab
cut	Verschiedene Optionen	Teilt die Ausgabezeile auf
opmnctl	*status -fmt %cmp32%prt32%por40%pid* und *@farm status -noheaders -fsep "|" -fmt %cmp%prt %clu%ins%por*	Dieser Befehl wird nur zum Erkennen der OC4J-Konnektivität verwendet. Ruft den Status des OPMN CTRL-Service ab
sortieren	*-u*	Dieser Befehl wird nur zum Erkennen der Weblogic-Konnektivität verwendet. Sortiert die Ausgabe

Apache-Webserver (unter Windows)

Befehl	Parameter	Beschreibung
httpd.exe	*-V*	Ruft die Version ab
opmnctl	*status -fmt %cmp32%prt32%por40%pid* und *@farm status -noheaders -fsep "|" -fmt %cmp%prt %clu%ins%por*	Dieser Befehl wird nur zum Erkennen der OC4J-Konnektivität verwendet. Ruft den Status des OPMN CTRL-Service ab

Apache Tomcat (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Tomcat (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
find	*-name*	Erstellt die Webserviceverbindungen. Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
version.sh/version.bat	-	Ruft die Tomcat-Version ab
java -cp " + $install_directory + "/lib/catalina.jar org.apache.catalina.util.ServerInfo	-	Ruft die Tomcat-Version ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf
find	*-name*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
ss	Verschiedene Optionen	(Nur für Linux) Listet die offenen Ports auf

Apache Tomcat WAR (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
version.sh/version.bat	-	Ruft die Tomcat-Version ab
netstat	Verschiedene Optionen	(Nur Windows) Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

App TNS-Service (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
netstat	Verschiedene Optionen	(Nur unter Windows) Listet die offenen Ports auf
grep	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe

BIG-IP Global Traffic Manager (GTM) F5 (unter F5 BIG-IP)

Befehl	Parameter	Beschreibung
show	*/gtm pool [wide_ip_pool_4_cmd[1].pool] members*	Dieser Befehl wird nur zum Erstellen von Verbindungen zu Poolmitgliedern verwendet. Ruft die Poolmitglieder ab
list	*/gtm server [servers_from_cmd[].server] addresses*	Dieser Befehl wird nur zum Erstellen von Verbindungen zu Poolmitgliedern verwendet. Listet die Alias-Serveradressen auf

BIG-IP Local Traffic Manager (LTM) F5 (unter F5 BIG-IP)

Befehl	Parameter	Beschreibung
b	*rule [rule name] list* und *virtual address [entry_point.ip_address]*	Dieser Befehl wird nur zum Erstellen von Verbindungen aus Regeln verwendet. Listet vorhandene Regeln für BIGPipe auf
list	*ltm rule [rule name]* und *data-group wts_routing_destination_prod | grep -A 1 [ep_uri]*	Dieser Befehl wird nur zum Erstellen von Verbindungen aus Regeln verwendet. Listet vorhandene Regeln für TMSH auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

BIG-IP Device Service Clustering

Befehl	Parameter	Beschreibung
show cm traffic-group -get	Verschiedene Optionen	Dieser Befehl wird zum Abrufen von Datenverkehr und Clustering-Informationen verwendet.

BMC CTRL-M Enterprise Manager (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	(Nur für Windows) Listet die offenen Ports auf

BMC CTRL-M Gateway (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
find	Verschiedene Optionen	Dieser Befehl wird nur zum Erstellen von Verbindungen zum Control M-Server verwendet. Sucht nach Datei- und Ordnerpfaden
xargs	*grep <string>*	Dieser Befehl wird nur zum Erstellen von Verbindungen zum IBM CTRL-M-Server verwendet. Führt den Befehl an allen Listen der Ausgabe aus

BMC IT Asset Management (ITAM)

Befehl	Parameter	Beschreibung
tnsping	Verschiedene Optionen	Ruft Informationen über Oracle-Verbindungen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CA Identity Manager-Bereitstellungsserver (für Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

Cassandra (für UNIX)

Befehl	Parameter	Beschreibung
find	Verschiedene Optionen	Sucht nach dem Pfad der base init-Konfigurationsdatei.
locate	Verschiedene Optionen	Sucht nach dem Pfad der base init-Konfigurationsdatei, wenn der Befehl find fehlschlägt
nodetool version	Verschiedene Optionen	Ruft die Version Apache Cassandra ab.
nodetool describecluster	Verschiedene Optionen	Ruft den Clusternamen ab
nodetool info	Verschiedene Optionen	Ruft Informationen über Rechenzentrum und Rack ab
nodetool ring	Verschiedene Optionen	Ruft die für Apache Cassandraausgeführte Arbeitsauslastung ab.
nodetool tablestats	Verschiedene Optionen	Ruft eine Liste der in einem Cluster verfügbaren Keyspaces ab
dse	*-v*	Ruft die DataStax-Version Cassandra ab.
dsetool ring	Verschiedene Optionen	Ruft die für DataStax Cassandraausgeführte Arbeitsauslastung ab.

Befehlszeilenschnittstelle Cisco ACE (unter Cisco CSM)

Befehl	Parameter	Beschreibung
show	*context, running*	Zeigt die angeforderten Informationen an
einbeziehen	-	Extrahiert Zeichenfolgen aus der Ausgabe
echo	-	Zeigt Zeichenfolgen in der Ausgabe an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cisco Global Site Selector (unter Cisco CSM)

Befehl	Parameter	Beschreibung
show	*gslb-config domain-list*	Zeigt die Domänenliste an
show	*gslb-config dns rule*	Zeigt die DNS-Regelausgabe an
show	*gslb-config answer-group*	Zeigt die VIP-Antwort an

Citrix Delivery Controller (unter Windows)

Befehl	Parameter	Beschreibung
powershell	*Add-PSSnapin Citrix.Broker.Admin.V2; Get-BrokerApplication -Name [entry_point.name] | select Name,CommandLineExecutable,CommandLineArguments,WorkingDirecto | Format-List* und *Add-PSSnapin Citrix.Broker.Admin.V2; Get-BrokerApplication -Name [entry_point.name] | select Name,CommandLineExecutable,CommandLineArguments,WorkingDirecto | Format-List* Und *Add-PSSnapin Citrix.Broker.Admin.V2; Get-BrokerMachine -DesktopGroupName ' [delivery_groups[1].name]*	Ruft die von diesem Delivery Controller verwalteten Anwendungen ab

Citrix Usage Collector (unter Windows)

Befehl	Parameter	Beschreibung
qfarm		Erkennt Epic-Symbole

Citrix XenApp (unter Windows)

Befehl	Parameter	Beschreibung
get_xenapp_apps.ps1	*[entry_point.icon_path]*	Führt Powershell-Befehle aus, mit denen Citrix-Symbolinformationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Citrix XenApp (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
		aus dem Citrix-Repository abgerufen werden
powershell	Verschiedene Optionen	Führt PowerShell-Befehle aus

Citrix Presentation Server (unter Windows)

Befehl	Parameter	Beschreibung
cscript	*//NoLogo*	Führt VB-Skripts ohne Popup-Fenster aus
GetAppsInFolder.wsf	*[entry_point.icon_path]*	Führt vbscript-Befehle aus, mit denen Citrix-Symbolinformationen aus dem Citrix-Repository abgerufen werden

Citrix NetScaler (unter Citrix NetScaler)

Befehl	Parameter	Beschreibung
show	*cs policy, cs action,cs Policy, lb vserver*	Dieser Befehl wird nur zum Erkennen von ausgehenden Verbindungen verwendet. Zeigt die angeforderten Informationen an
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

Citrix NetScaler Global Server Load Balancer (unter Citrix NetScaler)

Befehl	Parameter	Beschreibung
show	*ns.conf*	Dieser Befehl wird nur zum Erkennen von ausgehenden Verbindungen verwendet, wenn keine SNMP- oder SSH-Anmeldeinformationen bereitgestellt wurden. Zeigt den Inhalt der Datei ns.conf an

Connect-IT Service (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connect-IT Service (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf

EMC Documentum Docbase (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

FormEngine (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Allgemeine Anwendung (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
tasklist	Verschiedene Optionen	Listet alle laufenden Aufgaben auf
netsh	*http show servicestate*	Zeigt einen Snapshot des HTTP-Service an

Allgemeine Anwendung (unter Linux)

Befehl	Parameter	Beschreibung
systemctl list-units --type service	Verschiedene Optionen	Zeigt den Servicestatus an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Anwendung (unter Linux) (Fortsetzung)

Befehl	Parameter	Beschreibung
`/bin/systemctl status "+service_name +".service`	Verschiedene Optionen	Zeigt den Servicestatus an
`service --status-all`	Verschiedene Optionen	Zeigt den Servicestatus an
`read /etc/services`	Verschiedene Optionen	Erteilt Zugriff auf die Datei

HAProxy (auf UNIX oder Windows)

Befehl	Parameter	Beschreibung
`ls`	Verschiedene Optionen	(Nur unter Unix) Listet Dateien und Ordner im angegebenen Ordner auf
`tail`	Verschiedene Optionen	(Nur unter Unix) Zeigt das Ende der Ausgabe an

HP Service Manager-Anwendungsserver

Befehl	Parameter	Beschreibung
`tnsping`	Verschiedene Optionen	Ruft Informationen über Oracle-Verbindungen ab
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf.
`ss`	Verschiedene Optionen	Listet die offenen Ports auf

HP Service Manager-Index (unter Windows)

Befehl	Parameter	Beschreibung
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf

HP Service Manager Knowledge Base (unter Windows)

Befehl	Parameter	Beschreibung
`netstat`	Verschiedene Optionen	Listet die offenen Ports auf

IBM WebSphere Message Broker (unter Windows)

Befehl	Parameter	Beschreibung

`dmqdocbroker`	`-s -c getdocbasemap`
	und
	`-t [computer_system.primaryHostname] -s -c getdocbasemap`
		Ruft die Docbase-Informationen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere Message Broker (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	und *-s -c getservermap [docbas]* *-t [computer_system.primaryHostname] -s -c getdocbasemap* [docbase]	
del	Verschiedene Optionen	Löscht die XML-Datei mit den alten Bindungsinformationen
BTSTask	*ExportBindings / Destination:%TEMP %|MyBindings.xml / Database:[MgmtDbName] / server:[serverName]*	Dieser Befehl wird nur verwendet, wenn keine MSSQL-Anmeldeinformationen vorhanden sind. Extrahiert die Bindungsinformationen und fügt sie in die XML-Datei ein

IBM CTRL-M Server (unter Unix oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf

IBM CICS Transaction Gateway CTG (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur für Windows) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM CICS Transaction Gateway CTG (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
type	–	(Nur für Windows) Dieser Befehl wird nur zum Erstellen von CICS-Verbindungen verwendet. Zeigt den Dateiinhalt in der Ausgabe an

IBM DB2 (unter Linux)

Befehl	Parameter	Beschreibung
Quelle	*[installed_dir]db2profile*	Legt die DB2-Variablen fest
db2	list database directory	Zeigt die DB2-Installationsparameter an
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
Kopf	*-1*	Zeigt nur die erste Zeile der Ausgabe an
db2level	–	Zeigt die DB2-Version an
cat	–	Zeigt den Dateiinhalt in der Ausgabe an
xargs	*-I {} echo list tablespace containers for {} ';'*	Dieser Befehl wird zum Erstellen von Speicherverbindungen verwendet. Führt den Befehl an allen Listen der Ausgabe aus

IBM DB2 (unter Windows)

Befehl	Parameter	Beschreibung
db2cmd	*/c /w /i*	Listet die DB2-Verzeichnisse auf
db2	list database directory	Zeigt die DB2-Installationsparameter an
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien, Ordnern oder einer Standardausgabe
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
db2level	–	Zeigt die DB2-Version an
echo	Verschiedene Optionen	Dieser Befehl wird nur für Speicherverbindungen verwendet. Gibt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM DB2 (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
		Zeichenfolgen in der Ausgabe aus
findstr	Verschiedene Optionen	Dieser Befehl wird nur für Speicherverbindungen verwendet. Extrahiert Zeichenfolgen aus der Ausgabe
für	Verschiedene Optionen	Dieser Befehl wird nur für Speicherverbindungen verwendet. Führt Schleifen aus

IBM DB2 (unter IBM z/OS)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Ruft den DB2-Namen ab

IBM J2EE EAR (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

IBM WebSphere Application Server (unter UNIX)

Befehl	Parameter	Beschreibung
versionInfo.sh	–	Ruft die Version von Websphere Application Server ab

IBM Websphere Application Server (unter IBM z/OS)

Befehl	Parameter	Beschreibung
"oeconsol 'D OMVS,A=ALL' | grep "+ $taskname	–	Ruft die Aufgabe von Websphere Application Server ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM Websphere Application Server (unter IBM z/OS) (Fortsetzung)

Befehl	Parameter	Beschreibung
netstat	*-a | grep "+$port+" | awk '{print $1}'*	Ruft den Aufgabennamen vom Listenerport ab
ps -ef -o user,pid,ppid,comm | awk '{print $1,$2,$3, $4}'		Ruft Attribute für Prozesse ab
$install_dir+"/bin/ versionInfo.sh | grep Version | tail -1"		Ruft die Version aus dem Skript ab
$install_dir +"/properties/version/ BASE.product"		Ruft die Version aus der Versionsdatei ab (Failover)
"ls "+$conf_dir +"/*/*/applications/ */deployments/*/META-INF/application.xml \| xargs grep \|"<context-root>/"+$uri_search +"|""+" 1>/tmp/app.txt 2>/dev/null; cat /tmp/ app.txt"		Ruft die Liste der URI-Dateien ab
$ear_directory_name +"//*/*/wsdl/*.wsdl"*		Liest die WSDL-Dateien unter der erkannten Inklusion im Ear-Verzeichnis

IBM WebSphere Portal (unter Linux)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	*-name* *-type*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens

IBM WebSphere Portal (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere Portal (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

IBM WebSphere Message Broker-Flow (unter UNIX)

Befehl	Parameter	Beschreibung
find	*-name* *-type*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens
mqsiprofile	-	Legt die Variablen für WebSphere Message Broker fest
mqsireportbroker	*[broker name]*	Ruft die WebSphere Message Broker-Informationen ab
mqsibrowse	*[broker name] -t BROKERRESOURCES*	Zeigt die Message Broker-Informationsressourcen an
echo	*$ODBCINI*	(Nur unter Unix) Dieser Befehl wird nur zum Erstellen von Verbindungen mit IBM DB2 verwendet. Gibt Zeichenfolgen in der Ausgabe aus

IBM WebSphere Message Broker-Flow (unter Windows)

Befehl	Parameter	Beschreibung
mqsiprofile	-	Legt die Variablen für WebSphere Message Broker fest
mqsireportbroker	*[broker name]*	Ruft die WebSphere Message Broker-Informationen ab
ps	*-ef*	Ruft die Prozessinformationen ab
mqsibrowse	*[broker name] -t BROKERRESOURCES*	Zeigt die Message Broker-Informationsressourcen an
db2		Zeigt DB2-Installationsparameter an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere Message Broker-Flow (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
		Datenbankverzeichnis und Knotenverzeichnis

IBM WebSphere Message Broker (unter UNIX)

Befehl	Parameter	Beschreibung
mqsiprofile	–	Legt die Variablen für WebSphere Message Broker fest
mqsireportbroker	*[broker name]*	Ruft die WebSphere Message Broker-Informationen ab
mqsibrowse	*[broker name] -t BROKERRESOURCES*	Zeigt die Message Broker-Informationsressourcen an
find	*-name* *-type*	Dieser Befehl wird nur zum Erstellen der Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens
echo	*$ODBCINI*	Dieser Befehl wird nur zum Erstellen von Verbindungen mit IBM DB2 verwendet. Gibt Zeichenfolgen in der Ausgabe aus

IBM WebSphere Message Broker (unter Windows)

Befehl	Parameter	Beschreibung
mqsiprofile	–	Legt die Variablen für WebSphere Message Broker fest
mqsireportbroker	*[broker name]*	Ruft die WebSphere Message Broker-Informationen ab
ps	*-ef*	Ruft die Prozessinformationen ab
mqsibrowse	*[broker name] -t BROKERRESOURCES*	Zeigt die Message Broker-Informationsressourcen an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM MQ (auf UNIX) – früher IBM WebSphere MQ

Befehl	Parameter	Beschreibung
dspmq	–	Ruft den Status des Warteschlangenmanagers ab
dspmqver	–	Ruft die Version des Warteschlangenmanagers ab
runmqsc	*[queue manager]*	Ruft die Warteschlangeninformationen ab

IBM MQ (auf Windows)

Befehl	Parameter	Beschreibung
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dspmq	–	Ruft den Status des Warteschlangenmanagers ab
dspmqver	–	Ruft die Version des Warteschlangenmanagers ab
runmqsc	*[queue manager]*	Ruft die Warteschlangeninformationen ab

IBM MQ (unter z/OS)

Befehl	Parameter	Beschreibung
netstat	*-a | grep "+$port*	Ruft den MQ-Namen IBM ab.
df	*-k | grep MQ"*	Ruft das Dateisystem ab
"echo "+ $netstat_info[1].mq_name +" | cut -c1-4"	–	Ruft den Namen des Warteschlangenmanagers ab
"oeconsol '-"+ $queue_manager+" display qmgr ALL' "	–	Ruft die Informationen zum logischen MQ-Namen ab
"oeconsol '-"+ $queue_manager+" display queue ("+ $entry_point.queue_name +") ALL' | tr |"(|" |"# |" | tr |")|" |"|""	–	Ruft die Informationen der MQ-Warteschlange zusammen mit den Informationen zu ihren Verbindungen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM MQ (unter z/OS) (Fortsetzung)

Befehl	Parameter	Beschreibung
"oeconsol '-"+ $queue_manager+" display queue ("+$name +")'"	–	Ruft die MQ-Warteschlangeninformationen ab
"oeconsol '-"+ $queue_manager +" display channel(*) CONNAME where(QMNAME EQ "+ $remote_queue_mngr_name +")'"	–	Ruft die Kanalinformationen ab
"oeconsol '-"+ $queue_manager+" display qlocal(*) '"		Ruft die lokalen Warteschlangeninformationen ab

IBM MQ-Warteschlange (auf UNIX) – früher IBM WebSphere MQ-Warteschlange

Befehl	Parameter	Beschreibung
dspmq	–	Ruft den Status des Warteschlangenmanagers ab
dspmqver	–	Ruft die Version des Warteschlangenmanagers ab
runmqsc	*[queue manager]*	Ruft die Warteschlangeninformationen ab

IBM MQ-Warteschlange (auf Windows)

Befehl	Parameter	Beschreibung
dspmq	–	Ruft den Status des Warteschlangenmanagers ab
dspmqver	–	Ruft die Version des Warteschlangenmanagers ab
runmqsc	*[queue manager]*	Ruft die Warteschlangeninformationen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JBoss-Modul (unter Unix oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur unter Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
netstat	Verschiedene Optionen	(Nur unter Windows) Listet die offenen Ports auf

JBoss (unter UNIX und Windows)

Befehl	Parameter	Beschreibung
find	*-name*	Sucht nach Dateien und Ordnern im angegebenen Ordner
xargs	*grep <string>*	Sucht Zeichenfolgen in allen Dateien, die in der Ausgabedatei gefunden wurden
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
netstat	Verschiedene Optionen	Listet die offenen Ports auf

JRun (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JRun WAR Inc (unter UNIX und Windows)

Befehl	Parameter	Beschreibung
find	*-name*	Sucht nach Dateien und Ordnern im angegebenen Ordner
xargs	*grep <string>*	Sucht Zeichenfolgen in den Dateien, die in der Ausgabedatei gefunden wurden
grep	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf

MicrosoftMicrosoft Azure Event Hubs Exchange CAS (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
hostname	–	Ruft den Hostnamen ab
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
tasklist	Verschiedene Optionen	Listet alle laufenden Aufgaben auf
del	Verschiedene Optionen	Löscht die XML-Datei mit den alten Bindungsinformationen
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
powershell	*Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-ExchangeServer -status -Identity [hostname]| export-clixml $env:TEMP |exchange_pwrshell_output.xml* und	Dieser Befehl wird nur verwendet, wenn Sie keine TCP-Verbindungen verwenden. Ruft CAS-Status, Serverrollen und Exchange-Einrichtungsstruktur ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MicrosoftMicrosoft Azure Event Hubs Exchange CAS (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	Add-PSSnapin Microsoft.Exchange.Manage *Get-ExchangeServer -status -Identity [hostname]| export-clixml $env:TEMP |exchange_pwrshell_output* und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-ExchangeServer| format-table -autosize -HideTableHeaders Name,Fqdn,IsMailboxServer* und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-ExchangeServer | format-table -autosize -HideTableHeaders Name,Fqdn,IsMailboxServer* und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-MailboxServer | format-list*	**Wichtig:** Verwenden Sie das Dollarzeichen ($) nicht in Anmeldeinformationen für Exchange CAS, da Service-Mapping das Dollarzeichen für Mustervariablen im PowerShell-Befehl verwendet.
find	Verschiedene Optionen	Dieser Befehl wird nur verwendet, wenn PowerShell nicht funktioniert. Sucht nach bestimmten Zeichenfolgen in den Dateien und Ordnern
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

MicrosoftMicrosoft Azure Event Hubs Dynamic CRM (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MicrosoftMicrosoft Azure Event Hubs Dynamic CRM (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

MicrosoftMicrosoft Azure Event Hubs BizTalk-Orchestrierung (unter Windows)

Befehl	Parameter	Beschreibung
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus

MicrosoftMicrosoft Azure Event Hubs BizTalk Server (unter Windows)

Befehl	Parameter	Beschreibung
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
del	Verschiedene Optionen	Löscht die XML-Datei mit den alten Bindungsinformationen
BTSTask	*ExportBindings /Destination:%TEMP%\MyBindings.xml /Database:[MgmtDbName] /server:[serverName]*	Dieser Befehl wird nur verwendet, wenn keine MSSQL-Anmeldeinformationen vorhanden sind. Extrahiert die Bindungsinformationen und platziert sie in der XML-Datei

MicrosoftMicrosoft Azure Event Hubs Exchange-Back-End-Server (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
hostname	–	Ruft den Hostnamen ab
tasklist	Verschiedene Optionen	Listet alle laufenden Aufgaben auf

MicrosoftMicrosoft Azure Event Hubs Exchange-Front-End-Server (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
hostname	–	Ruft den Hostnamen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MicrosoftMicrosoft Azure Event Hubs Exchange-Front-End-Server (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
tasklist	Verschiedene Optionen	Listet alle laufenden Aufgaben auf

MicrosoftMicrosoft Azure Event Hubs FAST Search Server (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

MicrosoftMicrosoft Azure Event Hubs Exchange-Hub-Transport-Server (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
hostname	–	Ruft den Hostnamen ab
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
tasklist	Verschiedene Optionen	Listet alle laufenden Aufgaben auf
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
del	Verschiedene Optionen	Löscht die XML-Datei mit den alten Bindungsinformationen
powershell	*Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-ExchangeServer -status -Identity [entry_point.host_name]| export-clixml $env:TEMP |exchange_pwrshell_output.xml* und	Dieser Befehl wird nur verwendet, wenn Sie keine TCP-Verbindungen verwenden. Liefert den CAS-Status, die Serverrollen und die Exchange-Einrichtungsstruktur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MicrosoftMicrosoft Azure Event Hubs Exchange-Hub-Transport-Server (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	"Add-PSSnapin Microsoft.Exchange.Manage Get-ExchangeServer -status -Identity [entry_point.host_name] | export-clixml $env:TEMP |exchange_pwrshell_output	**Wichtig:** Verwenden Sie das Dollarzeichen ($) nicht in Anmeldeinformationen für Exchange Hub Transport-Server, da Service-Mapping das Dollarzeichen für Mustervariablen im PowerShell-Befehl verwendet.
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

MicrosoftMicrosoft Azure Event Hubs Internet Information Services (IIS) (unter Windows)

Befehl	Parameter	Beschreibung
appcmd.exe	Verschiedene Optionen	Dieser Befehl wird nur für IIS Version 7 und höher verwendet. Ruft Informationen zum angegebenen Anwendungsnamen ab

Virtuelles Verzeichnis für MicrosoftMicrosoft Azure Event Hubs Internet Information Services (IIS) (unter Windows)

Befehl	Parameter	Beschreibung
appcmd.exe	Verschiedene Optionen	Dieser Befehl wird nur für IIS Version 7 und höher verwendet. Ruft Informationen zum angegebenen Anwendungsnamen ab
iisapp.vbs	Verschiedene Optionen	Dieser Befehl wird nur für IIS Version 6 verwendet. Ruft Informationen zum angegebenen Anwendungsnamen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Virtuelles Verzeichnis für MicrosoftMicrosoft Azure Event Hubs Internet Information Services (IIS) (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
netstat	Verschiedene Optionen	Listet die offenen Ports auf

MicrosoftMicrosoft Azure Event Hubs .NET-Befehle (unter Windows)

Befehl	Parameter	Beschreibung
ildasm.exe	Text, der den exe-Prozesspfad enthält	Diese Datei ist erforderlich, um den Vorgang zum Einfügen einer Datei für den ILDisassembler-Alias auszuführen. Diese Datei zerlegt Zeichenfolgen aus der .exe-Befehlsdatei.
.findstr	Verschiedene Optionen	Ruft die Zeichenfolgen aus der Ausgabe ab
dir	Verschiedene Optionen	Listet alle Dateien im angegebenen Ordner auf
connection_strings_browser.exe	*-encrypted_configs[*].Name*	Dieser Befehl wird nur zum Erstellen von verschlüsselten Datenbankverbindungen verwendet. Diese Datei ist erforderlich, um den Vorgang zum Einfügen einer Datei für den ConnectionStringsBrowser-Alias auszuführen. Entschlüsselt die Datenbankverbindungen

MicrosoftMicrosoft Azure Event Hubs Exchange-Postfach (unter Windows)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf
hostname	–	Ruft den Hostnamen ab
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MicrosoftMicrosoft Azure Event Hubs Exchange-Postfach (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
tasklist	Verschiedene Optionen	Listet alle laufenden Aufgaben auf
del	Verschiedene Optionen	Löscht die XML-Datei mit den alten Bindungsinformationen
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
powershell	*Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-ExchangeServer -status -Identity [entry_point.host_name]| export-clixml $env:TEMP |exchange_pwrshell_output.xml* und *Add-PSSnapin Microsoft.Exchange.Manage Get-ExchangeServer -status | export-clixml $env:TEMP |exchange_pwrshell_output* und *Add-PSSnapin Microsoft.Exchange.Manage Get-ExchangeServer -status -Identity [entry_point.host_name]| export-clixml $env:TEMP |exchange_pwrshell_output.xml* und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-ClusteredMailBoxServerStatus | format-table -Property OperationalMachines* und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-ExchangeServer | format-table -autosize -HideTableHeaders Name,Fqdn,IsHubTransportServer*	Dieser Befehl wird nur verwendet, wenn Sie keine TCP-Verbindungen verwenden. Ruft den Status, die Serverrollen und die Einrichtungsstruktur des Exchange-Postfachs ab **Wichtig:** Verwenden Sie das Dollarzeichen ($) nicht in Anmeldeinformationen für das Exchange-Postfach, da Service-Mapping das Dollarzeichen für Mustervariablen im PowerShell-Befehl verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MicrosoftMicrosoft Azure Event Hubs Exchange-Postfach (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-ExchangeServer | format-table -autosize -HideTableHeaders Name,Fqdn,IsHubTransportServer* und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-StorageGroup -server [hostname] | select SystemFolderPath | Export-Csv out.csv -notype;cat out.csv* und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.Admin; Get-StorageGroup | select SystemFolderPath | Export-Csv out.csv -notype;cat out.csv* und *Add-PSSnapin Microsoft.Exchange.Management.PowerShell.E2010; Get-MailboxDatabase | select LogFolderPath | format-table -autosize -hideTableHeaders; Get-MailboxDatabase | select EdbFilePath| format-table -autosize -hideTableHeaders;Get-MailboxDatabase | select TemporaryDataFolderPath| format-table -autosize -hideTableHeaders*	
find	Verschiedene Optionen	Dieser Befehl wird nur verwendet, wenn PowerShell nicht funktioniert. Sucht nach bestimmten Zeichenfolgen in den Dateien und Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MicrosoftMicrosoft Azure Event Hubs Exchange-Postfach (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

MicrosoftMicrosoft Azure Event Hubs SharePoint (unter Windows)

Befehl	Parameter	Beschreibung
hostname	–	Ruft den Hostnamen ab

MicrosoftMicrosoft Azure Event Hubs SQL-Datenbank (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
hostname	–	Ruft den Hostnamen ab
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
sqlcmd	*-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Q select nvcname###inboundtransporturl FROM adm_ReceiveLocation rl, bts_receiveport rp where rl.receiveportid=rp.nid* und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect nID,nvcName,nApplicationID from bts_receiveport* und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database]*	Dieser Befehl wird nur zum Erkennen von Microsoft BizTalk verwendet. Ruft die BizTalk-Informationen aus der Datenbank ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MicrosoftMicrosoft Azure Event Hubs SQL-Datenbank (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	-U [username] -P '[password]' -y 0 -h-1 -Qselect nID,nvcName,nApplicationID from bts_sendport und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect nOrcPortID,nReceivePortID,nSendPortid from bts_orchestration_port_binding* und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect nID,nOrchestrationID from bts_orchestration_port* und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect nID,nvcFullName from bts_orchestration* und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect ah.Name###bo.nvcNamespace.bo.nvcName###ase.Name*	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MicrosoftMicrosoft Azure Event Hubs SQL-Datenbank (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	from bts_orchestration bo, adm_Host ah,adm_server ase,adm_Server2HostMapping ash where bo.nAdminHostID = ah.ID and ase.ID = ash.ServerID and ah.ID = ash.HostID und *-Stcp: [computer_system.primaryManagementIP], [port] -d [entry_point.database] -U [username] -P '[password]' -y 0 -h-1 -Qselect nID,nSendPortID,nvcAddress from bts_sendport_transport*	

MicrosoftMicrosoft Azure Event Hubs Message Queuing (MSMQ) (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf

MicrosoftMicrosoft Azure Event Hubs SQL-Datenbank (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf
sqlservr.exe		Ruft die Version der Datenbank aus der ausführbaren Datei ab

MongoDB-Datenbank (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
mongo	--eval db.printShardingStatus()	Ruft den Status von MondoDB ab, der für den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MongoDB-Datenbank (unter Windows oder UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
		Lastenausgleich verwendet wird
mongo	--db.Name()	Ruft den Namen der mit dem MongoDB-Server verbundenen Datenbank ab

MySQL-Server (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
ps	*--pid=[process.pid] --no-headers -o " %U : %p : %a"*	Ruft den Parameterwert „userid“ ab
mysqld-nt/mysqld/ mysqld.exe	*-V*	Ruft die Version ab
mysql	*--user=[username] --password=[password] --port=[jdbc_port] --skip-column-names --silent --execute="SHOW ENGINE NDB STATUS;;"* und *--user=[username] --password=[password] --port=[jdbc_port] --skip-column-names --silent --execute="SHOW SLAVE STATUS;;"* und *--user=[username] --password=[password] --port=[jdbc_port] --skip-column-names --silent --execute="select host from information_schema.processlist where command like '%%binlog%%';;"*	Dieser Befehl wird nur zum Erstellen von Clusterknoten-Verbindungen sowie primären und sekundären Replikationen verwendet. Ruft die Bereitstellungsstruktur des MySQL-Servers ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Server (unter Windows oder UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
which	*mysql*	Dieser Befehl wird nur zum Erstellen von Clusterknoten-Verbindungen sowie primären und sekundären Replikationen verwendet. Ruft den vollständigen Pfad der MySQL-Clusterknoten ab

MySQL-Cluster-MGM-Knoten (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Verschiedene Optionen	Listet die offenen Ports auf
ndb_mgmd	*-V* und *-e show*	Ruft die Version und den Status des MySQL Cluster MGM-Knotens ab

Nginx (unter UNIX)

Befehl	Parameter	Beschreibung
nginx	*-v*	Ruft die Version ab
egrep	*-v -e ^# -e "|t#"*	Dieser Befehl wird bei Bedarf zum Erstellen von HTTP-Verbindungen verwendet. Ignoriert Sonderzeichen

Oracle E-Business Suite (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
export	–	(Nur für Unix) Legt Variablen fest

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle E-Business Suite (unter Windows oder UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
sqlplus	Verschiedene Optionen	Erstellt die Verbindung zur Oracle-Instanz
awk	Verschiedene Optionen	(Nur für Unix) Ändert die Ausgabe
netstat	Verschiedene Optionen	(Nur für Windows) Listet offene Ports auf

Oracle Advanced Queue-Warteschlange (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
export	–	(Nur unter Unix) Legt eine Variable fest
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus
sqlplus	Verschiedene Optionen	Erstellt die Verbindung zur Oracle-Instanz
set	–	(Nur unter Windows) Legt eine Variable fest
netstat	Verschiedene Optionen	(Nur unter Windows) Listet die offenen Ports auf

Oracle Concurrent Server (unter Windows oder UNIX)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
netstat	Verschiedene Optionen	(Nur für Windows) Listet die offenen Ports auf
awk	Verschiedene Optionen	(Nur für Unix) Ändert die Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Discoverer Engine (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle Discoverer-Benutzeroberfläche (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle Form-Benutzeroberfläche (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle Fulfillment Server (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle HTTP Server (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle Metric-Client (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle OACORE-Server (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
find	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern

Oracle OAFM-Server (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
find	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Database (unter UNIX)

Befehl	Parameter	Beschreibung
export	–	Legt die Variable fest
sqlplus	*-s [username]/ [password]@[entry_point.instance]*	Dieser Befehl wird nur zum Abrufen der Informationen zur erweiterten Warteschlange verwendet. Ruft die Oracle-Version und Informationen zur erweiterten Warteschlange ab
echo	*-e set head off feed off pages 0 line 3000| |n|"select NAME || '##' || QUEUE_TABLE || '##' || QID || '##' || QUEUE_TYPE || '##' || RETENTION from DBA_QUEUES where OWNER = UPPER([entry_point.scheme]);* und *set head off feed off pages 0 line 3000| |n|"select NAME || '##' || QUEUE_TABLE || '##' || QID || '##' || QUEUE_TYPE || '##' || RETENTION from DBA_QUEUES where OWNER = UPPER([entry_point.scheme]);* und *select member as NEEBULA from v| $logfile;* und *select value as NEEBULA from v\|$parameter where name='log_archive_dest'* und *select file_name as NEEBULA from dba_data_files;* und	Dieser Befehl wird nur zum Abrufen der Informationen zur erweiterten Warteschlange verwendet. Ruft die Informationen zur erweiterten Warteschlange, den Speichergeräten und Datenbanklinks ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Database (unter UNIX) (Fortsetzung)

Befehl	Parameter	Beschreibung
	select DB_LINK,HOST from DBA_DB_LINKS	
lsnrctl	*version* Und *services*	Dieser Befehl wird nur zur Erkennung der RAC-Version (Real Application Cluster) verwendet. Ruft die RAC-Version ab

Oracle Database (unter Windows)

Befehl	Parameter	Beschreibung
set	*-*	Legt die Variable fest
sqlplus	*-s [username]/ [password]@[entry_point.instance]*	Dieser Befehl wird nur zum Abrufen der Informationen zur erweiterten Warteschlange verwendet. Ruft die Oracle-Version und Informationen zur erweiterten Warteschlange ab
echo	*-e set head off feed off pages 0 line 3000| |n|"select NAME || '##' || QUEUE_TABLE || '##' || QID || '##' || QUEUE_TYPE || '##' || RETENTION from DBA_QUEUES where OWNER = UPPER([entry_point.scheme]);* und *set head off feed off pages 0 line 3000| |n|"select NAME || '##' || QUEUE_TABLE || '##' || QID || '##' || QUEUE_TYPE || '##' || RETENTION from DBA_QUEUES where OWNER = UPPER([entry_point.scheme]);* und	Dieser Befehl wird nur zum Abrufen der Informationen zur erweiterten Warteschlange verwendet. Ruft die Informationen zur erweiterten Warteschlange, den Speichergeräten und Datenbanklinks ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Database (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
	select member as NEEBULA from v|$logfile;* und *select value as NEEBULA from v\|$parameter where name='log_archive_dest' und *select file_name as NEEBULA from dba_data_files;* und *select DB_LINK,HOST from DBA_DB_LINKS*	
lsnrctl	*version* Und *services*	Dieser Befehl wird nur zur Erkennung der RAC-Version (Real Application Cluster) verwendet. Ruft die RAC-Version ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf

Oracle iAS-Webmodul (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
find	Verschiedene Optionen	Dieser Befehl wird nur zum Erstellen von Webservices-Verbindungen verwendet. Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern
netstat	Verschiedene Optionen	Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Net Listener (unter UNIX)

Befehl	Parameter	Beschreibung
lsnrctl	*version* und *status*	Ruft die Version und den Status des Oracle Net Listener ab
export	–	Legt die Variable fest
crsctl	*status res -t* und *config service -d*	Ruft den Servicestatus und die Konfiguration ab

Oracle PeopleSoft (unter UNIX)

Befehl	Parameter	Beschreibung
psadmin	Verschiedene Optionen	Ruft Informationen aus dem PeopleSoft-Repository oder -Server ab
tnsping	Verschiedene Optionen	Ruft Informationen zur Datenbankinstanz ab, die dem Befehl tnsping übergeben wurden
sqlplus	Verschiedene Optionen	Stellt eine Verbindung mit der Datenbankinstanz her und führt die SQL-Abfrage aus

Oracle-Prozessmanager (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
find	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern

Oracle Report Server (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Report Server (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
find	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern

Oracle Tnslsnr-Engine (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle WebLogic-Modul (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

Oracle WebLogic Server (Version 10.3) (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle WebLogic-On-Demand-Router-Lastenausgleichsmodul (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
versionInfo.sh	–	Ruft die Version von Websphere Application Server ab

Oracle Tuxedo (unter Unix oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene	(Nur für Windows) Listet alle vorhandenen Dateien im angegebenen Ordner auf
find	Verschiedene	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
find	*-name*	Dieser Befehl wird nur zum Erstellen von Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens
tmadmin	*-v*	Ruft die Tuxedo-Version ab
netstat	Verschiedene	Ruft offene Ports ab
ss	Verschiedene Optionen	Listet die offenen Ports auf

Oracle Tuxedo-Portal (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle Tuxedo-Portal (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
dir	Verschiedene	(Nur für Windows) Listet alle vorhandenen Dateien im angegebenen Ordner auf
find	Verschiedene	(Nur für Windows) Sucht nach bestimmten Zeichenfolgen in Dateien und Ordnern
find	*-name*	Dieser Befehl wird nur zum Erstellen von Webserviceverbindungen verwendet. Sucht nach Dateien und Ordnern eines bestimmten Namens

PostgreSQL-Datenbank (unter UNIX und Windows)

Befehl	Parameter	Beschreibung
postgres	*-v*	Ruft die Version ab
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf

Red Hat Cluster Suite (unter Linux)

Befehl	Parameter	Beschreibung
ps	*-ef*	Zeigt den derzeit ausgeführten Prozess an
grep	Verschiedene Optionen	Durchsucht Nur-Text-Datensätze nach Zeilen, die dem regulären Ausdruck entsprechen
grep	*-v <string>*	Durchsucht Nur-Text-Datensätze nach Zeilen, die nicht dem regulären Ausdruck entsprechen
ps	*-ef | grep corosync | grep -v grep'*	Überprüft, ob der Corosync-Prozess auf dem Server ausgeführt wird Wenn der Prozess ausgeführt wird, läuft das Red Hat-Cluster auf diesem Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Red Hat Cluster Suite (unter Linux) (Fortsetzung)

Befehl	Parameter	Beschreibung
ifconfig	–	Zeigt Informationen zur aktuellen Netzwerkkonfiguration an
ip a	–	Zeigt Informationen zur aktuellen Netzwerkkonfiguration an
awk	Verschiedene Optionen	Ändert die Ausgabe
hostname	*-s*	Zeigt den vollständig qualifizierten Domänennamen (FQDN) an
hostname	*-f*	Zeigt die Kurzform des Hostnamens an

SAP BO BOXI ScheduleRouter (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
type	–	
tnsping	*instance*	Dieser Befehl wird zum Erstellen von Verbindungen zu Oracle verwendet.

SAP Business Objects CMS-Server (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	(Nur für Windows) Extrahiert Zeichenfolgen aus der Ausgabe
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
tnsping	*instance*	Dieser Befehl wird zum Erstellen von Verbindungen zu Oracle verwendet. Ruft die Version ab

SAP-Zentralinstanz (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAP-Zentralinstanz (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
disp + work	*-V*	Ruft die Version ab
ping	*-n 1*	(Nur für Windows) Überprüft, ob der Host antwortet
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Listet die offenen Ports auf	Listet die offenen Ports auf

SAP NetWeaver-Dialoginstanz (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
disp + work	*-V*	Ruft die Version ab
ping	*-c 1*	(Nur für Unix) Überprüft, ob der Host antwortet
ping	*-n 1*	(Nur für Windows) Überprüft, ob der Host antwortet
netstat	Verschiedene Optionen	Listet die offenen Ports auf

SAP Evaluated Receipt Settlement (ERS) (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
disp + work	*-V*	Ruft die Version ab
ping	*-n 1*	(Nur für Windows) Überprüft, ob der Host antwortet
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Listet die offenen Ports auf	Listet die offenen Ports auf

SAP HANA-Datenbank (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
hdbsql	*-v*	Ruft die Version ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAP HANA-Datenbankkatalog unter UNIX

Befehl	Parameter	Beschreibung
hdbsql	Verschiedene Optionen	• Ruft Schemainformationen ab • Ruft die Zeitzone ab • Ruft die Datenträgergröße ab

SAP-Java-Cluster (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
jlaunch	*-V*	Ruft die Version ab
ping	*-n 1*	(Nur für Windows) Überprüft, ob der Host antwortet
netstat	Verschiedene Optionen	Listet die offenen Ports auf

SAP Central Services (SCS) (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf
msg_server	*-V*	Ruft die Version ab
ping	*-n 1*	(Nur für Windows) Überprüft, ob der Host antwortet
netstat	Verschiedene Optionen	Listet die offenen Ports auf
ss	Listet die offenen Ports auf	Listet die offenen Ports auf

SQL Server Analysis Services (SSAS) (unter Windows)

Befehl	Parameter	Beschreibung
MsMdSrv.exe	*-n*	Ruft den Instanznamen ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf

SQL Server Integration Services-Auftrag (SSIS) (unter Windows)

Befehl	Parameter	Beschreibung
MsMdSrv.exe	*-n*	Ruft den Instanznamen ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SQL Server Integration Services-Auftrag (SSIS) (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach den vorgegebenen Zeichenfolgen in der Datei und den Ordnern
sqlcmd	*-Stcp: [computer_system.primaryManagementIP], [port] -y 0 -h-1 -E -Qselect convert(varchar(max), convert(varbinary(max),packagedata))from msdb.dbo.sysssispackages where name = '[name]' -o [tmp_dir]/[name].xml* und *-Stcp: [computer_system.primaryManagementIP], [port] -y 0 -h-1 -E -Qselect convert(varchar(max), job_id)###[command]@@@ from msdb.dbo.sysjobsteps* und *-Stcp: [computer_system.primaryManagementIP], [port] -y 0 -h-1 -E -Qselect [name]###convert(varchar(max), job_id) from msdb.dbo.sysjobs*	Dieser Befehl wird nur zum Erkennen von Aufträgen verwendet.

SQL Server Integration Services (SSIS) (unter Windows)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
find	Verschiedene Optionen	Sucht nach den vorgegebenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SQL Server Integration Services (SSIS) (unter Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
		Zeichenfolgen in der Datei und den Ordnern
sqlcmd	*-Stcp: [computer_system.primaryManagementIP], [port] -h-1 -E -QSELECT [name]###DB FROM msdb.dbo.sysssispackages* und *-Stcp: [computer_system.managementIP], [port] -h-1 -E -QSELECT [name]###DB FROM msdb.dbo.sysssispackages* und *-Stcp: [computer_system.primaryManagementIP], [port] -h-1 -E -QSELECT [name]###JOB FROM msdb.dbo.sysjobs* und *-Stcp: [computer_system.managementIP], [port] -h-1 -E -Q SELECT [name]###JOB FROM msdb.dbo.sysjobs*	Dieser Befehl wird nur verwendet, wenn Sie Aufträge erkennen müssen.

Sun Directory (unter Solaris)

Befehl	Parameter	Beschreibung
slapd-dirserv	*-D [instance] -v*	Ruft die Version ab
netstat	Verschiedene Optionen	Listet die offenen Ports auf

Sun JES (unter Solaris)

Befehl	Parameter	Beschreibung
configutil	–	Ruft die JES-Konfiguration ab

Sybase (unter Unix oder Windows)

Befehl	Parameter	Beschreibung
dataserverv	*-v*	Ruft die Version ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sybase (unter Unix oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
dir	Verschiedene Optionen	(Nur für Windows) Listet Dateien und Ordner im angegebenen Ordner auf

Symantec Enterprise Vault (unter Windows)

Befehl	Parameter	Beschreibung
findstr	Verschiedene Optionen	Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf
ping	*-n 1[ip]*	Überprüft, ob der SQL-Server ausgeführt wird

TIBCO ActiveMatrix Adapter (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
hostname	–	Ruft den Hostnamen ab
"IFS=$'|n';for i in `find " + $tra_home + " -type f | grep -v / tmp | egrep |".process $\|.substvar$|"`; do result=`grep |"" + $entry_point.queue + "|" $i`; echo $i### $result@@@; done| grep -v |"###@@@|""	–	Scannt die Bezeichnungsdatei und stellt die tatsächlichen Werte bereit

TIBCO ActiveMatrix BusinessWorks (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
TibcoFilesParser.ksh	–	(Nur für Unix) Diese Datei ist erforderlich, um den Vorgang zum Einfügen einer Datei auszuführen. Dadurch werden alle Tags in Tibco-Konfigurationsdateien ersetzt und im Ordner /tmp abgelegt.
hostname	–	Ruft den Hostnamen ab
cd	–	(Nur unter Unix) Ändert das Verzeichnis
chmod	–	(Nur unter Unix) Ändert Dateiberechtigungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TIBCO ActiveMatrix BusinessWorks (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
für	Verschiedene Optionen	(Nur unter Unix) Führt Schleifen aus
echo	Verschiedene Optionen	(Nur unter Unix) Druckt Zeichenfolgen in der Ausgabe
if	Verschiedene Optionen	(Nur unter Unix) Startet eine Bedingung
wc	*-l*	(Nur unter Unix) Zählt die Ausgabezeilen
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf

TIBCO ActiveMatrix BusinessWorks-Prozess (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
hostname	–	Ruft den Hostnamen ab
cd	–	(Nur unter Unix) Ändert das Verzeichnis
chmod	–	(Nur unter Unix) Ändert Dateiberechtigungen
für	Verschiedene Optionen	(Nur unter Unix) Führt Schleifen aus
echo	Verschiedene Optionen	(Nur unter Unix) Druckt Zeichenfolgen in der Ausgabe
if	Verschiedene Optionen	(Nur unter Unix) Startet eine Bedingung
wc	*-l*	(Nur unter Unix) Zählt die Ausgabezeilen
dir	Verschiedene Optionen	(Nur unter Windows) Listet Dateien und Ordner im angegebenen Ordner auf
findstr	Verschiedene Optionen	(Nur unter Windows) Extrahiert Zeichenfolgen aus der Ausgabe
netstat	Verschiedene Optionen	Listet die offenen Ports auf.
ss	Listet die offenen Ports auf	Listet die offenen Ports auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

TIBCO ActiveMatrix BusinessWorks-Prozess (unter UNIX oder Windows) (Fortsetzung)

Befehl	Parameter	Beschreibung
cut	Verschiedene Optionen	(Nur unter Unix) Teil die Ausgabezeile

TIBCO Enterprise Message Service(EMS)-Warteschlange (unter UNIX oder Windows)

Befehl	Parameter	Beschreibung
rm	*-f /tmp/ems.cmd*	Bereitet das EMS-Skript vor
tibemsadmin	*-server tcp://+[computer_system.primary.dns.name]:[port] -user [username] -password [password] -script [script]*	Stellt eine Verbindung mit dem EMS-Administrator her und ruft die Liste der EMS-Warteschlangenverbraucher ab
echo	Verschiedene Optionen	Gibt Zeichenfolgen in der Ausgabe aus

TIBCO Enterprise Message Service (EMS) (unter UNIX und Windows)

Befehl	Parameter	Beschreibung
rm	*-f /tmp/ems.cmd*	Bereitet das EMS-Skript vor
tibemsadmin	*-server tcp://+[computer_system.primary.dns.name]:[port] -user [username] -password [password] -script [script]*	Stellt eine Verbindung mit dem EMS-Administrator her und ruft die Liste der EMS-Warteschlangenverbraucher ab
echo	Verschiedene Optionen	(Nur unter Windows) Druckt Zeichenfolgen in der Ausgabe

Zugehörige Informationen

Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern

SNMP-basierte Abfragen

Service-Mapping greift über SNMP v1/v2c/v3 (Simple Network Management Protocol) auf Geräte der Netzwerkinfrastruktur wie Lastenausgleichsmodule und Router zu. Konfigurieren Sie SNMP-Community-Anmeldeinformationen, um diesen Zugriffstyp zu aktivieren.

Konfigurieren Sie SNMP-Community, wenn Sie SNMP v1/v2 verwenden, bzw. SNMPv3-Anmeldeinformationen, wenn Sie SNMP v3 verwenden. Betriebsinformationen finden Sie unter SSH-Anmeldeinformationen .

SNMP-basierte Abfragen haben das Format von Zeichenfolgen mit ganzen Zahlen.

Allgemeine SNMP-basierte Abfragen

Stellen Sie sicher, dass der Benutzer über Anmeldeinformationen für SNMPv3 verfügt, es sei denn, es wird eine schreibgeschützte Community-Zeichenfolge verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- 1.3.6.1.2.1.47.1.1.1.1.13
- 1.3.6.1.2.1.1.6
- 1.3.6.1.2.1.47.1.1.1.1
- 1.3.6.1.4.1.9.9.774.1.1.1
- 1.3.6.1.4.1.9.6

SNMP-basierte Abfragen für Switches und Router

- 1.3.6.1.4.1.9.9.46.1.3.1.1
- 1.3.6.1.4.1.9.9.68.1.2.1.1
- 1.3.6.1.2.1.17.1.4.1
- 1.3.6.1.2.1.17.4.3.1
- 1.3.6.1.2.1.17.7.1.2.2.1
- 1.3.6.1.2.1.17.2.15.1
- 1.3.6.1.4.1.9.9.23.1.2.1.1
- 1.3.6.1.4.1.45.1.6.13.2.1.1
- 1.0.8802.1.1.2.1.4.2.1
- 1.0.8802.1.1.2.1.4.1.1

A10 Thunder-Serie

- 1.3.6.1.4.1.1872.2.5.1.1.1.11
- 1.3.6.1.4.1.1872.2.5.3.1.3.2.1
- 1.3.6.1.4.1.1872.2.5.3.1.2.4.1
- 1.3.6.1.4.1.1872.2.5.1.3.1.10
- 1.3.6.1.4.1.1872.2.5.4.1.1.4.2.1
- 1.3.6.1.4.1.1872.2.5.3.1.6.3.1
- 1.3.6.1.4.1.22610.2.4.1.1.1
- 1.3.6.1.4.1.22610.2.4.1.6.2
- 1.3.6.1.4.1.22610.2.4.3.4.1.2.1
- 1.3.6.1.4.1.22610.2.4.3.2.1.2.1
- 1.3.6.1.4.1.22610.2.4.3.3.1.2.1
- 1.3.6.1.4.1.22610.2.4.3.4.3.1.1
- 1.3.6.1.4.1.22610.2.4.3.3.3.1.1

BIG-IP Local Traffic Manager (LTM) F5 (unter F5 BIG-IP) und BIG-IP Global Traffic Manager (GTM) F5

- 1.3.6.1.4.1.3375.2.1.6.3
- 1.3.6.1.4.1.3375.2.1.4.1
- 1.3.6.1.4.1.3375.2.1.3.3.3
- 1.3.6.1.4.1.3375.2.1.6.2
- 1.3.6.1.4.1.3375.2.1.2.1.1.2.1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- 1.3.6.1.4.1.3375.2.2.10.1.2.1
- 1.3.6.1.4.1.3375.2.3.12.4.2.1
- 1.3.6.1.4.1.3375.2.3.12.1.2.1
- 1.3.6.1.4.1.3375.2.1.4.1
- 1.3.6.1.4.1.3375.2.1.6.2
- 1.3.6.1.4.1.3375.2.1.4.2
- 1.3.6.1.4.1.3375.2.2.10.1.2.1
- 1.3.6.1.4.1.3375.2.2.5.6.2.1
- 1.3.6.1.4.1.3375.2.2.10.8.2.1
- 1.3.6.1.4.1.3375.2.2.5.6.2.1
- 1.3.6.1.4.1.3375.2.2.10.1.2.1
- 1.3.6.1.4.1.3375.2.1.4.1
- 1.3.6.1.4.1.3375.2.1.4.2
- 1.3.6.1.4.1.3375.2.1.6.2
- 1.3.6.1.4.1.3375.2.3.11.1.2.1
- 1.3.6.1.4.1.3375.2.3.12.3.2.1
- 1.3.6.1.4.1.3375.2.3.12.4.2.1
- 1.3.6.1.4.1.3375.2.2.5.6.2.1
- 1.3.6.1.4.1.3375.2.3.12.3.2.1
- 1.3.6.1.4.1.3375.2.3.12.4.2.1
- 1.3.6.1.4.1.3375.2.3.12.5.2.1
- 1.3.6.1.4.1.3375.2.3.6.7.2.1
- 1.3.6.1.4.1.3375.2.3.11.4.2.1
- 1.3.6.1.4.1.3375.2.3.3.1.2.1
- 1.3.6.1.4.1.3375.2.3.3.3.2.1
- 1.3.6.1.4.1.3375.2.3.9.1.2.1
- 1.3.6.1.4.1.3375.2.3.9.3.2.1

Cisco Content Services Switch (CSS)

- 1.3.6.1.4.1.2467.1.16.4.1
- 1.3.6.1.4.1.2467.1.31.3
- 1.3.6.1.2.1.1.2
- 1.3.6.1.4.1.2467.4.1
- 1.3.6.1.4.1.2467.4.2
- 1.3.6.1.4.1.2467.4.3
- 1.3.6.1.4.1.2467.4.4
- 1.3.6.1.2.1.1.1
- 1.3.6.1.4.1.2467.1.15.2.1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- 1.3.6.1.4.1.2467.1.16.4.1
- 1.3.6.1.4.1.2467.1.18.2.1

Cisco Global Site Selector (GSS)

- 1.3.6.1.2.1.1.5 - zum Abrufen des Hostnamens
- 1.3.6.1.2.1.1.1 - zum Abrufen des Produktnamens

Citrix Netscaler

- 1.3.6.1.4.1.5951.4.1.3.6.1
- 1.3.6.1.4.1.5951.4.1.3.2.1
- 1.3.6.1.4.1.5951.4.1.3.1.1
- 1.3.6.1.4.1.5951.4.1.2.7.1
- 1.3.6.1.4.1.5951.4.1.2.2.1
- 1.3.6.1.4.1.5951.4.1.2.11.1
- 1.3.6.1.4.1.5951.4.1.2.1.1
- 1.3.6.1.4.1.5951.4.1.1.6
- 1.3.6.1.4.1.5951.4.1.1.26.1
- 1.3.6.1.4.1.5951.4.1.1.24.1
- 1.3.6.1.4.1.5951.4.1.1.14
- 1.3.6.1.2.1.55.1.8.1
- 1.3.6.1.2.1.47.1.1.1.1
- 1.3.6.1.2.1.4.20.1
- 1.3.6.1.2.1.2.2.1
- 1.3.6.1.2.1.2.2.1
- 1.3.6.1.2.1.1.5

Citrix NetScaler Global Server-Lastenausgleichsmodul

- 1.3.6.1.4.1.5951.4.1.1.51.3.1.1
- 1.3.6.1.4.1.5951.4.1.2.1.1

HPE BladeSystem-Gehäuse

- 1.3.6.1.4.1.232.22.2.3.1
- 1.3.6.1.4.1.11.5.7.1.2

IBM WebSphere DataPower

- Für die Horizontal-Discovery des Hostservers von DataPower [cmdb_ci_datapower_server]:
  - 1.3.6.1.2.1.1.1
  - 1.3.6.1.2.1.1.5
  - 1.3.6.1.2.1.4.20.1
  - 1.3.6.1.2.1.2.2.1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- 1.3.6.1.4.1.14685.3.1.196.1
- 1.3.6.1.4.1.14685.3.1.11.1
- 1.3.6.1.4.1.14685.3.1.112.1

- Für die Top Down-Discovery des Hostservers für DataPower [cmdb_ci_datapower_server]:
  - 1.3.6.1.2.1.1.1
  - 1.3.6.1.2.1.1.5
  - 1.3.6.1.4.1.14685.3.1.11.1

Juniper Junos

1.3.6.1.4.1.2636.3.1.3

Filer Storage-Array für Netzwerkgerät

- 1.3.6.1.4.1.789.1.1.2
- 1.3.6.1.4.1.789.1.1.9

Radware Alteon NG

- 1.3.6.1.4.1.1872.2.5.4.2.32.1
- 1.3.6.1.4.1.1872.2.5.1.1.1.11
- 1.3.6.1.4.1.1872.2.5.3.1.3.2.1
- 1.3.6.1.4.1.1872.2.5.3.1.2.4.1
- 1.3.6.1.4.1.1872.2.5.1.3.1.10
- 1.3.6.1.4.1.1872.2.5.4.1.1.4.2.1
- 1.3.6.1.4.1.1872.2.5.3.1.6.3.1
- 1.3.6.1.4.1.1872.2.5.4.1.1.4.2.1
- 1.3.6.1.2.1.1.1
- 1.3.6.1.4.1.1872.2.5.4.1.1.4.5.1
- 1.3.6.1.4.1.1872.2.5.4.1.1.3.3.1
- 1.3.6.1.4.1.1872.2.5.4.1.1.2.2.1
- 1.3.6.1.2.1.4.24.4.1
- 1.3.6.1.4.1.89.35.1.13.1.2
- 1.3.6.1.4.1.89.2.12
- 1.3.6.1.4.1.89.2.4
- 1.3.6.1.4.1.89.35.1.40.52.1.1
- 1.3.6.1.4.1.89.35.1.13.1
- 1.3.6.1.4.1.89.35.1.30.1
- 1.3.6.1.2.1.68.1.3.1
- 1.3.6.1.4.1.89.35.1.13.1
- 1.3.6.1.4.1.89.35.1.11.1
- 1.3.6.1.4.1.89.35.1.40.52.1.1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

ITOM Content Service – Referenz

Erkennungsverhalten für Unix-basierte Lastenausgleichsmodule erstellen

Wenn Ihr Netzwerk Lastenausgleichsmodule verwendet, die auf Linux-Hosts ausgeführt werden, erstellen Sie ein Erkennungsverhalten, um sicherzustellen, dass Service-Mapping und Discovery diese korrekt erkennen.

Vorbereitungen

Stellen Sie sicher, dass Discovery aktiviert ist.

Erforderliche Rolle: service_mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Der Erkennungs- und Zuordnungsprozess beginnt mit der Identifizierung des Hosts durch Discovery. Nach Abschluss der Host-Erkennung startet Service-Mapping die Erkennung, um auf diesem Host ausgeführte Anwendungen zu erkennen und zuzuordnen.

Der Standarderkennungsprozess identifiziert ein Configuration Item (CI) als Linux-Server, wenn ein verwendeter SSH-Port gefunden wird. Dies kann zu einer falschen Erkennung von Lastenausgleichsmodulen führen, die unter Linux als Linux-Server ausgeführt werden. Erstellen Sie ein Erkennungsverhalten, um zuerst Netzwerkgeräte mit dem SNMP-Protokoll zu erkennen. Nachdem Discovery Unix-basierte Lastenausgleichsmodule korrekt erkannt und die entsprechenden CIs dafür erstellt hat, können Sie mit dem Erkennen und Zuordnen von Anwendungsservices in Service-Mappingfortfahren.

Discovery führt die Erkennung über einen MID-Server durch, der sich im privaten Unternehmensnetzwerk befindet. Ein Verhalten bestimmt:

- Welchen MID Server Discovery verwendet
- Welche Probes und Muster des ausgewählten MID-Servers ausgeführt werden

Prozedur

1. Erstellen Sie ein neues Verhalten zum Erkennen von Unix-basierten Lastenausgleichsmodulen:
   a. Navigieren zu **Service-Mapping** > **Administration** > **Verhalten**.
   b. Klicken Sie auf **Neu**.
   c. Geben Sie den Namen für dieses Verhalten ein.
   d. Klicken Sie mit der rechten Maustaste auf den Header und wählen Sie **Speichern** aus.
   e. Klicken Sie auf der Registerkarte **Discovery-Funktionalität** auf **Neu**.
   f. Geben Sie 1 in das Feld **Phase** ein.
   g. Wählen Sie **Nur SNMP** aus der Liste der **Funktionalitätendefinition** aus.
   h. Wählen Sie im Bereich **MID Server** die relevanten MID Servers aus.
   i. Aktivieren Sie das Kontrollkästchen **Aktiv**.
   j. Klicken Sie auf **Absenden**.
2. Erstellen Sie einen Erkennungszeitplan für das neu definierte Verhalten:
   a. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
   b. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Füllen Sie die Felder wie folgt aus:

Erkennungszeitplan-Formular für Discovery

Feld	Beschreibung
Name	Geben Sie einen eindeutigen, beschreibenden Namen für den Zeitplan ein.
Erkennen	Wählen Sie **Konfigurationselemente** aus.
Methode für MID Server-Auswahl	Wählen Sie **Verhalten verwenden** aus.
Verhalten	Wählen Sie das Verhalten aus, das Sie in Schritt 1 erstellt haben.
Aktiv	Aktivieren Sie das Kontrollkästchen, um diesen Zeitplan zu aktivieren. Wenn Sie das Kontrollkästchen deaktivieren, wird der Zeitplan deaktiviert. Sie können über dieses Formular jedoch weiterhin manuell eine Erkennung mit den konfigurierten Werten ausführen.
Max. Ausführungszeit	Legen Sie eine Zeitbegrenzung für die Ausführung dieses Zeitplans fest. Nach Ablauf der konfigurierten Zeit werden die verbleibenden Aufgaben für die Erkennung abgebrochen, auch wenn der Scan nicht abgeschlossen ist. Verwenden Sie dieses Feld, um die Systemlast auf ein gewünschtes Zeitfenster zu beschränken. Wenn in dieses Feld kein Wert eingegeben wird, wird dieser Zeitplan solange ausgeführt, bis er abgeschlossen ist.
„Ausführen“ und zugehörige Felder	Bestimmt den Ausführungszeitplan der Erkennung. Konfigurieren Sie die Häufigkeit im Feld **Ausführen** und in den anderen Feldern, die angezeigt werden, um eine genaue Zeit anzugeben. **Hinweis:** Für die Ausführungszeit wird immer die Systemzeitzone verwendet. Wenn Sie das optionale Feld **Als tz ausführen** hinzufügen, hat dies keine Auswirkungen auf die tatsächliche Ausführungszeit.

3. Erstellen Sie einen IP-Adressbereich für den Erkennungszeitplan:

Wichtig: Der IP-Bereich für den Zeitplan muss zum IP-Bereich von MID-Server passen, den Sie dem Verhalten zugewiesen haben. Auch der MID-Server muss über die entsprechende Anwendung oder die Anwendung **ALL** verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf der Registerkarte mit den Erkennungs-IP-Bereichen auf **Neu**.

b. Geben Sie den Namen für diesen IP-Bereich ein.

c. Konfigurieren Sie den IP-Bereich, indem Sie IP-Adressen in die Felder **IP-Startadresse** und **IP-Endadresse** eingeben.

4. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Musterbasierte Erkennung in Service-Mapping

MID-Server

Sicherstellen, dass Service-Mapping ordnungsgemäß eingerichtet ist

Stellen Sie vor dem Zuordnen von Anwendungsservices sicher, dass Sie die MID Servers für die Erkennung von Anwendungsservices konfiguriert und alle erforderlichen Host- und Anwendungsanmeldeinformationen angegeben haben.

Vorbereitungen

Um die Bereitschaft der Zuordnung basierend auf Predictive Intelligence zu überprüfen, installieren Sie Service Mapping Plus aus dem ServiceNow Store.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Service-Mapping führt einen automatischen Scan der folgenden Ressourcen und Konfigurationen durch, um Ihnen den Bereitschaftsstatus zu geben:

- (Obligatorisch) Es gibt MID Servers mit korrekt konfigurierten IP-Bereichen und Einstellungen für Anwendungen und Funktionen. Weitere Informationen finden Sie unter Konfiguration des MID Servers für Service-Mapping.

  Wenn bei dieser Überprüfung keine richtig konfigurierten MID Servers erkannt werden, können Sie die Massenerkennung nicht ausführen.

- (Optional) Es gibt Anmeldeinformationen für Betriebssysteme und Anwendungen wie in Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping beschrieben.
- (Optional) Während der horizontalen Erkennung wurden mindestens drei Lastenausgleichsmodule erkannt.
- (Optional) In den letzten 14 Tagen wurden durch die horizontale Erkennung mindestens 100 Hosts erkannt.
- (Optional) Die Datensammlung mithilfe von Netflow- oder VPC Flow-Protokollen ist konfiguriert. Diese Konfiguration ist erforderlich, um die datenverkehrsbasierte Erkennung in Service-Mapping zu verbessern. Weitere Informationen finden Sie unter Datenerfassung und -erkennung mit Netflow und Datenerfassung und -erkennung mit VPC-Flow-Protokollen.
- (Optional) Cloud-Discovery ist aktiviert und konfiguriert. Diese Einstellung ist erforderlich, um Anwendungsservices basierend auf IaaS zu erkennen.

Wenn eine optionale Ressource oder Konfiguration fehlt, können Sie Anwendungsservices zwar weiterhin zuordnen, dies kann jedoch dazu führen, dass einige CIs und Verbindungen nur teilweise erkannt werden.

Darüber hinaus führt Service-Mapping die Bereitschaftsprüfung für die Zuordnungsfunktionalität basierend auf Predictive Intelligence durch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die von Service-Mapping erkannt werden können oder bereits erkannt wurden. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mit der API erstellt wurden.
2. Überprüfen Sie, dass Service-Mapping eingerichtet und bereit für die Discovery ist.
   Wenn einige obligatorische Konfigurationen fehlen, wird der Fehler oben im Fenster angezeigt.

   a. Klicken Sie auf den Link im Fehler, oder klicken Sie auf das Symbol **Bereitschaftsprüfliste** ( ).

   b. Klicken Sie im Service-Mapping-Fenster „Bereitschaftsprüfliste“ auf den Link neben der Setup-Kategorie mit dem Fehlersymbol ( ).
   Sie können nur dann eine Discovery und Zuordnung durchführen, wenn das Fenster „Bereitschafts-Prüfliste“ keine Fehler enthält.

   c. Führen Sie die erforderliche Aktion aus, um das Setup abzuschließen.
   Konfigurieren Sie beispielsweise fehlende Anmeldeinformationen.

3. Wenn mehr als eine Setup-Kategorie einen Fehler aufweist, kehren Sie zum Fenster „Bereitschafts-Checkliste" zurück, und beheben Sie alle anderen Fehler.
4. Überprüfen Sie, dass Service-Mapping basierend auf Predictive Intelligence bereit für die Erkennung ist.

   a. Navigieren zu **Alle** > > **Service-Mapping** > **Bereitschaft des Anwendungsservice**und wählen Sie dann **Homepage**aus.

   b. Stellen Sie sicher, dass sich alle Elemente in der Liste **Prerequisites status** (Status der Voraussetzungen) im Status **Bereit** befinden.
   Wenn eine der Voraussetzungen nicht erfüllt ist, führen Sie das erforderliche Verfahren aus und wählen Sie dann **Check readiness** (Bereitschaft prüfen) aus.

Nächste Maßnahme

Geschäftsservices im Stapel zuordnen

Zugehörige Informationen

Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich

Schnellstarttests für Service-Mapping

Führen Sie nach der Aktualisierung und Bereitstellung neuer Anwendungen oder Integrationen Schnellstarttests durch, um sicherzustellen, dass Service-Mapping weiterhin funktioniert. Wenn Sie Service-Mappingangepasst haben, kopieren Sie die Schnellstarttests, und konfigurieren Sie sie für Ihre Anpassungen.

Service-Mapping-Schnellstarttests erfordern die Aktivierung des Plugins „Service-Mapping“ (com.snc.service-mapping) und das Laden der Demodaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping-Schnellstarttests

Test	Beschreibung	Release-Version
SM OOTB: Testet die Sichtbarkeit der SM-Anwendung nach Rollen	Validiert die Sichtbarkeit von Service-Mapping-Anwendungen und -Modulen für verschiedene Rollen. Der Test überprüft zum Beispiel, ob ein Anwender, der mit der Rolle service_mapping_user eingeloggt ist, auf das Administrations-Modul unter Service-Mapping zugreifen kann.	Madrid
SM OOTB: Verifizierung der Servicezuordnung	Testvorlage zur Erstellung anwenderdefinierter Tests, die verifizieren, dass die Topologie der wichtigsten Services nicht geändert wurde. Konfiguriert Werte unter „Datensätze der Testausführung“, um den Namen des zu testenden Service und die in diesem Service erwarteten Knoten zu identifizieren. Geben Sie für die Knotennamenwerte das Knotenattribut genau so ein, wie es in der Zuordnung angezeigt wird, z. B. „Apache-Server“. Wenn der Attributname für einen Knoten abgeschnitten ist oder anzeigt, dass ein Knoten ein CI-Cluster ist, konfigurieren Sie diesen Knotennamenswert so, dass er die Darstellung in der Zuordnung widerspiegelt, beispielsweise „11x ExchangeF“ für eine Gruppe von 11 Exchange-Frontend-Servern.	Orlando, aktualisiert in Paris

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping-Schnellstarttests (Fortsetzung)

Test	Beschreibung	Release-Version
	Hinweis: Sie können diesen Test nicht verwenden, um den Serviceinhalt über die oberste, nicht erweiterte Ebene hinaus zu überprüfen.	
SM OOTB: UI-Barrierefreiheit nach einem Upgrade überprüfen	Führen Sie diesen Test aus, um zu prüfen, ob die Service-Mapping-Anwenderoberfläche nach einem Upgrade vollständig funktionsfähig ist.	Orlando

Zugehörige Informationen

Einen automatisierten Test ausführen

Erweiterte Konfiguration von Service Mapping

Optimieren Sie die Zusammenarbeit von Service-Mapping mit anderen Komponenten und Modulen, und passen Sie die Datenanzeige in für Servicezuordnungen an.

Zusätzlich zu dem unter Service-Mapping konfigurieren beschriebenen Basissetup können Sie optionale Konfigurationen entsprechend den Anforderungen Ihres Unternehmens vornehmen.

- Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren
- Konfiguration der Tag-basierten Discovery
- Konfigurationsdateien nachverfolgen
- Nachverfolgung von Changes für die Change-Historie feintunen
- Datenerfassung und -erkennung mit Netflow
- Datenerfassung und -erkennung mit VPC-Flow-Protokollen
- Suchassistenten für Windows konfigurieren
- Anzeige für CI-Attribute ändern
- Unterstützung für Windows-Server mit nicht-englischen Betriebssystemen konfigurieren
- Datei rctrlx.exe auf MID Servers hochladen
- Optimieren Sie Service-Mapping mit MID-Affinität und Wiederverwendung von IPs

Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren

Service-Mapping kann CIs erkennen und zuordnen, indem der ein- und ausgehende Datenverkehr erkannt wird, den die CIs generieren. Erstellen Sie eine datenverkehrsbasierte Erkennungsregel, um zu bestimmen, welche Konfigurationselemente für die datenverkehrsbasierte Zuordnung verfügbar sind.

Vorbereitungen

Wenn in Ihrer ServiceNow-Instanz Domänentrennung eingesetzt wird und Sie Zugriff auf die globale Domäne haben, melden Sie sich bei der entsprechenden Domäne an. Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: service_mapping_admin

- Stellen Sie sicher, dass die Traffic-basierte Discovery auf der Produktebene Service-Mapping aktiviert ist: Navigieren Sie zu **Service-Mapping** > **Administration** > **Eigenschaften** und vergewissern Sie sich, dass das Kontrollkästchen **Traffic-basierte Discovery** aktiviert ist.
- Aktivieren Sie die datenverkehrsbasierte Erkennung für einen bestimmten für Service (siehe Beschreibung in Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping).

Warum und wann dieser Vorgang ausgeführt wird

Zusätzlich zur musterbasierten Zuordnung können Sie die datenverkehrsbasierte Erkennung verwenden.

Sie können Regeln erstellen, um Service-Mapping für die Verwendung der datenverkehrsbasierten Erkennung für bestimmte CIs zu konfigurieren. Sie können datenverkehrsbasierte Erkennungsregeln konfigurieren, um bestimmte CIs oder CI-Typen zu überwachen.

Regeln für bestimmte CIs haben Vorrang vor Regeln für CI-Typen. Wenn Sie beispielsweise keine Traffic-basierte Discovery auf Apache Tomcat-Servern verwenden möchten, können Sie eine Regel vom **CI-Typ** festlegen, die die Traffic-basierte Discovery für die Tomcat-Tabelle deaktiviert. Gleichzeitig können Sie eine Discovery-Regel erstellen, die die Traffic-basierte Discovery für einen bestimmten Tomcat-Server aktiviert. In diesem Fall verwendet Service-Mapping die Traffic-basierte Discovery unter allen Tomcat-Servern nur für diesen bestimmten Tomcat-Server.

Je nach Konfiguration ist das Systemverhalten bei der datenverkehrsbasierten Erkennung anders. Wenn die Discovery basierend auf Predictive Intelligence aktiviert ist, fügt Service-Mapping basierend auf Verbindungsregeln automatisch Verbindungen zu Serviceinstanzen hinzu. Service-Mapping generiert diese Vorschläge basierend auf datenverkehrsbezogenen Daten aus der Configuration Management Database (CMDB) und der Analyse von Anwendungsfingerabdrücken, CIs und Prozessen durch Predictive Intelligence.

Wenn Discovery-basierte Predictive Intelligence deaktiviert sind, fügt Service-Mapping automatisch datenverkehrsbasierte Verbindungen basierend auf den Daten CMDB zu Serviceinstanzen hinzu. Möglicherweise müssen Sie Verbindungen entfernen, die zu irrelevanten CIs führen, um Serviceinstanzen übersichtlicher zu gestalten. Weitere Informationen zur datenverkehrsbasierten Methode finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Wenn in Ihrer Instanz Domänentrennung verwendet wird, können Sie datenverkehrsbasierte Regeln für bestimmte Domänen erstellen. Regeln im Basissystem werden der globalen Domäne zugewiesen und gelten für alle Domänen aller Ebenen.

Wenn Sie eine Regel für eine bestimmte Domäne erstellen, wird die neue Regel nur für diese Domäne verwendet und ist in keiner anderen Domäne vorhanden. Wenn Sie eine vorhandene Regel in der globalen Domäne anpassen und einer bestimmten Domäne zuweisen, erstellen Sie eine Kopie der globalen Regel, die weiterhin in allen anderen Domänen verwendet wird, mit Ausnahme der Domäne mit der angepassten Version dieser Regel. Wenn Sie eine Regel in der globalen Domäne anpassen, wirkt sich die Änderung auf alle Domänen aus, mit Ausnahme derjenigen, in der eine angepasste Kopie dieser Regel verwendet wird.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Verkehrsbasierte Discovery**.
2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Definieren Sie die Regelparameter wie folgt:

Feld	Beschreibung
Aktion	Wählen Sie **Aktivieren** aus, um dem spezifischen CI oder CI-Typ datenverkehrsbasierte Verbindungen hinzuzufügen.
Regelumfang	Wählen Sie **Spezifischer CI**, aus um Datenverkehr für ein Konfigurationselement zu erkennen, bzw. **CI-Typ**, um Datenverkehr für alle Konfigurationselemente in einer der CI-basierten Tabellen zu erkennen.
CI/CI-Typ	Wählen Sie ein bestimmtes CI aus, oder wählen Sie die Tabelle mit den CIs aus, für die Sie Datenverkehr erkennen möchten.
Domäne	Wählen Sie die Domäne aus, zu der die Regel gehört.

4. Klicken Sie auf **Absenden**.
5. Definieren Sie zur Feinabstimmung der datenverkehrsbasierten Erkennung wie folgt erweiterte Parameter:

Parameter	Beschreibung
sa.traffic_based_discovery.conn_aging_time	Zeitraum in Stunden, für den eine datenverkehrsbasierte Verbindung seit der letzten Erkennung aktiv bleibt ◦ **Typ**: Ganzzahl ◦ **Standardwert**: 72 ◦ **Andere mögliche Werte**: beliebige Zahl über 24 ◦ **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sa.traffic_based_discovery.ignored_ports	Bei einer datenverkehrsbasierten Erkennung gefundene Ports, die ignoriert werden können. Diese Eigenschaft ist in der Tabelle für Systemeigenschaften [sys_properties] verfügbar. Ändern Sie diese Eigenschaft, um Ports zu definieren, die Service-Mapping bei der datenverkehrsbasierten Erkennung ignoriert. Dadurch wird die Erkennung effizienter, da keine Ressourcen für die Erkennung irrelevanter Verbindungen verschwendet werden. ◦ **Typ**: Zeichenfolge ◦ **Standardwert**: 445, 139, 111, 2049, 860, 3260, 135, 53

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
	◦ **Andere mögliche Werte**: alle relevanten Portnummern ◦ **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.traffic_based_discovery.max_connections	Maximale Anzahl datenverkehrsbasierter Verbindungen von einem einzelnen CI. Diese Eigenschaft ist in der Tabelle für Systemeigenschaften [sys_properties] verfügbar. Diese Eigenschaft trägt dazu bei, die Größe der Zuordnung angemessen zu halten, indem die Anzahl der möglichen CI-Verbindungen begrenzt wird. ◦ **Typ**: Ganzzahl ◦ **Standardwert**: 30 ◦ **Andere mögliche Werte**: beliebige Zahl über 1 ◦ **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]

Konfiguration der Tag-basierten Discovery

Sie können die Standardkonfiguration verfeinern, um zu steuern, welche CIs Service-Mapping während des Tag-basierten Discovery-Prozesses in Anwendungsservices aufgenommen werden.

Service-Mapping stellt vorkonfigurierte CI-Beziehungen bereit, die an der Tag-basierten Discovery teilnehmen können. Sie können diese CI-Beziehungen anpassen und die Standardkonfiguration mit einer der folgenden Methoden verfeinern:

- CIs basierend auf Klassen in die Tag-basierte Discovery einbeziehen;
- CIs basierend auf ihrem Installationsstatus ausschließen
- vorkonfigurierte CI-Beziehungen ausschließen
- CI-Beziehungen hinzufügen oder bearbeiten.

Informationen zum Anzeigen vorkonfigurierter CI-Beziehungen, die Service-Mapping während der Tag-basierten Discovery in Anwendungsservices einschließt, finden Sie unter Vorkonfigurierte CI-Beziehungen in Tag-basierter Discovery.

Informationen zum Anzeigen von mit Service-Mapping installierten Eigenschaften, die sich auf die Tag-basierte Discovery beziehen, finden Sie unter Eigenschaften im Zusammenhang mit der Tag-basierten Discovery.

Schließen Sie CIs basierend auf Klassen in die Tag-basierte Discovery ein

Verwenden Sie CI-Klassen, um zu identifizieren, welche CIs Service-Mapping während der Tag-basierten Discovery in Anwendungsservices einbezieht. Standardmäßig erscheint diese Liste leer und enthält alle CIs, die zu allen CI-Klassen gehören. Definieren Sie CI-Klassen und

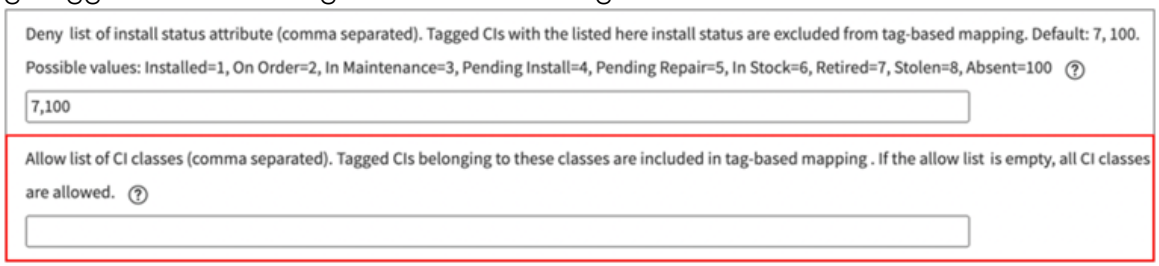
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

lassen Sie zu, dass nur CIs, die zu diesen Klassen oder ihren Erweiterungen gehören, an der Tag-basierten Discovery teilnehmen.

Vorbereitungen
Erfahren Sie mehr über die Konfiguration der Standardfunktion in Tag-basierter Discovery in Service-Mapping.

Erforderliche Rolle: service_mapping_admin

Prozedur
1. Navigieren zu **Service-Mapping** > **Administration** > **Eigenschaften**.
2. Geben Sie CI-Klassen durch Kommas getrennt in die Allow-Liste ein, die steuert, welche getaggten CIs an der Tag-basierten Zuordnung teilnehmen.



3. Klicken Sie auf **Speichern**.

Nächste Maßnahme
Wenn Sie die Standardkonfiguration verfeinern, nachdem Sie Anwendungen basierend auf Tags erstellt haben, finden Sie unter Zuvor erstellte Anwendungsservices neu berechnen für die nächsten Schritte.

Schließen Sie CIs basierend auf ihrem Installationsstatus in der Tag-basierten Discovery aus

Verwenden Sie den CI-Installationsstatus, um CI-Klassen zu erstellen und CIs während der Tag-basierten Erkennung aus Anwendungsservices auszuschließen. Standardmäßig schließen Anwendungsservices basierend auf Tags CIs mit dem Installationsstatus Deaktiviert oder Abwesend aus. Sie können diese Liste der ausgeschlossenen CIs erweitern, um zusätzliche Installationsstatus wie Ausstehende Installation oder Gestohlen hinzuzufügen.

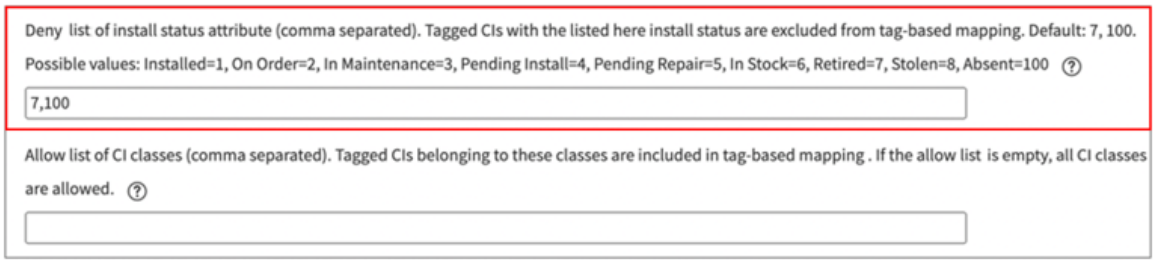
Vorbereitungen
Erfahren Sie mehr über die Konfiguration der Standardfunktion in Tag-basierter Discovery in Service-Mapping.

Erforderliche Rolle: service_mapping_admin

Prozedur
1. Navigieren zu **Service-Mapping** > **Administration** > **Eigenschaften**.
2. Geben Sie Werte für den Installationsstatus in die Deny-Liste ein, die steuert, welche CIs basierend auf dem Installationsstatus von der Tag-basierten Zuordnung ausgeschlossen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie Kommas, um die Werte zu trennen.



3. Klicken Sie auf **Speichern**.

Nächste Maßnahme

Wenn Sie die Standardkonfiguration verfeinern, nachdem Sie Anwendungen basierend auf Tags erstellt haben, finden Sie unter Zuvor erstellte Anwendungsservices neu berechnen für die nächsten Schritte.

Schließen Sie vorkonfigurierte CI-Beziehungen in der Tag-basierten Discovery aus

Schließen Sie vorkonfigurierte CI-Beziehungen aus dem Tag-basierten Discovery-Prozess aus, um die erstellten Anwendungsservices zu verfeinern. Service-Mapping besteht aus vorkonfigurierten CI-Beziehungen und schließt CIs in diese Beziehungen ein, auch wenn ihnen keine Tags zugewiesen sind. Wählen Sie aus, welche vorkonfigurierten CI-Beziehungen ausgeschlossen werden sollen, und wählen Sie, welche der verbleibenden CI-Beziehungen an der Tag-basierten Discovery teilnehmen.

Vorbereitungen

Erfahren Sie mehr über die Konfiguration der Standardfunktion in Tag-basierter Discovery in Service-Mapping.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

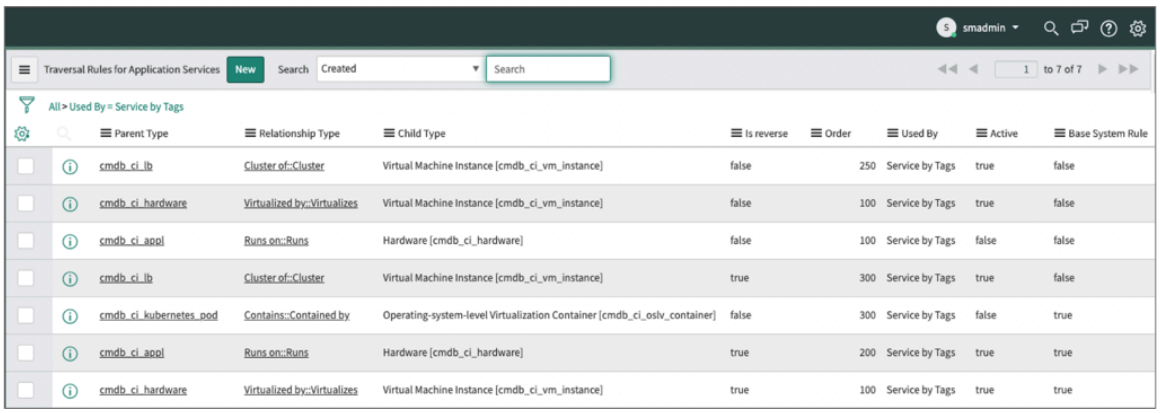
In der Tabelle „Durchlaufregeln für Anwendungsservices“ [svc_traversal_rules] werden die CI-Beziehungen gespeichert, die an der Tag-basierten Discovery teilnehmen. Standardmäßig haben vorkonfigurierte CI-Beziehungen, die in der Tag-basierten Discovery verwendet werden, den Wert **true** in der Spalte **Basissystemregel**. Verwenden Sie diese Informationen, um vorkonfigurierte CI-Beziehungen von der tagbasierten Discovery auszuschließen.

Wichtig: Vorkonfigurierte CI-Beziehungen, die für die Tag-basierte Discovery verwendet werden, können Sie in der Tabelle „Durchlaufregeln für Anwendungsservices“ [svc_traversal_rules] nicht löschen oder ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Service-Durchlaufregeln**.



Parent Type	Relationship Type	Child Type	Is reverse	Order	Used By	Active	Base System Rule
cmdb_ci_lb	Cluster of::Cluster	Virtual Machine Instance [cmdb_ci_vm_instance]	false	250	Service by Tags	true	false
cmdb_ci_hardware	Virtualized by::Virtualizes	Virtual Machine Instance [cmdb_ci_vm_instance]	false	100	Service by Tags	true	false
cmdb_ci_appl	Runs on::Runs	Hardware [cmdb_ci_hardware]	false	100	Service by Tags	false	false
cmdb_ci_lb	Cluster of::Cluster	Virtual Machine Instance [cmdb_ci_vm_instance]	true	300	Service by Tags	true	false
cmdb_ci_kubernetes_pod	Contains::Contained by	Operating-system-level Virtualization Container [cmdb_ci_oslv_container]	false	300	Service by Tags	false	true
cmdb_ci_appl	Runs on::Runs	Hardware [cmdb_ci_hardware]	true	200	Service by Tags	true	true
cmdb_ci_hardware	Virtualized by::Virtualizes	Virtual Machine Instance [cmdb_ci_vm_instance]	true	100	Service by Tags	true	true

2. Klicken Sie auf die vorkonfigurierte CI-Beziehung, die Sie von der Tag-basierten Discovery ausschließen möchten.

   Informationen zum Anzeigen dieser CI-Beziehungen finden Sie unter Vorkonfigurierte CI-Beziehungen in Tag-basierter Discovery

3. Deaktivieren Sie das Kontrollkästchen **Aktiv**.
4. Klicken Sie im Formular **„Durchlaufregeln für Anwendungsservices“auf Absenden**.

Nächste Maßnahme

Wenn Sie die Standardkonfiguration verfeinern, nachdem Sie Anwendungen basierend auf Tags erstellt haben, finden Sie unter Zuvor erstellte Anwendungsservices neu berechnen für die nächsten Schritte.

Fügen Sie CI-Beziehungen in der Tag-basierten Discovery hinzu, oder bearbeiten Sie sie

Aktivieren Sie vorkonfigurierte CI-Beziehungen, die Service-Mapping standardmäßig nicht enthält, oder fügen Sie zusätzliche Beziehungen hinzu, um sie im Tag-basierten Discovery-Prozess zu verwenden. Sie können beispielsweise eine CI-Beziehung zwischen Linux-Servern und Speichergeräten hinzufügen, um Server zu erkennen, die Speichergeräte hosten, basierend auf Tags.

Vorbereitungen

Erfahren Sie mehr über die Konfiguration der Standardfunktion in Tag-basierter Discovery in Service-Mapping.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

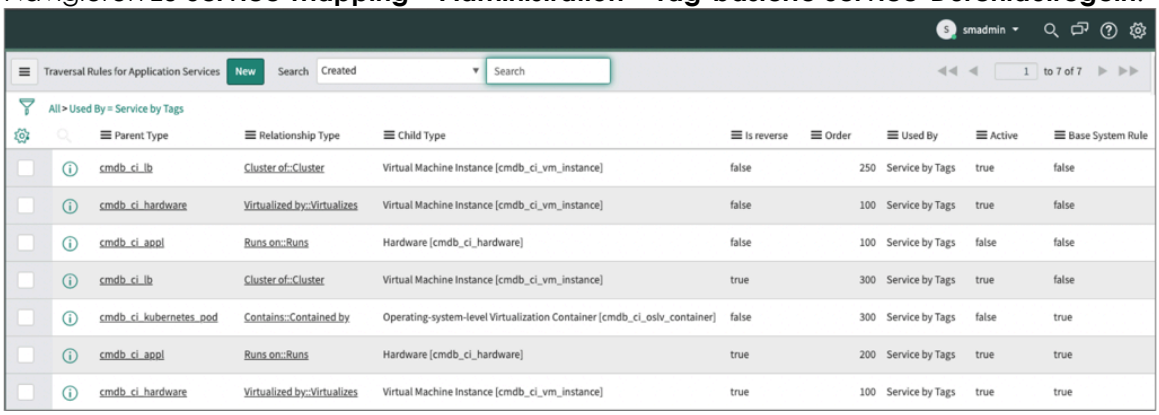
Die Tabelle „Anwendungsservices“ [svc_traversal_rules] wird gefiltert, um nur CI-Beziehungen anzuzeigen, die für die Tag-basierte Erkennung verwendet werden. Standardmäßig haben vorkonfigurierte CI-Beziehungen, die in der Tag-basierten Discovery verwendet werden, den Wert **true** in der Spalte **Basissystemregel**. Verwenden Sie diese Informationen, um neue CI-Beziehungen zu erstellen oder vorkonfigurierte CI-Beziehungen in der Tag-basierten Discovery zu bearbeiten.

Wichtig: Vorkonfigurierte CI-Beziehungen, die für die Tag-basierte Discovery verwendet werden, können Sie in der Tabelle „Durchlaufregeln für Anwendungsservices“ [svc_traversal_rules] nicht löschen oder ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Service-Durchlaufregeln**.



Parent Type	Relationship Type	Child Type	Is reverse	Order	Used By	Active	Base System Rule
cmdb_ci_lb	Cluster of::Cluster	Virtual Machine Instance [cmdb_ci_vm_instance]	false	250	Service by Tags	true	false
cmdb_ci_hardware	Virtualized by::Virtualizes	Virtual Machine Instance [cmdb_ci_vm_instance]	false	100	Service by Tags	true	false
cmdb_ci_appl	Runs on::Runs	Hardware [cmdb_ci_hardware]	false	100	Service by Tags	false	false
cmdb_ci_lb	Cluster of::Cluster	Virtual Machine Instance [cmdb_ci_vm_instance]	true	300	Service by Tags	true	false
cmdb_ci_kubernetes_pod	Contains::Contained by	Operating-system-level Virtualization Container [cmdb_ci_oslv_container]	false	300	Service by Tags	false	true
cmdb_ci_appl	Runs on::Runs	Hardware [cmdb_ci_hardware]	true	200	Service by Tags	true	true
cmdb_ci_hardware	Virtualized by::Virtualizes	Virtual Machine Instance [cmdb_ci_vm_instance]	true	100	Service by Tags	true	true

2. Klicken Sie auf die vorhandene CI-Beziehung, die Sie ändern möchten, oder klicken Sie auf **Neu**, um eine zusätzliche CI-Beziehung im Tag-basierten Discovery-Prozess zu verwenden.

   Informationen zum Anzeigen der standardmäßigen CI-Beziehungen finden Sie unter Vorkonfigurierte CI-Beziehungen in Tag-basierter Discovery.

3. Füllen Sie das Formular **„Durchlaufregeln für Anwendungsservices“** aus.
   Informationen zum Ausfüllen dieses Formulars finden Sie unter Ausfüllen des Formulars „Durchlaufregeln für Anwendungsservices“.
4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Wenn Sie die Standardkonfiguration verfeinern, nachdem Sie Anwendungen basierend auf Tags erstellt haben, finden Sie unter Zuvor erstellte Anwendungsservices neu berechnen für die nächsten Schritte

Berechnen Sie zuvor erstellte Anwendungsservices neu

Berechnen Sie Anwendungsservices neu, nachdem Sie die Standardkonfiguration verfeinert haben, um zu steuern, welche CIs in den Tag-basierten Discovery-Prozess aufgenommen werden sollen.

Vorbereitungen

Führen Sie die Schritte aus, um die Standardkonfiguration für den Tag-basierten Discovery-Prozess zu verfeinern. Weitere Informationen finden Sie unter Konfiguration der Tag-basierten Discovery.

Erforderliche Rolle: service_mapping_admin

Prozedur

1. Navigieren zu **Service-Mapping** > **Services** > **Anwendungsservices**.
2. Klicken Sie auf den entsprechenden Anwendungsservice.
3. Klicken Sie unter **Zugehörige Links** auf **Service neu berechnen**.
4. Wiederholen Sie diese Schritte für alle relevanten Tag-basierten Services.

Nachverfolgung von Changes für die Change-Historie feintunen

Definieren Sie CI-Felder, deren Changes in der Change-Historie für Anwendungsservices berücksichtigt werden. In der Ansicht der Change-Historie werden Changes angezeigt, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

an CIs vorgenommen wurden, aus denen Anwendungsservices bestehen, sowie Changes, die an den eigentlichen Anwendungsservices vorgenommen wurden.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Details zu Änderungen an einer Serviceinstanz und an ihren CIs werden in der CMDB gespeichert. In der Regel handelt es sich bei diesen Änderungen um das Hinzufügen oder Entfernen von CIs zu einer Serviceinstanz, das Aktualisieren oder Aktualisieren von CIs oder das Ändern von CI-Konfigurationsdateien. Das System stellt diese Daten zusammen, indem es CMDB-Tabellen abfragt und dann die Change-Historienansicht erstellt. In Bereitstellungen, für die Service-Mapping aktiviert ist, hängt die Art der Abfragen der Change-Informationen durch Service-Mapping von Discovery-Mustern ab, die von Service-Mapping für die Erkennung von CIs verwendet werden.

Änderungen an Konfigurationsdateien sind CIs zugeordnet, zu denen diese Dateien gehören. Karten zeigen Konfigurationsdateiänderungen als Änderungen an zugehörigen CIs an.

Prozedur
1. Navigieren zu **Alle** > **Konfiguration** > **Service-Baseline – Ausschlussliste**.
   In der daraufhin geöffneten Liste „Ausschlusslisten“ werden Datensätze angezeigt, die vom System dazu verwendet werden, Changes aus der Ansicht der Change-Historie auszuschließen.
2. Um Changes an einem weiteren Feld zu ignorieren, gehen Sie wie folgt vor:
   a. Klicken Sie auf **Neu**.
   b. Geben Sie den CI-Klassennamen in das Feld **Tabellenname** ein.
      Geben Sie beispielsweise `cmdb_ci` für die Klasse „Konfigurationselement“ [cmdb_ci] ein.

      Hinweis: Die Anwenderoberfläche von Service-Mapping bezieht sich auf CI-Klassen als CI-Typen.

   c. Geben Sie in das Feld **Feldname** den Namen des Felds ein, das Sie ausschließen möchten.
      Geben Sie beispielsweise `work_notes` ein, um Changes, die an den Arbeitsnotizen für Elemente vorgenommen werden, aus der Ansicht der Change-Historie auszuschließen.
   d. Wählen Sie **Absenden** aus.
3. Um zuvor ignorierte Changes wieder in die Change-Historie aufzunehmen, gehen Sie wie folgt vor:
   a. Aktivieren Sie die Kontrollkästchen neben den relevanten Datensätzen.
   b. Wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option **Löschen** aus.

Zugehörige Informationen

Change-Historie von Anwendungsservices in veraltet Mitarbeiterbereich anzeigen

Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenerfassung und -erkennung mit Netflow

Service-Mapping kann eine Erkennung basierend auf Daten durchführen, die mit dem Protokoll Netflow erfasst wurden. Netflow ist ein Protokoll das Service-Mapping zum Erfassen von Daten über CIs und ihren Verbindungen mit Netstat- und lsof-Befehlen nutzen kann.

Die Verwendung des Netflow-Protokolls zum Erfassen von Daten ist eine der Methoden der datenverkehrsbasierten Erkennung. Andere von Service-Mapping bereitgestellte Methoden verwenden die Befehle netstat und lsof und die VPC-Flow-Protokolle. Weitere Informationen finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

In Basissystemen verwendet die Traffic-basierte Discovery nur TCP-Daten, die mithilfe der Befehle *`netstat`*, *`ss`* und *`lsof`* erfasst wurden. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung bereichern, indem Sie Service-Mapping für die Verwendung des Protokolls Netflow konfigurieren.

Die Komponente, die Daten im Netflow-Format empfängt, ist der Netflow Collector. Sein Speicherort hängt davon ab, ob Sie die Datenerfassung für Testzwecke oder für den Standardbetrieb konfigurieren:

Zu Testzwecken

Dieses Setup führt zu einem halbautomatisierten Datenerfassungs-Flow, wobei Service-Mapping Daten nur importiert, wenn Sie sie manuell aus dem Netflow Collector kopieren. Sie platzieren den Netflow Collector auf einem Server innerhalb Ihres Unternehmensnetzwerks. Dies muss ein anderer Server sein als der Server, auf dem der MID-Server gehostet wird . Sie konfigurieren und testen dieses Setup wie in Einmaligen Datenimport mit Netflow zu Testzwecken konfigurieren beschrieben.

Für den Standardbetrieb

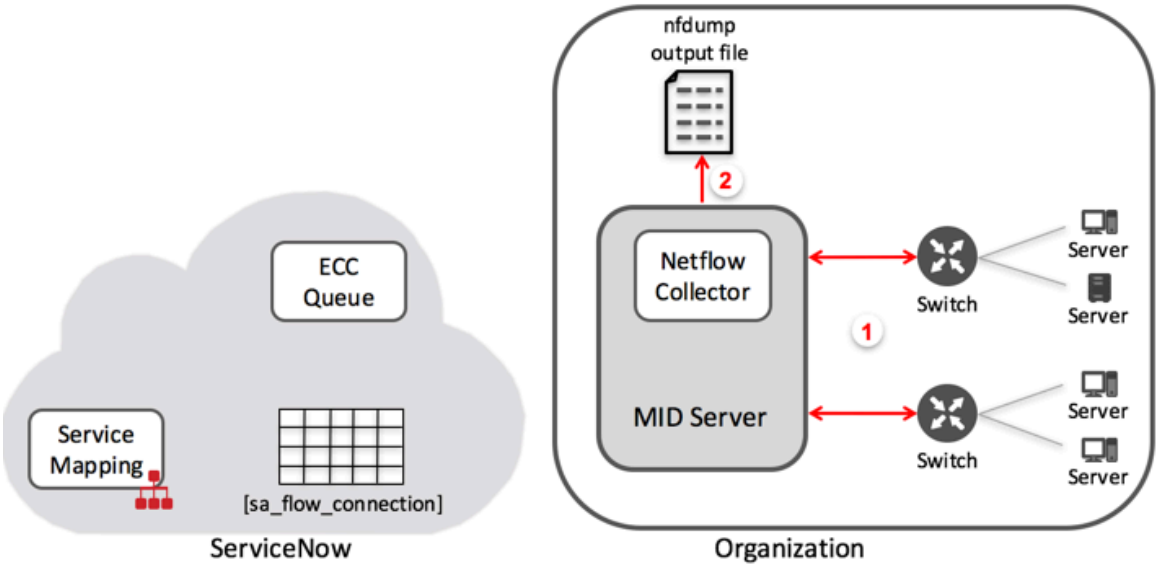
Dieses Setup führt zu einem vollständig automatisierten Datenerfassungs-Flow, bei dem alle beteiligten Komponenten Daten automatisch senden, sammeln und analysieren. Sie platzieren den Netflow Collector auf demselben Server wie den MID-Server innerhalb Ihres Unternehmensnetzwerks. Anweisungen dazu finden Sie unter Datenerfassung mit Netflow konfigurieren.

Die Netflow-basierte Erkennung folgt dem folgenden Flow:

1. Der Netflow-Daemon wird ausgeführt und empfängt Daten von Switches, die mit Servern in der Organisation kommunizieren. Der Netflow Collector schreibt die vom Netflow-Daemon empfangenen Daten.
2. Der Server, der den Netflow Collector hostet, verwendet das Netflow-Dienstprogramm nfdump, um die Daten in die nfdump-Ausgabedatei zu schreiben. Diese Datei fasst die Rohdaten aller für die Serverkommunikation verwendeten Switches zusammen.

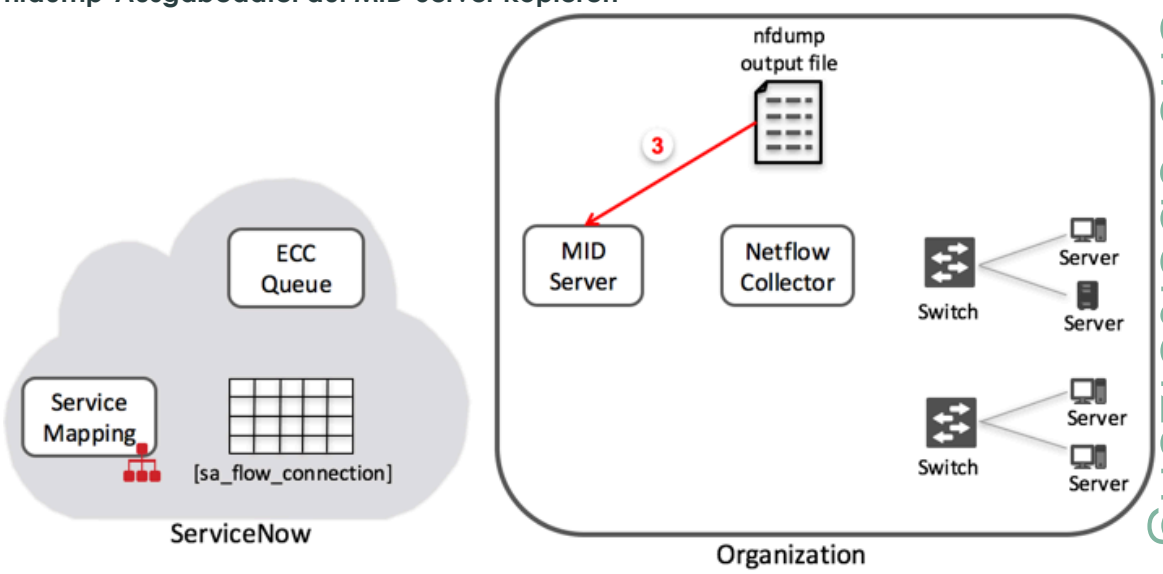
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Daten erfassen und in die nfdump-Ausgabedatei schreiben



3. In Test-Setups, in denen sich der Netflow Collector nicht auf demselben Server wie der MID-Server befindet, müssen Sie nfdump möglicherweise in das gzip-Format konvertieren. Anschließend müssen Sie die Rohdaten aus der nfdump-Ausgabedatei manuell auf den MID-Server kopieren.

nfdump-Ausgabedatei auf MID-Server kopieren

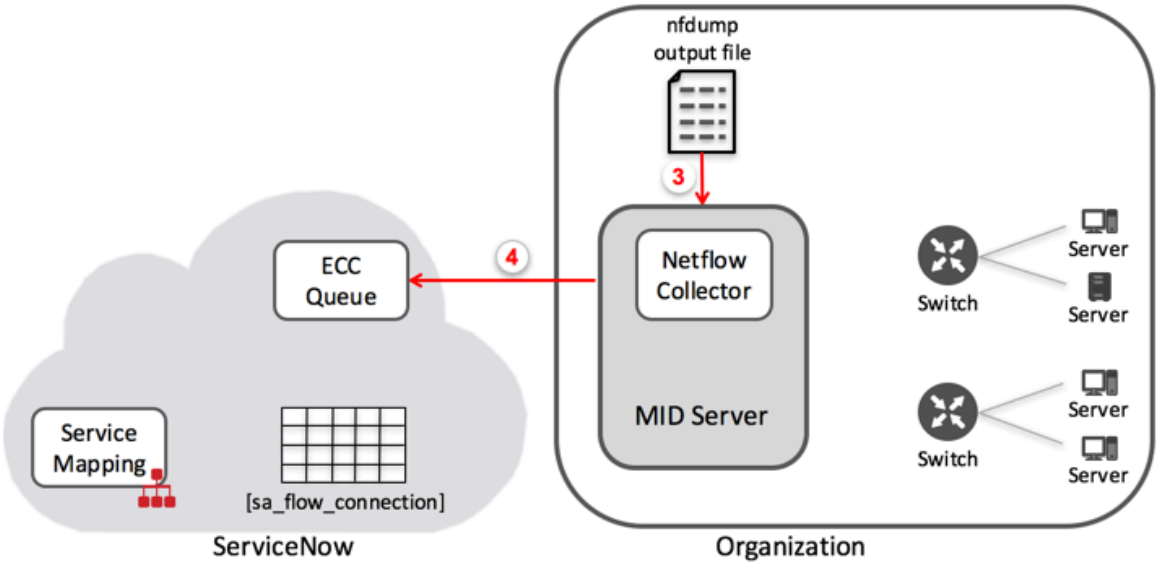


4. Der MID-Server verarbeitet die Rohdaten in der nfdump-Ausgabedatei und platziert die verarbeiteten Informationen in der ECC-Warteschlange.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

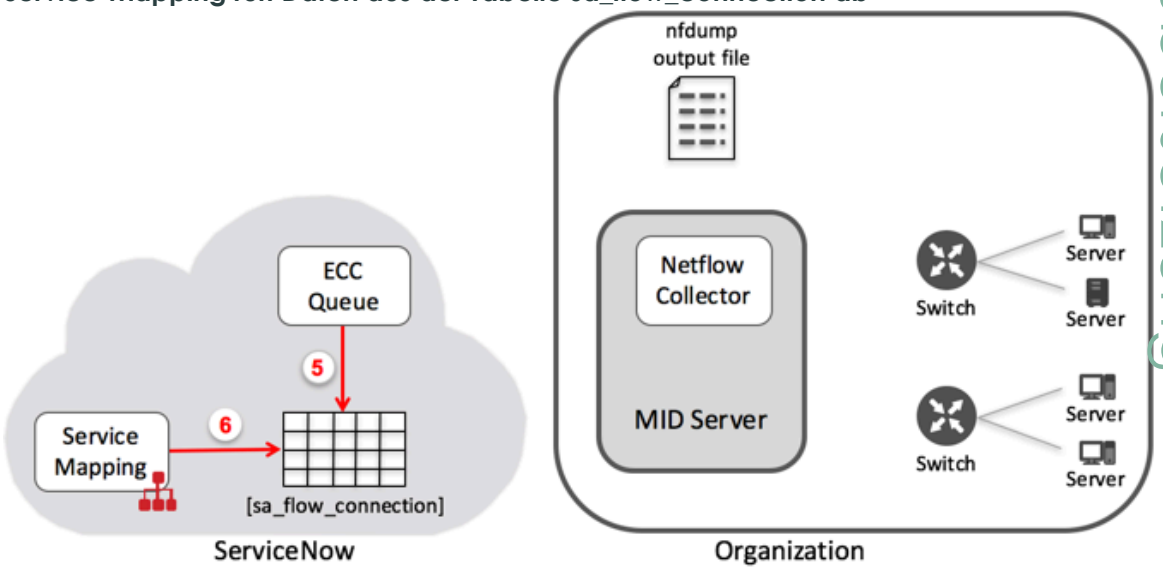
Rohdaten analysieren und in ECC-Warteschlange platzieren



5. Ein Sensor ruft die Prozessdaten aus der ECC-Warteschlange ab und schreibt sie in die Flow-Verbindungstabelle [sa_flow_connection].

6. Wann auch immer Service-Mapping die ECC-Warteschlange prüft und Informationen zu einem ermittelten CI empfängt, prüft es diese Tabellen auf alle Daten zu ausgehenden Verbindungen, die sich auf das CI beziehen: die Tabellen cmdb_tcp und sa_flow_connection. Wenn diese beiden Tabellen eindeutige Daten enthalten, die von den Mustern nicht erkannt wurden, werden von Service-Mapping die Informationen zu den CI-Verbindungen erweitert, und die Informationen werden der Zuordnung hinzugefügt.

Service-Mapping ruft Daten aus der Tabelle sa_flow_connection ab



Zugehörige Informationen

https://support.servicenow.com/kb_view.do?sysparm_article=KB0597467

Einmaligen Datenimport mit Netflow zu Testzwecken konfigurieren

Konfigurieren und testen Sie den Erkennungsprozess in Service-Mapping basierend auf Daten, die mit dem Protokoll Netflow erfasst wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Informieren Sie sich über die Datenverkehrsbasierte Erkennung in Service-Mapping.

Erforderliche Rolle: admin oder service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

In Basissystemen verwendet die Traffic-basierte Discovery nur TCP-Daten, die mithilfe der Befehle *netstat*, *ss* und *lsof* erfasst wurden. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung bereichern, indem Sie Service-Mapping für die Verwendung des Protokolls Netflow konfigurieren. Weitere Informationen darüber, wie Sie in Service-Mapping Netflow-Daten erfassen, finden Sie unter Datenerfassung und -erkennung mit Netflow.

Installieren Sie den Netflow Collector (nfdump) zu Testzwecken auf einem Unix-Server in Ihrer Organisation. In diesem Fall darf es sich nicht um denselben Server handeln, auf dem der MID-Server gehostet wird.

Konfigurieren Sie den ServiceNow-Connector so, dass er MID-Server veranlasst, Daten aus dem Flow-Protokoll zu erfassen und zu verarbeiten.

Prozedur

1. Laden Sie den Netflow Collector (nfdump) auf einen Unix-Server in Ihrer Organisation herunter, und installieren Sie ihn.
   - Laden Sie das nfdump-Paket für einen Linux-Server herunter, kompilieren Sie es und installieren Sie es. Sie können das nfdump-Paket von https://sourceforge.net/projects/nfdump/ herunterladen.
   - Installieren Sie für einen Ubuntu-Server das nfdump-Paket, ohne es vorher herunterzuladen oder zu kompilieren. Öffnen Sie das Befehlszeilenfenster und führen Sie den folgenden Befehl aus:

     ```
     sudo apt-get install nfdump
     ```

   - Wenn bei einem Ubuntu-Server der *apt-get*-Befehl fehlschlägt, laden Sie das nfdump-Paket herunter, speichern Sie es lokal, und installieren Sie es. Öffnen Sie das Befehlszeilenfenster und führen Sie die folgenden Befehle aus:

     ```
     sudo dpkg -i nfdump_1.6.15-3_i386.deb -

     sudo apt-get -f install
     ```

     Hinweis: Der Dateiname für das Paket nfdump hat das folgende Format: nfdump_<version number> .deb. In diesem Beispiel ist dies nfdump_1.6.15-3_i386.deb.

2. Konfigurieren Sie den Netflow-Collector, um Daten für einen Tag zu speichern.

   a. Öffnen Sie das Befehlszeilenfenster auf dem Server, auf dem sich der Netflow-Collector befindet.

   b. Erstellen Sie einen Cron-Job.
   `crontab -e`

   c. Geben Sie den folgenden Befehl mit den richtigen Pfaden ein.
   `*/10 * * * * /usr/local/bin/nfexpire -e /data/nfdump -t 1d`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Erstellen Sie eine Datei mit den nfdump-Daten.
   Verwenden Sie beispielsweise den folgenden Befehl:

   nfdump -q -m -R /data/nfdump/ -o extended -t 2016/07/06.07:00:00-2016/07/06.07:10:00 'inet and proto tcp' >> /tmp/my_file

4. Wenn die Datei sehr groß ist, können Sie sie mit dem folgenden Befehl im gzip-Format komprimieren:
   `gzip /tmp/my_file`
5. Kopieren Sie die nfdump-Datendatei auf den MID-Server.
6. Konfigurieren Sie Service-Mapping zum Empfangen von vom Netflow Collector erfassten Daten:

   a. Navigieren zu **Service-Mapping** > **Administration** > **Flow-Connectors**.

   b. Klicken Sie auf **Neu**.

   c. Klicken Sie auf die **ndfdump-Datei**.

   d. Konfigurieren Sie die Parameter auf der Seite für die ndfdump-Datei wie folgt:

Feld	Beschreibung
Name	Beschreibender Name für den Connector
nfdump-Datenpfad	Pfad zu einem Speicherort auf dem MID-Server, in dem Sie die nfdump-Datendatei in 5 gespeichert haben
MID Server	MID-Server, auf den Sie die nfdump-Datei kopiert haben
Gzip-Datei	Wenn Sie die nfdump-Datei in das gzip-Format konvertiert haben, bevor Sie sie auf dem MID-Server gespeichert haben, setzen Sie diesen Parameter auf „true“, um die Datei zu dekomprimieren.

   e. Klicken Sie auf **Absenden**.

7. Stellen Sie sicher, dass Service-Mapping Daten mit Netflow erfasst:
   a. Wählen Sie im Formular für die **nfdump-Datei** den neu konfigurierten Connector aus, und klicken Sie auf **Jetzt ausführen**, um den Datenerfassungs-Flow zu starten und die Tabelle „Flow-Verbindung“ [sa_flow_connection] zu füllen.
   b. Navigieren zu **Systemdefinitionen** > **Tabellen**.
   c. Klicken Sie auf die Tabelle „Flow-Verbindung“ [sa_flow_connection]
   d. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.
   e. Stellen Sie sicher, dass die Tabelle Daten enthält.

Nächste Maßnahme

Wenn Sie mit den Testergebnissen zufrieden sind, konfigurieren Sie die Netflow-basierte Datenerfassung (siehe Beschreibung in Datenerfassung mit Netflow konfigurieren).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenerfassung mit Netflow konfigurieren

Richten Sie in Service-Mapping die Erkennung basierend auf Daten ein, die mit dem Protokoll Netflow erfasst wurden. Dieses Setup führt zu einem vollständig automatisierten Datenerfassungs-Flow, bei dem alle beteiligten Komponenten Daten automatisch senden, sammeln und analysieren.

Vorbereitungen

Informieren Sie sich über die Datenverkehrsbasierte Erkennung in Service-Mapping.

Aktivieren Sie den folgenden regelmäßigen Auftrag: Flow Discovery-Planer [sysauto_script_74c676f0dbb0220060ff742eaf9619f2]+

Erforderliche Rolle: admin oder service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

In Basissystemen verwendet die Traffic-basierte Discovery nur TCP-Daten, die mithilfe der Befehle *netstat*, *ss* und *lsof* erfasst wurden. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung bereichern, indem Sie Service-Mapping für die Verwendung des Protokolls Netflow konfigurieren. Weitere Informationen über die Nutzung von Netflow durch Service-Mapping finden Sie unter Datenerfassung und -erkennung mit Netflow.

Konfigurieren Sie den ServiceNow Netflow-Connector so, dass er den MID-Server veranlasst, Daten aus dem Flow-Protokoll zu erfassen und zu verarbeiten.

Prozedur

1. Installieren Sie das nfdump-Paket auf einem Server, der in Ihrer Organisation den MID-Server hostet:
   - Laden Sie das nfdump-Paket für einen Linux-Server herunter, kompilieren Sie es und installieren Sie es. Sie können das nfdump-Paket von https://sourceforge.net/projects/nfdump/ herunterladen.
   - Installieren Sie für einen Ubuntu-Server das nfdump-Paket, ohne es vorher herunterzuladen oder zu kompilieren. Öffnen Sie das Befehlszeilenfenster und führen Sie den folgenden Befehl aus:

     ```
     sudo apt-get install nfdump
     ```

   - Wenn bei einem Ubuntu-Server der *apt-get*-Befehl fehlschlägt, laden Sie das nfdump-Paket herunter, speichern Sie es lokal, und installieren Sie es. Öffnen Sie das Befehlszeilenfenster und führen Sie die folgenden Befehle aus:

     ```
     sudo dpkg -i nfdump_1.6.15-3_i386.deb -

     sudo apt-get -f install
     ```

     Hinweis: Der Dateiname für das Paket nfdump hat das folgende Format: nfdump_<version number> .deb. In diesem Beispiel ist dies nfdump_1.6.15-3_i386.deb.

2. Konfigurieren Sie den Netflow-Collector so, dass die nfdump-Datei im erforderlichen Verzeichnis gespeichert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Öffnen Sie die Datei `/etc/init.d/nfdump`.

b. Ändern Sie den Parameter, der für das Speichern dieser Datei am erforderlichen Speicherort verantwortlich ist.
Geben Sie beispielsweise auf einem Ubuntu-Server den Speicherort mit dem Parameter *DEAMON_ARGS* an:

```
DATA_BASE_DIR="/var/cache/nfdump"

DAEMON_ARGS="-D -l $DATA_BASE_DIR -P $PIDFILE"
```

Betriebsinformationen finden Sie unter https://sourceforge.net/projects/nfdump/ .

3. Konfigurieren Sie die Switches so, dass ihre nfdump-Dateien an MID-Server weitergeleitet werden.
Der Standardwert für MID-Server ist Port 9995.
4. Konfigurieren Sie den Netflow-Collector, um Daten für einen Tag zu speichern.

a. Öffnen Sie das Befehlszeilenfenster auf dem Server, auf dem sich der Netflow-Collector befindet.

b. Erstellen Sie einen Cron-Job.
`crontab -e`

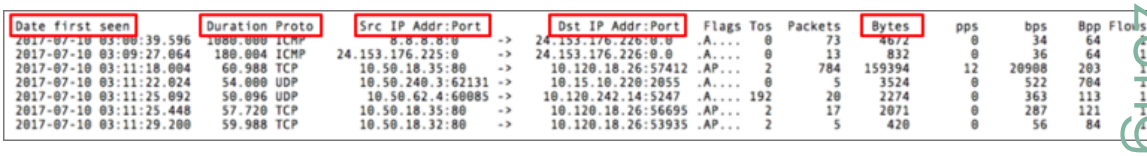
c. Geben Sie den folgenden Befehl mit den richtigen Pfaden ein.
`*/10 * * * * /usr/local/bin/nfexpire -e /data/nfdump -t 1d`

5. Stellen Sie sicher, dass der Netflow Collector ordnungsgemäß konfiguriert ist und von den Netzwerkressourcen die richtigen Daten erhält.

a. Führen Sie den folgenden Befehl aus:

```
nfdump -q -O tstart -R /data/nfdump/ -o extended
```

b. Überprüfen Sie in der Befehlsausgabe, ob die markierten Felder reale Daten enthalten:



Date first seen	Duration	Proto	Src IP Addr:Port		Dst IP Addr:Port	Flags	Tos	Packets	Bytes	pps	bps	Bpp	Flows
2017-07-10 03:08:39.596	1080.000	ICMP	8.8.8.8:0	->	24.153.176.226:0.0	.A....	0	73	4672	0	34	64	
2017-07-10 03:09:27.064	180.004	ICMP	24.153.176.225:0	->	24.153.176.226:0.0	.A....	0	13	832	0	36	64	
2017-07-10 03:11:18.004	60.988	TCP	10.50.18.35:80	->	10.120.18.26:57412	.AP...	2	784	159394	12	20908	203	
2017-07-10 03:11:22.024	54.000	UDP	10.50.240.3:62131	->	10.15.10.220:2055	.A....	0	5	3524	0	522	704	
2017-07-10 03:11:25.092	50.096	UDP	10.50.62.4:60085	->	10.120.242.14:5247	.A....	192	20	2274	0	363	113	
2017-07-10 03:11:25.448	57.720	TCP	10.50.18.35:80	->	10.120.18.26:56695	.AP...	2	17	2071	0	287	121	
2017-07-10 03:11:29.200	59.988	TCP	10.50.18.32:80	->	10.120.18.26:53935	.AP...	2	5	420	0	56	84	

6. Konfigurieren Sie Service-Mapping zum Empfangen von vom Netflow Collector erfassten Daten:

a. Navigieren zu **Service-Mapping** > **Administration** > **Flow-Connectors**.

b. Klicken Sie auf **Neu**.

c. Klicken Sie auf **nfdump-Installation**

d. Konfigurieren Sie die Parameter auf der Seite „ndfdump-Installation“ wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Beschreibender Name für den Connector
MID Server	MID-Server, auf dem der Netflow Collector installiert ist
nfdump-Datenverzeichnis	Datenverzeichnis, in dem in Ihrer Konfiguration der Netflow Collector die nfdump-Datei speichern soll

e. Klicken Sie auf **Absenden**.

7. Stellen Sie sicher, dass Service-Mapping Daten mit Netflow erfasst:

a. Wählen Sie im Formular **nfdump-Installation** den neu konfigurierten Connector aus, und klicken Sie auf **Jetzt ausführen**, um den Datenerfassungs-Flow zu starten und die Tabelle „Flow-Verbindung“ [sa_flow_connection] zu füllen.

b. Navigieren zu **Systemdefinitionen** > **Tabellen**.

c. Klicken Sie auf die Tabelle „Flow-Verbindung“ [sa_flow_connection]

d. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.

e. Stellen Sie sicher, dass die Tabelle Daten enthält.

Datenerfassung und -erkennung mit VPC-Flow-Protokollen

Service-Mapping kann eine Erkennung basierend auf Daten durchführen, die mit VPC-Flow-Protokollen erfasst wurden. Amazon VPC hostet Amazon EC2-Instanzen (Elastic Compute Cloud), die Amazon Web Services bereitstellen. VPC-Flow-Protokolle erfassen Daten über den IP-Datenverkehr, der von und zu Netzwerkschnittstellen in der VPC geleitet wird.

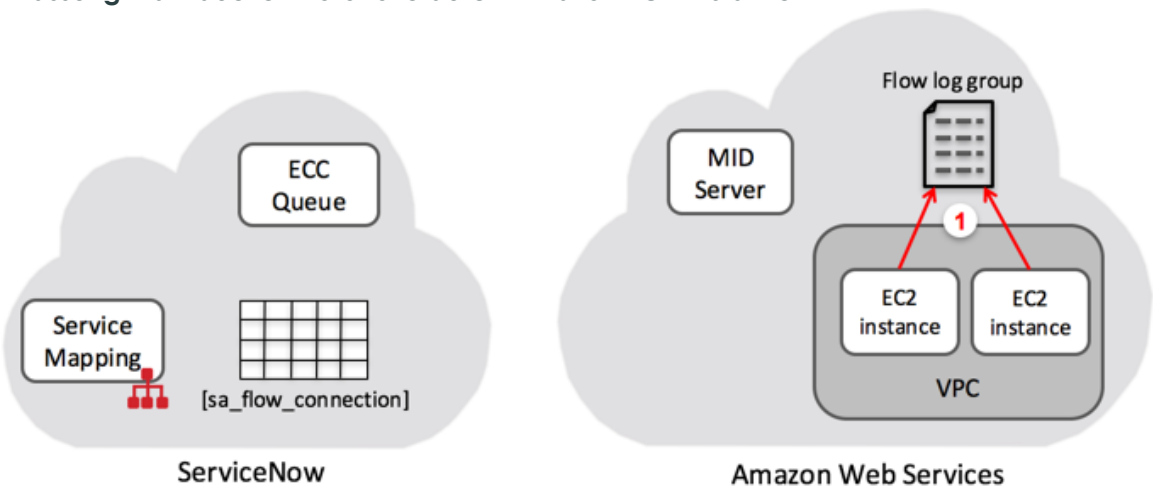
In Basissystemen verwendet die Traffic-basierte Discovery nur TCP-Daten, die mithilfe der Befehle *`netstat`*, *`ss`* und *`lsof`* erfasst wurden. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung bereichern, indem Sie Service-Mapping für die Verwendung von VPC-Flow-Protokollen konfigurieren.

Die Service-Mapping-Erkennung auf Basis von VPC-Flow-Protokollen folgt dem folgenden Flow:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

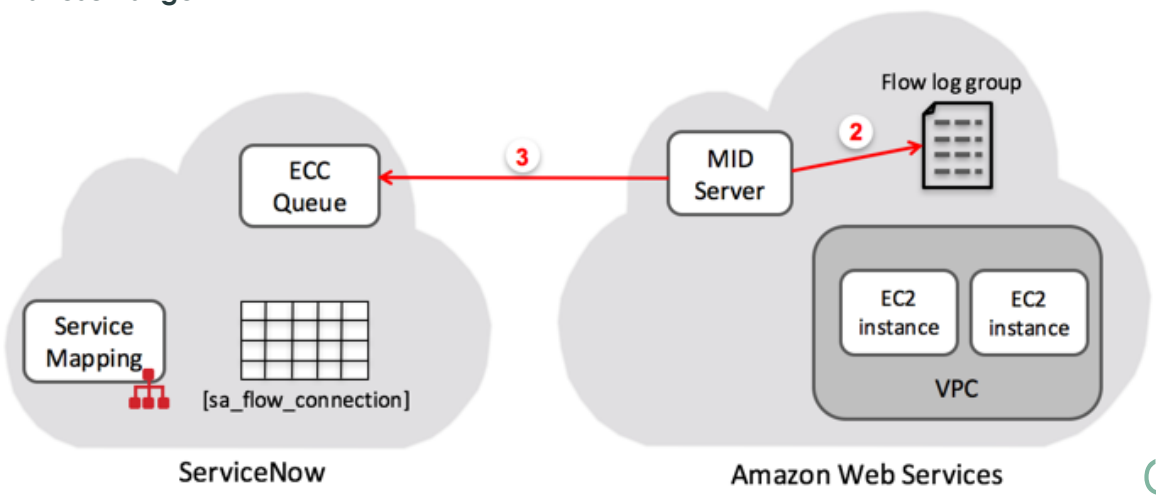
1. Amazon EC2-Instanzen erfassen ihre einzelnen Protokolle in Protokoll-Streams und leiten sie an die zentrale Flow-Protokollgruppe weiter.

Erfassung individueller Protokolle durch Amazon EC2-Instanzen



2. Der ServiceNow-Connector veranlasst den MID-Server, veranlasst, Daten aus dem Flow-Protokoll zu erfassen und zu verarbeiten.
3. Der MID-Server stellt die verarbeiteten Informationen in die ECC-Warteschlange.

MID-Server erfasst Daten aus dem Flow-Protokoll und platziert sie in die ECC-Warteschlange



4. Ein Sensor ruft die Prozessdaten aus der ECC-Warteschlange ab und schreibt sie in die Flow-Verbindungstabelle [sa_flow_connection].

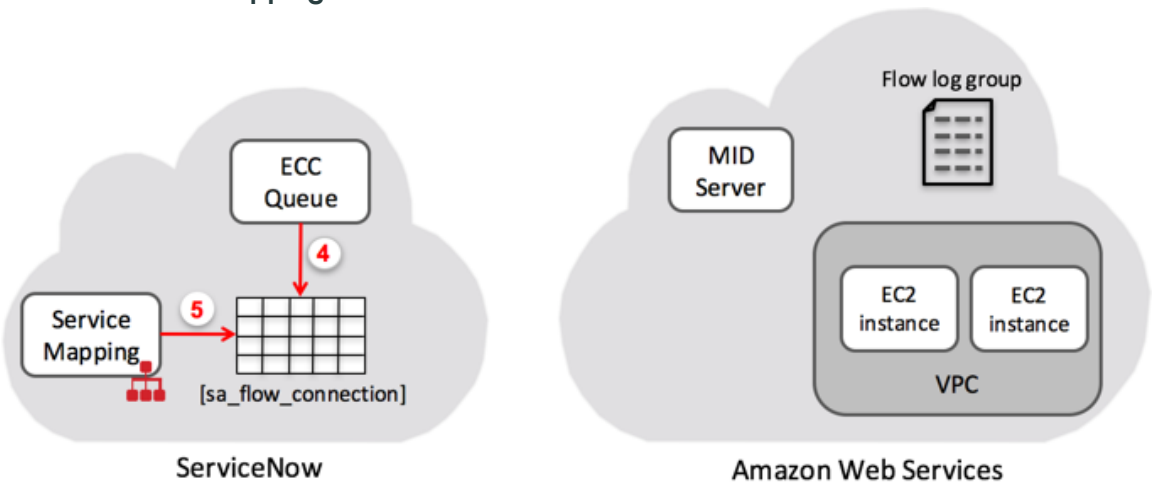
5. Wann auch immer Service-Mapping die ECC-Warteschlange prüft und Informationen zu einem ermittelten CI empfängt, prüft es diese Tabellen auf alle Daten zu ausgehenden Verbindungen, die sich auf das CI beziehen: die Tabellen cmdb_tcp und sa_flow_connection. Wenn diese beiden Tabellen eindeutige Daten enthalten, die von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

den Mustern nicht erkannt wurden, werden von Service-Mapping die Informationen zu den CI-Verbindungen erweitert, und die Informationen werden der Zuordnung hinzugefügt.

Gesammelte Daten werden in die Tabelle sa_flow_connection geschrieben, aus der Service-Mapping die Daten erfasst



Konfigurieren Sie in Bereitstellungen mit mehreren Flow-Protokollgruppen einen dedizierten Connector, der mit einem MID-Server pro Flow-Protokollgruppe arbeitet. Mehrere Flow-Protokollgruppen können dieselben AWS-Anmeldeinformationen verwenden.

Zugehörige Informationen

https://support.servicenow.com/kb_view.do?sysparm_article=KB0597467

Datenverkehrsbasierte Erkennung in Service-Mapping

Datenerfassung mit VPC-Flow-Protokollen konfigurieren

Aktivieren Sie Service-Mapping, um eine Erkennung basierend auf Daten durchzuführen, die mithilfe von VPC-Protokollen (Virtual Private Cloud) erfasst wurden. Diese Methode ist für Organisationen relevant, die Amazon Web Services (AWS) verwenden.

Vorbereitungen

Vergewissern Sie sich, dass die Anmeldeinformationen für das AWS-Konto im Modul Anmeldeinformationen der -Plattform konfiguriert sind, indem Sie zu navigieren **Service-Mapping** > **Anmeldeinformationen** > **AWS-Anmeldeinformationen**. Weitere Informationen zu AWS-Anmeldeinformationen finden Sie unter Cloud-Anmeldeinformationen .

Erforderliche Rolle: admin oder service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

In Basissystemen verwendet die Traffic-basierte Discovery nur TCP-Daten, die mithilfe der Befehle *netstat*, *ss* und *lsof* erfasst wurden. Die auf Netflow- und VPC-Protokollen basierende Discovery erfordert eine zusätzliche Konfiguration. Sie können Ihre datenverkehrsbasierte Erkennung bereichern, indem Sie Service-Mapping für die Verwendung von VPC-Flow-Protokollen konfigurieren. Weitere Informationen zum Erkennungs-Flow in Service-Mapping auf Basis von VPC-Flow-Protokollen finden Sie unter Datenerfassung und -erkennung mit VPC-Flow-Protokollen.

Amazon VPC hostet Amazon EC2-Instanzen (Elastic Compute Cloud), die Amazon Web Services bereitstellen. VPC-Flow-Protokolle erfassen Daten über den IP-Datenverkehr, der von und zu Netzwerkschnittstellen in der VPC geleitet wird.

Konfigurieren Sie den ServiceNow-Connector so, dass er MID-Server veranlasst, Daten aus dem Flow-Protokoll zu erfassen und zu verarbeiten. Konfigurieren Sie in Bereitstellungen mit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mehreren Flow-Protokollgruppen einen dedizierten Connector, der mit einem MID-Server pro Flow-Protokollgruppe arbeitet. Mehrere Flow-Protokollgruppen können dieselben AWS-Anmeldeinformationen verwenden.

Prozedur

1. Konfigurieren Sie VPC-Flow-Protokolle in der Amazon EC2-Konsole gemäß der Beschreibung in der offiziellen AWS-Dokumentation.
2. Konfigurieren Sie Service-Mapping für die Verwendung mit VPC-Flow-Protokollen:
   a. Navigieren zu **Service-Mapping** > **Administration** > **Flow-Connectors**.
   b. Klicken Sie auf **Neu**.
   c. Klicken Sie auf **AWS VPC-Flow-Protokolle**.
   d. Konfigurieren Sie auf der Seite „AWS VPC-Flow-Protokolle“ die Connector-Parameter wie folgt:

Feld	Beschreibung
Name	Beschreibender Name für den Connector
Gruppenname	Name der zentralen Flow-Protokollgruppe, an die Amazon EC2-Instanzen ihre Protokoll-Streams weiterleiten
MID Server	MID-Server, den Service-Mapping zum Erfassen der Daten aus der Flow-Protokollgruppe in AWS verwendet
AWS-Anmeldeinformationen	Wählen Sie die AWS-Anmeldeinformationen für das Konto aus, für das Sie Flow-Protokolle erfassen möchten.

   e. Klicken Sie auf **Absenden**.
3. Vergewissern Sie sich, dass Service-Mapping Daten mit VPC-Flow-Protokollen erfasst:
   a. Wählen Sie im Formular **AWS VPC-Flow-Protokolle** den neu konfigurierten Connector aus, und klicken Sie auf **Jetzt ausführen**, um den Datenerfassungs-Flow zu starten und die Tabelle „Flow-Verbindung“ [sa_flow_connection] zu füllen.
   b. Navigieren zu **Systemdefinitionen** > **Tabellen**.
   c. Klicken Sie auf die Tabelle „Flow-Verbindung“ [sa_flow_connection]
   d. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.
   e. Stellen Sie sicher, dass die Tabelle Daten enthält.

Suchassistenten für Windows konfigurieren

Mit dem Suchassistenten im Musterdesigner können Sie in Dateien oder Registrierungen suchen. Laden Sie grep-Dateien in Ihre Instanz hoch, um diese Funktion für die Suche auf Windows-Servern zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: admin oder service_mapping_admin

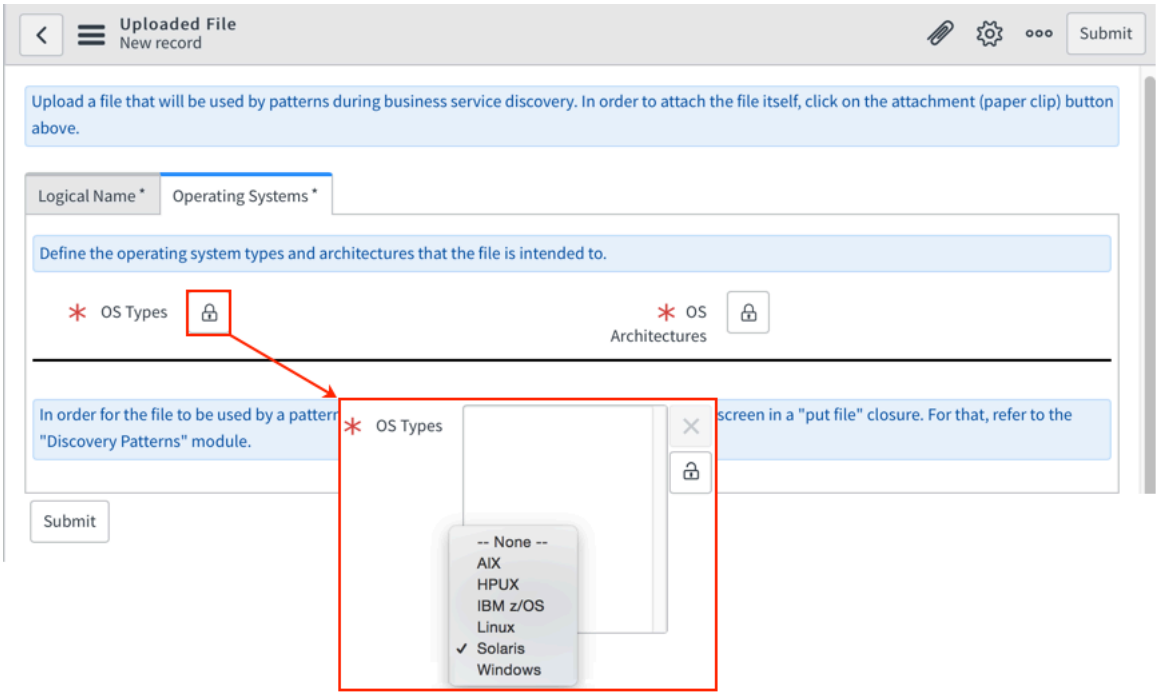
Warum und wann dieser Vorgang ausgeführt wird
grep ist ein Dienstprogramm, mit dem der Suchassistent Dateien nach Übereinstimmungen durchsucht. grep ist für Unix-basierte Systeme nativ, daher müssen Sie es nur für Windows-basierte Konfigurationselemente (CI) hochladen. Sobald Sie grep-Dateien in die Instanz hochladen, werden sie auf alle MID-Server übertragen, die anschließend die Dateien an alle Windows-basierten CIs in Ihrer Organisation verteilen.

Prozedur
1. Laden Sie die folgenden Dateien aus dem Internet auf den Computer herunter.
   - egrep.exe
   - libiconv2.dll
   - libintl3.dll
   - pcre3.dll
   - regex2.dll

   Beispielsweise können Sie die ZIP-Dateien für die Ordner **Dependencies** und **Binaries** vom folgenden Speicherort herunterladen: http://gnuwin32.sourceforge.net/packages/grep.htm
2. Extrahieren Sie die Dateien.

   Nach dem Extrahieren der heruntergeladenen Ordner befinden sich die Dateien an folgenden Speicherorten:
   - grep-2.5.4-bin/bin/egrep.exe
   - grep-2.5.4-dep/bin/libiconv2.dll
   - grep-2.5.4-dep/bin/libintl3.dll
   - grep-2.5.4-dep/bin/pcre3.dll
   - grep-2.5.4-dep/bin/regex2.dll
3. Navigieren zu **Musterdesigner** > **Hochgeladene Dateien**.
4. Klicken Sie auf **Neu**.
5. Geben Sie den ursprünglichen Dateinamen in das Feld **Name** auf der Registerkarte **Logischer Name** ein, z. B. `egrep.exe`.
6. Klicken Sie auf **BS-Typen** und wählen Sie **Windows** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **BS-Architekturen**, und wählen Sie sowohl die 32-Bit- als auch die 64-Bit-Option aus.
8. Klicken Sie auf das Symbol **Anhänge verwalten**.
9. Klicken Sie auf **Dateien wählen**.
10. Navigieren Sie im Ordner **Downloads** auf Ihrem Computer zu der Datei, deren Namen Sie zuvor eingegeben haben, z. B. `egrep.exe`.
11. Klicken Sie auf **Auswählen**.
12. Schließen Sie das Fenster „Anhänge“.
13. Wiederholen Sie Schritt 3 bis Schritt 11, um die restlichen Dateien hochzuladen:
    - libiconv2.dll
    - libintl3.dll
    - pcre3.dll
    - regex2.dll
14. Stellen Sie eine Verbindung zu jedem Windows-MID-Server her, und aktualisieren Sie die Umgebungsvariable PATH mit dem Speicherort des `bin`-Verzeichnisses, in dem `egrep.exe` installiert ist.

Anzeige für CI-Attribute ändern

Sie können steuern, welche Attribute der Configuration Items (CI) das System im Eigenschaftenbereich der für Service-Karten anzeigt.

Vorbereitungen

Machen Sie sich mit dem Konzept der Ansichten vertraut. Weitere Informationen zu Ansichten finden Sie unter Verwaltung von Ansichten .

Entscheiden Sie, für welche CI-Klassen Sie die Anzeige ändern möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entscheiden Sie, ob Sie die Anzeige für übergeordnete CI-Klassen ändern möchten, damit die Ansichtsänderungen in allen untergeordneten CI-Klassen wirksam werden. Führen Sie die folgenden Schritte aus, um die übergeordnete CI-Klasse einer CI-Klasse zu überprüfen:

Hinweis: Die Anwenderoberfläche von Service-Mapping bezieht sich auf CI-Klassen als CI-Typen.

1. Navigieren zu **Systemdefinition** > **Tabellen**.
2. Legen Sie das Suchfeld auf **Name** fest, und geben Sie die relevante CI-Klasse ein.

   Eine Liste mit allen CI-Klassen, die dem Namen entsprechen, wird angezeigt.
3. Überprüfen Sie die Spalte **Erweitert Tabelle**, um die übergeordnete CI-Klasse anzuzeigen.

Erforderliche Rolle: service_mapping_admin oder app_service_admin

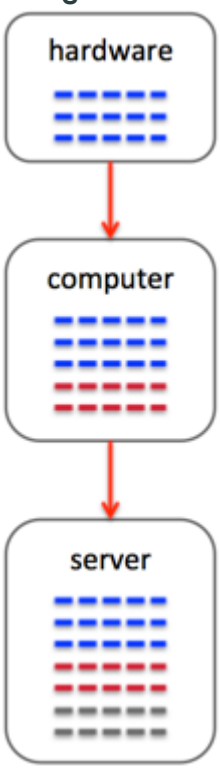
Warum und wann dieser Vorgang ausgeführt wird

Bei der Arbeit mit für Service-Karten werden im Eigenschaftenbereich Attribute für CIs und Verbindungen angezeigt, die Sie in einer Karte auswählen. Da eine große Anzahl von anzuzeigenden Attributen vorhanden ist, sollten Sie auswählen, welche Attribute in welcher Reihenfolge angezeigt werden.

Die Attribute und ihre Anzeigereihenfolge werden durch eine Kombination aus der CI-Typdefinition und der Ansicht für diesen CI-Typ bestimmt.

CMDB speichert die CI-Klasse in Form einer Hierarchie, in der einige CI-Klassen übergeordnete Elemente anderer CI-Klassen sind. Diese untergeordneten CI-Klassen leiten (zusätzlich zu den Attributen, die Sie speziell für sie konfigurieren) automatisch die Attribute der ihnen übergeordneten Klassen ab. Die CI-Klassenhierarchie wird häufig zum Konfigurieren des CI-Verhaltens, der Beziehungen und der Anzeige verwendet.

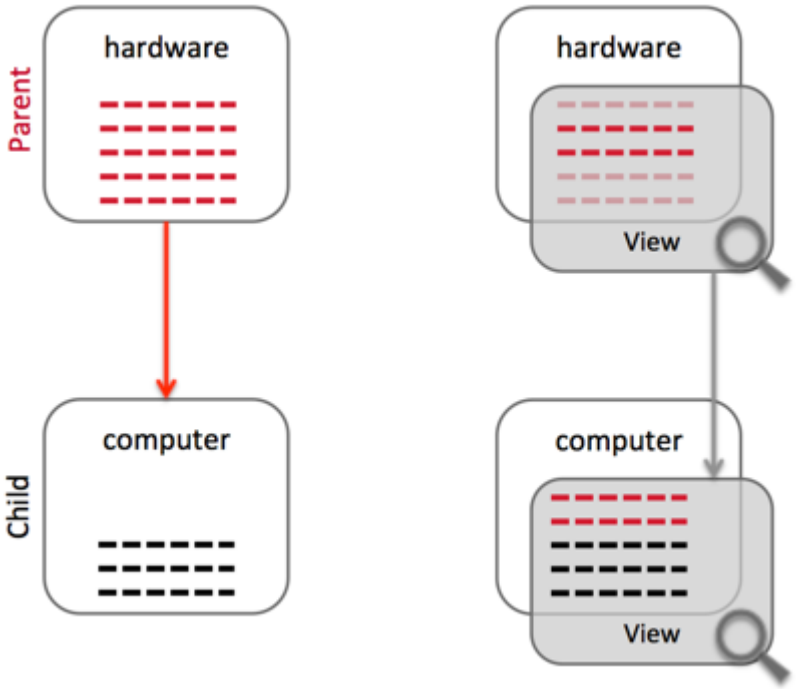
Untergeordnete CI-Klassen leiten Attribute von ihren übergeordneten Klassen ab



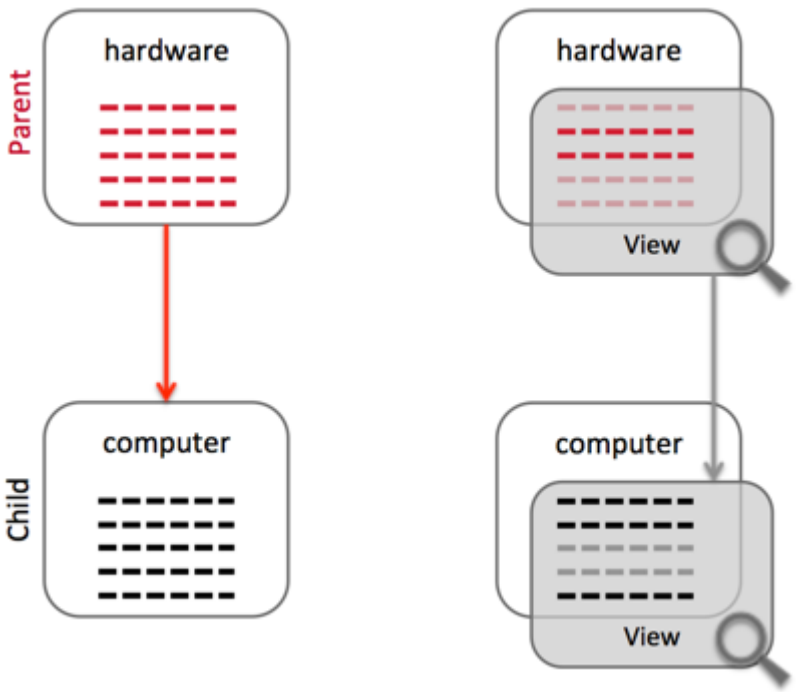
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Ansicht, die die Attributanzeige in für Service-Karten steuert, wird *sa_map_properties* genannt. Sie können diese Ansicht neuen CI-Klassen zuweisen oder die Ansicht für CI-Klassen ändern, die sie bereits verwenden. Verwenden Sie die CI-Typhierarchie zum Konfigurieren der *sa_map_properties view*.

- Die übergeordnete CI-Klasse ganz oben in der Hierarchie lautet *cmdb*.
- Wenn Sie die Ansicht für eine untergeordnete CI-Klasse nicht definieren, zeigt das System vom übergeordneten Element abgeleitete Attribute und zusätzlich alle Attribute dieser untergeordneten CI-Klasse an.

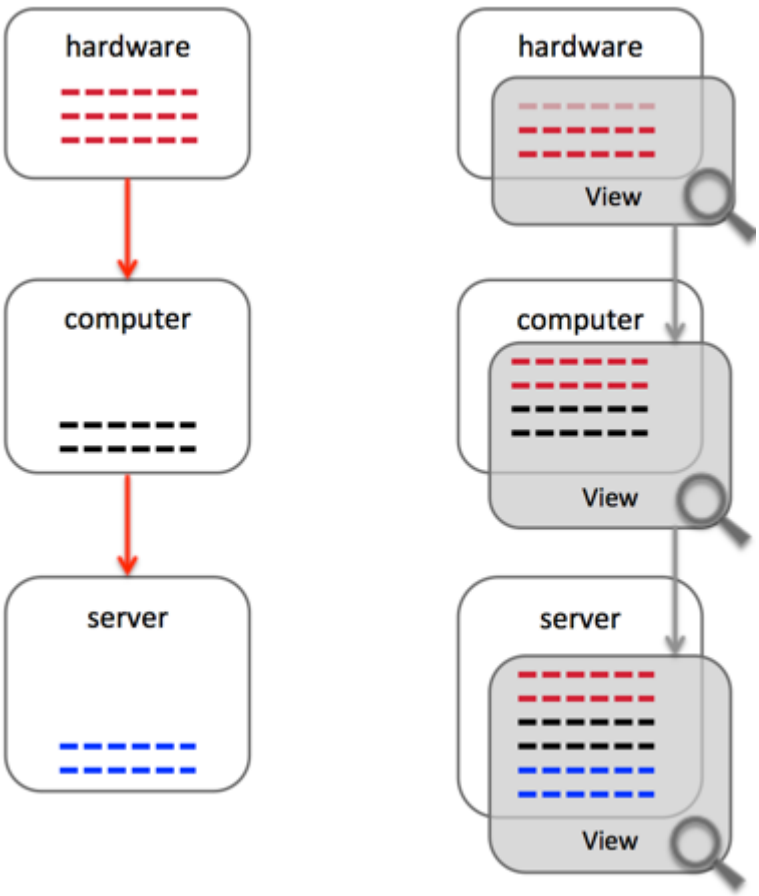


- Wenn Sie eine Ansicht für eine untergeordnete CI-Klasse definieren, enthält diese nur die Attribute, die Sie der untergeordneten CI-Klasse ausdrücklich hinzugefügt haben. Das System zeigt keines seiner übergeordneten Attribute automatisch an.



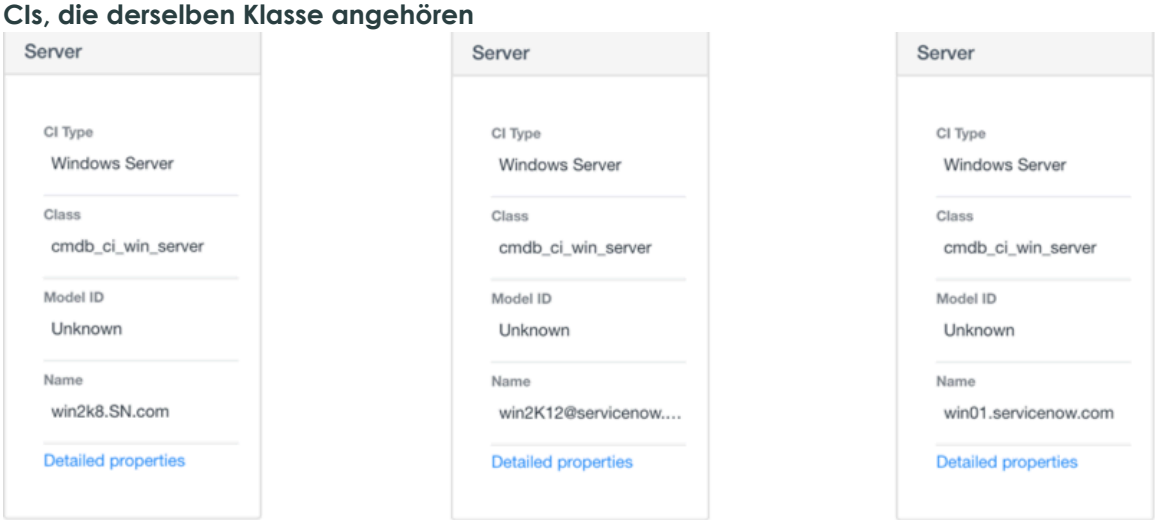
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie der Ansicht keine übergeordnete CI-Klasse oder deren untergeordnete CI-Klasse hinzufügen, verwendet das System die aufsteigende CI-Klasse, die der Ansicht hinzugefügt wurde, zusätzlich zu allen Attributen aller übergeordneten CI-Klassen in der Hierarchie zwischen diesen untergeordneten CI-Klassen sowie die übergeordnete CI-Klasse, die der Ansicht hinzugefügt wird.



Wenn Sie beispielsweise die Ansicht *sa_map_properties* für die CI-Klasse für Windows-Server definieren, werden im Eigenschaftenbereich für alle Windows-Server dieselben Attribute angezeigt: CI-Typ (Klasse), Klasse, Modell-ID und Name.

CIs, die derselben Klasse angehören

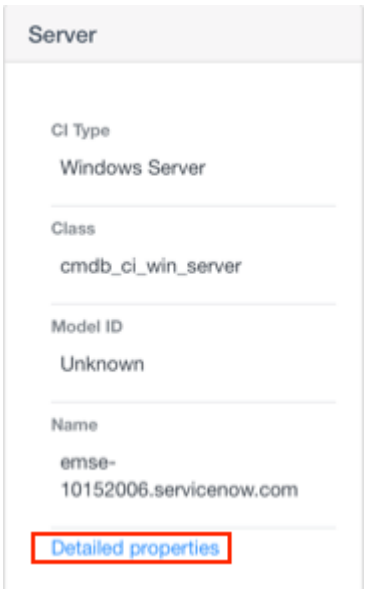


Sie können die Ansicht jederzeit ändern.

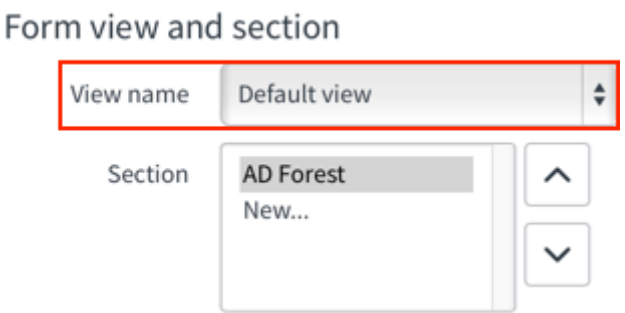
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Wählen Sie in der für Service-Karte das CI aus, dessen Attribute Sie ändern möchten.
3. Klicken Sie im Bereich **Eigenschaften** auf **Detaillierte Eigenschaften**.



4. Klicken Sie auf der Seite „Detaillierte CI-Eigenschaften“ auf das Symbol **Zusätzliche Aktionen**, und wählen Sie **Konfigurieren > Formularlayout** aus.
5. Legen Sie in der Liste **Name der Ansicht** unter **Formularansicht und -abschnitt** fest, welche Ansicht Sie ändern möchten:



   ◦ Wählen Sie **sa_map_properties** aus, wenn es in der Liste angezeigt wird, oder
   ◦ Wenn **sa_map_properties** nicht in der Liste angezeigt wird:
      a. Wählen Sie **Neu**.
      b. Geben Sie im Feld **Name der Ansicht** `sa_map_properties` ein.
      c. Klicken Sie auf **OK**.
6. Verwenden Sie den Slushbucket, um Attribute zu der Ansicht hinzuzufügen oder daraus zu entfernen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Speichern**.
8. Kehren Sie zur für Service-Karte zurück, und wählen Sie das CI, für das Sie die Ansicht geändert haben, erneut aus.
   Im Bereich **Eigenschaften** werden die Attribute angezeigt, die Sie für die Ansicht konfiguriert haben.
9. Wiederholen Sie bei Bedarf das Verfahren für weitere CI-Klassen.

Zugehörige Informationen

CI-Attribute in der Anwendungsservicezuordnung anzeigen –

Unterstützung für Windows-Server mit nicht-englischen Betriebssystemen konfigurieren

Sie können Ihre Now Platform so konfigurieren, dass sie Windows-Server unterstützt, die nicht das englische Windows-Betriebssystem (OS) verwenden.

Vorbereitungen

Sie können dieses Verfahren nur auf MID Serversn verwenden, die Standorte bedienen, die kein englisches Betriebssystem verwenden. Alternativ können Sie diese Konfiguration für alle MID Servers auf einmal durchführen, auch für MID Servers, die für Standorte mit englischen Betriebssystemen verwendet werden.

Erforderliche Rolle: mid_server

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihre Organisation Service-Mapping nicht bereitstellt, ist diese Konfiguration nicht erforderlich.

Manchmal entscheiden sich Unternehmen für die Verwendung von Betriebssystemen in lokalen Sprachen. Ein lokalisiertes Betriebssystem (BS) ist zwar benutzerfreundlich, stellt jedoch ein Problem dar, wenn es um die automatische Erkennung von Windows-Servern geht, auf denen das lokalisierte Betriebssystem ausgeführt wird. Während des Erkennungs- und Zuordnungsprozesses sendet Service-Mapping über einen MID-Server Erkennungsbefehle an die Windows-Server in Ihrer Infrastruktur. Wenn ein Windows-Server eine Nachricht in einer anderen Sprache als Englisch zurückgibt, erkennt Service-Mapping sie nicht als gültige Antwort, und die Interaktion schlägt fehl.

Wenn Ihre Organisation für einige der Windows-Server ein nicht englisches Betriebssystem verwendet, müssen Sie dieses Verfahren ausführen, um sicherzustellen, dass Service-Mapping auf alle Windows-Server zugreifen kann, nicht nur auf die mit dem englischen Betriebssystem. Diese Konfiguration ermöglicht es dem MID-Server, der sich zwischen Service-Mapping und Windows-Servern befindet, eine nicht englische Antwort von einem Windows-Server zu erkennen und die Sprache des CI-Betriebssystems in Englisch zu ändern.

Diese Konfiguration betrifft nur den Benutzer, für den Sie dieses Verfahren durchführen.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Eigenschaften** im Bereich **Module**.
2. Klicken Sie auf **Neu**.
3. Geben Sie im Feld **Name** `mid.servicewatch.wmi.mui` ein.
4. Im Feld **Wert** geben Sie `wahr` ein.
5. Wählen Sie im Feld **MID Server** den Server aus, auf den Sie diese Änderung anwenden möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
Änderung auf alle MID Server in Ihrer Organisation anwenden	Lassen Sie das Feld MID-Server leer.
Änderung auf einen bestimmten MID-Server anwenden	Wählen Sie den erforderlichen MID-Server aus der Liste aus.

6. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Musterbezogene Zuordnungsfehler beheben

MID-Server

Datei rctrlx.exe auf MID Servers hochladen

Laden Sie die Datei rctrlx.exe auf MID Servers hoch, um die Ausführung von Erkennungsbefehlen unter Microsoft Exchange 2007 und 2010 sowie Citrix XenApp zu ermöglichen.

Vorbereitungen
Erforderliche Rolle: admin oder service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird
Während des Erkennungsprozesses führt der MID-Server Service-Mapping und Discovery-Muster auf Anwendungen und Geräten innerhalb des Organisationsnetzwerks aus. Ein Muster ist eine Folge von Befehlen, deren Zweck darin besteht, Attribute eines CI und seiner ausgehenden Verbindungen zu ermitteln. Um Befehle korrekt über PowerShell auszuführen, führt der MID-Server Muster als Services mit der Datei rctrlx.exe aus. Die Datei rctrlx.exe ist Teil des Open Source-Dienstprogramms ManagePC und kann im Internet heruntergeladen werden.

Laden Sie für jeden MID-Server in Ihrer Bereitstellung eine `rctrlx.exe`-Datei hoch.

Prozedur

1. Laden Sie die Datei `rctrix.exe` aus dem Internet auf Ihren Computer herunter.

   Beispielsweise finden Sie unter https://github.com/leonsodhi/rctrlx/releases die neuesten Versionen der Datei `rctrlx.exe`:

2. Speichern Sie die Datei rctrlx.exe im Ordner für Windows 32-Bit-Server:

   ```
   <MID Server-Installationsverzeichnis>\agent\bin\sw_wmi\bin\32
   ```

   Zum Beispiel: C:\SN_MID\SN_MID_Dev\agent\bin\sw_wmi\bin\32.

3. Speichern Sie die Datei rctrlx.exe im Ordner für Windows 64-Bit-Server:

   ```
   <MID Server-Installationsverzeichnis>\agent\bin\sw_wmi\bin\64
   ```

   Zum Beispiel: C:\SN_MID\SN_MID_Dev\agent\bin\sw_wmi\bin\64.

Zugehörige Informationen

Musterbasierte Erkennung in Service-Mapping

MID-Server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optimieren Sie Service-Mapping mit MID-Affinität und Wiederverwendung von IPs

MID-Server, das zum Zuordnen eines Anwendungsservice erforderlich ist, wird in Subnetzen mit überlappenden IP-Bereichen und wiederverwendeten IP-Adressen möglicherweise falsch identifiziert. Um die erfolgreiche Erkennung von Ressourcen zu ermöglichen, die einem Subnetz zugeordnet sind, stellt Service-Mapping mehrere Eigenschaften für die Identifizierung MID-Server von bereit.

Die Netzwerke großer Organisationen sind häufig in zahlreiche Subnetze unterteilt, die jeweils als eigenes Netzwerk fungieren. Service-Mapping wählt den MID-Server basierend auf seinem IP-Bereich aus. Bei Subnetzen mit überlappenden IP-Bereichen und wiederverwendeten IP-Adressen besteht das Risiko einer falschen Identifizierung des für die Zuordnung eines Anwendungsservice benötigten MID-Servers. Daher kann die Discovery fehlschlagen, was zu unvollständigen oder ungenauen Servicezuordnungen führt.

Zwei in Service-Mapping enthaltene Eigenschaften bieten Systemadministratoren eine Lösung.

- MID-Affinität: Wenn eine Horizontal-Discovery konfiguriert wurde, können Sie die Systemeigenschaft *sm.topdown.reuse_mid_from_hd_schedule* aktivieren. Es identifiziert das Subnetz MID-Server, das zuvor während der Horizontal-Discovery konfiguriert wurde, und verwendet es für die Top Down-Discovery in Service-Mappingwieder. Die Konfiguration von MID-Server mit dieser Methode erfordert weniger Zeit und führt zu weniger Falschidentifizierungen.
- Netzwerkstandort: Nachdem den horizontalen Discovery-Zeitplänen Standorte zugewiesen wurden, können Sie die Systemeigenschaft *sm.network_location.detect_host_by_location* aktivieren, die dem Formular „Einstiegspunkt“ das Feld **„Netzwerkstandort“** hinzufügt. Der Discovery-Prozess von oben nach unten beginnt mit dem in diesem Formular definierten Einstiegspunkt und kann dann MID-Server und den Host anhand des im Horizontal-Discovery-Zeitplan angegebenen Speicherorts identifizieren.

Weitere Informationen zum Aktivieren der einzelnen Eigenschaften finden Sie unter Mit Service-Mapping installierte Komponenten

Zugehörige Informationen

Horizontale Erkennung planen

Konfiguration des MID Servers für Service-Mapping

Service-Mapping für die Verwendung mit Configuration Management Database (CMDB)konfigurieren

Konfigurieren Sie Service-Mapping, um die in Ihrem CMDB vorhandenen Daten zu verwenden, um eine Top Down-Discovery auszuführen und Anwendungsservices zuzuordnen.

Vorbereitungen

Stellen Sie sicher, dass die erforderlichen Tabellen gemäß dem in CMDB-basierte Zuordnungerläuterten Prozess mit Daten gefüllt sind.

- Tabelle „TCP-Verbindung (Transmission Control Protocol)“ [cmdb_tcp]
- Tabelle „Laufender Prozess“ [cmdb_running_process].
- Tabelle „Hardware“ [cmdb_ci_hardware].

Bestätigen Sie, dass Sie die Version Service-Mapping Plus August 2024 aus dem ServiceNow® Storeinstalliert haben.

Erforderliche Rolle: service_mapping_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Eingeben von `sys_properties.list` im Navigationsfilter.
2. Suchen Sie in der Tabelle „Systemeigenschaften“ [sys_properties] nach der Eigenschaft *`sa.topdown.enable_cmdb_based_mapping`*.
3. Legen Sie die Systemeigenschaft *`sa.topdown.enable_cmdb_based_mapping`* fest, um Service-Mapping für die Verwendung der Daten in Ihrem CMDBzu konfigurieren.
   a. Bestätigen Sie, dass der Wert im Feld **Typ** auf true | false festgelegt ist.
   b. Legen Sie das Feld **Wert** auf `true`fest.

Agent Client Collector zur Verwendung mit Service-Mappingkonfigurieren

Konfigurieren Sie Agent Client Collector, um Anwendungsservices zu erkennen und zuzuordnen, ohne Anmeldeinformationen für MID-Serverkonfigurieren zu müssen.

Vorbereitungen

Vergewissern Sie sich, dass Agent Client Collector Visibility – Inhalt Version 3.5.0 von ServiceNow® Storeinstalliert wurde.

Stellen Sie sicher, dass Agent Client Collector konfiguriert wurde. Weitere Informationen finden Sie unter Anwendungsmuster für Agent Client Collector.

Stellen Sie sicher, dass die Agents über die erforderlichen Berechtigungen verfügen, um die erforderlichen Anwendungsmusterbefehle für einen erfolgreichen Abschluss der Top Down-Discovery auszuführen. Weitere Informationen finden Sie unter SSH-Befehle, die während der probebasierten Discovery einen privilegierten Benutzer erfordern und SSH-Befehle, die während der probebasierten Discovery keinen privilegierten Benutzer erfordern.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Agent Client Collector ermöglicht die Erkennung und Zuordnung von Anwendungsservices, ohne dass Sie Anmeldeinformationen für MID-Servereinrichten müssen. Sie können sowohl eine Top-Down- als auch eine auf maschinellem Lernen Service-Mapping () basierende Bereitstellung bereitstellen und profitieren von einem vereinfachten Ansatz für die Zuordnung von Anwendungsservices.

Prozedur

1. Eingeben von `sys_properties.list` im Navigationsfilter.
2. Suchen Sie in der Tabelle „Systemeigenschaften“ [sys_properties] nach der Eigenschaft *`sa.topdown.mapping_with_acc_mode`*.
3. Legen Sie die Eigenschaft fest, um Agent Client Collector für Service-Mapping zu konfigurieren, und definieren Sie den Auswahlmodus MID-Server für die Top Down-Discovery.
   a. Bestätigen Sie, dass der Wert im Feld **Typ** auf Ganzzahl festgelegt ist.
   b. Bestimmen Sie, wie die Top Down-Discovery ausgeführt werden soll, indem Sie den **Wert** im Feld „Wert“ festlegen.
   Mögliche Werte:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `0` (Standardeinstellung) – Die Top Down-Discovery wird ausschließlich mit MID-Server ausgeführt.
- `1` : Die Top Down-Discovery versucht zunächst, mit Agent Client Collectorausgeführt zu werden. Wenn kein Agent verfügbar ist, wird standardmäßig MID-Serververwendet.
- `2` : Discovery von oben nach unten wird ausschließlich mit Agent Client Collector ausgeführt. Wenn dies nicht erfolgreich ist, wird der Prozess beendet.

Service Mapping verwenden

Als Service-Mapping -Administrator unterstützen Sie Unternehmen bei ihren Anstrengungen, kritische Anwendungsservices abzubilden und zu warten, damit sie serviceorientiert bleiben.

Greifen Sie über Einheitliche Übersicht auf die Funktion Service-Mapping Arbeitsbereichzu.

Zeigen Sie eine hierarchische Zuordnung von CIs und die Beziehungen zwischen ihnen an, indem Sie Zugriff auf die Funktion Einheitliche Übersicht für Service-Mapping Arbeitsbereichhinzufügen.

Vorbereitungen

Vergewissern Sie sich, dass Sie über Folgendes verfügen:

- Vancouver Release oder höher
- Service-Mapping Plus, Release November 2023
- CMDB-Arbeitsbereich, Version 4.0.1 oder höher

Erforderliche Rolle: sservice_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Überprüfen Sie Einheitliche Übersicht , um mehr über die Funktion Einheitliche Übersicht zu erfahren.

Hinweis: Die Funktion Einheitliche Übersicht bietet eingeschränkte Service-Mapping -Funktionalität.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Geben Sie *`sn_sm_scoped_app.sa.unified_map.enabled`* in das Suchfeld ein.
3. Bestätigen Sie, dass der Wert der Eigenschaft auf „true“ festgelegt ist.
4. Navigieren zu **Arbeitsbereiche** > *`Service-Mapping`*.

   Hinweis: Der Zugriff auf Einheitliche Übersicht ist nur über Service-Mapping Arbeitsbereichmöglich.

5. Wählen Sie das Widget Zugeordnete Anwendungsservices aus.
6. Aktivieren Sie die Checkbox neben dem gewünschten Anwendungsservice.
7. Wählen Sie die Schaltfläche **Karte anzeigen** aus.
   Eine neue Registerkarte wird geöffnet und zeigt Einheitliche Übersicht für den Anwendungsservice in CMDB Arbeitsbereichan.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Zeigen Sie die Attribute eines CI oder einer Beziehung an

Zeigen Sie Serviceinstanzen für ein CI an

Zeigen Sie historische Changes für ein CI an

Anwendungsservices zuordnen basierend auf Empfehlungen für automatisierte Services

Ordnen Sie einen neuen Anwendungsservice basierend auf automatisch generierten Vorschlägen zu. Verwenden Sie die Funktionen Empfehlungen für automatisierte Services oder Service-Fingerabdrücke, um mit wenigen Klicks einen neuen Anwendungsservice zu erstellen oder zu einem vorhandenen Service hinzuzufügen.

Vorbereitungen

- Service-Mapping Plus muss installiert sein. Weitere Informationen finden Sie unter Service-Mapping Plus installieren.
- Bestätigen Sie, dass die Anwendung bereit ist, Anwendungsservices zu erkennen und zuzuordnen. Weitere Informationen finden Sie unter Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie erhalten nicht nur automatisch generierte Vorschläge, sondern können einen Anwendungsservice auch anhand von Vorschlägen Service-Fingerabdrücke identifizieren und auswählen, die Informationen zu den Komponenten in den Anwendungsservice-Kandidaten enthalten. Weitere Informationen finden Sie unter Empfehlungen für automatisierte Services.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service-Mapping**
2. Wählen Sie **ML-basierte Kandidaten**aus.
3. Wählen Sie einen Anwendungsservice entweder basierend auf Kandidatenvorschlägen aus, oder identifizieren Sie Services mit der gewünschten Komponente.

Suchmethode	Aktionen
Wählen Sie basierend auf der gewünschten Komponente aus Kandidaten aus	**a.** Wählen Sie die Registerkarte Service-Fingerabdrücke aus. **b.** Überprüfen Sie die Liste der Service-Fingerabdrücke -Vorschläge, die Komponenten enthalten. **c.** Wählen Sie den gewünschten Anwendungsservice-Candidate aus.
Wählen Sie den Kandidaten anhand der grundlegenden Details aus	**a.** Wählen Sie die Registerkarte Vorschläge für Anwendungsservice aus. **b.** Überprüfen Sie die Liste der vorgeschlagenen Anwendungsservices. **c.** Wählen Sie Ihren bevorzugten Kandidaten aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wahlweise: Zeigen Sie eine Vorschau der Zuordnung an.

   a. Wählen Sie **Vorschauzuordnung**aus.

   b. Überprüfen Sie die Komponenten der vorgeschlagenen Anwendungsservicezuordnung.

      Hinweis: Diese Vorschauzuordnung kann sich vom Candidate unterscheiden, da keine fehlenden Verbindungen angezeigt werden. Weitere Informationen finden Sie im Artikel zur automatisierten Problembehandlung bei Servicevorschlägen [KB1205971] im ServiceNow Support Knowledge Base.

   c. Wählen Sie **Listennavigation** aus, um zur Kandidatenliste zurückzukehren.

5. Wählen Sie **Anwendungsservice zuordnen**aus.
6. Erstellen Sie entweder einen neuen Anwendungsservice mit dem vorgeschlagenen Candidate, oder fügen Sie den vorgeschlagenen Candidate einem vorhandenen Anwendungsservice hinzu.

Aktion	Sc te
Erstellen Sie einen neuen Anwendungsservice	a. Wählen Sie **Neuen Service erstellen aus**. b. Füllen Sie die Felder des Formulars aus. **Formular „Anwendungsservice zu-**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Sc te
ord- nen“.	
Name Vorab ausgefüllter, eindeutiger Name, der für den neuen Anwendungs vorgeschlage wird. Verwenden Sie diesen Namen. Geben Sie einen eindeutigen Namen ein, oder wählen Sie **Andere Namensvorsc** um zusätzliche Optionen zu erhalten. Weitere Informationen finden Sie unter Namensvorsc für Anwendungs Candidates.	
Nummer Vorab ausgefüllte eindeutige ID für	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Sc te
Fügen Sie einem vorhandenen Service einen Kandidaten hinzu	**a.** Wählen Sie **Zu bestehendem Service hinzu-**

den Anwendungs

Beschreibung des neuen Anwendungs

Der Benutzer, der Änderungen am zugeordneten Anwendungs genehmigt oder ablehnt.

Servicebesitze

Servicegrupp

Die bestimmte Anwendungs der Sie diesen Service hinzufügen möchten. Die Standardeins Alle bedeutet, dass der Anwendungs für alle Gruppen verfügbar ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Sc te
	fü-gen. **b.** Be-gin-nen Sie mit der Ein-ga-be des Na-mens des vor-han-de-nen Ser-vices und wäh-len Sie den ge-wünsch-ten Ser-vice aus der Lis-te aus.

Automatische Übersetzung

7. Wählen Sie **Service**zuordnen aus.
8. Wahlweise: Wählen Sie **Zuordnung anzeigen** aus, um den neuen oder geänderten Anwendungsservice anzuzeigen.

Zugehörige Informationen

Empfehlungen für automatisierte Services

Erstellen Sie einen Anwendungsservice für nicht zugeordnete Server

Ordnen Sie Anwendungsservice-Candidates zu, die nicht zugeordnete Server enthalten, und erstellen Sie einen Anwendungsservice mithilfe des Widgets für nicht zugeordnete Server des Arbeitsbereichs Service-Mapping. Das Widget hilft Ihnen, die Ressourcen Ihrer Organisation optimal zu nutzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass Predictive Intelligence aktiviert ist.
- Überprüft die Bereitschaft für maschinelles Lernen.
- Bestätigen Sie, dass die Daten trainiert sind.

Weitere Informationen finden Sie unter Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich

Wichtig:

Service-Mapping Plus v.1.10.0 oder höher:

Wie Sie Ihre Daten erfolgreich aktualisieren und Anwendungskandidaten für nicht zugeordnete Server anzeigen können, erfahren Sie in den Schritten zur Problembehandlung bei der Zuordnung nicht zugeordneter Server zu Anwendungsservice-Kandidaten [KB1585065] im Now Support Knowledge Base.

Erforderliche Rolle: sservice_mapping_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service-Mapping**.
2. Wählen Sie den nicht zugeordneten Server aus, für den Sie einen Anwendungsservice erstellen möchten.
   a. Wählen Sie auf der Kachel **Nicht zugeordnete Server** das Diagramm **Nicht zugeordnete Server mit Kandidaten-ID** aus.
   b. Überprüfen Sie in der Liste Nicht zugeordnete Server mit Kandidaten die Liste der vorgeschlagenen Kandidaten.
   Sie können nach Kandidaten-IDs oder nach Servern gruppieren, um Ihre Arbeit zu priorisieren, indem Sie mit der rechten Maustaste auf den entsprechenden Spaltennamen klicken und **Gruppieren nach**auswählen.
   c. Wählen Sie den gewünschten Kandidaten aus.
3. Wählen Sie **Anwendungsservice zuordnen**aus.

Ergebnisse

Der Anwendungsservice-Candidate wird in einen Anwendungsservice konvertiert, und die nicht zugeordneten Server werden zugeordnet.

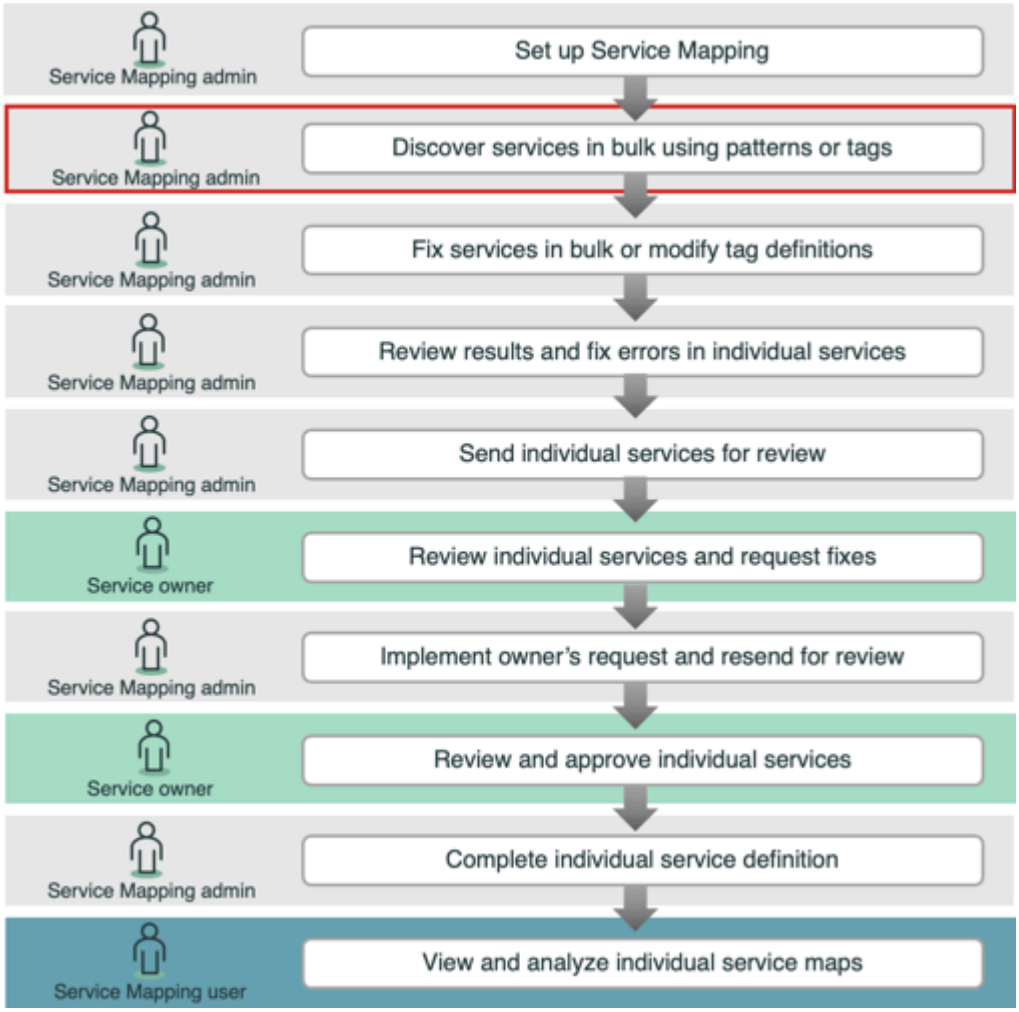
Anwendungsservice-Mapping mit klassisch Service-Mapping

Sie können die erste Zuordnung mehrerer oder einzelner Anwendungsservices in Ihrer Organisation mit einer Methode durchführen, die für Sie am besten geeignet ist.

Sie können Anwendungsservices zuordnen, nachdem Sie das Setup von Service-Mapping abgeschlossen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping-Workflow



Eine typische Organisation hat Hunderte von Anwendungsservices. Ihre individuelle Zuordnung kann zeit- und arbeitsaufwendig sein. Mit Service-Mapping können Sie die meisten IT-Services im Stapel zuordnen. Die gleichzeitige Zuordnung mehrerer Anwendungsservices ist sehr effektiv, aber nicht präzise. Möglicherweise müssen Sie Anwendungsservices, die bei der Stapelzuordnung ausgelassen wurden, individuell zuordnen.

Die Erkennungsmethode hängt davon ab, wie Sie Ihre Anwendungsservices vor der Zuordnung verwaltet haben und welche Informationen Sie über sie gesammelt haben:

- Ordnen Sie mehrere von vorgeschlagene Anwendungsservices zu klassisch Service-Mapping

  Service-Mapping verwendet Lastenausgleichsmodule in Ihrem Netzwerk, um mögliche Anwendungsservices (Kandidaten) zu identifizieren. Sie können alle oder ausgewählte Kandidaten im Stapel zuordnen und dabei mehrere Anwendungsservices in einem einzigen Vorgang erstellen. Diese Methode ist für Ihr Unternehmen geeignet, wenn es nicht allzu viele Informationen zu den Anwendungsservices gibt.

- Ordnen Sie Anwendungsservices mithilfe von Tags zu zu klassisch Service-Mapping

  Wenn Ihre Organisation Tags für die Asset-Verwaltung verwendet, können die Tags zum Zuordnen von Serviceinstanzen verwendet werden. Im Gegensatz zu anderen Zuordnungsmethoden ist es bei der tagbasierten Zuordnung nicht notwendig, Anmeldeinformationen zu konfigurieren oder Benutzern erweiterte Rechte zu gewähren. Sie können Tags effektiv verwenden, um mehrere Serviceinstanzen zuzuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mehrere Anwendungsservices aus einer CSV-Datei mit klassisch Service-Mapping zuordnen

  Diese Methode eignet sich für Sie, wenn Ihre Organisation organisationsübergreifende Zuordnungen und Analysen durchgeführt und Informationen zu geplanten Serviceinstanzen gesammelt hat. In diesem Fall können Sie die gesammelten Informationen in einer bestimmten Reihenfolge organisieren und als CSV-Datei speichern. Service-Mapping extrahiert Informationen aus dieser Datei und erstellt potenzielle Serviceinstanzen, die als Servicekandidaten bezeichnet werden.

- Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping

  Sie können individuelle, einzelne Anwendungsservices nacheinander zuordnen, indem Sie für jeden für Service Attribute definieren. Verwenden Sie diese Zuordnungsmethode für alle Anwendungsservices, die Service-Mapping während der Stapelzuordnung nicht erkennt. Sie müssen wissen oder planen, welche Attribute von Anwendungsservices für die Zuordnung erforderlich sind.

Ordnen Sie mehrere von vorgeschlagene Anwendungsservices zu klassisch Service-Mapping

Sie können mehrere von Service Mapping identifizierte und vorgeschlagene Anwendungsservices in einem einzigen Vorgang zuordnen. Diese Methode ist für Ihr Unternehmen geeignet, wenn es nicht allzu viele Informationen zu den Anwendungsservices gibt.

Vorbereitungen
Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird
Service-Mapping muss zum Zuordnen oder Überprüfen von Serviceinstanzen aktiviert sein.

Unmittelbar nachdem Sie die das Service-Mapping-Setup abgeschlossen haben, erstellt Service-Mapping automatisch potenzielle Anwendungsservices, die als Kandidaten bezeichnet werden:

1. Service-Mapping extrahiert Einträge direkt von Lastenausgleichsmodulen in Ihrem Netzwerk.

2. Von Service-Mapping werden Einträge des Lastenausgleichsmoduls in potenzielle Einstiegspunkte konvertiert und in der Tabelle der Einstiegspunktkandidaten [sa_cand_entry_point] gespeichert.

   Service-Mapping erstellt auch Kandidateneinstiegspunkte basierend auf Netflow und TCP und speichert sie in der gleichen Tabelle.

   Ein Einstiegspunkt ist ein Punkt, auf den Clients auf eine Serviceinstanz zugreifen. Service-Mapping startet den Zuordnungsprozess von diesem Punkt aus. Um beispielsweise Ihre E-Mail-Serviceinstanz zuzuordnen, definieren Sie eine IP-Adresse oder einen Hostnamen des E-Mail-Servers als Einstiegspunkt.

3. Um Duplikate zu vermeiden, überprüft Service-Mapping, ob potenzielle Einstiegspunkte, die aus Netflow- und VPC-Protokollen erstellt werden, eindeutig sind und nicht von vorhandenen Anwendungsservices verwendet werden.

4. Service-Mapping erstellt für jeden Einstiegspunkt einen Kandidaten für die Serviceinstanz.

   Nicht alle Kandidatenserviceinstanzen korrelieren mit tatsächlichen Serviceinstanzen. Service-Mapping filtert unwahrscheinliche Kandidaten heraus, indem ein Algorithmus angewendet wird, der Parameter wie leere IP-Adressen, Portnummern und VIP-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Trefferzahlen des Lastenausgleichsmoduls unter 1000 berücksichtigt. Service-Mapping speichert die Kandidaten in der Tabelle „Kandidateneinstiegspunkt" [sa_cand_entry_point] in der CMDB.

Während des Discovery- und Zuordnungsprozesses erstellt Service-Mapping aus jedem Kandidaten eine Serviceinstanz und weist ihr den vom Kandidaten abgerufenen Einstiegspunkt zu. Eine Massenzuordnung ist zwar eine effektive und schnelle Möglichkeit, zahlreiche Serviceinstanzen zu erstellen, das Ergebnis ist jedoch nicht präzise. Möglicherweise werden versehentlich falsche oder doppelte Serviceinstanzen erstellt, da das Lastenausgleichsmodul nur Rohdaten liefert. Während des Überprüfungs- und Genehmigungsprozesses überprüfen Sie alle zugeordneten Serviceinstanzen und entfernen diejenigen, die irrtümlich erstellt wurden.

Sie können die Liste der Kandidaten weiter filtern, indem Sie bestimmte Kandidaten auswählen, die in die Erkennung aufgenommen oder von ihr ausgeschlossen werden sollen. Die Zuordnung nur ausgewählter Kandidaten bietet die folgenden Vorteile:

- Verkürzt die Erkennungszeit
- Minimiert die Anzahl der potenziell irrelevanten Anwendungsservices

Sie können unerwünschte Kandidaten mit diesen Methoden aus der Liste entfernen, indem Sie sie entweder herausfiltern oder aus der Tabelle „Kandidateneinstiegspunkt" [sa_cand_entry_point] löschen. In beiden Fällen können Sie ausgeblendete oder gelöschte Kandidaten wieder in die Liste aufnehmen.

Prozedur

1. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die von Service-Mapping erkannt werden können oder bereits erkannt wurden. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mit der API erstellt wurden.
2. Überprüfen Sie, dass Service-Mapping eingerichtet und bereit für die Discovery ist.
   Wenn einige obligatorische Konfigurationen fehlen, wird der Fehler oben im Fenster angezeigt.

   a. Klicken Sie auf den Link im Fehler, oder klicken Sie auf das Symbol **Bereitschaftsprüfliste** ( ).

   b. Klicken Sie im Service-Mapping-Fenster „Bereitschaftsprüfliste" auf den Link neben der Setup-Kategorie mit dem Fehlersymbol ( ).
   Sie können nur dann eine Discovery und Zuordnung durchführen, wenn das Fenster „Bereitschafts-Prüfliste" keine Fehler enthält.

   c. Führen Sie die erforderliche Aktion aus, um das Setup abzuschließen.
   Konfigurieren Sie beispielsweise fehlende Anmeldeinformationen.

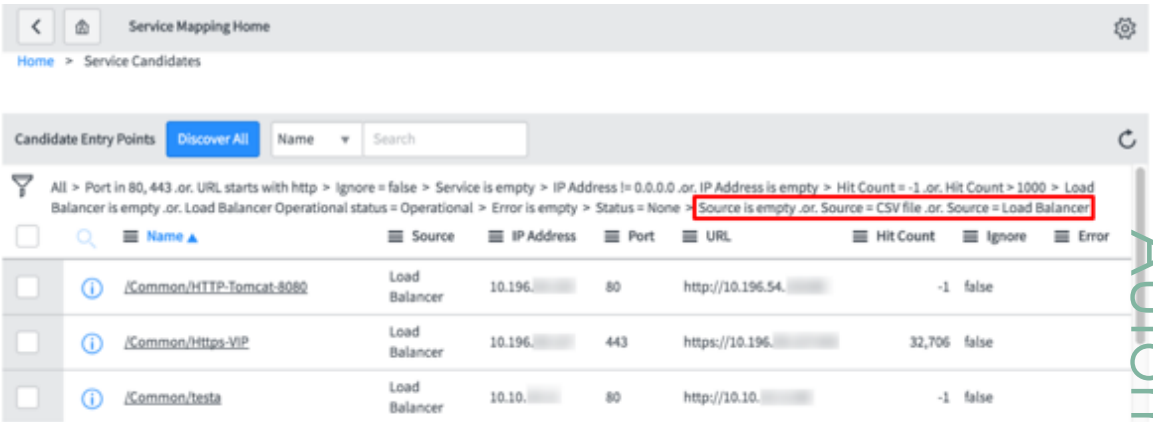
3. Um alle von Service-Mapping vorgeschlagenen Anwendungsservices zuzuordnen, klicken Sie auf **Alle erkennen** oder wählen Sie sie einzeln unter der Schaltfläche „Aktionen für ausgewählte Zeilen" aus und klicken Sie anschließend auf **Auswahl erkennen**.
4. So ordnen Sie von Service-Mapping vorgeschlagene ausgewählte Anwendungsservices zu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie unter der Kachel **Zuordnen** auf **Zusätzliche Optionen**.

b. Wählen Sie **Kandidatenliste anzeigen** aus.

c. Wahlweise: Zeigen Sie Kandidaten basierend auf datenverkehrsbasierten Verbindungen an, entfernen Sie die Bedingung, mit der Kandidaten herausgefiltert werden, die aus Lastenausgleichsmodulen abgerufen oder aus einer CSV-Datei importiert wurden.



Die Kandidatenliste enthält Kandidaten mit dem Quellattribut *netstat*.

d. Überprüfen Sie die Liste der Kandidaten, um zu entscheiden, welche Sie als Anwendungsservices erkennen möchten.

e. Erstellen Sie Anwendungsservices aus den relevanten Kandidaten:

Wenn Sie Anwendungsservices aus den meisten Kandidaten erstellen möchten	**i.** Filtern Sie irrelevante Kandidaten heraus, indem Sie sie auswählen und auf **Aktionen für ausgewählte Zeilen** und dann auf **Ausgewählte ignorieren** klicken. Die irrelevanten Kandidaten werden in der Liste ausgeblendet. **Hinweis:** Zum Anzeigen von Kandidaten, die Sie zuvor herausgefiltert haben, setzen Sie die Filterbedingung **Ignorieren** auf **true**. **ii.** Alternativ filtern Sie irrelevante Kandidaten heraus, indem Sie sie auswählen, auf **Aktionen für ausgewählte Zeilen** klicken und dann **Löschen** wählen. Die irrelevanten Kandidaten werden aus der Tabelle „Kandidateneinstiegspunkt" [sa_cand_entry_point], die die Kandidaten enthält, entfernt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Service-Mapping erstellt gelöschte Kandidaten jedes Mal neu, wenn Discovery eine horizontale Erkennung derselben Lastenausgleichsmodule durchführt oder Sie Kandidaten aus derselben CSV-Datei erneut importieren.

iii. Klicken Sie auf **Alle erkennen**.

Wenn Sie Anwendungsservices nur aus einigen Kandidaten erstellen möchten	**i.** Aktivieren Sie die Kontrollkästchen neben den relevanten Kandidaten. **ii.** Klicken Sie am unteren Bildschirmrand auf **Aktionen für ausgewählte Zeilen**. **iii.** Klicken Sie auf **Auswahl erkennen**.

Service-Mapping startet die Erkennung aller Kandidaten und erstellt Anwendungsservices aus ihnen. Wenn Sie viele Kandidaten haben, kann die Erkennung einige Zeit dauern.

Sobald der Erkennungsprozess abgeschlossen ist, erscheinen unter **Genehmigen** die Anwendungsservices, die Service-Mapping ohne Fehler und mit mindestens einem erkannten CI erkannt hat. Anwendungsservices, die mit Fehlern erkannt wurden, erscheinen auf der Kachel **Beheben**.

Nächste Maßnahme

- Wenn die Funktion für Verbindungsvorschläge aktiviert ist, fügt Service-Mapping datenverkehrsbasierte Verbindungen zu Anwendungsservices nicht automatisch hinzu, sondern macht entsprechende Vorschläge. CIs für mehrere Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen.
- Reparieren Sie die Anwendungsservices, die mit Fehlern erkannt wurden. Weitere Informationen finden Sie unter Fehler bei Anwendungsservices als Massenvorgang beheben.
- Überprüfen Sie die Liste der erstellten Anwendungsservices. Wenn Service-Mapping Anwendungsservices bei der Stapelzuordnung nicht wie erwartet erstellt hat, müssen Sie sie, wie in Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping beschrieben, manuell erstellen.
- Senden Sie ohne Fehler erkannte Anwendungsservices zur Genehmigung an die jeweiligen Eigentümer. Weitere Informationen finden Sie unter Anwendungsservicezuordnungen zur Überprüfung senden.
- Stellen Sie sicher, dass die Serviceinstanzen nicht zu groß sind:
  - Service-Mapping bietet nicht die Möglichkeit, die CI-Liste anstelle einer Zuordnung für eine Serviceinstanz anzuzeigen.
  - Es gibt keine Discovery-Meldung, die darauf hinweist, dass die Serviceinstanz zu groß ist:
    The map does not display the entire service, because it is too large. The number of CI connections exceeded the allowed maximum.

  Wenn einige Anwendungsservices zu groß sind, lösen Sie das Problem der Servicegröße:
  - Wenn Sie anwenderdefinierte Discovery-Muster und Zuordnungsergebnisse in sehr großen Serviceinstanzen verwenden, ändern Sie die Muster so, dass sie keine irrelevanten CIs zuordnen.
  - Teilen Sie den Service in kleinere Services auf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIs für mehrere Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

Wenn die Erkennung auf Basis von Predictive Intelligence aktiviert ist, enthalten die neu zugeordneten Anwendungsservices nur CIs und CI-Verbindungen, die anhand von Erkennungsmustern hinzugefügt wurden. Verwenden Sie Verbindungsvorschläge, um zu entscheiden, welche Konfigurationselemente (CIs) global ein- oder ausgeschlossen werden sollen. Anschließend aktualisiert Service-Mapping alle relevanten erkannten Anwendungsservices auf Grundlage Ihrer Entscheidungen.

Vorbereitungen

Standardmäßig ist die auf Fingerabdrücken basierte Discovery aktiviert. Stellen Sie sicher, dass die auf Fingerabdrücken basierte Discovery nicht deaktiviert wurde: Navigieren Sie zu **Alle** > **System Eigenschafts** > **Alle Eigenschaften**. Stellen Sie sicher, dass die folgende Eigenschaft nicht in der Liste angezeigt wird: *sys_property process.clustering.appfingerprint.enabled*.

Stellen Sie sicher, dass die Discovery basierend auf Predictive Intelligence aktiviert ist. Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties], und überprüfen Sie, ob die Eigenschaft *sa_ml.connection_suggestions.active* auf **True** gesetzt ist.

Mithilfe von Verbindungsvorschlägen können Sie CIs nur in Bezug auf von Service-Mapping erkannte Anwendungsservices hinzufügen oder entfernen.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Discovery basierend auf Predictive Intelligence aktiviert ist, fügt Service-Mapping basierend auf Verbindungsregeln automatisch Verbindungen zu Serviceinstanzen hinzu. Service-Mapping generiert diese Vorschläge basierend auf datenverkehrsbezogenen Daten aus der Configuration Management Database (CMDB) und der Analyse von Anwendungsfingerabdrücken, CIs und Prozessen durch Predictive Intelligence. Predictive Intelligence wertet Verbindungen zwischen Anwendungsfingerabdrücken, CIs und Prozessen aus und bewertet ihre Relevanz. Service-Mapping verwendet diese Informationen, um Verbindungen basierend auf Verbindungsregeln zu erstellen. Außerdem werden Verbindungsvorschläge für Server und Lastenausgleichsmodule generiert, damit Sie entscheiden können, welche Verbindungen den Serviceinstanzen hinzugefügt oder daraus entfernt werden sollen. Weitere Informationen finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Wenn Sie nicht sicher sind, welche datenverkehrsbasierten Verbindungen relevant sind, identifizieren Sie eine Gruppe von Anwendungsservices, die Ihr Unternehmen für diesen Zweck verwendet. Sie können in dieser Gruppe CI-Verbindungen für einen einzelnen Anwendungsservice hinzufügen oder entfernen. Verwenden Sie dann die Verbindungen, die Sie für diesen Service erstellt haben, als Beispiel für datenverkehrsbasierte Verbindungen für mehrere Anwendungsservices.

Prozedur

1. Wahlweise: Folgen Sie den Schritten unter Anwendungen basierend auf Fingerabdrücken erkennen, um Informationen zu allen Anwendungs-CIs in Verbindungsvorschlägen anzuzeigen.

   Wichtig: Wenn Sie keine fingerabdruckbasierte Erkennung verwenden, kann dies dazu führen, dass manche Anwendungs-CIs als allgemeine Anwendungen zugeordnet werden.

2. Navigieren zu **Service-Mapping** > **Administration** > **Verbindungsvorschläge**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Fenster für Verbindungsvorschläge wird geöffnet.

3. Erweitern Sie die relevante Gruppe, um die Verbindungsvorschläge anzuzeigen. Erweitern Sie beispielsweise die Gruppe **python - python**.
4. Überprüfen Sie die Vorschlagsdetails unter Beachtung der in Liste „Verbindungsvorschlagen“ aufgeführten Parameter.
5. Aktivieren Sie die Kontrollkästchen neben den relevanten Vorschlägen, und klicken Sie auf die Aktionsschaltfläche am unteren Rand des Fensters:

Aktion	Ergebnis
Hinzufügen	Service-Mapping nimmt Verbindungen und die CIs, zu denen sie hinführen, in die Serviceinstanz auf. Der *Decision*-Wert für hinzugefügte Verbindungen ändert sich in **Manuell hinzugefügt**.
Ausschließen	Service-Mapping schließt Verbindungen und die CIs, zu denen sie hinführen, aus der Serviceinstanz aus. Der *Decision*-Wert für entfernte Verbindungen ändert sich in **Manuell ausgeschlossen**.
Zurücksetzen	Service-Mapping macht sowohl manuell als auch nach Regel getroffene frühere Entscheidungen rückgängig. Der Wert *Decision* für zurückgesetzte Verbindungen ändern sich in **Unentschieden**. Diese Aktion ist nur relevant, wenn Sie bereits Verbindungsvorschläge zum Abschließen dieser Serviceinstanz verwendet haben.

6. Aktualisieren Sie die Verbindungsvorschläge, um die von Ihnen vorgenommenen Changes anzuzeigen:
   a. Klicken Sie auf das Listensteuerelemente-Symbol .
   b. Wählen Sie **Liste neu laden** aus.

Ergebnisse

Service-Mapping wendet die Changes an datenverkehrsbasierten Verbindungen im Hintergrund auf alle relevanten Anwendungsservices an.

CIs für mehrere Anwendungsservices mithilfe von Verbindungsregeln hinzufügen

Erstellen Sie Regeln für das automatische Hinzufügen von datenverkehrsbasierten Verbindungen und den CIs, zu denen sie führen, in erkannten Serviceinstanzen. Erstellen Sie Regeln, die mehreren Anwendungsservices CIs hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Analysieren Sie die Infrastruktur, die Sie zuordnen, um die häufigsten Verbindungen zu identifizieren. Diese gängigen Verbindungen sind gute Kandidaten für Verbindungsregeln.
- Anwendungen basierend auf Fingerabdrücken erkennen.
- Stellen Sie sicher, dass die Discovery basierend auf Predictive Intelligence aktiviert ist. Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties], und überprüfen Sie, ob die Eigenschaft *sa_ml.connection_suggestions.active* auf **True** gesetzt ist.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Verbindungsvorschläge verbessern die mit Predictive Intelligence generierten Verbindungsvorschläge. Jede Regel enthält eine Bedingung, die einen Aspekt einer datenverkehrsbasierten Verbindung beschreibt. Die in Bedingungen verfügbaren Felder stammen aus der Tabelle „Verbindungsvorschlag“ [sa_ml_connection_suggestion], die bei einer Erkennung von oben nach unten (einer sog. Top-Down-Discovery) gefüllt wird. Sie können Ihre Regeln direkt auf Verbindungsvorschlägen basieren. Erstellen Sie beispielsweise eine Regel für jede Verbindung mit dem Konfidenzniveau „Hoch“. Wenn Sie wissen, welche CIs Teil der Serviceinstanzen sein müssen, können Sie alternativ Felder auswählen, die auf diese CIs verweisen.

Weitere Informationen über die Bewertung und Anwendung von Verbindungsregeln mit Service-Mapping finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Neben Verbindungsregeln, die mehreren Services CIs hinzufügen, können Sie Regeln zum Hinzufügen von CIs zu bestimmten Anwendungsservices erstellen.

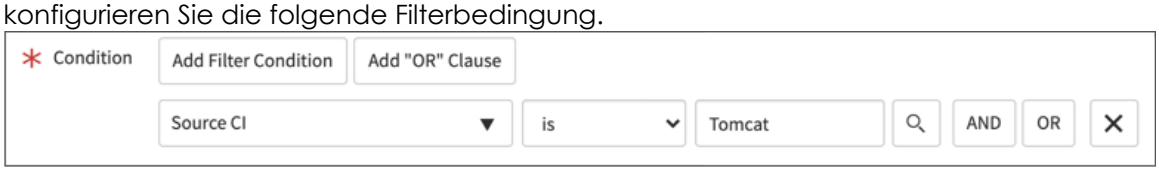
Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Verbindungsregeln**.
   Alternativ können Sie in einer Serviceanwendungszuordnung die Option auswählen **Vorschläge** > **Globale Regeln**.
2. Erstellen Sie eine neue Verbindungsregel, indem Sie auf **Neu** klicken.
   Alternativ können Sie eine vorhandene Regel anpassen, indem Sie in der Liste auf den Namen der Regeln klicken.

   Das Formular „Verbindungsregel“ wird geöffnet.
3. Wählen Sie **Aktiv** aus, um mit der Verwendung dieser Verbindungsregel zu beginnen. Service-Mapping wertet nur aktive Verbindungsregeln aus.
4. Geben Sie im Feld **Name** einen eindeutigen und aussagekräftigen Namen ein.
5. Geben Sie in das Feld **Reihenfolge** den Wert ein, den Service-Mapping für die Sequenz verwendet.
6. Konfigurieren Sie die Filterbedingung im Bereich **Bedingung**.

   a. Wählen Sie das Feld, den Operator und den Wert aus.

   Example
   Um beispielsweise ausgehende Verbindungen für einen Tomcat-Server hinzuzufügen, konfigurieren Sie die folgende Filterbedingung.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Um eine zusätzliche Filterbedingung zu erstellen, klicken Sie auf **Filterbedingung hinzufügen**.

c. Um eine zusätzliche Filterbedingung mit dem Operator ODER zu erstellen, klicken Sie auf **„ODER"-Klausel hinzufügen**.

7. Wählen Sie `Global` aus der Liste **Bereich** aus.
8. Wahlweise: Geben Sie Services an, für die diese Verbindungsregel nicht gilt.

a. Klicken Sie im Bereich **Ausgeschlossene Services** auf **Neu**.
Das Formular „Ausgeschlossener Service" wird geöffnet.

b. Wählen Sie den entsprechenden Service in der Liste **Erkannter Anwendungsservice** aus.

c. Klicken Sie auf **Absenden**.

9. Klicken Sie auf **Aktualisieren**.

Nächste Maßnahme
Gehen Sie wie folgt vor, um zu prüfen, ob Service-Mapping wie erwartet CIs hinzugefügt hat:

1. Nachdem die Anwendungsservices durch die geplanten Aufgaben neu erkannt wurden, öffnen Sie die Zuordnungen der Anwendungsservices, bei denen damit zu rechnen war, dass Service-Mapping CIs hinzufügt.
2. Überprüfen Sie, ob die CIs basierend auf den Verbindungsregeln korrekt hinzugefügt wurden.

Zugehörige Informationen

Erkennung auf Basis von Predictive Intelligence

Ordnen Sie Anwendungsservices mithilfe von Tags zu zu klassisch Service-Mapping

Verwenden Sie Tags, mit denen Sie Konfigurationselemente (CIs) in Ihrer Organisation kategorisieren und organisieren können, um Anwendungsservices zuzuordnen. Für die Tag-basierte Zuordnung ist es nicht erforderlich, Anmeldeinformationen zu konfigurieren oder Benutzern erhöhte Rechte zu gewähren.

Vorbereitungen
Analysieren, überprüfen und definieren Sie Tags, wie in Zuordnung von Anwendungsservices basierend auf Tags vorbereiten beschrieben.

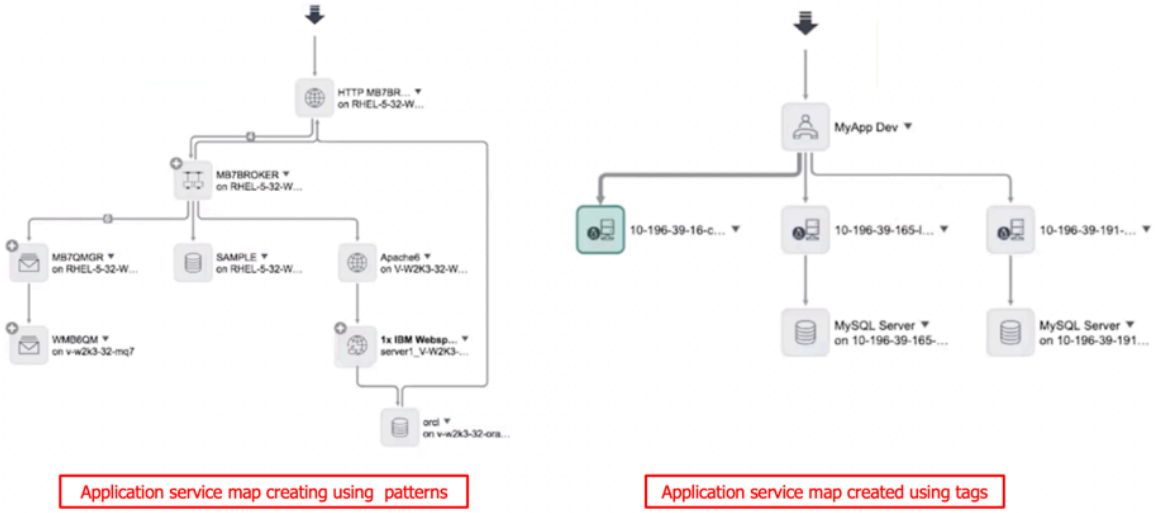
Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird
Ein Tag ist eine Bezeichnung, die aus einem Schlüssel-Wert-Paar besteht. Ihre Organisation verwendet möglicherweise Tags, um Assets zu kategorisieren und um die Abfrage- und Berichtsfunktionen zu verbessern. Discovery und Cloud Provisioning and Governance können die von allen wichtigen Cloud-Anbietern und Container-Ökosystemen verwendeten Tags erkennen. Sobald die Tags erkannt wurden, kann Service-Mapping auf Grundlage dieser Tags Serviceinstanzen erstellen. Beispielsweise können Sie Tags verwenden, um alle Anwendungsservices zuzuordnen, die Ihr Unternehmen in der Produktionsumgebung in der EMEA-Region verwendet. Sie können Tags effektiv verwenden, um mehrere Serviceinstanzen zuzuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Ergebnis der tagbasierten Zuordnung ist eine hierarchische Servicezuordnung, die möglicherweise weniger genau ist als der mit Mustern erstellte Anwendungsservice.

Vergleich von musterbasierten und Tag-basierten Zuordnungsergebnissen



Service-Mapping erstellt Namen für Tag-basierte Services anhand von Tag-Werten, die für die Tag-Definitionen erkannt wurden, denen diese Tag-basierten Services angehören. Beispielsweise lautet der Standardservicename für die Tag-Kategorien „Environment“ und „Application“ mit „Production“ und „HR“ als Tag-Werte „production :: hr“. Tag-basierte Servicenamen verwenden Kleinbuchstaben.

Wichtig: Wenn Sie nach der Zuordnung von Services Tag-Kategorien hinzufügen oder entfernen, implementiert Service-Mapping diese Änderungen nicht für zuvor zugeordnete Services, die zu dieser Servicefamilie gehören. Weitere Informationen finden Sie unter Tag-Definitionen für die Tag-basierte Zuordnung ändern oder aktualisieren.

In nach Domänen getrennten Bereitstellungen Service-Mapping füllt tagbasierte Services auf der Grundlage dieser Servicefamilie nur mit CIs, die zu dem Endknoten gehören, zu der die Servicefamilie gehört.

Zum Zuordnen eines einzelnen Anwendungsservices mithilfe von Tags ohne vorläufige Konfiguration verwenden Sie den Flow basierend auf Gemeinsames Servicedatenmodell. Weitere Informationen finden Sie unter Anwendungsservices mithilfe von Tags ausfüllen .

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Servicefamilien**.
2. Klicken Sie auf **Neu**.
3. Definieren Sie den Namen der Servicefamilienname.
4. Wahlweise: Wählen Sie **regelmäßige Aktualisierung von Servicekandidaten** für Service-Mapping aus, um Vorschläge für Serviceinstanzen neu zu generieren, die Tag-Kategorien entsprechen, die Sie für die Servicefamilie definieren.
5. Definieren Sie die Tag-Kategorien und Tag-Werte für die Zuordnung von Serviceinstanzen, die zu dieser Servicefamilie gehören.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie unter **Selected tag categories** (Ausgewählte Tag-Kategorien) die entsprechende Tag-Kategorie aus der Liste der Tag-Kategorien aus, die Sie zuvor definiert haben.

b. Wahlweise: Fügen Sie den Tag-Wert hinzu, um den Zuordnungsprozess zu präzisieren, z. B. „Produktion“.
Verwenden Sie für mehrere Tag-Werte Kommas als Trennzeichen: Staging, Produktion

c. Wahlweise: Zum Ändern der standardmäßigen Service-Namenskonvention legen Sie die Reihenfolge fest, in der von Service-Mapping die Tag-Werte im Kandidatennamen verwendet werden.
Beispiel: Die erste Kategorie der Servicefamilie ist „Umgebung“, und die zweite Kategorie ist „Anwendung“. Der Standardservicename, der dem Servicekandidaten von Service-Mapping zugewiesen wird, ist „Produktion::Finanzen“. Damit der Wert der Anwendungskategorie von Service-Mapping am Anfang des Namens verwendet wird, legen Sie den Wert für die Reihenfolge der Anwendungskategorie auf 1 fest.

d. Wahlweise: Wählen Sie andere Tag-Kategorien nach Bedarf für diese Servicefamilie aus. Die maximal zulässige Anzahl von Kategorien pro Servicefamilie beträgt drei.

6. Klicken Sie auf **View service candidates** (Servicekandidaten anzeigen).
7. Überprüfen Sie im Servicekandidatenfenster die vorgeschlagenen Servicekandidaten, und wählen Sie diejenigen aus, die Sie zuordnen möchten.
Wenn es keine Servicekandidaten gibt, stellen Sie sicher, dass in der Tabelle „Schlüsselwert“ [cmdb_key_value] für die von Ihnen für die Zuordnung verwendeten Tag-Schlüssel entsprechende Tag-Werte vorhanden sind.
8. Klicken Sie auf **Ausgewählte zuordnen**.

   Service-Mapping Von werden auf Grundlage der von Ihnen ausgewählten Kandidaten Serviceinstanzen erstellt.

   Wenn ein Fehler bezüglich des im System vorhandenen Servicenamens vorliegt, korrigieren Sie den Namen des Kandidaten, indem Sie die folgenden Schritte ausführen:

   a. Klicken Sie auf **View service candidates** (Servicekandidaten anzeigen).

   b. Klicken Sie auf den vorhandenen Namen, und ändern Sie ihn.

   c. Klicken Sie **OK** , um die Änderung zu speichern.

   d. Zeigen Sie die Servicekandidaten an, und ordnen Sie die relevanten zu.

      Neue Kandidaten enthalten nur die Serviceinstanz-CIs als Einstiegspunkte. Von dem geplanten Auftrag „Berechnete Services ausfüllen“ werden einmal täglich neue Tag-basierte Services zugeordnet.

9. Wahlweise: So ordnen Sie einen neuen für Service sofort zu, ohne auf das Ausfüllen des geplanten Auftrags zu warten:
   a. Wählen Sie den entsprechenden für Service aus.
   b. Klicken Sie im für Service-Formular links auf **Zusätzliche Informationen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Klicken Sie unter **Zugehörige Links**auf **Service neu berechnen**.

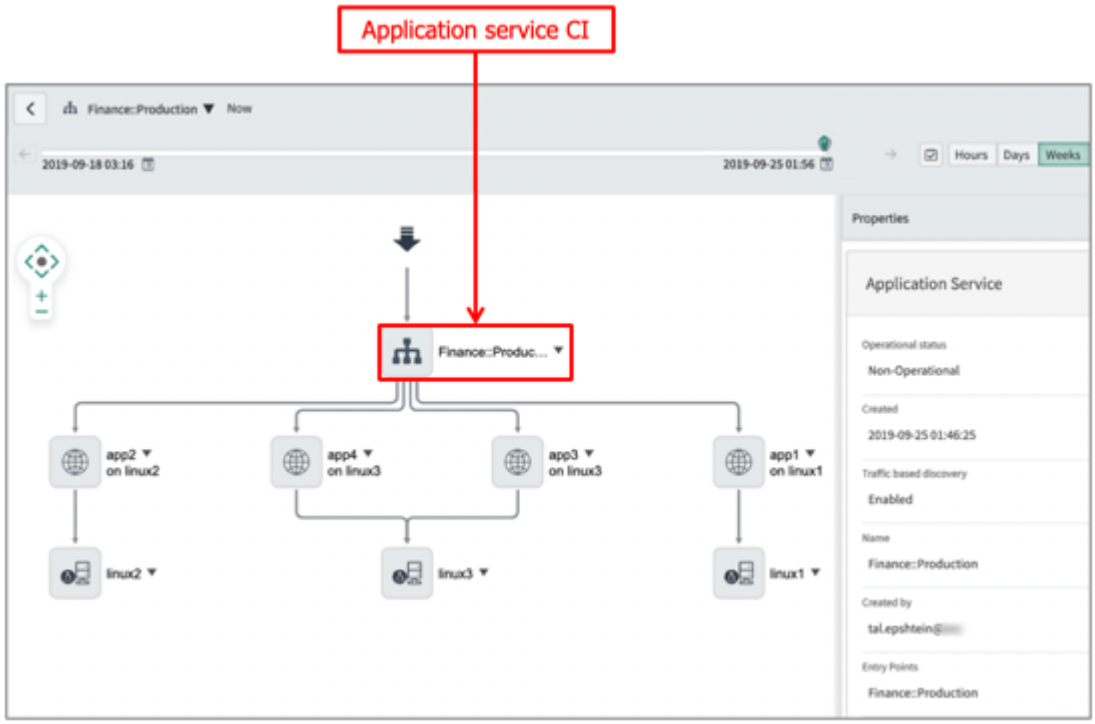
d. Klicken Sie oben im Formular auf **Karte anzeigen**, und überprüfen Sie das Zuordnungsergebnis.

10. Nachdem die geplante Aufgabe alle neuen Tag-basierten Services zugeordnet hat, navigieren Sie zur entsprechenden Tag-basierten Servicefamilie, und überprüfen Sie die neu zugeordneten Services, die unter **Zugeordnete Services** aufgeführt sind.

Ergebnisse

Alle tagbasierten Serviceinstanzen haben ihre jeweiligen Serviceinstanz-CIs als Einstiegspunkte.

Die Zuordnung für die Serviceinstanz „Finance::Production“ basierend auf Tags



Nächste Maßnahme

1. Nachdem die geplante Aufgabe alle neuen Tag-basierten Services zugeordnet hat, navigieren Sie zur entsprechenden Tag-basierten Servicefamilie, und überprüfen Sie die neu zugeordneten Services, die unter **Zugeordnete Services** aufgeführt sind.
2. Stellen Sie sicher, dass die Serviceinstanzen nicht zu groß sind: Die folgende Discovery-Meldung wird in einer Tag-basierten Serviceinstanz angezeigt: *`This tag-based service instance reached the maximum number of CIs. For more information, refer to the product documentation.`*

   Wenn einige Anwendungsservices zu groß sind, lösen Sie das Problem der Servicegröße:

   - Ändern Sie die für die Zuordnung verwendeten Tag-Definitionen, um sicherzustellen, dass Service-Mapping nur relevante CIs in der Serviceinstanz enthält.
   - Bei Bedarf konfigurieren Sie die Tag-basierte Erkennung, um zu ändern, welche CIs Service-Mapping in Tag-basierte Serviceinstanzen einschließt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Um die tagbasierten Services feinzutunen oder zu korrigieren, ändern Sie die Tag-Kategorien, die Sie für die Servicefamilie verwendet haben.

> **Wichtig:** Im Kartenfenster werden Zuordnungen für Tag-basierte und dynamische Services nur im Ansichtsmodus angezeigt. Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Zugehörige Informationen

Richtige Methode zur Erkennung und Zuordnung von Anwendungsservices auswählen

Konfiguration der Tag-basierten Discovery

Zuordnung von Anwendungsservices basierend auf Tags vorbereiten

Analysieren, überprüfen und definieren Sie Tags in Ihrer Organisation für eine erfolgreiche Zuordnung.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie zur Vorbereitung auf die Tag-basierte Zuordnung Tag-Kategorien, die Tags mit ähnlicher Verwendung enthalten.

Definieren Sie eine Tag-basierte Servicefamilie und Tags, die Sie für die Service-Mapping-Zuordnung verwenden möchten. Basierend auf den Tag-Definitionen für die Tag-basierte Servicefamilie erstellt Service-Mapping Servicekandidaten – vorgeschlagene Serviceinstanzen. Überprüfen Sie die Kandidaten und entscheiden Sie, welche Sie zum Erstellen der tatsächlichen Tag-basierten Serviceinstanzen verwenden möchten. Details zum Tag-basierten Prozess finden Sie unter Tag-basierte Erkennung in Service-Mapping.

CIs, die Tag-Werte für die von Ihnen ausgewählten Tag-Kategorien erkannt haben, werden Teil der Anwendungsservices. Service-Mapping erstellt einen separaten Servicekandidaten für jede Tag-Wert-Kombination. Wenn Sie die Kriterien einschränken, indem Sie zusätzlich zu Tag-Kategorien Tag-Werte definieren, ordnet Service-Mapping nur CIs zu, die die entsprechenden Werte aufweisen. CIs, denen mehr als ein Tag zugewiesen sind, können Teil mehrerer Services sein. Sie können eine Tag-Kategorie für Tags erstellen, die sich auf verschiedene Arten von Umgebungen beziehen, wenn Ihre Organisation die Tag-Werte „production“ und „staging“ verwendet. Bei der Tag-basierten Zuordnung wird nicht zwischen Groß- und Kleinschreibung unterschieden. Gleiche Schlüsselnamen und Schlüsselwerte mit Groß- und Kleinschreibung werden als identisch identifiziert.

> **Hinweis:** Service-Mapping enthält CIs, die Teil von CI-Beziehungen sind, auch wenn diesen CIs keine Tags zugewiesen sind. Weitere Informationen finden Sie unter Tag-basierte Erkennung in Service-Mapping.

Prozedur

1. Analysieren Sie die Tag-Nutzung in Ihrer Organisation, und erstellen Sie eine Liste aller Tags und ihrer Zwecke. Verwenden Sie die Schlüsselwerttabelle [cmdb_key_value], um die Tags in der CMDB anzuzeigen.

   Verwenden Sie Tag-Governance, um die Tag-Anwendung in Ihrer Organisation zu analysieren und zu optimieren. Weitere Informationen finden Sie unter Tag-Governance.

2. Falls erforderlich, weisen Sie CIs Tags zu, die Sie in Anwendungsservices aufnehmen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vermeiden Sie es, sehr große Anwendungsservices zu erstellen, die mehr als 5000 CI-Beziehungen enthalten. Derart große Anwendungsservices können zu Leistungsproblemen führen.

3. Erstellen und definieren Sie Tag-Kategorien, die Service-Mapping für die Zuordnung von Serviceinstanzen verwenden soll.

   Um beispielsweise alle Serviceinstanzen zuzuordnen, die Ihre Organisation in der Produktionsumgebung in der EMEA-Region verwendet, erstellen Sie die folgenden Tag-Kategorien: Anwendungen, EMEA-Region und Produktion.

   a. Navigieren zu **Service-Mapping** > **Administration** > **CI-Tag-Kategorien**.
   b. Wählen Sie eine zu ändernde **CI-Tag-Kategorie** aus, oder wählen Sie **Neu**.
   c. Definieren Sie den Tag-Kategorienamen, z. B. *Environment*.
   d. Doppelklicken Sie unter **CI tag keys** (CI-Tag-Schlüssel) auf die Zeile, und geben Sie den Tag-Schlüssel ein, z. B. *Env*.

      Da bei der tagbasierten Zuordnung Groß-/Kleinschreibung nicht berücksichtigt wird, werden Tag-Schlüssel-Varianten mit anderer Kapitalisierung, wie *Env*, *env* oder *ENV*, ebenfalls dieser Tag-Kategorie zugewiesen.

      Wiederholen Sie diesen Schritt, bis Sie alle Tag-Schlüssel-Varianten hinzugefügt haben, die Ihre Organisation für denselben Zweck verwendet, z. B. *Env* und *Environment*.

   Hinweis: Detaillierte Beispiele zum Definieren von Tag-basierten Zuordnungskriterien für Servicefamilien finden Sie unter Beispieldefinitionen für Servicefamilien in Tag-basierter Zuordnung.

4. Führen Sie Discovery aus, um CIs horizontal zu erkennen. Discovery befüllt die CMDB mit den CI-Daten einschließlich Tags.

   Wenn in Ihrer ServiceNow-Instanz Domänentrennung eingesetzt wird und Sie Zugriff auf die globale Domäne haben, melden Sie sich bei der entsprechenden Domäne an. Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.

Mehrere Anwendungsservices aus einer CSV-Datei mit klassisch Service-Mapping zuordnen

Diese Methode eignet sich für Sie, wenn Ihre Organisation organisationsübergreifende Zuordnungen und Analysen durchgeführt und Informationen zu geplanten Serviceinstanzen gesammelt hat. In diesem Fall können Sie die gesammelten Informationen in einer bestimmten Reihenfolge organisieren und als CSV-Datei speichern. Service-Mapping extrahiert Informationen aus dieser Datei und erstellt potenzielle Serviceinstanzen, die als Servicekandidaten bezeichnet werden.

Vorbereitungen

Führen Sie das unter Eine CSV-Datei für die Zuordnung der Kandidaten vorbereiten beschriebene Verfahren aus.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Service-Mapping muss zum Zuordnen oder Überprüfen von Serviceinstanzen aktiviert sein.

Bei Bedarf können Sie Servicekandidaten aus mehreren CSV-Dateien importieren.

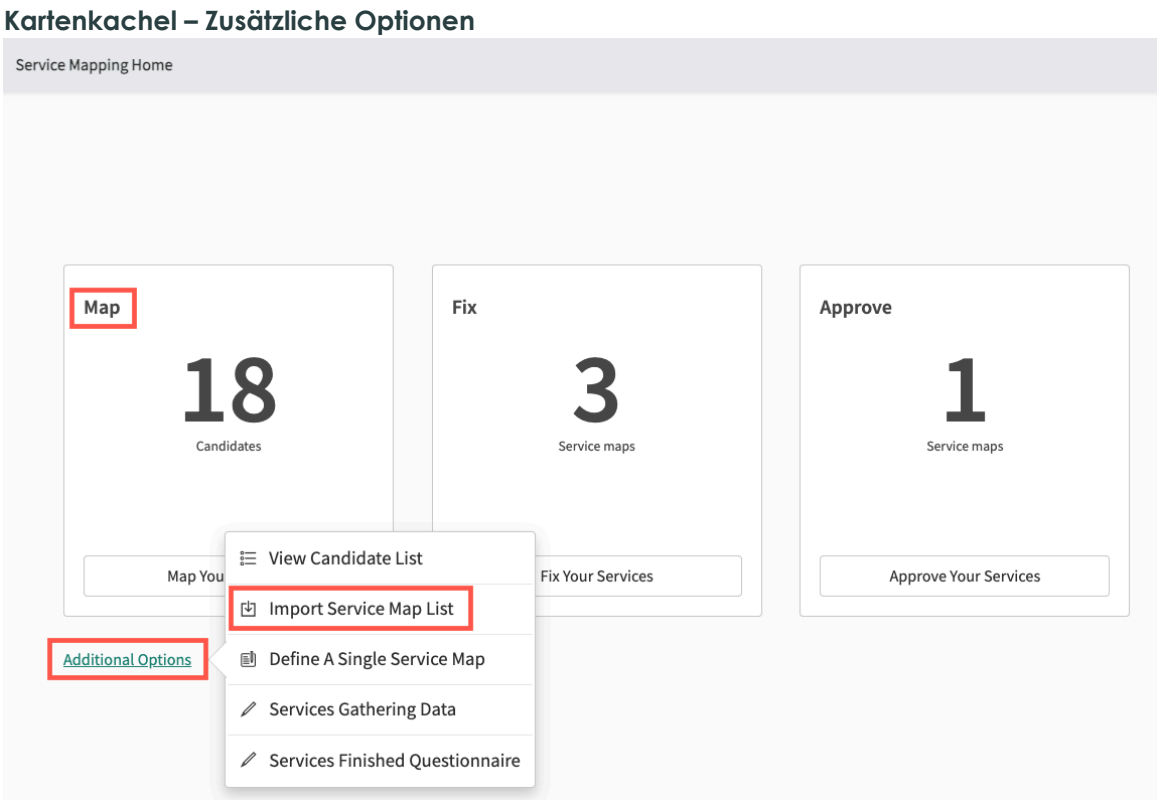
Beim erneuten Importieren von für Service-Kandidaten importiert Service-Mapping keine Kandidaten, die Sie zuvor ignoriert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Service-Mapping Konfigurationselemente (CIs) erkannt hat, die zu Ihrer Serviceinstanz gehören, wird die Erkennung der CIs erneut durchgeführt, damit Änderungen und Aktualisierungen ermittelt werden können. Erstellen oder ändern Sie Discovery-Zeitpläne, um zu steuern, wie oft Service-Mapping-Services oder CIs neu erkannt werden.

Prozedur

1. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die von Service-Mapping erkannt werden können oder bereits erkannt wurden. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mit der API erstellt wurden.
2. Wählen Sie unter der **KartenkachelZusätzliche Optionen**aus.
3. Wählen Sie **Servicezuordnungsliste importieren aus**.



4. Wählen Sie im Fenster „CSV-Datei importieren“ **Datei wählen**.
5. Navigieren Sie zu der CSV-Datei, die für den Import verwendet werden soll, und wählen Sie **Öffnen**aus.
6. Wählen Sie **Importieren**.
   Die importierten für Service-Kandidaten werden der Kandidatenliste hinzugefügt.
7. Überprüfen Sie, ob sich die Gesamtzahl der Service-Kandidaten auf der Kachel **Karte** um die erwartete Anzahl erhöht hat.
8. Wählen Sie auf der **KachelZuordnen Ihre Services zuordnen** aus, um Anwendungsservices aus den Kandidaten zu erstellen, die Sie aus der CSV-Datei importiert haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Überprüfen Sie die Liste der erstellten Anwendungsservices. Wenn Service-Mapping Anwendungsservices bei der Stapelzuordnung nicht wie erwartet erstellt hat, müssen Sie sie, wie in Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping beschrieben, manuell erstellen.
- Reparieren Sie die Anwendungsservices, die mit Fehlern erkannt wurden. Weitere Informationen finden Sie unter Fehler bei Anwendungsservices als Massenvorgang beheben.
- Senden Sie ohne Fehler erkannte Anwendungsservices zur Genehmigung an die jeweiligen Eigentümer. Weitere Informationen finden Sie unter Anwendungsservicezuordnungen zur Überprüfung senden.

Eine CSV-Datei für die Zuordnung der Kandidaten vorbereiten

Organisieren Sie Informationen zu potenziellen Anwendungsservices (Kandidaten) in Ihrer Organisation und speichern Sie sie in einer CSV-Datei.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Erstellen Sie eine XLSX-Datei.
2. Definieren Sie Einstiegspunktattribute für die Servicekandidaten in der XLSX-Datei. Kunden verwenden diese Einstiegspunkte für den Zugriff auf Services. Beispielsweise verwenden sie http://www.google.com:8080, um auf die Google-Seite zuzugreifen.

> ⚠ **Warnung:** Die Spaltenreihenfolge in der XLSX-Datei muss beibehalten werden. Die Eingabe von Attributen in falschen Spalten verursacht Zuordnungsfehler.

Spalte	Beschreibung
A	Geben Sie einen eindeutigen Namen für den geplanten für Service ein. Zum Beispiel„ NY Public Library" oder „Google". ⚠ **Warnung:** Service-Mapping importiert nur Anwendungsservices mit eindeutigen Namen. Wenn in den von Ihnen verwendeten CSV-Dateien mehrere Einträge mit demselben Namen vorhanden sind, überschreibt der zuletzt importierte Datensatz die vorherigen.
B	(Optional) Wenn Sie die URL kennen, die als Einstiegspunkt zu Ihrem für Service dient, geben Sie sie in diese Spalte ein. Geben Sie beispielsweise„ https://www.nypl.org/" oder „www.google.com:8080" ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	⚠ **Warnung:** Wenn Sie die URL definieren, müssen Sie die IP-Adresse, den Port, den FQDN und das Protokoll nicht definieren. Service-Mapping analysiert die URL, um die IP-Adresse, den Port und den FQDN zu extrahieren. Wenn keine URL vorhanden ist, die als Einstiegspunkt dient, definieren Sie andere Parameter in den Spalten C und E.
C	(Optional) Die IP-Adresse des Einstiegspunkts im IPv4-Format. Geben Sie diesen Parameter nur ein, wenn Sie in Spalte B keine URL eingegeben haben.
D	(Optional) Der Port des Einstiegspunkts. Beispiel: „8080“ für die Google-Seite. Geben Sie diesen Parameter nur ein, wenn Sie in Spalte B keine URL eingegeben haben. Wenn Sie weder URL noch Port angegeben haben, verwendet Service-Mapping Port 80 für das HTTP-Protokoll und Port 443 für das HTTPS-Protokoll.
E	(Optional) Der FQDN des Serviceeinstiegspunkts, z. B. „www.google.com“ für Google. Geben Sie diesen Parameter nur ein, wenn Sie in Spalte B keine URL eingegeben haben.

3. Speichern Sie die Datei auf einem Laufwerk, auf das Sie während des Imports zugreifen können, mit der Erweiterung *.csv*.

Nächste Maßnahme

Mehrere Anwendungsservices aus einer CSV-Datei mit klassisch Service-Mapping zuordnen

Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping

Neben der Stapelzuordnung von Anwendungsservices können Sie individuelle, einzelne Anwendungsservices zuordnen, indem Sie Attribute für jeden Anwendungsservice definieren. Verwenden Sie diese Zuordnungsmethode, wenn Sie bereits Details zum Anwendungsservice kennen oder planen. Service-Mapping muss zum Zuordnen oder Überprüfen von Anwendungsservices aktiviert sein.

Vorbereitungen

- Sicherstellen, dass Service-Mapping ordnungsgemäß eingerichtet ist.
- Wenn der für Service auf PaaS aufbaut, das von Microsoft Azure oder Amazon Web Services unterstützt wird, wählen Sie im Servicekonto der Cloud zuerst Rechenzentren erkennen und erstellen Sie dann horizontale Erkennungszeitpläne.

Erforderliche Rolle: service_mapping_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Zusätzlich zur Stapelzuordnung, die für die Zuordnung mehrerer Anwendungsservices sehr effektiv, aber nicht besonders präzise ist, können Sie auch einzelne Anwendungsservices zuordnen. Möglicherweise müssen Sie Anwendungsservices, die bei der Stapelzuordnung ausgelassen wurden, individuell zuordnen.

Das wichtigste Attribut, das Sie zur Erkennung eines Anwendungsservice kennen und konfigurieren müssen, ist ein Einstiegspunkt.

Ein Einstiegspunkt ist ein Punkt, auf den Clients auf eine Serviceinstanz zugreifen. Normalerweise ist dies entweder eine URL oder eine Kombination aus IP-Adresse und Port. Service-Mapping startet den Zuordnungsprozess von diesem Punkt aus. Um beispielsweise Ihre E-Mail-Serviceinstanz zuzuordnen, definieren Sie eine IP-Adresse oder einen Hostnamen des E-Mail-Servers als Einstiegspunkt.

Einstiegspunkte variieren je nach Art von für Service. Service-Mapping bietet eine Vielzahl vorkonfigurierter Einstiegspunkttypen, die viele häufig verwendete Anwendungen abdecken.

Zusätzlich zu Einstiegspunkten, die Service-Mapping erkennen kann, können Sie Einstiegspunkte hinzufügen, die Service-Mapping nicht erkennen kann. Sie können einen solchen Einstiegspunkt als Hinweis darauf hinzufügen, dass Ihr für Service ein Gerät oder eine Anwendung enthält.

Außerdem müssen Sie einen Eigentümer für den für Service definieren. Der Besitzer der Serviceinstanz ist ein Benutzer, der mit der Infrastruktur und den Anwendungen, aus denen der Service besteht, vertraut ist. Dieser Benutzer ist der Serviceinstanz-SME, der die Informationen bereitstellt, die für die erfolgreiche Erstellung einer Serviceinstanz erforderlich sind. Wenn ein Service zugeordnet ist, überprüft dieser Benutzer die Ergebnisse und genehmigt sie entweder oder schlägt Änderungen vor.

Nachdem Service-Mapping Konfigurationselemente (CIs) erkannt hat, die zu Ihrer Serviceinstanz gehören, wird die Erkennung der CIs erneut durchgeführt, damit Änderungen und Aktualisierungen ermittelt werden können. Erstellen oder ändern Sie Discovery-Zeitpläne, um zu steuern, wie oft Service-Mapping-Services oder CIs neu erkannt werden.

Alle Serviceinstanzen, sowohl manuell erstellte als auch von Service-Mappingerkannte, werden in der Tabelle „Zugeordnete Serviceinstanz“ [cmdb_ci_service_discovered] gespeichert.

Sie können einen einzelnen Anwendungsservice auch manuell erstellen, indem Sie den Flow basierend auf Gemeinsames Servicedatenmodellverwenden. Mit Gemeinsames Servicedatenmodell (CSDM) können Sie Servicetypen und Serviceangebote optimieren. Sie können Beziehungen zwischen Anwendungsservices und anderen servicebezogenen Objekten in CSDM hinzufügen: Geschäftsanwendung, technische Serviceangebote oder Business Service-Angebote. Weitere Informationen finden Sie unter Anwendungsservices erstellen .

Prozedur

1. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die von Service-Mapping erkannt werden können oder bereits erkannt wurden. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mit der API erstellt wurden.
2. Klicken Sie unter der Kachel **Zuordnen** auf **Zusätzliche Optionen**.
3. Klicken Sie auf **Einzelne Servicezuordnung definieren**.
4. Definieren Sie die grundlegenden für Service-Attribute:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Anwendungsservicenamen ein, der von keinem anderen Anwendungsservicetyp verwendet wird. Verwenden Sie selbsterklärende Namen wie`Mailing-Service` oder `Druckservice`.
Besitzer	Wählen Sie einen Besitzer aus, der für diese Serviceinstanz in der Organisation verantwortlich ist. Wenn der Besitzername nicht in der Liste angezeigt wird, erstellen Sie einen Benutzer für diese Person, und weisen Sie diesem Benutzer die Rolle sm_app_owner zu. Alternativ können Sie einen Benutzer mit der Rolle service_mapping_admin auswählen.

5. Wenn Sie die Einstiegspunkte nicht kennen, fordern Sie sie wie unter Informationen zu Einstiegspunkten für Anwendungsservices anfordern beschrieben vom Eigentümer des für Service an:
6. Führen Sie die folgenden Schritte aus, um einen Einstiegspunkt hinzuzufügen, den Service-Mapping erkennen kann.

   a. Klicken Sie auf **Erkennbar nach Servicezuordnung**.
   Die Seite bietet Kacheln für Anwendungen, die am häufigsten für Einstiegspunkte verwendet werden.

   b. Klicken Sie auf die Kachel, die der Anwendung entspricht, zu der der Einstiegspunkt gehört.

   Beispiel: **Webanwendung**, wenn Sie einen für Service mit einer Webschnittstelle erstellen. Wenn die Kacheln die erforderliche Anwendung nicht enthalten, klicken Sie auf **Weitere Typen anzeigen**, um eine Auswahl aus der Liste aller vorkonfigurierten Einstiegspunkttypen zu treffen.

   > **Wichtig:** Verwenden Sie keine zentralen IT-Komponenten wie MicrosoftMicrosoft Azure Event Hubs MQ oder Microsoft Active Directory als Einstiegspunkte. Durch die Verwendung solcher Einstiegspunkte werden große Services erstellt, die Leistungsprobleme bei der Zuordnung und Überwachung verursachen.

   c. Wahlweise: Wenn der erforderliche Einstiegspunkttyp nicht in der Liste angezeigt wird, müssen Sie ihn möglicherweise wie in Einstiegspunkttypen für Service-Mapping erstellen beschrieben erstellen.

   d. Konfigurieren Sie Attribute für den Einstiegspunkt, wie in Einstiegspunktattribute beschrieben.
   Einstiegspunktattribute hängen vom ausgewählten Typ ab.

   e. Klicken Sie auf **Hinzufügen**.
   Der Einstiegspunkt wird unter **Einstiegspunkte** hinzugefügt.

   f. Zum Hinzufügen weiterer Einstiegspunkte klicken Sie auf **Einstiegspunkt hinzufügen** und wiederholen Schritt 6.

7. Wahlweise: Führen Sie die folgenden Schritte aus, um einen statischen Einstiegspunkt hinzuzufügen, den Service-Mapping nicht erkennen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf **Manuell erstellt**.

b. Definieren Sie das CI, das als Einstiegspunkt dienen soll.

Feld	Beschreibung
CI-Typ	Wählen Sie den CI-Typ (CI-Klasse) für das hinzuzufügende CI aus. Jedes CI gehört zu einem CI-Typ, der eine Reihe von Attributen enthält, die für diese Art von CI konfiguriert wurden. *cmdb_ci_appl* für Anwendungen.
CI-Name	Wählen Sie das CI aus der Liste der CIs des ausgewählten CI-Typs aus. **Hinweis:** Um verzögerte Ergebnisse bei der Suche nach einem bestimmten CI zu vermeiden, sollten Sie Ihre Suche so spezifisch wie möglich gestalten. Eine Suche mit *<name> kann lange dauern und einen großen Datensatz zurückgeben.

Die Liste der CI-Typen enthält nur zulässige CI-Typen. Sie können beispielsweise keinen Anwendungscluster hinzufügen.

c. Klicken Sie auf **Absenden**.

8. Klicken Sie auf **Speichern** oder **Aktualisieren**, um alle von Ihnen bis zu diesem Zeitpunkt definierte Attribute zu speichern und weiter Attribute für diesen für Service zu konfigurieren. Service-Mapping speichert den neuen für Service in der Tabelle „Zugeordneter Anwendungsservice“ [cmdb_ci_service_discovered]. Außerdem wird im Hintergrund der Erkennungsprozess gestartet.
9. Um Definitionen zu speichern, führen Sie eine Erkennung dieses für Service durch, navigieren Sie zur Zuordnung für diesen für Service, und klicken Sie auf **Karte anzeigen**. Service-Mapping startet den Erkennungsprozess. Die Seite mit der Zuordnung für diesen für Service wird geöffnet und zeigt die gerade stattfindende Zuordnung an. Der für Service-Status wird auf „In Bearbeitung“ geändert.

Nächste Maßnahme

- Wenn Service-Mapping den für Service mit Fehlern erkennt, beheben Sie Fehler in einzelnen Anwendungsservices mithilfe von Erkennungsmeldungen.
- Stellen Sie sicher, dass die Serviceinstanzen nicht zu groß sind:
  - Service-Mapping bietet nicht die Möglichkeit, die CI-Liste anstelle einer Zuordnung für eine Serviceinstanz anzuzeigen.
  - Es gibt keine Discovery-Meldung, die darauf hinweist, dass die Serviceinstanz zu groß ist: *The map does not display the entire service, because it is too large. The number of CI connections exceeded the allowed maximum.*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn einige Anwendungsservices zu groß sind, lösen Sie das Problem der Servicegröße:

- Wenn Sie anwenderdefinierte Discovery-Muster und Zuordnungsergebnisse in sehr großen Serviceinstanzen verwenden, ändern Sie die Muster so, dass sie keine irrelevanten CIs zuordnen.
- Teilen Sie den Service in kleinere Services auf.

- Senden Sie ohne Fehler erkannte Anwendungsservices zur Genehmigung an die jeweiligen Eigentümer. Weitere Informationen finden Sie unter Anwendungsservicezuordnungen zur Überprüfung senden.

Informationen zu Einstiegspunkten für Anwendungsservices anfordern

Das wichtigste Attribut, das Sie zur Erkennung eines für Service kennen und konfigurieren müssen, ist ein Einstiegspunkt. Wenn Sie die Einstiegspunkte für den für Service nicht kennen, fordern Sie sie vom Eigentümer des für Service an:

Vorbereitungen

Das Anfordern von Informationen zu Einstiegspunkten ist ein optionaler Teil der Zuordnung eines einzelnen Anwendungsservice.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Einstiegspunkt ist ein Punkt, auf den Clients auf eine Serviceinstanz zugreifen. Normalerweise ist dies entweder eine URL oder eine Kombination aus IP-Adresse und Port. Service-Mapping startet den Zuordnungsprozess von diesem Punkt aus. Um beispielsweise Ihre E-Mail-Serviceinstanz zuzuordnen, definieren Sie eine IP-Adresse oder einen Hostnamen des E-Mail-Servers als Einstiegspunkt.

Einstiegspunkte variieren je nach Art von für Service. Service-Mapping bietet eine Vielzahl vorkonfigurierter Einstiegspunkttypen, die viele häufig verwendete Anwendungen abdecken.

Prozedur

1. Klicken Sie auf den Link **Daten anfordern**.
   Das Fenster „Anforderung von Daten“ wird geöffnet.
2. Wenn die Liste **Zugewiesen an** leer ist, wählen Sie den Namen des Verantwortlichen für den für Service aus.
3. Geben Sie Ihre Fragen zu für Service in das Feld **Beschreibung** ein.
   Beispielsweise können Sie nach den Einstiegspunkten fragen.
4. Klicken Sie auf **Absenden**.
   Das System öffnet die Aufgabe ServiceNow für den Eigentümer und sendet automatisch eine E-Mail-Benachrichtigung.
5. Überprüfen Sie die Informationen, die der Eigentümer auf den Registerkarten **Andere Eingabepunkte** und **Komponenten** hinzugefügt hat.
   Sobald der Besitzer fehlende Informationen bereitstellt, erhalten Sie eine E-Mail-Benachrichtigung.
6. Klicken Sie auf den Link in der E-Mail, um den Fragebogen für den entsprechenden für Service zu öffnen.
7. Setzen Sie die Zuordnung eines einzelnen Anwendungsservice fort.

Geben Sie Einstiegspunkte für die Zuordnung eines Anwendungsservice an

Als Anwendungsservice-Eigentümer erhalten Sie in einer E-Mail-Benachrichtigung möglicherweise eine Anforderung, Informationen zu den Einstiegspunkten bereitzustellen.

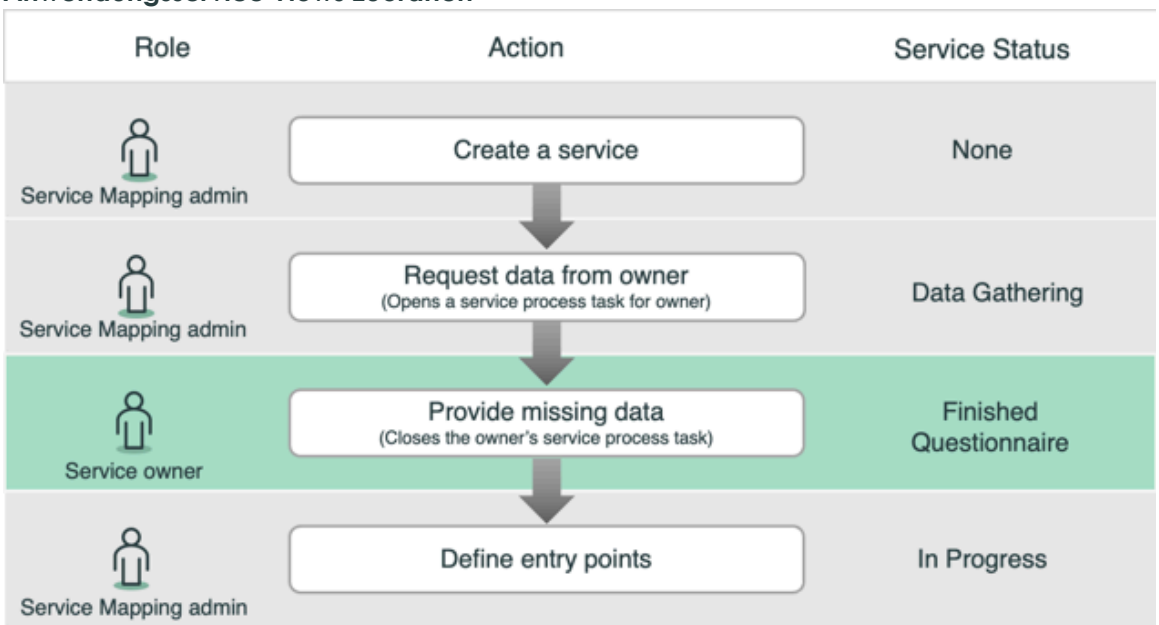
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie Informationen zu Einstiegspunkten bereit, damit Administratoren die Erkennung eines Anwendungsservice starten können.

Vorbereitungen
Erforderliche Rolle: sm_app_owner oder service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Informationen zu den für Service-Einstiegspunkten fehlen, kann ein Administrator die Zuordnung des für Services nicht starten. In diesem Fall sendet der Administrator eine Anforderung für fehlende Daten aus dem für Service-Formular, wodurch eine Serviceprozessaufgabe erstellt und Ihnen zugewiesen wird. Sie erhalten eine E-Mail-Benachrichtigung mit dem Link zur Fragebogenseite, auf der Sie die fehlenden Daten eingeben müssen. Die wichtigsten Informationen beziehen sich auf die Einstiegspunkte, jedoch sind zusätzliche Daten über Anwendungsservicekomponenten, deren Verbindungen oder Verwendung für den Administrator hilfreich. Wenn Sie die Dateneingabe abgeschlossen und den Fragebogen übermittelt haben, schließt das System die Serviceprozessaufgabe.

Anwendungsservice-Flows zuordnen



Prozedur
1. Klicken Sie auf den Link in der Benachrichtigungs-E-Mail, um auf die Seite **Fragebogen** zuzugreifen.
2. Sie können die Seite **Fragebogen** auch in der Liste der Ihnen zugewiesenen Aufgaben öffnen.
   a. Navigieren zu **Service-Mapping** > **Administration** > **Meine Aufgaben**.
   b. Wahlweise: Sortieren Sie die Liste der Serviceprozessaufgaben nach Bedarf.
   c. Klicken Sie auf die erforderliche Aufgabe.
   d. Klicken Sie auf den Formularlink des für Service.
   e. Klicken Sie im linken Bereich auf **Fragebogen**.
3. Geben Sie auf der Registerkarte **Geplante benutzerdefinierte Einstiegspunkte** Informationen zu den für Service-Einstiegspunkten ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Wenn Sie die genauen Attribute der Einstiegspunkte, wie z. B. die URL oder die IP-Adresse, nicht angeben können, fügen Sie allgemeine Informationen hinzu, die den Administrator leiten können. Beispielsweise den Typ der Anwendung wie Tomcat-Server.

4. Um Informationen zu anderen Komponenten hinzuzufügen, die diesen für Service enthalten, klicken Sie auf die Registerkarte **Komponenten** und geben die entsprechenden Daten ein.
5. Wenn Sie mit der Eingabe der Informationen fertig sind, klicken Sie auf **Aktionen** und anschließend auf **Fragebogen senden**.
   Die Ihnen zugewiesene Datenanforderungsaufgabe wird geschlossen. Der für Service-Status wird auf „In Bearbeitung“ geändert.
6. Wenn es weitere hilfreiche Informationen zu diesem für Service gibt, geben Sie diese im Feld **Hinweise** unter **Arbeitsnotizen** ein, und drücken die Eingabetaste, um Ihren Kommentar zu veröffentlichen.

CIs für einzelne Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

Wenn die Erkennung auf Basis von Predictive Intelligence aktiviert ist, enthalten die neu zugeordneten Anwendungsservices nur CIs und CI-Verbindungen, die anhand von Erkennungsmustern hinzugefügt wurden. Vervollständigen Sie einen Anwendungsservice mit den Vorschlägen, die Service-Mapping für CI-Verbindungen generiert.

Vorbereitungen

- Standardmäßig ist die auf Fingerabdrücken basierte Discovery aktiviert. Stellen Sie sicher, dass die auf Fingerabdrücken basierte Discovery nicht deaktiviert wurde: Navigieren Sie zu **Alle** > **System Eigenschafts** > **Alle Eigenschaften**. Stellen Sie sicher, dass die folgende Eigenschaft nicht in der Liste angezeigt wird: *`sys_property process.clustering.appfingerprint.enabled`*.
- Stellen Sie sicher, dass die Discovery basierend auf Predictive Intelligence aktiviert ist. Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties], und überprüfen Sie, ob die Eigenschaft *`sa_ml.connection_suggestions.active`* auf **True** gesetzt ist.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Discovery basierend auf Predictive Intelligence aktiviert ist, fügt Service-Mapping basierend auf Verbindungsregeln automatisch Verbindungen zu Serviceinstanzen hinzu. Service-Mapping generiert diese Vorschläge basierend auf datenverkehrsbezogenen Daten aus der Configuration Management Database (CMDB) und der Analyse von Anwendungsfingerabdrücken, CIs und Prozessen durch Predictive Intelligence. Predictive Intelligence wertet Verbindungen zwischen Anwendungsfingerabdrücken, CIs und Prozessen aus und bewertet ihre Relevanz. Service-Mapping verwendet diese Informationen, um Verbindungen basierend auf Verbindungsregeln zu erstellen. Außerdem werden Verbindungsvorschläge für Server und Lastenausgleichsmodule generiert, damit Sie entscheiden können, welche Verbindungen den Serviceinstanzen hinzugefügt oder daraus entfernt werden sollen. Weitere Informationen finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Wichtig: Mithilfe von Verbindungsvorschlägen können Sie CIs nur in Bezug auf von Service-Mapping erkannte Anwendungsservices hinzufügen oder entfernen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wahlweise: Folgen Sie den Schritten unter Anwendungen basierend auf Fingerabdrücken erkennen, um Informationen zu allen Anwendungs-CIs in Verbindungsvorschlägen anzuzeigen.

   Wichtig: Wenn Sie keine fingerabdruckbasierte Erkennung verwenden, kann dies dazu führen, dass manche Anwendungs-CIs als allgemeine Anwendungen zugeordnet werden.

2. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
3. Klicken **Vorschläge** > **Verbindungsvorschläge** oben in der Zuordnung, um Vorschläge für den gesamten Anwendungsservice anzuzeigen.
   Klicken Sie alternativ mit der rechten Maustaste auf ein CI, für das Sie Verbindungsvorschläge anzeigen möchten, und wählen Sie **Verbindungsvorschläge anzeigen** aus.
4. Überprüfen Sie die Vorschlagsdetails unter Beachtung der in Liste „Verbindungsvorschlagen“ aufgeführten Parameter.
5. Wahlweise: Wenn keine Anwendungs-CIs erkannt wurden, ermitteln Sie ein eigenständiges CI der Anwendungsklasse basierend auf Fingerabdrücken:
   a. Klicken Sie neben dem entsprechenden Vorschlag, der auf den Anwendungsfingerabdrücken (AFP) basiert, auf das **Vorschausymbol** .
   In der daraufhin geöffneten Liste „Verbindungsvorschlag“ werden Details zum betreffenden Vorschlag angezeigt.
   b. Klicken Sie neben **Ziel-AFP** auf das Symbol **Vorschau auf diesen Datensatz anzeigen**, und klicken Sie dann auf **Datensatz öffnen**.
   c. Klicken Sie auf **Anwendung erkennen**.
   d. Klicken Sie im Fenster „Vorgeschlagene Verbindungen prüfen“ auf **Aktualisierung**, um sicherzustellen, dass die angezeigten Informationen die erkannten CI-Klassen widerspiegeln.

   Wichtig: Wenn Sie keine fingerabdruckbasierte Erkennung verwenden, kann dies dazu führen, dass manche Anwendungs-CIs als allgemeine Anwendungen zugeordnet werden.

6. Aktivieren Sie die Kontrollkästchen neben den relevanten Vorschlägen, und klicken Sie auf die Aktionsschaltfläche am unteren Rand des Fensters:

Aktion	Ergebnis
Hinzufügen	Service-Mapping nimmt Verbindungen und die CIs, zu denen sie hinführen, in die Serviceinstanz auf. Der *Decision*-Wert für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Ergebnis
	hinzugefügte Verbindungen ändert sich in **Manuell hinzugefügt**.
Ausschließen	Service-Mapping schließt Verbindungen und die CIs, zu denen sie hinführen, aus der Serviceinstanz aus. Der *Decision*-Wert für entfernte Verbindungen ändert sich in **Manuell ausgeschlossen**.
Zurücksetzen	Service-Mapping macht sowohl manuell als auch nach Regel getroffene frühere Entscheidungen rückgängig. Der Wert *Decision* für zurückgesetzte Verbindungen ändern sich in **Unentschieden**. Diese Aktion ist nur relevant, wenn Sie bereits Verbindungsvorschläge zum Abschließen dieser Serviceinstanz verwendet haben.

7. Klicken Sie auf **Schließen**, um das Fenster „Vorgeschlagene Verbindungen prüfen“ zu schließen.

Ergebnisse
Die Anwendungsservice-Zuordnung spiegelt die von Ihnen vorgenommenen Änderungen wider. In der Zuordnung werden die von Ihnen hinzugefügten Verbindungen und die CIs angezeigt, zu denen sie führen.

Zugehörige Informationen

Datenverkehrsbasierte Erkennung in Service-Mapping

CIs für einzelne Anwendungsservices mithilfe von Verbindungsregeln hinzufügen

Erstellen Sie Regeln für das automatische Hinzufügen von datenverkehrsbasierten Verbindungen und den CIs, zu denen sie führen, in erkannten Serviceinstanzen. Fügen Sie mithilfe von Verbindungsregeln CIs für bestimmte Anwendungsservices hinzu.

Vorbereitungen
- Analysieren Sie die Infrastruktur, die Sie zuordnen, um die häufigsten Verbindungen zu identifizieren. Diese gängigen Verbindungen sind gute Kandidaten für Verbindungsregeln.
- Stellen Sie sicher, dass die Discovery basierend auf Predictive Intelligence aktiviert ist. Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties], und überprüfen Sie, ob die Eigenschaft *sa_ml.connection_suggestions.active* auf **True** gesetzt ist.
- Anwendungen basierend auf Fingerabdrücken erkennen.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird
Verbindungsvorschläge verbessern die mit Predictive Intelligence generierten Verbindungsvorschläge. Jede Regel enthält eine Bedingung, die einen Aspekt einer datenverkehrsbasierten Verbindung beschreibt. Die in Bedingungen verfügbaren Felder stammen aus der Tabelle „Verbindungsvorschlag“ [sa_ml_connection_suggestion], die bei einer Erkennung von oben nach unten (einer sog. Top-Down-Discovery) gefüllt wird. Sie können Ihre Regeln direkt auf Verbindungsvorschlägen basieren. Erstellen Sie beispielsweise

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Regel für jede Verbindung mit dem Konfidenzniveau „Hoch“. Wenn Sie wissen, welche CIs Teil der Serviceinstanzen sein müssen, können Sie alternativ Felder auswählen, die auf diese CIs verweisen.

Sie können Verbindungsregeln erstellen, die für bestimmte Anwendungsservices oder für alle Anwendungsservices gelten. Wenn die Regel für einen bestimmten Service gilt, die Regelbedingung jedoch auf ein CI verweist, das Teil mehrerer Services ist, fügt Service-Mapping dieses CI allen relevanten Services hinzu.

Weitere Informationen über die Bewertung und Anwendung von Verbindungsregeln mit Service-Mapping finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Neben Verbindungsregeln, die bestimmten Services CIs hinzufügen, können Sie Regeln zum Hinzufügen von CIs zu mehreren Anwendungsservices erstellen.

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Verbindungsregeln**.
   Alternativ können Sie in einer Serviceanwendungszuordnung die Option auswählen **Vorschläge** > **Lokale Regeln**.
2. Erstellen Sie eine neue Verbindungsregel, indem Sie auf **Neu** klicken.
   Alternativ können Sie eine vorhandene Regel anpassen, indem Sie in der Liste auf den Namen der Regeln klicken.
3. Wählen Sie **Aktiv** aus, um mit der Verwendung dieser Verbindungsregel zu beginnen. Service-Mapping wertet nur aktive Verbindungsregeln aus.
4. Geben Sie im Feld **Name** einen eindeutigen und aussagekräftigen Namen ein.
5. Geben Sie in das Feld **Reihenfolge** den Wert ein, den Service-Mapping für die Sequenz verwendet.
6. Konfigurieren Sie die Filterbedingung im Bereich **Bedingung**.

   a. Wählen Sie das Feld, den Operator und den Wert aus.

   Example
   Um beispielsweise ausgehende Verbindungen für einen Tomcat-Server hinzuzufügen, konfigurieren Sie die folgende Filterbedingung.

   b. Um eine zusätzliche Filterbedingung zu erstellen, klicken Sie auf **Filterbedingung hinzufügen**.

   c. Um eine zusätzliche Filterbedingung mit dem Operator ODER zu erstellen, klicken Sie auf **„ODER“-Klausel hinzufügen**.

7. Wählen Sie `Lokal` aus der Liste **Bereich** aus.
8. Wählen Sie in der Liste **Erkannter Anwendungsservice** einen vorhandenen Service aus, für den diese Regel gilt.
9. Klicken Sie auf **Aktualisieren**.

Nächste Maßnahme

Gehen Sie wie folgt vor, um zu prüfen, ob Service-Mapping wie erwartet CIs hinzugefügt hat:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Öffnen Sie die Zuordnung für den Anwendungsservice, den Sie für diese Verbindungsregel ausgewählt haben.
2. Klicken Sie oben im Kartenfenster auf **Erkennen**.
3. Nachdem der Anwendungsservice erneut erkannt wurde, überprüfen Sie, ob CIs basierend auf der Verbindungsregel korrekt hinzugefügt wurden.

Aktivieren Sie die Traffic-basierte Discovery für einen Anwendungsservice

Sorgen Sie dafür, dass Service-Mapping datenverkehrsbasierte Verbindungen verwendet, um die CIs zu erkennen, aus denen ein Anwendungsservice besteht.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Service-Mapping kann Konfigurationselemente (CIs) anhand ihrer datenverkehrsbasierten Verbindungen erkennen und zuordnen. Diese Methode wird als datenverkehrsbasierte Zuordnung bezeichnet und ergänzt die musterbasierte Zuordnung. Weitere Informationen dazu, wie Service-Mapping eine datenverkehrsbasierte Erkennung durchführt, finden Sie unter Datenverkehrsbasierte Erkennung in Service-Mapping.

Prozedur

1. Führen Sie in der klassischen Umgebung die folgenden Schritte aus:

   a. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die von Service-Mapping erkannt werden können oder bereits erkannt wurden. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mit der API erstellt wurden.

   b. Klicken Sie auf der Kachel **Abgeschlossen** auf **Ihre Services anzeigen**.

   c. Wählen Sie den entsprechenden Anwendungsservice.

   d. Klicken Sie auf **Zusätzliche Informationen**.

   e. Aktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.

   f. Klicken Sie auf **Aktualisieren**.

2. Alternativ führen Sie die folgenden Schritte in der Mitarbeiterbereich-Benutzeroberfläche aus:

   a. Navigieren zu **Mitarbeiterbereich** > **Mitarbeiterbereich-Startseite**.

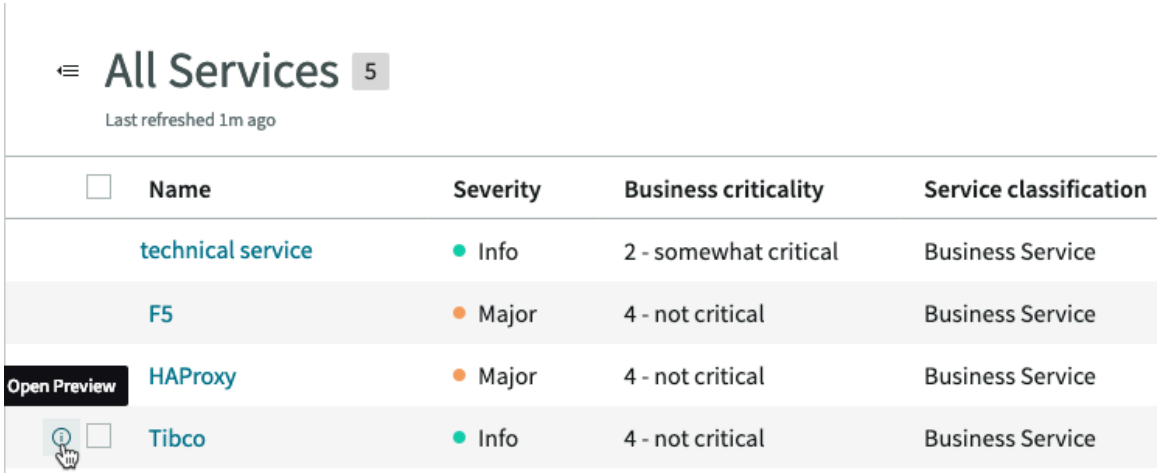
   b. Klicken Sie im linken Bereich auf **Listen**.

   c. Navigieren zu **Services** > **Alle Services**.
   Die Liste der Services zeigt Services im Status „Betriebsbereit“ an.

   d. Wählen Sie den entsprechenden Anwendungsservice.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Klicken Sie auf das Symbol **Vorschau öffnen**.



Der Detailbereich wird auf der rechten Seite geöffnet.

f. Aktivieren Sie im Bereich „Details" das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.

g. Klicken Sie auf **Aktualisieren**.

Anwendungsservices zuordnen, die Citrix XenApp und Presentation Server enthalten

Service-Mapping kann Anwendungsservices erkennen, die Citrix XenApp, Presentation Server und Citrix Usage Collector enthalten.

Erkannte Komponenten

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Citrix XenApp-Server	Windows	6.x> 6.5, 7.x <7.6	WMI WinRM	Horizontal und von oben nach unten	Citrix XenApp- oder Präsentationsserver
Citrix Presentation Server	Windows	4.x, 5.x, 6.x <6,5	WMI WinRM	Horizontal und von oben nach unten	Citrix XenApp- oder Präsentationsserver
Citrix-Nutzungssammler	Windows	7.x> 7,5, 8.x	WMI WinRM	Von oben nach unten	Citrix Collector
Allgemeine Anwendung basierend	Windows	-	WMI WinRM	Von oben nach unten	Symbolpfad der Citrix-Anwendung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
auf dem Symbolpfad					

Anwendungsservices zuordnen, die Citrix XenApp und Presentation Server enthalten

Ordnen Sie einen Anwendungsservice mit Citrix XenApps, Presentation Servern und Citrix Usage Collectors zu und vergewissern Sie sich, dass Service-Mapping alle Citrix-Komponenten richtig erkannt hat.

Vorbereitungen

- Erteilen Sie einem Benutzer die Berechtigung zum Lesen und Abfragen des Citrix-Repository:
  - Bei Versionen 4.5 und höher ein PowerShell-Skript vom XenApp-Server.
  - Für Versionen vor 4.5 ein MicrosoftMicrosoft Azure Event Hubs Visual Basic Script (VBScript) vom Citrix-Präsentationsserver
- Konfigurieren Sie auf der Now Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben.

  Hinweis: Um diese Anmeldeinformationen später für XenAPP zu verwenden, legen Sie das Attribut **Alias für Anmeldeinformationen** auf cmdb_ci_appl_citrix_xenapp fest. Um diese Anmeldeinformationen später für Citrix zu verwenden, legen Sie das Attribut **Alias für Anmeldeinformationen** auf cmdb_ci_appl_citrix_collector fest.

- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren
- Konfigurieren Sie einen Benutzer mit Berechtigungen zum Ausführen von PowerShell-Befehlen auf dem Citrix-Server.
- (Nur für die Erkennung von Citrix Presentation Server) Ermitteln Sie den Symbolpfad für den Einstiegspunkt:
  1. Navigieren Sie in der Citrix Access Management Console zu **Präsentationsserver** > **Anwendungen**.
  2. Suchen Sie den Ordner „Icon Path“ in der Navigationsstruktur.
  3. Klicken Sie mit der rechten Maustaste auf den Ordner „Icon Path“, und klicken Sie auf **Pfad kopieren**.
- (Nur für die Erkennung von Citrix XenApp Server) Ermitteln Sie den Symbolpfad für den Einstiegspunkt, indem Sie das Attribut „Distinguished Name“ für den Symbolpfad überprüfen.

Erforderliche Rolle: service_mapping_admin

Prozedur

1. Erstellen Sie eine Serviceinstanz.
   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**.
   b. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.

c. Geben Sie im Feld **Name** einen beschreibenden Namen für die Serviceinstanz ein.

2. Definieren Sie den Einstiegspunkt für diesen für Service:

a. Wählen Sie die Kachel **Citrix XenApp** aus.

b. Definieren Sie die Einstiegspunktattribute.

Attribut	Beschreibung
Host	Die URL der Citrix XenApp bzw. des Presentation Server. Die URL muss eine VIP-IP oder einen physischen Host enthalten.
Port	Der Port, den die Citrix XenApp oder der Presentation Server auf dem Host verwendet
Pfad für Symbol	Der Pfad zum logischen Anwendungsspeicherort, wie er in der Citrix Access Management-Konsole angezeigt wird. Der Pfad muss mit dem Application-Ordner beginnen. Beispiel: /Application/Jane/Windows Media Player.
URL	Die URL muss eine VIP-IP oder einen physischen Host enthalten. Beispiel: http://<host>/Citrix/StoreWeb.

c. Klicken Sie auf **Hinzufügen**.

d. Klicken Sie auf **Speichern**.

3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.

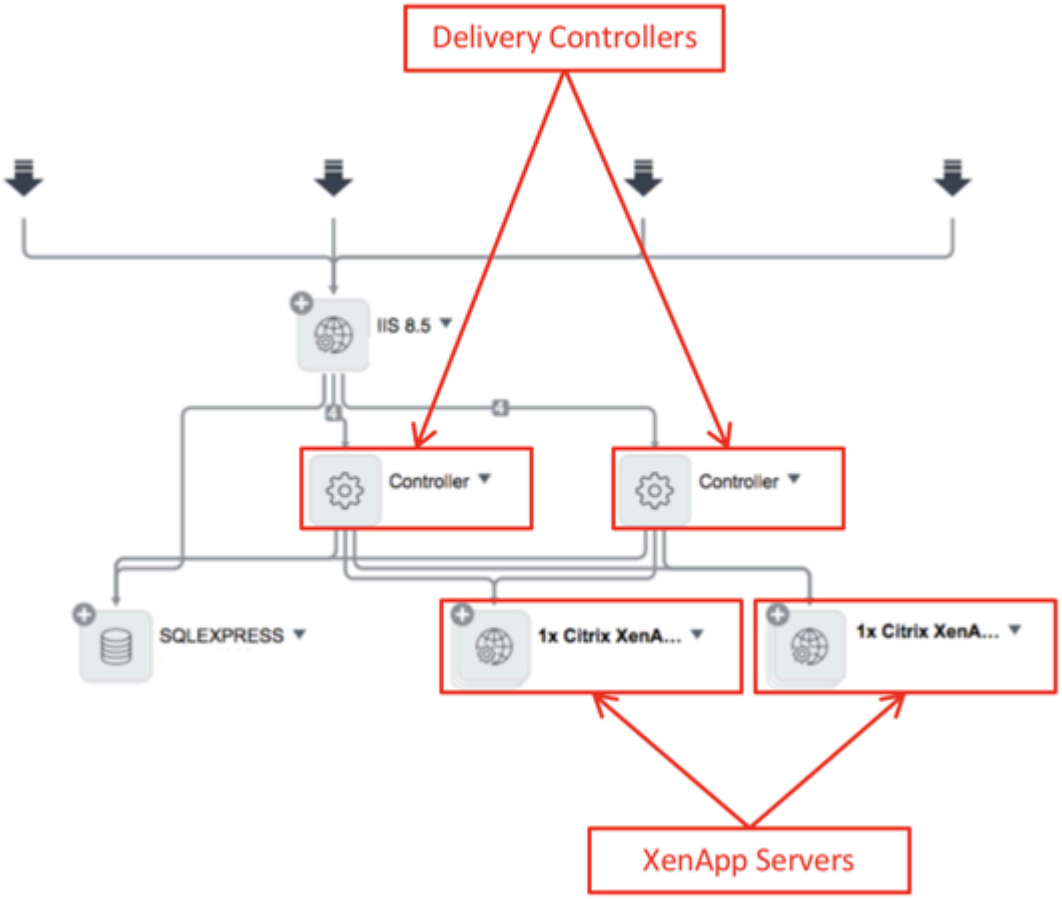
4. Klicken Sie auf **Aktualisieren**.

5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:

a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist. Es kann einige Minuten dauern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Überprüfen Sie die Anwendungsservicezuordnung, und stellen Sie sicher, dass sie dem folgenden Beispiel ähnelt.



Trouble?

Wenn das Zuordnungsergebnis nicht Ihren Erwartungen entspricht, führen Sie eine grundlegende Fehlerbehebung durch.

Symptom	Ursache	Lösung
Erkennung fehlgeschlagen. Das Erkennungsprotokoll zeigt eine Nachricht an, die mit dem folgenden Text beginnt: Sie haben keine ausreichenden Berechtigungen.	Die Anzeigeabschnitte des Musters schlagen fehl, da der Benutzer keine Berechtigungen zum Ausführen von PowerShell-Befehlen hat.	Stellen Sie sicher, dass Sie einem Benutzer Berechtigungen zum Ausführen von PowerShell-Befehlen auf Servern mit Citrix XenApp, Presentation Server oder Citrix Usage Collector bereitgestellt haben.
Erkennung fehlgeschlagen. Das Erkennungsprotokoll zeigt eine Fehlermeldung an, die den folgenden Text enthält:	Der MID-Server kann PowerShell-Befehle nicht remote ausführen, da die Ausführungsrichtlinie auf den Zielservern auf RemoteSigned festgelegt ist.	Verwenden Sie den Befehl `set-executionpolicy remotesigned` auf den Zielservern, damit MID-Server PowerShell-Befehle erfolgreich auszuführen kann.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
CategoryInfo : NotSpecified: (:) [], PSSecurityException + FullyQualifiedErrorId : RuntimeException		
Erkennung fehlgeschlagen. Das Erkennungsprotokoll zeigt eine Fehlermeldung an, die den folgenden Text enthält: Import-XAFarm: Das PowerShell-Snapin für allgemeine Citrix-Befehle ist nicht installiert.	Der Zielhost verfügt nicht über diese PowerShell-Bibliothek: PowerShell-Snapin für allgemeine Citrix-Befehle.	Laden Sie das PowerShell-SDK für Citrix XenApp herunter, und installieren Sie es auf allen Servern, auf denen Citrix XenApp, Presentation Server oder Citrix Usage Collector gehostet wird.
Die Anwendungsservicezuordnung enthält den Citrix Delivery Controller, jedoch nicht Citrix XenApp, Citrix Presentation Server oder Citrix Usage Collector.	Der von Ihnen definierte Symbolpfad ist falsch.	Überprüfen Sie den Symbolpfad und geben Sie ihn in den Einstiegspunktattributen für den Anwendungsservice erneut ein.

Zuordnung von Anwendungsservices, die Microsoft Exchange Server enthalten

Service-Mapping kann Service Instanzs mit einem Microsoft Exchange -Server und den Exchange Server-Komponenten erkennen.

Erkannte Komponenten

Wenn E-Mail-Services in Ihrer Organisation Microsoft Exchange Server bereitstellen, umfasst der erkannte Anwendungsservice die folgenden Komponenten:

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
MicrosoftMicrosoft Azure Event Hubs Azure Active Directory Domain Services	Windows	13, 30, 31, 44, 47, 52, 56, 69	WMI WinRM	Von oben nach unten	Active Directory Servicemuster
MicrosoftMicrosoft Azure Event Hubs Server (als Microsoft Exchange Komponente)	Windows	2003, 2007, 2010, 2013, 2016	WMI WinRM	Horizontal und von oben nach unten	ExchangeFrontEndServer auf Windows; PatternExchangeBackEndServ auf Windows-Muster
HUB-Transport-Server (als Microsoft	Windows	2003, 2007, 2010, 2013, 2016	WMI	Horizontal und von	Hub-Transport-Server auf

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Exchange Komponente)			WinRM	oben nach unten	Windows-Muster
Clientzugriffsserver (CAS) (als eine Microsoft Exchange-Komponente)	Windows	2003, 2007, 2010, 2013, 2016	WMI WinRM	Horizontal und von oben nach unten	CAS auf Windows-Muster

Normalerweise möchten Sie keine mit dem Exchange Server verbundenen Outlook-Clients erkennen, um Störungen zu vermeiden. Ist dies der Fall, deaktivieren Sie die datenverkehrsbasierte Erkennung für diesen Anwendungsservice.

Informationen zum Erkennung-Flow finden Sie unter „Musterbasierte Erkennung“ in Service-Mapping. Wenn Benutzer nicht mit den erforderlichen Berechtigungen versehen werden, führt Service-Mapping möglicherweise eine datenverkehrsbasierte Erkennung durch.

Einschränkungen

Discovery und Service-Mapping können Exchange Server nicht erkennen, wenn seine Konfiguration keine öffentlichen Ordner, Edge-Transporte und öffentliches Messaging unterstützt. Erstellen Sie ein Muster, oder passen Sie das vorhandene Muster an, um Exchange Server mit einer solchen Konfiguration zu erkennen.

Anwendungsservices zuordnen, die Microsoft Exchange-Server enthalten

Ordnen Sie einen Anwendungsservice zu, der einen Microsoft Exchange-Server enthält, und vergewissern Sie sich, dass Service-Mapping alle Serverkomponenten von Microsoft Exchange richtig erkannt hat.

Vorbereitungen

- Konfigurieren Sie auf der Now Platform einen Domänenbenutzer für den Zugriff auf das Windows-Betriebssystem wie in Windows-Anmeldeinformationen beschrieben. Verwenden Sie als Windows-Anmeldeinformationen Anwendername und Passwort des Microsoft Exchange Server-Administrators. Zum Beispiel Anwendername: local \administrator und Passwort: Are1300.

  Hinweis: Wenn Sie Windows-Anmeldeinformationen für einen anderen Benutzer als den Microsoft Exchange Server-Administrator konfigurieren, verwendet Service-Mapping die Traffic-basierte Discovery, die zur Zuordnung aller Microsoft Exchange-Clients führt.

- (Für Exchange CAS 2010 und 2013, 2016) Konfigurieren Sie auf der Now Platform Applicative-Anmeldeinformationen , indem Sie den CI-Typ auf „Exchange-Postfach“ einstellen.

  Warnung: Verwechseln Sie den CI-Typ der Exchange Mailbox nicht mit dem CI-Typ des Exchange Mailbox-Servers.

  Service-Mapping verwendet diese Applicative-Anmeldeinformationen für den Zugriff auf den Ordner „of/Servers/Servers.slab“ im Admin Center (EAC) Key Exchange. Service-Mapping verwendet auch die Applicative-Anmeldeinformationen, um die folgenden PowerShell-Befehle für MID Serversauszuführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Get-ExchangeServer
- Get-ExchangeServer
- Get-Mailboxserver
- Get-ClusteredMailBoxServerStatus
- Get-ExchangeServer
- Get-StorageGroup
- Get-MailboxDatabase

- (Für Microsoft Exchange CAS 2010 und 2016) Installieren Sie das Microsoft.Exchange.Management.PowerShell.E2010-Modul auf dem Windows Server, der Microsoft Exchange-CAS hostet.
- (Für Microsoft Exchange CAS 2007) Installieren Sie das Microsoft.Exchange.Management.PowerShell.Admin-Modul auf dem Windows Server, der Microsoft Exchange-CAS hostet.
- (Für Microsoft Exchange CAS 2007, 2010) Laden Sie das rctrlx-Tool zum Ausführen von PowerShell-Befehlen auf Now Platform hoch, wie in Datei rctrlx.exe auf MID Servers hochladen beschrieben.
- (Für Microsoft Exchange CAS 2007 und 2010) Statten Sie einen Exchange Mailbox-Betriebssystem-Benutzer mit den Rechten zum Ausführen von Exchange-Services unter Windows und der Berechtigung zum Abfragen des Exchange-Repositorys aus:

  Konfigurieren Sie auf der Now Platform die Windows-Anmeldeinformationen , indem Sie das Attribut *Credential alias* auf [cmdb_ci_exchange_mailbox] einstellen. Wenn Sie dieses Attribut konfigurieren, können Sie die Anmeldeinformationen für dieses CI später in Mustern verwenden.

- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
- Vergewissern Sie sich, dass Sie den Einstiegspunkt kennen, der zum Erkennen des Microsoft Exchange-Servers erforderlich ist. Verwenden Sie die URL für den Outlook-Webzugriff im folgenden Format:

  `http(s)://<hostname>:<port>/owa`

  Zum Beispiel `http(s)://myhost:<443>/owa`

Erforderliche Rolle: service_mapping_admin

Prozedur

1. Erstellen Sie eine Serviceinstanz.

   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**.

   b. Klicken Sie auf **Neu**.
   Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.

   c. Geben Sie im Feld **Name** einen beschreibenden Namen für die Serviceinstanz ein.

2. Definieren Sie den Einstiegspunkt für diesen für Service:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie die Kachel **Webanwendung** aus.
Die Option **Erkennbar durch Service Mapping** ist standardmäßig ausgewählt.

b. Geben Sie im Feld **URL** die URL des Outlook-Webzugriffs ein.
Beispiel: http(s)://myhost:<443>/owa.

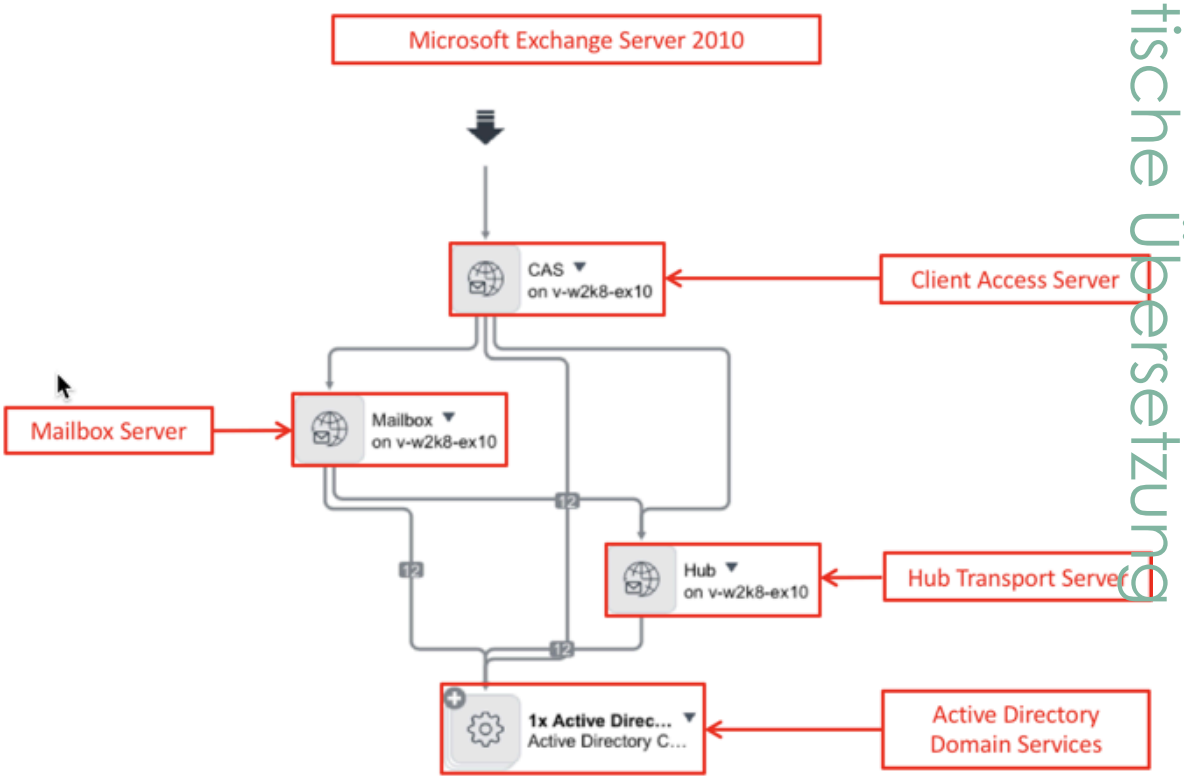
c. Klicken Sie auf **Hinzufügen**.

d. Klicken Sie auf **Speichern**.

3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:

a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist.
Es kann einige Minuten dauern.

b. Überprüfen Sie die Anwendungsservice-Zuordnung, und stellen Sie sicher, dass das Servicelayout wie in den Beispielen unten aussieht.



Trouble?

Wenn das Zuordnungsergebnis nicht Ihren Erwartungen entspricht, führen Sie eine grundlegende Fehlerbehebung durch.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
Erkennung fehlgeschlagen. Das Erkennungsprotokoll zeigt eine Nachricht an, die mit dem folgenden Text beginnt: Sie müssen das PowerShell-Snapin für allgemeine Exchange-Befehle installiert haben, um dieses Skript zu verwenden.	Die Anzeigeabschnitte des Musters schlagen fehl, da der Benutzer keine Berechtigungen zum Ausführen von PowerShell-Befehlen hat.	Stellen Sie sicher, dass Sie einem Benutzer Berechtigungen zum Ausführen von PowerShell-Befehlen auf Servern bereitgestellt haben, die Serverkomponenten von Microsoft Exchange wie CAS hosten.
Erkennung fehlgeschlagen. Das Erkennungsprotokoll zeigt eine Fehlermeldung an, die mit dem folgenden Text beginnt: [servername.destination.com] Die Verbindung zum Remote-Server ist mit der folgenden Fehlermeldung fehlgeschlagen: Der WinRM-Client kann die Anforderung nicht verarbeiten. Der vom Client angeforderte Authentifizierungsmechanismus wird vom Server nicht unterstützt, oder der unverschlüsselte Datenverkehr ist in der Servicekonfiguration deaktiviert. Überprüfen Sie die Einstellung für unverschlüsselten Datenverkehr in der Servicekonfiguration, oder geben Sie einen der vom Server unterstützten Authentifizierungsmechanismen an.	Die Anzeigeabschnitte des Musters schlagen fehl, da der MID-Server auf der zu erkennenden Komponente nicht als vertrauenswürdiger Host konfiguriert ist.	Fügen Sie den MID Server der Liste der vertrauenswürdigen Hosts auf allen Hosts hinzu, die Sie erkennen möchten.
Die Anwendungsservice-Zuordnung ist sehr groß, da sie Verbindungen zu allen Outlook-Clients enthält.	(In Bereitstellungen mit Microsoft Exchange Server 2007, 2010 oder 2013) Service-Mapping hat Verbindungen mithilfe einer datenverkehrsbasierten Erkennung erstellt, die alle offenen Verbindungen verfolgt, anstatt PowerShell-Befehle zu verwenden.	Stellen Sie sicher, dass Sie einem Benutzer Berechtigungen zum Ausführen von PowerShell-Befehlen auf Servern bereitgestellt haben, die Serverkomponenten von Microsoft Exchange wie CAS hosten.

Tibco BusinessWorks- und EMS-Erkennung

Discovery kann Tibco ActiveMatrix BusinessWorks und Enterprise Message Service (EMS) erkennen. Service-Mapping kann Anwendungsservices erkennen, die Tibco BusinessWorks, Enterprise Message Service (EMS) und die zugehörigen Komponenten enthalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery für Tibco ActiveMatrix BusinessWorks gesammelte Daten

Die folgenden Daten werden in der ActiveMatrix Business Works-Tabelle `[cmdb_ci_appl_tibco_matrix]` gesammelt.

Tabelle und Feld	Beschreibung
ActiveMatrix Business Works [cmdb_ci_appl_tibco_matrix]	
Name [name]	Die Attribute des ActiveMatrix BusinessWorks-Konfigurationselements
Version [version]	
TCP-Port(s) [tcp_port]	
Klasse [sys_class_name]	
Vollständig qualifizierter Domänenname [fqdn]	
IP-Adresse [ip_address]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Installationsverzeichnis [install_directory]	
Projekt [project]	

Von Discovery für Tibco Enterprise Message Service gesammelte Daten

In der Standardeinstellung verwendet Discovery das Muster *`Enterprise Message Service`*, um Tibco Enterprise Message Service zu erkennen.

Eine Liste der privilegierten Befehle, die Sie für Discovery und Service Mapping benötigen, finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern - dort finden Sie auch eine Liste der Befehle, für die erhöhte Rechte zum Erkennen und Zuordnen von Unix-basierten Hosts in Ihrer Organisation erforderlich sind.

Hinweis: Weitere Informationen zur Migration von Probe zu Muster finden Sie im Wissensartikel KB0694477 .

Tabelle und Feld	Feldname
Tibco Enterprise Message Services [cmdb_ci_appl_tibco_message]	
Name [name]	Attribute des Konfigurationselements Tibco Enterprise Message Services.
Version [version]	
Klasse [sys_class_name]	
Vollständig qualifizierter Domänenname [fqdn]	
IP-Adresse [ip_address]	
Installationsverzeichnis [install_directory]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Feldname
TCP-Port(s) [tcp_port]	
Konfigurationsverzeichnis [config_directory]	
Konfigurationsdatei [config_file]	
Installationsverzeichnis [install_directory]	

Durch Service-Mapping erfasste Daten

Service-Mapping kann Anwendungsservice erkennen, die Tibco ActiveMatrix BusinessWorks (einschließlich BusinessWorks Process), Tibco Enterprise Message Service (EMS) und die Tibco Enterprise Message Service- (EMS-)Warteschlange enthalten.

Anwendungsservices zuordnen, die Tibco BusinessWorks und EMS enthalten

Ordnen Sie einen Anwendungsservice zu, der Tibco BusinessWorks und Enterprise Message Service (EMS) enthält, und vergewissern Sie sich, dass von Service-Mapping alle Tibco-Komponenten korrekt erkannt wurden.

Vorbereitungen

- (Beim Hosting auf Unix) Konfigurieren Sie die Applicative-Anmeldeinformationen für Tibco EMS.
- (Beim Hosting auf einem Windows-Server) Konfigurieren Sie auf der Now Platform Windows-Anmeldeinformationen .
- (Beim Hosting auf einem Unix-Server) Konfigurieren Sie auf der Now Platform SSH-Anmeldeinformationen .
- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

Erforderliche Rolle: service_mapping_admin

Prozedur

1. Erstellen Sie eine Serviceinstanz.
   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**.
   b. Klicken Sie auf **Neu**.
      Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.
   c. Geben Sie im Feld **Name** einen beschreibenden Namen für die Serviceinstanz ein.
2. Definieren Sie den Einstiegspunkt für diesen Anwendungsservice:
   a. Wählen Sie die Kachel **Sonstige Anwendung**.
      Die Option **Erkennbar durch Service Mapping** ist standardmäßig ausgewählt.
   b. Wählen Sie in der Liste „Eingangspunkttyp auswählen“ den Eintrag `HTTP(s)-Endpunkt, TCP-Endpunkt, Tibco BW-Endpunkt` aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Definieren Sie den Einstiegspunkt wie folgt:

- Die URL des Prozesses, der dem Tibco BusinessWorks-Projekt entspricht, z. B. `http://10.xx.xx.xx:6710/GetMemberActivitiy/Processes/ServiceGetMemberActivitiy.service` .
- (Optional) Der Hostname, auf dem das BusinessWorks-Projekt als Service ausgeführt wird.

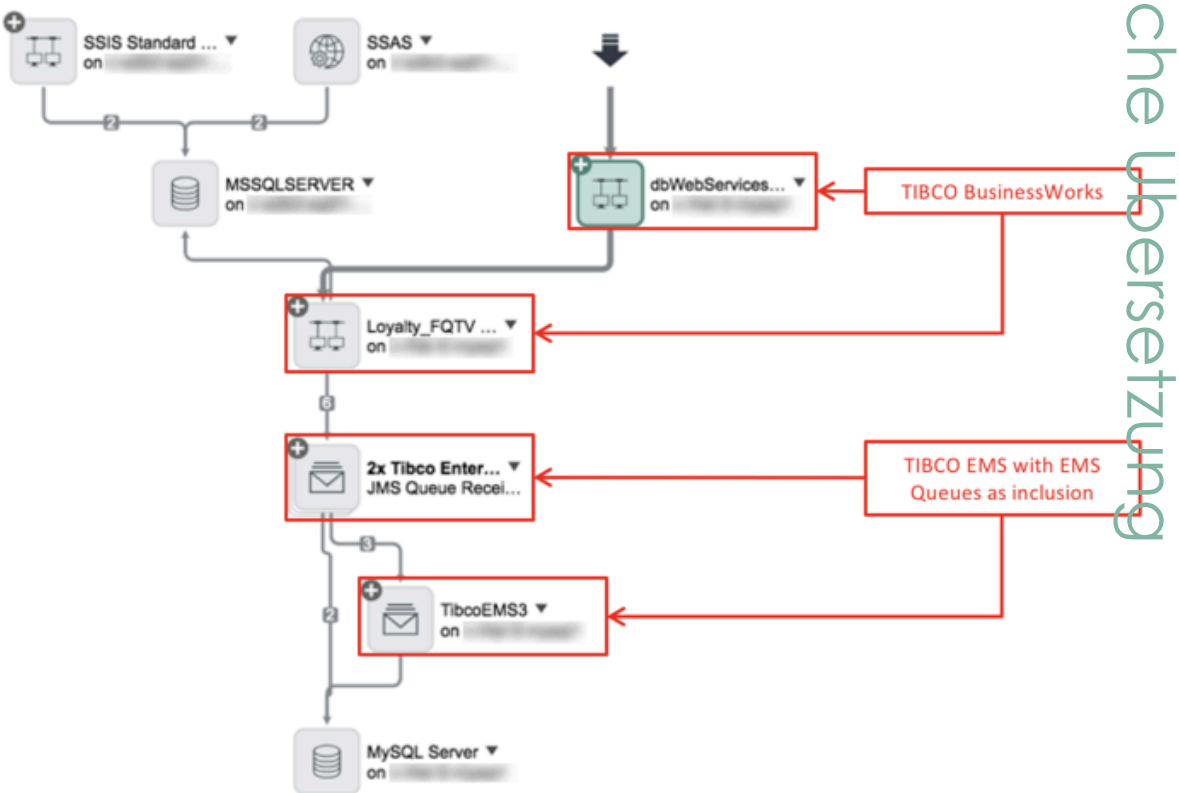
d. Klicken Sie auf **Hinzufügen**.

e. Klicken Sie auf **Speichern**.

3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:

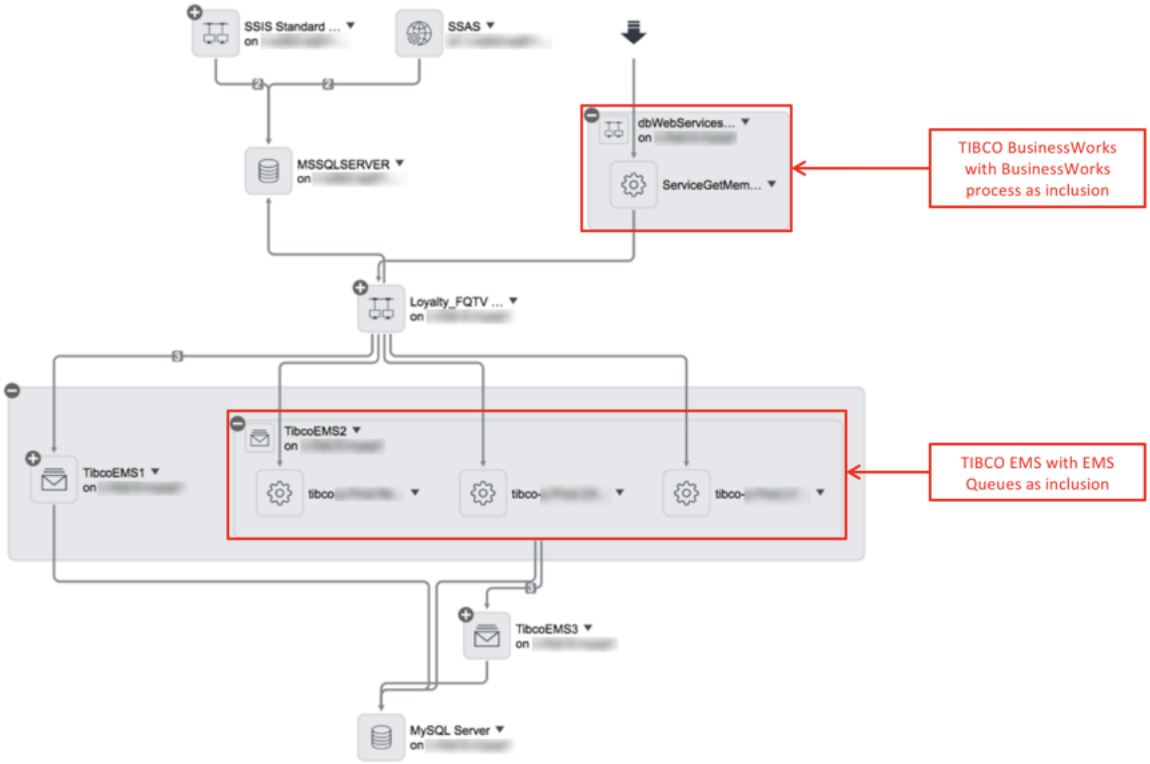
a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist. Es kann einige Minuten dauern.

b. Überprüfen Sie die Zuordnung des Anwendungsservice, und stellen Sie sicher, dass das Servicelayout wie in den folgenden Beispielen aussieht.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie außerdem sicher, dass die BusinessWorks-CIs mit eingeschlossen sind und jedes der Elemente jeweils einen BusinesWorks-Prozess enthält. Stellen Sie außerdem sicher, dass die EMS-CIs eingeschlossen sind und EMS-Warteschlangen enthalten.



Trouble?

Wenn das Zuordnungsergebnis nicht Ihren Erwartungen entspricht, führen Sie eine grundlegende Fehlerbehebung durch.

Symptom	Ursache	Lösung
(Nur für Bereitstellungen, bei denen BusinessWorks auf einem Unix-Server gehostet wird) Die für Service-Zuordnung zeigt das BusinessWorks-CI ohne Einbeziehung des BusinessWorks-Prozesses. Das Erkennungsprotokoll zeigt die Fehlermeldung an, dass der Benutzer nicht über ausreichende Anmeldeinformationen verfügt.	Service-Mapping konnte den Befehl `TibcoFilesParser.ksh` nicht ausführen.	Stellen Sie sicher, dass Sie einem Benutzer erhöhte Rechte gewährt haben, wie in Service-Mapping-Befehle, die keinen privilegierten Benutzer erfordern beschrieben.
Service-Mapping konnte die ausgehenden Verbindungen von EMS zum EMS-Prozess nicht erkennen.	Service-Mapping konnte den Befehl `tibemsadmin` nicht ausführen.	Stellen Sie sicher, dass Sie einem Benutzer erhöhte Rechte gewährt haben, wie in Service-Mapping-Befehle, die keinen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
		privilegierten Benutzer erfordern beschrieben.

Anwendungsservices zuordnen, die Oracle GlassFish-Server enthalten

Service-Mapping kann Anwendungsservices erkennen, die Oracle GlassFish-Server enthalten.

Erkannte Komponenten

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Oracle GlassFish Server	Windows UNIX	3.1, 4.0, 4.1	WMI WinRM SSH	Horizontal und von oben nach unten	GlassFish Server
Oracle GlassFish WAR-Datei	Windows UNIX	3.1, 4.0, 4.1	WMI WinRM SSH	Horizontal und von oben nach unten	GlassFish WAR

Anwendungsservices zuordnen, die Oracle GlassFish-Server enthalten

Ordnen Sie einen für Service, der Oracle GlassFish-Server enthält, korrekt zu.

Vorbereitungen

- (Beim Hosting auf einem Windows-Server) Konfigurieren Sie in der Now Platform Windows-Anmeldeinformationen .
- (Beim Hosting auf einem Linux- oder UNIX-Server) (Optional) Konfigurieren Sie in der Now Platform SSH-Anmeldeinformationen .
- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .

Erforderliche Rolle: service_mapping_admin

Prozedur

1. Erstellen Sie eine Serviceinstanz.

   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**.

   b. Klicken Sie auf **Neu**.
   Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.

   c. Geben Sie im Feld **Name** einen beschreibenden Namen für die Serviceinstanz ein.

2. Definieren Sie den Einstiegspunkt für diesen Anwendungsservice:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie die Kachel **Sonstige Anwendung**.
Die Option **Erkennbar durch Service Mapping** ist standardmäßig ausgewählt.

b. Definieren Sie den Einstiegspunkt, indem Sie die Felder ausfüllen.

Feld	Beschreibung
Typ des Einstiegspunkts auswählen	Einstiegspunkttyp: ▪ HTTP(S)-Endpunkt ▪ TCP-Endpunkt ▪ TIBCO BW-Endpunkt
URL	Die URL des Prozesses, die mit dem GlassFish-Server korreliert, z. B. `http://10.196.xx.xx:28080/hello/`. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **HTTP(S)-Endpunkt** ausgewählt ist.
Host	Der Server, der den GlassFish-Server hostet. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **Tibco BW-Endpunkt** oder **TCP-Endpunkt** ausgewählt ist.
Host-Name	Der Hostname des Servers, der den GlassFish-Server hostet. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **HTTP(S)-Endpunkt** ausgewählt ist.
Port	Der Port, den der mit dem GlassFish-Server korrelierende Prozess verwendet. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **Tibco BW-Endpunkt** oder **TCP-Endpunkt** ausgewählt ist.
Prozessname	Der Name des Prozesses, der mit dem GlassFish-Server korreliert. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **Tibco BW-Endpunkt** ausgewählt ist.
Kommentare	Freitextkommentar, um Informationen zum Endpunkt bereitzustellen. Dieses Feld wird angezeigt, wenn in **Einstiegspunkttyp auswählen** die Option **HTTP(S)-Endpunkt** oder **TCP-Endpunkt** ausgewählt ist.

c. Klicken Sie auf **Hinzufügen**.

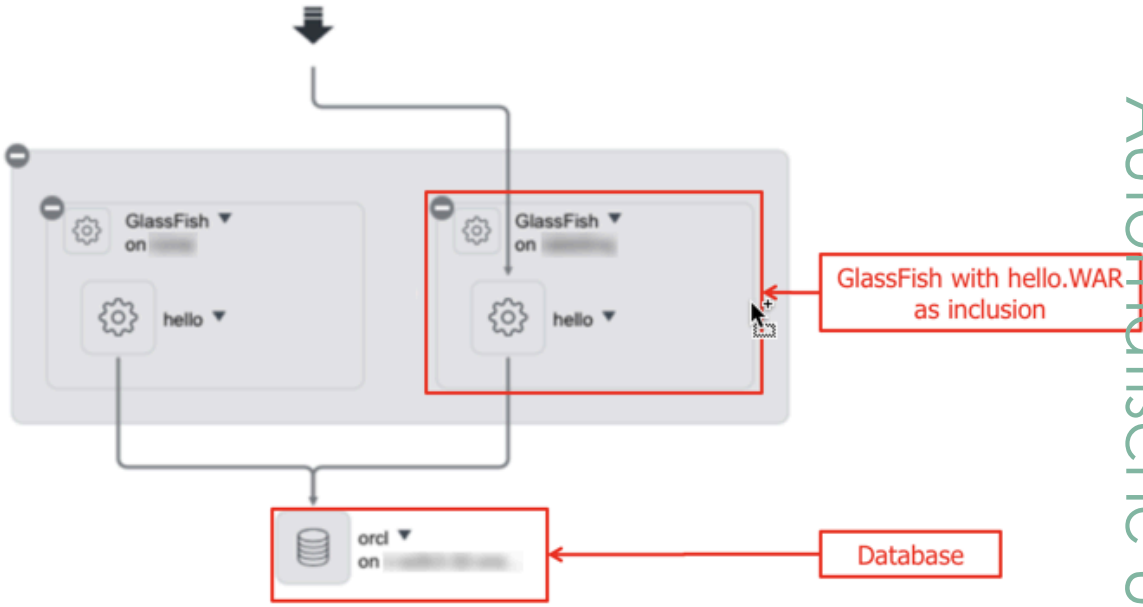
d. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:

   a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist. Es kann einige Minuten dauern.

   b. Überprüfen Sie die Zuordnung des Anwendungsservices, und stellen Sie sicher, dass das Servicelayout wie im folgenden Beispiel aussieht.



Stellen Sie außerdem sicher, dass die GlassFish-Server-CIs eingeschlossen sind und jedes von ihnen eine WAR-Datei enthält.

Trouble?

Wenn das Zuordnungsergebnis nicht Ihren Erwartungen entspricht, führen Sie eine grundlegende Fehlerbehebung durch.

Symptom	Ursache	Lösung
Service-Mapping kann das GlassFish-Server-CI nicht erkennen. Das Erkennungsprotokoll zeigt die folgende Meldung an: Der Prozess wird nicht ausgeführt, oder der Port ist nicht korrekt. Das CI wurde nicht erkannt, da auf dem Host 10.196.xx.xx keine Anwendung auf Port 28080 ausgeführt wird. Stellen Sie sicher, dass die Anwendung ausgeführt wird,	Auf dem Port, der Teil des Einstiegspunkts ist, wird kein Prozess ausgeführt.	1. Stellen Sie sicher, dass der Einstiegspunkt korrekt ist. 2. Wenn der Einstiegspunkt korrekt ist, überprüfen Sie, ob hier ein Prozess für den Port ausgeführt wird, indem Sie eine schnelle Erkennung auf dem Host ausführen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
und führen Sie eine schnelle Erkennung auf dem Host aus.		

Anwendungsservices zuordnen, die Oracle Tuxedo-Plattform enthalten

Service-Mapping kann Anwendungsservices erkennen, die die Oracle Tuxedo-Plattform und die zugehörigen Komponenten enthalten.

Erkannte Komponenten

Name	Plattform	Version	Protokoll	Discovery-Typ	Muster (oder Sonde, falls angezeigt)
Oracle Tuxedo	Windows UNIX	10.x, 11.x, 12.x	WMI WinRM SSH	Horizontal und von oben nach unten	Tuxedo
Oracle Tuxedo-Portal	Windows UNIX	10.x, 11.x, 12.x	WMI WinRM SSH	Horizontal und von oben nach unten	Tuxedo Portal - Muster

Anwendungsservices zuordnen, die Oracle Tuxedo-Plattform enthalten

Ordnen Sie einen Anwendungsservice zu, der eine Oracle Tuxedo-Plattform enthält, und vergewissern Sie sich, dass Service-Mapping alle Tuxedo-Komponenten richtig erkannt hat.

Vorbereitungen

- Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen .
- (Optional) Informationen zum Verwenden des WinRM-Protokolls finden Sie unter Vertrauenswürdige WinRM-Hosts auf dem MID-Server konfigurieren .
- (Wenn auf Unix gehostet wird) Geben Sie einem Benutzer die erweiterten Rechte zum Ausführen von Befehlen, die in Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern beschrieben werden.

Erforderliche Rolle: service_mapping_admin

Prozedur

1. Erstellen Sie eine Serviceinstanz.

   a. Navigieren zu **Alle** > **Service-Mapping** > **Serviceinstanzen**.

   b. Klicken Sie auf **Neu**.
   Die Option **Erkennbar von Service-Mapping** ist standardmäßig ausgewählt.

   c. Geben Sie im Feld **Name** einen beschreibenden Namen für die Serviceinstanz ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Definieren Sie den Einstiegspunkt für diesen Anwendungsservice:

   a. Wählen Sie die Kachel **Sonstige Anwendung**.

   b. Wählen Sie `TCP-Endpunkt` aus der Liste aus.

   c. Definieren Sie den Einstiegspunkt wie folgt:
      - Ein Host des Servers, der den Tuxedo-Prozess hostet.
      - Ein Port auf diesem Server, der vom Tuxedo-Prozess geöffnet wird.

   d. Klicken Sie auf **Hinzufügen**.

   e. Klicken Sie auf **Speichern**.

3. Klicken Sie links auf **Zusätzliche Informationen**, und deaktivieren Sie das Kontrollkästchen **Datenverkehrsbasierte Erkennung**.
4. Klicken Sie auf **Aktualisieren**.
5. Stellen Sie sicher, dass das Zuordnungsergebnis zufriedenstellend ist:

   a. Klicken Sie auf **Karte anzeigen**, und warten Sie, bis die Zuordnung abgeschlossen ist. Es kann einige Minuten dauern.

   b. Überprüfen Sie die Zuordnung des Anwendungsservices.

Trouble?

Wenn das Zuordnungsergebnis nicht Ihren Erwartungen entspricht, führen Sie eine grundlegende Fehlerbehebung durch.

Symptom	Ursache	Lösung
Service-Mapping kann das Tuxedo-CI nicht erkennen. Das Erkennungsprotokoll zeigt die Meldung an, dass die Anmeldeinformationen für die Ausführung des Befehls nicht ausreichen, einschließlich „permissions.tmadadmin -v“.	Der angegebene Benutzer hat keine erhöhten Berechtigungen zum Ausführen dieses Befehls.	Stellen Sie sicher, dass Sie einem Benutzer die Berechtigungen zum Ausführen von Befehlen mit erhöhten Rechten gewährt haben.
Service-Mapping kann das Tuxedo-CI nicht erkennen. Das Erkennungsprotokoll zeigt die Meldung an, dass der Benutzer das Skript „tux.env“ nicht ausführen kann.	Der angegebene Benutzer ist nicht berechtigt, das Skript „tux.env“ auszuführen.	Stellen Sie sicher, dass Sie einem Benutzer die Berechtigungen zum Ausführen des Skripts „tux.env“ gewährt haben.

Tag-Definitionen für die Tag-basierte Zuordnung ändern oder aktualisieren

Sie können Tag-Definitionen ändern, die Service-Mapping für die Tag-basierte Zuordnung verwendet. Service-Mapping verwendet aktualisierte Tag-Definitionen, um neue Tag-basierte Services zu erstellen, ohne Tag-bezogene Änderungen auf zuvor zugeordnete Services anzuwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Wenn Sie eine neue Tag-Kategorie erstellen oder eine vorhandene Tag-Kategorie ändern müssen, beachten Sie die Voraussetzungen unter Ordnen Sie Anwendungsservices mithilfe von Tags zu zu klassisch Service-Mapping.

Lesen Sie die Empfehlungen in Zuordnung von Anwendungsservices basierend auf Tags vorbereiten.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

In den folgenden Fällen können Sie Tag-Kategorien einer Tag-basierten Servicefamilie hinzufügen oder daraus entfernen:

- Wenn Sie mit den Ergebnissen der tagbasierten Zuordnung nicht zufrieden sind, z. B. wenn der Service zu groß ist, da er irrelevante CIs enthält
- Wenn sich die Verwendung von Tags in Ihrer Organisation ändert, z. B. durch neue Tags.

Wenn Sie für eine tagbasierte Servicefamilie definierte Tag-Kategorien ändern oder eine tagbasierte Servicefamilie insgesamt löschen, werden alle zugeordneten Services von dieser tagbasierten Servicefamilie getrennt. Diese Services sind weiterhin vorhanden und werden von Service-Mapping weiterhin mit der ursprünglichen Tag-Definition aktualisiert. Um zu vermeiden, dass Tag-basierte Services auf veralteten Tag-Definitionen basieren, löschen Sie alle vorhandenen Tag-basierten Services.

Service-Mapping generiert neue Tag-basierte Servicekandidaten, die Sie zum Zuordnen von Services auf Grundlage der geänderten Tag-Definition verwenden.

Wichtig: Neue Services, die auf geänderten Tag-Definitionen basieren, überschreiben zuvor zugeordnete Services nicht.

Prozedur

1. Löschen Sie vorhandene tagbasierte Services:
   a. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Servicefamilien**.
   b. Wählen Sie die Tag-basierte Servicefamilie aus, für die Sie die Tag-Definition ändern möchten.
   c. Klicken Sie unter **Zugeordnete Services** auf **Zugeordnete Services löschen**, um alle Services zu löschen.
   d. Oder klicken Sie auf das Symbol **Zum Löschen markieren** neben dem entsprechenden Service in der Liste, und klicken Sie dann auf **Löschen**.
2. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Servicefamilien**.
3. Wählen Sie den Tag-basierten Service aus, für den Sie die Tag-Definition ändern möchten.
4. Führen Sie unter **Ausgewählte Tag-Kategorien** eine der folgenden Aktionen aus:
   - Fügen Sie eine neue Tag-Kategorie hinzu, indem Sie auf die leere Zeile doppelklicken und die entsprechende Tag-Kategorie aus der Liste der zuvor definierten Tag-Kategorien auswählen.
   - Entfernen Sie eine Tag-Kategorie, indem Sie neben der Kategorie auf das Symbol **Zum Löschen markieren** klicken.
   - Ändern Sie die Verwendung einer Tag-Kategorie, die bereits der Servicefamilie zugeordnet ist, indem Sie die Tag-Werte oder die Reihenfolge der Servicenamen ändern.

     Verwenden Sie für mehrere Tag-Werte Kommas als Trennzeichen. Die Servicebenennungs-Reihenfolge definiert, wie Service-Mapping den Tag-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorienamen in den Namen der Anwendungsservices verwendet, die für die Servicefamilie generiert werden.

- Ändern Sie die Tag-Kategorie selbst, indem Sie auf den Tag-Kategorienamen klicken und dann die CI-Tag-Schlüssel definieren.

5. Klicken Sie auf **Aktualisieren**.

Nächste Maßnahme

Tag-basierte Anwendungsservices neu zuordnen, um Tag-Änderungen widerzuspiegeln

Tag-basierte Anwendungsservices neu zuordnen, um Tag-Änderungen widerzuspiegeln

Erstellen Sie Tag-basierte Services neu, wenn sich die Art und Weise, wie Tags in Ihrer Organisation verwendet werden, geändert hat oder nachdem Tag-Definitionen für Tag-basierte Servicefamilien geändert wurden.

Vorbereitungen

Ändern Sie bei Bedarf Tag-Definitionen für die relevante tagbasierte Servicefamilie.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Ordnen Sie vorhandene Tag-basierte Services neu zu, nachdem Sie Tag-Definitionen manuell geändert haben. Wenn Ihre Organisation neue Tag-Schlüssel oder Tag-Werte verwendet, sollten Sie eventuell auch die vorhandenen Services neu zuordnen. In beiden Fällen aktualisiert Service-Mapping die vorhandenen Services nicht automatisch mit den Tag-Änderungen.

Prozedur

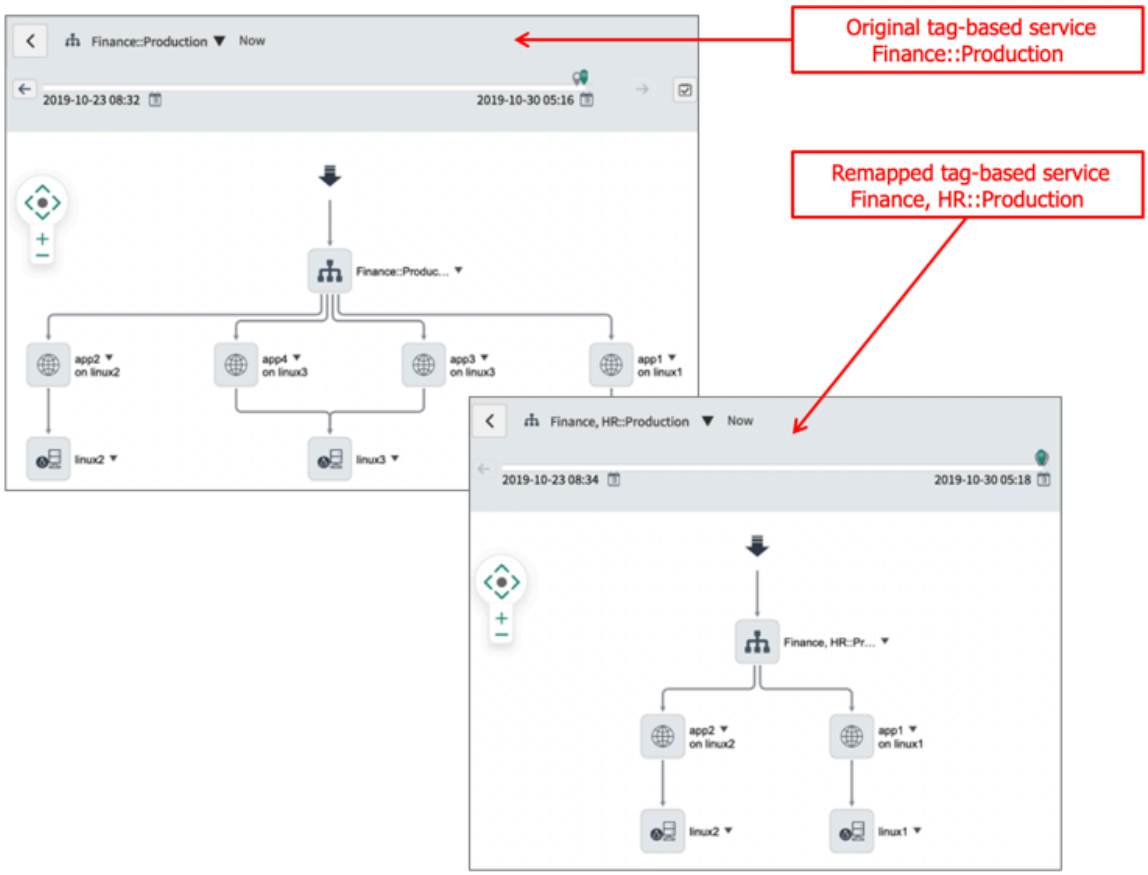
1. Navigieren zu **Service-Mapping** > **Administration** > **Tag-basierte Servicefamilien**.
2. Wählen Sie die Tag-basierte Servicefamilie aus, deren Tag-Definitionen sich geändert hat.
3. Klicken Sie unter **Zugehörige Links** auf **Kandidaten manuell aktualisieren**, um neue Servicekandidaten mit den geänderten Tag-Definitionen zu generieren.
4. Überprüfen Sie im Fenster „Servicekandidat“ die vorgeschlagenen Servicekandidaten, und wählen Sie diejenigen aus, die Sie zuordnen möchten.
   Wenn keine Servicekandidaten vorhanden sind, stellen Sie sicher, dass Sie die Tag-Werte ausgewählt haben, die in der Tabelle Schlüsselwert [cmdb_key_value] vorhanden sind.
5. Klicken Sie auf **Ausgewählte zuordnen**.
   Service-Mapping erstellt Anwendungsservices anhand der von Ihnen ausgewählten Kandidaten.
6. Überprüfen Sie die neu erstellten Services unter **Zugeordnete Services**, um sicherzustellen, dass das Ergebnis Ihren Erwartungen entspricht.
   Wenn Service-Mapping anbietet, anstatt einer Zuordnung für einen Anwendungsservice die CI-Liste anzuzeigen, ist der Service zu groß. Nehmen Sie ein Feintuning vor, wie unter Tag-Definitionen für die tagbasierte Zuordnung ändern oder aktualisieren beschrieben.

Ergebnisse

Sie haben den Anwendungsservice basierend auf den neuesten Tag-Definitionen zugeordnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neu zugeordneter Tag-basierter Anwendungsservice



Nächste Maßnahme

Stellen Sie sicher, dass die Serviceinstanzen nicht zu groß sind:

- Service-Mapping bietet nicht die Möglichkeit, die CI-Liste anstelle einer Zuordnung für eine Serviceinstanz anzuzeigen.
- Es gibt keine Discovery-Meldung, die darauf hinweist, dass die Serviceinstanz zu groß ist: *`The map does not display the entire service, because it is too large. The number of CI connections exceeded the allowed maximum.`*

Wenn der Service zu groß ist, führen Sie die folgenden Aktionen aus:

- Ändern Sie die für die Zuordnung verwendeten Tag-Definitionen, um sicherzustellen, dass Service-Mapping nur relevante CIs in der Serviceinstanz enthält.
- Bei Bedarf konfigurieren Sie die Tag-basierte Erkennung, um zu ändern, welche CIs Service-Mapping in Tag-basierte Serviceinstanzen einschließt.

Fehler bei Anwendungsservices als Massenvorgang beheben

Von Service-Mapping werden Fehler nach ihrer Ursache klassifiziert, z. B. fehlende Anmeldeinformationen oder Zeitüberschreitung bei einer Aufgabe. Für einen schnellen und effizienten Prozess beheben Sie jeweils die Fehler im Stapelverfahren, die zu derselben Kategorie gehören.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin oder admin

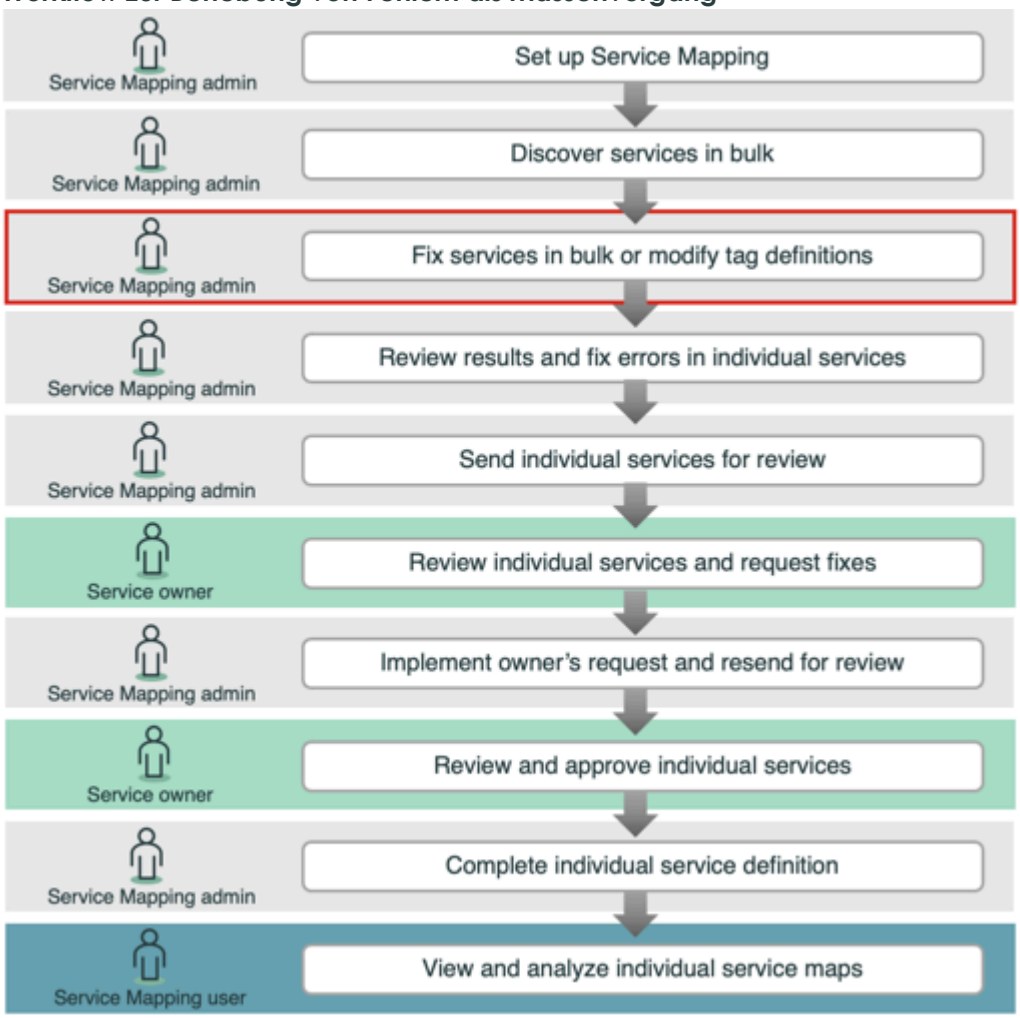
Warum und wann dieser Vorgang ausgeführt wird

Sie können Fehler nach Kategorie anzeigen, z. B. **Konfiguration**, **Netzwerk** und **Anmeldeinformationen**. Jede Kategoriespalte enthält auch einen Fehlerzähler.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Teil des Service-Mapping-Workflows können Sie, nachdem Sie Anwendungsservices als Massenvorgang zugeordnet haben, mehrere Fehler im Zusammenhang mit Anwendungsservices gleichzeitig (als Gruppe) beheben.

Workflow zur Behebung von Fehlern als Massenvorgang



Nach der ersten Zuordnung erkennt Service-Mapping Konfigurationselemente (CIs) regelmäßig neu und aktualisiert die Liste der Fehler ständig. Erkennungszeitpläne definieren, wie oft Service-Mapping den Erkennungsprozess für CIs ausführt. Service-Mapping erkennt nur CIs von Anwendungsservices mit dem Status „Betriebsbereit“.

Manche Erkennungsfehler sind eventuell keiner Kategorie zugewiesen:

- Nachdem Service-Mapping von der Version Jakarta oder älter aktualisiert wurde.
- Wenn Konfigurationselemente (CIs) vorhanden sind, denen Fehler zugeordnet sind und die zuerst aus Anwendungsservices entfernt und dann den Anwendungsservices erneut hinzugefügt wurden.

Prozedur

1. Navigieren zu **Alle** > **Service-Mapping** > **Startseite** und klicken Sie dann im Feld **Reparieren auf Servicesreparieren**.
   Die Zahl im Feld **Korrigieren** gibt die Anzahl der betroffenen Servicezuordnungen an.
   Klicken Sie auf **Aktualisieren** ( ), um die Anzeige zu aktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Um die Fehler für einen bestimmten Service zu beheben, klicken Sie auf **Fehler nach Service verwalten**.

2. Wenn nicht kategorisierte Fehler vorhanden sind, können Sie sie nach für Service kategorisieren:

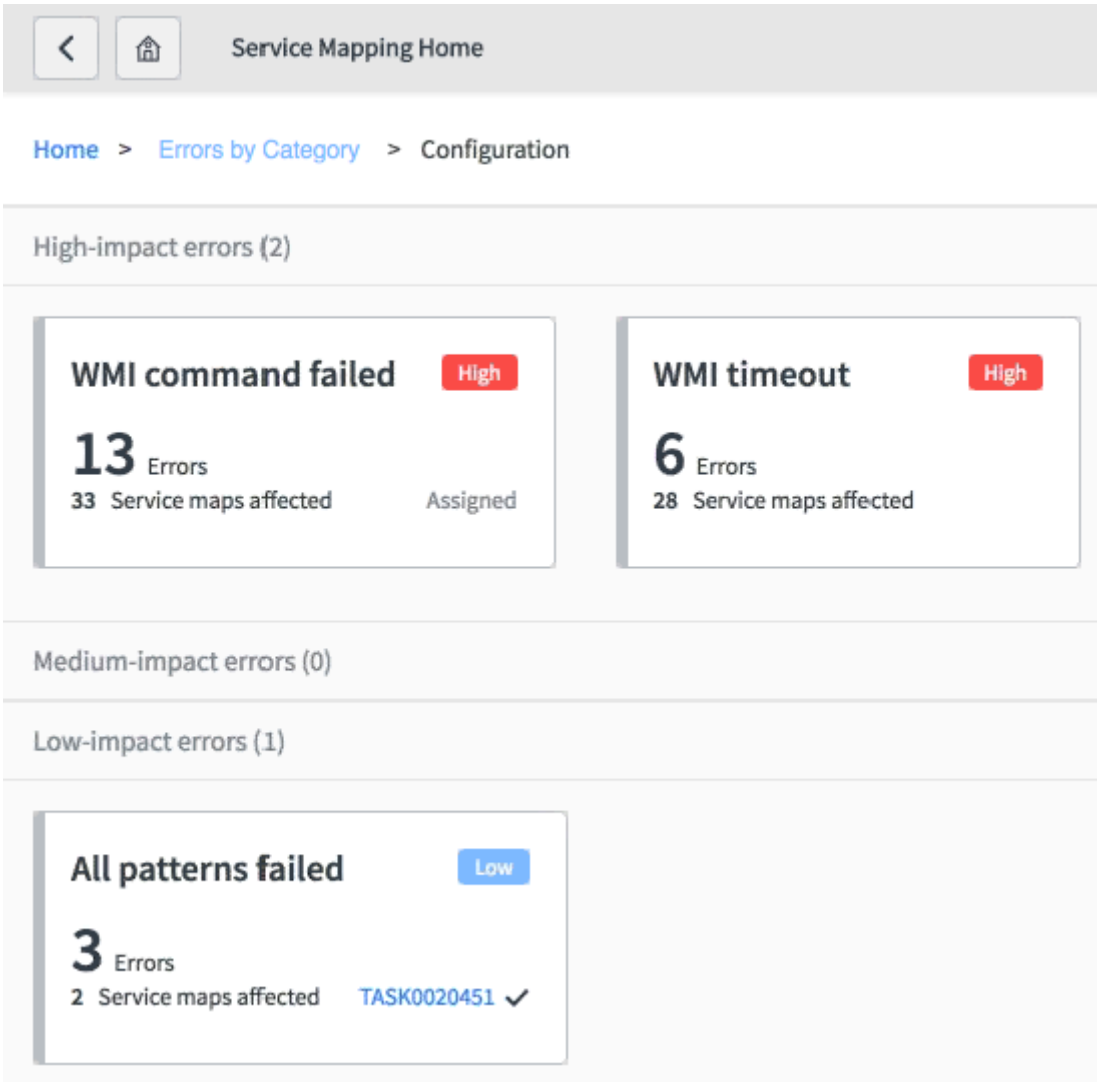
   a. Klicken Sie auf **Nicht kategorisierte Fehler nach Service anzeigen**.

   b. Klicken Sie auf den entsprechenden Servicenamen.

   c. Klicken Sie in der für Service-Zuordnung auf **Erkennung ausführen**.
   Service-Mapping erkennt alle CIs, die mit Fehlern erkannt wurden und zu diesem für Service gehören.

3. Wenn nicht kategorisierte Fehler vorhanden sind, kategorisieren Sie sie durch Klicken auf **Relevante CIs erneut erkennen** und per Klick auf **Weiter** in der Bestätigungsnachricht.
   Service-Mapping erkennt alle CIs, die mit Fehlern erkannt wurden und zu Anwendungsservices mit dem Status „Betriebsbereit“ gehören.
4. Klicken Sie in das Feld einer Fehlerkategorie.
   Im Beispiel unten sind Konfigurationsfehler ausgewählt.
   - Auf der Seite „Fehler nach Kategorie“ werden Fehler nach hohen, mittleren und geringen Auswirkungen auf die Services sortiert.
   - Für jede Auswirkungskategorie werden Fehler nach Fehlercode (möglicherweise die Ursache) in Felder gruppiert.
   - Wenn Fehleraufgaben zugewiesen wurden, werden die Aufgabennummern im Feld angezeigt. Klicken Sie auf eine Aufgabe, um Details anzuzeigen. Zeigen Sie auf eine Aufgabe, um Kommentare anzuzeigen, die die zuweisende Person möglicherweise hinzugefügt hat. Ein Häkchen zeigt an, dass eine Aufgabe abgeschlossen ist.

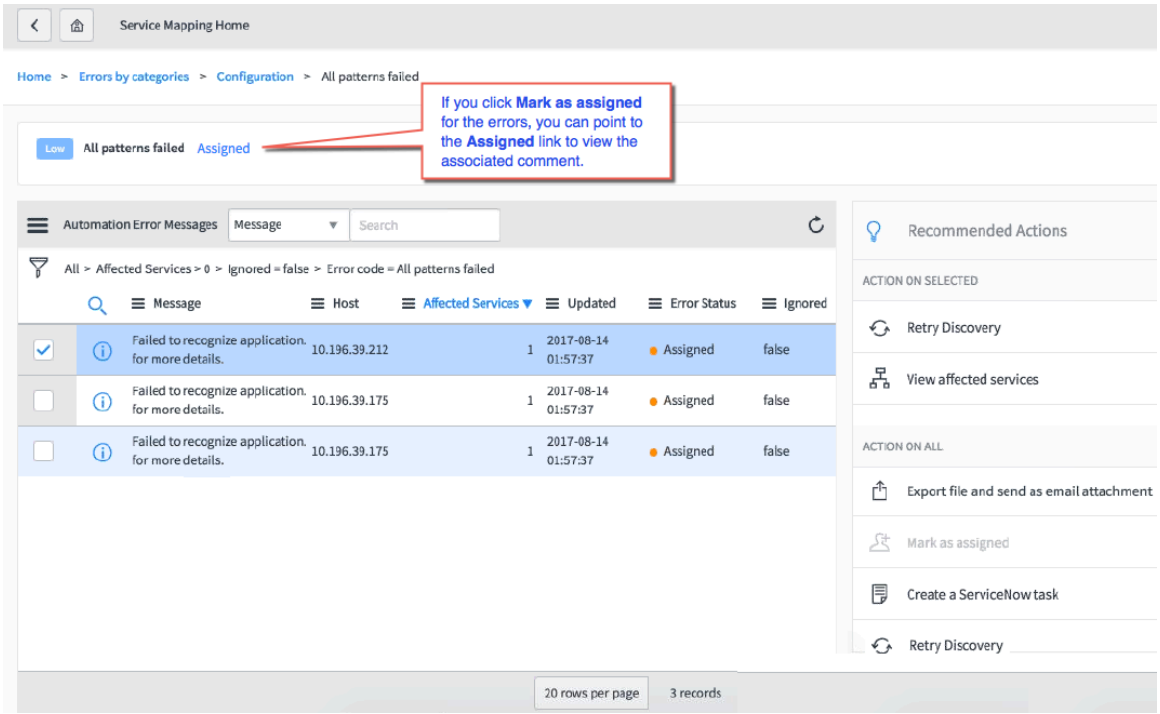
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf das Feld, um eine Liste der Fehler anzuzeigen, die denselben Fehlercode aufweisen.
   Sie können eine der **Empfohlenen Aktionen** auf ausgewählte Elemente bzw. alle Elemente in der Liste anwenden.

   Im Beispiel ist **Alle Muster fehlgeschlagen** ausgewählt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Klicken Sie auf eine Aktion im Abschnitt **Aktion auf alle**, oder wählen Sie Fehler aus, und klicken Sie auf eine Aktion im Abschnitt **Aktion auf Ausgewählte**.

   Discovery erneut starten

   Führt den kompletten Discovery-Prozess aus. Normalerweise führen Sie Discovery aus, nachdem Sie die Korrekturanweisungen befolgt haben, die angezeigt werden, wenn Sie auf **Anweisungen anzeigen** klicken.

   Betroffene Services anzeigen

   Zeigt eine Popup-Liste aller Services an, die vom ausgewählten Fehler betroffen sind. Klicken Sie in der Liste auf einen Service, um Servicedetails anzuzeigen.

   Als zugewiesen markieren

   Wenden Sie die Aktion **Als zugewiesen markieren** an, wenn Sie eine Out-of-Band-Aktion ausführen möchten, um eine Person zu benachrichtigen, die den Fehler beheben soll (normalerweise eine Person, die die ServiceNow-Instanz nicht verwendet). Sie können im Popup-Fenster **Als zugewiesen markieren** einen **Kommentar** eingeben. Klicken Sie auf **Aktualisieren**, um das **Fehlerstatus**-Feld im Fehlerdatensatz auf **Zugewiesen** zu setzen und den **Kommentar** mit dem Fehler zu verknüpfen. Zeigen Sie zum Anzeigen des Kommentars auf den Link **Zugewiesen**.

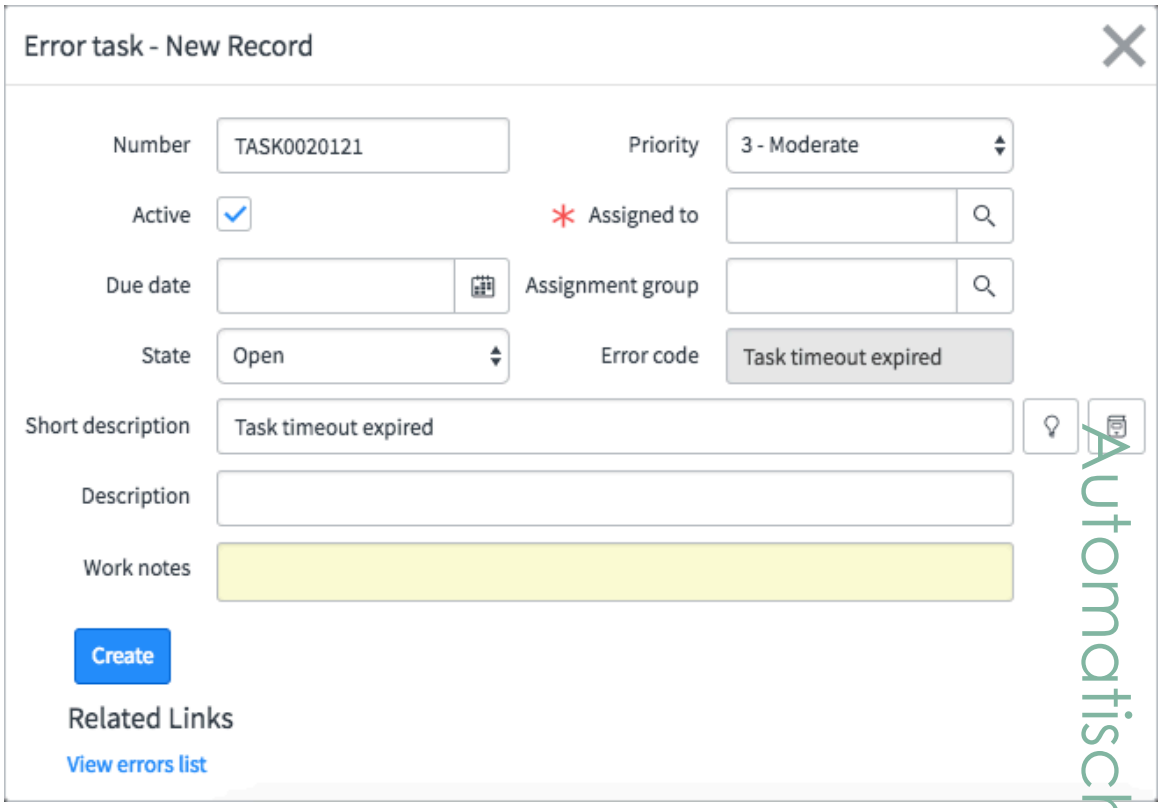
   > **Hinweis:** Die Aktion **ServiceNow-Aufgabe erstellen** setzt auch das **Fehlerstatus**-Feld im Fehlerdatensatz auf **Zugewiesen**.

   ServiceNow-Aufgabe erstellen

   Öffnet das ServiceNow-Fehleraufgabenformular in einem Popup-Fenster, in dem Sie eine Aufgabe für die ausgewählten Fehler erstellen und zuweisen können. Setzt das **Fehlerstatus**-Feld im Fehlerdatensatz auf **Zugewiesen**. Informationen zum Erstellen von Fehleraufgaben finden Sie unter Tabelle erstellen und Aufgaben aus Incidents, Problemen oder Change-Anforderungen erstellen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Aktion **Als zugewiesen markieren** setzt auch das **Fehlerstatus**-Feld im Fehlerdatensatz auf **Zugewiesen**.



Discovery erneut starten

Führt den kompletten Discovery-Prozess aus. Normalerweise führen Sie Discovery aus, nachdem Sie die Korrekturanweisungen befolgt haben, die angezeigt werden, wenn Sie auf **Anweisungen anzeigen** klicken.

Anweisungen anzeigen

Zeigt ein Problembehebungsverfahren in einem Popup-Fenster an. Führen Sie die Schritte aus, um den Fehler zu beheben.

Fehler ignorieren

Klicken Sie mit der rechten Maustaste auf einen Fehler, und wählen Sie dann **Fehler ignorieren** aus, um den Wert **Ignoriert** auf **true** zu setzen.

Das System führt die Aktion für die Elemente aus, zeigt zuerst **In Bearbeitung** und anschließend das Ergebnis (Erfolg oder Fehlschlag) der Aktion an. Wenn der Fehler behoben ist, wird das **Fehlerstatus**-Feld im Fehlerprotokoll auf **Gelöst** gesetzt.

Hinweis: Wenn eine Aktion (z. B. Discovery) im Gange ist, aber zu lange dauert, können Sie auf **Stopp** klicken, um sie anzuhalten.

7. Klicken Sie auf **Fertig**, um die Statusmeldung zu schließen.
8. Wenn Sie eine Aktion für eine Auswahl ausgeführt haben und der Fehler behoben wurde, können Sie auf **Alle korrigieren** klicken, um die gleiche Aktion auf alle Elemente in der Liste anzuwenden.

Fehler in individuellen Anwendungsservicezuordnungen beheben

Sie können Erkennungsprobleme in jeder Anwendungsservicezuordnung einzeln behandeln.

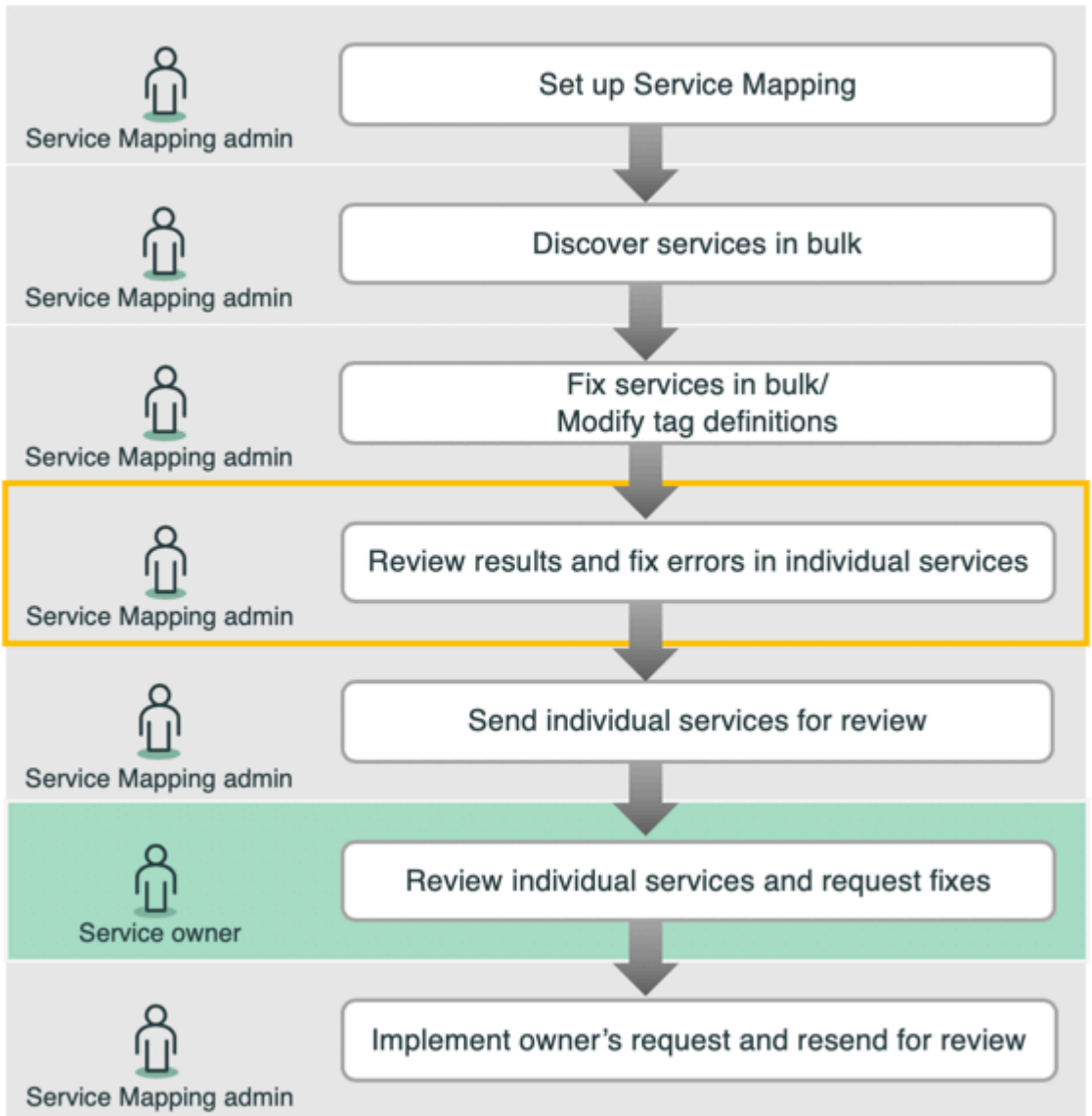
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: service_mapping_admin

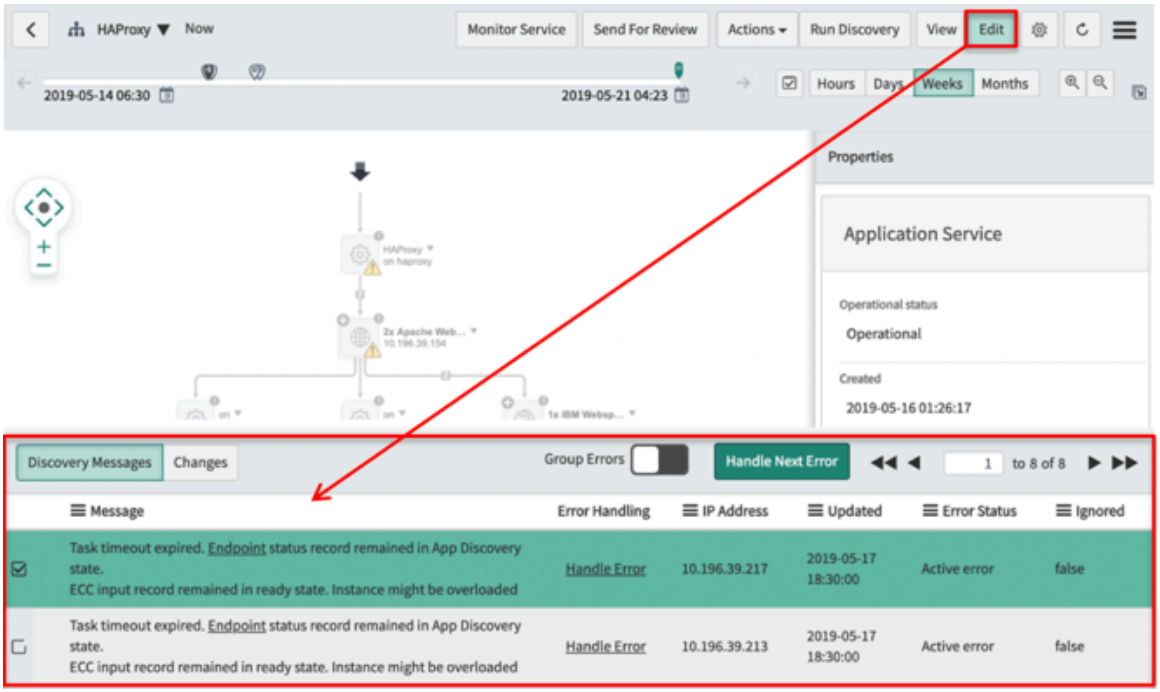
Warum und wann dieser Vorgang ausgeführt wird
Sie können Fehler in einzelnen Anwendungsservices jederzeit beheben. Nach der ersten Zuordnung von Anwendungsservices in Ihrer Organisation beheben Sie normalerweise Fehler in einzelnen Anwendungsservices, nachdem Sie Fehler in mehreren Services als Massenvorgang behoben haben. Möglicherweise müssen Sie aber auch noch später Fehler in einem genehmigten und abgeschlossenen Anwendungsservice beheben.

Service-Mapping-Workflow



Prozedur
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Stellen Sie sicher, dass die Zuordnung im Bearbeitungsmodus geöffnet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Fehlerhafte CIs werden mit dem Warnsymbol (⚠) auf der Karte angezeigt. Discovery-Nachrichten auf der Registerkarte **Discovery-Nachrichten** bieten kurze Fehlerbeschreibungen.

3. Wahlweise: Gruppieren Sie Fehler nach Typen, indem Sie auf **Fehler gruppieren** klicken. Die Erkennungsfehlermeldungen auf der Registerkarte **Discovery-Nachrichten** sind nach vordefinierten Typen (Fehlercodes) sortiert.
4. Um einen Fehler aus der Liste zu prüfen und zu beheben, klicken Sie auf **Fehler behandeln** neben der Fehlerbeschreibung.
   Oder
5. Um den ersten Fehler in der größten Fehlergruppe zu prüfen, klicken Sie in der Zuordnung oben links auf **Nächsten Fehler behandeln**.
6. Um zu erfahren, wie der Fehler behoben werden kann, klicken Sie im rechten Fensterbereich unter **Aktion für Auswahl** auf **Anweisungen öffnen**.

   Hinweis: Anweisungen sind nur für die am häufigsten vorkommenden Fehler verfügbar.

7. Klicken Sie auf die entsprechende halbautomatisierte Lösungsoption, um den Fehler im rechten Fensterbereich unter **Aktion für Auswahl** zu beheben.
   Die Fehlerlösungsoptionen variieren, da sie vom spezifischen Erkennungsfehler abhängen, der dem ausgewählten CI zugeordnet ist.

Verwenden Sie diese Option	Zu diesem Zweck
Management-IP hinzufügen	Geben Sie die Management-IP ein, um eine Erkennung für die Hostressourcen und -verbindungen auszulösen. Normalerweise benötigen Sie diese Lösung für Anwendungsservices, die nicht erkannte Geräte wie Lastenausgleichsmodule als Einstiegspunkte haben. Die Management-IP-Adresse eines Netzwerkgeräts ist die Adresse, die Sie ver-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie diese Option	Zu diesem Zweck
	wenden, um das Gerät über SNMP oder ein anderes Verwaltungsprotokoll zu erreichen. **Hinweis:** Das System speichert die von Ihnen konfigurierte Management-IP nicht.
Neue WMI-Anmeldeinformationen erstellen	Öffnen Sie das Windows-Anmeldeinformationsformular, und konfigurieren Sie fehlende Windows-Anmeldeinformationen für das ausgewählte CI. Siehe Windows-Anmeldeinformationen .
Neue SSH-Anmeldeinformationen erstellen	Öffnen Sie das SSH-Anmeldeinformationsformular, und konfigurieren Sie fehlende SSH-Anmeldeinformationen für das ausgewählte CI. Siehe SSH-Anmeldeinformationen .
Neuen privaten SSH-Schlüssel erstellen	Öffnen Sie das Formular für private SSH-Schlüssel, und konfigurieren Sie die fehlenden Anmeldeinformationen für das ausgewählte CI. Siehe Anmeldeinformationstyp des privaten SSH-Schlüssels .
Neue SNMP-Anmeldeinformationen erstellen	Öffnen Sie das SNMP-Anmeldeinformationsformular, und konfigurieren Sie fehlende SNMP-Anmeldeinformationen für das ausgewählte CI. Siehe SNMP-Anmeldeinformationen .
Discovery-Protokoll anzeigen	Im Protokoll erfahren Sie, in welcher Phase ein Fehler aufgetreten ist und was ihn verursacht hat.
Überspringen und fortsetzen	Fügen Sie das CI, dessen Erkennung fehlgeschlagen ist, manuell hinzu, und konfigurieren Sie Attribute des Einstiegspunkts, ab dem Service-Mapping die Erkennung fortsetzen soll. Weitere Informationen finden Sie unter Fehler überspringen, um mit der Erkennung eines Anwendungsservice fortzufahren.
Erkennung wiederholen	Führen Sie den Erkennungsprozess für das ausgewählte CI aus, nachdem Sie versucht haben, einen zugehörigen Erkennungsfehler zu beheben.
Betroffene Services anzeigen	Zeigen Sie eine Liste aller Services an, die vom ausgewählten Fehler betroffen sind. Klicken Sie in der Liste auf einen Service, um Servicedetails anzuzeigen.

8. Wenn keine Anweisungen oder halbautomatisierte Lösungsoptionen verfügbar sind, beheben Sie die Fehler auf Basis der Symptome und Erkennungsmeldungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Zum Ignorieren eines irrelevanten Fehlers klicken Sie mit der rechten Maustaste auf die entsprechende Fehlermeldung auf der Registerkarte **Discovery-Nachrichten** und wählen `Toggle Ignore State (Ignorieren-Status umschalten)`.
   Der ignorierte Fehler verschwindet aus der Zuordnung und aus der Liste der Erkennungsfehlermeldungen.

   Hinweis: Bei Bedarf können Sie ignorierte Fehler trotzdem anzeigen, indem Sie die Option **Ignorierte Fehler einschließen** im Menü **Weitere Optionen** aktivieren. Weitere Informationen finden Sie unter Ansicht für Anwendungsservicezuordnung ändern.

10. Um den nächsten Fehler in der größten Fehlergruppe zu prüfen, klicken Sie auf **Nächsten Fehler behandeln**.
11. Wenn Sie mit dem Überprüfen und Behandeln von Fehlern fertig sind, klicken Sie auf eine beliebige Stelle in der Zuordnung, um den Bereich **Fehler beheben** zu schließen.

Nächste Maßnahme
Wenn Sie die meisten Fehler gelöst haben, senden Sie die für Service zur Überprüfung.

Zugehörige Informationen

Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping

Fehler in einzelnen Anwendungsservices mithilfe von Discovery-Nachrichten beheben

Service-Mapping bietet keine halbautomatisierten Lösungsoptionen für Fehler, die eine erweiterte Lösung erfordern. Beheben Sie solche Fehler mithilfe von Symptomen und Erkennungsmeldungen.

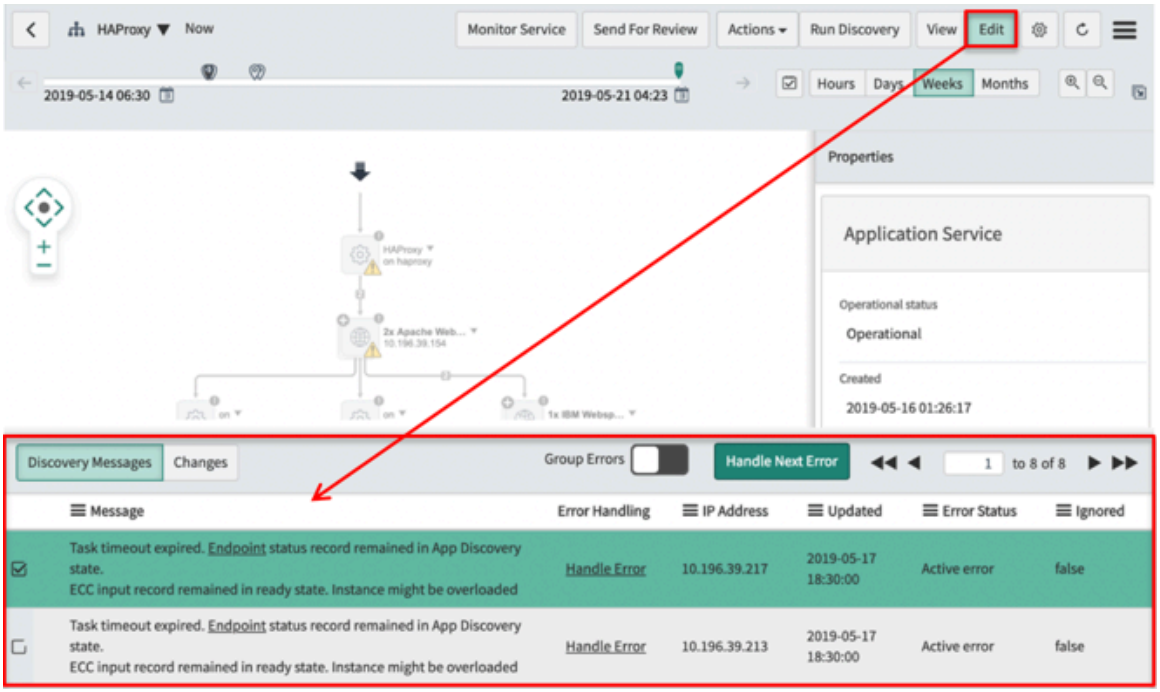
Vorbereitungen
Versuchen Sie, Fehler mit halbautomatisierten Lösungsoptionen zu beheben, wie in Fehler in individuellen Anwendungsservicezuordnungen beheben beschrieben.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Fehler in einzelnen Anwendungsservices jederzeit beheben.

Prozedur
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Klicken Sie neben der betreffenden Serviceinstanz **auf Karte anzeigen**.
3. Stellen Sie sicher, dass die Zuordnung im Bearbeitungsmodus geöffnet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Fehlerhafte CIs werden mit dem Warnsymbol (⚠) auf der Karte angezeigt. Discovery-Nachrichten auf der Registerkarte **Discovery-Nachrichten** bieten kurze Fehlerbeschreibungen.

4. Beheben Sie Fehler basierend auf den Symptomen und Erkennungsmeldungen.

Symptom	Lösung
Die folgende Erkennungsmeldung wird angezeigt: `Die Zuordnung zeigt nicht den gesamten Service an, da er zu groß ist. Die Anzahl der CI-Verbindungen hat das zulässige Maximum überschritten.`	Reduzienen Sie die Größe des Anwendungsservice. ◦ Führen Sie für einen Anwendungsservice, der mit musterbasierter und datenverkehrsbasierter Erkennung zugeordnet ist, die folgenden Aktionen aus: ▪ Wenn Sie anwenderdefinierte Discovery-Muster und Zuordnungsergebnisse in sehr großen Serviceinstanzen verwenden, ändern Sie die Muster so, dass sie keine irrelevanten CIs zuordnen. ▪ Teilen Sie den Service in kleinere Services auf. ◦ Führen Sie für einen Anwendungsservice, der aus einem Anwendungsservice umgewandelt wurde, die folgenden Aktionen aus: ▪ Überprüfen Sie die konvertierte Serviceinstanz, um CI-Beziehungen zu identifizieren, die für diesen Service irrelevant oder redundant sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Lösung
	Entfernen Sie solche CI-Beziehungen in der CMDB. ▪ Entscheiden Sie, wie viele Ebenen zugehöriger CIs Sie in diese Serviceinstanz aufnehmen müssen. Ändern Sie bei Bedarf die Anzahl der bei der Konvertierung verwendeten Ebenen, um die Servicegröße zu reduzieren.
Die folgende Discovery-Meldung wird in einer Tag-basierten Serviceinstanz angezeigt: *This tag-based service instance reached the maximum number of CIs. For more information, refer to the product documentation.*	Führen Sie die folgenden Aktionen aus: ◦ Ändern Sie die für die Zuordnung verwendeten Tag-Definitionen, um sicherzustellen, dass Service-Mapping nur relevante CIs in der Serviceinstanz enthält. ◦ Bei Bedarf konfigurieren Sie die Tag-basierte Erkennung, um zu ändern, welche CIs Service-Mapping in Tag-basierte Serviceinstanzen einschließt.
◦ Die für Service-Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Konfigurationselements an. ◦ Die folgende Erkennungsmeldung wird für das Konfigurationselement angezeigt: `Fehler beim Ausführen des Befehls mit sudo auf dem Host <IP-Adresse des Hosts>`.	KB0621669: Resolving failure to execute commands using sudo during Discovery in Service Mapping (Fehler beim Ausführen von Befehlen mit sudo während der Erkennung in Service Mapping beheben)
Die folgende Fehlermeldung wird für das Konfigurationselement angezeigt: `Zugriff verweigert`.	KB0564283: Resolving an issue of denied access to a Windows Server (Problem mit verweigertem Zugriff auf einen Windows-Server beheben)
◦ Die für Service-Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Windows-Servers an. ◦ Die folgende Erkennungsmeldung für den Windows-Server angezeigt: `RPC-Server nicht verfügbar`.	KB0564282: Resolving issue of RPC Server unavailable during Windows Server discovery in Service Mapping (Problem eines nicht verfügbaren RPC-Servers während der Windows Server-Ermittlung in Service Mapping beheben)
◦ In der für Service-Zuordnung wird anstatt des Lastenausgleichsmodul-CI das Warnsymbol ⚠ angezeigt. ◦ Die folgende Erkennungsmeldung wird angezeigt: `Service Mapping hat eine horizontale Erkennung ausgelöst, um den Host x.x.x.x zu finden, da dieser Host nicht in der CMDB war. Die horizontale Erkennung`	KB0610414: Resolving failure to discover operating system for a load balancer (Fehler beim Erkennen des Betriebssystems für ein Lastenausgleichsmodul beheben)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Lösung
`ist fehlgeschlagen. Weitere Informationen finden Sie unter Erkennungsstatus.`	
Anstelle der Zuordnung wird die folgende Erkennungsmeldung angezeigt: `Die Zuordnung kann nicht angezeigt werden. Topologie zu groß.`	KB0596671: Beheben eines großen Topologieproblems in für Service Karten
Eine virtuelle IP (VIP) für das Service-CI eines Lastenausgleichsmoduls wird manchmal mit den IP-Adressen eines anderen Lastenausgleichsmoduls aktualisiert.	KB0610412: Resolving load balancers merging into one CI in Service Mapping (Zusammenführung von Lastenausgleichsmodulen in ein einzelnes CI in Service Mapping beheben)
Die Zuordnung zeigt für Lastenausgleichsmodule falsche virtuelle IP-Namen an.	KB0610413: Resolving incorrect virtual IP names of load balancers in Service Mapping (Falsche virtuelle IP-Namen von Lastenausgleichsmodulen in Service Mapping beheben)
Die für Service-Zuordnung besteht jedes Mal aus verschiedenen CIs, wenn Sie den Zuordnungsprozess für dieselben Einstiegspunkte ausführen, um denselben für Service zu erkennen.	KB0595227: Troubleshooting inconsistent mapping results (Problembehandlung bei inkonsistenten Zuordnungsergebnissen)
In der für Service-Zuordnung ist kein Lastenausgleichsmodul-CI vorhanden. Es gibt Verbindungen, die direkt vom Einstiegspunkt des für Service zu den CIs der nächsten Ebene wechseln. Die übrigen CIs verschwinden ebenfalls aus der Zuordnung.	KB0621529: Resolving the issue of a load balancer disappearing from the application service map (Problem, dass ein Lastenausgleichsmodul nicht mehr in der Anwendungsservicezuordnung angezeigt wird, lösen)
◦ Die für Service-Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Konfigurationselements an. ◦ Die folgende Erkennungsmeldung wird für das Konfigurationselement angezeigt: `Timeout des SSH-Befehls auf dem Host`.	KB0621670: Resolving the issue of SSH command time-out during discovery in Service Mapping (Problem einer Zeitüberschreitung des SSH-Befehls während der Erkennung in Service Mapping lösen)
Ein Cluster-CI wird getrennt von allen CIs in den darüber oder darunter liegenden Zuordnungsebenen angezeigt.	KB0621531: Auflösen getrennter Cluster-CIs auf der für Service Zuordnen
◦ In der Zuordnung wird entweder das Konfigurationselement (CI) des Lastenausgleichsmoduls mit einem Warnsymbol oder nur das Warnsymbol ⚠ angezeigt. ◦ Die folgende Erkennungsmeldung wird für das CI angezeigt, das als Lastenausgleichsmodul im für Service	KB0621576: Resolving failure to discover VIP for a load balancer (Fehler beim Erkennen des VIP für ein Lastenausgleichsmodul beheben)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Lösung
fungieren soll: `Anwendung wurde nicht erkannt. Weitere Details finden Sie im Erkennungsprotokoll.`	
Die für Service-Zuordnung zeigt ein anderes Lastenausgleichsmodul als das, das Sie in diesem Anwendungsservice erwartet haben.	KB0621616: Business service map displays a wrong load balancer in Service Mapping (Business Service-Übersicht in Service Mapping zeigt ein falsches Lastenausgleichsmodul an)
◦ Die für Service-Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Konfigurationselements an. ◦ Die folgende Erkennungsmeldung wird für das Konfigurationselement angezeigt: `Timeout des SSH-Befehls auf dem Host.`	KB0621670: Resolving the issue of SSH command time out during discovery in Service Mapping (Problem einer Zeitüberschreitung des SSH-Befehls während der Erkennung in Service Mapping lösen)
◦ Die für Service-Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Konfigurationselements an. ◦ Die folgende Erkennungsmeldung wird für das Konfigurationselement angezeigt: `Kein aktiver MID Server für IP X.X.X.X gefunden`	KB0622808: Resolving a failure to find a MID Server for an IP address (Fehler bei der Suche nach einem MID Server für eine IP-Adresse beheben)
◦ Die für Service-Zuordnung zeigt das Warnungssymbol (⚠) oben oder anstelle des Konfigurationselements an. ◦ Die folgende Erkennungsmeldung wird für das Konfigurationselement angezeigt: `„64\rctrlx" wird nicht als interner oder externer Befehl, ausführbares Programm oder Batch-Datei erkannt.`	Führen Sie das unter Datei rctrlx.exe auf MID Servers hochladen beschriebene Verfahren aus.
Ein CI oder ein Segment der Zuordnung ist ausgegraut, nachdem Service-Mapping die Erkennung von oben nach unten für einen zuvor zugeordneten für Service ausgeführt hat. In diesem Anwendungsservice konnte das CI bzw. konnten die Verbindungen, die zu diesem CI führten, von Service-Mapping nicht erneut erkannt werden.	Führen Sie die nachfolgenden Schritte durch: **a.** (Optional für ausgegraute Segmente) Identifizieren Sie das fehlerhafte CI, das zum Ausgrauen des Segments führt. **b.** Verwenden Sie die Erkennungsmeldung, die diesem fehlerhaften CI zugeordnet ist, um das Problem zu lösen.

5. Klicken Sie auf **Discovery ausführen**.

Fehler überspringen, um mit der Erkennung eines Anwendungsservice fortzufahren

Wenn Sie wissen, aus welchen Konfigurationselementen (Configuration Items, CI) und Verbindungen Ihre Serviceinstanz besteht, können Sie Service-Mapping aktivieren, um die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery der Serviceinstanz fortzusetzen, auch wenn einige Fehler auftreten. Sie können Fehler überspringen und die Fehlerbehebung später durchführen, um die Zuordnung des größten Teils der Serviceinstanz abzuschließen, auch wenn einige CIs fehlen.

Vorbereitungen

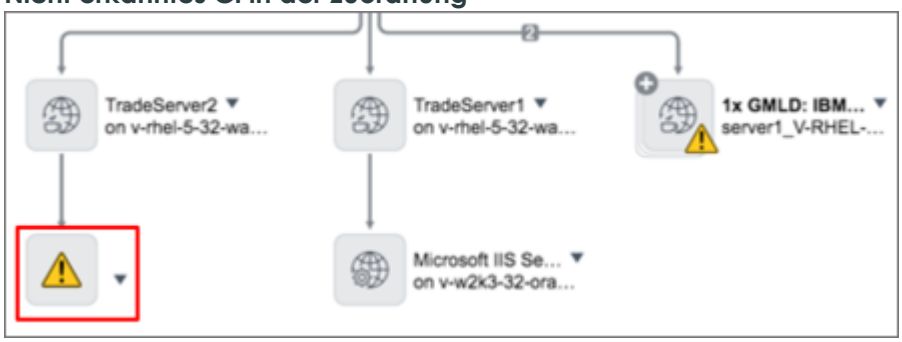
Machen Sie sich mit der Struktur des Anwendungsservice vertraut, um zu erfahren, welche CIs die nächste Ebene nach dem problematischen CI bilden. Wenden Sie sich bei Bedarf an den Anwendungsservice-Eigentümer, um die erforderlichen Informationen zu erhalten.

Erforderliche Rolle: service_mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Normalerweise wird die Erkennung eines Anwendungsservices beendet, wenn Service-Mapping ein CI nicht identifizieren kann. In diesem Fall wird in der Zuordnung anstelle des nicht erkannten CI ein Warnungssymbol angezeigt. Das nicht erkannte CI enthält keine CIs oder ausgehenden Verbindungen.

Nicht erkanntes CI in der Zuordnung

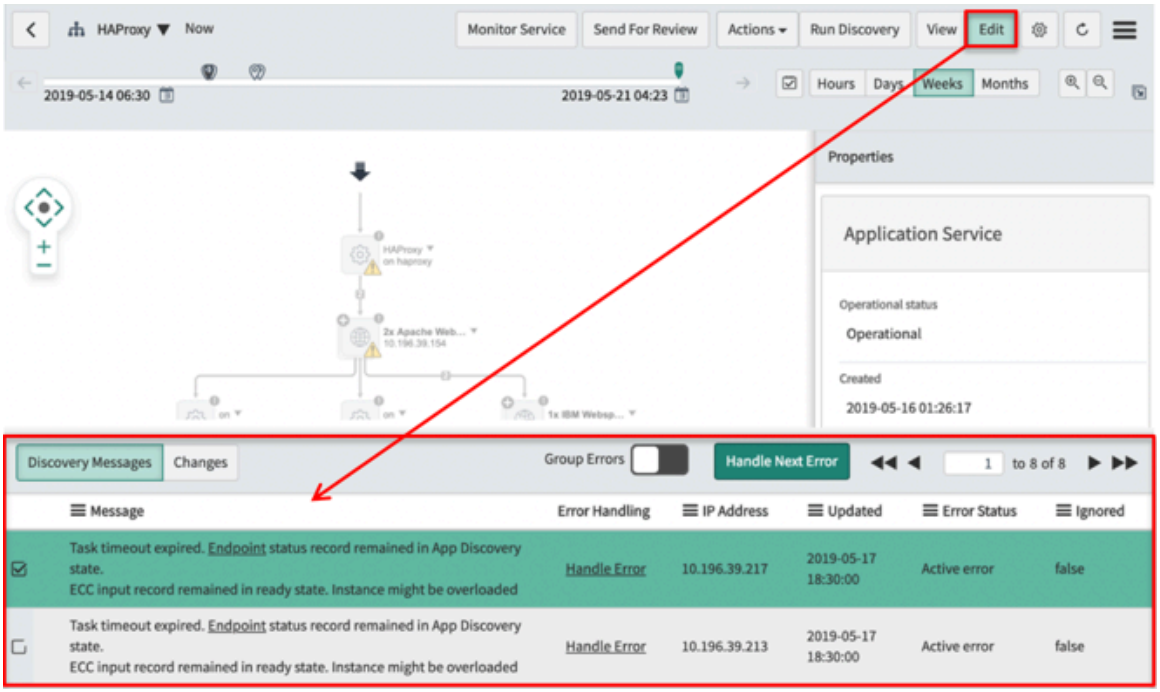


Sie können das Problem des nicht erkannten CI überwinden und die Erkennung von den CIs aus neu starten, die zur nächsten Ebene hinter dem problematischen CI gehören. Fügen Sie dazu manuell ein CI hinzu, wenn Sie wissen, welches das nicht erkannte CI ist und was die eingehende Verbindung des CI der nächsten Ebene ist. Service-Mapping verwendet während der Erkennung eingehende Verbindungen für den Zugriff auf ein CI. Diese Verbindungen werden als Endpunkte bezeichnet.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Stellen Sie sicher, dass die Zuordnung im Bearbeitungsmodus geöffnet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Stellen Sie sicher, dass sich die Zuordnung nicht in der Host-Ansicht befindet.
4. Klicken Sie auf den Pfeil neben dem nicht erkannten CI, und wählen Sie **Überspringen und fortsetzen**.
5. Definieren Sie Attribute des CI, das Sie anstelle des nicht erkannten CI manuell platzieren möchten.

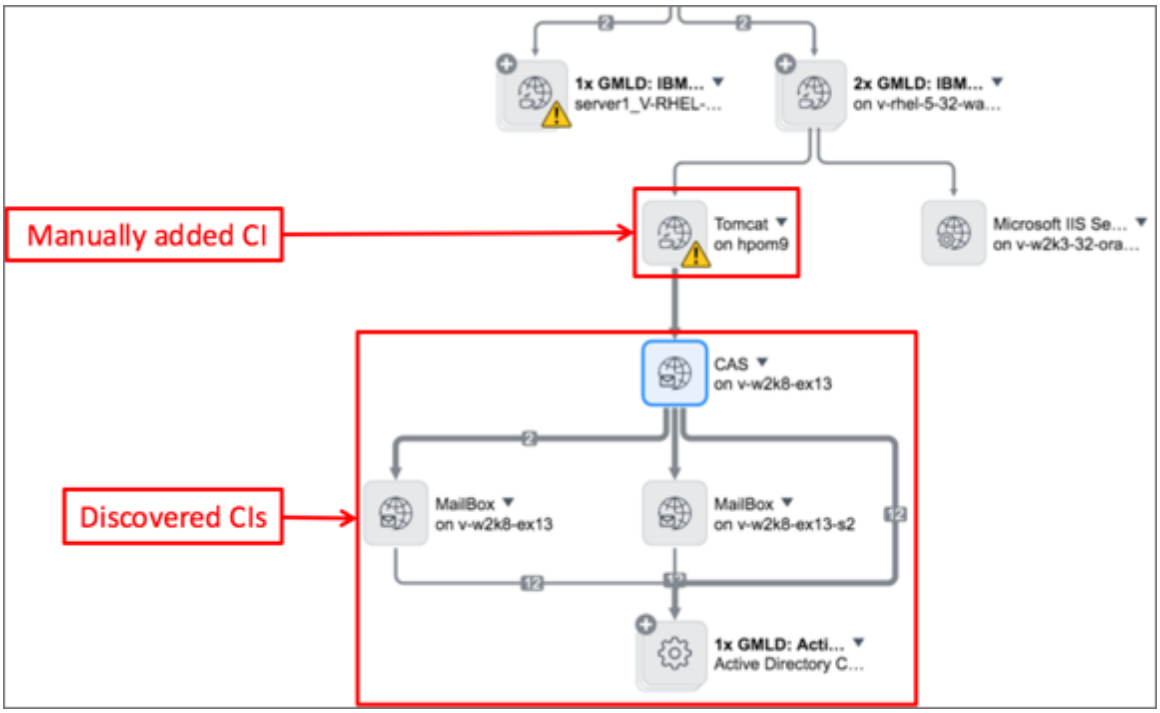
Feld	Beschreibung
CI-Typ	Wählen Sie den CI-Typ (CI-Klasse) für das hinzuzufügende CI aus. Jedes CI gehört zu einem CI-Typ, der eine Reihe von Attributen enthält, die für diese Art von CI konfiguriert wurden. *cmdb_ci_appl* für Anwendungen.
CI-Name	Wählen Sie das CI aus der Liste der CIs des ausgewählten CI-Typs aus. **Hinweis:** Um verzögerte Ergebnisse bei der Suche nach einem bestimmten CI zu vermeiden, sollten Sie Ihre Suche so spezifisch wie möglich gestalten. Eine Suche mit *<name> kann lange dauern und einen großen Datensatz zurückgeben.

Hinweis:

Wenn der CI-Typ nicht in der Liste angezeigt wird, lässt Service-Mapping das manuelle Hinzufügen von CIs dieses Typs nicht zu. Sie können beispielsweise keinen Anwendungscluster oder Endpunkt manuell hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Konfigurieren Sie Attribute des Einstiegspunkts, ab dem Service-Mapping fortgesetzt wird, indem Sie den Einstiegspunkttyp auswählen und relevante Felder eingeben.
   Wenn der erforderliche Einstiegspunkttyp nicht in der Liste „Einstiegspunkttyp auswählen“ angezeigt wird, müssen Sie ihn wie in Einstiegspunkttypen für Service-Mapping erstellen beschrieben erstellen.
7. Klicken Sie auf **Absenden**.
   Die Zuordnung zeigt das manuell hinzugefügte CI anstelle des nicht erkannten CI. Service-Mapping startet die Erkennung für CIs der nächsten Stufen. Nach Abschluss des Erkennungsprozesses zeigt die Zuordnung unter dem manuell hinzugefügten CI alle erkannten CIs an.



Nächste Maßnahme

So erkennen Sie das problematische CI automatisch:

1. Führen Sie die erforderliche Fehlerbehebung durch, damit Service-Mapping das problematische CI erkennen kann. Beispielsweise müssen Sie eventuell das relevante Muster anpassen, fehlende Anmeldeinformationen bereitstellen oder die datenverkehrsbasierte Erkennung optimieren.
2. Navigieren Sie zur betreffenden für Service-Zuordnung.
3. Klicken Sie auf **Discovery ausführen**.
4. Überprüfen Sie nach Abschluss des Erkennungsprozesses, ob Service-Mapping das CI erkannt hat. Wenn Service-Mapping das CI erkannt hat, zeigt die Zuordnung das tatsächliche CI ohne das Warnsymbol (⚠) an.

Zugehörige Informationen

Von ITOM-Transparenz verwendete Erkennungsmuster

Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren

Voraussetzungen für die Erkennung von oben nach unten mit Service-Mapping

Musterbezogene Zuordnungsfehler beheben

Sie können Zuordnungsfehler beheben, die durch Muster verursacht werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service Mapping Teil 2 | Problembehandlung

Dieses Video zeigt eine alternative Methode zur Behebung von Musterfehlern.

Vorbereitungen
Überprüfen Sie in der Erkennungsmeldung, ob der Zuordnungsfehler tatsächlich auf ein falsches Muster zurückzuführen ist. Wenn die Meldung „Anwendung konnte nicht erkannt werden“ lautet, ist der Fehler musterbezogen.

Sie müssen mit dem Musterdesignermodul von Service-Mapping vertraut sein.

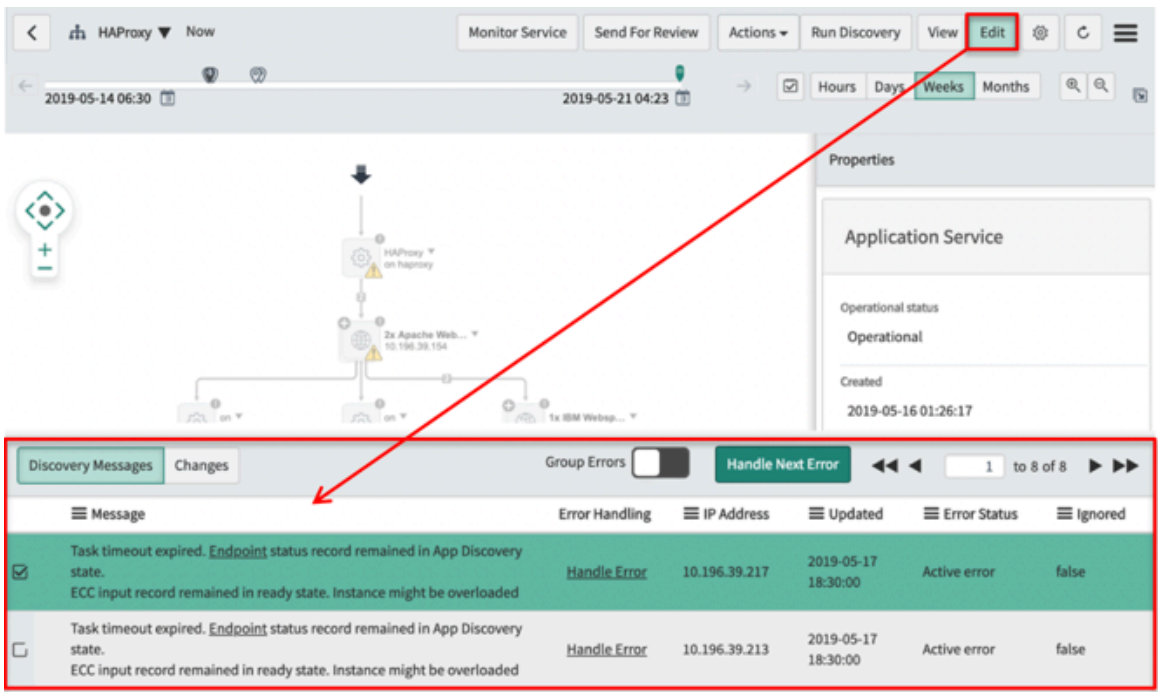
Erforderliche Rolle: admin und service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Konfigurationselemente (CIs) vorhanden sind, die Service-Mapping nicht ordnungsgemäß zuordnen konnte, werden sie auf der für Service-Zuordnung mit Warnsymbolen ⚠ angezeigt. In der Regel treten Zuordnungsfehler auf, wenn Service-Mapping keine Verbindung zu einem CI herstellen oder dieses aufgrund eines ungenauen Musters nicht erkennen kann.

Sie können problematische Schritte in Ihrem Muster identifizieren und beheben, ohne alle Schritte und Vorgänge im Muster zu überprüfen. So können Sie musterbezogene Fehler schnell und effektiv beheben.

Prozedur

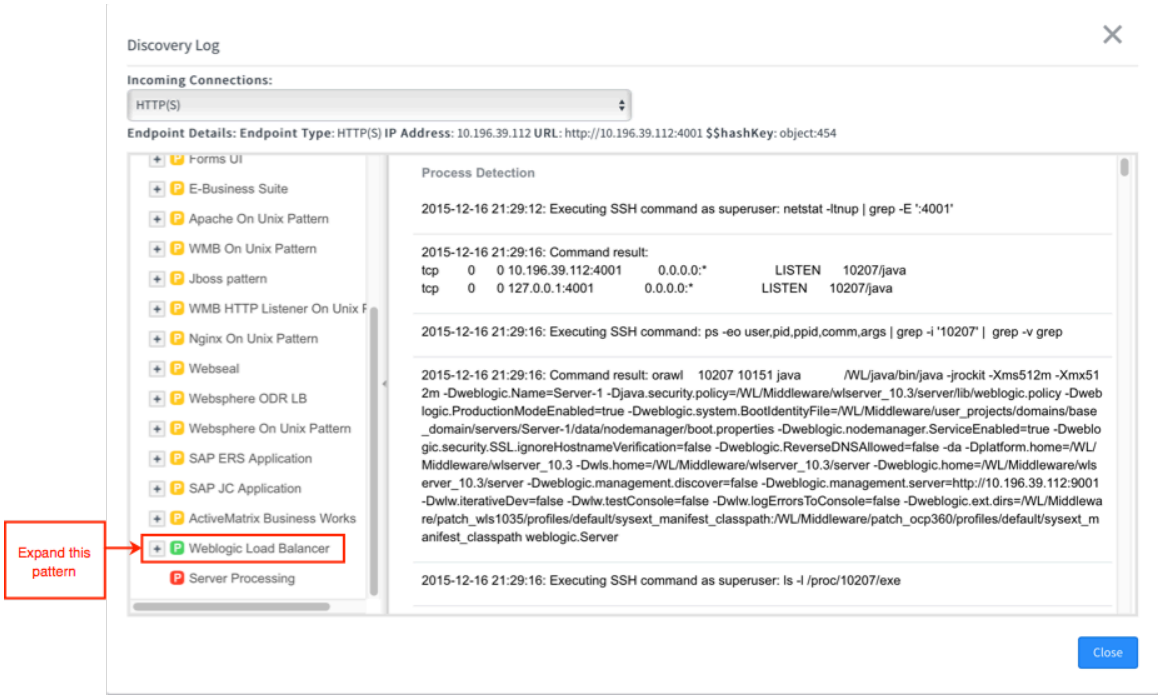
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Stellen Sie sicher, dass die Zuordnung im Bearbeitungsmodus geöffnet wird und Erkennungsmeldungen und Fehler anzeigt.



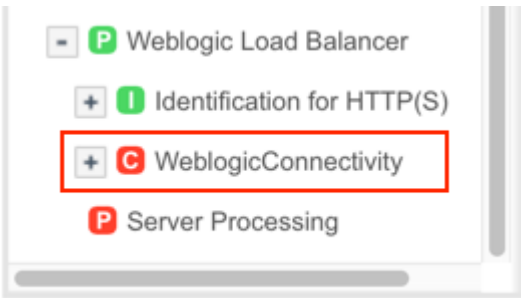
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie mit der rechten Maustaste auf das CI mit dem Warnsymbol (⚠), und wählen Sie **Discovery-Protokoll anzeigen** aus.
4. Erweitern Sie das fehlgeschlagene Muster, das über dem rot markierten Ergebnis angezeigt wird.



5. Erweitern Sie den fehlgeschlagenen Abschnitt, und klicken Sie auf den fehlgeschlagenen Schritt.

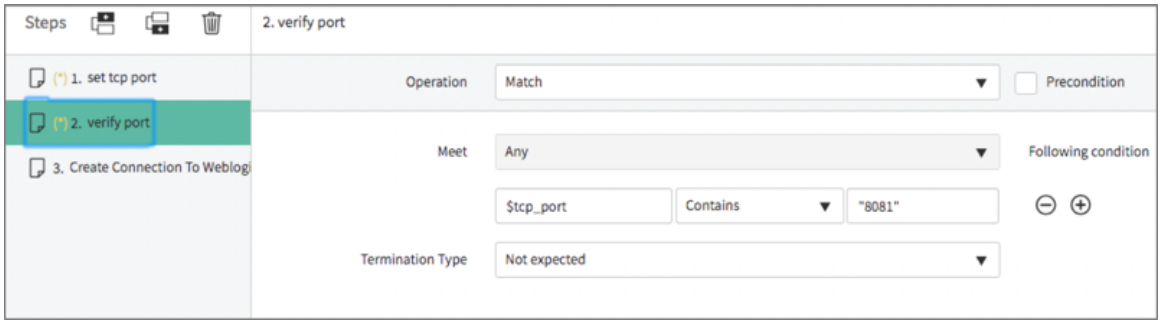


6. Klicken Sie auf **Debuggen**.
7. Klicken Sie auf den ersten Schritt, und warten Sie, bis der Musterdesigner ihn ausgeführt hat.

   Wiederholen Sie diese Aktion für weitere Schritte in der angegebenen Reihenfolge, bis Sie den fehlerhaften Schritt erreicht haben, der den Fehler verursacht.

   Im folgenden Beispiel lautet die Portnummer 8081 anstatt 8080, was das Problem verursacht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Klicken Sie auf **OK**.
9. Korrigieren Sie das Musterattribut, das das Problem verursacht.
10. Klicken Sie auf **Testen**.
11. Stellen Sie sicher, dass der Musterdesigner eine Erfolgsmeldung zurückgibt.
12. Klicken Sie auf **Speichern**.
13. Klicken Sie auf **Aktivieren**.
14. Kehren Sie zur für Service-Zuordnung zurück, die den Zuordnungsfehler enthielt.
15. Klicken Sie mit der rechten Maustaste auf das CI, für das das Muster repariert wurde, und wählen Sie **Discovery fortsetzen**.
16. Stellen Sie sicher, dass das CI erkannt und richtig zugeordnet wird.

Anwendungsservicezuordnungen prüfen und genehmigen

Nachdem der Administrator Service-Mapping IT-Services zugeordnet und Fehler darin behoben hat, arbeiten der Administrator und der Eigentümer zusammen, um die Servicezuordnungen zu überprüfen und zu genehmigen. Der Überprüfungs- und Genehmigungsprozess ist nur für erkannte und manuell erstellte Serviceinstanzen verfügbar.

Service-Mapping muss zum Zuordnen oder Überprüfen von Serviceinstanzen aktiviert sein.

Benutzer, die die Überprüfung und Genehmigung durchführen, haben die Rollen eines Service-Mapping-Administrators. Ein Service-Mapping-Administrator ist für die Zuordnung, Korrektur und Wartung von Anwendungsservices verantwortlich. Der Besitzer der Serviceinstanz überprüft, ob die Serviceinstanzzuordnungen vollständig sind und alle wichtigen Komponenten, aus denen sie bestehen, korrekt dargestellt werden. Bei Bedarf hinterlässt der Besitzer Kommentare, die als Ablehnungsnachrichten bezeichnet werden, auf Serviceinstanzzuordnungen, die der Administrator Service-Mapping implementieren muss.

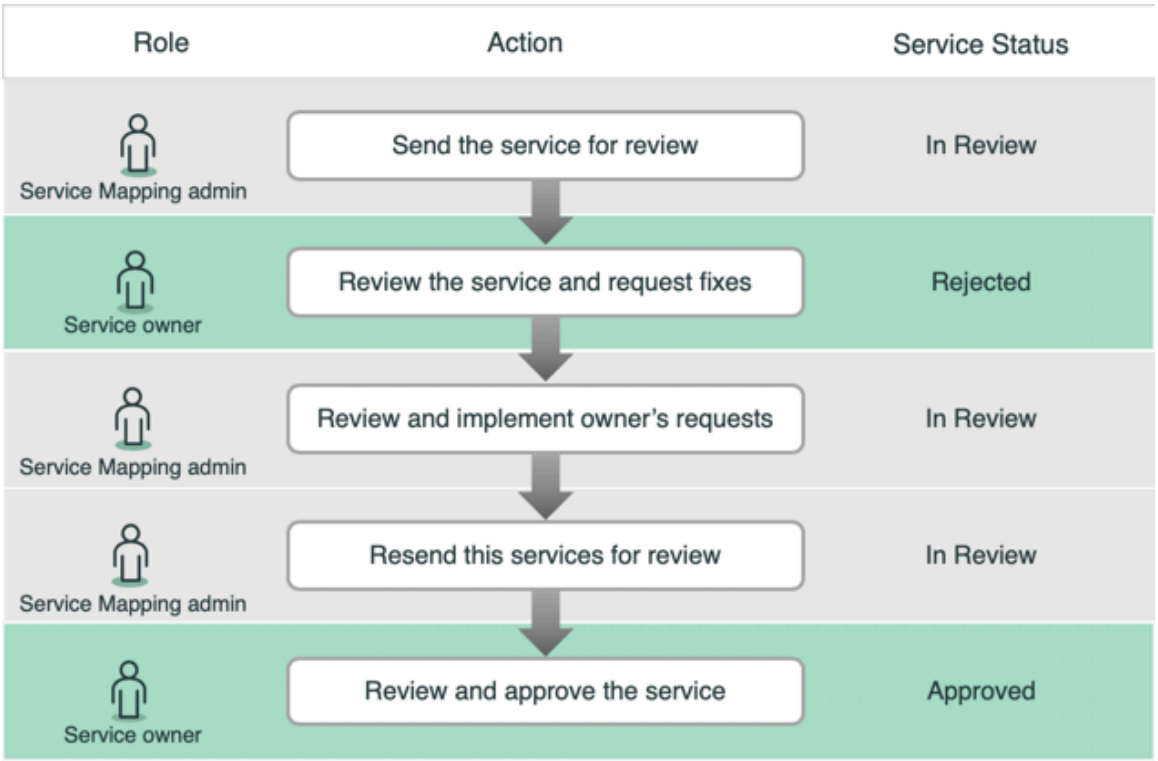
Der Überprüfungs- und Genehmigungsprozess wird in den folgenden Phasen durchgeführt:

1. Nach der erstmaligen Zuordnung der Serviceinstanzen behebt der Administrator Fehler und sendet einzelne Serviceinstanzen zur Überprüfung. Das System erstellt eine Serviceprozessaufgabe, die dem Besitzer der Serviceinstanz zugewiesen wird, und sendet eine diesbezügliche E-Mail-Benachrichtigung.
2. Der Besitzer der Serviceinstanz überprüft, ob die Serviceinstanzzuordnungen vollständig sind und alle wichtigen Komponenten, aus denen sie bestehen, korrekt dargestellt werden. Bei Bedarf hinterlässt der Besitzer Kommentare, die als Ablehnungsnachrichten bezeichnet werden, auf Serviceinstanzzuordnungen, die der Administrator Service-Mapping implementieren muss. Die dem Inhaber zugewiesene Serviceprozess-Aufgabe wird geschlossen. Das System sendet eine E-Mail-Benachrichtigung an den Administrator, dass der Inhaber Kommentare geschrieben hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Der Administrator erhält die E-Mail-Benachrichtigung, zeigt die Anforderungen des Besitzers an und implementiert sie.
4. Der Administrator sendet die Serviceinstanzzuordnungen erneut zur Überprüfung. Das System erstellt erneut eine Serviceprozessaufgabe, die dem Besitzer der Serviceinstanz zugewiesen wird, und sendet eine diesbezügliche E-Mail-Benachrichtigung.
5. Wenn die überarbeiteten Serviceinstanzzuordnungen zufriedenstellend sind, genehmigt der Besitzer der Serviceinstanz sie. Wenn nicht, fordert der Verantwortliche weitere Fehlerkorrekturen an, die der Administrator umsetzen muss.

Klicken Sie zum Anzeigen der Dokumentation für eine Überprüfungsphase auf das entsprechende Feld im Diagramm.



1. Senden Sie für Service zur Überprüfung
2. Business Service prüfen und Korrekturen anfordern
3. Anforderungen des Eigentümers prüfen und implementieren
4. Anwendungsservices erneut zur Überprüfung senden
5. Überprüfen und genehmigen Sie die Anwendungsservices

Die Prüfung des Anwendungsservice kann einige Zeit in Anspruch nehmen, da Änderungen erforderlich sind und der Zuordnungsprozess für den Anwendungsservice wiederholt ausgeführt werden muss. Normalerweise sind mehrere Iterationen erforderlich, um das gewünschte Ergebnis zu erzielen.

Sobald der Eigentümer einen Anwendungsservice genehmigt hat, ändert sich der Status des Anwendungsservice in „Genehmigt“ und er erscheint in der Liste der abgeschlossenen Anwendungsservices auf der **Startseite**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservicezuordnungen zur Überprüfung senden

Nachdem Sie einen Anwendungsservice zugeordnet haben, senden Sie ihn zur Überprüfung an den Verantwortlichen des Anwendungsservice, um sicherzustellen, dass die Zuordnung korrekt ist.

Vorbereitungen

Führen Sie eine erste Fehlerbehebung wie in Fehler bei Anwendungsservices als Massenvorgang beheben und Fehler in individuellen Anwendungsservicezuordnungen beheben beschrieben durch.

Erforderliche Rolle: service_mapping_admin

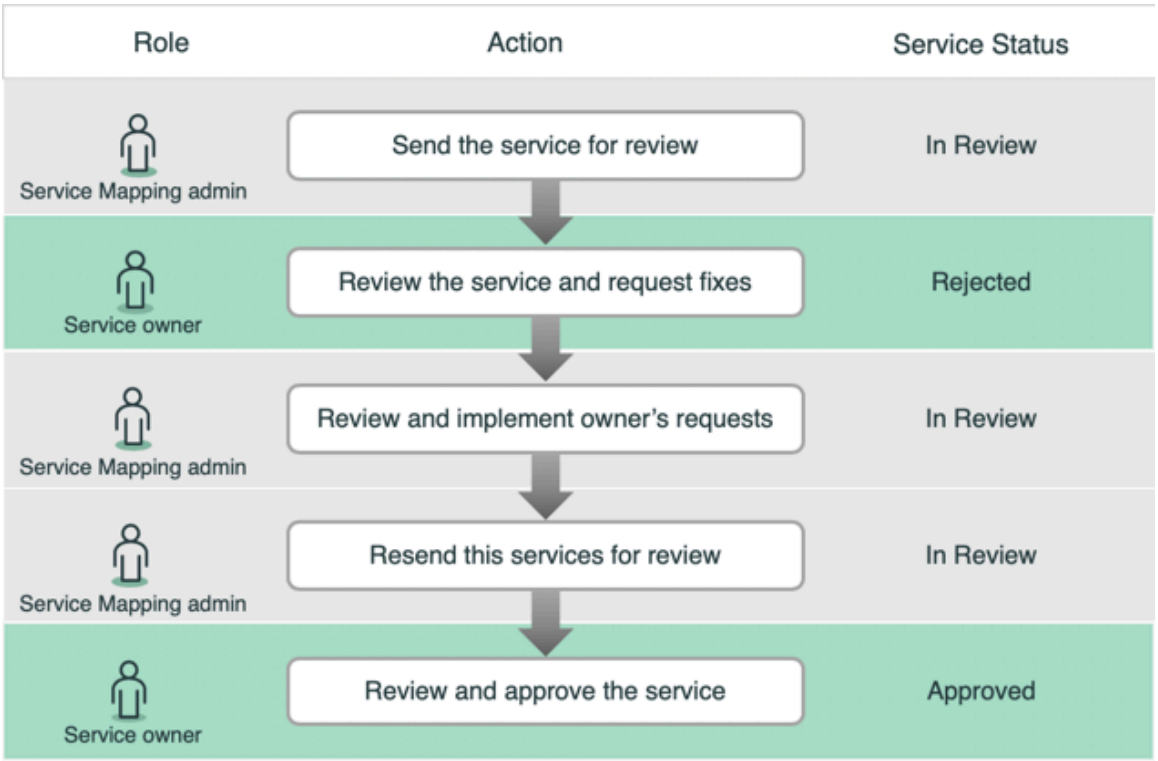
Warum und wann dieser Vorgang ausgeführt wird

Sie können zwar Fehler im Stapelverfahren beheben, müssen jedoch Anwendungsservices immer einzeln nacheinander zur Prüfung senden.

Das Senden von Anwendungsservicezuordnungen zur Überprüfung ist Teil des Überprüfungs- und Genehmigungsprozesses. Normalerweise senden Sie jede Anwendungsservicezuordnung zweimal zur Überprüfung: Das erste Mal für die erste Prüfung durch den Eigentümer und das zweite Mal, nachdem Sie das Eigentümerfeedback implementiert haben.

Nach der erstmaligen Zuordnung der Anwendungsservices beheben Sie Fehler und senden einzelne Anwendungsservices zur Überprüfung. Das System erstellt eine Serviceprozessaufgabe, die dem Besitzer der Serviceinstanz zugewiesen wird, und sendet eine diesbezügliche E-Mail-Benachrichtigung.

Klicken Sie zum Anzeigen der Dokumentation für eine andere Überprüfungsphase auf das entsprechende Feld im Diagramm.



1. Überprüfung des folgenden Elements: für Service und Korrekturen anfordern
2. Anforderungen des Eigentümers prüfen und implementieren
3. Senden Sie erneut für Service zur Überprüfung
4. Überprüfen und genehmigen Sie die für Service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. So senden Sie einen für Service zur Überprüfung über das für Service-Formular:
   a. Öffnen Sie die Serviceinstanzzuordnung.
   b. Sortieren Sie die Liste der geplanten Anwendungsservices nach Status und scrollen Sie, um die Services mit dem Status **in Bearbeitung** anzuzeigen, oder verwenden Sie den Filter, um die Liste einzugrenzen.
   c. Klicken Sie auf den erforderlichen für Service.
   d. Klicken **Aktionen** > **Zur Überprüfung senden**.
2. Sie können einen für Service auch über dessen Zuordnung zur Überprüfung senden:
   a. Navigieren zu **Service-Mapping** > **Startseite**.
      Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die von Service-Mapping erkannt werden können oder bereits erkannt wurden. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mit der API erstellt wurden.
   b. Klicken Sie auf die Kachel **Genehmigen**.
   c. Klicken Sie auf **Zur Überprüfung senden**.
   d. Klicken Sie auf den erforderlichen für Service.
      Die Zuordnung für diesen für Service wird geöffnet.
   e. Klicken Sie in der oberen Ecke des Fensters **auf Zur Überprüfung senden**.

Nächste Maßnahme

Wenn Sie eine E-Mail-Benachrichtigung erhalten, dass der Eigentümer Kommentare zu diesem für Service gesendet hat, überprüfen und implementieren Sie die Anforderungen des Eigentümers.

Anwendungsservicezuordnungen prüfen

Als Eigentümer des Anwendungsservice für die Anwendungsservicezuordnung erhalten Sie eine E-Mail-Benachrichtigung, dass Ihnen die Anwendungsservicezuordnung zur Überprüfung zugewiesen ist. Überprüfen Sie die Zuordnungsergebnisse auf Richtigkeit, und geben Sie entweder Ihr Feedback ab, oder genehmigen Sie die Anwendungsservicezuordnung. Der Überprüfungs- und Genehmigungsprozess ist nur für erkannte und manuell erstellte Serviceinstanzen verfügbar.

Vorbereitungen

Erforderliche Rolle: sm_app_owner

Warum und wann dieser Vorgang ausgeführt wird

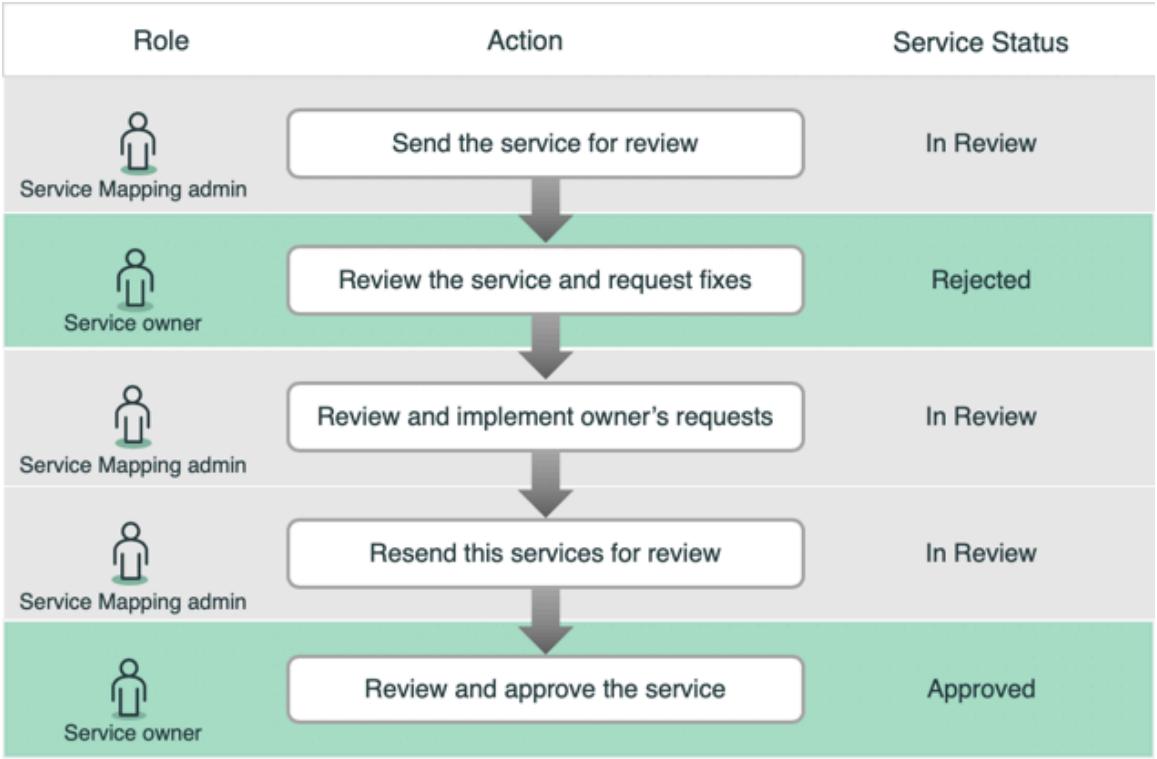
Im Idealfall überprüft nur der Verantwortliche des Anwendungsservice den geplanten Anwendungsservice. Allerdings können Benutzer mit der Rolle sm_app_owner oder service_mapping_admin diese Aufgabe auch ausführen.

Das Überprüfen von Anwendungsservicezuordnungen ist Teil des Überprüfungs- und Genehmigungsprozesses. Die Prüfung des Anwendungsservice kann einige Zeit in Anspruch nehmen, da Änderungen erforderlich sind und der Zuordnungsprozess für den Anwendungsservice wiederholt ausgeführt werden muss. Normalerweise sind mehrere Iterationen erforderlich, um das gewünschte Ergebnis zu erzielen. Sobald Sie mit dem Ergebnis der Erkennung zufrieden sind, genehmigen Sie den Anwendungsservice.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Sie Korrekturen angefordert oder den Anwendungsservice genehmigt haben, wird die Ihnen zugewiesene Serviceprozessaufgabe geschlossen.

Klicken Sie zum Anzeigen der Dokumentation für eine andere Überprüfungsphase auf das entsprechende Feld im Diagramm.



1. Anwendungsservice zur Überprüfung senden
2. Anforderungen des Eigentümers prüfen und implementieren
3. Anwendungsservices erneut zur Überprüfung senden

Prozedur

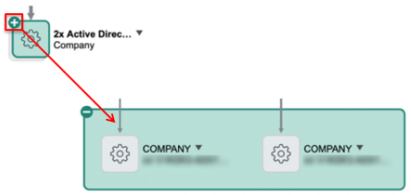
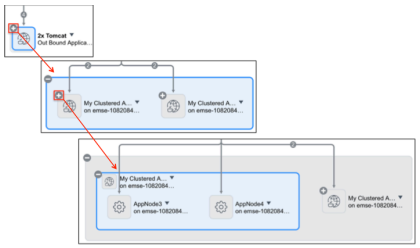
1. Klicken Sie auf den Link zur Anwendungsservicezuordnung in der E-Mail-Benachrichtigung. Die Zuordnung des Anwendungsservice wird in der ServiceNow-Instanz geöffnet.
2. Sie können den Anwendungsservice zur Prüfung auch aus der Liste der Ihnen zugewiesenen Aufgaben öffnen.
   a. Navigieren zu **Service-Mapping** > **Administration** > **Meine Aufgaben**.
   b. Wahlweise: Sortieren Sie die Liste der Serviceprozessaufgaben nach Bedarf.
   c. Klicken Sie auf die erforderliche Aufgabe.
   d. Klicken Sie auf den Link des Anwendungsservice-Formulars.
   e. Klicken Sie auf **Karte anzeigen**.
3. Überprüfen Sie in der Anwendungsservicezuordnung, ob alle wichtigen CIs aus dem Anwendungsservice erkannt und korrekt zugeordnet wurden.

Zweck	Aktion
Stellen Sie sicher, dass keine CI-Verbindungen fehlen.	Achten Sie auf CIs ohne Connectors zu anderen CIs. Beispielsweise fehlen in der folgenden Abbildung beim CI win2K12 Verbindungen zum Webserver.

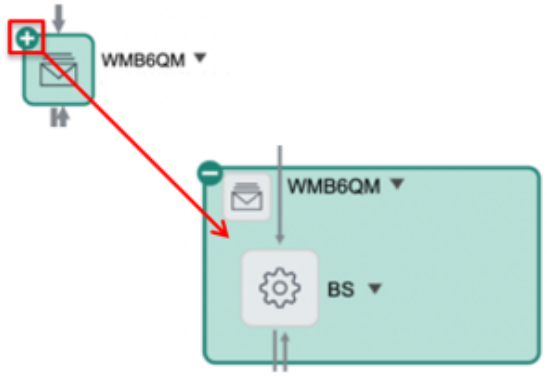
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zweck	Aktion
	 Wenn Verbindungen und CIs, zu denen sie führen, fehlen, spiegelt die Zuordnung nicht den tatsächlichen Status desfür Service und seinem Betrieb wider. Es können auch falsche Daten an Ereignismanagement übertragen werden, was zu einem ungenauen Monitoring führt.
Vergewissern Sie sich, dass nur CIs vorhanden sind, die zum Service gehören.	Überprüfen Sie alle CIs, die die Anwendungsservicezuordnung enthält, um CIs zu identifizieren, die nicht zu diesem Anwendungsservice gehören. In der Regel handelt es sich um Anwendungen, die interne Services unterstützen. Beispielsweise ist die Verbindung zwischen Microsoft Internet Information Services (IIS) und Active Directory möglicherweise nicht Teil des Anwendungsservice.
Überprüfen Sie, ob die Verbindungen zwischen CIs korrekt sind.	Zeigen Sie CI-Verbindungsattribute in einer Anwendungsservicezuordnung in an klassisch Service-Mapping.
Überprüfen Sie, ob Cluster richtig dargestellt werden.	Klicken Sie auf das Pluszeichen (+) neben einem CI. Es gibt zwei Clustertypen: Anwendungscluster In einem Anwendungscluster sind zwei oder mehr Anwendungen oder Geräte so konfiguriert, dass sie zusammenarbeiten und denselben Zweck erfüllen. Normalerweise bieten Cluster Hochverfügbarkeit oder Lastenausgleich. Ein Beispiel sind Webserver, die hinter einem Lastenausgleichsmodul arbeiten. Dieser Clustertyp wird als Stapel von CIs mit einer Bezeichnung angezeigt, die die Anzahl der CIs in diesem Cluster mit dem Multiplikationszeichen zeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zweck	Aktion
	 Anwendungscluster können ein Cluster innerhalb eines Clusters haben, jedoch nie mehr als zwei Ebenen:  BS-Cluster In einem BS-Cluster hostet ein Server zwei identische Betriebssysteme. Normalerweise bietet der Cluster ein Failover. Dieser Clustertyp wird als CI mit einem Pluszeichen und der Anzahl der CIs in diesem Cluster angezeigt.
Überprüfen Sie, ob Inklusionen richtig dargestellt werden.	Klicken Sie auf das Pluszeichen (+) neben einem CI. Bei einer Inklusion hostet ein Server Anwendungen, die als unabhängige Objekte behandelt werden. Beispielsweise kann das virtuelle IIS-Verzeichnis auf einem Windows-Dienst als Host ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zweck	Aktion
	

4. Führen Sie die folgenden Schritte aus, um den Servicezuordnungsadministrator über eine erforderliche Änderung oder Korrektur zu benachrichtigen:

   a. Klicken Sie über der Zuordnung auf **Aktionen**.

   b. Wählen Sie **Servicezuordnung ablehnen**.

   c. Geben Sie im Fenster „Ablehnungsnachricht hinzufügen“ Ihren Kommentar ein, und klicken Sie auf **Hinzufügen**.
   Der neue Kommentar wird auf der Registerkarte **Discovery-Nachrichten** unter der Zuordnung angezeigt. Der Status des Anwendungsservice wird in „Abgelehnt“ geändert.

   d. Fügen Sie bei Bedarf weitere Kommentare hinzu.

5. Wenn Sie mit den Ergebnissen zufrieden sind, genehmigen Sie diesen Anwendungsservice, indem Sie auf **Aktionen** klicken und dann den **Service genehmigen**.
   Der Status des Anwendungsservice ändert sich in „Genehmigt“ und er erscheint in der Liste der abgeschlossenen Anwendungsservices auf der **Startseite**. Der operative Status ändert sich in „Funktionsfähig“. Ab diesem Zeitpunkt können andere Anwendungen Daten verwenden, die von Service-Mapping gesammelt und organisiert wurden.

Zugehörige Informationen

Fehler in individuellen Anwendungsservicezuordnungen beheben

Anwendungsservices feinabstimmen, um Eigentümeranforderungen zu implementieren

Als Administrator bearbeiten und optimieren Sie Zuordnungen basierend auf Kommentaren des Eigentümers des Anwendungsservice.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

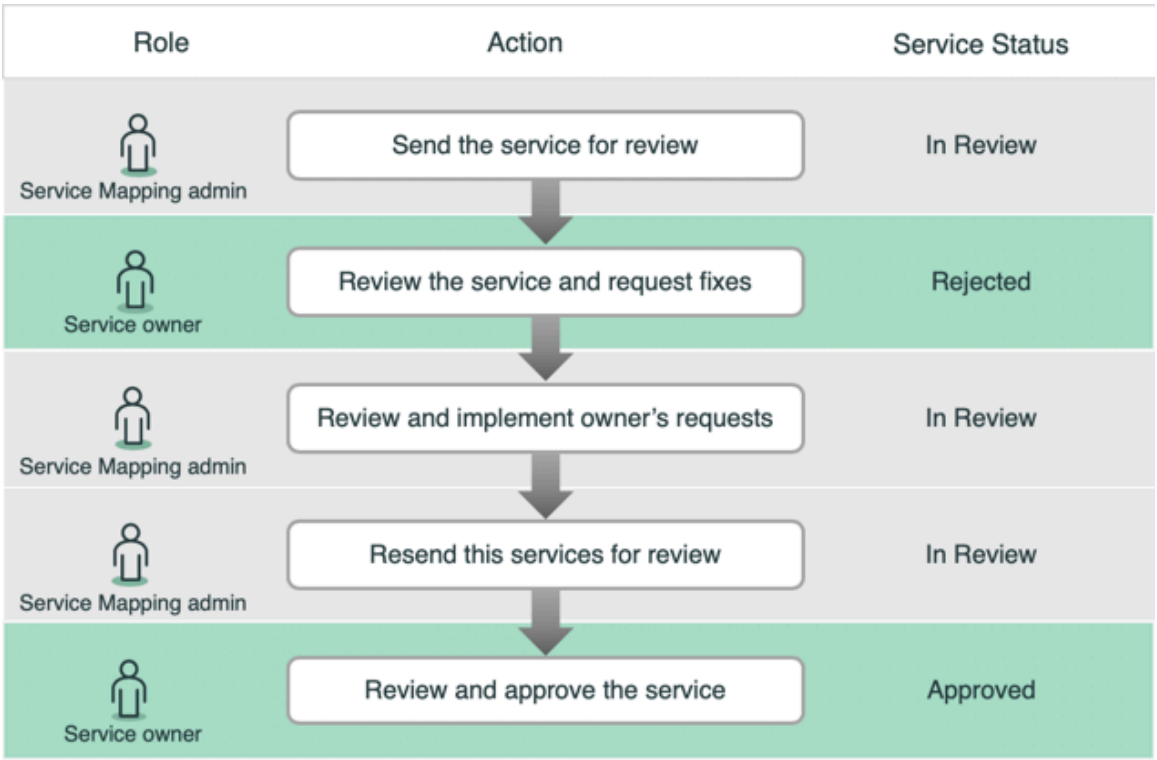
Sie können erkannte und manuell erstellte Serviceinstanzen bearbeiten.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Die Überprüfung von Eigentümeranforderungen ist Teil des Überprüfungs- und Genehmigungsprozesses.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klicken Sie zum Anzeigen der Dokumentation für eine andere Überprüfungsphase auf das entsprechende Feld im Diagramm.



1. Senden Sie für Service zur Überprüfung
2. Überprüfung des folgenden Elements: für Service und Korrekturen anfordern
3. Anwendungsservices erneut zur Überprüfung senden
4. Überprüfen und genehmigen Sie die für Service

Prozedur

1. Navigieren Sie zu dem entsprechenden Anwendungsservice.

   a. Klicken Sie auf der **Startseite** auf **Genehmigen**.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die von Service-Mapping erkannt werden können oder bereits erkannt wurden. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mit der API erstellt wurden.

   b. Klicken Sie auf **Reparatur abgelehnt**.

   c. Klicken Sie mit der rechten Maustaste auf den erforderlichen Anwendungsservice und wählen Sie **Serviceformular öffnen**.
   Das Formular für diesen Anwendungsservice wird geöffnet.

2. Klicken Sie links auf **Nachrichten ablehnen**.
   Die Eigentümerkommentare werden auf der Registerkarte **Service-Discovery-Nachrichten** angezeigt.
3. Überprüfen Sie die Ablehnungsnachrichten, um Kommentare anzuzeigen, die der Eigentümer des Anwendungsservice hinterlassen hat.
4. Klicken Sie auf **Karte anzeigen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Implementieren Sie die vom Eigentümer des Anwendungsservice angeforderten Änderungen.
6. Klicken Sie auf die Discovery-Nachricht, die den von Ihnen behobenen Servicefehler beschreibt, und klicken Sie rechts unter **Aktion für Auswahl** auf **Als gelöst markieren**.
7. Senden Sie den Anwendungsservice gegebenenfalls erneut zur Überprüfung.

CIs einem Anwendungsservice manuell hinzufügen

Fügen Sie Configuration Items (CIs) zu manuell erstellten Anwendungsservices oder zu von Service-Mapping erkannten Services hinzu. Sie können erkannte und manuell erstellte Serviceinstanzen bearbeiten.

Vorbereitungen

- Stellen Sie sicher, dass der CI-Typ für das CI, das Sie hinzufügen möchten, vorhanden ist. Erstellen Sie bei Bedarf den CI-Typ wie in CI-Typen für Service-Mapping und Discovery erstellenbeschrieben.
- Fügen Sie bei Bedarf für das Gerät oder die Anwendung, die Sie hinzufügen möchten, der CMDB CIs hinzu. Weitere Informationen finden Sie unter CMDB füllen .

Erforderliche Rolle: app_service_admin oder service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Um einem Anwendungsservice ein CI hinzufügen zu können, muss eine Beziehung zwischen dem neuen CI und einem CI in dem Anwendungsservice erstellt werden. Sie können einem manuell erstellten Anwendungsservice auf eine der folgenden Arten CIs hinzufügen:

- Methode zum Füllen des Anwendungsservice hinzufügen

  Navigieren zu **CSDM** > **Technologiemanagement-Services verwalten** > **Anwendungsservice**. Wählen Sie einen Anwendungsservice aus, und wählen Sie dann auf der Registerkarte **Anwendungsservice auffüllen** eine Methode zum Füllen des Anwendungsservice aus. Weitere Informationen finden Sie unter Anwendungsservice erstellen .

- Mit der Anwendungsservicezuordnung wie im Folgenden beschrieben

  Der Standardbeziehungstyp der hinzugefügten Verbindung lautet in diesem Fall *Depends on::Used by*. Sie können diesen Standardbeziehungstyp ändern, indem Sie den Wert der Eigenschaft Mit Anwendungsservices installierte Komponenten ändern.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Informationen zu dem CI in dem für Service, mit dem Sie ein neues CI verbinden, werden in der CMDB aktualisiert. Diese Informationen umfassen den Typ der Beziehung zwischen den CIs. Falls andere Anwendungsservices denselben Anwendungsfluss verwenden, erkennt die CMDB dies und fügt das manuell hinzugefügte CI analog zu diesen Anwendungsservices hinzu. Sie haben beispielsweise manuell einen IBM WebSphere Message Broker zu einem IBM WebSphere HTTP-Listener im Kundenportalservice der Bank hinzugefügt. Vom System wird dieser IBM WebSphere Message Broker auch demselben HTTP-Listener im internen Portalservice der Bank hinzugefügt, da dieser HTTP-Listener von ihm verwendet wird. Die gleiche Logik gilt, wenn Sie ein manuell hinzugefügtes CI entfernen: Das System entfernt es aus allen Anwendungsservices, in denen entweder Sie es manuell hinzugefügt haben oder das System es analog hinzugefügt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können ein CI nur manuell mit tatsächlichen CIs verbinden, die in der CMDB vorhanden sind, nicht mit einer Visualisierung anderer Elemente in der Karte wie Cluster oder Grenzen. Außerdem ist es nicht zulässig, einem Anwendungsservice CIs dieser CI-Typen hinzuzufügen:

- cmdb_ci_file_system
- cmdb_ci_network_adapter
- cmdb_ci_storage_device
- cmdb_ci_disk_partition
- cmdb_ci_memory_module
- cmdb_ci_ip_address
- cmdb_ci_storage_pool_member
- dscy_net_base
- cmdb_ci_storage_export
- cmdb_ci_endpoint
- cmdb_ci_translation_rule
- cmdb_ci_qualifier
- cmdb_ci_application_cluster
- cmdb_ci_config_file

Bei Bedarf können Sie verhindern, dass CIs anderer CI-Typen zu Serviceinstanzen hinzugefügt werden, indem Sie die Tabelle Manuelle CI-Einschlüsse/Ausschlüsse [svc_manual_ci_exclusions_inclusions.list] ändern.

In Umgebungen mit Domain Separation werden nur CIs, die zu derselben Domäne gehören, wie der für Service, dem für Service hinzugefügt. Wenn es eine Domänenhierarchie gibt, müssen CIs zur gleichen untergeordneten Domäne gehören wie der für Service.

Wenn Sie mit einem von Service-Mapping erkannten für Service arbeiten, fügen Sie manuell ein CI hinzu:

- Um anzugeben, dass ein für Service ein Gerät oder eine Anwendung enthält, die Service-Mapping nicht erkennen kann. Fügen Sie beispielsweise dem Produktionsflächenservice eine Klimaanlage hinzu.
- Um einen temporären Platzhalter für ein CI hinzufügen, das Service-Mapping nicht ermittelt hat. In diesem Fall planen Sie die erforderliche Fehlerbehebung, um sicherzustellen, dass Service-Mapping dieses CI in der Zukunft ermittelt. Fügen Sie beispielsweise einen IBM WebSphere Message Broker zum Kundenportalservice der Bank hinzu.
- Um einen für Service zu erstellen, der Einstiegspunkte und CIs, die automatisch von Service-Mapping ermittelt wurden, mit Einstiegspunkten und CIs aus der CMDB kombiniert. Nachdem Sie manuell einen Einstiegspunkt hinzugefügt haben, können Sie den für Service mit CIs aus der CMDB basierend auf den dort definierten Beziehungen aktualisieren.

Weitere Informationen zu Service-Mappingfinden Sie unter Musteranpassung und Traffic-basierte Discovery für CI-Typen oder bestimmte CIs aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Klicken Sie bei Bedarf auf **Bearbeiten**, um sicherzustellen, dass sich die Karte im Bearbeitungsmodus befindet.

   Wenn Service-Mapping bereitgestellt ist, wird im Bearbeitungsmodus unterhalb der Zuordnung der Abschnitt „Discovery-Nachrichten“ angezeigt.
3. Um ein CI mit einem anderen CI in der Karte zu verbinden, klicken Sie mit der rechten Maustaste auf das CI, mit dem Sie das neue CI verbinden möchten, und wählen Sie dann **Ein CI hinzufügen** aus.
4. Geben Sie im Dialogfeld „Ein CI hinzufügen“ das hinzuzufügende CI an:

Feld	Beschreibung
CI-Typ	Wählen Sie den CI-Typ (CI-Klasse) für das hinzuzufügende CI aus. Jedes CI gehört zu einem CI-Typ, der eine Reihe von Attributen enthält, die für diese Art von CI konfiguriert wurden. *cmdb_ci_appl* für Anwendungen.
CI-Name	Wählen Sie das CI aus der Liste der CIs des ausgewählten CI-Typs aus. **Hinweis:** Um verzögerte Ergebnisse bei der Suche nach einem bestimmten CI zu vermeiden, sollten Sie Ihre Suche so spezifisch wie möglich gestalten. Eine Suche mit *<name> kann lange dauern und einen großen Datensatz zurückgeben.

   Die Liste der CI-Typen enthält nur zulässige CI-Typen. Sie können beispielsweise keinen Anwendungscluster hinzufügen.
5. Klicken Sie auf **Absenden**.
   Das manuell hinzugefügte CI wird in der Karte angezeigt.

   Hinweis: Wenn Sie ein CI, das eine Anwendung ist, manuell als untergeordnetes Element zu einem Service hinzufügen, der bereits das übergeordnete Anwendungs-CI enthält, wird das neu hinzugefügte untergeordnete Anwendungs-CI in der Inklusion ausgeblendet. Klicken Sie auf das Pluszeichen (+) neben dem übergeordneten Anwendungs-CI, um das untergeordnete Anwendungs-CI anzuzeigen.
6. Wahlweise: Wenn Service-Mapping aktiviert ist, fügen Sie eine erkennbare ausgehende Verbindung für das manuell hinzugefügte CI hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie mit der rechten Maustaste auf das manuell hinzugefügte CI.

b. Wählen Sie **Manuell eine Verbindung hinzufügen**.

> **Hinweis:** Wenn Sie die Option **Manuell eine Verbindung hinzufügen** im Rechtsklick-Menü nicht sehen, stellen Sie sicher, dass Sie mit dem Benutzer angemeldet sind, der zu derselben Domäne gehört wie der Anwendungsservice.

c. Konfigurieren Sie Attribute für den Einstiegspunkt wie in Einstiegspunktattributebeschrieben.

d. Klicken Sie auf **Absenden**.
Discovery und Service-Mapping versuchen, dieses CI zu erkennen. Bei Erfolg wird das CI auf der Karte angezeigt. Andernfalls erscheint ein Warnsymbol (⚠).

7. Wahlweise: Wenn Service-Mapping aktiviert ist und Sie möchten, dass von Service-Mapping ein CI, das Sie zuvor manuell hinzugefügt haben, automatisch erkannt wird:

a. Passen Sie das relevante Muster an, oder optimieren Sie die verkehrsabhängige Erkennung, um Service-Mapping für die Erkennung des CI freizuschalten.

b. Navigieren Sie zur betreffenden für Servicezuordnung.

c. Klicken Sie auf **Discovery ausführen**.

d. Überprüfen Sie nach Abschluss des Erkennung-Prozesses, ob Service-Mapping das CI erkannt hat durch Überprüfen des Connectors, der zum CI führt.
Wenn Service-Mapping das CI erkannt hat, erscheinen zwei Connectors, ein manueller und ein automatisch erkannter, für das CI.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Klicken Sie mit der rechten Maustaste auf das CI, das Sie manuell hinzugefügt haben. In dem Beispiel ist es IBM WebSphere Message Broker.

f. Wählen Sie **Manuell hinzugefügtes CI entfernen**.
Die Karte zeigt das CI mit nur einem Connector, der zu ihm führt. Wenn für dieses CI manuell hinzugefügte Verbindungen vorhanden sind, werden diese zusammen mit dem manuell hinzugefügten CI entfernt.

Zugehörige Informationen

Anwendungsservices verknüpfen

addCI()

Nicht zu Anwendungsservices gehörende CIs entfernen

Entfernen Sie CIs, die fälschlicherweise als Teil eines Anwendungsservice von Service-Mappingzugeordnet wurden. Unnötige CIs in der Zuordnung können irrelevante Warnungen in Ereignismanagementgenerieren. Beispielsweise kann Service-Mapping beim Erstellen eines Anwendungsservice für ein Webportal automatisch eine Verbindung zu nicht verbundenen externen Services wie Paypal erkennen.

Vorbereitungen

Sie entfernen CIs nur aus Anwendungsservices, die von Service-Mapping erkannt wurden.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch Entfernung von CIs aus der Zuordnung werden auch alle zugehörigen Verbindungen entfernt. Wenn Sie beispielsweise ein CI der zweiten Ebene aus der Zuordnung entfernen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden auch alle CIs der dritten Ebene entfernt, die über ausgehende Verbindungen mit ihm verbunden sind.

Je nachdem, warum Service-Mapping ein unerwünschtes CI zugeordnet hat, können Sie es mit den folgenden Methoden entfernen:

- Fügen Sie Zuordnungsgrenzen hinzu, um die unnötigen CIs zu entfernen. Eine Grenze bewirkt, dass Service-Mapping die Erkennung ab diesem Punkt anhält und ausgehenden Verbindungen nicht folgt. Nutzen Sie diese Methode, um CIs zu entfernen, die Service-Mapping anhand von Mustern oder einer datenverkehrsbasierten Erkennung erkannt hat.
- Optimieren Sie die Traffic-basierte Discovery. Service-Mapping kann Konfigurationselemente (CIs) anhand ihrer datenverkehrsbasierten Verbindungen erkennen und zuordnen. Diese Methode wird als datenverkehrsbasierte Zuordnung bezeichnet und ergänzt die musterbasierte Zuordnung. Service-Mapping generiert Verbindungsvorschläge basierend auf datenverkehrsbasierten Verbindungen und der Analyse von Anwendungsfingerabdrücken durch Predictive Intelligence. Wenn die Funktion für Verbindungsvorschläge aktiviert ist, fügt Service-Mapping Anwendungsservices nicht automatisch datenverkehrsbasierte Verbindungen hinzu und bietet Vorschläge. Überprüfen Sie die Vorschläge, und wählen Sie die hinzuzufügenden oder zu entfernenden CIs aus.

  Wenn die Funktion für Verbindungsvorschläge deaktiviert ist, fügt Service-Mapping Anwendungsservices datenverkehrsbasierte Verbindungen und CIs automatisch hinzu. Entfernen Sie Verbindungen, die zu irrelevanten CIs führen, um die Anwendungsservices übersichtlicher zu gestalten.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Entfernen Sie CIs, die nicht zu diesem für Service gehören, indem Sie die folgenden Aktionen ausführen.

Aktion	Schritte
Zuordnungsgrenzen hinzufügen	**a.** Klicken Sie mit der rechten Maustaste auf den Connector, der zu dem CI führt, das Sie entfernen möchten. **b.** Wählen Sie **Grenze markieren** aus. Das CI wird in der Zuordnung als Grenze markiert ( ). **Hinweis:** Vergewissern Sie sich, dass Sie die Zuordnung in der Bearbeitungs-ansicht anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Schritte
(Wenn die Funktion für Verbindungsvorschläge deaktiviert ist) Mithilfe datenverkehrsbasierter Verbindungen erkannte CIs entfernen	**a.** Klicken Sie mit der rechten Maustaste auf das CI in der Zuordnung. **Hinweis:** Sie können datenverkehrsbasierte Verbindungen für ein CI anzeigen, auch wenn Sie die datenverkehrsbasierte Erkennung für einen für Service deaktiviert haben, zu dem das CI gehört. **b.** Wählen Sie **Traffic-basierte Verbindungen anzeigen**. Die Liste der datenverkehrsbasierten Verbindungen wird geöffnet. Weitere Informationen finden Sie unter Liste der datenverkehrsbasierten Verbindungen. **c.** Suchen Sie in der **Liste der Traffic-basierten Verbindungen** nach der Verbindung, die zur Erkennung des unerwünschten CI verwendet wird. **d.** Wählen Sie für diese Verbindung im Feld **Benutzerentscheidung** die Option `Entfernen` aus. **e.** Klicken Sie auf **Schließen**.
(Wenn die Funktion für Verbindungsvorschläge aktiviert ist) Mithilfe datenverkehrsbasierter Verbindungen erkannte CIs entfernen	Führen Sie das unter CIs für einzelne Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen beschriebene Verfahren aus.

Zugehörige Informationen

Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren

Zuordnungssegmente auf andere Anwendungsservices übertragen

Sie können eine Verzweigung eines Service entfernen und auf einen anderen (neuen oder vorhandenen) Anwendungsservice platzieren. Übertragen Sie Zuordnungssegmente, um große Services zu teilen oder Services anders als das ursprüngliche Zuordnungsergebnis zu organisieren.

Vorbereitungen

Sie können erkannte und manuell erstellte Serviceinstanzen bearbeiten.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie ein Zuordnungssegment auf einen anderen Anwendungsservice übertragen, erstellen Sie eine Verknüpfung zwischen dem ursprünglichen Anwendungsservice und dem Anwendungsservice, in den Sie das Zuordnungssegment platziert haben. Die Verbindung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mit dem obersten CI im Segment wird zum Einstiegspunkt, wenn Sie es auf einen anderen (vorhandenen oder neuen) Anwendungsservice übertragen.

Die ursprüngliche Servicezuordnung zeigt den Link zum anderen Anwendungsservice anstelle des Zuordnungssegments. Der Service, der den Verweis enthält, wird zu einem abhängigen Service. Der Service, der als Referenz angezeigt wird, ist ein enthaltener Service.

Wenn Sie ein Zuordnungssegment auf einen anderen Anwendungsservice übertragen, werden die Informationen zur Verbindung mit dem obersten CI im übertragenen Segment in der CMDB aktualisiert. Wenn andere Anwendungsservices dieselbe eingehende Verbindung (Endpunkt) verwenden, erkennt die CMDB dies und ersetzt Zuordnungssegmente, die aus derselben Verbindung stammen, per Analogie mit den verbundenen Service-CIs.

Sie können Links nicht zu mehreren Anwendungsservices aus derselben Verbindung einfügen.

Wenn Sie Ereignismanagement für die Serviceüberwachung in Ihrer Organisation verwenden, enthalten abhängige Anwendungsservices Warnungen, die für die enthaltenen Services generiert wurden.

Prozedur

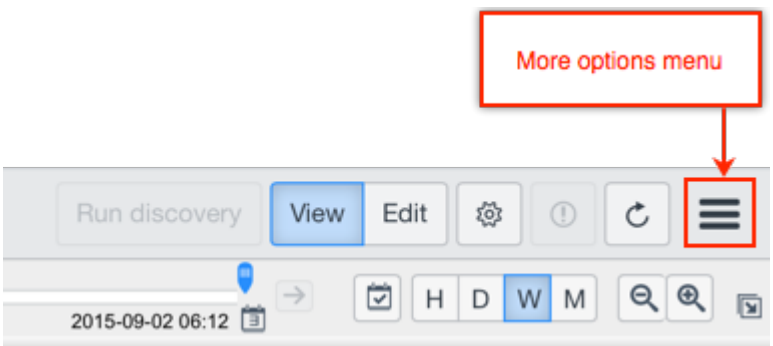
1. Öffnen Sie die Anwendungsservicezuordnung, die das Segment enthält, das Sie übertragen möchten:

   a. Navigieren zu **Service-Mapping** > **Anwendungsservices**.

   b. Klicken Sie auf **Karte anzeigen** neben dem relevanten für Service .

   c. Wahlweise: Klicken Sie auf **Bearbeiten**, um in den Bearbeitungsmodus zu wechseln.

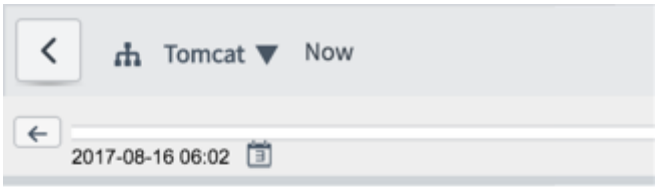
   d. Wenn die Hostansicht aktiviert ist, schalten Sie sie aus, indem Sie zuerst auf **Weitere Optionen** klicken und dann den Schalter für **In Host-Ansicht anzeigen** umschalten.

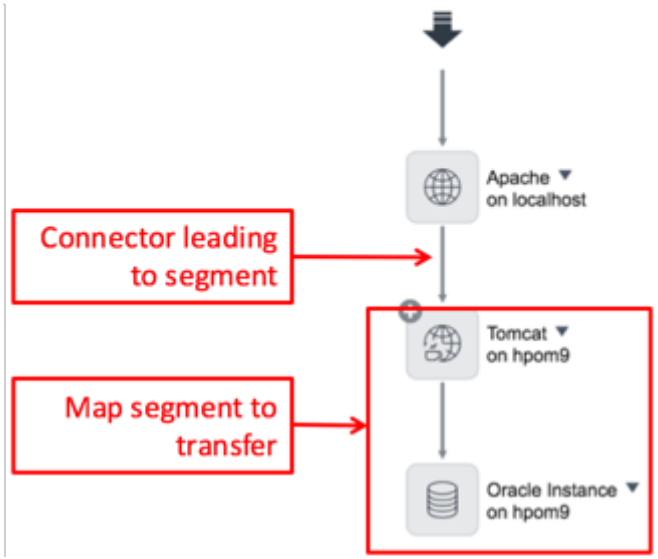


2. Identifizieren Sie das Segment der Zuordnung, das Sie übertragen möchten.
3. Klicken Sie im oberen Bereich dieses Segments mit der rechten Maustaste auf die Verbindung, die zum CI führt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.





4. So übertragen Sie das Segment in eine vorhandene Anwendungsservicezuordnung und stellen eine Verbindung her:

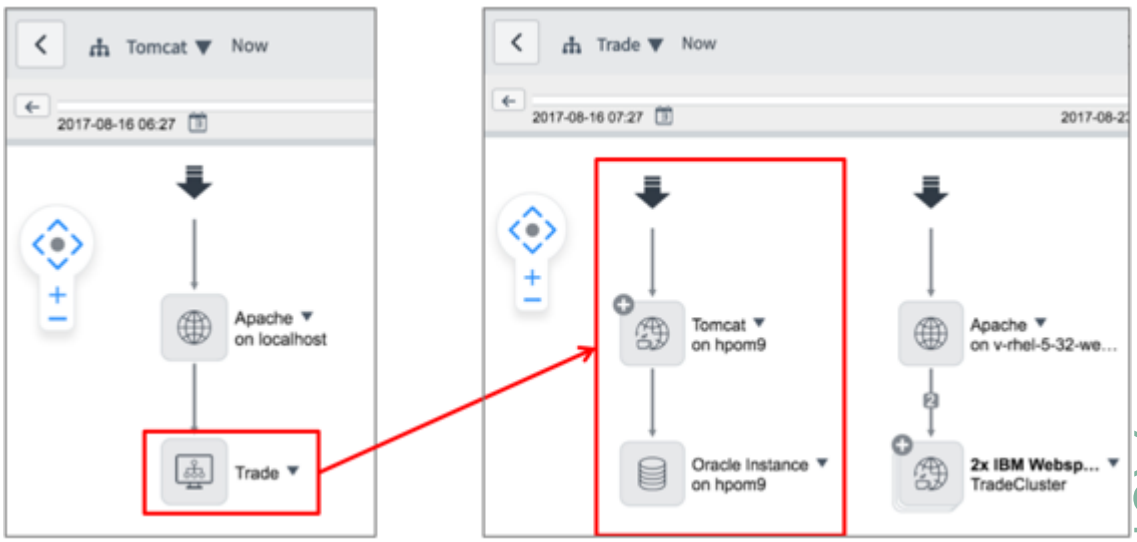
a. Wählen Sie **Mit vorhandenem Service verbinden** aus.

b. Wählen Sie im Fenster „Zu vorhandenem Discovery-Service hinzufügen“ den Anwendungsservice aus, an den Sie das Segment übertragen möchten.

c. Klicken Sie auf **Auswählen**.
Die Zuordnung zeigt das Symbol des enthaltenen Anwendungsservice anstelle des übertragenen Segments an. Die Anwendungsservicezuordnung, an die Sie das Segment übertragen haben, zeigt es unter dem neu hinzugefügten Einstiegspunkt an. Beispielsweise beinhaltet die Anwendungsservicezuordnung „Tomcat“ den Anwendungsservice „Trade“ als enthaltenen Service. Der Anwendungsservice „Tomcat“ wird zu einem vom Service „Trade“ abhängigen Service. Die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservicezuordnung „Trade“ zeigt das Segment, das vom Anwendungsservice „Tomcat“ übertragen wurde.



5. So übertragen Sie das Segment in eine neue Zuordnung des für Service und stellen eine Verbindung her:

a. Wählen Sie **Neuen Service von hier erstellen** aus.

b. Definieren Sie im Fenster „Neuen Discovery-Service erstellen“ Attribute für den für Service, den Sie für dieses Segment erstellen möchten:

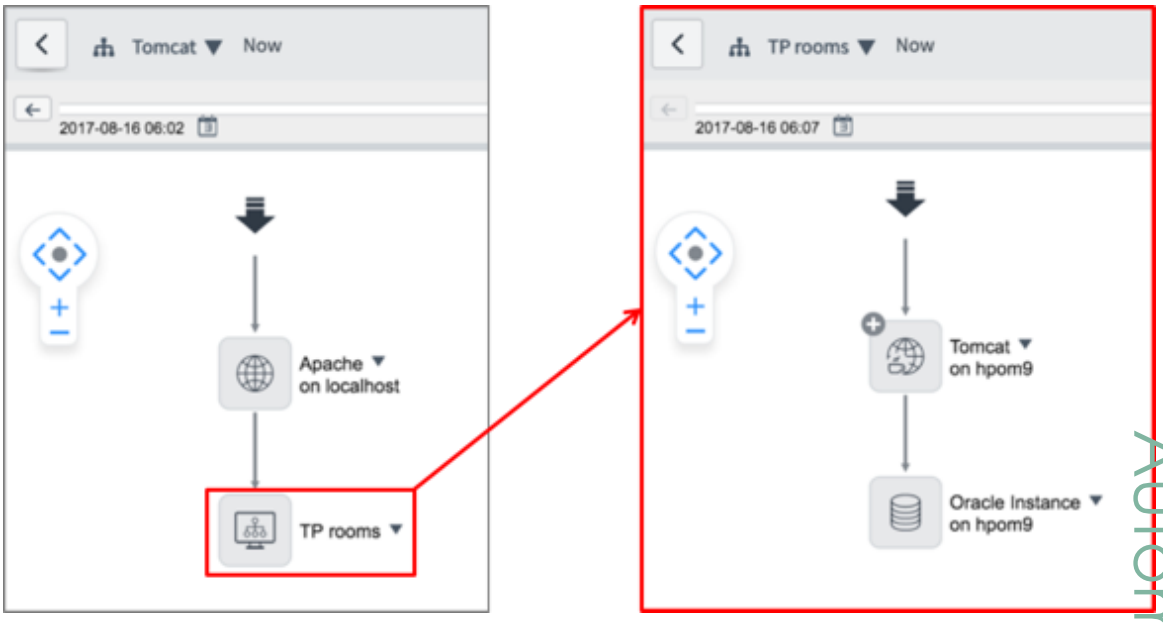
Feld	Beschreibung
Name	Geben Sie den Namen des für Service ein. Dieser Name muss eindeutig sein. Verwenden Sie selbsterklärende Namen wie `Mailing-Service` oder `Druckservice`.
Gruppe	(Optional) Schränken Sie den Zugriff auf einen für Service ein, indem Sie ihn zu einer Gruppe von für Services hinzufügen. Benutzer müssen dann über die Servicegruppenrolle verfügen, um auf den für Service zugreifen zu können.
Relevanz	(Optional) Wählen Sie die Option aus, die widerspiegelt, wie wichtig dieser für Service für den Betrieb Ihrer Organisation ist. Weitere Informationen zur Relevanz von für Services finden Sie unter Wichtigkeit für Anwendungsservices definieren.

c. Klicken Sie auf **Erstellen**.
Die Zuordnung zeigt das Symbol des enthaltenen Anwendungsservice anstelle des übertragenen Segments an. Der neue Anwendungsservice wird in der Liste der Anwendungsservices angezeigt und enthält das übertragene Segment der Zuordnung. Beispielsweise enthält der Anwendungsservice „Tomcat“ den Service „TP Rooms“ als enthaltenen Service. Der Anwendungsservice „Tomcat“ wird zu einem vom Service „TP

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

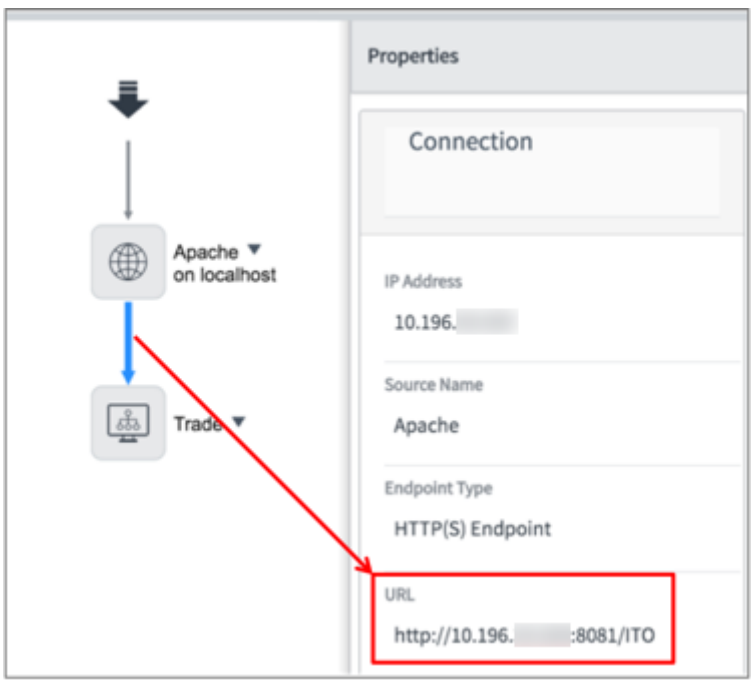
Rooms“ abhängigen Service. Die Anwendungsservicezuordnung „TP Rooms“ enthält das Segment, das vom Anwendungsservice „Tomcat“ übertragen wurde.



Nächste Maßnahme

So machen Sie diesen Vorgang rückgängig:

1. Klicken Sie in der Zuordnung des für Service, die das verbundene Service-CI enthält, auf die Verbindung, die zum CI führt.
2. Beachten Sie im Eigenschaftsbereich das URL-Attribut der Verbindung.



3. Doppelklicken Sie auf das verbundene Service-CI.

   Die Zuordnung des für Service für das CI mit dem übertragenen Segment wird geöffnet.

4. Klicken Sie auf **Formular „Servicezuordnung“**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Suchen Sie unter „Einstiegspunkte“ auf der linken Seite nach dem Einstiegspunkt mit der gleichen URL, die Sie sich notiert haben.
6. Klicken Sie auf der Registerkarte „Einstiegspunkt“ auf **Löschen** und anschließend zur Bestätigung auf **Entfernen**.

   Dieser Einstiegspunkt wird aus dem Formular des für Service entfernt.

   Das übertragene Segment wird aus der Zuordnung dieses für Service entfernt.
7. Navigieren Sie zur Zuordnung, die das verbundene Service-CI enthielt.

   Anstelle des CI für einen verbundenen Service zeigt diese Zuordnung eine Grenze ( ) an.
8. Klicken Sie auf das Grenz-CI und anschließend auf **Markierung für Grenze aufheben**.

   Die Zuordnung wird aktualisiert und zeigt das Segment des für Service an.

Zugehörige Informationen

Abhängige Anwendungsservices in klassisch Service-Mapping anzeigen

Enthaltene Anwendungsservices in klassisch Service-Mapping anzeigen

Benutzerzugriff auf Anwendungsservices steuern

Anwendungsservices verknüpfen

Sie können zwei Anwendungsservices manuell verknüpfen, indem Sie einen Verweis auf einen Anwendungsservice in einen anderen Anwendungsservice einfügen. Der Service, der den Verweis enthält, wird zu einem abhängigen Service. Der Service, den Sie als Referenz einschließen, ist ein enthaltener Service. Sie können Anwendungsservices untereinander verknüpfen, um Abhängigkeiten für die Überwachung der Auswirkungen in Ereignismanagement zu erstellen.

Vorbereitungen

Sie können erkannte und manuell erstellte Serviceinstanzen bearbeiten.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

Vergewissern Sie sich, dass Sie Name und Servicetyp des Anwendungsservice kennen, dem Sie einen Verweis hinzufügen möchten.

Erforderliche Rolle: app_service_admin oder service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Um eine Verbindung herzustellen, fügen Sie einen Verweis auf den Anwendungsservice als ausgehende Verbindung des relevanten CI in dem anderen Anwendungsservice hinzu. Sie können beispielsweise den Anwendungsservice „UK Portal“ als Link zum Anwendungsservice „Online Store“ hinzufügen. In diesem Fall wird der Service „Online Store“ zu einem vom Service „UK Portal“ abhängigen Service bzw. dieser zu einem enthaltenen Service.
Der Service „Online Store“ spiegelt Erkennungsfehler für den enthaltenen Service im Zuordnungsmodus „Bearbeiten“ sowie Warnungen in Ereignismanagement wider.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für verknüpfte Anwendungsservices

Wenn Sie einen Anwendungsservice mit einem anderen Anwendungsservice verbinden, werden die Informationen über das CI, mit dem Sie den Service verknüpft haben, in der CMDB aktualisiert. Die CMDB erkennt andere Anwendungsservices, die denselben Anwendungs-Flow verwenden, und fügt den enthaltenen Anwendungsservice analog zu diesen Anwendungsservices hinzu. Die gleiche Logik gilt, wenn Sie einen enthaltenen Anwendungsservice entfernen: Das System entfernt ihn aus allen Anwendungsservices, in denen entweder Sie diesen Service manuell verknüpft haben oder das System diesen Service analog dazu verknüpft hat.

Wenn Sie Service-Mapping verwenden, möchten Sie möglicherweise Anwendungsservices verknüpfen, um Folgendes zu erstellen:

- Eine Abhängigkeit zwischen zwei Anwendungsservices.
- Einen Platzhalter für einen Kartenteil, den Service-Mapping nicht erkennen konnte. Wenn Sie ein Muster erstellen oder ändern, um das CI zu erkennen, das als Einstiegspunkt für das enthaltene für Service dient, kann Service-Mapping diesen enthaltenen Service erkennen.
- Einen Hinweis darauf, dass ein für Service eine Verzweigung enthält, die Service-Mapping nicht erkennen kann

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können einen für Service bei Bedarf beliebig vielen für Services als enthaltenen Service hinzufügen.

Prozedur

1. Navigieren zu **Service-Mapping** > **Anwendungsservices**.
2. Klicken Sie neben dem zugehörigen Anwendungsservice auf **Karte anzeigen**.
3. Klicken Sie bei Bedarf auf **Bearbeiten**, um sicherzustellen, dass sich die Karte im Bearbeitungsmodus befindet.
4. Klicken Sie mit der rechten Maustaste auf das CI, mit dem Sie einen Anwendungsservice als Referenz verknüpfen möchten.
5. Wählen Sie **CI hinzufügen**.
6. Wählen Sie im Dialogfeld „CI hinzufügen“ den Anwendungsservice aus, den Sie als enthaltenen Service hinzufügen möchten:

Feld	Beschreibung
CI-Typ	Wählen Sie den entsprechenden Servicetyp aus dieser Liste aus: ◦ `Tag-basierter Anwendungsservice` ◦ `Zugeordneter Anwendungsservice` für erkannte oder manuell erstellte Anwendungsservices ◦ `Berechneter Anwendungsservice` für dynamische Services ◦ `Dynamic CI-Gruppe`
CI-Name	Wählen Sie den Namen des Anwendungsservice, den Sie als enthaltenen Service verknüpfen möchten.

7. Klicken Sie auf **Absenden**.
   Das Symbol für den enthaltenen Service wird in der Zuordnung angezeigt.

Zugehörige Informationen

Anwendungsservices

Abhängige Anwendungsservices in klassisch Service-Mapping anzeigen

Enthaltene Anwendungsservices in klassisch Service-Mapping anzeigen

Als generische Anwendungen identifizierte CIs erkennen

Service-Mapping identifiziert Anwendungskonfigurationselemente (CIs), die nicht ordnungsgemäß als generische Anwendungen erkannt wurden. Identifizieren Sie generische Anwendungen korrekt, indem Sie ein vereinfachtes Erkennungsmuster aus einer Anwendungsservicezuordnung erstellen, anstatt mithilfe des Musterdesigners ein vollständig funktionsfähiges Muster von Grund auf neu zu erstellen.

Vorbereitungen

Sie können erkannte und manuell erstellte Serviceinstanzen bearbeiten.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es ist wichtig, dass Sie die Discovery-Prozessklassifizierung verstehen.

Wenden Sie sich an den Eigentümer des Anwendungsservice, um ihn um Informationen über das als generische Anwendung erkannte CI zu bitten.

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird
ServiceNow -Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Configuration Items (CIs) umfassen.

Erstellen Sie im Rahmen der Erstellung eines vereinfachten Musters für die vollständige und ordnungsgemäße Erkennung von Anwendungs-CIs die folgenden erforderlichen Elemente:

CI-Typ

Alle Anwendungen und Hosts in Ihrer Organisation müssen über einen entsprechenden Typ von Konfigurationselement bzw. Configuration Item (CI) verfügen, der dafür erforderlich ist, dass diese Anwendungen und Hosts richtig erkannt und verarbeitet werden. Ein CI-Typ (oder eine Klasse) enthält mehrere wichtige Definitionen, die für alle zugehörigen CIs gelten. Vorkonfigurierte CI-Typen bilden eine Hierarchie, in der untergeordnete CI-Typen Attribute von ihren übergeordneten Elementen ableiten.

Definieren Sie den Namen und die Bezeichnung des CI-Typs für Service-Mapping, um einen untergeordneten CI-Typ für den CI-Typ der Anwendung [cmdb_ci_appl] zu erstellen. Weitere Informationen zu CI-Typen finden Sie unter CI-Typen für Service-Mapping und Discovery erstellen.

Prozessklassifizierung

Service-Mapping nutzt Prozessinformationen, die von Discovery gesammelt und klassifiziert wurden, um relevante Muster zum Erkennen eines Anwendungs-CI auszuführen. Während der horizontalen Erkennung überprüft Discovery, ob die Attribute der von der Anwendung ausgeführten Prozesse den von Ihnen definierten Klassifizierungskriterien entsprechen. Wenn eine Übereinstimmung gefunden wird, verwendet Discovery den vorhandenen Bezeichner der Anwendungsregel, um zu überprüfen, ob das Anwendungs-CI neu ist oder bereits in der CMDB vorhanden ist. Anschließend aktualisiert Discovery entweder einen vorhandenen Datensatz oder erstellt einen neuen Datensatz für dieses Anwendungs-CI in der CMDB.

Vor dem Starten der Top Down-Discovery eines Anwendungs-CI prüft Service-Mapping dessen Prozessklassifizierung im CMDB. Anschließend werden nur die Muster ausgeführt, die für dieses Anwendungs-CI relevant sind.

Erstellen Sie eine Prozessklassifizierung, indem Sie die Klassifizierungskriterien basierend auf vorkonfigurierten Prozessattributen definieren. Die neue Prozessklassifizierung wird der Tabelle „Prozessklassifizierung“ [discovery_classy_proc] hinzugefügt. Informationen zur Prozessklassifizierung finden Sie unter Discovery-Klassifizierer.

Muster

Ein Muster ist eine Folge von Befehlen, deren Zweck darin besteht, Attribute eines CI und seiner ausgehenden Verbindungen zu ermitteln. Wenn Sie ein vereinfachtes Muster für eine generische Anwendung erstellen, weist Service-Mapping das neue vereinfachte Muster dem CI-Typ zu, den Sie als Teil dieses Prozesses definieren. Der Standardname für das Muster beginnt mit „ga_“.

Verknüpfung eines Symbols mit diesem CI-Typ

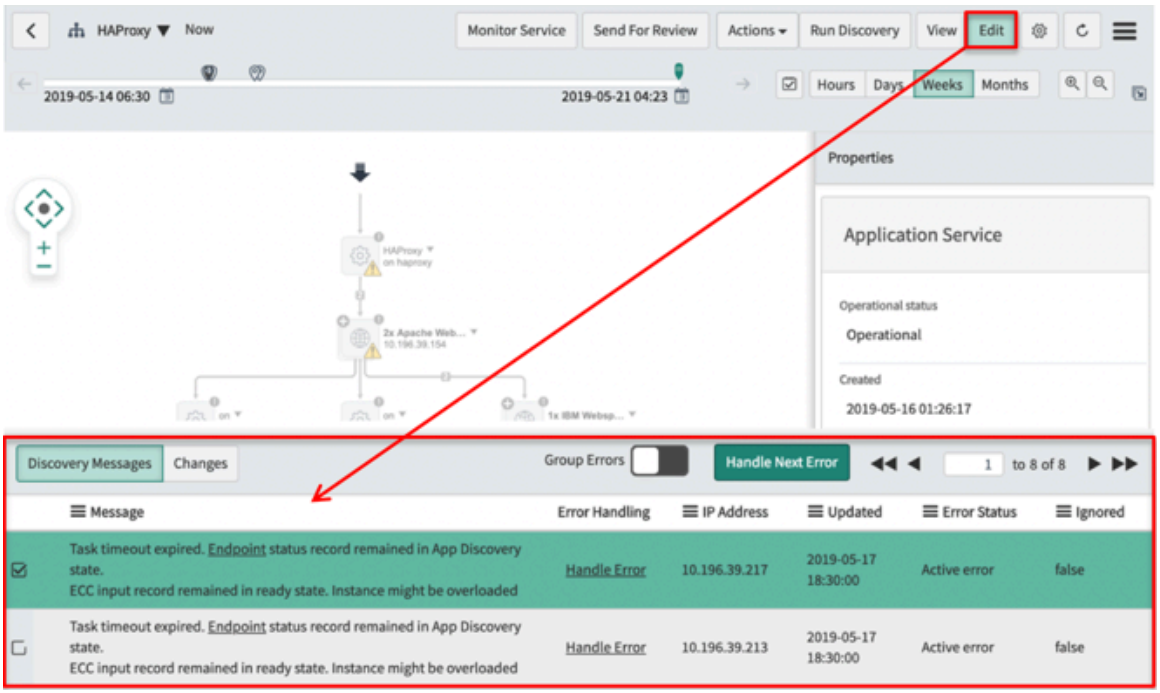
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jeder CI-Typ ist einem Symbol zugeordnet. Wenn ein CI erkannt und als zu einem CI-Typ gehörend klassifiziert wird, zeigt die Zuordnung das zugehörige Symbol zur Darstellung dieses CI an.

Sie können keine vereinfachten Muster aus generischen Anwendungen erstellen, die auf mehreren Prozessen basieren. In diesem Fall müssen Sie entweder ein voll funktionsfähiges Muster mit dem Musterdesigner erstellen oder einen neuen CI-Typ erstellen.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Wahlweise: Klicken Sie auf **Bearbeiten**, um in den Bearbeitungsmodus zu wechseln.



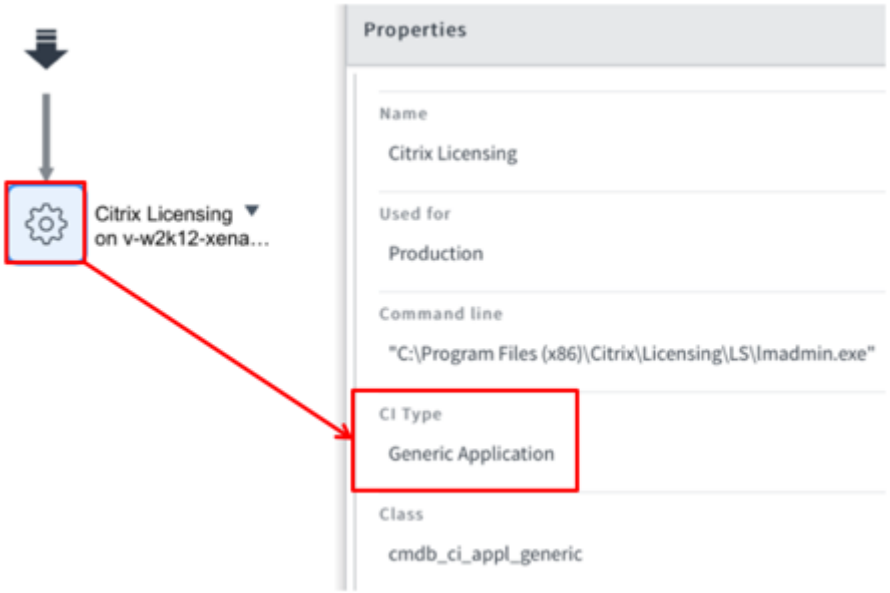
3. Klicken Sie in der Zuordnung mit der rechten Maustaste auf das relevante CI einer generischen Anwendung.

   Das Attribut *CI Type* im Bereich **Anwendung** lautet „Allgemeine Applikation“.

   Im Basissystem zeigt die Zuordnung CIs generischer Anwendungen mit dem Zahnradsymbol an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie **Muster für diese allgemeine Applikation erstellen** aus.
5. Definieren Sie den CI-Typ für die Anwendung.

Feld	Beschreibung
Bezeichnung	Name des CI-Typs. Beispiel: „Citrix-Lizenzierungsserver“
Name	Der Tabellenname, der Daten für diesen CI-Typ enthält. Beispiel: cmdb_ci_app_license_server. Verwenden Sie einen Namen, der mit vorhandenen CI-Typnamen übereinstimmt. Normalerweise beginnen CI-Typnamen mit „cmdb_ci_app“.
Symbol	Wählen Sie den Namen des vorhandenen Symbols aus, mit dem diese Anwendung in Zuordnungen dargestellt werden soll.

6. Erstellen Sie die Prozessklassifizierung für dieses CI, indem Sie Klassifizierungskriterien zur Identifizierung des Prozesses definieren, der von der generischen Anwendung ausgeführt wird.
   Im Basissystem gibt es zwei Bedingungen, die auf dem Namen und dem Befehl des laufenden Prozesses basieren. Die Werte werden von der letzten Prozesserkennung eingetragen.

   a. Wählen Sie das CI-Attribut aus der Liste aus.
      Die Attribute in der Liste stammen aus der Tabelle „Laufender Prozess“ [cmdb_running_process].

   b. Wählen Sie einen Operator aus der Liste aus.
      Wenn Sie `Ist Leer` auswählen, wird das zweite Feld irrelevant und wird ausgeblendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Geben Sie den Wert für die Übereinstimmung an.
Das Wertfeld zeigt einen dynamisch generierten Vorschlag aus der letzten Prozesserkennung an.

d. Zum Hinzufügen einer abhängigen Bedingung klicken Sie auf **ODER** oder **UND**.

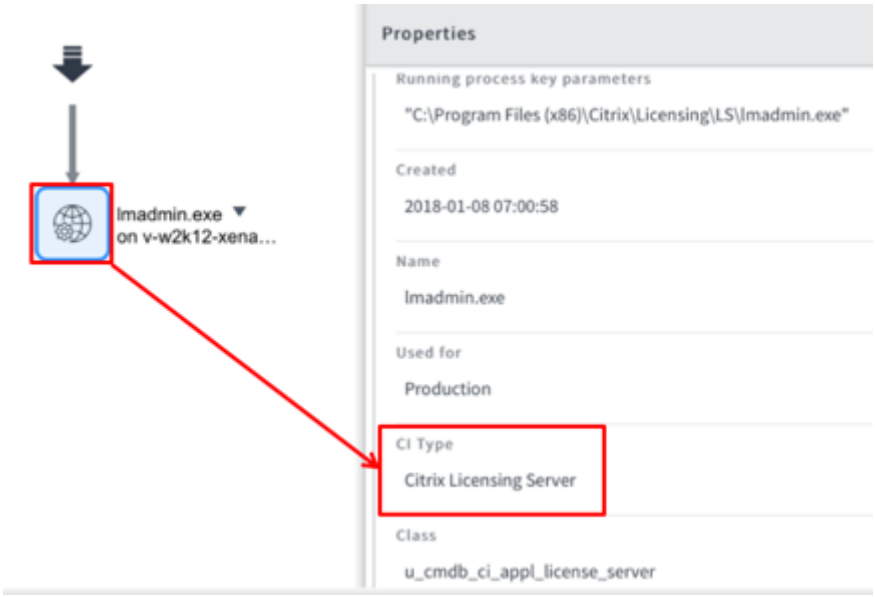
Hinweis: Wenn der Wert in der ersten Bedingung nicht eindeutig ist (Beispiel: „Java.exe"), verwenden Sie zusätzliche Bedingungen, um die Ergebnisse einzugrenzen.

Um beispielsweise einen Citrix-Lizenzierungsserver zu erkennen, verwenden Sie die folgenden Klassifizierungskriterien: den Prozessnamen `lmadmin.exe` mit dem Befehl `C:\Programmdateien (x86)\Citrix\Licensing\LS\lmadmin.exe`.

e. Um eine Bedingung auf oberster Ebene hinzuzufügen, klicken Sie auf **Neue Kriterien**.

7. Klicken Sie auf **Erstellen**.
Sobald Service-Mapping die Erstellung von CI-Typ, Muster und Prozessklassifizierung abgeschlossen hat, wird die Erkennung des CI fortgesetzt, das ursprünglich als generische Anwendung identifiziert wurde.
8. Vergewissern Sie sich, dass Service-Mapping das CI erwartungsgemäß erkannt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beachten Sie, dass Service-Mapping den Namen des Prozesses für die CI-Bezeichnung in der Zuordnung verwendet.

Nächste Maßnahme

Wenn Service-Mapping das CI immer noch nicht wie erwartet erkannt hat, müssen Sie die Übereinstimmungs- und Klassifizierungskriterien für den Prozessklassifizierer feinabstimmen und erweiterte Klassifizierungsparameter konfigurieren.

Wenn Sie mit dem Ändern von Mustern im Musterdesigner vertraut sind, können Sie das vereinfachte Muster auch erweitern, indem Sie Vorgänge definieren, die weitere Attribute für das CI erkennen.

Sie können Discovery so konfigurieren, dass ein anderer Bezeichner verwendet wird. Weitere Informationen finden Sie unter Discovery-Bezeichner.

Zugehörige Informationen

Musterbasierte Erkennung in Service-Mapping

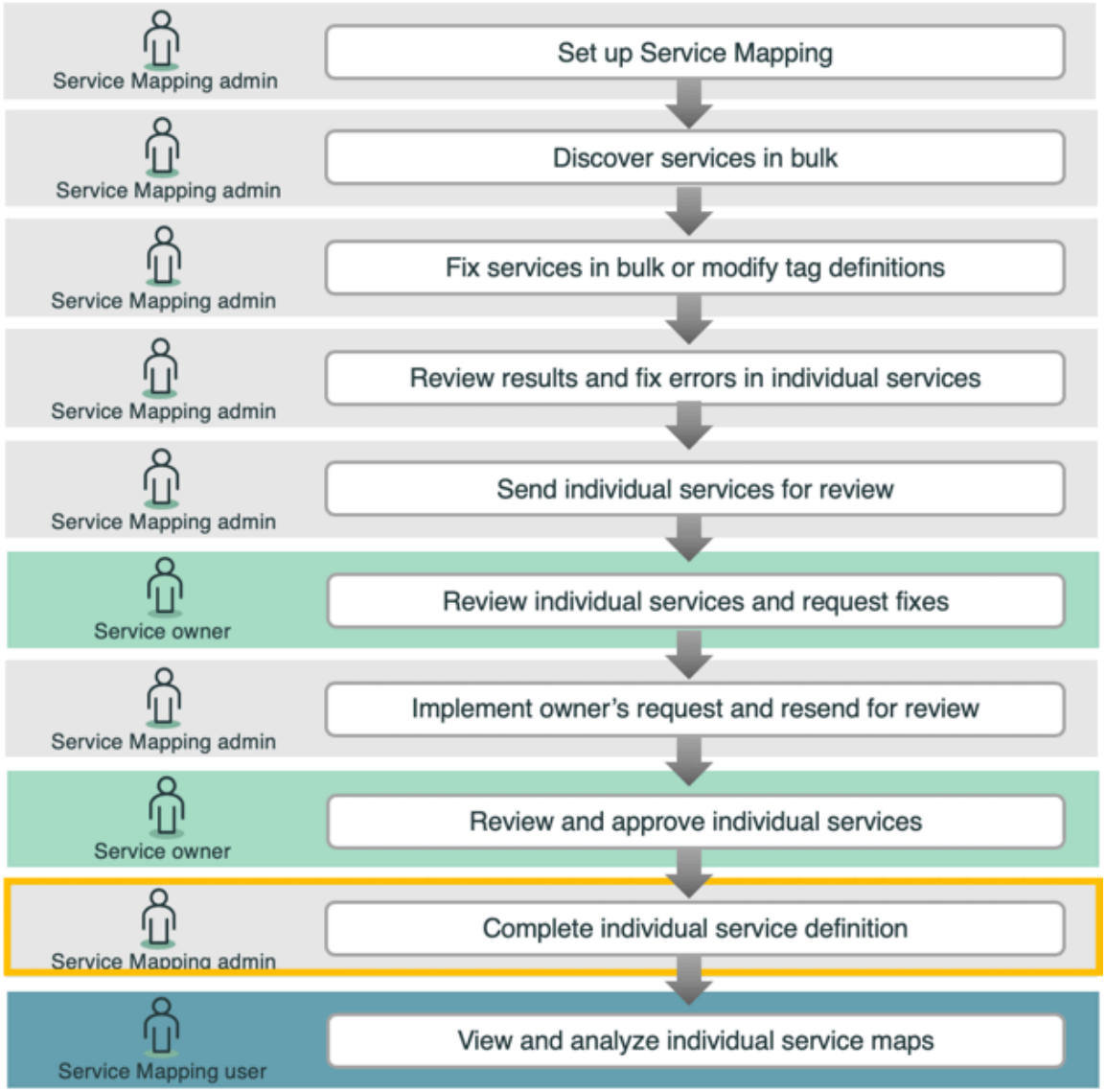
Fertigstellung des Anwendungsservice

Nachdem ein Anwendungsservice geprüft und genehmigt wurde, können Sie Attribute definieren, die seine Erkennung verbessern, seine Bedeutung widerspiegeln und den Zugriff auf ihn steuern.

Es gibt mehrere Konfigurationen, die Sie ausführen müssen, um die Definition eines Anwendungsservice abzuschließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping-Workflow



Automatische Übersetzung

Wichtigkeit für Anwendungsservices definieren

Wählen Sie für jede Serviceinstanz eine Relevanzstufe aus, die widerspiegelt, wie wichtig sie für Ihre Unternehmensabläufe ist.

Vorbereitungen

Bestimmen Sie, wie wichtig der Anwendungsservice für Ihr Unternehmen ist.

Erforderliche Rolle: service_mapping_admin

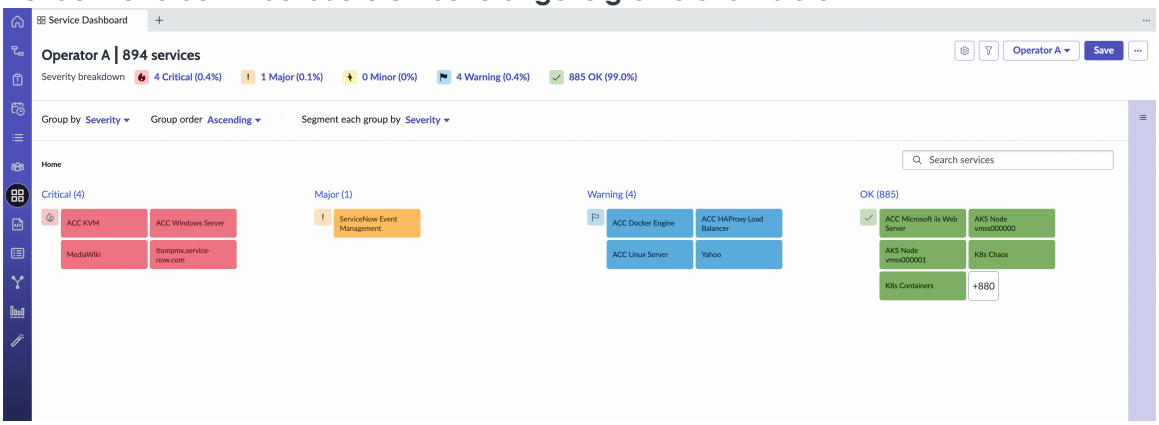
Warum und wann dieser Vorgang ausgeführt wird

In der Regel können Sie Serviceinstanzen, die sich auf Ihren Kundenstamm oder Ihren Umsatz auswirken, eine hohe Relevanz zuweisen, während Sie internen Serviceinstanzen, die den Mitarbeitern der Organisation geringfügige Unannehmlichkeiten bereiten, eine niedrige Relevanz zuweisen. Beispielsweise können Sie für eine Serviceinstanz, die Vertriebsfunktionen über die Organisationswebsite unterstützt, eine hohe Relevanz festlegen. Eine Serviceinstanz, die internes Drucken für die Mitarbeiter der Organisation bereitstellt, kann eine geringe Relevanz erhalten.

Sie können auch einen Kritikalitätswert verwenden, um Wiederherstellungsstrategien zu definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der Betreiber-Arbeitsbereich-Seite angezeigte Relevanzstufen



Prozedur

1. Führen Sie in der klassischen Umgebung die folgenden Schritte aus:

   a. Navigieren zu **Alle** > **Service-Mapping** > **Startseite**.
   Auf der Homepage werden nur Informationen zu Serviceinstanzen angezeigt, die von Service-Mapping erkannt werden können oder bereits erkannt wurden. Auf der Homepage werden keine Informationen zu Serviceinstanzen angezeigt, die manuell oder mit der API erstellt wurden.

   b. Klicken Sie auf der Kachel **Abgeschlossen** auf **Ihre Services anzeigen**.

   c. Wählen Sie den entsprechenden Anwendungsservice.

   d. Klicken Sie auf **Zusätzliche Informationen**.

   e. Wählen Sie die entsprechende Option aus der Liste **Geschäftsrelevanz** aus.

   f. Klicken Sie auf **Aktualisieren**.

2. Alternativ führen Sie die folgenden Schritte in der Mitarbeiterbereich-Benutzeroberfläche aus:

   a. Navigieren zu **Mitarbeiterbereich** > **Mitarbeiterbereich-Startseite**.

   b. Klicken Sie im linken Bereich auf **Listen**.

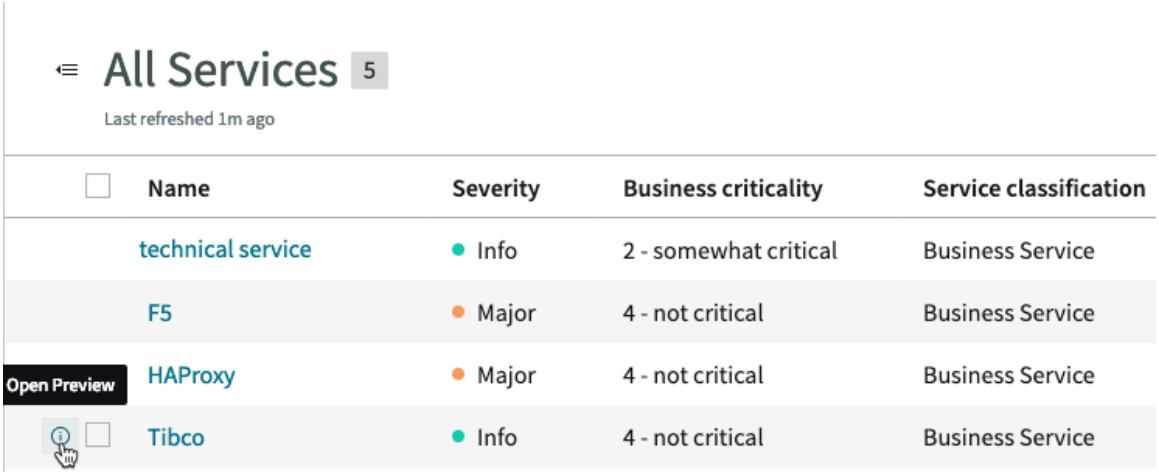
   c. Navigieren zu **Services** > **Alle Services**.
   Die Liste der Services zeigt Services im Status „Betriebsbereit“ an.

   d. Wählen Sie den entsprechenden Anwendungsservice.

   e. Klicken Sie auf das Symbol **Vorschau öffnen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Detailbereich wird auf der rechten Seite geöffnet.

f. Wählen Sie die entsprechende Option aus der Liste **Geschäftsrelevanz** aus.

g. Klicken Sie auf **Aktualisieren**.

Gruppen-Anwendungsservices

Organisieren Sie Anwendungsservices nach Gruppen, um Aktionen für mehrere Services gleichzeitig auszuführen und den Benutzerzugriff auf Services zu steuern. Sie können Ereignismanagement verwenden, um die Serviceintegrität nach Servicegruppen nachzuverfolgen.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin oder app_service_admin

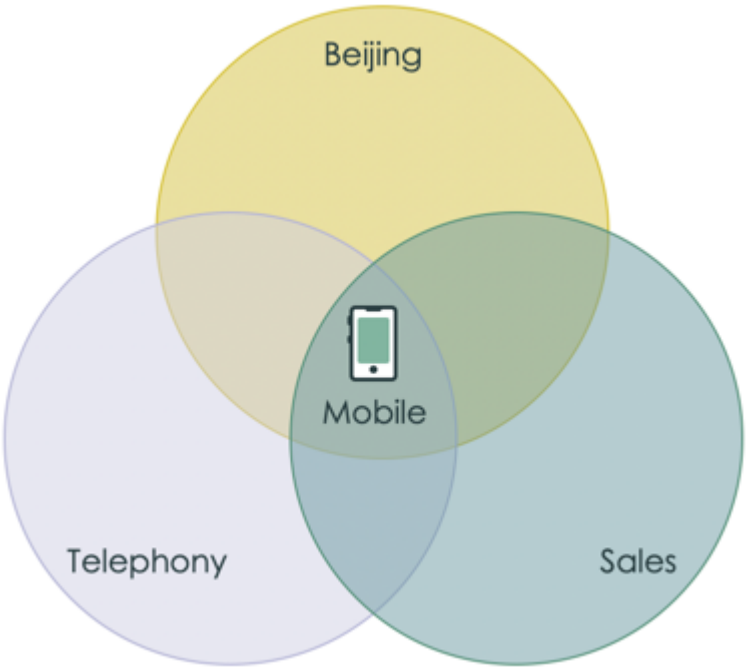
Warum und wann dieser Vorgang ausgeführt wird

In der Regel verfügen Unternehmen über Hunderte von Services, sodass es nicht praktikabel ist, sie einzeln zu verwalten. Servicegruppen können Servicelisten wesentlich kürzer machen und einfacher verwalten, insbesondere in großen Organisationen oder Diensteanbietern.

Wie Sie Serviceinstanzen gruppieren, hängt vom Benutzer und von den Richtlinien zur Servicebereitstellung in Ihrem Unternehmen ab. Die Beziehung zwischen Serviceinstanzen in Gruppen ist rein logisch, und dieselbe Serviceinstanz kann mehreren Gruppen angehören. Zum Beispiel kann der Mobile-Service zu den folgenden Servicegruppen gehören: Vertrieb, Peking und Telefonie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine Serviceinstanz, die verschiedenen Gruppen angehört



Sie können eine Servicegruppe in eine andere Servicegruppe einbetten, um eine Hierarchie von Servicegruppen zu erstellen. Wenn Benutzer Zugriff auf eine übergeordnete Servicegruppe haben, haben sie automatisch Zugriff auf alle untergeordneten Gruppen. Standardmäßig werden alle neuen Services der Servicegruppe **Alle** zugewiesen, mit der alle Benutzer Serviceinstanzen anzeigen und verwalten können. Wenn Sie einer Servicegruppe eine Rolle zuweisen, können die Benutzer mit dieser Rolle auf Serviceinstanzen in dieser Servicegruppe und in der Servicegruppe **Alle** zugreifen. Um Benutzern mit dieser Rolle den Zugriff auf andere Services zu ermöglichen, weisen Sie diese Rolle der jeweiligen Servicegruppe zu. Weisen Sie der Servicegruppe **Alle** keine Anwenderrollen direkt zu.

Wenn Service-Mapping aktiviert ist, können Servicegruppen eine Mischung von manuell erstellten Anwendungsservices und den von Service-Mapping erkannten Anwendungsservices enthalten.

Sie können Now Platform Benachrichtigungen verwenden, um Benutzer zu warnen, wenn der Servicegruppenschweregrad zu „kritisch“ geändert wird. Der Gesamtschweregrad der Gruppe wird durch den höchsten Warnungsschweregrad innerhalb der Gruppe bestimmt.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **Applikationsservices** > **Servicegruppen**.
2. Klicken Sie auf **Neu**.
3. Geben Sie den Namen der neuen für Service-Gruppe im Feld **Name** ein.
4. Um diese Gruppe in eine andere Gruppe einzubetten, geben Sie den Namen der anderen Gruppe in dem Feld **Übergeordnete Gruppe** ein.
5. Klicken Sie mit der rechten Maustaste auf die Kopfzeile des Formulars, und klicken Sie auf **Speichern**.
6. Fügen Sie der neu erstellten Servicegruppe eine Serviceinstanz hinzu.

   a. Klicken Sie im Abschnitt Servicegruppenmitglieder auf **Neu**.

   b. Geben Sie im Feld **Name** den Namen der Serviceinstanz ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie Ereignismanagement verwenden, können Sie auch einen Benachrichtigungs-Gruppennamen eingeben.

c. Klicken Sie auf **Absenden**.

7. Alternativ können Sie eine Serviceinstanz aus dem Formular „Serviceinstanz“ einer Gruppe hinzufügen.
   a. Navigieren zu **Alle** > **Konfiguration** > **Serviceinstanzen** > **Serviceinstanzen**.
   b. Wählen Sie die Serviceinstanz aus, die Sie einer Servicegruppe hinzufügen möchten.
   c. Im Abschnitt **Servicegruppenmitglieder** doppelklicken Sie **Neue Zeile einfügen**.
   d. Geben Sie den Namen der Servicegruppe ein, der Sie die ausgewählte Serviceinstanz hinzufügen möchten.
   e. Klicken Sie auf das Symbol **OK** ( ).
   f. Klicken Sie auf **Aktualisieren**.

Benutzerzugriff auf Anwendungsservices steuern

Weisen Sie Servicegruppen Benutzerrollen zu, um Benutzern Zugriff auf Anwendungsservices in Ihrer Organisation zu gewähren. Ihre Organisation kann aus Sicherheits- oder Geheimhaltungsgründen den Zugriff auf bestimmte Services einschränken.

Vorbereitungen

Stellen Sie sicher, dass Sie die Benutzerbereitstellungsaufgaben für die Benutzer ausgeführt haben, denen Sie Zugriff gewähren möchten:

1. Fügen Sie Anwender zu Anwendergruppen hinzu .
2. Erstellen Sie neue Rollen .
3. Weisen Sie Anwendern oder Anwendergruppen Rollen zu .

Stellen Sie außerdem sicher, dass Sie Servicegruppen erstellt haben, wie in Gruppen-Anwendungsservices beschrieben.

Erforderliche Rolle: app_service_admin oder service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Im Basissystem bieten die folgenden Rollen Zugriff auf Anwendungsservices:

app_service_admin

Erstellt und ändert Serviceinstanzen, erstellt Servicegruppen, zeigt Serviceinstanzzuordnungen an und bearbeitet sie.

app_service_user

Zeigt Zuordnungen für funktionsfähige Serviceinstanzen an und ruft Serviceinhalte mithilfe der getContent - GET REST API ab. Die ITIL-Rolle, die als die grundlegende Help Desk-Technikerrolle dient, enthält die Rolle „app_service_user“.

Service-Mapping bietet diese vorkonfigurierten Rollen:

service_mapping_admin

Richtet die Service-Mapping-Anwendung ein. Ermöglicht die Zuordnung, Korrektur und Wartung von Serviceinstanzen. Führt auch eine erweiterte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration und Anpassung des Produkts durch. Weisen Sie diese Rolle Anwendungsadministratoren zu.

service_mapping_user

Zeigt Zuordnungen für funktionsfähige Serviceinstanzen an, um Change oder Migration zu planen und die Kontinuität und Verfügbarkeit von Services zu analysieren. Weisen Sie diese Rolle Anwendungsbenutzern zu.

sm_app_owner

Stellt Informationen bereit, die für die erfolgreiche Zuordnung einer Serviceinstanz erforderlich sind. Wenn ein Dienst zugeordnet ist, überprüft dieser Benutzer die Ergebnisse und genehmigt sie entweder oder schlägt Änderungen vor. Weisen Sie die Rolle sm_app_owner Benutzern zu, die Besitzer von Serviceinstanzen sind und mit der Infrastruktur und den Anwendungen vertraut sind, aus denen die Services bestehen.

Hinweis: Benutzer mit der Rolle „itil“ können alle Serviceinstanzen anzeigen.

Ereignismanagement bietet diese vorkonfigurierten Rollen:

evt_mgmt_admin

Hat Lese- und Schreibzugriff auf alle Ereignismanagement-Funktionen zum Konfigurieren von Ereignismanagement.

evt_mgmt_operator

Neben den evt_mgmt_user-Berechtigungen können auch Vorgänge für Warnungen wie Bestätigen, Schließen, Öffnen von Vorfällen und Ausführen von Korrekturen aktiviert werden.

evt_mgmt_user

Hat Lesezugriff auf alle Ereignismanagement-Funktionen. Hat Schreibzugriff auf Alarme, um die Alarmlebensdauer zu verwalten. Hat die Rolle, um Vorfälle verwalten zu können, die aus Alerts erstellt werden.

evt_mgmt_integration

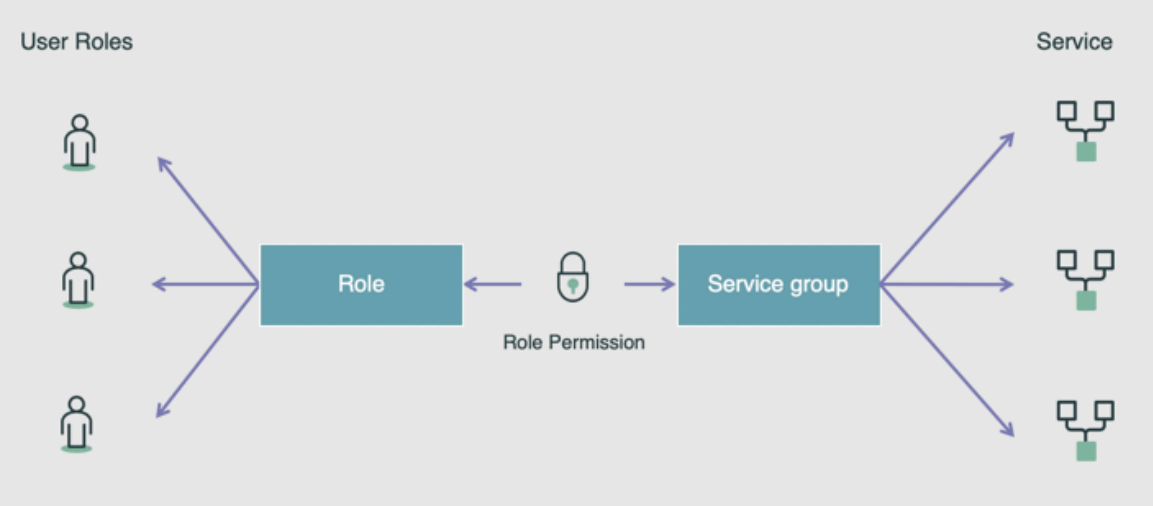
Hat Zugriff auf die Tabellen Event [em_event] und Registered Nodes [em_registered_nodes], um sie mit externen Ereignisquellen zu integrieren.

In der Regel verfügen Unternehmen über Hunderte von Services, sodass es nicht praktikabel ist, sie einzeln zu verwalten. Servicegruppen können Servicelisten wesentlich kürzer machen und einfacher verwalten, insbesondere in großen Organisationen oder Diensteanbietern. In einer Hierarchie von Servicegruppen gewährt der Zugriff auf eine übergeordnete Servicegruppe automatisch Zugriff auf alle untergeordneten Servicegruppen.

Benutzer erben Berechtigungen von Rollen, die ihnen zugewiesen sind. Sie können einige Rollen direkt Servicegruppen zuweisen, damit alle Benutzer mit dieser Rolle auf alle Anwendungsservices zugreifen können, die zu dieser Gruppe gehören. Die meisten Unternehmen entscheiden sich jedoch dafür, ihre Rollen als Hierarchie zu organisieren. Es ist hilfreich, Rollen über mehrere ServiceNow Anwendungen zu verwalten. Beispielsweise kann der Service-Mapping -Administrator [service_mapping_admin] Teil einer umfassenderen Administratorrolle wie dem -Administrator [admin] sein. Sie können Benutzer zu Benutzergruppen hinzufügen und dann den Benutzergruppen Rollen zuweisen, um allen Gruppenbenutzern gleichzeitig Berechtigungen dieser Rolle zu erteilen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einer Anwendungsservicegruppe eine Rolle zuweisen



Standardmäßig werden alle neuen Services der Servicegruppe **Alle** zugewiesen, mit der alle Benutzer Serviceinstanzen anzeigen und verwalten können. Wenn Sie einer Servicegruppe eine Rolle zuweisen, können die Benutzer mit dieser Rolle auf Serviceinstanzen in dieser Servicegruppe und in der Servicegruppe **Alle** zugreifen. Um Benutzern mit dieser Rolle den Zugriff auf andere Services zu ermöglichen, weisen Sie diese Rolle der jeweiligen Servicegruppe zu. Weisen Sie der Servicegruppe **Alle** keine Anwenderrollen direkt zu.

Prozedur

1. Navigieren Sie zu einem der folgenden Elemente:
   - **Konfiguration** > **Applikationsservices** > **Zuständigkeiten der Servicegruppe**.
   - Wenn Service-Mapping aktiviert ist: **Service-Mapping** > **Services** > **Zuständigkeiten der Servicegruppe**.
   - Wenn Ereignismanagement aktiviert ist: **Ereignismanagement** > **Services** > **Zuständigkeiten der Servicegruppe**.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular „Zuständigkeiten der Anwendungsservicegruppe“ aus.

Feld	Beschreibung
Anwendungsservice-Gruppe	Servicegruppe, der Sie eine Rolle zuweisen möchten.
Rolle	Rolle, die Sie der ausgewählten Servicegruppe zuweisen möchten. Zum Beispiel financial_services_admin.

3. Klicken Sie auf **Absenden**.

Example:

So verwalten Sie den Zugriff auf Services, die vertrauliche Finanzinformationen in Ihrer Organisation enthalten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Organisieren Sie die Services in der Gruppe „Finanzservices“.
2. Erstellen Sie eine neue Benutzerrolle, die Rolle des Finanzservice-Administrators [financial_services_admin], die die Rolle [app_service_admin] enthält.
3. Weisen Sie die Administratorrolle „Finanzservices“ der Gruppe „Finanzservices“ zu.

Damit können nur Benutzer mit der Administratorrolle „Finanzservices“ auf Anwendungsservices zugreifen, die zu der Gruppe „Finanzservices“ gehören.

Erkennung von oben nach unten mithilfe von Service-Mapping planen

Nachdem Service-Mapping Konfigurationselemente (CIs) erkannt hat, die zu Ihrer Serviceinstanz gehören, wird die Erkennung der CIs erneut durchgeführt, damit Änderungen und Aktualisierungen ermittelt werden können. Erstellen oder ändern Sie Discovery-Zeitpläne, um zu steuern, wie oft Service-Mapping-Services oder CIs neu erkannt werden. Sie können beispielsweise anwenderdefinierte Discovery-Zeitpläne erstellen, um eine redundante Belastung der Infrastruktur zu vermeiden.

Vorbereitungen

Definieren Sie Anwendungsservices, bevor Sie Erkennungszeitpläne für die Erkennung von CIs definieren, die Teil dieser Services sind.

Stellen Sie beim Erstellen eines Zeitplans für CI-Typen oder für bestimmte CIs sicher, dass sich mindestens ein Anwendungsservice, der das entsprechende CI enthält, im Status *operational* befindet.

Erfahren Sie mehr über die verschiedenen Arten von Top Down-Discovery-Zeitplänen.

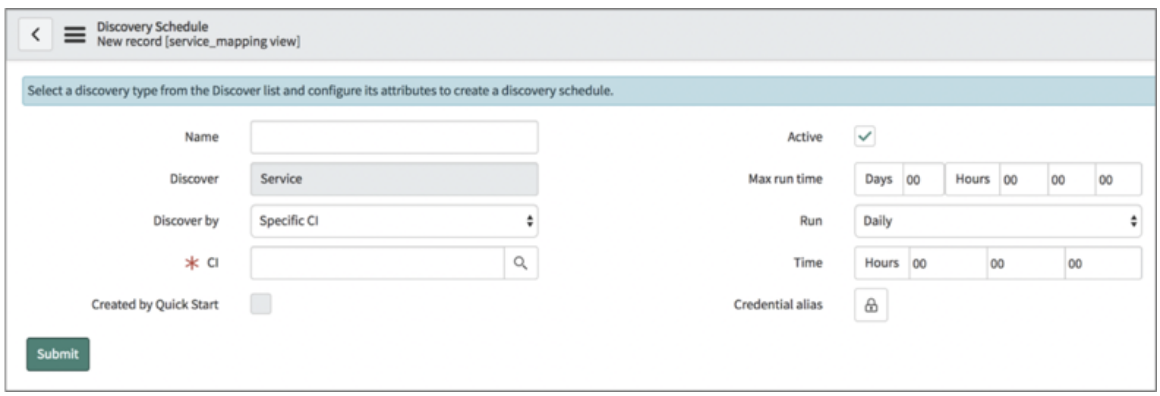
Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Service-Mapping** > **Administration** > **Discovery-Zeitpläne**.
2. Um einen neuen Erkennungszeitplan zu erstellen, klicken Sie auf **Neu**.
   Oder

   Klicken Sie zum Anpassen des generischen Zeitplans für alle Anwendungs-CIs auf **Alle Applikationen** oder **Load Balancer-Service**.



3. Füllen Sie in neu installierten oder zurückgesetzten Instanzen die Felder im Formular „Discovery-Zeitplan“ wie folgt aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie für einen neuen spezifischen Zeitplan einen eindeutigen und beschreibenden Namen ein.
Erkennen	Standardmäßig ist der Wert für dieses Feld `Service`, wodurch angegeben wird, dass Sie den Zeitplan für eine Erkennung von oben nach unten erstellen. Sie können diesen Wert nicht ändern.
Erkennen bis	Die Zeitplantypen für eine bestimmte Top Down-Discovery: ◦ CI-Typ ◦ Spezifischer CI ◦ Serviceattribute ◦ Servicegruppenattribute
CI-Typ	Dieses Feld ist verfügbar, wenn unter „Select Discovery (Erkennung auswählen)“ die Option „CI-Typ“ ausgewählt ist. Wählen Sie für einen neuen CI-Typ-basierten Zeitplan den entsprechenden Anwendungs-CI-Typ aus der Liste aus.
CI	Dieses Feld ist verfügbar, wenn `Spezifisches CI` unter **Erkennen nach**ausgewählt wird. Wählen Sie für einen neuen Zeitplan für ein bestimmtes CI das entsprechende CI aus der Liste aus.
Zu erkennende Services filtern	Dieser Bereich enthält den Bedingungsgenerator und ist verfügbar, wenn `Serviceattribute` unter **Erkennen von ausgewählt**werden. Verwenden Sie den Filter, um die Filterkriterien für Services zu erstellen. Service-Mapping erkennt nur Services, die die definierten Kriterien erfüllen.
Zu erkennende Gruppen filtern	Dieses Feld enthält den Bedingungsgenerator und ist verfügbar, wenn `Servicegruppenattribute` unter **Erkennen von**ausgewählt werden. Verwenden Sie den Filter, um die Filterkriterien für Servicegruppen zu erstellen. Service-Mapping erkennt nur Services, die zu den Gruppen gehören, die die definierten Kriterien erfüllen.

4. Wahlweise: Um einen Discovery-Zeitplan basierend auf Serviceattributen zu erstellen, klicken Sie auf **Ausgewählte Services anzeigen**, um eine Vorschau der Liste der Services anzuzeigen, die den von Ihnen eingegebenen Filterkriterien entsprechen, und wählen Sie **Schließen**aus.
5. Wahlweise: Um einen Discovery-Zeitplan basierend auf Servicegruppenattributen zu erstellen, klicken Sie auf **Ausgewählte Gruppen anzeigen**, um eine Vorschau der Liste der Gruppen anzuzeigen, die den eingegebenen Filterkriterien entsprechen, und wählen Sie **Schließen**aus.
6. Definieren Sie die Häufigkeit für die erneute Erkennung, indem Sie die entsprechende Option in der **Liste** Ausführen auswählen.
   Weitere Informationen finden Sie unter Ausführungsoptionen für Discovery-Zeitpläne.
7. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Musterbasierte Erkennung in Service-Mapping

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery-Zeitpläne von oben nach unten

Erfahren Sie mehr über Zeitpläne, die die Top Down-Discovery von Anwendungsservices auslösen.

Wenn Sie einen neuen Anwendungsservice definieren, führt Service-Mapping die Erkennung aller CIs durch, die an diesem Anwendungsservice beteiligt sind, und erstellt die Zuordnung. Nach Abschluss der ersten Zuordnung generiert Service-Mapping die Zuordnungen für Anwendungsservices regelmäßig neu, indem die CIs, aus denen ein Anwendungsservice besteht, erneut erkannt werden.

Standardmäßig ist Service-Mapping mit diesen generischen Zeitplänen vorkonfiguriert:

Alle Anwendungen

Dieser Zeitplan löst die Erkennung von oben nach unten aller CIs vom Anwendungstyp [cmdb_ci_appl] aus.

Load Balancer-Service

Dieser Zeitplan startet die Erkennung von oben nach unten aller CIs des Servicetyps Lastenausgleichsmodul [cmdb_ci_lb_service].

Die generischen Zeitpläne lösen einmal täglich die Erkennung aller Anwendungen und Lastenausgleichsservices in Ihrer Organisation aus. Normalerweise reichen diese vorkonfigurierten Zeitpläne aus, um die Informationen für Anwendungsservices zu aktualisieren. Wenn bestimmte CIs oder Services jedoch häufiger erkannt werden müssen, können Sie die folgenden anwenderdefinierten Discovery-Zeitpläne erstellen:

Typen der Erkennung von oben nach unten planen

Zeitplantyp	Beschreibung	Beispiel
Services	Service-Mapping erkennt alle CIs, die zu bestimmten Services gehören und Filterkriterien erfüllen.	In Ihrem Unternehmen sind einige Anwendungsservices kritischer als andere und es ist wichtig, dass Sie die Erkennung solcher Services mit hoher Relevanz häufiger wiederholen. Erstellen Sie einen benutzerdefinierten Erkennungszeitplan, um alle Services zu erkennen, deren Wert für geschäftliche Relevanz auf *most critical* gesetzt ist. Alternativ werden bestimmte Services in Ihrer Organisation häufiger als einmal pro Tag geändert. Sie können benutzerdefinierte Zeitpläne erstellen, damit solche Services häufiger neu erkannt werden. Sie können auch einen Zeitplan dieses Typs erstellen, um Anwendungsservices in einer Test- und Entwicklungsumgebung zu erkennen, in der sich Services noch nicht im Status *operational* befinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typen der Erkennung von oben nach unten planen (Fortsetzung)

Zeitplantyp	Beschreibung	Beispiel
Services, die zu einer Gruppe gehören	Service-Mapping erkennt alle CIs, die zu Services gehören, die Gruppen zugewiesen sind, welche Filterkriterien erfüllen. Service-Mapping erkennt nur Services, die sich direkt in der Gruppe befinden und definierte Filterkriterien erfüllen. Service-Mapping erkennt keine Services in eingebetteten Gruppen. Beachten Sie, dass Sie Zeitpläne basierend auf Servicegruppen definieren können, auch wenn Ihre Rolle keinen Zugriff auf diese Servicegruppen hat.	In einer verteilten Organisation mit Büros an mehreren geografischen Standorten möchten Sie möglicherweise einen benutzerdefinierten Erkennungszeitplan erstellen, um die Erkennung von Services an einem dieser Standorte zu wiederholen. Beispielsweise kann ein Zeitplan die erneute Erkennung aller Services, die für den EMEA-Standort relevant sind, um 7 Uhr GMT auslösen, während ein anderer Zeitplan die erneute Erkennung von Services für den US-Hauptsitz um 7 Uhr PT starten kann.
Für CI-Typen	Service-Mapping erkennt alle Anwendungs-CIs, die zu diesem Anwendungstyp gehören. Einige Anwendungs-CI-Typen werden tendenziell häufiger geändert und aktualisiert als andere, daher können Sie die Last verwalten, indem Sie den Erkennungszeitplan an die Art der einzelnen CI-Typen anpassen. Wenn Sie Erkennungszeitpläne auf Grundlage von Anwendungs-CI-Typen definieren, gelten für dasselbe CI möglicherweise mehrere Zeitpläne. Um zu vermeiden, dass dieselben CIs mehr als ein Mal erkannt werden, wird dem spezifischsten Zeitplan immer Vorrang eingeräumt. Wenn Sie beispielsweise separate Erkennungszeitpläne für einen übergeordneten CI-Typ und seinen untergeordneten CI-Typ erstellen, werden CIs, die zum untergeordneten CI-Typ gehören, anhand des spezifischen Zeitplans erkannt. Wenn kein Zeitplan für einen untergeordneten CI-Typ vorhanden ist, wird für die Erkennung der untergeordneten CIs der Zeitplan des übergeordneten CI-Typs verwendet.	Wenn Sie eine bestimmte Anwendung häufiger ändern als andere, möchten Sie die Erkennung möglicherweise häufiger durchführen als bei anderen CIs. Erstellen Sie in diesem Fall einen benutzerdefinierten Erkennungszeitplan für einen solchen Anwendungs-CI-Typ.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typen der Erkennung von oben nach unten planen (Fortsetzung)

Zeitplantyp	Beschreibung	Beispiel
	Dieser Zeitplan erkennt nur CIs, die zu Anwendungsservices mit dem Status *operational* gehören.	
Bestimmte CIs	Service-Mapping erkennt nur ein einziges CI, das Sie für diesen Zeitplan angegeben haben. Wenn Sie einen Erkennungszeitplan für ein bestimmtes CI sowie einen Zeitplan für den CI-Typ definieren, zu dem dieses CI gehört, verwendet Service-Mapping den Zeitplan für dieses spezifische CI und nicht den generischen Zeitplan für seinen CI-Typ. Dieser Zeitplan erkennt nur CIs, die zu Anwendungsservices mit dem Status *operational* gehören.	Für seltene Fälle, in denen ein bestimmtes CI neu erneut erkannt wird und häufig Erkennungsfehler verursacht

Ein Teil der Erkennung eines Anwendungs-CI besteht in der Identifizierung seines Hosts. Service-Mapping prüft, ob das Gerät, das dieses Anwendungs-CI hostet, in der CMDB vorhanden ist. Für einen Lastenausgleichsservice überprüft Service-Mapping, ob das Lastenausgleichsgerät, das diesen Lastenausgleichsservice hostet, in der CMDB vorhanden ist. Wenn nicht, veranlasst Service-Mapping Discovery, eine horizontale Erkennung durchzuführen. Daher führt Discovery eine Hosterkennung durch und aktualisiert die Informationen zu den Hosts in der CMDB. Bei Bedarf können Sie die Zeitpläne, die die horizontale Erkennung auslösen, wie folgt verwalten:

- Horizontale Erkennung planen — für eine standardmäßige horizontale Erkennung
- Zeitplan für standardmäßige serverlose Erkennung erstellen – zum Erkennen von CIs mithilfe eines Protokolls wie REST, ohne die IP-Adresse von Geräten oder Hosts zu verwenden
- Zeitplan für hostbasierte serverlose Erkennung erstellen – zum Erkennen von CIs, die sich auf einem bereits erkannten Host befinden und diesen Host als Proxy-Server verwenden

Zugehörige Informationen

Erkennung von oben nach unten mithilfe von Service-Mapping planen

Servicedefinition von einer Instanz zur anderen übertragen

Sparen Sie Zeit und Aufwand, indem Sie Definitionen von Serviceinstanzen aus der Quellinstanz exportieren und diese Definitionen in die Zielinstanz importieren. Sie können diese Methode verwenden, um Definitionen von Serviceinstanzen nur des erkannten Typs zu kopieren.

Normalerweise pflegen Sie zwei ServiceNow-Instanzen in Ihrer Organisation: eine für die Produktion und eine für die Entwicklung. Führen Sie die erste Zuordnung von Anwendungsservices in Ihrer Organisation in der Entwicklungsinstanz durch, die Sie zum Testen verwenden. Die Ergebnisse der anfänglichen Zuordnung erfordern häufig eine grundlegende Fehlerbehebung oder Feinabstimmung. Sobald Sie die Zuordnung der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservices in Ihrer Quellinstanz abgeschlossen haben, übertragen Sie die Servicedefinitionen auf die Ziel- bzw. Produktionsinstanz.

Beachten Sie, dass Sie nicht die tatsächlichen Anwendungsservices exportieren können, sondern nur die Servicedefinitionen. Die Zuordnung ist ein dynamischer Prozess, und das Zuordnungsergebnis spiegelt die tatsächliche Infrastruktur und deren Konfiguration wider. Daher sehen die Services, die Sie aus einer Instanz exportiert und in eine andere importiert haben, möglicherweise unterschiedlich aus.

Standardmäßig exportieren Sie die folgenden Servicedefinitionen:

- Servicename
- Nutzung der datenverkehrsbasierten Erkennung
- Eingabepunkt
- Business-Relevanz
- Gruppe, zu der der Service gehört

  Wenn diese Servicegruppe Teil einer Servicegruppenhierarchie ist, werden auch alle übergeordneten Servicegruppen in dieser Hierarchie exportiert.

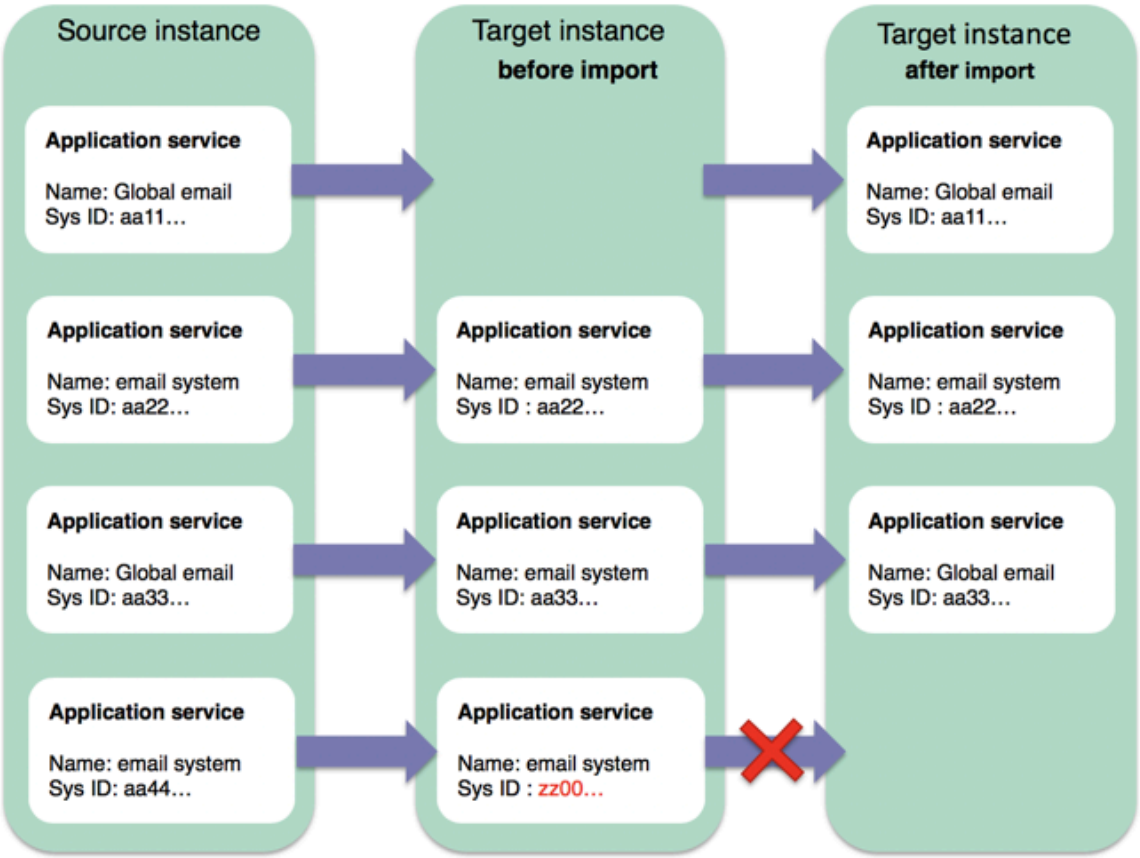
- Kommentare

Das System verwendet das Sys-ID-Attribut [sys_id], um Services in den Quell- und Zielinstanzen zu identifizieren, und implementiert den Import von Servicedefinitionen gemäß den folgenden Regeln:

- Wenn in der Zielinstanz keine Service-Sys-ID vorhanden ist, erstellt das System in der Zielinstanz einen neuen Service.
- Wenn in der Zielinstanz bereits eine Sys-ID und ein Name für einen Service vorhanden sind, aktualisiert das System diesen Service, indem die vorhandenen Servicedefinitionen mit den importierten Definitionen überschrieben werden.
- Wenn in der Zielinstanz eine Service-Sys-ID vorhanden ist, die jedoch einem anderen Servicenamen zugeordnet ist, aktualisiert das System den Service mit dieser Sys-ID. Das System überschreibt Servicedefinitionen, einschließlich des Servicenamens.
- Wenn derselbe Name in der Quell- und Zielinstanz für verschiedene Services verwendet wird, importiert das System keine Servicedefinitionen.
- Manuelle Services können nicht exportiert werden. Ebenso können Sie manuell hinzugefügte Einstiegspunkte nicht exportieren. Beim Importieren von Definitionen eines Service mit manuellen Einstiegspunkten nimmt das System keine Änderungen an den Einstiegspunkten vor.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flow für Servicedefinitionen exportieren



Bei der Übertragung von Servicedefinitionen zwischen Instanzen werden der Domäne des Benutzers importierte Serviceinstanzen und Servicegruppen zugewiesen.

Standardmäßig weist das System Anwendungsservices, deren Definitionen Sie importiert haben, den Status *Non-operational* zu.

Bei der Übertragung von Servicedefinitionen wird die Standardfunktion für Import Sets bereitgestellt, die auf der Now Platformverfügbar ist. Wenn Sie Servicedefinitionen aus der Quellinstanz exportieren, erstellt das System eine JSON-Datei mit den exportierten Daten. Wenn Sie Servicedefinitionen in die Zielinstanz kopieren, importieren Sie die Daten aus dieser JSON-Datei, die zu einem Import Set wird.

Servicedefinitionen exportieren

Erstellen Sie ein Import Set, das Servicedefinitionen enthält. Dieses Import Set verwenden Sie, um Servicedefinitionen in eine andere Instanz zu importieren.

Vorbereitungen

- Entscheiden Sie, welche Servicedefinitionen Sie exportieren möchten.

  Wichtig: Sie können diese Methode verwenden, um Definitionen von Anwendungsservices nur des erkannten Typs zu kopieren.

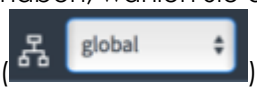
- Stellen Sie sicher, dass sich die Quell- und Zielinstanzen im selben ServiceNow-Release befinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Öffnen Sie die Quellinstanz, aus der Sie Servicedefinitionen kopieren möchten.
- Nehmen Sie bei Bedarf eine Feinabstimmung der Importsatz-Erstellung vor, indem Sie die relevanten Eigenschaften unter ändern **Service-Mapping** > **Administration** > **Eigenschaften**. Weitere Informationen finden Sie unter Mit Service-Mapping installierte Komponenten.

Erforderliche Rolle: service_mapping_admin

Prozedur

1. Wenn Ihre Instanz Domänentrennung nutzt und Sie Zugriff auf die globale Domäne haben, wählen Sie die Domäne, zu der der für Service gehört, über die Domänenauswahl (

) aus.
Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.
2. Navigieren zu **Service-Mapping** > **Services** > **Anwendungsservices**.
3. Wählen Sie die Anwendungsservices aus, die Sie exportieren möchten.
4. Klicken Sie am unteren Seitenrand auf **Aktionen für ausgewählte Zeilen**, und wählen Sie **Export Services (Services exportieren)** aus.
Das Import Set wird im Ordner `Downloads` angezeigt. Der Dateiname folgt der folgenden Konvention: export_service_<DatumUhrzeit>.json.
5. Kopieren Sie bei Bedarf das Import Set an einen anderen Speicherort auf dem Computer.

Servicedefinition aus einer Instanz in eine andere importieren

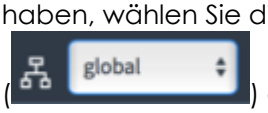
Importieren Sie Definitionen der Anwendungsservices aus der Quellinstanz.

Vorbereitungen

- Stellen Sie sicher, dass sich die Quell- und Zielinstanzen im selben ServiceNow-Release befinden.
- Öffnen Sie die Zielinstanz, in die Sie Servicedefinitionen kopieren möchten.

Erforderliche Rolle: import_admin

Prozedur

1. Wenn Ihre Instanz Domänentrennung nutzt und Sie Zugriff auf die globale Domäne haben, wählen Sie die Domäne, zu der der für Service gehört, über die Domänenauswahl (

) aus.
Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.
2. Navigieren zu **Service-Mapping** > **Services** > **Servicedefinitionen importieren**.
3. Klicken Sie im Fenster „Servicedefinitionen importieren“ auf **Datei auswählen**, navigieren Sie zur JSON-Datei, die Servicedefinitionen enthält, und klicken Sie auf **OK**.
4. Wahlweise: Klicken Sie auf **Vorschau anzeigen**, und überprüfen Sie die Definitionen in der ausgewählten JSON-Datei.
5. Klicken Sie auf **Importieren**.
6. Klicken Sie auf **Ja**, um zu bestätigen, dass Sie zum Importieren von Servicedefinitionen bereit sind.

> **Wichtig:** Während des Imports überschreibt das System die aktuellen Servicedefinitionen unwiderruflich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Fortschrittsfenster zeigt die Erfolgsnachricht an.

Service-Mapping startet automatisch die Erkennung von Services, die importierte Einstiegspunkte enthalten.

7. Überprüfen Sie importierte oder aktualisierte Services, nachdem Service-Mapping den Zuordnungsprozess abgeschlossen hat.
   Wenn das Übertragungsergebnis nicht Ihren Erwartungen entspricht, gehen Sie wie in der folgenden Tabelle beschrieben vor, um eine grundlegende Fehlerbehebung durchzuführen.

Trouble?

Symptom	Ursache	Lösung
Kürzlich an einem für Service vorgenommene Änderungen werden nicht angezeigt.	Definitionen von vorhandenen Anwendungsservices werden während der Übertragung immer überschrieben.	1. Nehmen Sie die erforderlichen Änderungen an den Definitionen dieses für Service erneut vor. 2. Führen Sie die Erkennung von oben nach unten dieses für Service aus, indem Sie in der Servicezuordnung auf **Discovery ausführen** klicken.
Eine importierte Servicegruppe wird nicht angezeigt.	Der Import eines dieser Gruppe zugewiesenen Anwendungsservice ist fehlgeschlagen und die Gruppe wurde vom System nicht erstellt, da sie leer zu sein scheint.	1. Beheben Sie das Problem, das verhindert hat, dass das System den für Service importiert, der zu dieser Gruppe gehört. 2. Importieren Sie das Import Set erneut. 3. Überprüfen Sie, ob die Servicegruppe angezeigt wird.
Einer importierten Servicegruppe wurden anscheinend falsche Anwendungsservices zugewiesen.	Dies ist eine andere Servicegruppe mit demselben Namen, nicht die von Ihnen importierte Servicegruppe. Das System konnte die Servicegruppe nicht importieren, da die Quellinstanz bereits eine Servicegruppe mit demselben Namen bzw. mit demselben Namen und derselben Sys-ID hat.	1. Überprüfen Sie das Importprotokoll. 2. Wenn ein Fehler besagt, dass eine Datensatzerstellung während der Ausführung der Geschäftsregel „Check Name Uniqueness (Eindeutigkeit des Namens prüfen)“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
		fehlgeschlagen ist, gehen Sie wie folgt vor: **a.** Benennen Sie die Servicegruppe in der Quellinstanz um. **b.** Exportieren Sie die dieser Gruppe zugewiesenen Anwendungsservices erneut. **c.** Importieren Sie das letzte Import Set in die Zielinstanz. **3.** Wenn ein Fehler besagt, dass eine Datensatzerstellung fehlgeschlagen ist, weil die Sys-ID bereits vorhanden ist, gehen Sie wie folgt vor: **a.** Erstellen Sie die Servicegruppe in der Quellinstanz neu, und achten Sie darauf, dass Sie einen anderen Gruppennamen und eine andere Sys-ID angeben. **b.** Exportieren Sie die dieser Gruppe zugewiesenen Anwendungsservices erneut. **c.** Importieren Sie das letzte Import Set in die Zielinstanz. **4.** Stellen Sie sicher, dass die Servicegruppe in der Quellinstanz korrekt angezeigt wird.

Analyse und Wartung von Anwendungsservices mithilfe von klassisch Service-Mapping

Service-Mapping erstellt Zuordnungen, mit deren Hilfe Sie die Architektur und Organisation von Anwendungsservices anzeigen können. Diese Zuordnungen sind nützlich bei der Planung von Änderungen oder Migrationen sowie zur Analyse der Kontinuität und Verfügbarkeit von Services.

Zuordnungen sind in folgenden Fällen nützlich:

Migration eines kompletten für Service oder seiner Segmente planen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die Zuordnung, um anzuzeigen, welche Konfigurationselemente (CIs) verschoben werden müssen oder welche CIs redundant werden.

Upgrade oder Ersetzung eines CI planen

Überprüfen Sie die Zuordnung, um zu sehen, welche anderen CIs betroffen sind, wenn das CI während der Wartung nicht betriebsbereit ist. Sie können die Ausfallzeit bewerten und planen oder Vorkehrungen treffen, um Ausfallzeiten zu vermeiden.

Da dasselbe CI für mehrere Anwendungsservices verwendet werden kann, überprüfen Sie das CI mit der Anwendung Dependency Views. Mit dieser Anwendung können Sie alle Anwendungsservices anzeigen, zu denen ein CI gehört.

für Service auf hohe Verfügbarkeit und Kontinuität analysieren

Verwenden Sie die Zuordnung, um CIs zu identifizieren, die für die Serviceleistung wichtig sind. Entscheiden Sie, ob Sie diese CIs durch die Erstellung von Clustern stärken möchten.

Problembehebung bei Anwendungsservices

Verwenden Sie die Zuordnung, um die Auswirkungen eines Problems zu verstehen und zu bestimmen, welches CI das Problem verursacht.

Anwendungsservicezuordnungen in klassisch Service-Mapping

Zuordnungen bieten Ihnen eine Visualisierung von Daten zu Konfigurationselementen (CIs), die Anwendungsservices umfassen, sowie Beziehungen und Verbindungen zwischen diesen CIs.

Eine neue Zuordnung wird jedes Mal erstellt, wenn Sie einen Anwendungsservice manuell erstellen oder einen Anwendungsservice mithilfe von Service-Mapping zuordnen. Das System aktualisiert die Zuordnung jedes Mal, wenn Sie dem Anwendungsservice CIs hinzufügen oder wenn Service-Mapping eine Erkennung für CIs ausführt, die zu diesem Anwendungsservice gehören.

Hinweis:

Die für eine Zuordnung verfügbaren Informationen und Aktionen hängen von Ihrer Rolle ab:

- Als Servicebenutzer [app_service_user] oder Service-Mapping -Benutzer [service_mapping_user] können Sie die Zuordnung im Ansichtsmodus anzeigen.
- Als Serviceadministrator [app_service_admin] oder Service-Mapping -Administrator [service_mapping_admin] können Sie Anwendungsservices im Ansichtsmodus anzeigen und erkannte und manuell erstellte Services im Bearbeitungsmodus ändern.

Wichtig: Sie können Tag-basierte und dynamische Services nicht über die Zuordnung optimieren oder bearbeiten.

- Als Service-Mapping -Administrator [service_mapping_admin] können Sie Discovery-Nachrichten und -Fehler anzeigen, die von Service-Mapping generiert wurden, und Services im Bearbeitungsmodus ändern. Außerdem können Sie die Zuordnung neu laden, um sicherzustellen, dass sie die neuesten Informationen enthält.
- Als Serviceverantwortlicher [sm_app_owner] können Sie Services, die mithilfe von Service-Mapping erkannt wurden, im Ansichtsmodus anzeigen, Feedback hinterlassen und genehmigen.

Hinweis: Der Überprüfungs- und Genehmigungsprozess ist nur für erkannte und manuell erstellte Serviceinstanzen verfügbar.

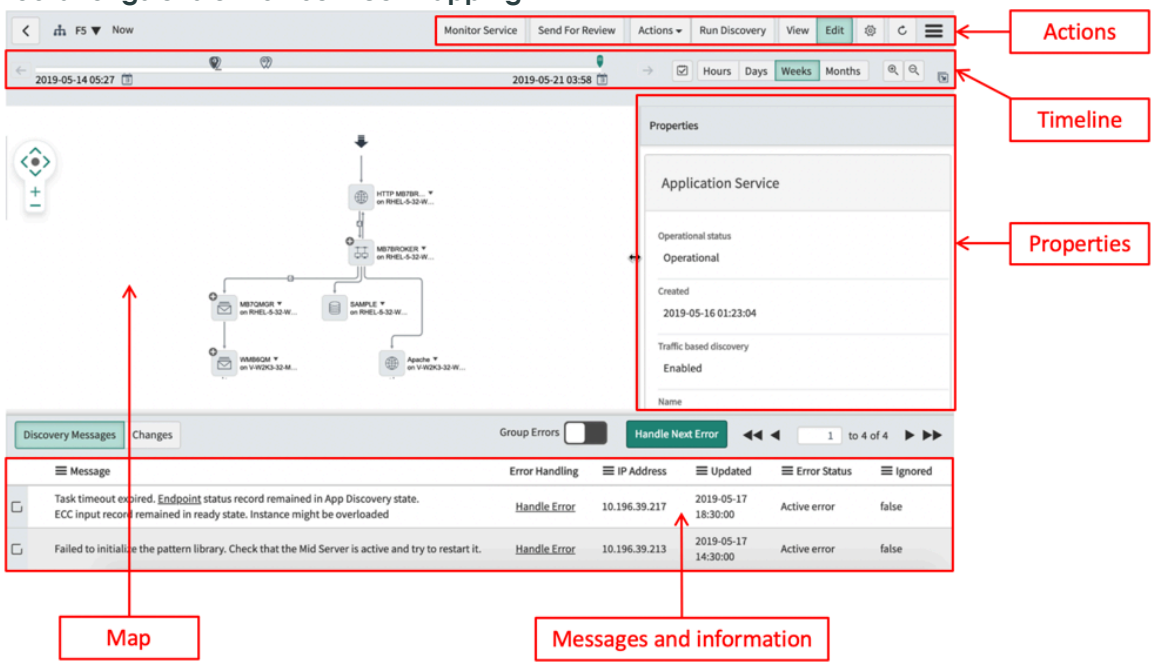
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionen und Informationen sind im Zusammenhang mit der automatischen Erkennung mit Service-Mapping sind nicht verfügbar bei CIs, die Service-Mapping nicht erkennen kann. Beispiel: Für manuell erstellte für Service, die Service-Mapping nicht erkennt, wird die Registerkarte „Discovery-Nachrichten“ nicht angezeigt.

Zuordnungsfenster

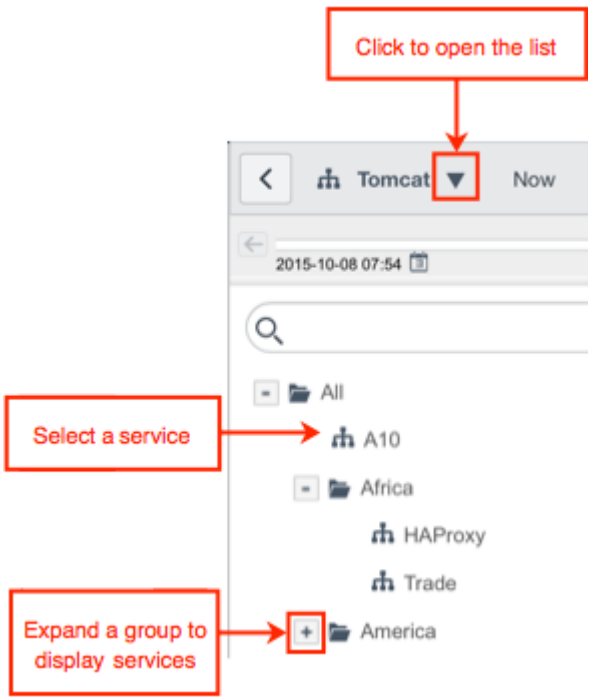
Neben der Zuordnung selbst werden im Zuordnungsfenster auch der Bereich „Eigenschaften“ und Registerkarten mit zusätzlichen Informationen angezeigt.

Zuordnungsfenster von Service-Mapping



Von diesem Fenster aus können Sie direkt zu einer anderen Anwendungsservicezuordnung navigieren, indem Sie diesen in der Liste auswählen.

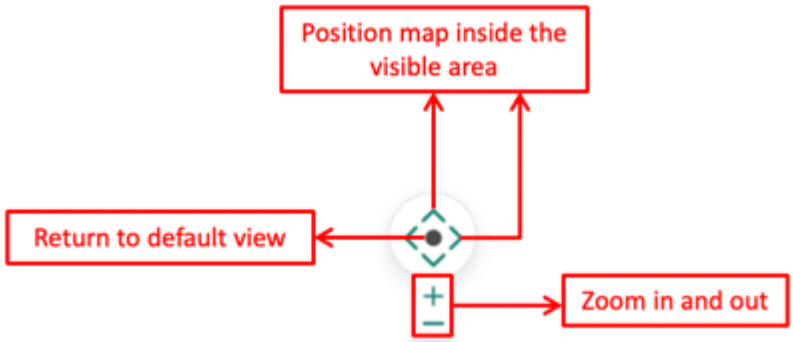
Serviceliste



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig wird die gesamte Zuordnung in der Mitte des sichtbaren Fensterbereichs der Zuordnung angezeigt. Mit den folgenden Steuerungen können Sie die Zuordnung vergrößern und verkleinern sowie positionieren, je nachdem, welches Segment der Zuordnung Sie sehen möchten:

Zuordnungsnavigation



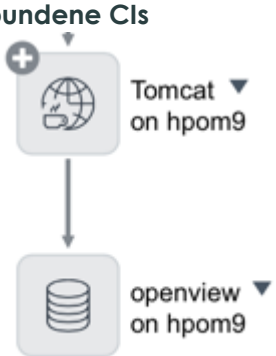
Sie können auch auf eine beliebige Stelle im Zuordnungsbereich klicken und das gewünschte Segment der Zuordnung in den sichtbaren Bereich ziehen.

Sie können Änderungen an einem für Service als Ganzes sowie an einzelnen CIs anzeigen, die zu einem Service gehören, indem Sie einen Zeitraum auswählen. Weitere Informationen finden Sie unter Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen.

Elemente und ihr Erscheinungsbild zuordnen

Jede Zuordnung besteht aus Symbolen, die CIs darstellen, und Pfeilen, die die Verbindungen zwischen diesen darstellen.

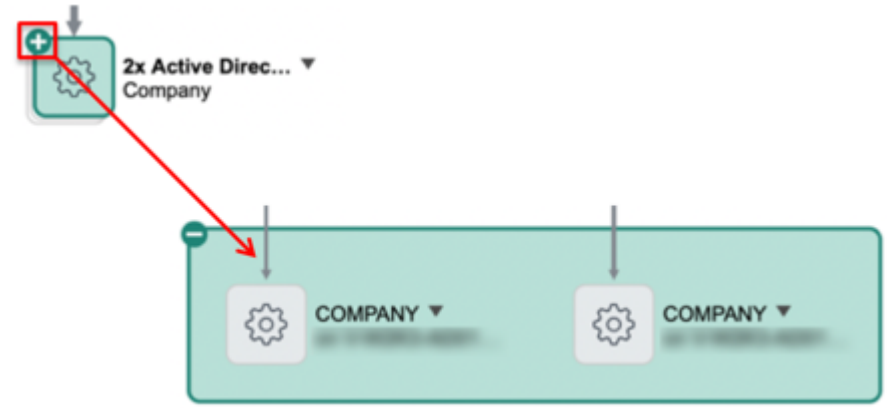
Verbundene CIs



Einige Zuordnungselemente (wie Anwendungscluster) können weitere Elemente enthalten. In der Zuordnung werden Anwendungscluster als Stapel von CIs mit Pluszeichen (+) daneben angezeigt. Die Clusterbezeichnung enthält die Anzahl der CIs im Cluster mit dem Multiplikationszeichen.

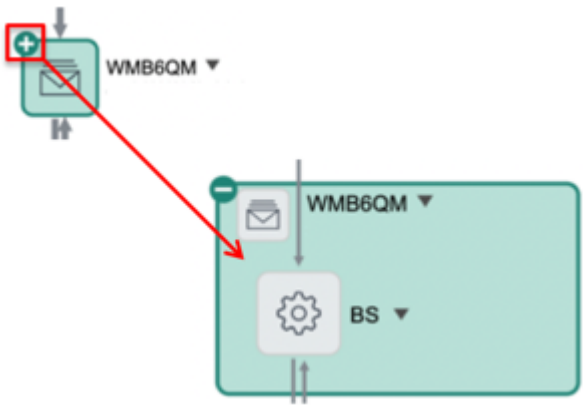
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Cluster



Wenn das CI Inklusionen aufweist, wird neben dem CI-Symbol das Pluszeichen (+) angezeigt, und die enthaltene Anwendung wird angezeigt, wenn Sie es erweitern.

Inklusion



Ein BS-Cluster wird als CI mit einem Pluszeichen und der Anzahl der CIs im Cluster angezeigt.

BS-Cluster-CI

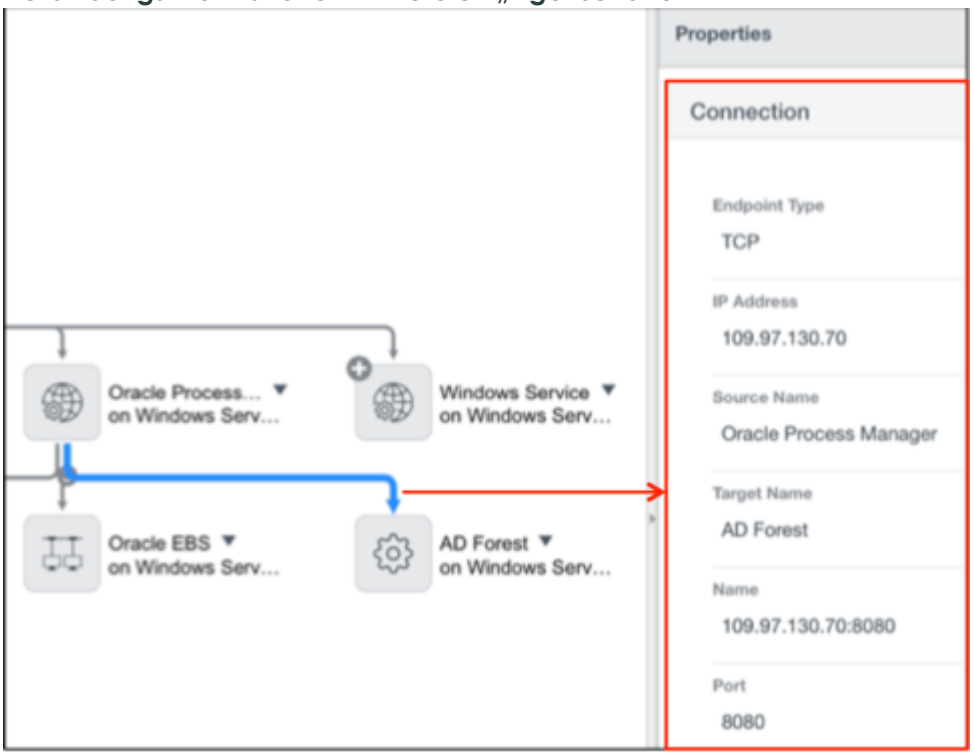
CI-Attribute und CI-bezogene Nachrichten

Wenn eine Zuordnung geladen ist und keine Elemente ausgewählt sind, werden im Eigenschaftenbereich die Details dieses für Service angezeigt.

Ausgewählte Geräte, Anwendungen oder Connectors werden blau angezeigt und sind hervorgehoben. Informationen zum ausgewählten Zuordnungselement werden im Eigenschaftenbereich rechts von der Zuordnung angezeigt. Der Bereich „Eigenschaften“ enthält die Links zur Seite „Detaillierte Eigenschaften“.

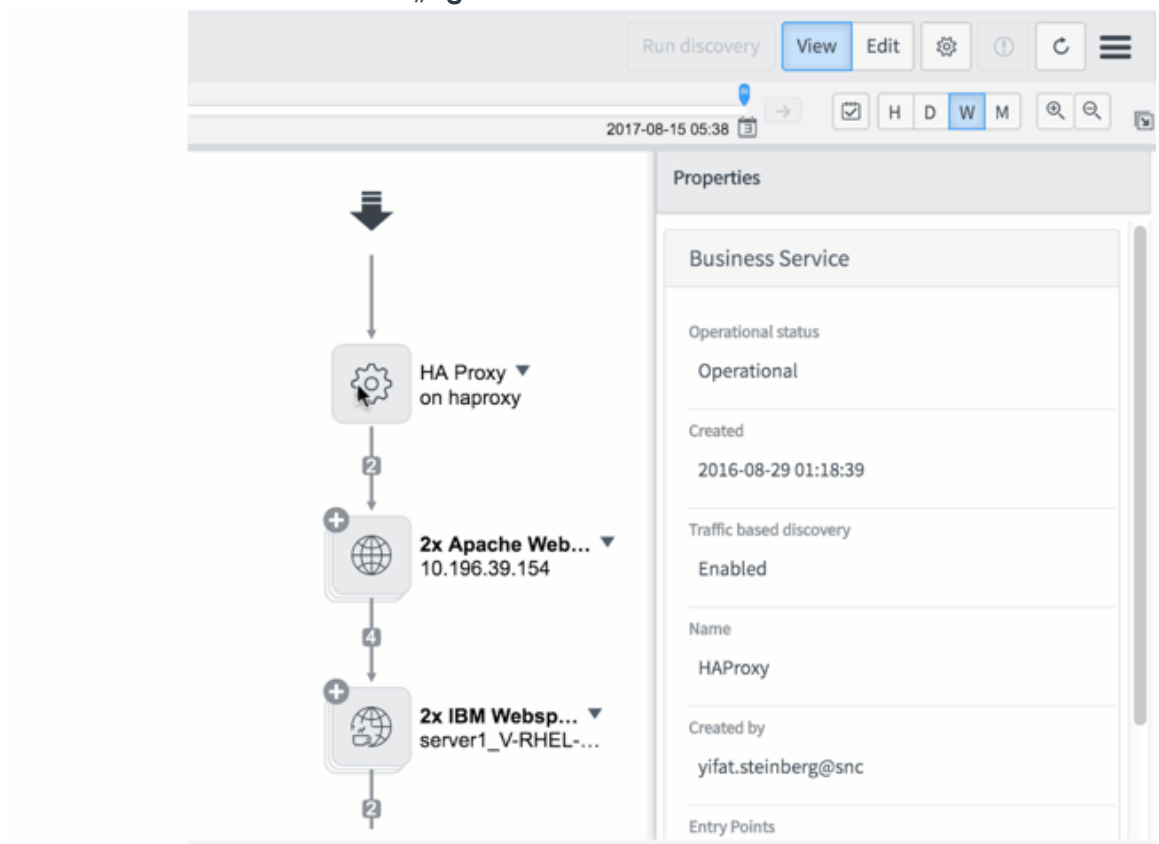
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verbindungsinformationen im Bereich „Eigenschaften“



Die Attribute für den Server, auf dem die Anwendungen gehostet werden, und die Anwendungen selbst werden im Bereich „Eigenschaften“ getrennt angezeigt.

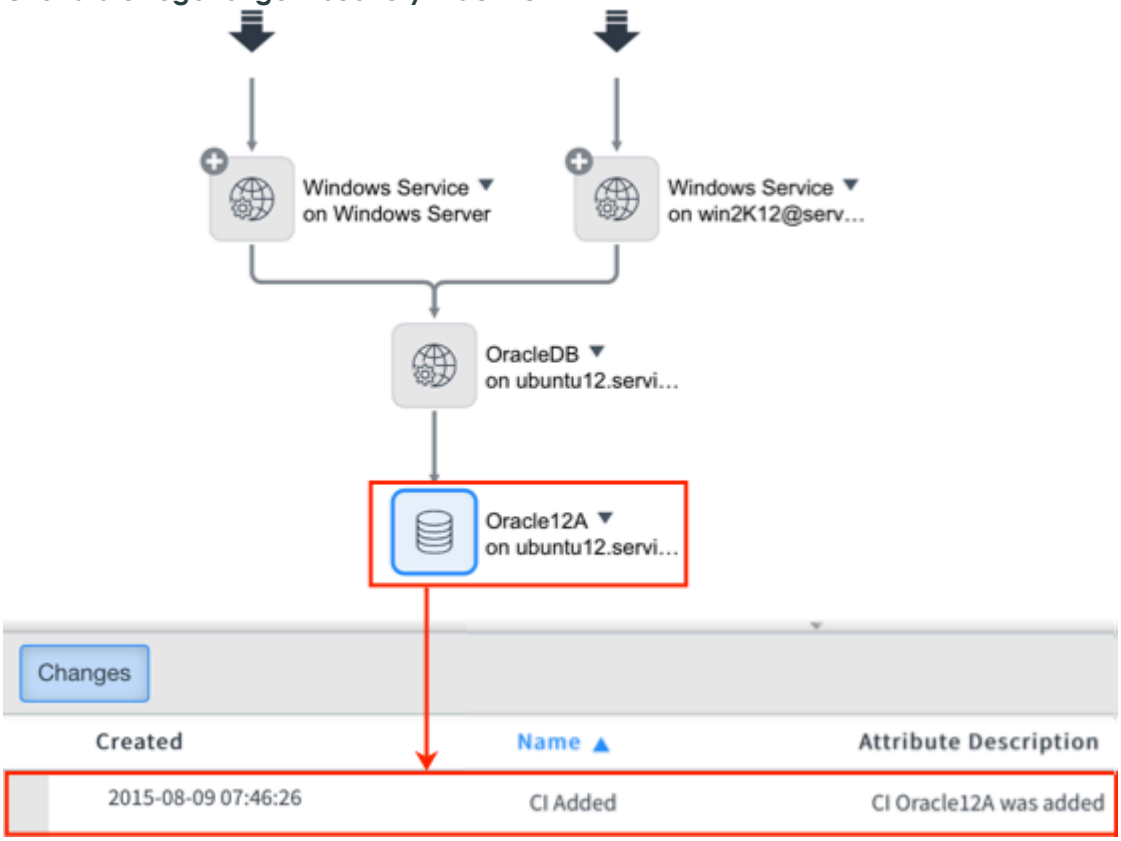
Serverinformationen im Bereich „Eigenschaften“



Wenn Informationen zum ausgewählten CI oder zur ausgewählten Verbindung vorhanden sind, werden diese auf der Registerkarte unten im Fenster hervorgehoben.

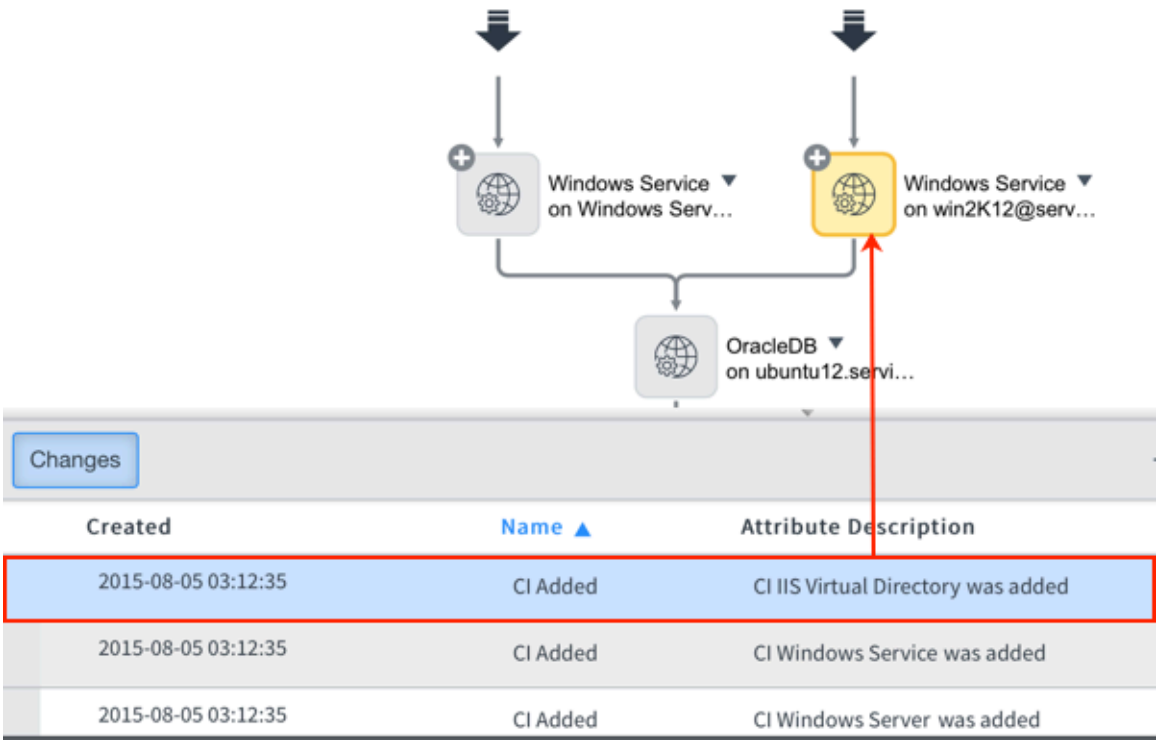
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI und die zugehörige Discovery-Nachricht



Wenn Sie Informationen auf einer Registerkarte im Zuordnungsfenster unten auswählen, wird das zugehörige CI in Gelb angezeigt.

Die Meldung und das CI, für das sie generiert wird

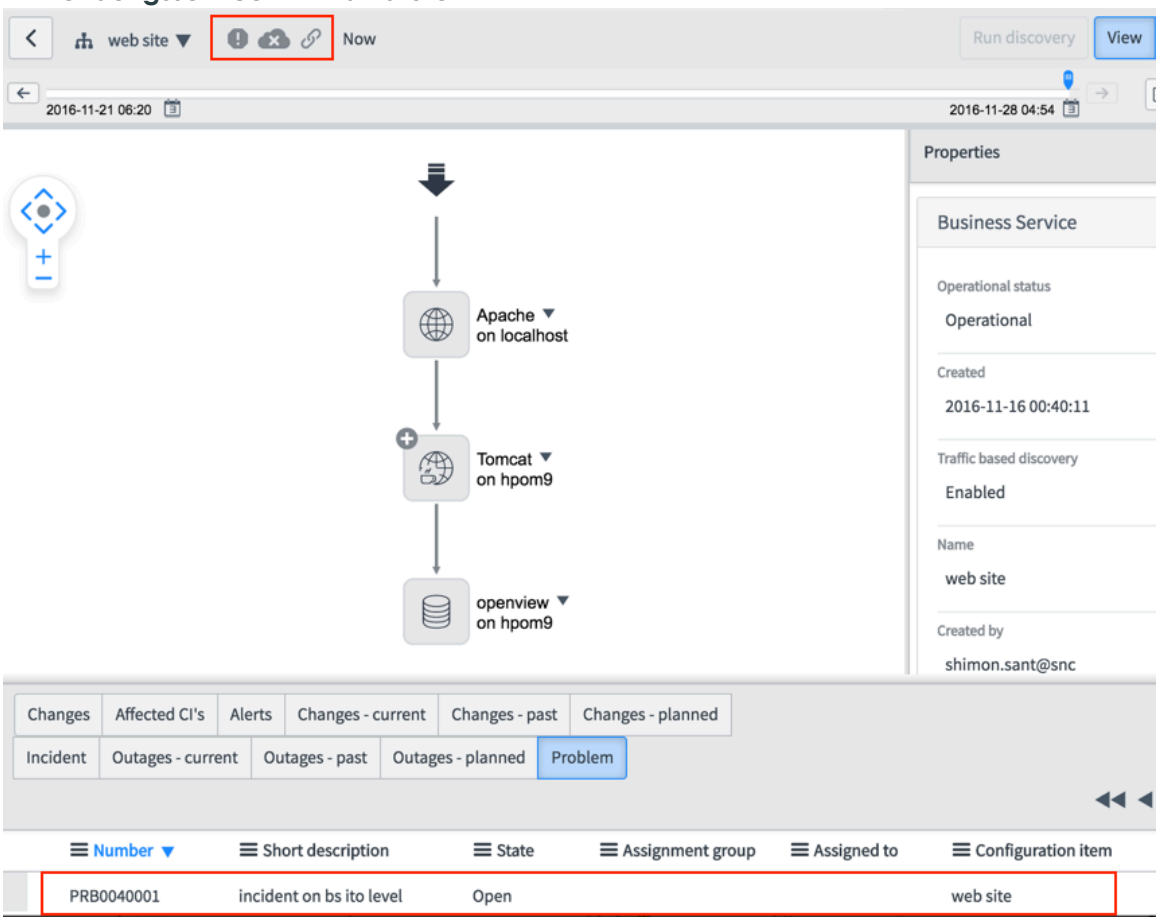


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungsindikatoren

Sie können zusätzliche Informationen für ein CI oder den für Service selbst anzeigen, indem Sie zugehörige Datensätze anzeigen, zum Beispiel Warnungen, Ausfälle, Incidents und Probleme. Wenn Sie diese Funktion aktivieren, werden neben relevanten CIs und dem Namen des für Service Datensatzindikatoren angezeigt. Die Datensätze selbst werden auf den Registerkarten unten im Zuordnungsfenster angezeigt.

Anwendungsservice mit Indikatoren

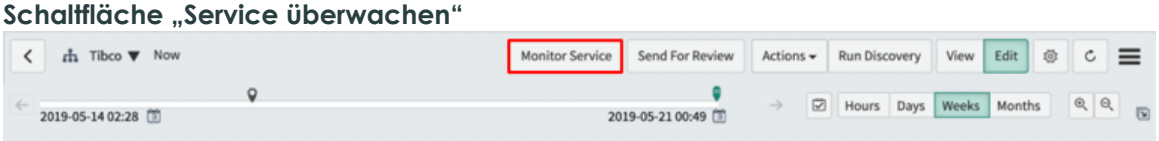


Zuordnungsansichten

Passen Sie eine Zuordnungsansicht an, um irrelevante Informationen auszuschließen und die Übersichtlichkeit zu erhöhen (siehe Beschreibung in Ansicht für Anwendungsservicezuordnung ändern).

Um diesen für Service im Ereignismanagement zu öffnen und Warnungen zu CIs anzuzeigen, die Teil des für Service sind, klicken Sie oben im Fenster auf **Service überwachen**.

Schaltfläche „Service überwachen“



Zugehörige Informationen

Zeigen Sie CI-Attribute in einer Anwendungsservice-Zuordnung in an klassisch Service-Mapping

Anzeige für CI-Attribute ändern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansicht für Anwendungsservicezuordnung ändern

Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen

Zeigen Sie CI-Attribute in einer Anwendungsservice-Zuordnung in an klassisch Service-Mapping

Die Anwendungsservicezuordnung zeigt Attribute für jedes Configuration Item (CI), das Teil des Anwendungsservice ist, sowie für den Anwendungsservice selbst an. Die Attribute stammen aus dem CMDB.

Vorbereitungen
Erforderliche Rolle: service_mapping_admin oder service_mapping_user

Warum und wann dieser Vorgang ausgeführt wird
Sie können für jedes CI die folgenden Informationen anzeigen:

Namensschild

Der CI-Name. Dieses Attribut wird entweder im CI vorkonfiguriert oder während der CI-Installation konfiguriert.

Grundlegende Attribute

Eine Zusammenfassung der wichtigsten CI-Attribute.

Detaillierte Attribute

Eine vollständige Liste aller für das CI erfassten Attribute.

Jeder CI-Typ (CI-Klasse) hat unterschiedliche Attribute. Beispielsweise hat der Linux-Server-Typ andere Attribute als der SQL-Instanz-Typ.

Wenn Service-Mapping bereitgestellt wird, hängt die Darstellung von CIs in der Zuordnung von der Ansicht ab, die Sie für die Zuordnung auswählen. Die zur Ansicht verfügbaren Attribute hängen auch von dem Service-Mapping Setup ab. Weitere Informationen finden Sie in der Beschreibung der mit Service-Mapping installierten Komponenten.

Prozedur

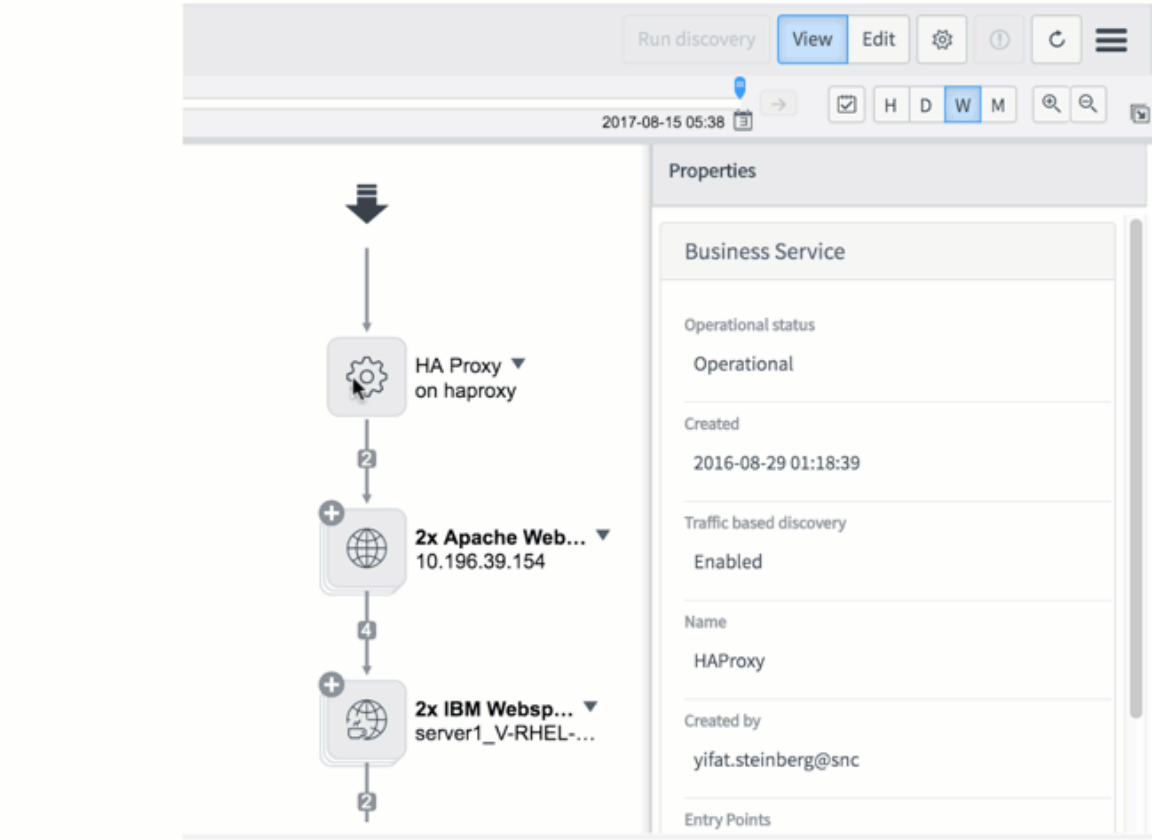
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Klicken Sie bei Bedarf auf **Bearbeiten**, um sicherzustellen, dass sich die Karte im Bearbeitungsmodus befindet.

   Wenn Service-Mapping bereitgestellt ist, wird im Bearbeitungsmodus unterhalb der Zuordnung der Abschnitt „Discovery-Nachrichten“ angezeigt.
3. Um den vollständigen Namen eines CI anzuzeigen, dessen Name auf der Karte gekürzt wurde, zeigen Sie auf das CI.

   Ein Tooltip zeigt den vollständigen CI-Namen an.
4. Klicken Sie auf ein CI, um seine Details im Bereich **Eigenschaften** anzuzeigen.

   Die Attribute von Anwendungen und die Server, auf denen sie gehostet werden, werden separat angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Um detailliertere Attribute für das CI anzuzeigen, klicken Sie auf **Detaillierte Eigenschaften** am unteren Rand des Bereichs „Eigenschaften“.
6. Wahlweise: Gehen Sie folgendermaßen vor, um Konfigurationsdateien anzuzeigen, die einem CI in Umgebungen zugeordnet sind, in denen Service-Mapping oder Discovery sowie die Nachverfolgung von Änderungen an Konfigurationsdateien für ein CI aktiviert sind:
   - Überprüfen Sie die Liste der Dateien unter **Verfolgte Dateien** im Bereich **Eigenschaften**. Klicken Sie auf den Dateinamen, um die tatsächliche Datei zu öffnen.
   - Klicken Sie auf die Registerkarte **Betroffene CIs**, und zeigen Sie die Liste der Konfigurationsdateien an. Klicken Sie auf den Dateinamen, um die tatsächliche Datei zu öffnen.

Zeigen Sie CI-Verbindungsattribute in einer Anwendungsservicezuordnung in an klassisch Service-Mapping

Sie können Attribute von Verbindungen zwischen Konfigurationselementen (CIs) anzeigen.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin oder service_mapping_user

Warum und wann dieser Vorgang ausgeführt wird

Für jede Verbindung können Sie die folgenden Informationen anzeigen:

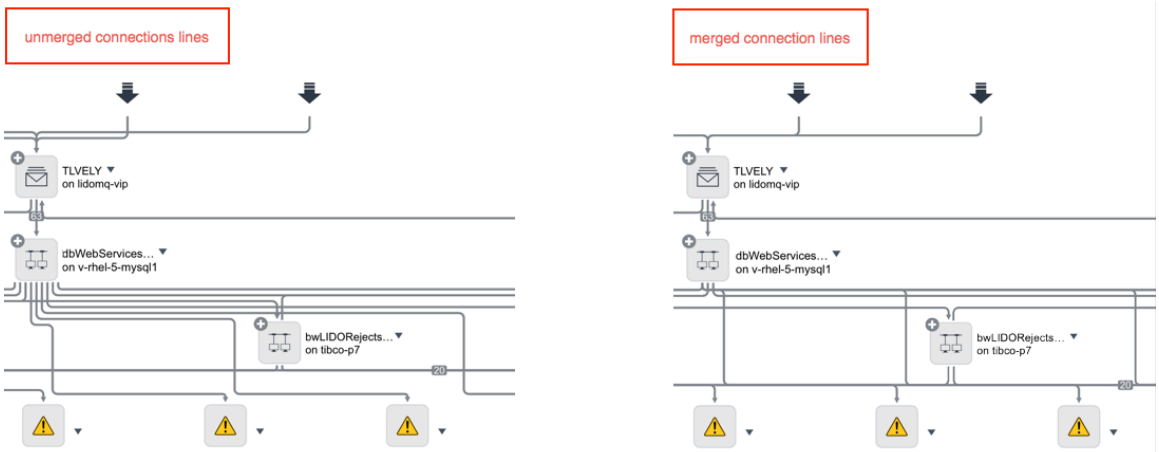
- Quell- und Ziel-CIs einer Verbindung im Kontextmenü (Rechtsklick-Menü)
- Vollständige Liste aller über die Verbindung erfassten Attribute im Bereich „Eigenschaften“

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßig führt Service-Mapping Verbindungslinien für dasselbe CI zusammen, damit die Anwendungsservicezuordnung übersichtlich bleibt. Dadurch lässt sich die Zuordnung leichter interpretieren.

Zusammengeführte Verbindungslinien



Jeder Verbindungstyp besitzt andere Attribute. Für eine zusammengeführte Verbindungslinie werden alle zugrunde liegenden Verbindungen aufgelistet.

Wie in der Zuordnung eines für Service Verbindungsattribute angezeigt werden, hängt von folgenden Faktoren ab:

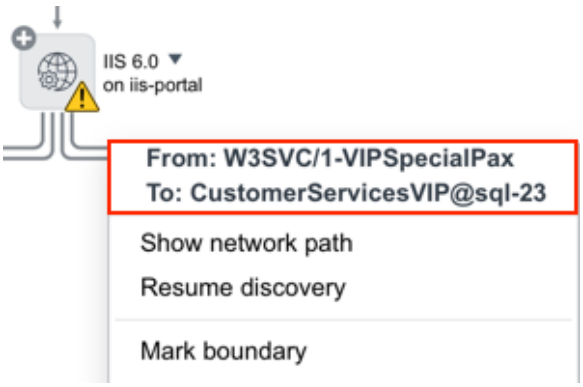
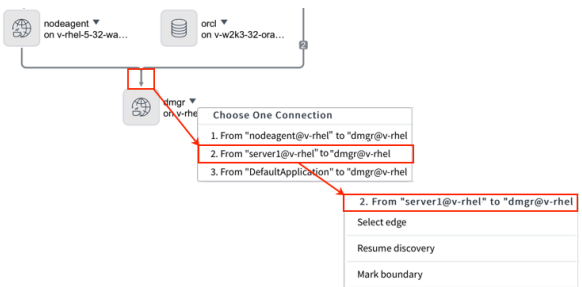
- Ansichten, die Sie für CIs konfigurieren, definieren, welche Verbindungsattribute im Eigenschaftenbereich der Zuordnung angezeigt werden.
- Verbindungslinien in der Zuordnung sind abhängig von der Ansicht, die Sie für die Zuordnung auswählen.
- Zum Anzeigen verfügbare Attribute hängen ebenfalls vom Setup von Service-Mapping ab. Weitere Informationen finden Sie in der Beschreibung der mit Service Mapping installierten Komponenten.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Zeigen Sie Verbindungsattribute wie folgt an:

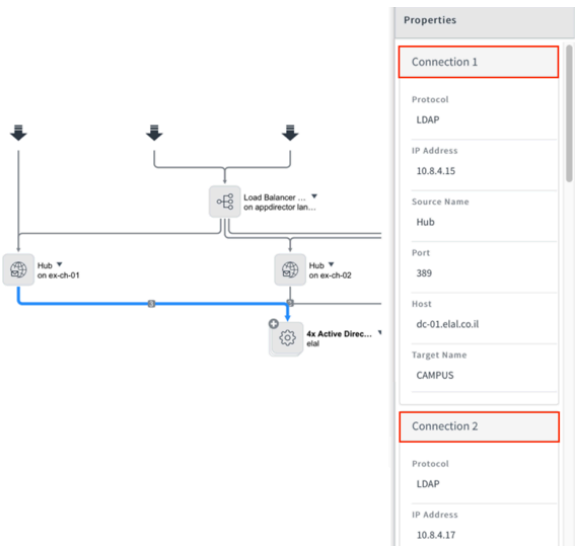
Anzuzeigende Elemente	Aktion
Quell- und Ziel-CI einer regulären Verbindung	Klicken Sie mit der rechten Maustaste auf die Verbindung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

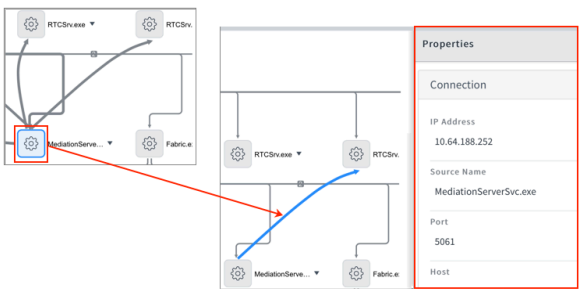
Anzuzeigende Elemente	Aktion
	
(Verfügbar für mit Service-Mapping erkannte Anwendungsservices) Quell- und Ziel-CI einer zusammengeführten Verbindung	◦ Klicken Sie mit der rechten Maustaste auf die zusammengeführte Verbindungslinie mit einer Zahl, und wählen Sie die entsprechende Verbindung aus. Oder ◦ Wenn ein Segment einer Verbindungslinie von mehreren zusammengeführten Verbindungen gemeinsam verwendet wird, gibt es keinen Hinweis darauf, dass es sich um eine zusammengeführte Linie handelt. Klicken Sie mit der rechten Maustaste auf die Verbindungslinie, die aus einem CI heraus- oder in ein CI hineinführt, und wählen Sie die entsprechende Verbindung aus. 
Quell- und Ziel-CI einer Verbindung, wenn die Bereichsstrukturansicht aktiviert ist Die Spanning Tree-Ansicht vereinfacht eine für	**a.** Klicken Sie auf das CI, dessen Verbindungen Sie anzeigen möchten. In der Zuordnung werden alle verborgenen Verbindungen für dieses CI angezeigt.

Automatische Übersetzung

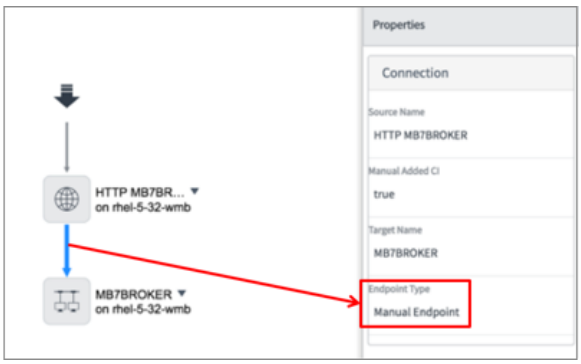
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzuzeigende Elemente	Aktion
Servicezuordnung, bei der die meisten Verbindungslinien verborgen sind.	**b.** Klicken Sie mit der rechten Maustaste auf die entsprechende Verbindungslinie.
Detailattribute einer regulären Verbindung im Bereich **Eigenschaften**	Klicken Sie auf die Verbindungslinie.
(Verfügbar für mit Service-Mapping erkannte Anwendungsservices) Detailattribute einer zusammengeführten Verbindung im Bereich **Eigenschaften**.	Klicken Sie auf die zusammengeführte Verbindungslinie, die mit einer Zahl gekennzeichnet ist. Alle zugrunde liegenden Verbindungen werden im Bereich **Eigenschaften** separat angezeigt. 
Detailattribute eines Verbindungssegments, das von mehr als einer zusammengeführten Verbindung genutzt wird, im Bereich **Eigenschaften**	Klicken Sie mit der rechten Maustaste auf die Verbindungslinie, die aus einem CI heraus- oder in ein CI hineinführt, und wählen Sie die entsprechende Verbindung sowie anschließend **Edge auswählen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzuzeigende Elemente	Aktion
	Die Detailattribute werden im Bereich **Eigenschaften** angezeigt. **Hinweis:** Bei gemeinsam genutzten Segmenten gibt es keinen Hinweis darauf, dass es sich um eine zusammengeführte Linie handelt.
(Verfügbar für mit Service-Mapping erkannte Anwendungsservices) Detaileigenschaften einer Verbindung im Bereich **Eigenschaften**, wenn die Bereichsstrukturansicht aktiviert ist. Die Spanning Tree-Ansicht vereinfacht eine für Servicezuordnung, bei der die meisten Verbindungslinien verborgen sind.	**a.** Klicken Sie auf das CI, dessen Verbindungen Sie anzeigen möchten. In der Zuordnung werden alle verborgenen Verbindungen für dieses CI angezeigt. **b.** Klicken Sie auf die erforderlich Verbindungslinie. 
(Verfügbar für mit Service-Mapping erkannte Anwendungsservices) Datenverkehrsbasierte Verbindungen für ein CI.	**a.** Klicken Sie mit der rechten Maustaste auf das CI, dessen datenverkehrsbasierte Verbindungen Sie prüfen möchten. **b.** Wählen Sie **Traffic-basierte Verbindungen anzeigen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzuzeigende Elemente	Aktion
Hinweis: Sie können datenverkehrsbasierte Verbindungen für ein CI anzeigen, auch wenn Sie die datenverkehrsbasierte Erkennung für einen für Service deaktiviert haben, zu dem das CI gehört.	Die Liste der datenverkehrsbasierten Verbindungen wird geöffnet und zeigt Informationen aus der Tabelle „Liste der Traffic-basierten Verbindungen“ an. **c.** Wenn Sie die Anzeige dieser Liste beenden möchten, klicken Sie auf **Schließen**.
Manuell hinzugefügte Verbindung. Manuell können Sie eine Verbindung oder ein CI hinzufügen. In beiden Fällen ist die Verbindung, die Sie manuell hinzufügen, ein Einstiegspunkt zur nächsten Ebene des Anwendungs-Flow.	Klicken Sie auf die manuell hinzugefügte Verbindung. Im Bereich **Eigenschaften** wird unter **Endpunkttyp** die Option „Manueller Endpunkt“ angezeigt. 

Liste der datenverkehrsbasierten Verbindungen (wenn Discovery basierend auf Predictive Intelligence deaktiviert ist)

Feld	Beschreibung
IP	Die IP-Adresse der Anwendung, die mit dem ausgewählten CI verbunden ist.
Port	Der Port des ausgewählten CI, der zur Kommunikation mit der anderen Anwendung verwendet wird.
Prozess	Die ID des Prozesses im ausgewählten CI.
Bereits in der Darstellung	◦ **Ja** – wenn diese Verbindung in der Zuordnung angezeigt wird. ◦ **Nein** – wenn diese Verbindung nicht Teil der Serviceinstanz und nicht in der Zuordnung ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Systementscheidung	Die Einstellung legt fest, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Der Wert stammt von dem Algorithmus, den Service-Mapping Verwendet.
Benutzerentscheidung	(Optional) Die Einstellung überschreibt die Einstellung Systementscheidung, in der festgelegt wird, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Wenn die Systementscheidungseinstellung für eine Verbindung beispielsweise Behalten lautet und Sie diese Verbindung entfernen möchten, wählen Sie `Entfernen`.

Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen

Sie können die Änderungen anzeigen, die an einem Anwendungsservice als Ganzes oder an den einzelnen Konfigurationselementen (CIs), aus denen der Service besteht, vorgenommen wurden. Die Change-Historie ist nützlich für Wartungs-, Planungs- oder Fehlerbehebungsverfahren.

Vorbereitungen

Erforderliche Rolle: admin, service_mapping_admin, service_mapping_user, app_service_admin oder app_service_user

Warum und wann dieser Vorgang ausgeführt wird

Details zu Änderungen an einer Serviceinstanz und an ihren CIs werden in der CMDB gespeichert. In der Regel handelt es sich bei diesen Änderungen um das Hinzufügen oder Entfernen von CIs zu einer Serviceinstanz, das Aktualisieren oder Aktualisieren von CIs oder das Ändern von CI-Konfigurationsdateien. Das System stellt diese Daten zusammen, indem es CMDB-Tabellen abfragt und dann die Change-Historienansicht erstellt. In Bereitstellungen, für die Service-Mapping aktiviert ist, hängt die Art der Abfragen der Change-Informationen durch Service-Mapping von Discovery-Mustern ab, die von Service-Mapping für die Erkennung von CIs verwendet werden.

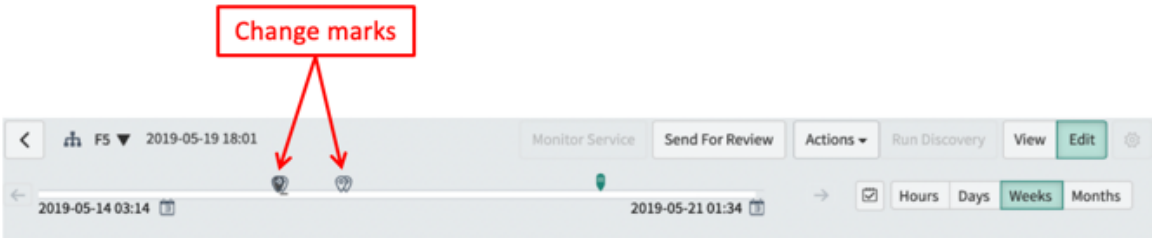
Änderungen an Konfigurationsdateien sind CIs zugeordnet, zu denen diese Dateien gehören. Karten zeigen Konfigurationsdateiänderungen als Änderungen an zugehörigen CIs an.

Sie können zwar Change-Datensätze für ein bestimmtes CI im Kontext von Anwendungsservices anzeigen, aber Sie können den detaillierten Verlauf eines bestimmten CI auch getrennt von seinem für Service anzeigen (siehe Verlaufszeitleiste) .

Wenn die Now Platform für die Validierung von Changes konfiguriert ist, werden alle Changes bewertet und als gültig oder nicht angezeigt. Wenn ein Change gültig ist, wird sein Change-Datensatz in der Zuordnung der Serviceinstanz als genehmigt markiert. Weitere Informationen zum Konfigurieren der Plattform für die Validierung von Changes finden Sie unter Vorgeschlagene Changes verwalten .

Changes an dem für Service erscheinen in der Verlaufszeitleiste.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Art der Änderungsmarke hängt von der Art der Changes ab, die sie darstellt:

Hellgrauer Ballon ( )

Nicht genehmigte Change, die das Verhalten der Serviceinstanz nicht beeinflusst. Zum Beispiel eine Change in einem Netzwerkpfad oder das Hinzufügen eines Knotens zu einem Cluster.

Dunkelgrauer Ballon ( )

Nicht genehmigte Change, die das Verhalten der Serviceinstanz ändert.

Grüner Ballon ( )

Eine genehmigte Change in Bereitstellungen, bei denen die Now Platform für die Validierung der Changes konfiguriert ist.

Doppelter Ballon ( )

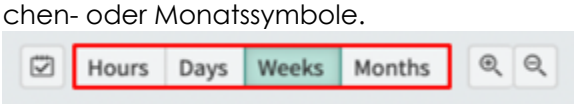
Mehrere getrennte Changes, die kurz hintereinander stattfanden.

Sie können Zeiten auf der Verlaufsskala markieren, indem Sie Baselines erstellen, um schnell zur markierten Ansicht zurückzukehren.

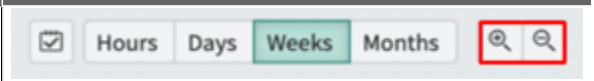
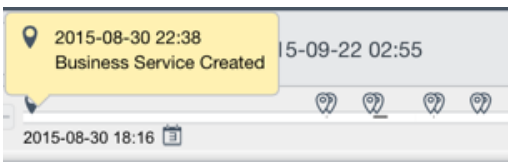
Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Zeigen Sie auf der Registerkarte **Changes** unten auf der Seite die Change-Datensätze an, die für diesen für Service erstellt wurden.

   Wenn Service-Mapping bereitgestellt ist, wird im Bearbeitungsmodus unterhalb der Zuordnung der Abschnitt „Discovery-Nachrichten“ angezeigt.
3. Legen Sie auf der Verlaufszeitleiste den Zeitbereich der Änderungen fest, die Sie anzeigen möchten.

Option	Aktion
Zeitbereich der Verlaufszeitleiste festlegen	Klicken Sie auf die Stunden-, Tages-, Wochen- oder Monatssymbole. 
Den Zeitbereich vergrößern oder verkleinern	Klicken Sie auf die Symbole zum Vergrößern und Verkleinern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

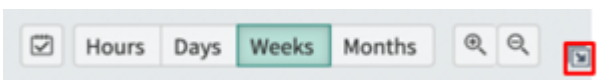
Option	Aktion
	
Um die obere Grenze Ihres Verlaufsbereichs zu ändern,	klicken Sie auf die Verlaufsskala. Die Zeit, die als Obergrenze dient, wird über der Verlaufszeitleiste angezeigt. **Hinweis:** Sie können den unteren Grenzwert für Ihren Verlaufsbereich nicht auf eine Zeit vor der Erstellung dieser Serviceinstanz festlegen. Diese Zeit ist mit dem Event **IT-Service erstellt** auf der Verlaufszeitleiste markiert. 

Die Zuordnung zeigt die Verlaufsansicht der Serviceinstanz für die von Ihnen ausgewählte Zeit.

Hinweis: Die Registerkarte **Änderung** zeigt alle Änderungssätze - auch die, die aus der Verlaufsansicht herausgefiltert werden.

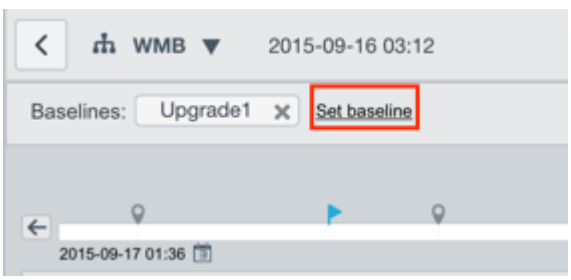
4. Um eine Zeit auf der Zeitskala zu markieren, legen Sie eine Baseline fest:

   a. Klicken Sie auf das Symbol **Vergleichen**.



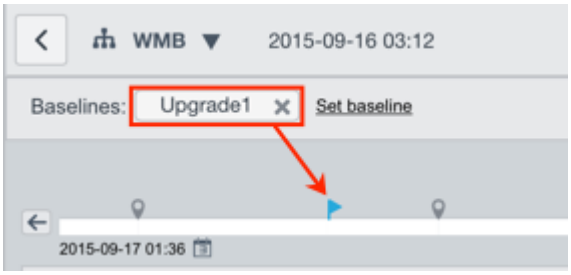
   b. Navigieren Sie zu der Zeit, zu der Sie eine Baseline auf der Verlaufsskala markieren möchten.

   c. Klicken Sie auf **Baseline festlegen**.

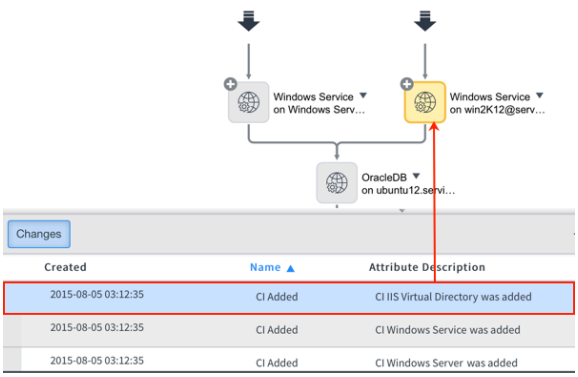
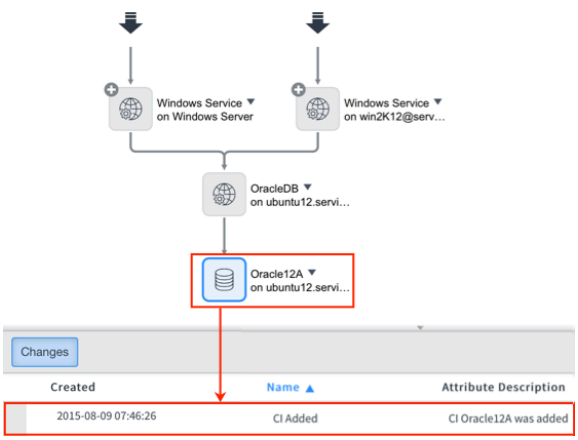


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Geben Sie den Namen der Baseline ein, und klicken Sie auf **OK**.
Die neue Baseline wird als Schaltfläche oberhalb der Verlaufsskala und als blaue Flagge auf der Verlaufsskala angezeigt.



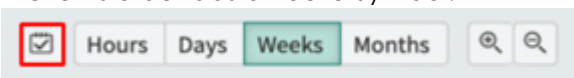
5. Zeigen Sie die Change-Historie an.

Option	Aktion
Für Änderungsdatensätze verantwortliche CIs anzeigen	Wählen Sie einen Änderungsdatensatz über die Registerkarte **Änderungen**. Das zugehörige CI ist in der Karte gelb markiert. 
Nur Change-Datensätze anzeigen, die sich auf ein CI beziehen	Wählen Sie das erforderliche CI oder die Verbindung auf der Karte. Auf der Registerkarte **Änderungen** werden nur Änderungsdatensätze angezeigt, die sich auf das ausgewählte CI oder die ausgewählte Verbindung beziehen. 

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
Konfigurationsdateien zu ausgewählten Zeitpunkten in der Vergangenheit anzeigen	**a.** Stellen Sie die Zeit auf der Verlaufsskala ein. **b.** Scrollen Sie in dem Fenster **Eigenschaften** zu **Verfolgte Konfigurationsdateien**, und klicken Sie auf den Dateinamen. Die neue Registerkarte wird mit dem Inhalt der verfolgten Konfigurationsdatei zu dem ausgewählten Zeitpunkt angezeigt.
Das Netzwerk zum ausgewählten Zeitpunkt in der Vergangenheit anzeigen	**a.** Stellen Sie die Zeit auf der Verlaufsskala ein. **b.** Klicken Sie mit der rechten Maustaste auf die Verbindung, und wählen Sie **Netzwerkpfad anzeigen**. Die neue Registerkarte wird mit der Netzwerk- oder Speicherpfadkarte für den von Ihnen ausgewählten Zeitpunkt angezeigt. **Hinweis:** Sie können den Netzwerkpfad für Verbindungen, die als Grenzen für dieses für Service markiert sind, nicht anzeigen.

6. Um die Verlaufsansicht zu verlassen und den aktuellen Status des für Service anzuzeigen, klicken Sie auf das aktuelle Symbol.



Zugehörige Informationen

Anwendungsservicezuordnung im Basissystem anzeigen

Zwei Versionen eines Anwendungsservice in klassisch Service-Mapping vergleichen

Nachverfolgung von Changes in Konfigurationsdateien ändern

Nachverfolgung von Changes für die Change-Historie feintunen

Zwei Versionen eines Anwendungsservice in klassisch Service-Mapping vergleichen

Sie können eine Zusammenfassung der Änderungen des Anwendungsservice auf einen Blick anzeigen, indem Sie zwei Versionen eines Anwendungsservice vergleichen. Diese Funktion ist hilfreich zur Überprüfung des Status des Anwendungsservice vor und nach einer bestimmten Änderung oder einem bestimmten Problem.

Vorbereitungen

Erforderliche Rolle: admin, app_service_admin, app_service_user, service_mapping_admin oder service_mapping_user

Warum und wann dieser Vorgang ausgeführt wird

Geben Sie zwei Zeitpunkte an, für die Sie die beiden Versionen eines Anwendungsservice vergleichen möchten. Sie können die Änderungsindikatoren in der Zeitleiste verwenden, um einen Zeitpunkt vor und einen anderen nach einer Änderung anzugeben, für die Details

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

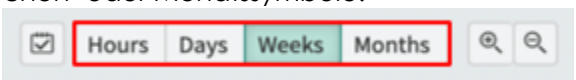
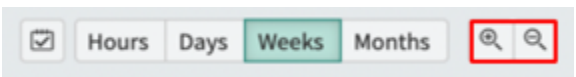
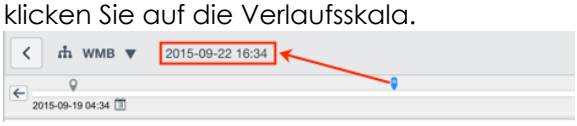
angezeigt werden sollen. Zum Beispiel können Sie, wenn Sie wissen, dass das Fehlschlagen eines Anwendungsservice zu einem bestimmten Zeitpunkt begonnen hat, zwei Versionen des Anwendungsservice (eine vor und eine nach Einsetzen des Problems) vergleichen. Dieser Vergleich zeigt Ihnen die Zusammenfassung der Changes, die möglicherweise zu den Problemen geführt haben.

Wenn Service-Mapping bereitgestellt ist, werden alle Änderungen an einem CI, einschließlich der dem CI zugeordneten Konfigurationsdateien, nachverfolgt und angezeigt. Wenn Sie zwei Versionen eines Anwendungsservice vergleichen, können Sie Änderungen an Konfigurationsdateien als Änderungen an CIs sehen. Sie können auch zwei Versionen einer Konfigurationsdatei vergleichen, um die tatsächlichen Changes in den Dateien innerhalb des für den Vergleich angegebenen Zeitraums anzuzeigen.

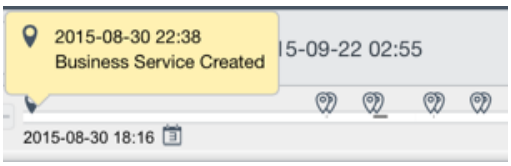
Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Klicken Sie bei Bedarf auf **Bearbeiten**, um sicherzustellen, dass sich die Karte im Bearbeitungsmodus befindet.

   Wenn Service-Mapping bereitgestellt ist, wird im Bearbeitungsmodus unterhalb der Zuordnung der Abschnitt „Discovery-Nachrichten“ angezeigt.
3. Legen Sie auf der Verlaufszeitleiste den Zeitbereich der Änderungen fest, die Sie anzeigen möchten.

Option	Aktion
Zeitbereich der Verlaufszeitleiste festlegen	Klicken Sie auf die Stunden-, Tages-, Wochen- oder Monatssymbole. 
Den Zeitbereich vergrößern oder verkleinern	Klicken Sie auf die Symbole zum Vergrößern und Verkleinern. 
Um die obere Grenze Ihres Verlaufsbereichs zu ändern,	klicken Sie auf die Verlaufsskala.  Die Zeit, die als Obergrenze dient, wird über der Verlaufszeitleiste angezeigt.

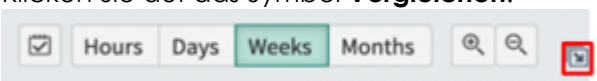
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	Hinweis: Sie können den unteren Grenzwert für Ihren Verlaufsbereich nicht auf eine Zeit vor der Erstellung dieser Serviceinstanz festlegen. Diese Zeit ist mit dem Event **IT-Service erstellt** auf der Verlaufszeitleiste markiert. 

Die Zuordnung zeigt die Verlaufsansicht der Serviceinstanz für die von Ihnen ausgewählte Zeit.

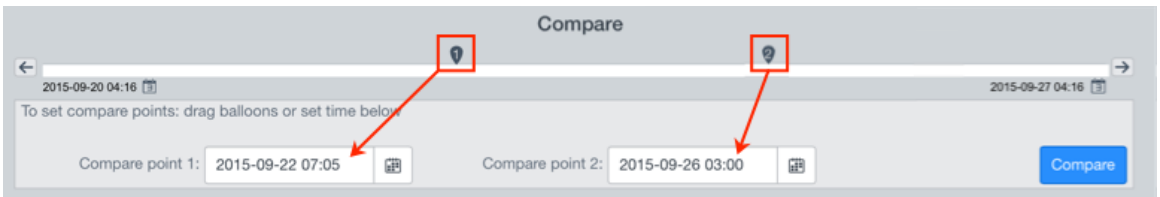
Hinweis: Die Registerkarte **Änderung** zeigt alle Änderungssätze - auch die, die aus der Verlaufsansicht herausgefiltert werden.

4. Klicken Sie auf das Symbol **Vergleichen**.



5. Stellen Sie **Vergleichspunkt 1** und **Vergleichspunkt 2** als die beiden Zeitpunkte für den Vergleich ein.

   Sie können die Zeiger auf der Verlaufsskala ziehen, um entsprechende Zeitpunkte festzulegen.



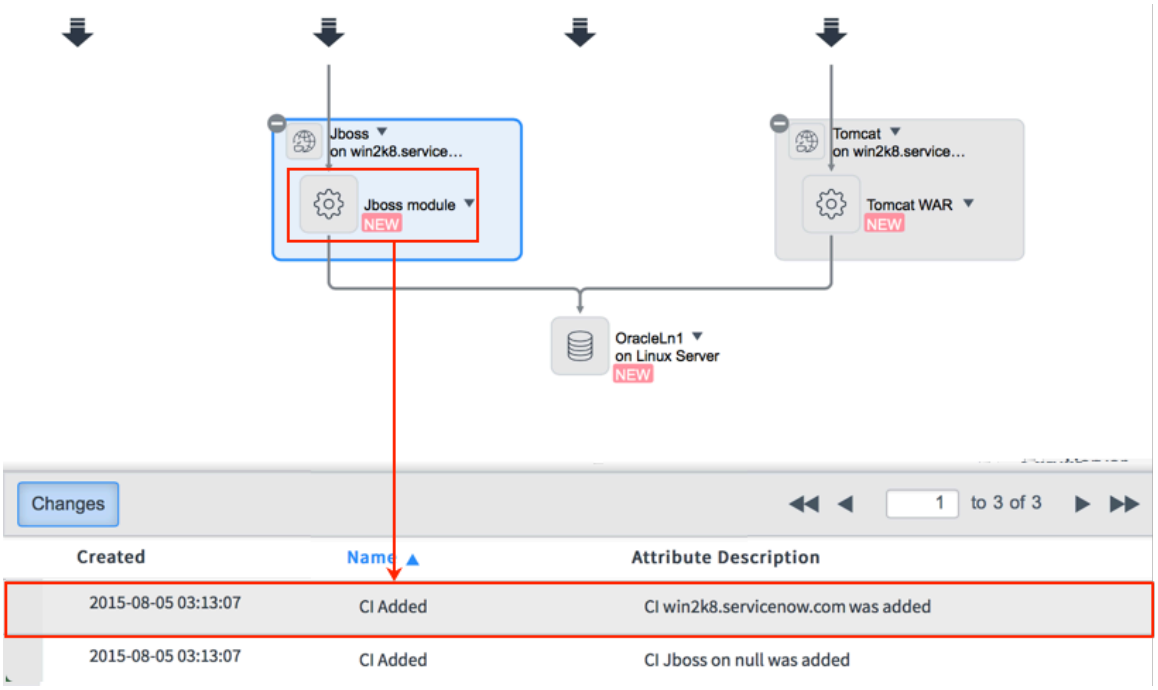
Configuration Management DatabaseWenn die Verlaufsskala den für den Vergleich festgelegten Zeitpunkt nicht enthält, wird der entsprechende Zeiger neben dem Vergleichspunkt in gelb angezeigt:

Hinweis: Wenn während des von **Vergleichspunkt 1** und **Vergleichspunkt 2** angegebenen Zeitintervalls keine Änderungen an dem Service vorgenommen werden, werden keine Änderungsdetails angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Vergleichen**.
   Die Vergleichsansicht wird in einer separaten Registerkarte geöffnet.
7. Wählen Sie ein markiertes CI aus, um den entsprechenden Änderungsdatensatz über die Registerkarte **Änderungen** anzuzeigen.



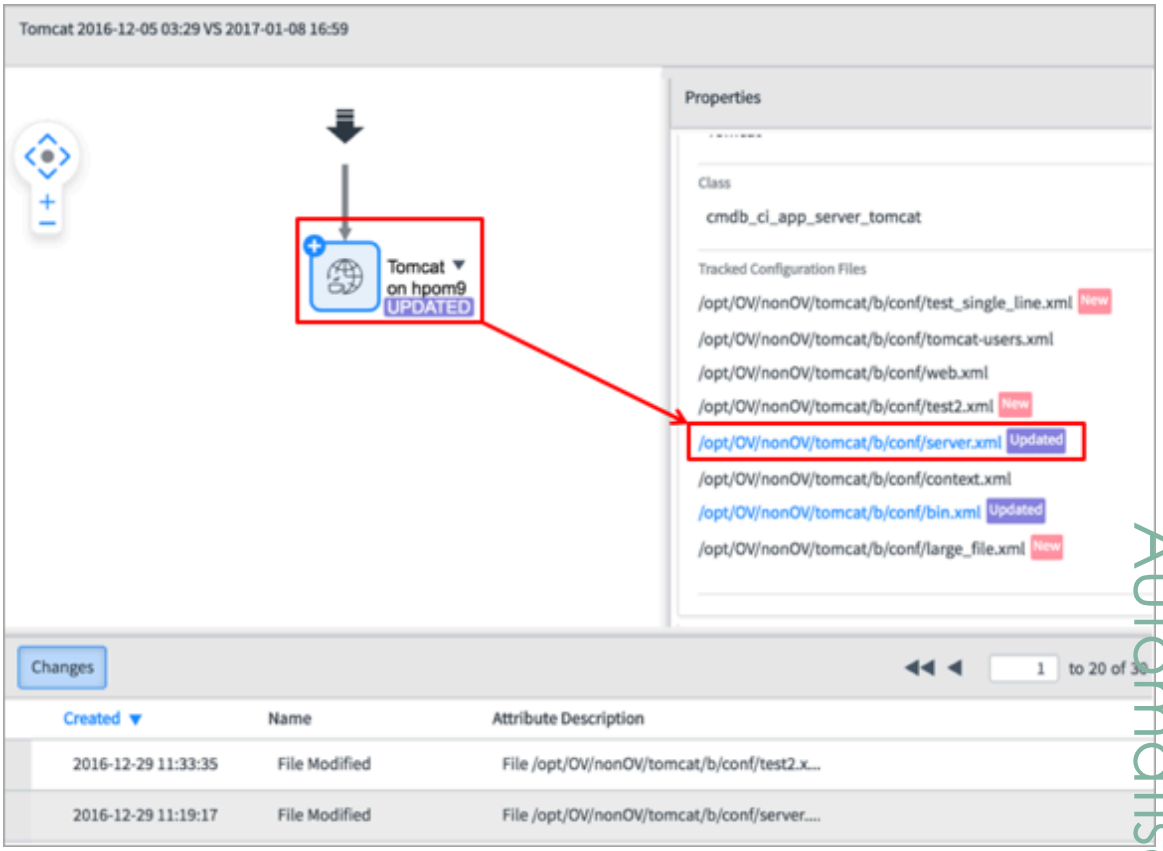
8. Wahlweise: Wenn Service-Mapping bereitgestellt wird, können Sie zwei Versionen einer Konfigurationsdatei vergleichen, die auf der Karte als „Aktualisiert“ angezeigt wird:

   a. Wählen Sie das CI aus, das der aktualisierten Konfigurationsdatei zugeordnet ist.

   b. Klicken Sie im Bereich **Eigenschaften** auf den Link zur aktualisierten Datei.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Registerkarte **Versionen von verfolgten Konfigurationsdateien vergleichen** wird geöffnet und zeigt zwei Versionen der Konfigurationsdatei nebeneinander an.

c. Überprüfen Sie die tatsächlichen Änderungen.

(Optional) Hervorhebungsfarben geben die Art der Änderung an:

- Lila - Aktualisierte Linie
- Pink - Neue Linie
- Grau - Zeile gelöscht

d. Navigieren Sie mit den Pfeilen in der oberen rechten Ecke zwischen den Änderungen.

e. Schließen Sie die Registerkarte **Versionen von verfolgten Konfigurationsdateien vergleichen**, wenn Sie fertig sind.

9. Schließen Sie die Vergleichsansicht, wenn Sie fertig sind.

Zugehörige Informationen

Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen

Versionen von CI-Konfigurationsdateien vergleichen

Abhängige Anwendungsservices in klassisch Service-Mapping anzeigen

Überprüfen Sie, welche Anwendungsservices von einem Anwendungsservice abhängig sind, und öffnen Sie Zuordnungen für abhängige Anwendungsservices.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: service_mapping_user

Warum und wann dieser Vorgang ausgeführt wird
Der Service, der einen Verweis auf eine andere Serviceinstanz enthält, wird zu einem abhängigen Service. Der Service, den Sie als Referenz einschließen, ist ein enthaltener Service.

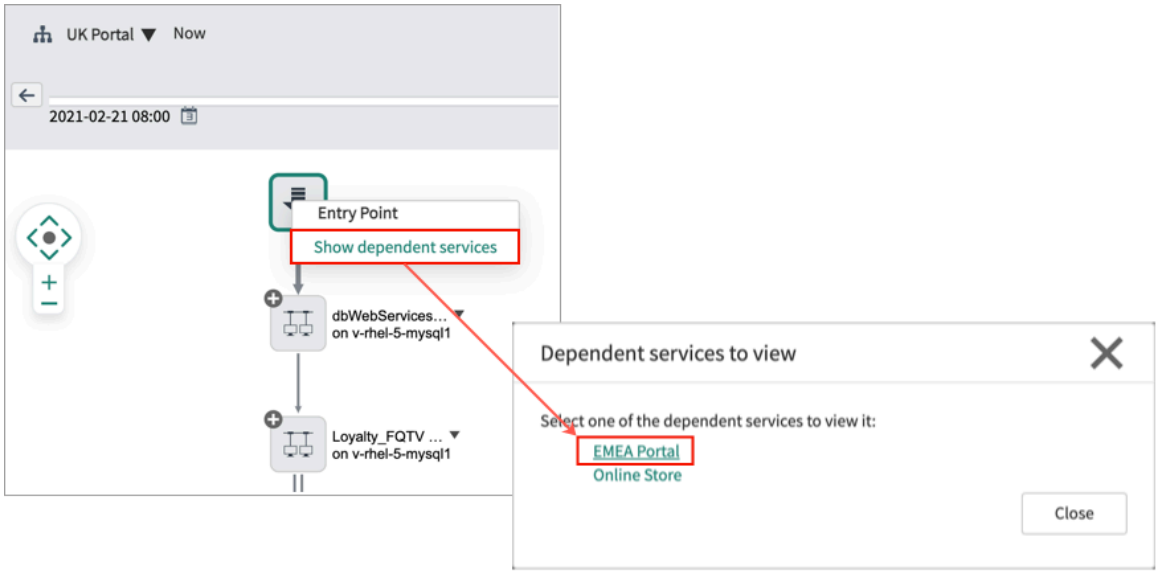
Abhängige Servicezuordnung mit Verweis auf enthaltenen Anwendungsservice

Prozedur
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Klicken Sie mit der rechten Maustaste auf den Einstiegspunkt, und wählen Sie **Abhängige Services anzeigen** aus.
   Im Popup-Fenster werden die Links zu allen abhängigen Services für diesen Anwendungsservice angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf den Link für den abhängigen Service, dessen Zuordnung Sie anzeigen möchten.



Im Zuordnungsfenster wird die Zuordnung für den ausgewählten abhängigen Service angezeigt.

Zugehörige Informationen

Anwendungsservices verknüpfen

Enthaltene Anwendungsservices in klassisch Service-Mapping anzeigen

Ein enthaltener Anwendungsservice ist eine Referenz, die in einem anderen, abhängigen Anwendungsservice enthalten ist. Sie können die Zuordnung des enthaltenen Service direkt aus der Zuordnung des abhängigen Service öffnen.

Vorbereitungen

Erforderliche Rolle: service_mapping_user

Warum und wann dieser Vorgang ausgeführt wird

Der Service, der einen Verweis auf eine andere Serviceinstanz enthält, wird zu einem abhängigen Service. Der Service, den Sie als Referenz einschließen, ist ein enthaltener Service.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängige Servicezuordnung mit Verweis auf enthaltenen Anwendungsservice

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Klicken Sie mit der rechten Maustaste auf das CI, das den enthaltenen Service darstellt, und wählen Sie **Enthaltenen Service anzeigen** aus.
   Die Zuordnung zeigt eine automatische Umleitung zur Webadresse für den enthaltenen Service. Es müssen keine zusätzlichen Registerkarten geöffnet werden.

CI-Abhängigkeiten überprüfen

Sie können prüfen, ob ein bestimmtes Konfigurationselement (CI) Teil eines anderes Anwendungsservice ist und ob es von anderen CIs abhängig ist.

Vorbereitungen

Erforderliche Rolle: admin, app_service_admin, app_service_user

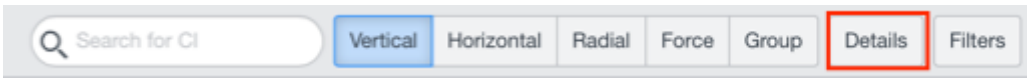
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Service-Mapping zeigt die Position eines CI in einem bestimmten Anwendungsservice. Ihre Organisation kann dasselbe CI jedoch auch in anderen Anwendungsservices verwenden. Wenn Sie Änderungen an diesem CI vornehmen möchten, müssen Sie sicherstellen, dass die Änderungen keine Auswirkungen auf andere Anwendungsservices haben.

Prozedur

1. Klicken Sie in der Zuordnung mit der rechten Maustaste auf das relevante CI, und wählen Sie **Ansicht der Abhängigkeiten öffnen** aus.
   Die Seite „Abhängigkeitsansichten“ wird in einer neuen Registerkarte geöffnet und zeigt das ausgewählte CI in der Mitte.
2. Klicken Sie auf **Details**.



3. Klicken Sie auf die Registerkarte **Zugehörige Services**.
   Die Liste der Links zu allen Anwendungsservices, die dieses CI enthalten, wird auf der Registerkarte **Zugehörige Services** angezeigt.
4. Klicken Sie auf den entsprechenden Link, um die Zuordnung eines anderen Anwendungsservice anzuzeigen, der dieses CI enthält.

Zugehörige Informationen

Anwendungsservicezuordnungen in klassisch Service-Mapping

Abhängigkeitsansichten

Netzwerk- oder Speicherpfad in klassisch Service-Mapping anzeigen

Um Probleme mit der Serviceleistung zu beheben oder um Ihr Netzwerk zu warten, können Sie einen Drilldown ausführen, um die Objekte hinter einer Verbindung in einer Zuordnung anzuzeigen. Für manuell erstellte Services oder Services in Instanzen mit Edge Encryption ist diese Funktion nicht verfügbar.

Vorbereitungen

Erforderliche Rolle: admin, service_mapping_admin oder service_mapping_user

Warum und wann dieser Vorgang ausgeführt wird

Durch die Anzeige eines Netzwerk- oder Speicherpfads können Sie Router, Switches und Hostports anzeigen, die Teil der Verbindung sind. Die folgenden Verbindungstypen sind vorhanden:

Netzwerkpfad

Die Infrastrukturroute zwischen zwei CIs vom Typ Host.

Speicherpfad

Die Infrastrukturroute zwischen einem CI vom Typ Host und einem CI vom Typ Speicher.

Service-Mapping erkennt keine Netzwerkgeräte im WAN oder in der öffentlichen Cloud, sondern nur solche, die sich im lokalen Netzwerk Ihrer Organisation befinden, und zeigt sie an. Wenn Service-Mapping auf eine Verbindung zwischen zwei Anwendungen stößt, wird mithilfe von traceroute der Pfad vom Quellhost zum Zielhost ermittelt. Dann verwendet Service-Mapping die SNMP-Anmeldeinformationen, um die im Pfad gefundenen Geräte zu erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping kann Geräte für Speicherpfade mit den folgenden Protokollen anzeigen:

- Fiber Channel: Storage Area Network (SAN)
- IP-Ethernet: Internet Small Computer Systems Interface (iSCSI) oder Network Attached Storage (NAS)

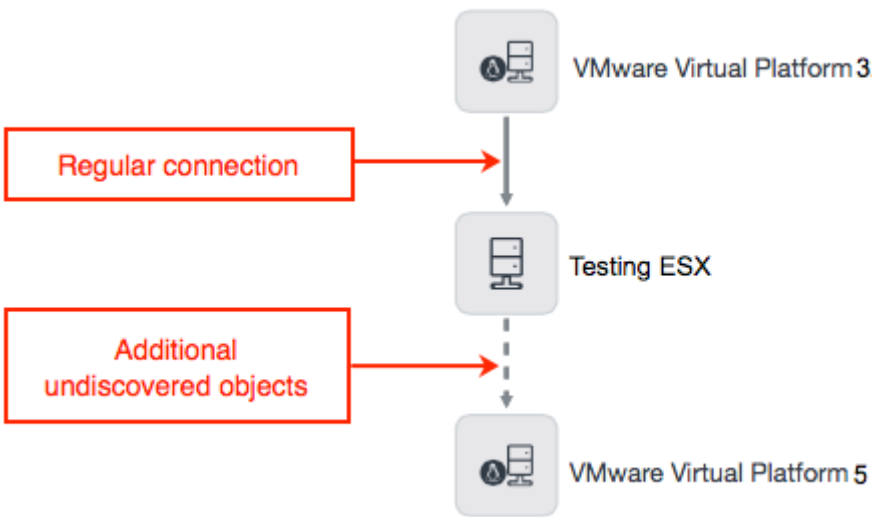
> **Hinweis:** Für Speicherpfade, die Fibre Channel verwenden, zeigt Service-Mapping keine Fibre Channel Switches an.

Zwischen einem Host-CI und einem Speicher-CI können zwei separate Speicherpfade mit unterschiedlichen Protokollen vorhanden sein: Fibre Channel und IP-Ethernet. Wenn das der Fall ist, zeigt die Zuordnung des für Service eine Verbindungslinie für beide Protokolle an.

Sie können die Change-Historie für Netzwerk- und Speicherpfade für Anwendungsservices anzeigen. Eine Überprüfung der Pfadhistorie für manuelle oder technische Services wird nicht unterstützt.

Prozedur

1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Klicken Sie in der Zuordnung mit der rechten Maustaste auf die Verbindung für den Netzwerk- oder Speicherpfad, den Sie sehen möchten.
3. Wählen Sie **Netzwerkpfad anzeigen** oder **Speicherpfad anzeigen** aus.
4. Wählen Sie bei Bedarf den Protokolltyp aus, und klicken Sie im Dialogfeld „Protokolltyp auswählen“ auf **Auswählen**.
   Die Ansicht mit dem Netzwerk- oder Speicherpfad wird auf einer neuen Registerkarte geöffnet.



Wenn Service-Mapping nicht alle Objekte in einer Verbindung erkennen kann, wird die Connector-Linie im Netzwerk- oder Speicherpfad wie oben dargestellt gepunktet angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Verwenden Sie für Speicherpfade die Registerkarte „Speicherzuordnung“ am unteren Bildschirmrand, um die Korrelation zwischen Dateisystemen auf dem Host und dem Speichervolume oder dem freigegebenen Ordner auf dem Speichergerät anzuzeigen.
6. Führen Sie die Schritte unter Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen aus , um die Change-Historie für Netzwerkpfade anzuzeigen.
7. Wenn Sie von Ereignismanagement aus auf die Netzwerk- oder Speicherpfadzuordnung zugreifen, wird die Liste der zu diesem Pfad gehörenden Warnungen unten im Bildschirm angezeigt.

Zugehörige Informationen

Anwendungsservicezuordnungen in klassisch Service-Mapping

SNMP-basierte Abfragen

Liste der einem Anwendungsservice zugehörigen CIs anzeigen

Zeigen Sie eine vollständige Liste von CIs an, aus denen ein Anwendungsservice besteht, einschließlich der CIs, die nicht in der Anwendungsservicezuordnung angezeigt werden: nachverfolgte Konfigurationsdateien, Endpunkte, Prozesse und Netzwerkgeräte.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin oder service_mapping_user

Warum und wann dieser Vorgang ausgeführt wird

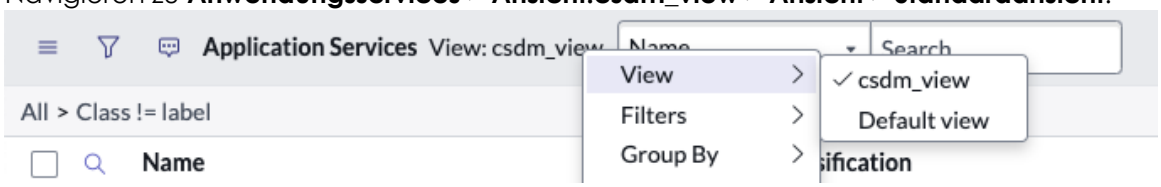
Standardmäßig werden in Anwendungsservicezuordnungen Anwendungs-CIs und Verbindungen zwischen diesen angezeigt. Die übrigen CIs hinter Anwendungen und die Verbindungen zwischen ihnen sind ausgeblendet. In der CI-Liste werden die folgenden zusätzlichen CIs angezeigt:

- Server, die Anwendungen hosten
- Netzwerkgeräte wie Router oder Switches
- Prozesse, die auf Hosting-Servern ausgeführt werden. Prozesse werden zur Identifizierung und Klassifizierung von Anwendungen verwendet.
- Nachverfolgte Konfigurationsdateien für Anwendungen, die Teil des Service sind
- Endpunkte, die zu den Anwendungen gehören. Endpunkte enthalten Informationen, die für die Verbindung mit Anwendungen erforderlich sind, zum Beispiel Hosts und Ports.
- Das Anwendungsservice-CI für diesen Anwendungsservice

Die CI-Listen für leere Anwendungsservices, die keine CIs enthalten, enthalten nur ein einziges CI: für den Anwendungsservice selbst.

Prozedur

1. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
2. Navigieren zu **Anwendungsservices** > **Ansicht:csdm_view** > **Ansicht** > **Standardansicht**.

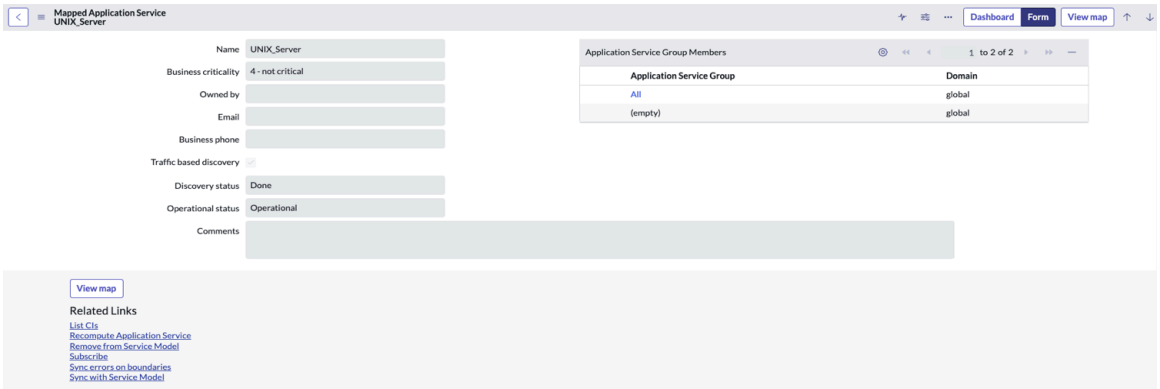


3. Klicken Sie auf den Namen des Anwendungsservice, für den Sie die Liste der CIs anzeigen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Erkennungsstatus des ausgewählten Service muss **Fertig** lauten.

4. Klicken Sie unter Zugehörige Links auf **CIs auflisten**.



5. Zeigen Sie die vollständige Liste der CIs an, die Teil des ausgewählten Anwendungsservice sind.
6. Klicken Sie in Ihrem Browser auf die Schaltfläche „Zurück“, um zur Seite „Zugeordneter Anwendungsservice“ zurückzukehren, wenn Sie die Überprüfung der CI-Liste abgeschlossen haben.
7. Wählen Sie **Karte anzeigen** aus, um zur Anwendungsservice-Zuordnung zu navigieren.

Anwendungsservicezuordnungen in PDFs konvertieren

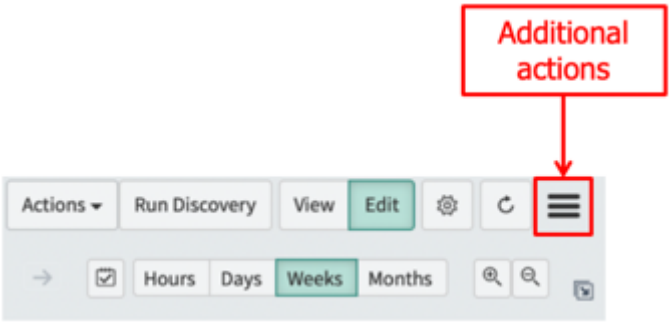
Sie können eine PDF-Datei für eine Zuordnung erstellen, um Informationen über den Serviceinhalt mit anderen Personen zu teilen. PDF-Dateien sind besonders nützlich während des Überprüfungs- und Genehmigungsprozesses für von Service-Mapping erkannte Anwendungsservices.

Vorbereitungen
Erforderliche Rolle: app_service_admin, app_service_user

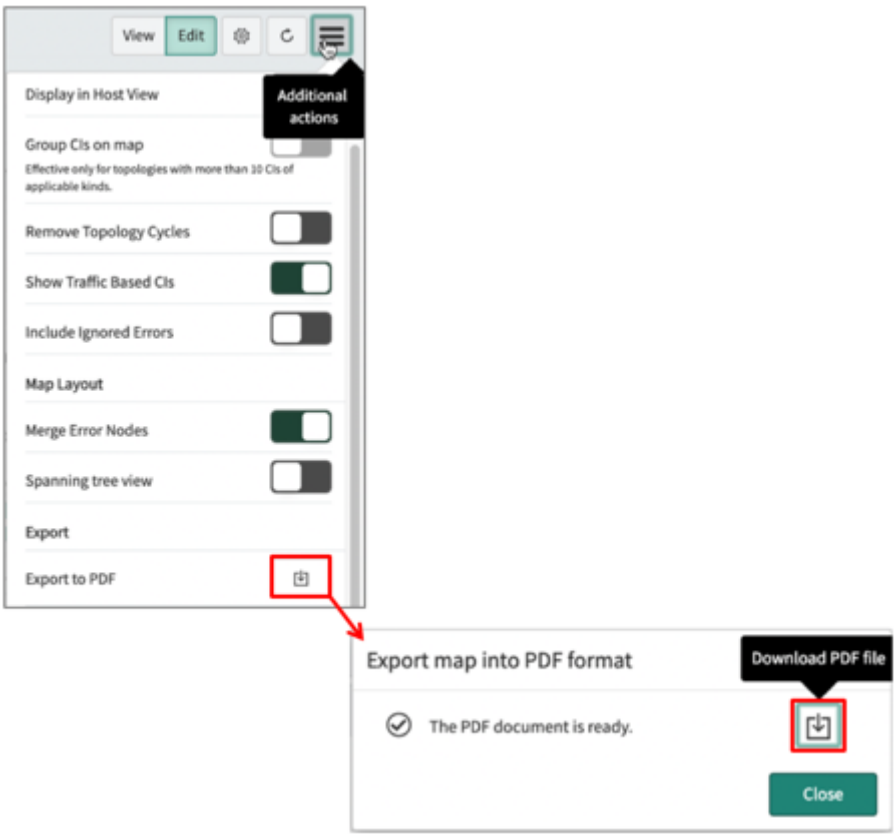
Warum und wann dieser Vorgang ausgeführt wird
Die PDF-Datei der Anwendungsservicezuordnung zeigt den Namen des Anwendungsservice und den genauen Zeitpunkt der Erstellung der PDF-Datei.

Prozedur
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Klicken Sie auf das Menü **Zusätzliche Aktionen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf die Schaltfläche neben der Option **PDF-Export**.



4. Wenn die PDF-Datei fertig ist, klicken Sie im Dialogfeld „Zuordnung im PDF-Format exportieren“ auf die Schaltfläche **PDF herunterladen**.
Das PDF-Dokument wird in den Ordner „Downloads“ auf Ihrem Computer geladen.

Ansicht für Anwendungsservicezuordnung ändern

Passen Sie eine Zuordnungsansicht an, um relevante Informationen anzuzeigen und die Übersichtlichkeit zu erhöhen.

Vorbereitungen

Erforderliche Rolle: app_service_admin, app_service_user, service_mapping_admin oder service_mapping_user

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig sind Servicezuordnungen präzise und enthalten alle Details zu allen CIs, die Sie manuell hinzugefügt haben oder die von Service-Mapping zugeordnet wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

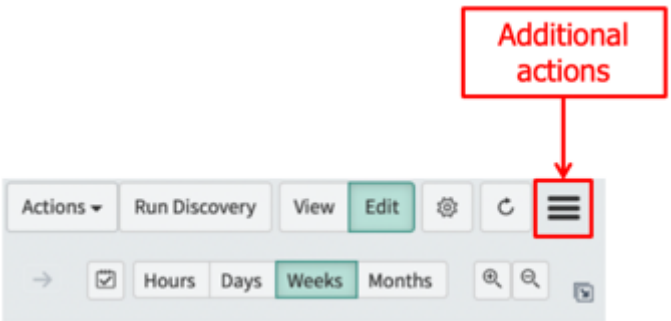
Obwohl sie ein umfassendes Bild vermittelt, könnte die Verwendung einer solchen Zuordnung schwierig sein. Durch das Anpassen der Zuordnungen können Sie:

- die Navigation in der Zuordnung erleichtern
- irrelevante Informationen ausblenden
- wichtige Informationen anzeigen

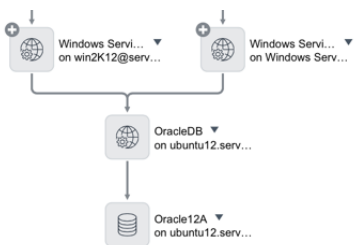
Attribute, die Sie beim Anpassen von Zuordnungen anzeigen oder ausblenden, werden nicht dauerhaft entfernt und können nach Bedarf wieder angezeigt oder ausgeblendet werden. Das System speichert die Änderungen in der Zuordnungsansicht und zeigt die letzte Zuordnungsansicht an, wenn Sie eine Serviceinstanz erneut öffnen.

Prozedur

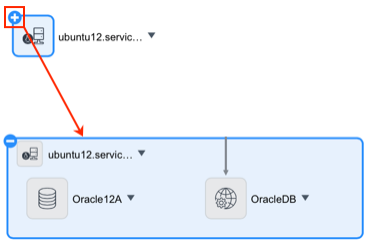
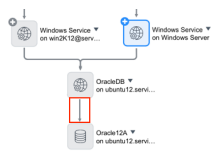
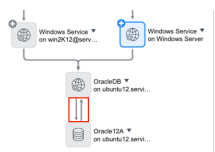
1. Öffnen Sie die Serviceinstanzzuordnung.
   a. Navigieren zu **Alle** > **CSDM** > **Technologiemanagement-Services verwalten** > **Serviceinstanz**.
   b. Wählen Sie die benötigte Serviceinstanz aus.
   c. Wählen Sie auf der Seite der Serviceinstanz **Karte anzeigen**aus.
2. Klicken Sie auf das Menü **Zusätzliche Aktionen**.



3. Wählen Sie die relevante Option aus:

Option	Wenn aktiviert	Wenn deaktiviert
In Host-Ansicht anzeigen Diese Option ist nur verfügbar, wenn das Service-Mapping-Plugin aktiviert ist. Wechseln Sie zwischen der CI-Ansicht, in der Hosts ausgeblendet werden, und der Host-Ansicht, in der CIs ausgeblendet werden. Die Host-Ansicht kann dabei helfen zu bestimmen, dass von Service-Mapping alle Hosts richtig erkannt und zugeordnet wurden, und	Von der Servicezuordnung werden Host-CIs dargestellt. Klicken Sie auf die Plus-Symbole, um Anwendungs-CIs anzuzeigen, die auf den Hosts ausgeführt werden.	In der Servicezuordnung werden Anwendungs-CIs dargestellt.  Im Bereich **Eigenschaften** werden nur Informationen zu Servern angezeigt, die als Hosts fungieren, sowie zu Anwendungen, die auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
hilft, Verbindungen zu jedem Host zu finden. Die Host-Ansicht vereinfacht auch die Zuordnung, insbesondere wenn viele Anwendungen auf wenigen Hosts ausgeführt werden. Die Host-Ansicht ist nur für Serviceinstanzen nützlich, die mit Service-Mappingerkannt wurden. Diese Ansicht enthält keine zusätzlichen Informationen für manuell erstellte Serviceinstanzen.	 Im Bereich **Eigenschaften** werden nur Informationen zu Servern angezeigt, die als Hosts fungieren.	diesen Hosts ausgeführt werden.
CIs in Zuordnung gruppieren Vereinfachen Sie Zuordnungen, indem Sie CIs gruppieren, die zu demselben Typ gehören und auf Servern gehostet werden, die sich Präfix und Domänennamen teilen. Die Zuordnung gibt den Anwendungs-Flow weiterhin korrekt wieder, da gruppierte CIs zur selben Ebene gehören. Diese Option ist für Serviceinstanzen relevant, die aus mehr als 10 CIs bestehen.	In der Serviceinstanzzuordnung werden Gruppen von CIs angezeigt. Die Zuordnung ist kompakter.	In der Serviceinstanzzuordnung werden alle CIs separat angezeigt. Die Zuordnung ist größer.
Topology Cycles entfernen Diese Option ist nur für Anwender mit den folgenden Rollen verfügbar: Service-Mapping-Administrator [service_mapping_admin] und Service-Mapping-Anwender [service_mapping_user]. Blenden Sie Verbindungen aus, die zu demselben Configuration Item (CI) zurückkehren, von dem sie stammen, um die	In der Serviceinstanzzuordnung werden Topologiezyklen ausgeblendet. 	In der Zuordnung der Serviceinstanz werden Topologiezyklen angezeigt. 

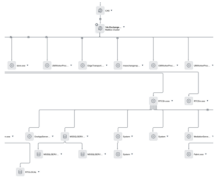
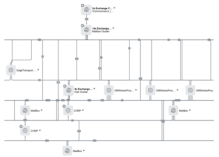
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
Übersichtlichkeit der Zuordnung zu verbessern. Normalerweise sind diese zurückkehrenden Verbindungen für die Analyse oder Fehlerbehebung von Serviceinstanzen irrelevant.		
Datenverkehrsbasierte CIs anzeigen Diese Option ist nur für Anwender mit den folgenden Rollen verfügbar: Service-Mapping-Administrator [service_mapping_admin] und Service-Mapping-Anwender [service_mapping_user]. Zeigen Sie mithilfe von datenverkehrsbasierter Zuordnung gefundene Configuration Items (CIs) an.	In der Zuordnung der Serviceinstanz werden CIs und Hosts angezeigt, die Service-Mapping mithilfe von Mustern und Traffic-basierter Discovery erkannt hat. Das Erkennen des eingehenden und ausgehenden Datenverkehrs von CIs führt zwar zu einer inklusiven Zuordnung, kann aber auch zur Zuordnung vieler redundanter CIs führen, die den Betrieb der Serviceinstanz nicht beeinflussen.	In der Zuordnung der Serviceinstanz werden nur CIs und Hosts angezeigt, die anhand von Mustern erkannt wurden.
Fehlerknoten zusammenführen Diese Option ist nur für Anwender mit der Rolle eines Service-Mapping-Administrators [service_mapping_admin] verfügbar. Führen Sie CIs mit Fehlern zusammen, die durch dasselbe Quell-CI verursacht werden, um die Zuordnung eines für Service übersichtlicher zu gestalten. Ein Erkennungs- oder Betriebsfehler in einem CI wirkt sich häufig auf alle darunter liegenden Verbindungen in der Hierarchie aus, wodurch Ihre Ansicht überfrachtet wird. Sie können durch dasselbe	Alle CIs mit identischen Fehlern sind in der Zuordnung des für Service in einem einzelnen CI zusammengeführt. Die Zahl in der Connector-Zeile gibt die Anzahl der CIs mit diesem Fehler an. 	In der Zuordnung des für Service werden alle CIs mit identischen Fehlern separat angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
CI verursachte, identische Fehler entfernen, indem Sie sie in der Zuordnung zu einem einzelnen Objekt zusammenführen. Wenn beispielsweise ein CI einen Fehler in sechs damit verbundenen CIs verursacht, können Sie in der Zuordnung nur ein einziges CI mit diesem Fehler anzeigen. Die Connector-Zeile gibt die Anzahl der tatsächlichen Verbindungen wieder.		
Zuordnungsindikatoren Diese Option ist nur für Anwender mit den folgenden Rollen verfügbar: Serviceanwender [app_service_user] und Service-Mapping-Anwender [service_mapping_user]. Zeigen Sie zusätzliche Informationen für ein CI oder die Serviceinstanz selbst an, indem Sie zugehörige Datensätze wie Warnungen, Ausfälle, Incidents und Probleme anzeigen. Das Basissystem bietet Kartenindikatoren für die folgenden Datensatztypen: ◦ Betroffene CIs ◦ Offene Warnungen ◦ Aktuelle, geplante oder kürzlich erfolgte Change-Anforderungen ◦ Offene Incidents ◦ Aktuelle, geplante oder kürzlich erfolgte Ausfälle ◦ Offene Probleme Weitere Informationen finden Sie unter Ereignismanagement-Kartenindikatoren (Video) .	Für jeden Datensatztyp, der für die Anzeige festgelegt ist, werden der entsprechende Indikator und die Registerkarte angezeigt. Beispielsweise wird die Registerkarte **Incidents** unter der Zuordnung angezeigt. Der Indikator **Incidents** wird neben CIs angezeigt, denen Incidents zugeordnet sind. 	In der Zuordnung der Serviceinstanz werden CIs ohne zugehörige Indikatoren angezeigt.
	Wenn ein Datensatz dem für Service selbst zugeordnet ist, wird der Indikator neben dem Namen des für Service angezeigt. 	Neben dem Namen des für Service sind keine Zuordnungsindikatoren zu sehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
Strukturansicht wird segmentiert Vereinfachen Sie die Zuordnung, indem Sie CIs in einer Baumstruktur anordnen und manche der Verbindungslinien verbergen. Diese Option ist besonders für sehr große Karten nützlich.	In der Zuordnung wird eine Serviceinstanz als Struktur angezeigt.  Um tatsächliche Verbindungen anzuzeigen, zeigen Sie auf ein CI. Weitere Informationen zum Anzeigen von Verbindungen finden Sie unter Zeigen Sie CI-Verbindungsattribute in einer Anwendungsservicezuordnung in an klassisch Service-Mapping.	Die Zuordnung spiegelt die tatsächliche Struktur einer Serviceinstanz wider. 
Ignorierte Fehler einschließen Diese Option ist nur für Anwender mit der Rolle eines Service-Mapping-Administrators [service_mapping_admin] verfügbar. Sie können Fehler anzeigen, die zuvor in der Zuordnung ausgeblendet wurden.	In der Zuordnung werden alle (aktiven und ignorierten) Fehler angezeigt.	Ignorierte Fehler werden in der Zuordnung nicht angezeigt.

Analyse und Wartung von Anwendungsservices mithilfe von veraltet Mitarbeiterbereich

Service-Mapping erstellt Zuordnungen, mit deren Hilfe Sie die Architektur und Organisation von Anwendungsservices anzeigen können. Diese Zuordnungen sind nützlich bei der Planung von Änderungen oder Migrationen sowie zur Analyse der Kontinuität und Verfügbarkeit von Services.

Anwendungsservicezuordnungen in veraltet Mitarbeiterbereich

Zuordnungen bieten Ihnen eine Visualisierung von Daten zu Konfigurationselementen (CIs), die Anwendungsservices umfassen, sowie Beziehungen und Verbindungen zwischen diesen CIs.

Eine neue Zuordnung wird jedes Mal erstellt, wenn Sie einen für Service manuell erstellen oder einen für Service mithilfe von Service-Mappingzuordnen. Das System aktualisiert die Zuordnung jedes Mal, wenn Sie CIs zu für Service hinzufügen oder wenn Service-Mapping eine Erkennung für CIs ausführt, die zu für Service gehören.

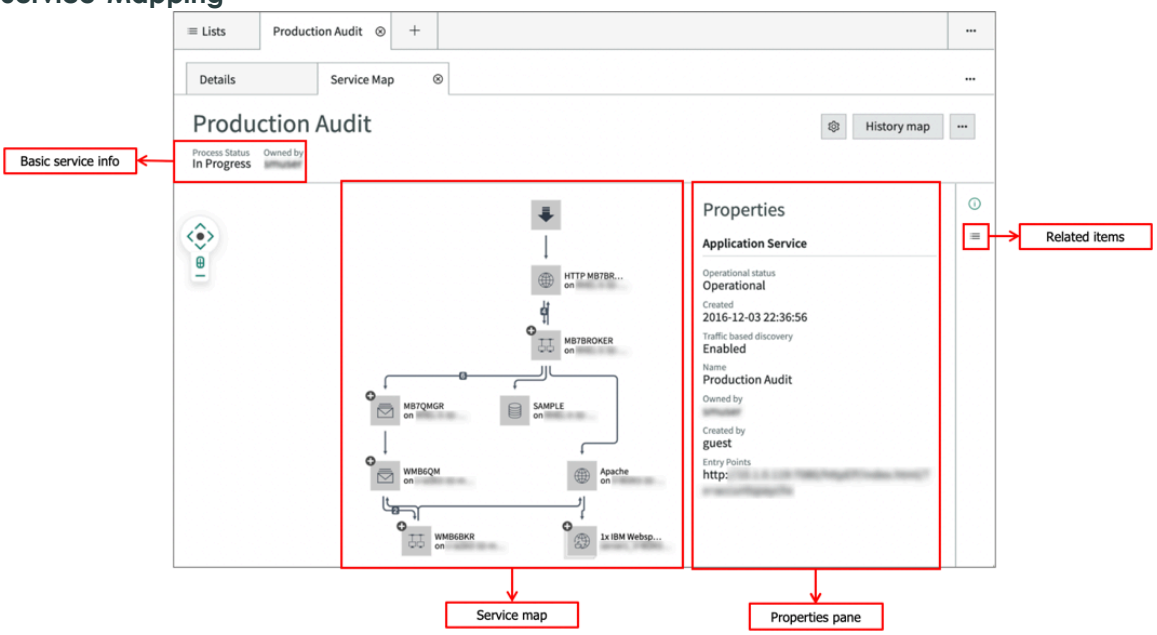
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungsfenster

Neben der Zuordnung selbst können in der Servicezuordnung auch grundlegende Serviceinformationen wie Schweregrad, Status und Anwendungsbesitzer des Service angezeigt werden. Auch im Eigenschaftenbereich für den Service können Sie zusätzliche Serviceinformationen anzeigen. Klicken Sie auf das Symbol „Zugehörige Elemente“, um alle Warnungen oder Änderungen anzuzeigen, die mit CIs in diesem Anwendungsservice verknüpft sind oder den Anwendungsservice selbst betreffen.

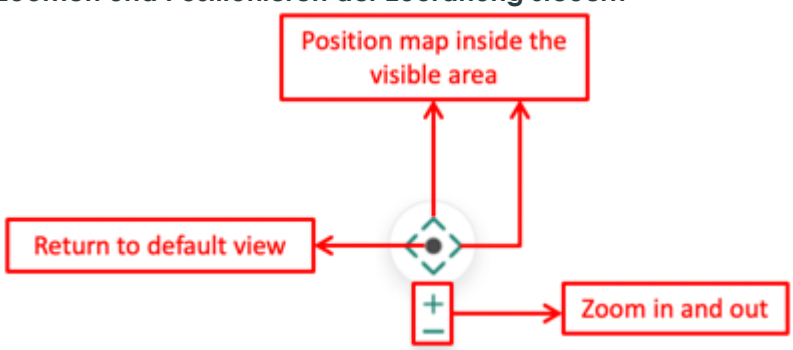
Die Serviceinstanzzuordnung in der Ansicht Ereignismanagement spiegelt den Schweregradstatus der CIs wider, die zu der Serviceinstanz gehören.

Service-Mapping



Standardmäßig wird die gesamte Zuordnung in der Mitte des sichtbaren Fensterbereichs der Zuordnung angezeigt. Positionieren Sie die Zuordnung und vergrößern oder verkleinern Sie sie mit den folgenden Steuerungen.

Zoomen und Positionieren der Zuordnung steuern



Sie können auch auf eine beliebige Stelle im Zuordnungsbereich klicken und das gewünschte Segment der Zuordnung in den sichtbaren Bereich ziehen.

CI-Attribute und CI-bezogene Nachrichten

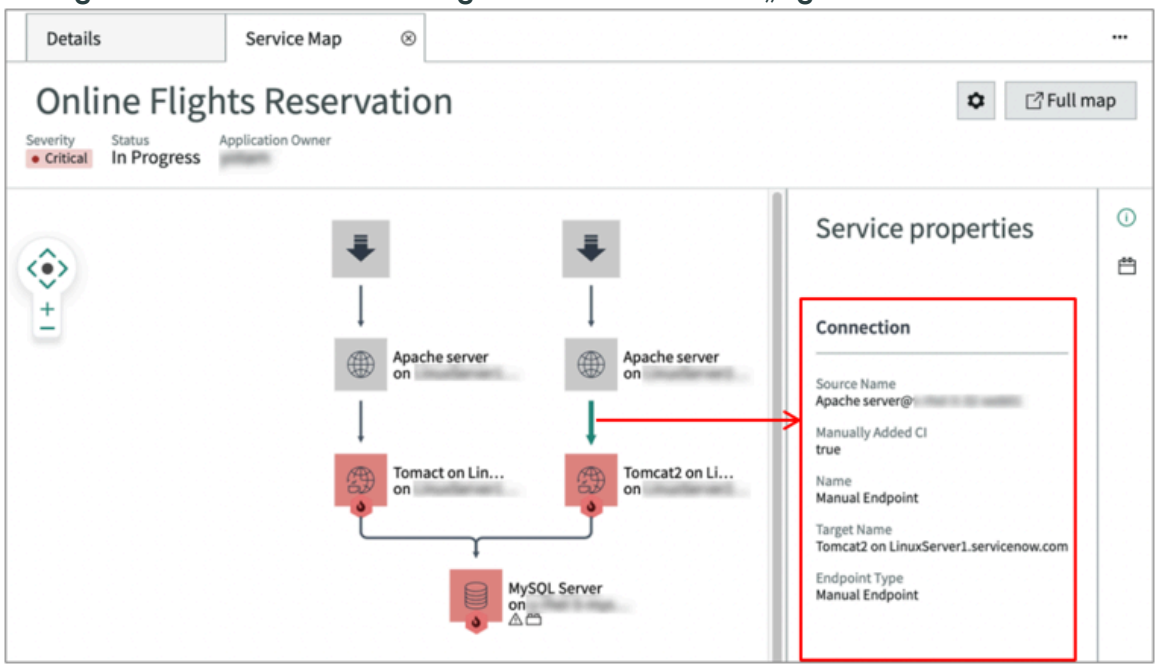
Wenn eine Zuordnung geladen ist und keine Elemente ausgewählt sind, werden im Bereich „Serviceeigenschaften“ die Details dieses für Service angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

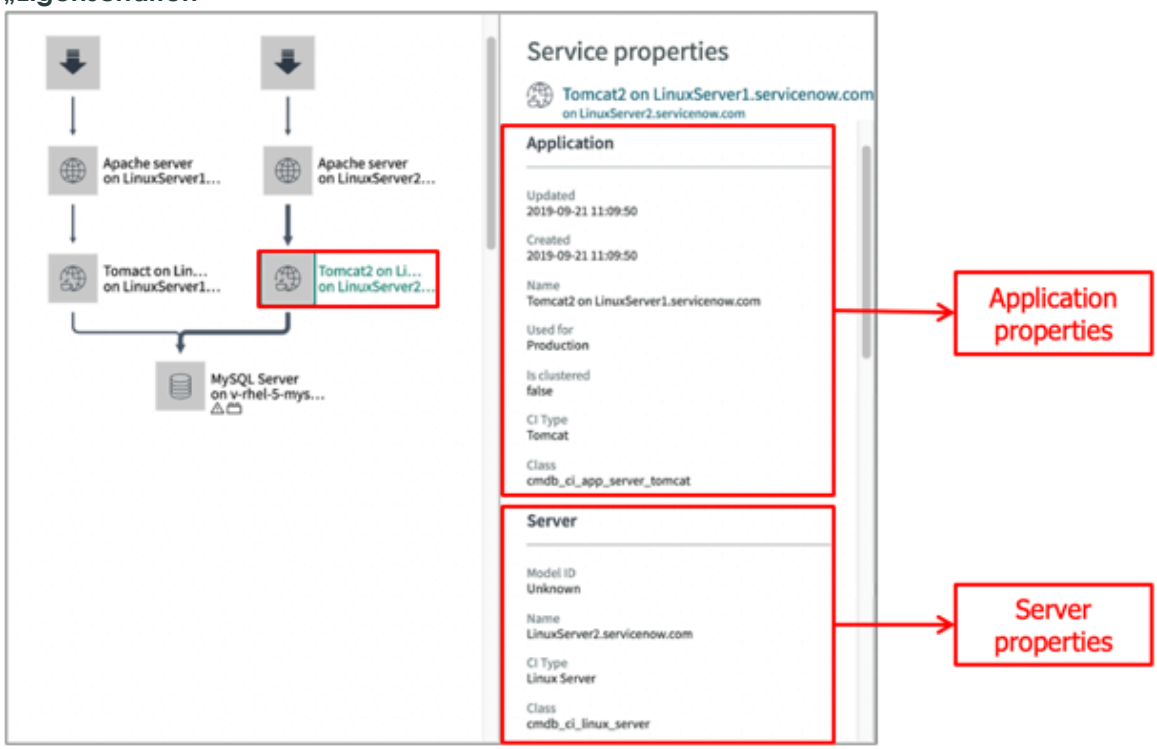
Ausgewählte Geräte, Anwendungen oder Connectors werden grün angezeigt und sind hervorgehoben. Informationen zum ausgewählten Zuordnungselement werden im Eigenschaftenbereich rechts von der Zuordnung angezeigt.

Anzeige der Attribute für Verbindungen und CIs im Bereich „Eigenschaften“



Die Attribute für den Server, auf dem die Anwendungen gehostet werden, und die Anwendungen selbst werden im Bereich „Eigenschaften“ getrennt angezeigt.

Separate Anzeige der Attribute für Hosts und Anwendungen im Bereich „Eigenschaften“



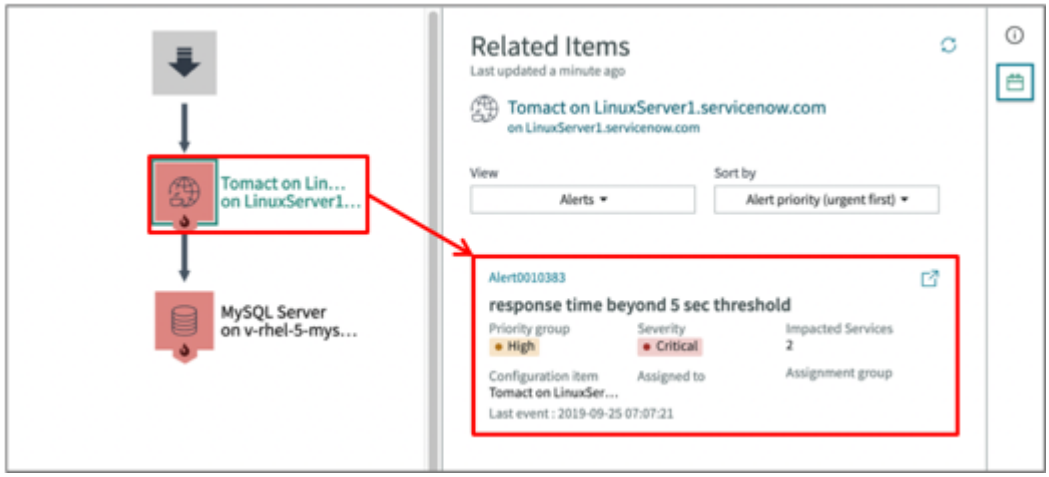
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zu Next-Gen BSM zugehörige Elemente

Klicken Sie auf das Symbol **Zugehörige Elemente**, um alle Warnungen oder Änderungen anzuzeigen, die mit diesem Anwendungsservice oder seinen CIs verknüpft sind.

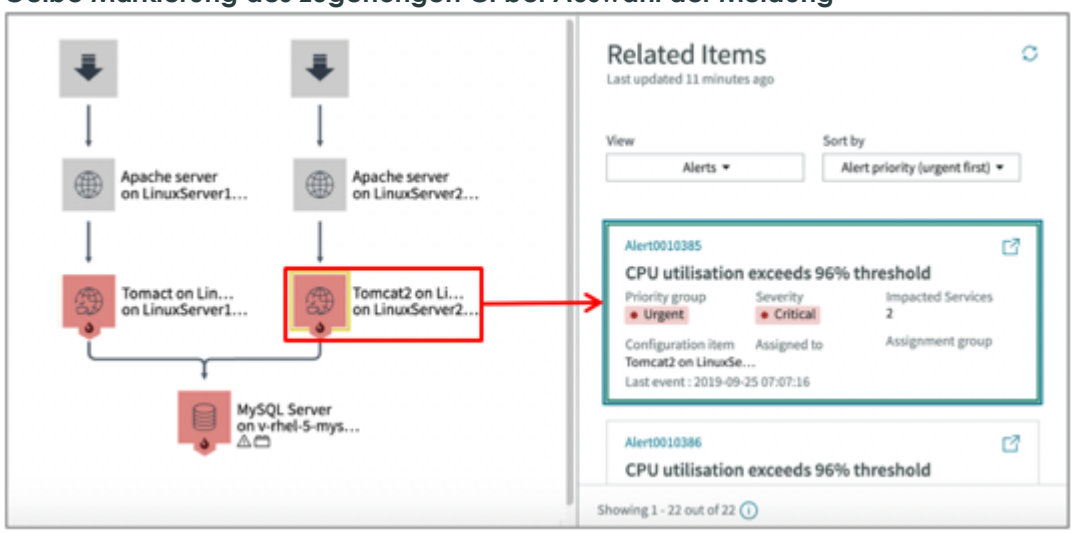
Wenn Informationen zum ausgewählten CI oder zur ausgewählten Verbindung vorhanden sind, werden diese im Bereich „Zugehörige Elemente“ rechts im Fenster hervorgehoben.

CIs zur Anzeige zugehöriger Informationen auswählen



Wenn Sie Informationen im Bereich „Zugehörige Elemente“ im Zuordnungsfenster rechts auswählen, wird das zugehörige CI in Gelb angezeigt.

Gelbe Markierung des zugehörigen CI bei Auswahl der Meldung



Sie können andere zugehörige Elemente wie geplante Änderungen oder Fälle anzeigen, die dem Anwendungsservice zugeordnet sind. Weitere Informationen finden Sie unter Ändern Sie die Ansicht für eine Anwendungsservice-Zuordnung in veraltet Mitarbeiterbereich.

Zugehörige Informationen

Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen

Zeigen Sie in Zuordnungen für Anwendungsservices an veraltet Mitarbeiterbereich

Verwenden Sie Zuordnungen, um Details von Anwendungsservices anzuzeigen. Zuordnungen zeigen Konfigurationselemente (CIs), aus denen Anwendungsservices bestehen, Verbindungen zwischen diesen CIs und andere servicebezogene Details.

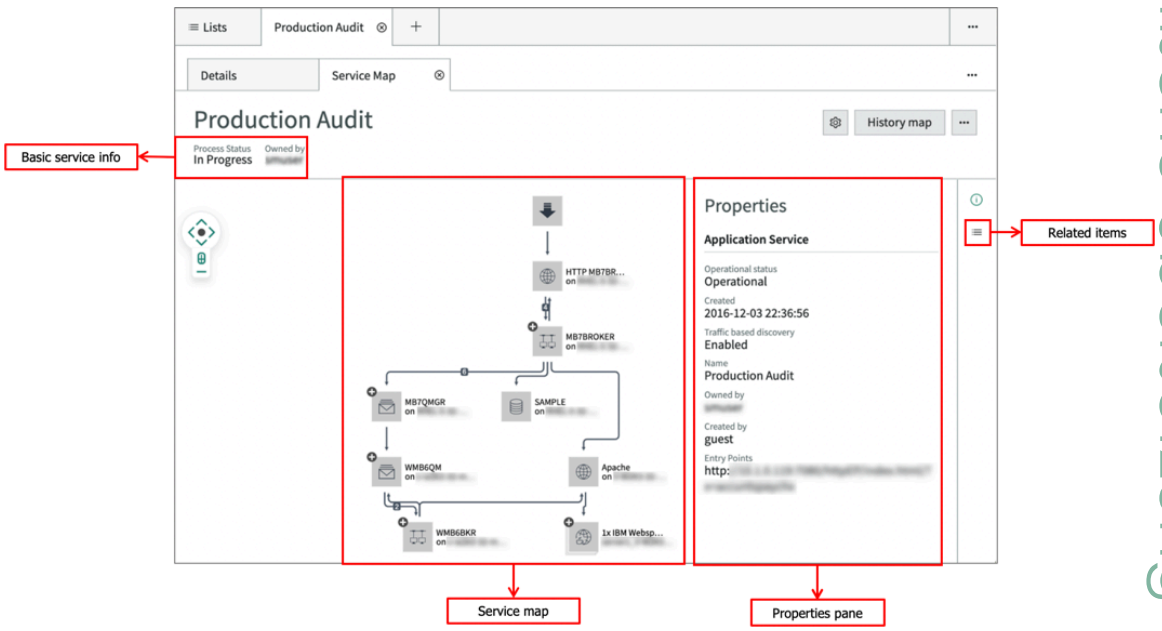
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sm_app_owner, service_mapping_user, evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird
Die Serviceinstanzzuordnung in der Ansicht Ereignismanagement spiegelt den Schweregradstatus der CIs wider, die zu der Serviceinstanz gehören. Weitere Informationen zum Anzeigen von Servicedetails in Zuordnungen finden Sie unter Anwendungsservicezuordnungen in veraltet Mitarbeiterbereich.

Prozedur
1. Klicken Sie in Mitarbeiterbereich im linken Bereich auf das Symbol **Listen**.
2. Navigieren zu **Alle** > **Services** > **Alle Services**.
   Die Liste der Services zeigt Services im Status „Betriebsbereit“ an.
3. Klicken Sie auf den Namen der entsprechenden Serviceinstanz.
   Die Registerkarte „Service“ wird geöffnet und zeigt Servicedetails auf der Registerkarte „Details“ an.
4. Klicken Sie auf **Servicezuordnung**.

   Die Registerkarte „Servicezuordnung“ wird geöffnet und zeigt die Zuordnungsübersicht dieses Anwendungsservice an.



5. Klicken Sie auf CIs oder deren Verbindungen, um die Details im Bereich „Serviceeigenschaften“ auf der rechten Seite anzuzeigen.
6. Zeigen Sie zusätzliche Informationen für ein CI oder den Anwendungsservice selbst an, indem Sie zugehörige Datensätze wie Warnungen, Ausfälle, Incidents und Probleme anzeigen.
   Weitere Informationen finden Sie unter Ändern Sie die Ansicht für eine Anwendungsservice-Zuordnung in veraltet Mitarbeiterbereich.
7. Um auf die Servicezuordnung in der Standard-UI von Ereignismanagement zuzugreifen, die den vollständigen Funktionsumfang für Zuordnungen bietet, klicken Sie auf **Vollständige Karte**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Service-Mapping

Change-Historie von Anwendungsservices in veraltet Mitarbeiterbereich anzeigen

Zeigen Sie Änderungen an, die an einer Serviceinstanz und den einzelnen Configuration Items (CIs) vorgenommen wurden, aus denen der Service in Mitarbeiterbereichbesteht. Sie können auch den Servicestatus vor und nach einem bestimmten Change oder Problem vergleichen. Die Change-Historie ist nützlich für Wartungs-, Planungs- oder Problembehebungsverfahren.

Vorbereitungen

Erforderliche Rolle: admin, service_mapping_admin, service_mapping_user, app_service_admin oder app_service_user

Warum und wann dieser Vorgang ausgeführt wird

Details zu Änderungen an einer Serviceinstanz und an ihren CIs werden in der CMDB gespeichert. In der Regel handelt es sich bei diesen Änderungen um das Hinzufügen oder Entfernen von CIs zu einer Serviceinstanz, das Aktualisieren oder Aktualisieren von CIs oder das Ändern von CI-Konfigurationsdateien. Das System stellt diese Daten zusammen, indem es CMDB-Tabellen abfragt und dann die Change-Historienansicht erstellt. In Bereitstellungen, für die Service-Mapping aktiviert ist, hängt die Art der Abfragen der Change-Informationen durch Service-Mapping von Discovery-Mustern ab, die von Service-Mapping für die Erkennung von CIs verwendet werden.

Änderungen an einem Anwendungsservice werden an der Verlaufszeitleiste angezeigt.

Darstellung der Änderungen am Anwendungsservice

Geben Sie zwei Zeitpunkte an, für die Sie die beiden Versionen eines Anwendungsservice vergleichen möchten. Mithilfe von Change-Markierungen auf der Zeitleiste können Sie Zeitpunkte angeben, die vor und nach der Änderung liegen, dessen Details Sie sehen möchten. Zum Beispiel können Sie, wenn Sie wissen, dass das Fehlschlagen eines Anwendungsservice zu einem bestimmten Zeitpunkt begonnen hat, zwei Versionen des Anwendungsservice (eine vor und eine nach Einsetzen des Problems) vergleichen. Dieser Vergleich zeigt Ihnen die Zusammenfassung der Changes, die möglicherweise zu den Problemen geführt haben.

Der Standardbereich der Zeitleiste ist die letzte Woche. Die Obergrenze für den Zeitbereich ist der Moment, in dem Sie die Zuordnung in der Ansicht „Change-Historie“ geöffnet haben. Wenn der Anwendungsservice vor weniger als einer Woche erstellt wurde, beginnt der Zeitbereich ab dem Zeitpunkt der Serviceerstellung.

Der Zeitbereich darf nicht mehr als 1000 Änderungen enthalten. Wenn sich innerhalb des ausgewählten Bereichs mehr Änderungen befinden, wird die Verlaufsskala automatisch so angepasst, dass 1000 Änderungen angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Den Validierungsstatus von Änderungen sowie Änderungen an zugehörigen Elementen, zum Beispiel nachverfolgte Konfigurationsdateien, können Sie in der klassischen UI von Service-Mapping anzeigen. Weitere Informationen finden Sie unter Change-Historie von Anwendungsservices in klassisch Service-Mapping anzeigen und Zwei Versionen eines Anwendungsservice in klassisch Service-Mapping vergleichen.

Prozedur

1. Klicken Sie in Mitarbeiterbereich im linken Bereich auf das Symbol **Listen**.
2. Navigieren zu **Alle** > **Services** > **Alle Services**.
   Die Liste der Services zeigt Services im Status „Betriebsbereit“ an.
3. Klicken Sie auf den Namen der entsprechenden Serviceinstanz.
   Die Registerkarte „Service“ wird geöffnet und zeigt Servicedetails auf der Registerkarte „Details“ an.
4. Klicken Sie auf **Servicezuordnung**.

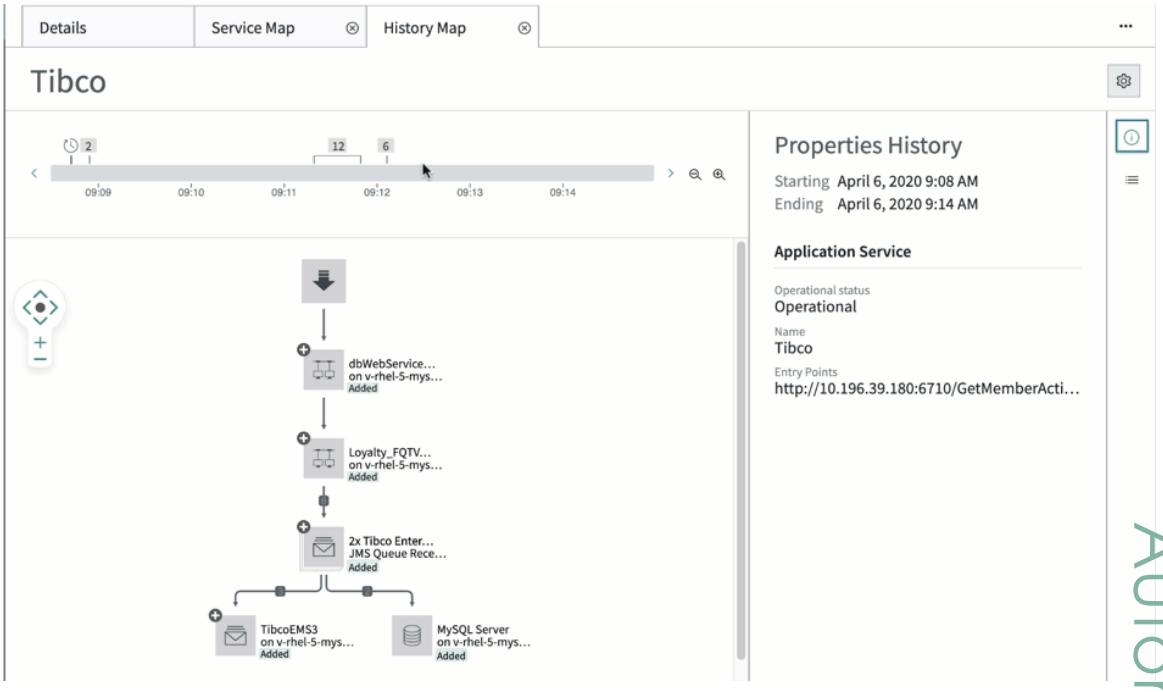
   Die Registerkarte „Servicezuordnung“ wird geöffnet und zeigt die Zuordnungsübersicht dieses Anwendungsservice an.
5. Klicken Sie auf **Change History Map (Change-Historienzuordnung)**.
   Die Registerkarte „Verlaufszuordnung“ zeigt die Zuordnung in der Verlaufsansicht an. Standardmäßig ist der Zeitraum eine Woche.
6. Um den Anwendungsservice vor und nach einer Änderung zu vergleichen, gehen Sie wie folgt vor:

   a. Ändern Sie den Zeitbereich auf der Zeitleiste, indem Sie neben der Zeitleiste auf die Schaltflächen **Vergrößern** oder **Verkleinern** klicken.
   Alternativ zeigen Sie auf die Zeitleiste und scrollen.

   Die Zuordnung zeigt Änderungen an CIs. CIs werden als hinzugefügt, aktualisiert oder gelöscht markiert.

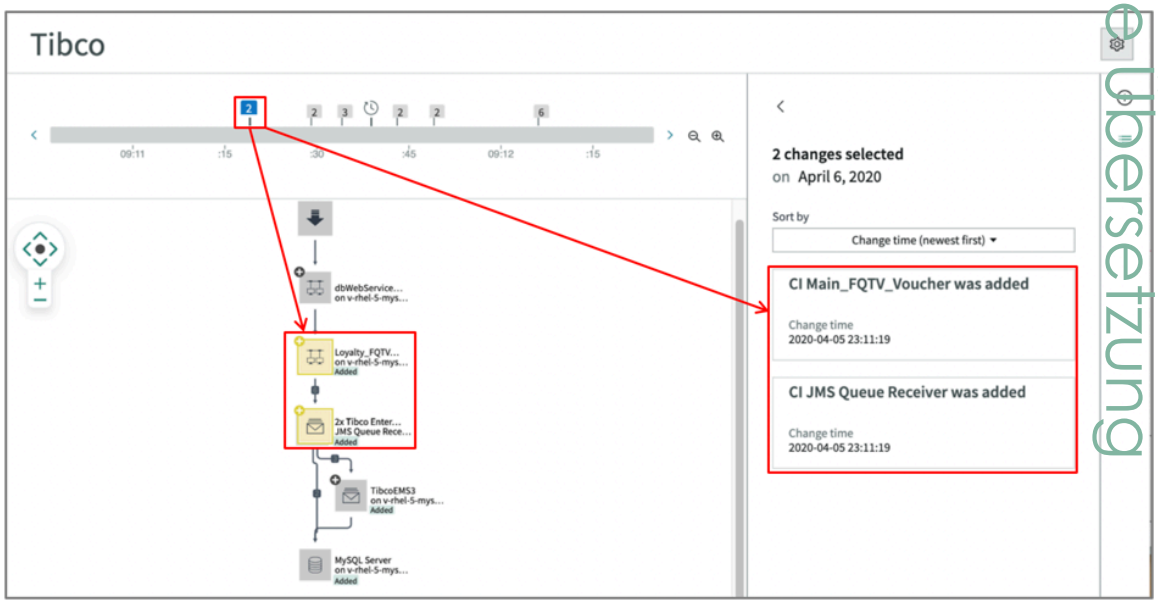
   Im Bereich **Eigenschaftenverlauf** wird eine Vergleichsübersicht der Änderungen an diesem Anwendungsservice angezeigt. Klicken Sie auf **Change-Historie** , um Change-Datensatzkarten für diesen Anwendungsservice anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



b. Mit einer der folgenden Methoden können Sie Änderungen in der Zuordnung fokussieren:

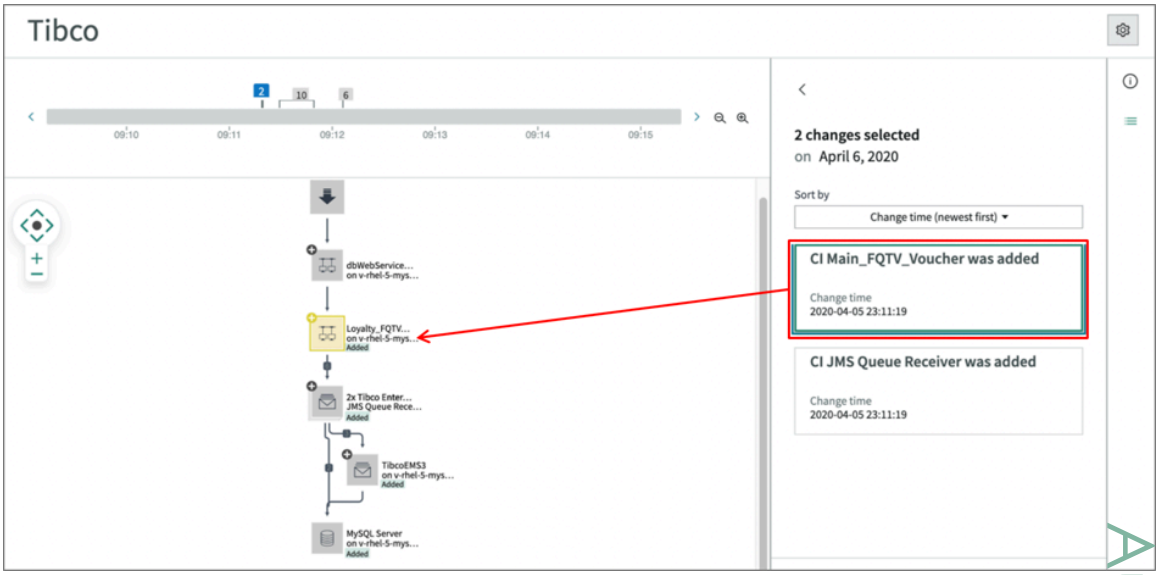
- Um das für den Change-Datensatz verantwortliche CI zu markieren und die Change-Datensatzkarte anzuzeigen, klicken Sie auf die Change-Markierung auf der Zeitleiste. Sie können mehrere CIs markieren, indem Sie auf die Markierung für mehrere Changes klicken.



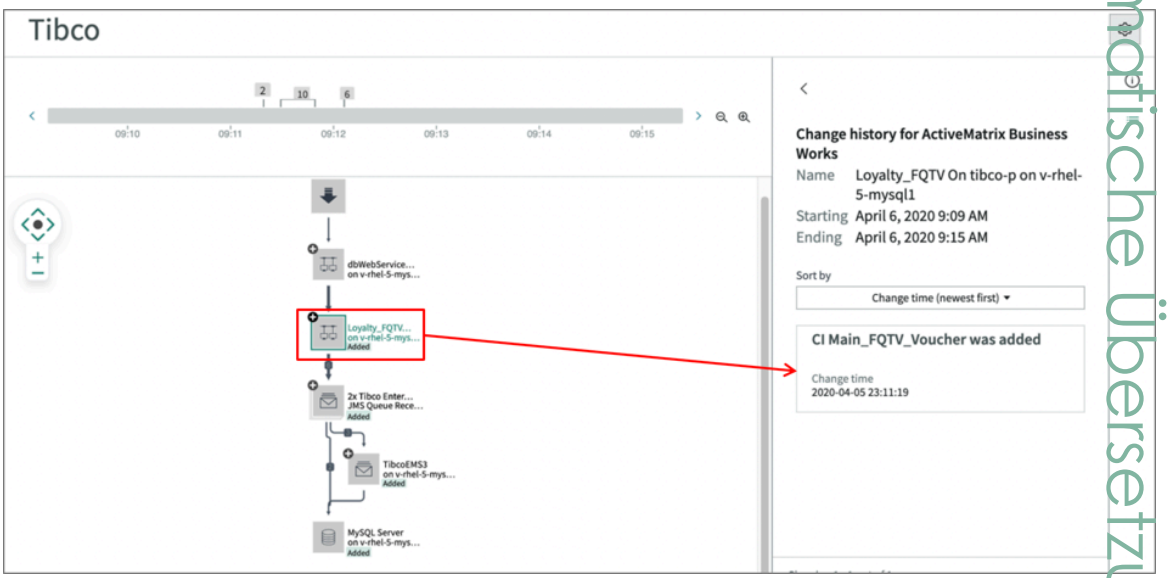
- Um das für den Change verantwortliche CI in der Zuordnung zu markieren, klicken Sie auf die Change-Datensatzkarte im Bereich „Change-Historie“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Klicken Sie zum Anzeigen der zugehörigen Change-Datensatzkarte im Bereich „Change-Historie“ auf das CI in der Zuordnung.



Ändern Sie die Ansicht für eine Anwendungsservice-Zuordnung in veraltet Mitarbeiterbereich

Passen Sie eine Zuordnungsansicht an, um relevante Informationen anzuzeigen und die Übersichtlichkeit zu erhöhen.

Vorbereitungen

Erforderliche Rolle: service_mapping_user, sm_app_owner, evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig sind Servicezuordnungen präzise und enthalten alle Details zu allen CIs, die Sie manuell hinzugefügt haben oder die von Service-Mapping zugeordnet wurden. Obwohl sie ein umfassendes Bild vermittelt, könnte die Verwendung einer solchen Zuordnung schwierig sein. Durch das Anpassen der Zuordnungen können Sie:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- die Navigation in der Zuordnung erleichtern
- irrelevante Informationen ausblenden
- wichtige Informationen anzeigen

Attribute, die Sie beim Anpassen von Zuordnungen anzeigen oder ausblenden, werden nicht dauerhaft entfernt und können nach Bedarf wieder angezeigt oder ausgeblendet werden. Das System speichert die Änderungen in der Zuordnungsansicht und zeigt die letzte Zuordnungsansicht an, wenn Sie eine Serviceinstanz erneut öffnen.

Die Serviceinstanzzuordnung in der Ansicht Ereignismanagement spiegelt den Schweregradstatus der CIs wider, die zu der Serviceinstanz gehören.

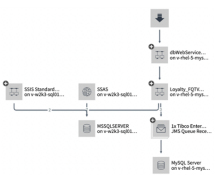
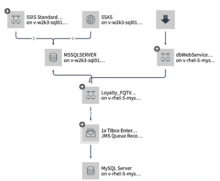
Prozedur

1. Klicken Sie in Mitarbeiterbereich im linken Bereich auf das Symbol **Listen**.
2. Navigieren zu **Services** > **Alle Services**.
   Die Liste der Services zeigt Services im Status „Betriebsbereit“ an.
3. Klicken Sie auf den Namen des betreffenden für Service.
   Die Registerkarte „Service“ wird geöffnet und zeigt Servicedetails auf der Registerkarte „Details“ an.
4. Klicken Sie auf **Servicezuordnung**.
5. Klicken Sie auf die Schaltfläche **Kartenanzeigeeinstellungen öffnen**.

6. Wählen Sie die relevante Option aus:

Option	Wenn aktiviert	Wenn deaktiviert
In Host-Ansicht anzeigen Die Host-Ansicht vereinfacht auch die Zuordnung, insbesondere wenn viele Anwendungen auf wenigen Hosts ausgeführt werden. Die Host-Ansicht ist nur für Serviceinstanzen nützlich, die mit Service-Mappingerkannt wurden. Diese Ansicht enthält keine zusätzlichen Informationen für manuell erstellte Serviceinstanzen.	Von der Servicezuordnung werden Host-CIs dargestellt.	In der Servicezuordnung werden Anwendungs-CIs dargestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
CIs in Zuordnung gruppieren Vereinfachen Sie Zuordnungen, indem Sie CIs gruppieren, die zu demselben Typ gehören und auf Servern gehostet werden, die sich Präfix und Domänennamen teilen. Die Zuordnung gibt den Anwendungs-Flow weiterhin korrekt wieder, da gruppierte CIs zur selben Ebene gehören. Diese Option ist für Serviceinstanzen relevant, die aus mehr als 10 CIs bestehen.	In der Serviceinstanzzuordnung werden Gruppen von CIs angezeigt. Die Zuordnung ist kompakter.	In der Serviceinstanzzuordnung werden alle CIs separat angezeigt. Die Zuordnung ist größer.
Topology Cycles entfernen Blenden Sie Verbindungen aus, die zu demselben Configuration Item (CI) zurückkehren, von dem sie stammen, um die Übersichtlichkeit der Zuordnung zu verbessern. Normalerweise sind diese zurückkehrenden Verbindungen für die Analyse oder Fehlerbehebung von Serviceinstanzen irrelevant.	In der Serviceinstanzzuordnung werden Topologiezyklen ausgeblendet.	In der Zuordnung der Serviceinstanz werden Topologiezyklen angezeigt.
Strukturansicht wird segmentiert Vereinfachen Sie die Zuordnung, indem Sie CIs in einer Baumstruktur anordnen und manche der Verbindungslinien verbergen. Diese Option ist besonders für sehr große Karten nützlich.	In der Zuordnung wird eine Serviceinstanz als Struktur angezeigt. 	Die Zuordnung spiegelt die tatsächliche Struktur einer Serviceinstanz wider. 
Datenverkehrsbasierte CIs anzeigen Diese Option ist nur für Anwender mit	In der Zuordnung der Serviceinstanz werden CIs und Hosts angezeigt, die Service-Mapping mithilfe	In der Zuordnung der Serviceinstanz werden nur CIs und Hosts angezeigt,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Wenn aktiviert	Wenn deaktiviert
den folgenden Rollen verfügbar: Service-Mapping-Administrator [service_mapping_admin] und Service-Mapping-Anwender [service_mapping_user]. Zeigen Sie mithilfe von datenverkehrsbasierter Zuordnung gefundene Configuration Items (CIs) an.	von Mustern und Traffic-basierter Discovery erkannt hat. Das Erkennen des eingehenden und ausgehenden Datenverkehrs von CIs führt zwar zu einer inklusiven Zuordnung, kann aber auch zur Zuordnung vieler redundanter CIs führen, die den Betrieb der Serviceinstanz nicht beeinflussen.	die anhand von Mustern erkannt wurden.
Zuordnungsindikatoren Zeigen Sie zusätzliche Informationen für ein CI oder die Serviceinstanz selbst an, indem Sie zugehörige Datensätze wie Warnungen, Ausfälle, Incidents und Probleme anzeigen. Das Basissystem stellt Zuordnungsindikatoren für die folgenden Datensatztypen bereit: ◦ Betroffene CIs ◦ Änderungen: Aktuell, in der Vergangenheit oder geplant ◦ Ausfälle: Aktuell, in der Vergangenheit oder geplant ◦ Problem Weitere Informationen erhalten Sie im Video Event Management Map Indicators (Zuordnungsindikatoren in Event Management) .	Für jeden Datensatztyp, der für die Anzeige festgelegt ist, werden der entsprechende Indikator und die Registerkarte angezeigt. Beispielsweise wird die Registerkarte **Incidents** unter der Zuordnung angezeigt. Der Indikator **Incidents** wird neben CIs angezeigt, denen Incidents zugeordnet sind.	In der Zuordnung der Serviceinstanz werden CIs ohne zugehörige Indikatoren angezeigt.
	Wenn dem Anwendungsservice selbst ein Datensatz zugeordnet ist, wird der Indikator neben dem Namen des Anwendungsservice angezeigt.	Neben dem Anwendungsservicenamen sind keine Zuordnungsindikatoren zu sehen.

Service-Mapping-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Zuordnen und Optimieren von Anwendungsservices mithilfe von Service-Mapping-Listen und -Formularen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping Arbeitsbereich

Greifen Sie auf die Statistiken Service-Mapping an einem zentralen Ort zu. Verwenden Sie die im Dashboard angezeigten Informationen, um neue Services zu erstellen oder vorhandene Ressourcen und Services zu analysieren, zu überwachen und zu aktualisieren.

Auf Service-Mapping-Homepage zugreifen

Navigieren zu **Arbeitsbereiche** > **Service-Mapping**.

Anwendungsfälle

Beispiele dafür, wie Ihre Organisation dieses Dashboard verwenden kann, finden Sie in den folgenden Anwendungsfällen.

Anwender	Dashboard-Verwendung
service_mapping_admin	• Greifen Sie auf das Bereitschafts-Dashboard zu, um die Bereitschaft für maschinelles Lernen (ML) sicherzustellen, bevor Sie Anwendungsservices zuordnen. • Zeigen Sie Detailinformationen zu Servicezuordnungen in verschiedenen Kategorien an. • Greifen Sie auf Empfehlungen für automatisierte Services zu, um Anwendungsservice-Kandidaten zu bewerten, neue Anwendungsservices zu erstellen oder einen vorhandenen Service zu ergänzen. • Verwenden Sie nicht zugeordnete Server, die mit einem Anwendungsservice-Candidate verknüpft sind, um neue Anwendungsservices zu erstellen.

Indikatoren

Zugeordnete Anwendungsservices

Anzahl der zuvor zugeordneten Anwendungsservices Wählen Sie diese Option aus, um bestimmte Informationen zu diesen Services anzuzeigen, z. B. Betriebsstatus und Geschäftsrelevanz.

ML-gestützte Kandidaten

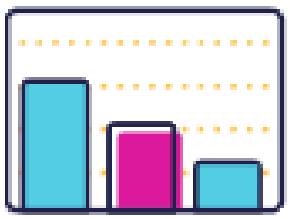
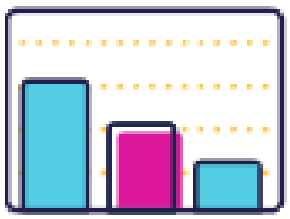
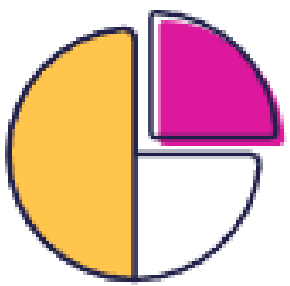
Die Anzahl der Anwendungsservice-Candidates, die durch maschinelles Lernen identifiziert wurden. Wählen Sie diese Option, um auf die Funktion Empfehlungen für automatisierte Services zuzugreifen.

Zugeordnete Server

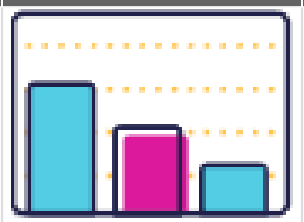
Die Anzahl der Server, die derzeit mit einem Anwendungsservice verbunden sind. Wählen Sie diese Option, um Informationen wie den Betriebsstatus und den Besitzer anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berichte

Titel	Typ	Quelltabelle	Beschreibung
Nicht zugeordnete Server	Balkenbericht 		Ein Balkenbericht, der nicht zugeordnete Server darstellt, die mit einem Anwendungsservice-Candidate abgeglichen wurden, sowie Server ohne Candidate. Wählen Sie **Nicht zugeordnete Server mit Candidate** aus, um Server anzuzeigen, die Sie zum Erstellen eines neuen Anwendungsservice verwenden können. Weitere Informationen finden Sie unter Erstellen Sie einen Anwendungsservice für nicht zugeordnete Server.
Servicezuordnungen nach Betriebsart	Balkenbericht 	cmdb_ci_service_discovered	Ein Balkenbericht, in dem die zugeordneten Anwendungsservices nach Vorgangstyp gruppiert dargestellt werden.
Servicezuordnungen nach Erstellungsmethode	Kreisbericht 	cmdb_ci_service_discovered	Ein Kreisbericht, in dem die zugeordneten Anwendungsservices nach Erstellungsmethode gruppiert dargestellt werden.
Servicezuordnungen nach Relevanz	Balkenbericht	cmdb_ci_service_discovered	Ein Balkenbericht, in dem die zugeordneten Anwendungsservices

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			nach der Relevanzstufe gruppiert dargestellt werden.

Zusätzliche Komponenten

Mit Daten befüllen

Wählen Sie aus, um die Daten zu aktualisieren und die auf dieser Seite angezeigten Informationen zu aktualisieren.

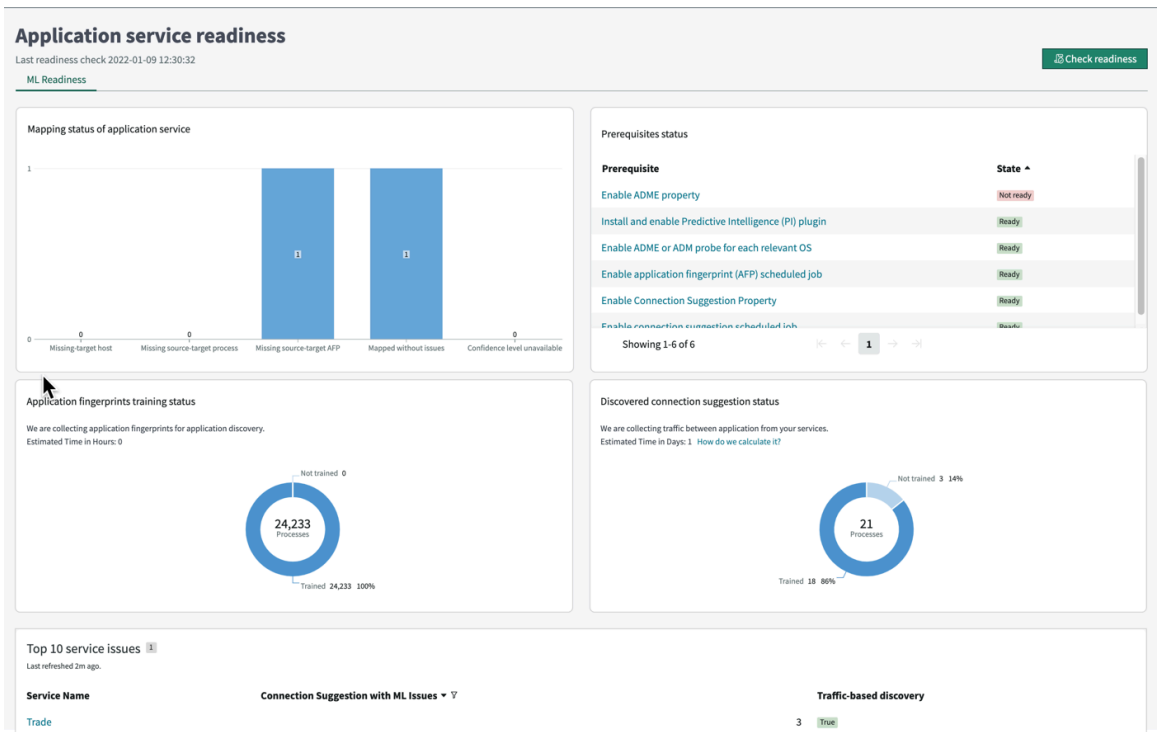
Suchen Sie nach dem Server

Um einen bestimmten Server zu finden, beginnen Sie mit der Eingabe in dieses Feld, und wählen Sie **Suchen**aus. Wählen Sie den Namen des Servers aus, um detailliertere Informationen zu erhalten.

Bereitschafts-Dashboard des Anwendungsservice

Wählen Sie das Symbol für das Dashboard „Bereitschaft des Anwendungsservice“ aus.

Verwenden Sie diese Option, um sicherzustellen, dass Predictive Intelligenceaktiviert ist, um die Bereitschaft für maschinelles Lernen zu überprüfen und um zu bestätigen, dass Ihre Daten trainiert wurden.



Weitere Informationen zur Anwendungsbereitschaft finden Sie unter Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

- Empfehlungen für automatisierte Services
- Anwendungsservices zuordnen basierend auf Empfehlungen für automatisierte Services
- Namensvorschläge für Anwendungsservice-Candidates

Namensvorschläge für Anwendungsservice-Candidates

Empfehlungen für automatisierte Services bietet aussagekräftige Namensvorschläge für die Serviceidentifizierung, auf die Sie auf der Registerkarte **Anwendungsservicevorschläge** im Arbeitsbereich Service-Mapping zugreifen können.

Namensvorschläge für Candidate für Anwendungsservice

Namensvorschlag	Beschreibung
Namensvorschlag für Candidate	Der Namensvorschlag für den primären Kandidaten priorisiert den Namen Service-Fingerabdrücke und stellt ihn dann bei Bedarf anderen Namensvorschlägen zurück.
Servicefingerabdruck	Namensvorschläge aus maximal drei Service-Fingerabdrücke, die sich auf den Kandidaten beziehen.
Lastenausgleichsmodul	Namensvorschläge aus den Namen der drei wichtigsten Lastenausgleichsmodul-Services, die dem Kandidaten zugeordnet sind.
Prozess	Namensvorschläge aus den Befehlszeilen des Prozesseinstiegspunkts für den Kandidaten. Ein Algorithmus identifiziert die relevantesten Wörter und macht die drei besten Namensvorschläge.
Eingabepunkt	Namensvorschläge, die von allen dem Kandidaten zugeordneten Einstiegspunkt-IP-Adressen übernommen wurden. Vorschläge für Einstiegspunktnamen sind ab Version 1.12.3 veraltet. Diese Spalte wird weiterhin angezeigt, ist jedoch nicht mehr mit Daten gefüllt. Es wird schließlich entfernt.
AFP (Fingerabdruck der Anwendung)	Namensvorschläge aus den drei häufigsten Fingerabdrücken der Anwendung, die dem Kandidaten zugeordnet sind.

Zugehörige Informationen

- Empfehlungen für automatisierte Services
- Anwendungsservices zuordnen basierend auf Empfehlungen für automatisierte Services

Dashboard für die Anwendungsservice-Bereitschaft in konfigurierbarer Arbeitsbereich

Überprüfen Sie die Informationen im Dashboard, um sicherzustellen, dass Sie bereit sind, Anwendungsservices basierend auf maschinellem Lernen (ML) zu erkennen und zuzuordnen. Service-Mapping verwendet von Predictive Intelligence verarbeitete Daten, um Vorschläge für datenverkehrsbasierte Verbindungen zu generieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Dashboard „Bereitschaft des Anwendungsservice“ ist Teil von Service-Mapping Plusund verfügbar unter ServiceNow Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Predictive Intelligence wertet Verbindungen zwischen Anwendungsfingerabdrücken, CIs und Prozessen aus und bewertet ihre Relevanz. Service-Mapping verwendet diese Informationen, um Verbindungen basierend auf Verbindungsregeln zu erstellen. Außerdem werden Verbindungsvorschläge für Server und Lastenausgleichsmodule generiert, damit Sie entscheiden können, welche Verbindungen den Serviceinstanzen hinzugefügt oder daraus entfernt werden sollen.

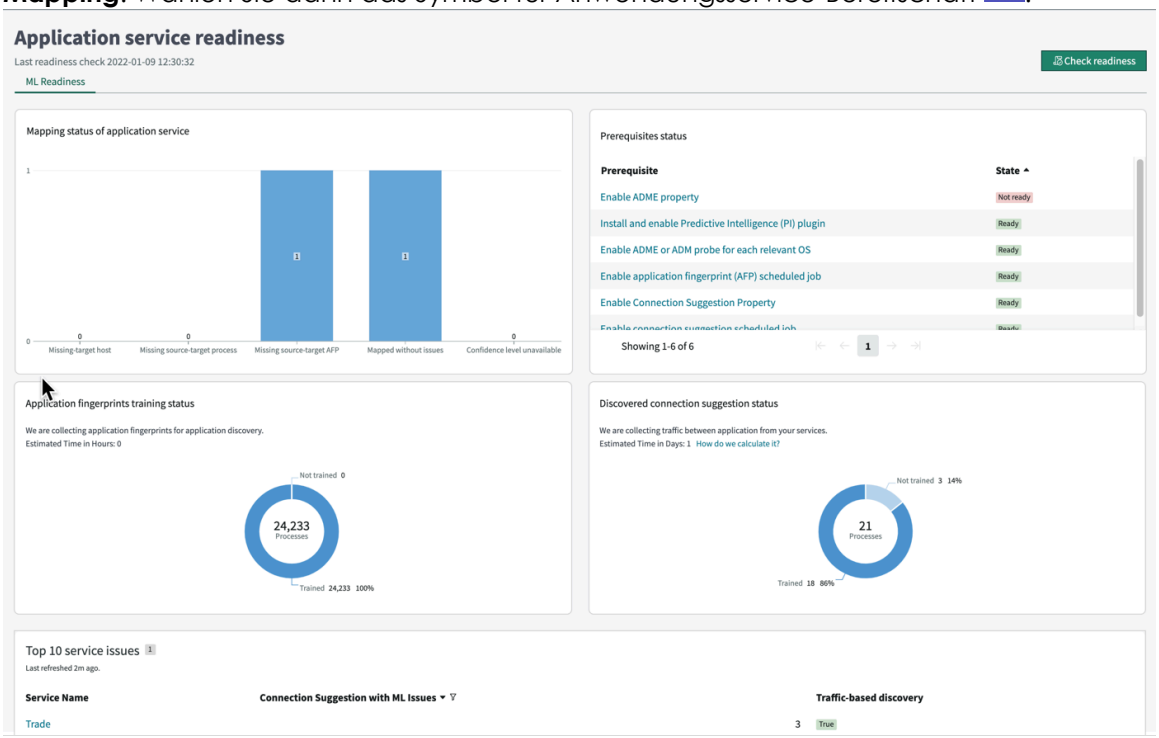
Widgets auf der ML-Dashboard-Seite zeigen die Informationen zu Voraussetzungen und Problemen im Zusammenhang mit der Service-Discovery basierend auf Predictive Intelligence an. Wählen Sie Links in den Widgets und Berichten aus, um zur zugehörigen Liste oder zum zugehörigen Formular zu navigieren.

Erforderliche Now Platform-Rollen

service_mapping_admin

Auf das Dashboard für Anwendungsservice-Bereitschaft zugreifen

Um das Dashboard zu öffnen, wechseln Sie zu: **Arbeitsbereiche** > **Service-Mapping**. Wählen Sie dann das Symbol für Anwendungsservice-Bereitschaft .



Berichte

Das Dashboard enthält die folgenden Berichte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
Mapping status of application service (Zuordnungsstatus des Anwendungsservice)	Ein Balkenbericht	ML-Related Service Status [ml_related_service_status] (ML-bezogener Servicestatus)	Ein Balkenbericht, der die Zusammenfassung von ML-bezogenen Problemen in zugeordneten Anwendungsservices enthält. Ausführliche Informationen finden Sie unter Zuordnungsstatus der Anwendungsservices.
Application fingerprints training status (Trainingsstatus von Anwendungsfingerabdrücken)	Ein Ring-Bericht	AFP-Trainingsstatus [afp_training_status]	Ein Ringbericht, der den Trainingsstatus von Anwendungsfingerabdrücken zeigt. Predictive Intelligence trainiert Vorhersagemodelle und ML-Lösungen (maschinelles Lernen). Zeigen Sie mit Predictive Intelligence den Trainingsstatus für Anwendungs-Fingerabdrücke an, um zu verstehen, ob Ihre Bereitstellung für die Zuordnung bereit ist.
Discovered connection suggestion status (Status erkannter Verbindungsvorschläge)	Ein Ring-Bericht	Connection Suggestions Training Status [connection_suggestion_training_status] (Verbindungsvorschläge-Trainingsstatus)	Ein Ringbericht, der den Status von Verbindungsvorschlägen anzeigt. Details finden Sie unter Status der erkannten Verbindungsvorschläge.

Zuordnungsstatus der Anwendungsservices

Überprüfen Sie die Zusammenfassung der ML-bezogenen Probleme in zugeordneten Anwendungsservices.

Kategorie	Beschreibung
Ohne Probleme zugeordnet	Die Anzahl der erkannten Serviceinstanzen ohne ML-bezogene Probleme.
Quell-Ziel-AFP fehlt	Die Anzahl der Serviceinstanzen, für die einige Anwendungsfingerabdrücke für einen Quell- oder Zielprozess fehlen. Um diese

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorie	Beschreibung
	Probleme zu beheben, kalibrieren Sie die auf Fingerabdrücken basierte Discovery.
Quell-Ziel-Prozess fehlt	Die Anzahl der Serviceinstanzen, für die einige Quell-/Zielprozessinformationen fehlen. Um diese Probleme zu beheben, lassen Sie die Zielhosts erneut erkennen und stellen Sie sicher, dass die relevanten Prozesse erkannt werden.
Konfidenzniveau nicht verfügbar	Das Konfidenzniveau gibt die Wahrscheinlichkeit an, dass diese Verbindung Teil der Serviceinstanzen ist. Wenn das Konfidenzniveau als **N/V** angezeigt wird, warten Sie, bis das Training der Anwendungsfingerabdrücke abgeschlossen ist.
Zielhost fehlt	Die Anzahl der Serviceinstanzen, für die einige CI-Verbindungen nicht vollständig erkannt wurden, da die Horizontal-Discovery keine Host-CIs erkannt hat. Um diese Probleme zu beheben, lassen Sie die Zielhosts erneut erkennen und stellen Sie sicher, dass die relevanten Prozesse erkannt werden.

Status der Voraussetzungen

erfordert die Integration mehrerer Module und Anwendungen: Anmeldeinformationen, Predictive Intelligence, erweiterte Erkennung von Application Dependency Mapping (ADME) und geplante Aufgaben. Überprüfen Sie die Liste der Voraussetzungen und stellen Sie sicher, dass der Status aller Voraussetzungen **Bereit** lautet.

Voraussetzung	Beschreibung
Installieren und aktivieren Sie das Plugin „Predictive Intelligence (PI)“.	Service-Mapping verwendet Predictive Intelligence, um Verbindungsvorschläge zu generieren. **1.** Stellen Sie sicher, dass das Plugin „Predictive Intelligence“ als **Installiert** angezeigt wird. **2.** Klicken Sie auf die Kachel Predictive Intelligence und überprüfen Sie, ob der **Status** als **Aktiv** angezeigt wird. Wenn der Status **Inaktiv** ist, wählen Sie unter **Zugehörige Links** den Link **Aktivieren/ Reparieren** aus.
Aktivieren Sie die Eigenschaft ADME.	Service-Mapping verwendet ADME-Proben. Stellen Sie sicher, dass die Eigenschaft *glide.discovery.enable_adme* auf **true** festgelegt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzung	Beschreibung
Aktivieren Sie alle relevanten ADME-Datensammler-Proben.	Es gibt mehrere ADME-Proben für verschiedene Arten von Betriebssystemen. Aktivieren Sie alle erforderlichen Proben, um Konfigurationselemente (CIs) in Ihrer Umgebung zu erkennen.
Stellen Sie die Mindestanzahl der laufenden Prozesse sicher.	Prüfen Sie, ob die Clustering-Lösung genügend Prozessgruppen erstellt hat, die zu Vorschlägen werden. Wenn weniger Prozesse als erforderlich vorhanden sind, kalibrieren Sie die auf Fingerabdrücken basierte Discovery.
Aktivieren Sie die regelmäßige AFP-Aufgabe (Application Fingerprint).	Stellen Sie sicher, dass die geplante Aufgabe *Applications suggestion - ITOM Autodisco* für die auf Fingerabdrücken basierte Discovery auf **Aktiv** festgelegt ist.
Aktivieren Sie die Eigenschaft „Verbindungsvorschlag“.	Stellen Sie sicher, dass die Discovery basierend auf Predictive Intelligence aktiviert ist. Navigieren Sie zur Tabelle „Systemeigenschaft“ [sys_properties], und überprüfen Sie, ob die Eigenschaft *sa_ml.connection_suggestions.active* auf **True** gesetzt ist.
Aktivieren Sie die regelmäßige Aufgabe für Verbindungsvorschläge.	Stellen Sie sicher, dass der **Status** der regelmäßigen Aufgabe *Service Mapping - Traffic Process to Process* **Aktiv** ist. Diese regelmäßige Aufgabe löst die Generierung von Verbindungsvorschlägen aus.

Status der erkannten Verbindungsvorschläge

Predictive Intelligence wertet Verbindungen zwischen Anwendungsfingerabdrücken, CIs und Prozessen aus und bewertet ihre Relevanz. Service-Mapping verwendet diese Informationen, um Verbindungen basierend auf Verbindungsregeln zu erstellen. Außerdem werden Verbindungsvorschläge für Server und Lastenausgleichsmodule generiert, damit Sie entscheiden können, welche Verbindungen den Serviceinstanzen hinzugefügt oder daraus entfernt werden sollen.

Das Konfidenzniveau gibt die Wahrscheinlichkeit an, dass diese Verbindung Teil der Serviceinstanzen ist.

- **Hoch** – Es handelt sich wahrscheinlich um eine Verbindung zu einer internen Komponente, die nur von dieser Komponente oder Anwendung verwendet wird.
- **Mittel** – Es handelt sich wahrscheinlich um eine Verbindung zu einer Middleware-Komponente, die von mehreren Services verwendet wird, z. B. IBM MQ oder Oracle WebLogic Server.
- **Niedrig** – Es handelt sich wahrscheinlich um eine Verbindung zu einer Anwendung, die auf zahlreichen Servern im Unternehmen bereitgestellt wird, normalerweise zu Überwachungszwecken. Zum Beispiel Tivoli Enterprise Monitoring Agents oder MID-Server.
- **Sehr niedrig** – Es handelt sich wahrscheinlich um eine Verbindung zu einer zentralen Anwendung, die von der gesamten Organisation verwendet wird, z. B. Microsoft Active Directory oder Okta.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Verbindungsvorschläge ohne das Konfidenzniveau für die Zuordnung von Serviceinstanzen verwenden.

Serviceprobleme

Überprüfen Sie die Liste der Serviceinstanzen, die am häufigsten von ML-bezogenen Problemen betroffen sind. Die Liste der am stärksten betroffenen Services ist verfügbar, wenn die Funktion für Verbindungsvorschläge in Ihrer Bereitstellung aktiviert ist. Die Liste zeigt Servicenamen und die Anzahl der ML-bezogenen Probleme für jeden von ihnen. Sie gibt auch an, ob die datenverkehrsbasierte Funktion für die Services aktiviert ist.

Zugehörige Informationen

- Weitere Informationen zu ADME-Probes
- Erkennung mithilfe von ADME-Probes aktivieren und konfigurieren
- Auf Fingerabdrücken basierte Erkennung kalibrieren
- Sicherstellen, dass die auf Fingerabdrücken basierte Erkennung Vorschläge generiert
- Troubleshooting guide for Service Mapping ML Connection Suggestions (Fehlerbehebungsleitfaden für ML-Verbindungsvorschläge von Service Mapping) [KB0963421]

Mit Service-Mapping Plus installierte Komponenten

Bei der Aktivierung des Service-Mapping Plus-Plugins werden mehrere Arten von Komponenten installiert, z. B. Tabellen und regelmäßige Aufgaben.

Hinweis: Die Anwendung Service-Mapping Plus ist im verfügbar ServiceNow Store .

Installierte geplante Aufgaben

Regelmäßige Aufgabe	Beschreibung
Update statistics for application service readiness dashboard (Statistiken für das Dashboard der Anwendungsservice-Bereitschaft aktualisieren)	Aktualisiert die im Dashboard „Application Service Readiness“ (Bereitschaft von Anwendungsservices) angezeigten Informationen. Wird stündlich ausgeführt. Wird darüber hinaus ausgeführt, wenn die Schaltfläche **Check readiness** (Bereitschaft prüfen) im **Dashboard „Application Service Readiness“** (Bereitschaft von Anwendungsservices) ausgewählt wird. Das System löst diesen regelmäßigen Auftrag nicht früher als fünf Minuten nach der letzten Ausführung aus.

Installierte Tabellen

Tabelle	Beschreibung
ML-Related Service Status [ml_related_service_status] (ML-bezogener Servicestatus)	Enthält die Informationen zu ML-bezogenen Problemen in zugeordneten Anwendungsservices.
Top ML Error Services [top_ml_err_services_list] (Services mit meisten ML-Fehlern)	Enthält die Liste von bis zu 10 Anwendungsservices mit der größten Anzahl von ML-bezogenen Problemen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
ML Dashboard Prerequisites [ml_dashboard_prerequisites] (ML-Dashboard-Voraussetzungen)	Enthält die Links zu Formularen und Tabellen, die die Einrichtung der Zuordnung basierend auf ML erfordern, sowie die Statusinformationen für diese Konfigurationen.
AFP-Trainingsstatus [afp_training_status]	Enthält den Status des Trainings der Anwendungsfingerabdrücke.
Connection Suggestions Training Status [connection_suggestion_training_status] (Verbindungsvorschläge-Trainingsstatus)	Enthält den Status der Verbindungsvorschläge.
ML P2P ETA – Berechnungskonstanten [sa_ml_p2p_eta_values_list]	Speichert die Informationen darüber, wie das System die verbleibende Zeit für das Training von Verbindungsvorschlägen berechnet.

Installierte Eigenschaften

Eigenschaft	Beschreibung
sa.asc.logger_level	Fügt dem Systemprotokoll für den Anwendungsservice-Candidate Nachrichten hinzu. • **Typ:** Zeichenfolge • **Standardwert:** Fehler • **Andere mögliche Werte:** debug **Hinweis:** Wenn Sie die Eigenschaft auf „debuggen“ festlegen, werden sowohl Debug- als auch Fehlermeldungen angezeigt.
sa.topdown.enable_cmdb_based_mapping	Diese Eigenschaft ermöglicht die CMDB-basierte Zuordnung mit CMDB anstelle von MID-Server. • **Typ:** boolean • **Standardwert:** false • **Andere mögliche Werte:** true
sn_sm_scoped_app_app.sa.unified_map.enabled	Aktiviert den Zugriff auf Einheitliche Übersicht über den Arbeitsbereich Service-Mapping. • **Typ:** boolean • **Standardwert:** false • **Andere mögliche Werte:** true
sn_cmdb_ws_config_property.unifiedmap.map_service_node_limit	Um eine hohe Leistung sicherzustellen, begrenzt diese Eigenschaft die Anzahl der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Knoten, die in einer Zuordnung angezeigt werden können. • **Typ:** Ganzzahl • **Standardwert:** 250 Höhere Werte können die Leistung beeinträchtigen, da Einheitliche Übersicht beim Öffnen alle Elemente und zugehörigen Details lädt. **Hinweis:** Die Eigenschaft *unifiedmap.map_search.max_nodes* in der arbeitsbereichspezifischen Tabelle [sn_cmdb_ws_config_property] ersetzt die veraltete Eigenschaft *sn_cmdb_ws.node.map.max.edge.count*.

Mit Service-Mapping installierte Komponenten

Bei Aktivierung des Service-Mapping-Plugins werden mehrere Arten von Komponenten installiert, zum Beispiel Tabellen, Benutzerrollen und regelmäßige Aufgaben.

Für diese Funktion sind Demodaten verfügbar.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
[app_service_admin]	Erstellt und ändert Serviceinstanzen, erstellt Servicegruppen, zeigt Serviceinstanzzuordnungen an und bearbeitet sie.	[itil]
[app_service_user]	Zeigt Zuordnungen für funktionsfähige Serviceinstanzen an und ruft Serviceinhalte mithilfe der getContent - GET REST API ab. Die ITIL-Rolle, die als die grundlegende Help Desk-Technikerrolle dient, enthält die Rolle „app_service_user“.	[cmdb_read]
[itom_admin]	Konfigurieren Sie IT Operations Management-Anwendungen mit dem geführten Setup für ITOM.	[sn_bm_client.benchmark_data_viewer] [sm_itom_license.reader]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Hinweis: Das ITOM Guided Setup umfasst nicht Service-Mapping.	
[sam_core_admin]	Eine interne Rolle	[sam_core_user]
[sam_core_user]	Eine interne Rolle	[itil]
[service_mapping_admin]	Richtet die Service-Mapping-Anwendung ein. Ermöglicht die Zuordnung, Korrektur und Wartung von Serviceinstanzen. Führt auch eine erweiterte Konfiguration und Anpassung des Produkts durch. Weisen Sie diese Rolle Anwendungsadministratoren zu.	• [app_service_admin] • [app_service_owner] • [discovery_admin] • [itil_admin] • [itom_admin] • [sam_core_admin] • [personalize_dictionary] • [pd_admin] • [pd_user] • [service_mapping_user]
[sm_app_owner]	Stellt Informationen bereit, die für die erfolgreiche Zuordnung einer Serviceinstanz erforderlich sind. Wenn ein Dienst zugeordnet ist, überprüft dieser Benutzer die Ergebnisse und genehmigt sie entweder oder schlägt Änderungen vor. Weisen Sie die Rolle sm_app_owner Benutzern zu, die Besitzer von Serviceinstanzen sind und mit der Infrastruktur und den Anwendungen vertraut sind, aus denen die Services bestehen.	[service_mapping_user]
[sm_itom_license.reader]	Zeigen Sie Abonnementinformationen und Statistiken für IT Operations Management-Anwendungen an.	[cmdb_read]
[service_mapping_user]	Zeigt Zuordnungen für funktionsfähige Serviceinstanzen an, um Change oder Migration zu planen und die Kontinuität und Verfügbarkeit von	• [sam_core_user.service_mapping_user] • [itil.service_mapping_user]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Services zu analysieren. Weisen Sie diese Rolle Anwendungsbenutzern zu.	
[sn_svc_err.admin]	Behebt Erkennungsfehler als Massenvorgang mithilfe der Fehler-Framework-Funktion in Service-Mapping und Discovery.	[itil]
[pd_admin]	Erzeugt neue und modifiziert vorhandene Muster, die Service-Mapping und Discovery für die Horizontal- und die Top Down-Discovery verwenden.	[pd_user]

Hinweis: Benutzer mit der Rolle „itil“ können alle Serviceinstanzen anzeigen.

Regelmäßige Aufgaben installiert

Regelmäßige Aufgabe	Beschreibung
Aufgeschobene Discovery-Bereinigung [sysauto_script_ba4bee737f0022008f1c3b19be0e908]	Wird jede Minute ausgeführt. Erkennt und löscht Erkennungszeitpläne für TCP-Verbindungen, die sich nicht mehr im aktiven Status befinden (5 Minuten ohne Aktivität).
Abfragebasierte Services aktualisieren [sysauto_script_08745913f31131002e6bae47166a10ff]	Wird alle 10 Minuten ausgeführt. Aktualisiert Abfragen für alle definierten technischen Services.
Anwendungsservicestatus aktualisieren [sysauto_script_5641702ac32102003e76741e81dce9e6]	Wird jede Minute ausgeführt. Aktualisiert das Discovery-Statusattribut für Anwendungsservices. Der Discovery-Status wird als Gesamtstatus für alle Endpunkte berechnet, die ein für Service enthält.
Flow Discovery-Planer [sysauto_script_74c676f0dbb0220060ff742eaf961ef2]	Wird alle 10 Minuten ausgeführt. Löst Netzwerk-Flow-Discovery aus und schreibt die Daten in die Tabelle [sa_flow_connector]. Diese regelmäßige Aufgabe ist standardmäßig deaktiviert. Aktivieren Sie diese regelmäßige Aufgabe, um CIs mithilfe von Netflow zu erkennen (siehe Beschreibung in Datenerfassung und -erkennung mit Netflow).
Einstiegspunktkandidaten aus Netflow- und netstat-Daten generieren [sysauto_script_b0b95067c3d0030039a3553a81d3ec5]	Wird täglich ausgeführt. Scannt die TCP-Verbindungstabelle [cmdb_tcp] und analysiert diese Daten, um Einstiegspunkte zu generieren und in der Tabelle „Kandidateneinstiegspunkte“ [sa_cand_entry_point] zu speichern. Diese regelmäßige

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
	Aufgabe unterstützt das Generieren von Einstiegspunkten, die für die Zuordnung mehrerer Anwendungsservices (als Massenvorgang) erforderlich sind. Diese regelmäßige Aufgabe ist standardmäßig aktiviert.
Thread-Sicherungen speichern [sysauto_script_a49cd030c302020039a3553a81a3fgefb]	Standardmäßig nicht aktiv. Wenn die Aufgabe aktiviert wird, werden Thread-Sicherungen gesammelt, und die Daten werden in der Tabelle [sys_thread_dump] gespeichert.
Statistiken für langsame Schritte speichern [sysauto_script_dc0de690c302020039a3553a81b3ter2]	Wird jede Minute ausgeführt. Sammelt Daten zur langsamen Ausführung von Musterschritten und schreibt diese Daten in die Tabelle [sys_step_pattern].
Anzahl der Server berechnen [sys_trigger_db438f407f510200f128134f8dfa91c6]	Wird jeden Sonntag ausgeführt. Aktualisiert die Lizenzierungsmetrik mit der Gesamtanzahl der erkannten Server in der Instanz. Diese Informationen dienen zur Abrechnung. In Instanzen mit Domänentrennung wird die Anzahl für jede Domäne aktualisiert.
DNS-Suche für alle Einstiegspunkte und manuellen Verbindungsendpunkte ausführen [f178ab457fb213001952baf8befa91d3]	Führt für alle Einstiegspunkte und manuellen Verbindungsendpunkte die Probe zur DNS-Suche aus und aktualisiert Informationen über die entsprechenden IP-Adressen in der CMDB. Diese regelmäßige Aufgabe ist standardmäßig deaktiviert.
[SM-Deduplizierungs-Tracker für bestimmte Erkennungsquellen]	In einigen Fällen identifizieren Service-Mapping und Discovery- oder Überwachungstools von Drittanbietern dasselbe Konfigurationselement (CI) unterschiedlich. Das führt dazu, dass die Anwendungstabelle CMDB zwei Datensätze für dasselbe CI enthält. Diese regelmäßige Aufgabe scannt die CMDB-Anwendungstabellen mit den Informationen über CIs, die als generische Anwendungen identifiziert wurden. Wenn die regelmäßige Aufgabe aufgrund des CI-Typs und der Erkennungsquelle doppelte Datensätze identifiziert, wird eine Deduplizierungsaufgabe erstellt.
[sys_auto_flush_5211e7e1c320220039a3553a81b3ceeg]	Bereinigt in der Tabelle [sa_flow_connection] Datensätze, die in den letzten sieben Tagen nicht aktualisiert wurden
[sys_auto_flush_956d498b938503006a7031f635fbeec]	Bereinigt in der Tabelle [sa_performance_statistics] Datensätze, die Statistiken über die gesamte Ereignisverarbeitungszeit enthalten und vor mehr als 30 Tagen erstellt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regelmäßige Aufgabe	Beschreibung
[sys_auto_flush_ce1a978193001200e0e931f635be0]	Löscht in der Tabelle [sa_performance_statistics] Datensätze, die vor mehr als 2 Tagen erstellt wurden
[sys_auto_flush_b24d9c30c302020039a3553a81b3e]	Löscht in der Tabelle [sys_thread_dump] Datensätze, die vor mehr als 7 Tagen erstellt wurden
[sys_auto_flush_cf129ebe7f223200995cbaf8bef0]	Löscht in der Tabelle [sa_ml_feature_data] Datensätze, die in den letzten 7 Tagen nicht aktualisiert wurden und einen Sonderstatus aufweisen (leeres Bezeichnungsfeld)
[sys_auto_flush_d2516be1c320220039a3553a81b3e]	Löscht in der Tabelle [sa_flow_service] Datensätze, die in den letzten 7 Tagen nicht aktualisiert wurden
[sys_auto_flush_db416be1c320220039a3553a81b3e]	Löscht in der Tabelle [sa_flow_server_comm] Datensätze, die in den letzten 7 Tagen nicht aktualisiert wurden.
[sys_auto_flush_41d9b007b71310105984eb25de]	Löscht die Tabelle für Verbindungsvorschläge [sa_ml_connection_suggestion] aus den alten Datensätzen, die den folgenden Bedingungen entsprechen: • Sie wurden in den letzten 7 Tagen nicht aktualisiert. • Der Vorschlagsdatensatz enthält eine aktive erkannte TCP-Verbindung (TCP-Verbindungsdatensatz fehlt nicht). • Dem Datensatz ist keine Benutzerentscheidung vom Typ „Hinzufügen“ oder „Entfernen“ zugeordnet.

Installierte Tabellen

Tabelle	Beschreibung
Skripts für Aufgabe vor Service Mapping [sa_pre_task_script]	Enthält Skripts, die Service-Mapping in der Instanz ausführt, und sammelt Informationen, die bei der Identifizierung des relevanten Musters für ein CI helfen
Verkehrsbasierte Verbindungsqualifizierer [cmdb_ci_qualifier_traffic_based_connection]	Veralteter Inhalt. Wird in der aktuellen Version nicht verwendet.
Dynamic CI-Gruppe [cmdb_ci_query_based_service]	Enthält technische Services

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Komponenten [sa_bs_components]	Enthält Informationen über Komponenten, die Teil des für Service sind. Kunden geben diese Informationen manuell auf der Registerkarte „Fragebogen“ im Formular des für Service ein.
Kandidateneinstiegspunkte [sa_cand_entry_point]	Enthält Informationen über potenzielle Einstiegspunkte, die Service-Mapping aus Lastenausgleichsmodulen oder datenverkehrsbasierten Verbindungen abgerufen hat
Dashboard-Ansicht [sa_dashboard_view]	Enthält eine Konfiguration, die definiert, welche Services in der Servicestruktur angezeigt werden
Service-Discovery-Nachrichten [sa_discovery_message]	Enthält Erkennungsmeldungen und -fehler, die Service-Mapping während des Erkennungsprozesses generiert
ITOM-Fehleraufgabe [sa_error_handler_task]	Enthält Informationen, die Service-Mapping und Discovery zur Fehlerbehandlung verwenden
Fehler-EP ALS manueller EP [sa_errors_as_manual_ep]	Enthält Daten zu Fehlern, die Kunden während des folgenden Verfahrens überspringen: Fehler überspringen, um mit der Erkennung eines Anwendungsservice fortzufahren.
Manuelle Verbindungen [sa_manual_connections]	Enthält Informationen über Endpunkte, die Kunden beim Hinzufügen manueller Verbindungen verwenden
ML-Featuredaten [sa_ml_feature_data]	Interne Tabelle
ML-Modell [sa_ml_model]	Interne Tabelle
ML-Datenverkehrvalidierung [sa_ml_traffic_validation]	Interne Tabelle
Leistungsstatistiken [sa_performance_statistics]	Interne Tabelle zum Speichern von Leistungsdaten zur Auswirkungsberechnung in Ereignismanagement
Servicezuordnungen [sa_service_counters]	Speichert Daten über die Anzahl der CIs und Erkennungsfehler pro erkanntem Service
Eingabepunkte für Simulation [sa_simulation_entry_points]	Interne Tabelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Serviceaufgabenprozess [service_process_task]	Speichert Datenanforderungen und Überprüfungsanforderungen für Anwendungsservices.
Langsame Schritte [sys_step_pattern]	Speichert Informationen über die langsame Ausführung von Musterschritten. Diese Daten werden zur Überwachung und Problembehandlung verwendet.
Thread-Sicherung [sys_thread_dump]	Interne Tabelle zum Speichern von Leistungsdaten für die Fehlerbehebung in Ereignismanagement
Automatisierungsfehler-Kategorie [automation_error_category]	Speichert alle unterstützten Kategorien für Fehler
Automatisierungsfehler-Kategorien-Statistik [automation_error_category_stats]	Speichert die neuesten Fehlerstatistiken für alle Fehlerkategorien
Automatisierungsfehlercode [automation_error_code]	Speichert alle unterstützten Fehlercodes für Erkennungsfehler
Automatisierungs-Fehlercode-Statistik [automation_error_code_stats]	Speichert die neuesten Fehlerstatistiken für alle Fehlercodes
Statistik zu Automatisierungsfehler-Discovery-Kategorien [automation_error_discovery_category_stats]	Veraltet.
Statistik zum Automatisierungsfehler-Discovery-Code [automation_error_discovery_code_stats]	Veraltet.
Automatisierungsfehler-Discovery-Nachricht [automation_error_discovery_msg]	Speichert die neuesten Fehlermeldungen
Automatisierungsfehlerkategorien – Statistiken [automation_error_instance_category_stats]	Speichert die neuesten Fehlerstatistiken für alle Kategorien pro Instanz (Discovery-Status)
Automatisierungsfehler-Kategorien-Statistik [automation_error_instance_code_stats]	Speichert die neuesten Fehlerstatistiken für alle Fehlercodes pro Instanz (Discovery-Status)
Automatisierungsfehler − Instanzmeldung [automation_error_instance_msg]	Speichert alle der Instanz zugeordneten neuesten Fehler (Discovery-Status)
Automatisierungsfehler − Instanzmeldung	Speichert die letzte Aktualisierungszeit für jede Anwendung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[automation_error_stats_update_time]	
Automatisierungsfehlervorschlag [automation_error_suggestion]	Enthält alle konfigurierten Vorschläge, die an der Benutzeroberfläche für verschiedene Fehlercodes angezeigt werden
Automatisierungsquellenapplikation [automation_source_application]	Enthält die Quellanwendungen, die das Fehler-Framework von Discovery und Service-Mapping verwenden
Zuordnung zwischen Vorschlag und Fehlercode [suggestion_error_code_m2m]	Enthält Informationen über die Zuordnung zwischen Fehlercode und Empfehlung
ITOM-Fehleraufgabe [sa_error_handler_task]	Enthält die für verschiedene Fehlergruppen konfigurierten Aufgaben
Applicative-Anmeldeinformationen [sa_applicative_credentials]	Enthält Anmeldeinformationen, die beim Ausführen von anwendungsspezifischen Befehlen auf Servern verwendet werden
Service-Mapping CI-Attribute [sa_ci_attr]	Enthält CI-Attribute, die nur für den Erkennungsprozess relevant sind
Zugehörige CI-Typen [sa_ci_to_pattern]	Weist Mustern CI-Typen zu (nur relevant für die horizontale Erkennung durch Discovery)
Muster-Debugger-Sitzung [sa_debug_session]	Diese interne Tabelle wird für die Komponenten des Musterdesigners verwendet.
Status der Muster-Debugger-Sitzung für UI [sa_debug_session_status]	Diese interne Tabelle wird für die Komponenten des Musterdesigners verwendet.
Sa zurückgestellte Service-Discovery [sa_deferred_service_discovery]	Diese interne Tabelle wird für die Service-Mapping-Komponenten verwendet.
Service-Discovery-Protokoll [sa_discovery_log]	Enthält von Service-Mapping gesammelte Discovery-Protokolle
Service-Discovery-Nachrichten [sa_discovery_message]	Enthält Nachrichten, die von Service-Mapping während der Serviceerkennung erstellt wurden
Sa-Endpunkt-Status [sa_endpoint_status]	Enthält den Discovery-Status für Endpunkte in Service-Mapping

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Hostskripts suchen [sa_find_host_scripts]	Enthält die Namen von Skripteinbindungen, die basierend auf den Endpunkt-Glide-Datensätzen nach Hosts suchen
nfdump-Datei [sa_flcon_file_nfdump]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
nfdump-Installation [sa_flcon_local_nfdump]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
AWS VPC-Flow-Protokolle [sa_flcon_vpc_flow_log]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
SA-Flow-Verbindung [sa_flow_connection]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
Flow-Connector [sa_flow_connector]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
Flow-Serverkommunikation [sa_flow_server_comm]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
IP/Port und Statistiken für Fluss-Services [sa_flow_service]	Diese interne Tabelle enthält Informationen für die Netflow-basierte Erkennung.
Host-Klasse zu Fähigkeit [sa_host_class_to_capability]	Ordnet den Servertyp den für Service-Mapping erforderlichen Fähigkeiten zu
Infrapfad zu Elementen [sa_infra_path_assoc]	Enthält Daten zu Komponenten, die Teil eines Netzwerkpfads sind
Externe Discovery-Befehle zuordnen [sa_mapping_ext_commands]	Enthält Daten über benutzerdefinierte Befehle, die vom Benutzer erstellt wurden
Netzwerkpfade [sa_network_paths]	Enthält Daten zu Netzwerkpfaden, die von Service-Mapping erkannt wurden.
Horizontale erkannte ausgelagerte Payloads [sa_paged_payload]	Service-Mapping verwendet die Daten in dieser Tabelle, um die von MID-Server gesendete Nutzlast zu teilen, wenn die Erkennung zu einer sehr großen Nutzlast führt.
Discovery-Muster [sa_pattern]	Enthält vorkonfigurierte und benutzerdefinierte Muster, die Service-Mapping für die Erkennung verwendet
Service-Mapping-Entwurfsmuster	Enthält nicht aktivierte Erkennungsmuster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sa_pattern_draft]	
Service-Mapping-Beziehungsattribute [sa_rel_attr]	Enthält während des Service-Erkennungsprozesses verwendete Beziehungsattribute
Bez. zu Infrapfad [sa_rel_to_infra_path]	Ordnet Beziehungen Netzwerk- oder Speicherpfaden zu
Servicezuordnung für Servernutzung [sa_server_usage]	Enthält die Anzahl der von Service-Mapping verwendeten Server
Dateisystem zu Speicherpfad [sa_storage_paths]	Enthält Daten zu von Service-Mapping erkannten Speicherpfaden
Speicherpfad-Verbindungszuordnung [sa_storage_path_connectivity_map]	Ordnet das Dateisystem dem Speichervolume zu
Verkehrsbasierte Discoveryregeln [sa_traffic_based_rules]	Enthält Daten über die Konfiguration der datenverkehrsbasierten Erkennung
Hochgeladene Date [sa_uploaded_file]	Enthält Daten zu Dateien, die auf den MID-Server hochgeladen und von Service-Mapping verwendet werden
Configuration Item [cmdb_ci]	Speichert Daten über alle Konfigurationselemente (CIs) in CMDB
Applikation [cmdb_ci_appl]	Speichert Daten über alle Konfigurationselemente (CIs) vom Typ Anwendung in CMDB
IP-Service [cmdb_ip_service]	Speichert Daten zur Unterstützung der Erkennung ohne Anmeldeinformationen für die ursprüngliche Tabelle
Applikationskategorie [discovery_category_appl]	Speichert Daten über Anwendungskategorien, die vom Musterdesigner zur Verwaltung von Musterbibliotheken verwendet werden
Geräteklassifizierungskategorie [discovery_category_device_class]	Speichert Informationen über die Beziehung zwischen einem Geräteklassifizierer und einem Protokoll, das bei einer horizontalen Erkennung durch Discovery verwendet wird
Geräteinfokategorie [discovery_category_device_info]	Speichert Informationen über die Gerätekategorie, die bei einer horizontalen Erkennung durch Discovery verwendet wird
Protokollkategorie	Speichert Informationen über die Protokollkategorie, die bei einer horizontalen Erkennung durch Discovery verwendet wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[discovery_category_protocol]	
HTTP-Klassifizierung [discovery_classy_http]	Speichert die HTTP-Klassifizierungsdefinition
Übereinstimmung der HTTP-Klassifizierung [discovery_classy_http_match]	Speichert die HTTP-Klassifizierungsbedingungen und die Informationen über das Muster, das bei Übereinstimmung mit der Klassifizierungsbedingung gestartet werden soll
Startprogramm für Discovery-Muster [discovery_pattern_launcher]	Speichert Informationen über den Musterstartmechanismus
Cloud-Ausführungsmuster [discovery_ptrn_cld_lchr]	Speichert Informationen über den Musterstartmechanismus für die Erkennung von Cloud-Anwendungen
Ausführungsmuster ohne Server [discovery_ptrn_hostless_lchr]	Speichert Informationen über den Musterstartmechanismus für die serverlose Erkennung
Parameter für Discovery-Muster [discovery_ptrn_lnch_param]	Speichert die Parameter für die serverlose/Cloud-Anwendungsausführung
Eingabeparameter für Muster [discovery_ptrn_lnch_param_def]	Speichert die nach Mustern gesammelten Schlüsselparameter
Applicative-Anmeldeinformationen [sa_applicative_credentials]	Speichert die Applicative-Anmeldeinformationen
Zugehörige CI-Typen [sa_ci_to_pattern]	Speichert zugehörige CIs in Mustern
Benutzerdefinierter Vorgang [sa_custom_operation]	Speichert Informationen über von Benutzern definierte Erkennungsmustervorgänge
Benutzerdefinierte Vorgangsparameter [sa_custom_operation_param]	Speichert benutzerdefinierte Vorgangsparameter für Erkennungsmuster
Benutzerdefinierte Analysestrategie [sa_custom_parsing_strategy]	Speichert Informationen über von Benutzern definierte Musteranalysestrategien
Debug-Sitzung [sa_debug_session]	Speichert Informationen aus Debug-Sitzungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Status der Muster-Debugger-Sitzung für UI [sa_debug_session_status]	Speichert Informationen zum Status der Debug-Sitzung für UI-Zwecke
Sa zurückgestellte Service-Discovery [sa_deferred_service_discovery]	Enthält Informationen zum Starten der Debug-Sitzung von oben nach unten, wenn der relevante Host noch nicht erkannt wurde
Discovery-Protokoll [sa_discovery_log]	Das Protokoll mehrerer Erkennungsvorgänge
Hostskripts suchen [sa_find_host_scripts]	Enthält Skripts zum Suchen von Hosts in der CMDB basierend auf den Einstiegspunktinformationen
Host-Klasse zu Fähigkeit [sa_host_class_to_capability]	Enthält Informationen, die den Hosttyp zu MID-Server-Fähigkeiten zuordnen. Beispielsweise wird das Linux-Betriebssystem der SSH-WMI-Fähigkeit zugeordnet.
Zuordnung von Discovery-Befehlen [sa_mapping_ext_commands]	Enthält anpassbare Vorgänge für den Musterdesigner
Horizontale erkannte ausgelagerte Payloads [sa_paged_payload]	Enthält die Nutzlast der IE-Ausgabe, wenn der Teilungsmechanismus bereitgestellt wird
Discovery-Muster [sa_pattern]	Speichert veröffentlichte Muster
Servicezuordnungsentwurfsmuster [sa_pattern_draft]	Speichert die geänderte Version von Mustern
Mustererweiterungen [sa_pattern_extension]	Speichert Mustererweiterungsabschnitte
Muster des Vor-/Post-Skripts [sa_pattern_prepost_script]	Speichert Vor-/Nach-/Vor-Ausführungskripts für Muster
Snapshot von erkannten horizontalen Nutzlasten [sa_payload_snapshot]	Speichert die Nutzlast der IE-Ausgabe zum Löschen pro Haupt-CI
Nachverfolgte Datei – Definition [sa_tracked_file_definition]	Speichert die Definitionen der Funktion zur Dateinachverfolgung
Hochgeladene Date [sa_uploaded_file]	Speichert von der Muster-Engine verwendete Skripts und Dateien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Eigenschaften

Hinweis: Um die Tabelle „Systemeigenschaft“ [sys_properties] zu öffnen, geben Sie im Navigationsfilter *sys_properties.list* ein.

Eigenschaft	Beschreibung
sa.max_relations_in_service	Die maximale Anzahl von CI-Beziehungen für einen Service. Wenn der Wert überschritten wird, werden einige Services automatisch von der Anzeige in der Zuordnungsansicht ausgeschlossen. Sehr große Anwendungsservices können zu Leistungsproblemen führen. Anstelle von Karten können Benutzer für große Anwendungsservices CI-Listen anzeigen. • **Typ**: Ganzzahl • **Standardwert**: 5.000 • **Grenzwert**: 10.000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
best_practice.check_connectivity.expand_listening_pid	Diese Eigenschaft steuert, welche PIDs Service-Mapping während des Hop-Vorgangs bei der Konnektivitätsprüfung prüft. Wenn diese Eigenschaft true ist, überprüft Service-Mapping die Konnektivität nur für PIDs, deren Ports sich im Status *listening* befinden, nicht jedoch, wenn der Status *connected* lautet. • **Typ**: Boolesch • **Standardwert**: true • **Weitere mögliche Werte**: false • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
com.snc.sw.mapping.reaper.checkpoints_to_keep	Die maximale Anzahl von Change-Markierungen, die in der Verlaufszeitleiste des Service verwaltet werden. Wenn Sie den Wert auf Null oder eine negative Ganzzahl setzen, wird die Standardeinstellung überschrieben, und alle Change-Markierungen werden maximal drei Monate lang beibehalten. Mit der Eigenschaft „com.snc.sw.mapping.reaper.ignored_services_from_optimiz können Sie bestimmte Services ausschließen und Change-Markierungen basierend auf Intervallen entfernen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Ganzzahl • **Standardwert**: 1.000
com.snc.sw.mapping.reaper.ignored_services	Diese Eigenschaft enthält die durch Kommas getrennten Service-IDs. Anstelle der durch die Eigenschaft „com.snc.sw.mapping.reaper.checkpoints_to_keep“ angegebenen Anzahl behalten diese Services alle Change-Kennzeichnungen für maximal drei Monate. **Typ**: Ganzzahl
com.snc.sw.mapping.reaper.max_reap_size	Die maximale Anzahl von Change-Markierungen, die jedes Mal gelöscht werden, wenn das System alte und nicht verwendete Datensätze aus dem Verlauf der Änderungen an dem Service entfernt. Wenn Sie den Wert auf Null oder eine negative Ganzzahl festlegen, wird der Grenzwert überschrieben, und alle unnötigen Change-Markierungen können entfernt werden. • **Typ**: Ganzzahl • **Standardwert**: 100000
glide.service_mapping.computation_depth	Diese Eigenschaft steuert die maximale Tiefe der für Service-Zuordnung. • **Typ**: Ganzzahl • **Standardwert**: 25 • **Andere mögliche Werte**: beliebige Zahl über 1 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa_ml.connection_suggestions.active	Aktivieren Sie die Funktion zum Generieren von Verbindungsvorschlägen, die auf der datenverkehrsbasierten Erkennung basiert. Service-Mapping generiert Verbindungsvorschläge anhand der von Predictive Intelligence analysierten Daten. Wenn diese Funktion aktiviert ist, können Sie Verbindungsvorschläge zum Verwalten von CI-Verbindungen in Anwendungsservices verwenden. • **Typ**: Boolesch • **Standardwert**: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Hinweis: Wenn die datenverkehrsbasierte Erkennung in Ihrer Bereitstellung vor Release Quebec aktiviert war und Sie diese Funktion verwendet haben, um mindestens einen Anwendungsservice zu erkennen, ist der Wert standardmäßig auf *false* festgelegt. • **Weitere mögliche Werte**: false • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.debugger.max_timeout	Maximale Zeitüberschreitung (in Sekunden) seit der letzten Serveraktivität während einer Ausführung des Muster-Debuggers • **Typ**: Ganzzahl • **Standardwert**: 120 • **Andere mögliche Werte**: beliebige Zahl über 60 • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**. Weitere Informationen finden Sie unter KB0854603: Zeitüberschreitung bei Muster-Debugger-Sitzung .
sa.discovery_task_timeout_min	Maximale Zeit für eine Service-Mapping-Aufgabe in Minuten (einschließlich Warten auf Ausführung in internen Warteschlangen und ECC-Warteschlange) • **Typ**: Zeichenfolge • **Standardwert**: 120 • **Andere mögliche Werte**: beliebige Zahl über 30 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.enable_gray_out_on_resume_discovery	Hiermit wird die Unterstruktur ausgegraut, nachdem Service-Mapping die Erkennung am Edge wieder aufgenommen hat, oder die Erkennung wird für die gesamte Topologie erneut ausgeführt. • **Typ**: Boolesch • **Standardwert**: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Weitere mögliche Werte**: false • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.excluded_discovery_sources	Fügen Sie diese Eigenschaft hinzu, um Discovery-Quellen bei der Hosterkennung auszuschließen. • **Standardwert**: EventManagement • **Andere mögliche Werte**: zusätzliche Discovery-Quellen, hinzugefügt nach EventManagement, getrennt durch ein Komma
sa.map.enable_loops_on_service_split	Ermöglicht es Ihnen, einen für Service mit einem anderen, bereits vorhandenen für Service zu verbinden, auch wenn die CI-Verbindung (Endpunkt), die Sie herstellen, Teil dieses anderen für Service ist. Diese Eigenschaft trägt dazu bei, Schleifen oder Zyklen in Servicezuordnungen zu vermeiden. • **Typ**: Boolesch • **Standardwert**: false • **Weitere mögliche Werte**: true • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sa_ml.connection_suggestions.lb.routing.enabled	Status, wenn ein Zielhost ein Mitglied des Lastenausgleichsmoduls ist oder nicht in der Liste „Verbindungsvorschlagen“ ist. • **Typ**: true/false • **Standardwert**: true • **Weitere mögliche Werte**: false • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties].
sa.network_path_calculation.arp_enableadded gemäß DOC 1074513 in Vancouver	Steuert Abfragen an die ARP-Tabelle. Daten werden nur berechnet, wenn der Wert auf „wahr“ festgelegt ist. **Hinweis:** Weitere Informationen zum Abfragen der ARP-Tabelle finden Sie im Artikel ARP-Eigenschaftsdokumentation für Service-Mapping [KB1311037] in der Now Support Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: true/false • **Standardwert**: false • **Weitere mögliche Werte**: true • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.network_path_calculation.active	Aktiviert die Netzwerkpfadberechnung • **Typ**: true/false • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sa.rediscovery.batch_size	Anzahl der in einem einzigen Stapel ausgeführten Erkennungsaufgaben • **Typ**: Ganzzahl • **Standardwert**: 100 • **Andere mögliche Werte**: beliebige Zahl über 10 • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sa.service_history.max_allowed_bubbles	Anzahl der Änderungen, die auf der Verlaufsskala und der Registerkarte „Changes“ angezeigt werden • **Typ**: Ganzzahl • **Standardwert**: 3000 • **Andere mögliche Werte**: beliebige Zahl über 3000 **Wichtig:** Das Erhöhen des Werts für diese Eigenschaft kann zu Leistungsprobleme beim Laden von Zuordnungen des für Service führen. • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sa.service.max_ci_service_population	Die maximale Anzahl von CI-Verbindungen, die Anwendungsservices während der folgenden Vorgänge hinzugefügt werden: Konvertieren von manuellen Services, die in Ereignismanagement erstellt wurden, in Anwendungsservices mit Changes von CMDB.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Ganzzahl • **Standardwert**: 1.000 • **Grenzwert**: 2000 • **Speicherort**: Zur Tabelle „Systemeigenschaften“ [sys_properties] hinzufügen . Das Erhöhen des Standardwerts kann zu Leistungsproblemen führen.
sa.storage_path_calculation.active	Aktiviert die Speicherpfadberechnung • **Typ**: true/false • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sa.topdown.mapping_with_acc_mode	Diese Eigenschaft ermöglicht die Top Down-Discovery und das Service-Mapping mit Agent Client Collector, indem der Auswahlmodus MID-Server für die Top Down-Discovery definiert wird. • **Typ:** Ganzzahl • **Standardwert:** 0 • **Andere mögliche Werte:** 1,2 0: Discovery von oben nach unten wird ausschließlich mit MID-Server ausgeführt. 1: Die Top Down-Discovery versucht zunächst, mit Agent Client Collectorausgeführt zu werden. Wenn kein Agent verfügbar ist, wird standardmäßig MID-Serververwendet. 2: Discovery von oben nach unten wird ausschließlich mit Agent Client Collector ausgeführt. Wenn dies nicht erfolgreich ist, wird der Prozess beendet.
sa.traffic_based_discovery.active	Datenverkehrsbasierte Erkennung • **Typ**: true/false • **Standardwert**: false • **Weitere mögliche Werte**: true • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Hinweis: Diese Eigenschaft gilt nur für datenverkehrsbasierte Legacy-Verbindungen. Wenn auf maschinellem Lernen (ML) basierende Verbindungsvorschläge aktiviert sind, stellen Sie sicher, dass der Eigenschaftswert auf „`false`"festgelegt bleibt.
sa.traffic_based_discovery.conn_aging_time	Zeitraum in Stunden, für den eine datenverkehrsbasierte Verbindung seit der letzten Erkennung aktiv bleibt • **Typ**: Ganzzahl • **Standardwert**: 72 • **Andere mögliche Werte**: beliebige Zahl über 24 • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sa.traffic_based_discovery.ignored_ports	Bei einer datenverkehrsbasierten Erkennung gefundene Ports, die ignoriert werden können. Diese Eigenschaft ist in der Tabelle für Systemeigenschaften [sys_properties] verfügbar. Ändern Sie diese Eigenschaft, um Ports zu definieren, die Service-Mapping bei der datenverkehrsbasierten Erkennung ignoriert. Dadurch wird die Erkennung effizienter, da keine Ressourcen für die Erkennung irrelevanter Verbindungen verschwendet werden. • **Typ**: Zeichenfolge • **Standardwert**: 445, 139, 111, 2049, 860, 3260, 135, 53 • **Andere mögliche Werte**: alle relevanten Portnummern • **Speicherort**: Tabelle „Systemeigenschaft" [sys_properties]
sa.traffic_based_discovery.max_connections	Maximale Anzahl datenverkehrsbasierter Verbindungen von einem einzelnen CI. Diese Eigenschaft ist in der Tabelle für Systemeigenschaften [sys_properties] verfügbar. Diese Eigenschaft trägt dazu bei, die Größe der Zuordnung angemessen zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	halten, indem die Anzahl der möglichen CI-Verbindungen begrenzt wird. • **Typ**: Ganzzahl • **Standardwert**: 30 • **Andere mögliche Werte**: beliebige Zahl über 1 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sa.update_paths_in_service_model.active	Aktualisiert Netzwerk- und Speicherpfade im Servicemodell • **Typ**: true/false • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
service_watch.implied_match.endpoint.black_list	Liste Liste von Endpunkttypen, auf die Service-Mapping während der Musterausführung von oben nach unten keine Prozessabgleichlogik anwendet • **Typ**: Zeichenfolge • **Standardwert**: cmdb_ci_endpoint_ssis_mssql, cmdb_ci_endpoint_ssas_mssql • **Andere mögliche Werte**: kommagetrennte Liste von Endpunkten • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sm.service.export.blacklist	Schließt die genannten Felder aus dem Datensatz in der Exportdatei der Servicedefinition aus • **Typ**: Zeichenfolge • **Standardwert**: [leer] • **Andere mögliche Werte**: durch Kommas getrennte Liste von Feldern • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sm.service.export.blacklist.cmdb_ci_endpoint	Schließt die genannten Felder aus dem Einstiegspunkt-Datensatz in der Exportdatei der Servicedefinition aus

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Zeichenfolge • **Standardwert**: [leer] • **Andere mögliche Werte**: durch Kommas getrennte Liste von Feldern • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sm.service.export.blacklist.cmdb_ci_service_discovered	Schließt die genannten Felder aus dem Anwendungsservice-Datensatz in der Exportdatei der Servicedefinition aus • **Typ**: Zeichenfolge • **Standardwert**: discovery_status,operational_status,process_status,work_no • **Andere mögliche Werte**: durch Kommas getrennte Liste von Feldern • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sm.service.export.blacklist.cmdb_ci_service_group	Schließt die genannten Felder aus dem Servicegruppen-Datensatz in der Exportdatei der Servicedefinition aus Trennen Sie die einzelnen Felder mit Kommas. • **Typ**: Zeichenfolge • **Standardwert**: [leer] • **Andere mögliche Werte**: durch Kommas getrennte Liste von Feldern • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sm.service.export.max_services_limit	Definiert die maximal zulässige Anzahl von zu exportierenden Services • **Typ**: Ganzzahl • **Standardwert**: 100 • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sm.service.export.skip_empty_fields	Schließt Felder mit einem leeren Wert aus dem Datensatz in der Exportdatei der Servicedefinitionen aus. • **Typ**: Boolesch • **Standardwert**: true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sm.service.export.skip_reference_fields	Schließt Referenzfelder aus dem Datensatz in der Exportdatei der Servicedefinition aus • **Typ**: Boolesch • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sm.service.export.skip_sys_fields	Schließt Felder, die mit „sys_“ beginnen, aus dem Datensatz in der Exportdatei der Servicedefinition aus • **Typ**: Boolesch • **Standardwert**: true • **Weitere mögliche Werte**: false • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sm.service.import.auto_start_discovery	Aktiviert die automatische Erkennung aller erfolgreich importierten Einstiegspunkte • **Typ**: Boolesch • **Standardwert**: false • **Weitere mögliche Werte**: true • **Standort**: **Service-Mapping** > **Administration** > **Eigenschaften**.
sn_cloud_migration.categories.inclusion_list	Kommagetrennte Allow-Liste von Kategorien für die Cloud-Migration. Am Migrationsprozess können nur Ressourcen teilnehmen, die hier aufgelisteten Kategorien zugewiesen sind. • **Typ**: Zeichenfolge • **Standardwert**: Physisch, VMware, HyperV, IBM HMC, OpenStack, Solaris, Nutanix, Amazon AWS, Microsoft Azure, Google Cloud, IBM Cloud • **Standort**: **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration** > **Administration** > **Eigenschaften**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
sn_cloud_migration.server_status.inclusion_list	Kommagetrennte Allow-Liste des Serverstatus für die Cloud-Migration. Am Migrationsprozess können nur Server mit einem hier aufgeführten Installationsstatus teilnehmen. • **Typ**: ? • **Standardwert**: 1 • **Anderer möglicher Wert**: Installiert = 1, Bestellt = 2, In Wartung = 3, Ausstehende Installation = 4, Ausstehende Reparatur = 5, Auf Lager = 6, Stillgelegt = 7, Gestohlen = 8, Abwesend = 100 • **Standort**: **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration** > **Administration** > **Eigenschaften**
sn_cloud_migration.os.exclusion_list	Kommagetrennte Deny-Liste von Betriebssystemen für die Cloud-Migration. Server, deren Betriebssystem hier aufgeführt ist, werden vom Migrationsprozess ausgeschlossen. • **Typ**: Zeichenfolge • **Standardwert**: ESX, Windows 2000, Windows XP. • **Standort**: **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration** > **Administration** > **Eigenschaften**
sn_cloud_migration.vm_state.inclusion_list	Kommagetrennte Allow-Liste von VM-Instanzstatus für die Cloud-Migration. Am Migrationsprozess können nur VMs mit einem hier aufgeführten Status teilnehmen. • **Typ**: ?? • **Standardwert**: Ein • **Andere mögliche Werte**: Ein, Aus, Angehalten, Geplant, Wird gestartet, Wird gestoppt, Stillgelegt, Beendet, Fehler, Abgebrochen, Wird angehalten, Wird beendet • **Standort**: **Cloud-Migration** > **Arbeitsbereich für Cloud-Migration** > **Administration** > **Eigenschaften**
	Die Anzahl der CI-Beziehungen, nach deren Überschreiten Anwendungsservices nicht automatisch in der Zuordnungsansicht angezeigt werden. Sehr große Anwendungsservices können zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Leistungsproblemen führen. Anstelle von Karten können Benutzer für große Anwendungsservices CI-Listen anzeigen. Durch das Festlegen eines negativen Werts wird die Anzahl der hinzugefügten CI-Beziehungen nicht eingeschränkt. Wenn ein ungültiger Wert wie eine Zeichenfolge festgelegt wird, entspricht dies dem Standardwert 5000. • **Typ**: Ganzzahl • **Standardwert**: 5.000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
svc_by_tags.classes.whitelist	Diese Eigenschaft enthält die Liste der zulässigen CI-Klassen, getrennt durch Kommas. Die Tag-basierte Zuordnung schließt die CIs ein, die zu diesen Klassen gehören. Ein leeres Feld „Wert“ gibt an, dass alle CI-Klassen einbezogen werden.
svc_by_tags.install_status.blacklist	Diese Eigenschaft enthält die Liste der Ausschlüsse basierend auf dem Installationsstatus, getrennt durch Kommas. Die tagbasierte Zuordnung schließt CIs mit Tags mit den folgenden Installationsstatus aus: **Standardwert**: 7.100 **Andere mögliche Werte**: Installiert = 1, Bestellt = 2, In Wartung = 3, Ausstehende Installation = 4, Ausstehende Reparatur = 5, Auf Lager = 6, Deaktiviert = 7, Gestohlen = 8
svc_by_tags.max.categories.per.family	Legen Sie die maximale Anzahl der pro Servicefamilie zulässigen Kategorien fest. • **Typ**: Ganzzahl • **Standardwert**: 3
svc_by_tags.max.traversal.rules.active	Legen Sie die maximal zulässige Anzahl von CI-Beziehungen fest, die sich im aktiven Status befinden können. Service-Mapping verwendet für die Tag-basierte Erkennung nur aktive CI-Beziehungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Ganzzahl • **Standardwert**: 5 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
svc_by_tags.max_ci_limit	Legen Sie die maximal zulässige Anzahl von CIs fest, die ein auf Tags basierender Anwendungsservice enthalten kann. • **Typ**: Ganzzahl • **Standardwert**: 1.000 • **Grenzwert**: 2000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
sm.topdown.reuse_mid_from_hd_schedule	Verwenden Sie die während der Horizontal-Discovery konfigurierte MID-Server -Komponente für die Top Down-Discovery. • **Typ:** boolean • **Standardwert:** false • **Andere mögliche Werte:** true • **Standort: Service-Mapping** > **Administration** > **Eigenschaften**
sm.network_location.detect_host_by_location	Wählen Sie den Standort des Subnetzes, damit der entsprechende Host und MID-Serveridentifiziert werden können. **Wichtig:** Um die besten Ergebnisse zu erzielen, müssen Sie diese Eigenschaft und „sm.topdown.reuse_mid_from_hd_schedule“ gleichzeitig aktivieren. • **Typ:** boolean • **Standardwert:** false • **Andere mögliche Werte:** true • **Standort: Service-Mapping** > **Administration** > **Eigenschaften**

Domain Separation und Service-Mapping

Die Domänentrennung wird in Service-Mapping unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

So funktioniert Domain Separation in Service-Mapping

Wechseln Sie in Umgebungen mit Domänentrennung zu relevanten Blattdomänen, um auf Aktionen im Zusammenhang mit der Zuordnung durch Service-Mapping zuzugreifen. Ein Endknoten ist eine untergeordnete Domäne der untersten Ebene, d. h. sie verfügt selbst nicht über untergeordnete Domänen.

Die Domänentrennung wird etwas anders gehandhabt als die einfache Konfiguration separater Domänen. Beachten Sie, dass Sie die entsprechende Blattdomäne auswählen oder angeben müssen, um in Umgebungen mit Domänentrennung die folgenden Zuordnungsaktionen durchzuführen:

- Beim Erstellen eines für Service wird der für Service der Domäne des Benutzers zugewiesen.
- Beim manuellen Hinzufügen eines CI zu einem für Service können Sie nur CIs auswählen, die zu der Servicedomäne gehören.
- Beim manuellen Hinzufügen von Verbindungen zu CIs zu für Service müssen Benutzer derselben Domäne angehören wie der Anwendungsservice.
- Bei der Übertragung von Servicedefinitionen zwischen Instanzen werden der Domäne des Benutzers importierte Serviceinstanzen und Servicegruppen zugewiesen.

Domain Separation und Empfehlungen für automatisierte Services

Empfehlungen für automatisierte Services unterstützt Domänentrennung. Das bedeutet:

- Quell- und Zielprozess müssen sich in derselben Domäne befinden, um eine Verbindung herzustellen.
- Der Benutzer kann nur die Daten in der aktuellen Domäne anzeigen.

Hinweis: Stellen Sie nach der Installation von Service-Mapping Plus mit Domain Separation-Unterstützung sicher, dass sich alle Inhalte in der entsprechenden Domäne befinden. Eine detaillierte Erklärung der erforderlichen Schritte finden Sie im Artikel Service-Mapping Plus für domänengetrennte Instanzen [KB1303398] in der Now Support Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Empfehlungen für automatisierte Services unterstützt Domain Separation ab Version 1.9.0. Für lokale Instanzen wird derzeit kein Support angeboten. Wenden Sie sich an das Produktmanagement, um weitere Informationen zu erhalten.

Weiteren Kontext finden Sie unter Thema Von ITOM-Transparenz verwendete Erkennungsmuster und Konfiguration des MID Servers für Service-Mapping. Die folgenden Themen enthalten operative Informationen zur Verwendung von Service-Mapping in Bereitstellungen mit Domänentrennung:

- Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren
- Ordnen Sie Anwendungsservices mithilfe von Tags zu zu klassisch Service-Mapping
- Muster erstellen oder anpassen
- Einstiegspunkttypen für Service-Mapping erstellen
- Muster verbessern, ohne ihre Identifizierungsabschnitte zu ändern

Zugehörige Informationen

Domänentrennung

Empfohlene Domain Separation-Verfahren für Service Provider

Neuberechnung des Service-Mappings

Halten Sie Anwendungsservices auf dem neuesten Stand, und verfolgen Sie Änderungen an Services mithilfe der Neuberechnungsfunktion des Anwendungsservice von Service-Mappingnach. Neuberechnungsaufträge berechnen zugeordnete Anwendungsservices neu, wenn Änderungen an einem zugehörigen Configuration Item (CI) in der Configuration Management Database (CMDB) auftreten.

Die häufigsten Änderungen, die eine Neuberechnung verursachen können, sind:

- Topologieänderungen: Die Beziehung des zugeordneten CI zu anderen CIs ändert sich. Diese Änderungen können das Hinzufügen einer neuen Beziehung oder das Entfernen einer vorherigen Beziehung umfassen.
- CI-Changes: Ein Feldwert der CI-Changes.

Diese Änderungen können durch Horizontal-Discovery, Top Down-Discovery, Service Graph Connectors oder manuelle Vorgänge verursacht werden. Wenn sich die CI-Änderung nicht auf die Topologie oder die Servicezuordnungen auswirkt, wird der Neukompositionsprozess ohne Änderungen am Service beendet.

Im Systemzeitplaner sind zwei Arten von Neuberechnungsaufträgen verfügbar: Service-Mapping -Neuberechnung und Service-Mapping -Schnellberechnung. Bei der schnellen Neuberechnung werden Services ausgewählt, die nur CI-Änderungen als Teil des neuesten Batches enthalten und keine Topologieänderungen enthalten.

Neuberechnungsaufträge sind so konfiguriert, dass sie alle fünf Sekunden ausgeführt werden. Nachdem die Aufträge initiiert wurden, beginnen sie mit dem Service, der am längsten gewartet hat. Wenn der Auftrag abgeschlossen ist, kann sich die Auswirkung von Topologieänderungen in der Topologie der Zuordnung oder in den Servicezuordnungen widerspiegeln. Sie können CI-Änderungen anzeigen, indem Sie den Zuordnungsknoten des CI auswählen. Erfolgreiche Neuberechnungen werden als einzelner Prüfpunkt auf der Zeitleiste des Anwendungsservice angezeigt, unabhängig davon, ob es sich um einen Change oder einen Batch von Changes handelt.

Sie können den Neuberechnungstyp, die Häufigkeit und andere Faktoren nach Bedarf konfigurieren. Weitere Informationen zu Service-Mappingfinden Sie im Artikel Service-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mapping-Neuberechnungsaufträge: Konfiguration und Best Practices [KB1001151] in der Knowledge Base von Now Support.

Liste „Verbindungsvorschlagen“

Überprüfen Sie die Details der Verbindungsvorschläge, um zu entscheiden, welche Verbindungen für Anwendungsservices relevant sind.

Spalten der Liste „Verbindungsvorschlagen“

Spalte	Beschreibung
Von	Die CI-Klasse oder der Fingerabdruckprozess des CI, das die Verbindungsquelle ist. Dieses Feld wird nur angezeigt, wenn Sie auf Verbindungsvorschläge zugreifen, indem Sie zu navigieren **Service-Mapping** > **Administration** > **Verbindungsvorschläge**.
An	Die CI-Klasse oder der Fingerabdruckprozess des CI, das das Verbindungsziel ist
Zielhost	Der Host des CI, das das Verbindungsziel ist Wenn in der Spalte **VIP** der Wert **true** angezeigt wird, ist der Zielhost Mitglied eines Lastenausgleichsmoduls. Wenn Sie einen solchen Zielhost auswählen, fügt das System das Lastenausgleichsmodul und alle zugehörigen Mitglieder als CIs im Anwendungsservice hinzu.
IP	Die IP-Adresse des CI, das das Verbindungsziel ist
Port	Der Port des CI, das das Verbindungsziel ist
Vertrauen	Das Konfidenzniveau gibt die Wahrscheinlichkeit an, dass diese Verbindung Teil der Serviceinstanzen ist. • **Hoch** – Es handelt sich wahrscheinlich um eine Verbindung zu einer internen Komponente, die nur von dieser Komponente oder Anwendung verwendet wird. • **Mittel** – Es handelt sich wahrscheinlich um eine Verbindung zu einer Middleware-Komponente, die von mehreren Services verwendet wird, z. B. IBM MQ oder Oracle WebLogic Server. • **Niedrig** – Es handelt sich wahrscheinlich um eine Verbindung zu einer Anwendung, die auf zahlreichen Servern im Unternehmen bereitgestellt wird, normalerweise zu Überwachungszwecken. Zum Beispiel Tivoli Enterprise Monitoring Agents oder MID-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalten der Liste „Verbindungsvorschlagen“ (Fortsetzung)

Spalte	Beschreibung
	• **Sehr niedrig** – Es handelt sich wahrscheinlich um eine Verbindung zu einer zentralen Anwendung, die von der gesamten Organisation verwendet wird, z. B. Microsoft Active Directory oder Okta. Wenn das Konfidenzniveau als **N/V** angezeigt wird, warten Sie, bis das Training der Anwendungsfingerabdrücke abgeschlossen ist. Siehe Statusbericht des Trainings der Anwendungsfingerabdrücke. Das Konfidenzniveau ist nur verfügbar, wenn die auf Fingerabdrücken basierte Erkennung aktiviert ist.
Entscheidung	Der Wert, der die vorherige Aktion für diesen Verbindungsvorschlag angibt: • **Manuell hinzugefügt** – Sie haben eine Verbindung auf Grundlage dieses Vorschlags hinzugefügt. • **Manuell ausgeschlossen** – Sie haben eine Verbindung auf Grundlage dieses Vorschlags entfernt. • **Unentschieden** – Sie haben die vorherige Entscheidung zum Hinzufügen oder Entfernen einer Verbindung basierend auf diesem Vorschlag zurückgesetzt. • **Durch Regel hinzugefügt** − Service-Mapping hat eine Verbindung auf Grundlage einer Verbindungsregel hinzugefügt.
Regel	Die Regel, die von Service-Mapping zum Hinzufügen einer Verbindung angewendet wurde.
VIP	Der Zielhost ist Mitglied eines Lastenausgleichsmoduls. Das System zeigt diese Informationen nur für Lastenausgleichsmodule an, die Sie zuvor mithilfe der horizontalen Erkennung erkannt haben. Dieses Feld wird nur angezeigt, wenn Sie auf Verbindungsvorschläge zugreifen, indem Sie zu navigieren **Service-Mapping** > **Administration** > **Verbindungsvorschläge**.
Entscheidung geändert von	Der Benutzer, der die Entscheidung zuletzt geändert hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalten der Liste „Verbindungsvorschlagen“ (Fortsetzung)

Spalte	Beschreibung
	Wenn die Entscheidung durch eine Regel geändert wurde, zeigt dieses Feld den MID-Server-Anwender an. Dieses Feld wird nur angezeigt, wenn Sie auf Verbindungsvorschläge zugreifen, indem Sie zu navigieren **Service-Mapping** > **Administration** > **Verbindungsvorschläge**.
Aktualisiert	Der Zeitstempel der letzten Änderung dieser Verbindung

Zugehörige Informationen

- Erkennung auf Basis von Predictive Intelligence
- CIs für einzelne Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen
- CIs für mehrere Anwendungsservices mithilfe von Verbindungsvorschlägen hinzufügen oder entfernen

Einstiegspunktattribute

Service-Mapping bietet eine Vielzahl vorkonfigurierter Einstiegspunkttypen, die viele häufig verwendete Anwendungen abdecken. Überprüfen Sie die Attributdefinitionen, damit die Einstiegspunkte Ihren Anwendungsservices korrekt hinzugefügt werden.

Ein Einstiegspunkt ist ein Punkt, auf den Clients auf eine Serviceinstanz zugreifen. Einstiegspunkte werden als Datensätze in den Endpunkttabellen [cmdb_ci_endpoint] gespeichert.

Es gibt einige allgemeine Attribute, die von fast allen Einstiegspunkttypen gemeinsam verwendet werden, wie in der folgenden Tabelle beschrieben:

Allgemeine Attribute

Attribut	Beschreibung
Host/Hostname/Host Name	Der Wert des Zielservers, auf dem der Dienst ausgeführt wird. Dieser Wert kann einen echten Hostnamen, einen Aliasnamen, eine IP-Adresse oder eine VIP-Adresse enthalten. **Wichtig:** Verwenden Sie für die Discovery und Zuordnung keine localhost- oder loopback-Adresse (127.0.0.1).
Port	Die Portnummer des Dienstes, den Sie ermitteln möchten.
Name	Der Name des Dienstes, den Sie entdecken möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Attribute (Fortsetzung)

Attribut	Beschreibung
URL	Die URL des Service, den Sie erkennen möchten, im folgenden Format: http(s):// (Adresse):(Port). Wenn Sie den Port nicht angeben, verwendet das System den Standardport 443.
Netzwerkstandort	Standort des entsprechenden Subnetzwerks. **Hinweis:** Dieses Feld ist optional und nur sichtbar, wenn der Netzwerkstandort aktiviert ist.

Informationen zum Konfigurieren von Einstiegspunkten für Subnetze finden Sie unter Optimieren Sie Service-Mapping mit MID-Affinität und Wiederverwendung von IPs.

Es gibt einige Attribute, die Sie je nach Einstiegspunkt unterschiedlich konfigurieren, wie in der folgenden Tabelle beschrieben:

Einstiegspunktattribute, die für einige Einstiegspunkte spezifisch sind

Einstiegspunkttyp	Attribut	Beschreibung
Active Directory-Domäne zu Domänencontroller-Endpunkt	Domänenname	Der AD-Domänenname
	Forest-Name	Der Name des Active Directory Forest (AD Forest)
	Domänencontroller – Distinguished Name	Der Distinguished Name des AD-Domänencontrollers. Normalerweise handelt es sich um eine Kompilierung des Domänencontroller- und des Hostnamens.
	Domänencontroller-Name	Der Name des AD-Domänencontrollers
Active Directory-Gesamtstruktur – Endpunkt	Forest-Name	Der Name des Active Directory Forest (AD Forest)
AWS-Ressourcenamensendpunkt	ARN	Der Name der Amazon-Ressource
Anwendung zu Speicherendpunkt	Durch Applikation verwendete Datei	Der Pfad zu der von einer Anwendung verwendeten Datei Beispiel: mssql verwendet c:\applications\mssql\users.db. Service-Mapping füllt dieses Attribut anhand von Mustern auf.
	Dateisystemname	Das Dateisystem, das die von einer Anwendung verwendete Datei enthält. Wenn mssql beispielsweise c:\applications\mssql\users.db verwendet, ist der Wert „c:“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstiegspunktattribute, die für einige Einstiegspunkte spezifisch sind (Fortsetzung)

Einstiegspunkttyp	Attribut	Beschreibung
	Angeschlossene Array-IDs	N/V
Erweiterte Warteschlange	Schema	Der Name der Oracle DB-Tabelle, in der die Warteschlange definiert ist
	Instanz	Der Name der Oracle-Instanz
	Warteschlange	Der Name der Warteschlange
BizTalk-Verbindung	Adapteradresse	Die Verbindungszeichenfolge für den Biztalk-Adapter. Dies kann ein Pfad, eine URL, ein Host oder ein Port sein.
	Transporttyp	Der Typ des Biztalk-Adapters. Beispielsweise eine URL, Datei-SOAP oder FTP.
CRM-Komponente	Rolle	Die Rolle des CRM. Lassen Sie das Feld leer, wenn diese unbekannt ist.
DB2 UDB	Instanz	Der Name der DB2-Instanz
DCTM-Verbindung zu Broker	Repository	Der Name des Dokumentations-Repository
DCTM-Index-Agent-Verbindung	Instanzname	Der Name der Instanz des Dokumentationsindex-Agent
	Repository	Der Name des Dokumentations-Repository
DCTM-Jobprozessor	Repository	Der Name des Dokumentations-Repository
Citrix Delivery Controller	Farm-Typ	Der Typ des Delivery-Controllers
	Controller-Name	Der Name des Citrix-Controllers
DocBase-Verbindung	Repository	Der Name des Dokumentations-Repository
EJB	JNDI-Name	Der jndi-Name der Ziel-EJB
EMS	Warteschlange	Name der Tibco EMS-Warteschlange
EMS JNDI	JNDI-Name	Der jndi-Name der Tibco EMS-Verbindung
F5-Spiegel	Ursprüngliche IP	Die IP-Adresse des zweiten F5-Gerätepaars
	Ursprünglicher Host	Der Hostname des zweiten F5-Gerätepaars
Schnellsuche	Repository	Der Name des Repository für die schnelle Suche
ITAM Asset Center	Ordner	Der Pfad zum Konfigurationsordner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstiegspunktattribute, die für einige Einstiegspunkte spezifisch sind (Fortsetzung)

Einstiegspunkttyp	Attribut	Beschreibung
JMS-Fluss	JMS-Projekt	Der Name des Tibco-Projekts
JMS-Fluss	Abfragename	Name der Tibco EMS-Warteschlange
JMS-Server	Abfragename	Der Name der auf dem JMS-Server definierten Warteschlange
HTTP-Listener für WMB-Abhängigkeit	Verzeichnis	Der Pfad zum WMB-Installationsverzeichnis
LDAP	Protokoll	Der Protokollname: `ldap`
	Typ	Der LDAP-Abfragetyp. Dieses Attribut wird nicht unterstützt. Leer lassen.
MQ	Abfragename	Der Name der IBM MQ-Warteschlange.
MQ-Fluss	Quelle-IP	Die IP der Quell-IP, die eine Verbindung mit MQ herstellt
	Abfragename	Der Name der IBM MQ-Warteschlange.
MQ Cross-memory	Befehlszeile	Die Befehlszeile von MQ
	Abfragename	Der Name der IBM MQ-Warteschlange.
MSMQ Flow	Abfragename	Der Name der MS MQ-Warteschlange.
MS SQL-Server	Instanz	Der Name der MSSQL-Instanz
MySQL Cluster-Datenknoten	Knoten-ID	Die ID der MySQL-Instanz
	Knotengruppe	Die Gruppe der MySQL-Instanz
MySQL Cluster-MGM	Knoten-ID	Die ID der MySQL-Instanz
Sekundärer MySQL-Server	Konfig.-IP	Die IP des MySQL-Konfigurationsservers
	Konfig.-Port	Der Port des MySQL-Konfigurationsservers
Oracle-DB	Schema	Der Name der Tabelle auf der Oracle-Instanz
	Instanz	Der Name der Oracle-Instanz
Oracle ESB-Verbindung	Adapterdaten	Der Inhalt des Adapters
	Adaptertyp	Der Typ des Adapters
Oracle RAC-DB	Servicename	Der Name des Oracle RAC-Services
PostgreSQL-DB	Instanz	Der Name der PostgreSQL-Datenbank
Remote-TCP Cross-Speicher	Source_ IP	Die IP des Quellhostprozesses

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstiegspunktattribute, die für einige Einstiegspunkte spezifisch sind (Fortsetzung)

Einstiegspunkttyp	Attribut	Beschreibung
	Quell-Port	Der Port des Quellprozesses
SAP APP-EP	SID	Der SID-Name der SAP-Instanz
	Instanz	Der Name der Instanz.
SAP BO-Server	Servername	Der Name des BO-Servers
Sharepoint-Verbindung	Ursprungs-URL	Die URL des IIS
SSAS	Projekt	Der Name des SSAS-Projekts (kann leer sein)
SSAS für MSSQL	Instanz	Der Name der MSSQL-Instanz
	Clienttyp	Der Typ des verbundenen Clients
SSIS	Auftrag	Der Name des SSIS-Auftrags kann leer sein.
SSIS-Datei	Paketdateiname	Der Name der Paketdatei
SSIS für MSSQL	Instanz	Der Name der MSSQL-Instanz
	Clienttyp	Der Typ des verbundenen Clients
StoreParameters-Komponenten	Front	Die Parameter der Citrix-Anwendung
	Farm	Der Farm-Host für die Citrix-Anwendung
	Anwendungsname	Der Name der Citrix-Anwendung
XenApp- oder Präsentationsserver	Typ	Der Type der Citrix-Anwendung
	Farm	Der Farm-Host für die Citrix-Anwendung
	Symbol-Pfad	Der logische Pfad der Citrix-Anwendung
	Argument	Die Parameter der Citrix-Anwendung
	Pfad	Der logische Pfad der Citrix-Anwendung
	Ausführung	Der EXE-Name der Citrix-Anwendung
	IP-Adresse	Die IP des Hosts gehört zur Citrix-Farm.
Sybase	Instanz	Der Name der Sybase-Instanz
Tibco Konf.-Datei	Konfigurationsdatei	Der Pfad zum Tibco BW-Projekt
	Prozessname	Der Name des Tibco BW-Hauptprozesses
	Warteschlangenport	Der Port der vom Tibco-Prozess verwendeten Warteschlange

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstiegspunktattribute, die für einige Einstiegspunkte spezifisch sind (Fortsetzung)

Einstiegspunkttyp	Attribut	Beschreibung
	Konfig.-IP	Die IP der Quelle der Warteschlange
Tibco BW	Prozessname	Der Name des Tibco BW-Hauptprozesses
TIBCO Datei-Listener	Datei	Der Pfad der Datei wird von Tibco BW für die Integration verwendet.
TIBCO Hawk	Konfigurationsverzeichnis	Der Pfad zum Tibco Hawk-Konfigurationsordner
WMB-Abhängigkeit	Befehlszeile	Die Befehlszeile von WMB
XenApp- oder Presentation Server-Komponenten	Farm	Der Farm-Host für die Citrix-Anwendung
	Symbol-Pfad	Der logische Pfad der Citrix-Anwendung

Zugehörige Informationen

Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping

Einstiegspunkttypen für Service-Mapping erstellen

MID-Server-Eigenschaften, die von Service-Mapping verwendet werden

Service-Mapping verwendet die MID-Server-Parameter während der Erkennung und Zuordnung. Ändern Sie keine Standardwerte für diese Parameter, es sei denn, Sie beheben Probleme im Erkennungsprozess.

Allgemeine Eigenschaften

Eigenschaft	Beschreibung
mid.file_tracking.file_path_forbidden_strings	Kommagetrennte Liste von Zeichenfolgen, nach denen in nachverfolgten Dateipfaden gesucht werden soll. Sobald eine Zeichenfolge in dieser Liste in einem nachverfolgten Dateipfad gefunden wurde, wird die Datei aus der weiteren Verarbeitung entfernt. • **Standardwert**: mit Status ERROR abgeschlossener Auftrag • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SSH-bezogene Eigenschaften

Eigenschaft	Beschreibung
mid.sa.ssh.path	Verzeichnis im Zielsystem, in dem MID-Server nach auszuführenden Befehlen sucht. • **Standardwert**: /usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.truncate_last_line_regex	Regulärer Ausdruck einer Zeile, den MID-Server am Ende der SSH-Befehlsantwort entfernt. • **Standardwert**: Command.*performed by.* • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.remove_first_line_regex	Regulärer Ausdruck einer Zeile, den MID-Server am Anfang jeder SSH-Befehlsantwort entfernt. • **Standardwert**: [leere Zeichenfolge] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.privileged_command_message	Eingabeaufforderung, die MID-Server mit Befehlen mit Rechten auf Sudo-Ebene sendet. Beispiel: Ein Befehl auf Sudo-Ebene wird mit „Password:“ gesendet. • **Standardwert**: [leere Zeichenfolge] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
mid.sa.ssh.restricted_shell_regex	Regulärer Ausdruckstext, der beim Öffnen der Nachricht einer eingeschränkten Shell enthalten ist. Mit einer eingeschränkten Shell führt der SSH-Provider während der Sitzungsinitialisierung einige Befehle nicht aus. • **Standardwert**: eingeschränkte Shell • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.terminal_cols	Anzahl der Spalten in den Terminalfenstern, die mit der SSH-Sitzung geöffnet werden. • **Standardwert**: 300 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.terminal_rows	Anzahl der Zeilen in den Terminalfenstern, die mit der SSH-Sitzung geöffnet werden. • **Standardwert**: 800 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.time_between_change_shell_and_prompt	Wartezeit zwischen dem Ändern einer Shell während der Initialisierung und dem Zeitpunkt, zu dem die Shell-Eingabeaufforderung angezeigt wird (in Millisekunden). • **Standardwert**: 1.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
mid.sa.ssh.connect_timeout	Zeitüberschreitung für die anfängliche SSH-Verbindung (in Millisekunden). • **Standardwert**: 2.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.max_chars_single_response	Maximale Anzahl von Zeichen, die in einer einzelnen SSH-Befehlsantwort zulässig sind. • **Standardwert**: 1.0000.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.break_session_chars	ASCII-Wert des Zeichens, das zum Unterbrechen einer Sitzung verwendet wird. • **Standardwert**: 7 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.no_change_shell_regex	Regulärer Textausdruck in der Befehlsantwort nach dem Senden von „su“, um zum Superuser zu wechseln. Wenn der reguläre Ausdruck übereinstimmt, ändert MID-Server die Shell nicht. • **Standardwert**: pfsh • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.permission_denied_regex	Regulärer Ausdruck von Befehlsantworten, die der MID-Server als Zugriffsproblem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	erkennt und eine entsprechende Meldung generiert. • **Standardwert**: Berechtigung verweigert • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.more_line_command_regex	Wenn die SSH-Antwort die Terminalgröße überschreitet, sendet das System die Zeile „more“, die dem regulären Ausdruck entspricht. Wenn der MID Server die Zeile „more“ erkennt, sendet er das Leerzeichen. Dies ist relevant für proprietäre Systeme, die eine nicht standardmäßige Eingabeaufforderung „more“ senden. • **Standardwert**: [leer] • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.become_superuser_command	Ein SSH-Befehl zur Umwandlung in einen Superuser. • **Standardwert**: su • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.prompt_changing_command_regex	SSH-Befehle, die die Shell-Eingabeaufforderung ändern. Wenn der vom MID Server gesendete Befehl mit dem regulären Ausdruck übereinstimmt, erwartet der MID Server eine Änderung der Eingabeaufforderung des Servers. • **Standardwert**: changeto\\s+[^\\s]+ • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.ignore_errors_on_commands_regex	Regulärer Ausdruck für den Befehl, für den der MID Server Berechtigungsfehler ignoriert. • **Standardwert**: stat.* | istat.* | perl.* • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.prompt_last_char_regex	Regulärer Ausdruck des letzten Zeichens in der Standardaufforderung des Servers. • **Standardwert**: [$#>\\]\\:] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.timeout	Zeitüberschreitung des SSH-Befehls (in Millisekunden). • **Standardwert**: 60.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.port	SSH-Portnummer. Um mehr als einen Port hinzuzufügen, trennen Sie Portnummern durch Kommata. Beispiel: 22,33,44. • **Standardwert**: 22 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
mid.sa.ssh.connect.retry	Anzahl der SSH-Verbindungswiederholungen. • **Standardwert**: 1 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.additional_setup	Befehl, den MID-Server sendet, nachdem die SSH-Sitzung erstellt wurde. • **Standardwert**: [leer] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.expect_after_su	Regulärer Ausdruck des letzten Zeichens in der Aufforderung nach dem Senden von „su“. • **Standardwert**: [:$#>\\]] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.privileged_command_last_char	Zeichen, das das letzte erwartete Zeichen in der Zeichenfolge eines Befehlsergebnisses angibt. Sobald dieses Zeichen im Ergebnis erkannt wird, wartet der MID Server nicht auf weitere Ausgaben. • **Standardwert**: [leer] • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.prompt	Zeichenfolge, die die nicht standardmäßige SSH-Eingabeaufforderung darstellt. Der MID-Server verwendet diese Zeichenfolge beim

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Analysieren von Ergebnissen von SSH-CLI-Befehlen. • **Standardwert**: SERVNOW> • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.proprietary_system_trial_count	Anzahl der zusätzlichen Wartezeiten auf proprietären Nicht-UNIX/Linux-Systemen. Der MID-Server wartet nach der anfänglichen Wartezeit von 5 Sekunden auf eine Antwort. Nach den ersten 5 Sekunden wartet der MID Server so oft auf die Antwort, wie durch diesen Parameter definiert. Die zusätzliche Wartezeit beginnt mit 1 Sekunde und erhöht sich bei jeder Iteration um 1 Sekunde. • **Standardwert**: 10 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.restart_after_unstopped_threads	Anzahl der zulässigen nicht angehaltenen Threads, bevor MID-Server neu gestartet wird, wenn versucht wird, die SSH-Sitzung zu schließen. • **Standardwert**: 50 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.stty_command	stty-Befehl zum Konfigurieren der entsprechenden Einstellungen. Der MID-Server führt diesen Befehl aus, wenn das SSH-Terminal initialisiert wird. • **Standardwert**: [leer] • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.inocrrect_password_regex	Erwartete Zeichenfolge, die das SSH-Terminal zurückgibt, wenn der MID-Server während beim Anmeldeprozess ein falsches Passwort verwendet. • **Standardwert**: Sorry, try again | incorrect password attempt • **Typ**: • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.max_unstopped_threads	Identisch mit Parameter mid.sa.ssh.restart_after_unstopped_threads. • **Standardwert**: 50 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.ssh.idle_after_sudo	Zeitraum (in Millisekunden), den der MID-Server nach dem Senden eines sudo-Befehls wartet, ohne Aktivität in der Zeile zu erwarten. • **Standardwert**: 3000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.

WMI-bezogene Eigenschaften

Wichtig: Ab New York Patch 10 und höher wird WMI Collector nicht mehr unterstützt. Weitere Informationen finden Sie unter KB0791835 WMI Collector deprecation details (Details zur Einstellung der Unterstützung von WMI Collector).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften	Beschreibung
mid.servicewatch.wmi.host	Host/IP des Servers, auf dem ServiceNow WMI Collector ausgeführt wird. • **Standardwert**: localhost • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist unter bestimmten MID-Server Parametern verfügbar, wie unter MID-Server-Parameter hinzufügen beschrieben.
mid.servicewatch.wmi.port	Port, an dem der ServiceNow WMI Collector-Service auf Anforderungen des MID Servers lauscht. • **Standardwert**: 8585 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist unter bestimmten MID-Server Parametern verfügbar, wie unter MID-Server-Parameter hinzufügen beschrieben.
mid.sa.wmi.timeout	Zeitüberschreitung bei Befehlsausführung in Millisekunden. Diese Eigenschaft steuert auch die PowerShell-Befehle. • **Standardwert**: 60.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist unter bestimmten MID-Server Parametern verfügbar, wie unter MID-Server-Parameter hinzufügen beschrieben.
mid.sa.wmi.max_bytes_in_response	Maximale Anzahl von Zeichen, die in einer Antwort zulässig sind. • **Standardwert**: 20.971.520 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.servicewatch.wmi.get_file_on_shared_drive_from_collector	Der MID-Server versucht, auf die angeforderte Datei auf einem freigegebenen Laufwerk direkt vom MID-Server aus zuzugreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften	Beschreibung
	• **Standardwert**: true • **Typ**: true/false • **Speicherort:** Diese Eigenschaft ist unter bestimmten MID-Server Parametern verfügbar, wie unter MID-Server-Parameter hinzufügen beschrieben.
mid.sa.wmi.access_denied_regex	Regulärer Ausdruck von Fehlermeldungen, die vom Server zurückgegeben werden und die der MID Server als Zugriffsproblem betrachtet und es daher mit anderen Anmeldeinformationen versucht. • **Standardwert**: Access is denied | Access denied | service installation failed | User credentials cannot be used for local connections | System error 1312 | generic failure | Insufficient privilege | user rights | HRESULT: 0x800706BA • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.wmi.send_retry_count	Anzahl der Kommunikationsversuche mit dem ServiceNow WMI Collector-Service für jede Anforderung. • **Standardwert**: 1 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.servicewatch.wmi.mui	Der MID-Server unterstützt die MUI-Konfiguration (Multilingual UI). • **Standardwert**: false • **Typ**: true/false • **Speicherort:** Diese Eigenschaft ist unter bestimmten MID-Server Parametern verfügbar, wie unter MID-Server-Parameter hinzufügen beschrieben.
mid.powershell_api.winrm.remote_port	Legen Sie den Port fest, den WinRM für die Verbindung zu Remotehosts verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften	Beschreibung
	• **Standardwert**: 5985 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist unter bestimmten MID-Server Parametern verfügbar, wie unter MID-Server-Parameter hinzufügen beschrieben.
mid.windows.management_protocol	Verwaltungsprotokoll, das der MID Server für die Verbindung mit Windows-Servern verwendet. Zulässige Werte sind WMI und WinRM. • **Standardwert**: WMI • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist unter bestimmten MID-Server Parametern verfügbar, wie unter MID-Server-Parameter hinzufügen beschrieben.
mid.servicewatch.wmi.protocol	Kommunikationsprotokoll zwischen MID-Server und WMI Collector. Erlaubte Werte: http/https. • **Standardwert**: http • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist unter bestimmten MID-Server Parametern verfügbar, wie unter MID-Server-Parameter hinzufügen beschrieben.
mid.use_powershell	Ermöglicht die Verwendung von PowerShell zum Ausführen von Befehlen auf Windows-Servern. • **Standardwert**: false • **Typ**: true/false • **Speicherort:** Diese Eigenschaft ist unter bestimmten MID-Server Parametern verfügbar, wie unter MID-Server-Parameter hinzufügen beschrieben.
mid.sa.prefer_powershell	Macht PowerShell zur bevorzugten Methode zum Ausführen von Befehlen auf Windows-Servern. **Hinweis:** Wenn Sie diesen Parameter auf „true“ setzen, müssen Sie auch den Parameter mid.sa.use_powershell auf „true“ festlegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften	Beschreibung
	• **Standardwert**: false • **Typ**: true/false • **Standort: MID-Server** > **Eigenschaften**
mid.win.baseboard.or.bios.insertion	Bewirkt, dass das Muster *Windows OS – Servers* anstelle der Baseboard-Seriennummer die BIOS-Seriennummer erkennt. • **Mögliche Werte**: false – zum Ausfüllen der BaseBoard-Nummer; true – zum Ausfüllen der BIOS-Seriennummer. • **Typ**: true/false • **Standardwert**: false • **Standort: MID-Server** > **Eigenschaften**

SNMP-bezogene Eigenschaften

Eigenschaft	Beschreibung
mid.snmp.request.timeout	Zeit (in Millisekunden), die der MID Server auf eine Antwort für jede OID-Anforderung wartet. • **Standardwert**: 1.500 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.snmp.port	SNMP-Port. • **Standardwert**: 161 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.snmp.retry	Anzahl der SNMP-Wiederholungen. • **Standardwert**: 1 • **Typ**: Ganzzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.snmp.table_size_limit	Maximale Tabellengröße, die in die SNMP-Tabellenanforderungen aufgenommen werden soll. • **Standardwert**: 20.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.snmp.table_walk_limit	Maximale Anzahl von Anforderungen in der SNMP-Walk-Sitzung. • **Standardwert**: 10.000 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.snmp.get_table_timeout_sec	Maximale Zeit (in Sekunden), die für das Laden einer gesamten SNMP-Tabelle zulässig ist. • **Standardwert**: 600 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.snmp.walk_timeout_sec	Maximale Zeit (in Sekunden), die für die SNMP-Walk-Sitzung zulässig ist. • **Standardwert**: 600 • **Typ**: Ganzzahl • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.snmp.discover_engine	Autorisierende Discovery Engine-ID in SNMP V3-Sitzungen. • **Standardwert**: true • **Typ**: true/false • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.snmp.snmp_v2_disabled	Verwendung von SNMP Version 2 deaktivieren • **Standardwert**: false • **Typ**: true/false • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.
mid.sa.snmp.failed_status_oid	OID, die den Status „Fehlgeschlagen“ angibt. Wenn ein SNMP-Ergebnis mit dieser OID beginnt, betrachtet der MID-Server es als Fehler. • **Standardwert**: 1.3.6.1.6.3.15.1.1.3 • **Typ**: Zeichenfolge • **Speicherort:** Diese Eigenschaft ist im Basissystem nicht verfügbar. Sie können die Eigenschaft wie unter MID-Server-Eigenschaft erstellen beschrieben hinzufügen.

Vorkonfigurierte CI-Beziehungen in der tagbasierten Discovery

An der Tag-basierten Discovery sind standardmäßig mehrere vorkonfigurierte CI-Beziehungen beteiligt. In der Tabelle „Durchlaufregeln für Anwendungsservices“ [svc_traversal_rules] werden diese Beziehungen gespeichert.

Wichtig: Vorkonfigurierte CI-Beziehungen, die für die Tag-basierte Discovery verwendet werden, können Sie in der Tabelle „Durchlaufregeln für Anwendungsservices“ [svc_traversal_rules] nicht löschen oder ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorkonfigurierte CI-Beziehungen, die standardmäßig bei der Tag-basierten Erkennung berücksichtigt werden

CI	Beziehung	CI
VM-Instanz [cmdb_ci_vm_instance]	Virtualisiert::Virtualisiert von	Hardware [cmdb_ci_hardware]
Hardware [cmdb_ci_hardware]	Wird ausgeführt:Wird ausgeführt auf	Anwendung [cmdb_ci_appl]
Kubernetes-Pod [cmdb_ci_kubernetes_pod]	Enthält::Enthalten in	Virtualisierungscontainer auf Betriebssystemebene [cmdb_ci_oslv_container]

Zusätzliche vorkonfigurierte CI-Beziehungen für die tagbasierte Erkennung

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Kubernetes-Service [cmdb_ci_kubernetes_service]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
OpenShift-Projekt [cmdb_ci_openshift_project]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes-Pod [cmdb_ci_kubernetes_pod]	Enthalten in::Enthält	Kubernetes-Cluster [cmdb_ci_kubernetes_cluster]
Kubernetes-Pod [cmdb_ci_kubernetes_pod]	Cluster::Cluster von	Kubernetes-Service [cmdb_ci_kubernetes_service]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	Bereitgestellte OpenShift-Konfiguration [cmdb_ci_openshift_dep_conf]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Buildkonfiguration [cmdb_ci_openshift_build_conf]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Route [cmdb_ci_openshift_route]
Kubernetes-Namespace [cmdb_ci_kubernetes_namespace]	Enthält::Enthalten in	OpenShift-Image-Stream [cmdb_ci_openshift_images_stream]

Eigenschaften im Zusammenhang mit der Tag-basierten Discovery

Das Plugin „Service Mapping“ enthält mehrere Eigenschaften, die sich speziell auf die Tag-basierte Discovery beziehen.

Hinweis: Um die Tabelle „Systemeigenschaft“ [sys_properties] zu öffnen, geben Sie im Navigationsfilter `sys_properties.list`ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
svc_by_tags.classes.whitelist	Diese Eigenschaft enthält die Liste der zulässigen CI-Klassen, getrennt durch Kommas. Die Tag-basierte Zuordnung schließt die CIs ein, die zu diesen Klassen gehören. Ein leeres Feld „Wert“ gibt an, dass alle CI-Klassen einbezogen werden.
svc_by_tags.install_status.blacklist	Diese Eigenschaft enthält die Liste der Ausschlüsse basierend auf dem Installationsstatus, getrennt durch Kommas. Die tagbasierte Zuordnung schließt CIs mit Tags mit den folgenden Installationsstatus aus: **Hinweis:** In diesem Kontext werden von Durchlaufregeln übermittelte CIs nicht als getaggt betrachtet. Diese Eigenschaft gilt nur für ursprüngliche CIs mit Tags. **Standardwert**: 7.100 **Andere mögliche Werte**: Installiert = 1, Bestellt = 2, In Wartung = 3, Ausstehende Installation = 4, Ausstehende Reparatur = 5, Auf Lager = 6, Deaktiviert = 7, Gestohlen = 8
svc_by_tags.max.categories.per.family	Legen Sie die maximale Anzahl der pro Servicefamilie zulässigen Kategorien fest. • **Typ**: Ganzzahl • **Standardwert**: 3
svc_by_tags.max.traversal.rules.active	Legen Sie die maximal zulässige Anzahl von CI-Beziehungen fest, die sich im aktiven Status befinden können. Service-Mapping verwendet für die Tag-basierte Erkennung nur aktive CI-Beziehungen. • **Typ**: Ganzzahl • **Standardwert**: 5 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
svc_by_tags.max_ci_limit	Legen Sie die maximal zulässige Anzahl von CIs fest, die ein auf Tags basierender Anwendungsservice enthalten kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Ganzzahl • **Standardwert**: 1.000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]

Durchlaufregeln für Anwendungsservices-Formularabschluss

Füllen Sie das Formular „Durchlaufregeln für Anwendungsservices“ aus, um während der tagbasierten Discovery eine vorhandene CI-Beziehung zu bearbeiten oder eine neue CI-Beziehung hinzuzufügen.

Feld	Beschreibung
Regeldefinition	Wählen Sie eine vorkonfigurierte CI-Beziehung aus. Erstellen Sie alternativ eine neue CI-Beziehung: **1.** Klicken Sie auf **Neu**. **2.** Wählen Sie die CI-Klasse aus der Liste **Übergeordneter Typ** aus. **3.** Wählen Sie den Beziehungstyp aus der Liste **Beziehungstyp** aus. **4.** Wählen Sie die CI-Klasse aus der Liste **Untergeordneter Typ** aus. **5.** Klicken Sie auf **Absenden**. Die neue CI-Beziehung wird der Tabelle „Regeldefinitionen für CI-Beziehungstyp“ [cmdb_rel_type_rule_definitions_list] hinzugefügt. Um beispielsweise Linux-Server zu erkennen, die Speichergeräte hosten, wählen Sie die folgenden Werte aus: • Übergeordneter Typ: Linux Server [cmdb_ci_linux_server] • Beziehungstyp: Enthält::Enthalten in • Untergeordneter Typ: Speichergerät [cmdb_ci_storage_device]
Ist umgekehrt	Aktivieren Sie dieses Kontrollkästchen in den folgenden Fällen: • Wenn das getaggte CI in der Beziehung ein CI der untergeordneten CI-Klasse ist. • Wenn das CI, das bereits Teil des Service in der Beziehung ist, ein CI der untergeordneten CI-Klasse ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Verwendet von	Wählen Sie nur **Service nach Tags**aus. **Hinweis:** Wählen Sie nicht **Neuberechnung des Service**aus. Dies verhindert das Bearbeiten vorhandener CI-Beziehungen oder das Hinzufügen neuer Beziehungen und erzeugt eine Fehlermeldung.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um diese CI-Beziehung in der Tag-basierten Erkennung zu verwenden. Deaktivieren Sie dieses Kontrollkästchen alternativ, um diese CI-Beziehung von der Tag-basierten Erkennung auszuschließen. **Hinweis:** Standardmäßig sind an der Tag-basierten Erkennung nur fünf CI-Beziehungen beteiligt. Um die maximale Anzahl aktiver CI-Beziehungen zu ändern, bearbeiten Sie den Wert für die Eigenschaft svc_by_tags.max.traversal.rules.active in der Tabelle „Systemeigenschaften“ [sys_properties].
Reihenfolge	Geben Sie eine Zahl für die Reihenfolge ein. Das System verwendet CI-Beziehungen zur Erkennung in aufsteigender Reihenfolge..

Tastaturkürzel zur Benutzung von Service-Mapping im Eingabehilfemodus

Im Eingabehilfemodus können Sie über eine Tastatur auf alle für Servicezuordnungen und Serviceformulare zugreifen.

Wenn die gesamte Zuordnung ausgewählt ist, enthält die Informationsnachricht oben im Fenster Anleitungen zur Navigation innerhalb der Zuordnung.

Aktion	Tastaturkürzel
Kontextmenüs aufrufen	Platz
Cluster erweitern	Geben Sie Folgendes ein:
Aus dem Bereich **Eigenschaften** in den Zuordnungsbereich wechseln	Escape-Taste
Im Menü „Weitere Optionen“ Optionen ein- und ausblenden	Platz
CIs und Verbindungen in der Zuordnung auswählen	Pfeiltaste
In der Zeitleiste können Sie die Zeit im aktuell ausgewählten Zeitraum bearbeiten.	Zahlen (1-9)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Tastaturkürzel
Im Fenster der für Servicezuordnung durch UI-Elemente navigieren	Registerkarte

Beispieldefinitionen für Servicefamilien in Tag-basierter Zuordnung

Erstellen Sie bei der Vorbereitung der Zuordnung von Anwendungsservices basierend auf Tags Tag-Kategorien, die Tags mit ähnlicher Verwendung enthalten. Definieren Sie eine Tag-basierte Servicefamilie und die Tags, die Sie für die Zuordnung verwenden möchten. Zusätzlich zu Tag-Kategorien können Sie auch Tag-Werte definieren, um die Kriterien für die von Service-Mappingerstellten Servicekandidaten einzugrenzen. Verwenden Sie diese Beispiele als Leitfaden.

Ausführliche Informationen zum Definieren von Servicefamilien in Tag-basierter Zuordnung finden Sie unter Zuordnung von Anwendungsservices basierend auf Tags vorbereiten.

Beispiele für die Definition von Tag-basierten Zuordnungskriterien für Servicefamilien

Definitionen der Servicefamilie	Kategorie	Schlüssel	Wert (optional)	Ergebnis
Beispiel 1: eine Tag-Kategorie, keine Werte	Umgebung	ENV	Nicht definiert	Service-Mapping erstellt für den ENV-Schlüssel einen Servicekandidaten für jeden Tag-Wert. Jeder Servicekandidat enthält nur CIs mit demselben Wert für den ENV-Schlüssel.
Beispiel 2: eine Tag-Kategorie, ein Wert	Umgebung	ENV	Produktion	Service-Mapping erstellt einen Servicekandidaten, der nur CIs enthält, die den ENV-Tag-Schlüssel mit dem Tag-Wert „production" enthalten.
Beispiel 3: eine Tag-Kategorie, zwei Werte	Umgebung	ENV	Staging, Production	Service-Mapping erstellt zwei Servicekandidaten: Einer enthält CIs mit dem Tag-Wert „production"; ein weiterer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für die Definition von Tag-basierten Zuordnungskriterien für Servicefamilien (Fortsetzung)

Definitionen der Servicefamilie	Kategorie	Schlüssel	Wert (optional)	Ergebnis
				enthält CIs mit dem Tag-Wert „staging".
Beispiel 4: zwei Tag-Kategorien, keine Werte	Umgebung Applikation	ENV App	Nicht definiert	Service-Mapping erstellt für alle definierten Tag-Schlüssel einen Servicekandidaten für jede Kombination von Tag-Werten.
Beispiel 5: zwei Tag-Kategorien, zwei Werte für jede Kategorie	Umgebung Applikation	ENV App	Production, Staging HR, Finance	Service-Mapping erstellt vier Servicekandidaten: production::hr, production::finance, staging::hr, staging::finance.

Liste der datenverkehrsbasierten Verbindungen

In diesem Diagramm finden Sie Informationen zu datenverkehrsbasierten Verbindungen, wenn Sie CIs aus einem Anwendungsservice entfernen.

Liste der datenverkehrsbasierten Verbindungen (wenn Discovery basierend auf Predictive Intelligence deaktiviert ist)

Feld	Beschreibung
IP	Die IP-Adresse der Anwendung, die mit dem ausgewählten CI verbunden ist.
Port	Der Port des ausgewählten CI, der zur Kommunikation mit der anderen Anwendung verwendet wird.
Prozess	Die ID des Prozesses im ausgewählten CI.
Bereits in der Darstellung	• **Ja** – wenn diese Verbindung in der Zuordnung angezeigt wird. • **Nein** – wenn diese Verbindung nicht Teil der Serviceinstanz und nicht in der Zuordnung ist.
Systementscheidung	Die Einstellung legt fest, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Der Wert stammt von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste der datenverkehrsbasierten Verbindungen (wenn Discovery basierend auf Predictive Intelligence deaktiviert ist) (Fortsetzung)

Feld	Beschreibung
	dem Algorithmus, den Service-Mapping Verwendet.
Benutzerentscheidung	(Optional) Die Einstellung überschreibt die Einstellung Systementscheidung, in der festgelegt wird, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Wenn die Systementscheidungseinstellung für eine Verbindung beispielsweise Behalten lautet und Sie diese Verbindung entfernen möchten, wählen Sie `Entfernen`.

Von ITOM-Transparenz verwendete Erkennungsmuster

Von Service-Mapping und Discovery werden Muster in den jeweiligen Discovery-Prozessen verwendet, die die meisten branchenüblichen Netzwerkgeräte und Anwendungen abdecken. Sie können diese Muster anpassen und neue erstellen.

ServiceNow -Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Configuration Items (CIs) umfassen.

Was sind Erkennungsmuster?

Ein Muster ist eine Folge von Befehlen, deren Zweck darin besteht, Attribute eines CI und seiner ausgehenden Verbindungen zu ermitteln. Service-Mapping und Discovery teilen sich einen Satz vorkonfigurierter Muster, die die meisten häufig verwendeten Geräte und Anwendungen abdecken. Muster können den Infrastruktur- oder Anwendungstyp aufweisen. Infrastrukturmuster werden nur von Discovery zum Erstellen von Gerätelisten verwendet. Anwendungsmuster dienen Service-Mapping und Discovery, die für ihre Zwecke dieselben Anwendungsmuster verwenden. Discovery führt beispielsweise die Horizontal-Discovery mit dem Apache-Webservermuster aus, um alle Apache-Webserver in Ihrer Organisation zu suchen und aufzulisten. Service-Mapping führt die Top Down-Discovery mit demselben Muster aus, um einen bestimmten Apache-Webserver zu erkennen und in einer Serviceinstanzzuordnung zu platzieren.

Hinweis: Mustervorgänge bieten derzeit keine Unterstützung mehrerer Sprachen. Wenn die Werte, die von Mustervorgängen zurückgegeben werden, nicht in Englisch vorliegen, können die zurückgegebenen Daten nicht richtig analysiert werden, und die Muster-Discovery schlägt fehl.

Musterverwendung von Service-Mapping und Discovery

Produkt	Mustertyp	Ergebnis
Discovery	Infrastrukturmuster	Bestandsliste der Geräte
	Anwendungsmuster	Bestandsliste der Anwendungen
Service-Mapping	Anwendungsmuster	Serviceinstanz map

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für die Erkennung von Geräten, die als Hosts für Anwendungen agieren, verlässt sich Service-Mapping auf Discovery. Als Teil des Erkennungsprozesses von oben nach unten weist Service-Mapping Discovery an, seine horizontale Erkennung im Hintergrund durchzuführen. Service-Mapping verwendet dann die Informationen zu den Hosts, die bei der horizontalen Erkennung ermittelt werden, zum Erstellen von für Service-Karten.

Muster aller Typen werden in der Tabelle „Erkennungsmuster“ [sa_pattern] gespeichert.

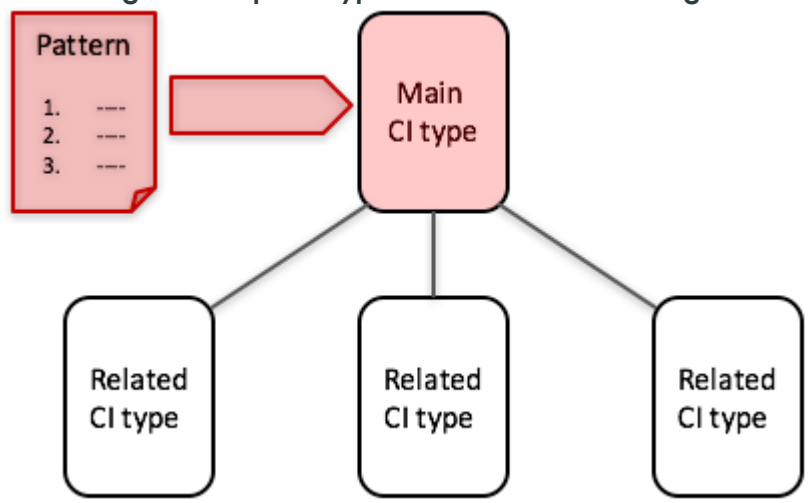
Discovery verwendet eine Kombination aus Probes und Mustern. Weitere Informationen finden Sie unter Prozess-Flow der horizontalen Erkennung mit Probes und Sensoren.

Korrelation zwischen Muster und CI-Typ

Muster werden den CI-Typen zugewiesen, die zur Erkennung dienen. Bei Bedarf können Sie pro Muster mehrere CI-Typen zuweisen. In diesem Fall definieren Sie einen Haupt-CI-Typ und mehrere zugehörige CI-Typen. Beispiel: Ein Muster zur Erkennung von BIG-IP Global Traffic Manager (GTM) F5 weist BIG-IP Global Traffic Manager (GTM) F5 als Haupt-CI-Typ und zugehörige CI-Typen für den DNS-Namen, den Netzwerkadapter und andere Komponenten auf.

Bei der Erkennung von oben nach unten durch Service-Mapping dient jedes Anwendungsmuster nur zur Erkennung des Haupt-CI-Typs.

Erkennung des Haupt-CI-Typs während der Erkennung von oben nach unten

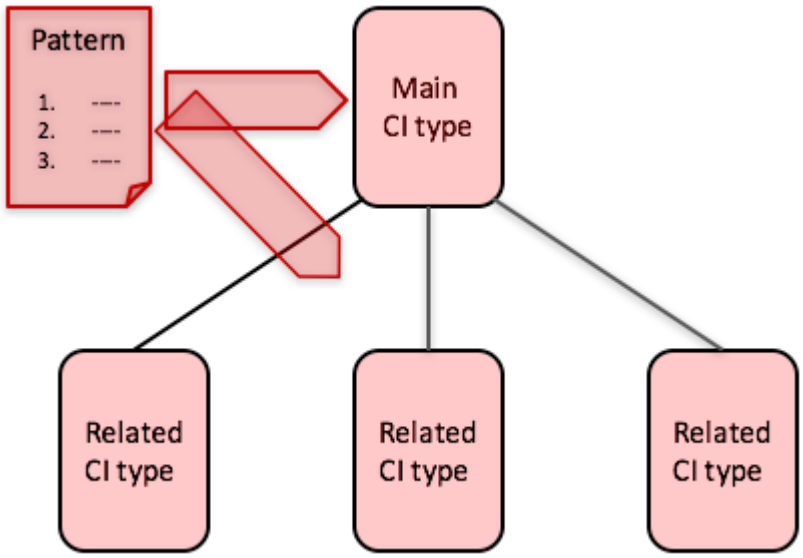


Gleichzeitig verwendet Service-Mapping in der Regel mehr als ein Muster, um denselben CI-Typ zu erkennen, da ein CI-Typ verschiedene Protokolle, Betriebssysteme, Einstiegspunkte usw. verwenden kann.

Im Gegensatz zur Erkennung von oben nach unten verwendet der Prozess der horizontalen Erkennung jedes Muster, um einen Haupt-CI-Typ mit allen zugehörigen CI-Typen zu erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennung des Haupttyps und der zugehörigen CI-Typen während der horizontalen Erkennung



Warum Muster aus dem ServiceNow Store installieren

ServiceNow veröffentlicht monatlich neue Discovery-Muster im ServiceNow Store , um sicherzustellen, dass Ihr Unternehmen die neuesten Geräte und Anwendungen nach Branchenstandard erkennen kann. Hauptversionen von ServiceNow enthalten Muster, die zuvor im ServiceNow Store veröffentlicht wurden.

Ab Tokyo gibt ServiceNow alle Discovery-Muster mit den folgenden Anwendungen frei:

Muster für Discovery und Service-Mapping (sn_itom_pattern)

Diese Anwendung stellt die neuesten Versionen von Discovery-Mustern bereit, deren ursprüngliche Version ServiceNow im ServiceNow Store veröffentlichte.

Visibility Content (sn_pattern_design)

Diese Anwendung stellt die aktualisierte Version der Muster bereit, die bis Tokyo Teil der Familien-Releases waren.

Sie können die neuesten verfügbaren Versionen der Musteranwendungen aus dem ServiceNow Store installieren. Alternativ können Sie diese Anwendungen als Plugins auf Ihrer Instanz von ServiceNow installieren.

Warum Muster anpassen

Sie können Muster in den folgenden Fällen anpassen:

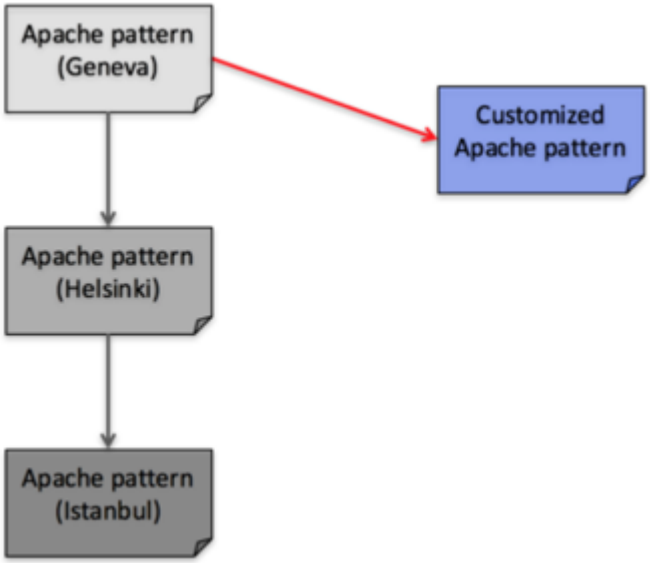
- Wenn Ihr Unternehmen proprietäre Geräte und Anwendungen verwendet, erstellen Sie Muster für diese Elemente, damit Discovery und Service-Mapping sie erkennen können.
- Wenn Sie Schlüsselattribute von CI-Typen mit entsprechenden Mustern ändern, ändern Sie die relevanten Muster entsprechend der Änderung.

Musterversionen

Wenn Sie ein Muster anpassen, erstellen Sie tatsächlich eine Kopie des ursprünglichen vorkonfigurierten Musters. Während Service-Mapping oder Discovery die angepasste Version verwenden, wird die ursprüngliche Version nicht gelöscht. Wenn Sie ein Update des Musters aus dem ServiceNow Store herunterladen, wird das ursprüngliche Muster aktualisiert, nicht die angepasste Kopie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausschluss eines benutzerdefinierten Musters von einem Upgrade



Wenn Sie das angepasste Muster verwerfen und das aktualisierte ursprüngliche Muster verwenden möchten, können Sie wie in Musterversion auswählen beschrieben zum ursprünglichen Muster zurückkehren.

Wer Muster anpassen kann

Anwender müssen über die Rolle pd_admin verfügen, um Muster anzupassen. Im Basissystem enthält die Rolle service_mapping_admin die pd_role. Das Anpassen von Mustern erfordert Grundkenntnisse in der Programmierung.

Muster für Instanzen mit Domänentrennung

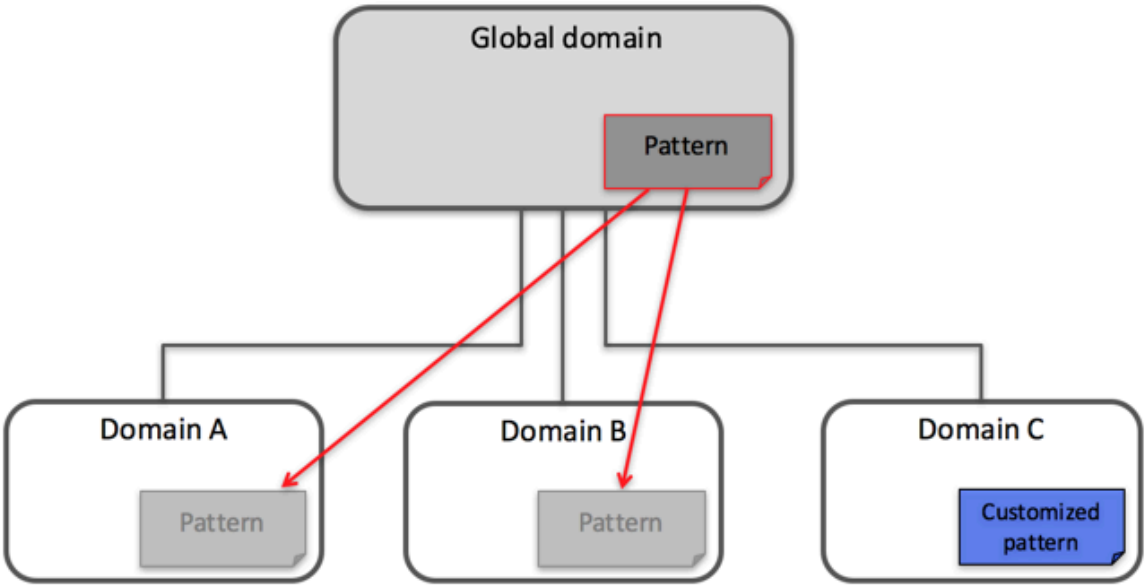
In Instanzen, die Domänentrennung verwenden, können Muster domänenspezifisch sein und nur Domänen umfassen, für die Sie sie erstellt haben, oder global und auf alle Domänen angewendet werden.

Muster gehören zu Domänen. Standardmäßig werden alle vorkonfigurierten Muster der globalen Domäne zugewiesen und gelten für alle Domänen aller Ebenen.

Sie können Muster für bestimmte Domänen erstellen. In diesem Fall wird das neue Muster nur für diese Domäne verwendet und ist in keiner anderen Domäne vorhanden. Wenn Sie ein vorhandenes Muster in der globalen Domäne anpassen und einer bestimmten Domäne zuweisen, erstellen Sie eine Kopie des globalen Musters, das weiterhin in allen anderen Domänen verwendet wird, mit Ausnahme der Domäne mit der angepassten Version dieses Musters. Wenn Sie ein Muster in der globalen Domäne anpassen, wirkt sich die Änderung entsprechend auf alle Domänen aus, mit Ausnahme derjenigen, die eine angepasste Kopie dieses Musters verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Globale oder domänenspezifische Muster



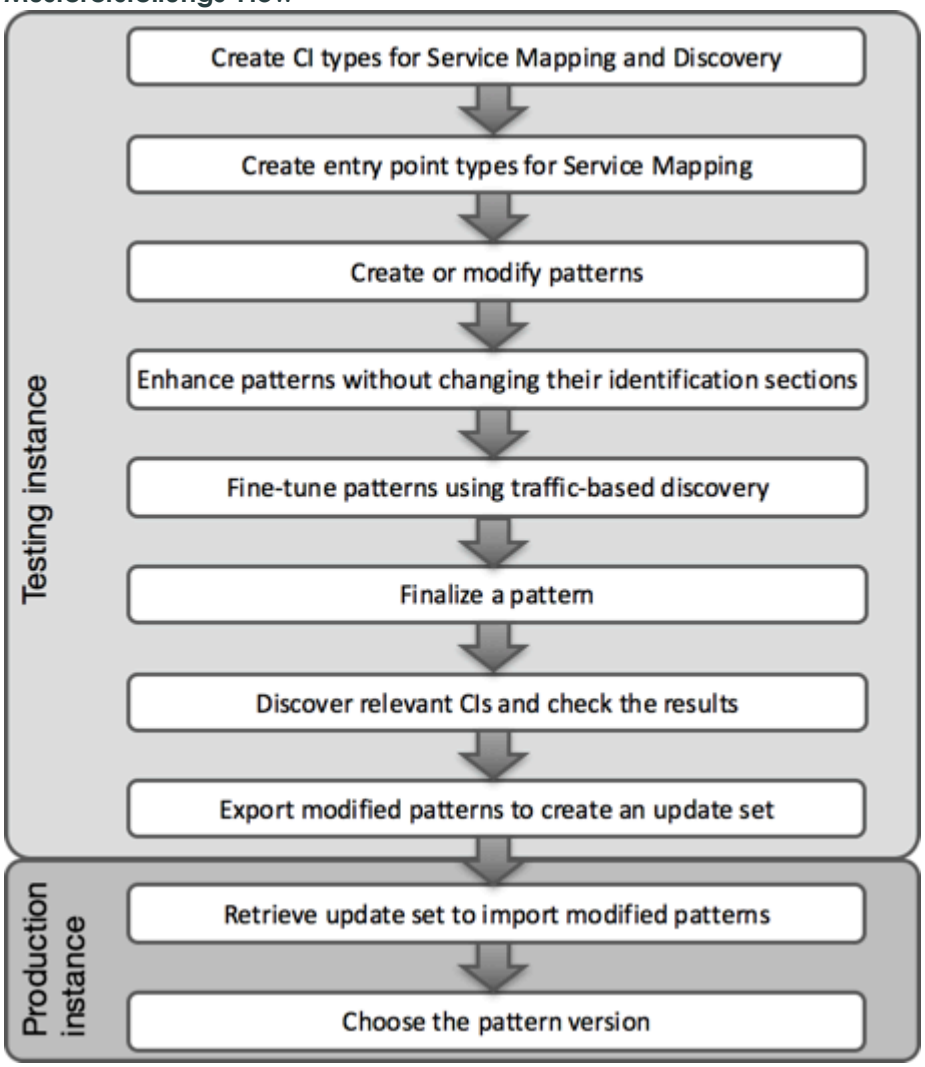
Erstellungs- oder Änderungs-Flow für Muster

Normalerweise pflegen Sie zwei ServiceNow-Instanzen in Ihrer Organisation: für die Produktion und für die Entwicklung. Erstellen oder ändern Sie Muster, testen Sie sie und überprüfen Sie die Ergebnisse in der Entwicklungsinstanz. Wenn Sie mit den Discovery-Ergebnissen zufrieden sind, exportieren Sie relevante Muster aus der Entwicklungsinstanz, um einen Update-Satz zu erstellen. Anschließend rufen Sie den Aktualisierungssatz in Ihrer Produktionsinstanz ab und legen Sie ihn fest.

Wenn Sie ein Muster für Anwendungen und Geräte erstellen, die in der Anwendung ITOM Visibility Global Content nicht unterstützt werden, erstellen Sie zuerst CI-Typen für sie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mustererstellungs-Flow



Zugehörige Informationen

- Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte
- Klassendiagramme und Klassenattribute für wichtige CMDB-Klassen
- Beschreibung der wichtigsten CMDB-Tabellen im Basissystem
- CMDB CI Class Models: ServiceNow Store-App, die Klassenmodelle hinzufügt, die die CMDB-Klassenhierarchie erweitern
- Informationen zu den verschiedenen Optionen zum Füllen der CMDB
- ServiceNow Store-Apps, die vordefinierte Service Graph-Connectors zum Importieren und Integrieren gängiger Daten von Drittparteien in CMDB-Klassen bereitstellen
- KB0747679: Pre/Post Processing Scripts for patterns (Vor-/Nachverarbeitungsskripts für Muster)

Verfügbare Erkennungsmuster

ITOM-Transparenz wird mit einer umfangreichen Musterbibliothek geliefert.

ServiceNow veröffentlicht monatlich neue Discovery-Muster im ServiceNow Store , um sicherzustellen, dass Ihr Unternehmen die neuesten Geräte und Anwendungen nach Branchenstandard erkennen kann. Hauptversionen von ServiceNow enthalten Muster, die zuvor im ServiceNow Store veröffentlicht wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine vollständige Liste der Geräte und Anwendungen, die ITOM-Transparenz erkennen kann, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Apache Cassandra Discovery von Datenbanken

ServiceNow Discovery findet die Datenbank Apache und die DataStax-Datenbank Cassandra auf UNIX mithilfe des verteilten Cassandra-DB-Musters. Um einige dieser Ressourcen zu erkennen, müssen Sie Muster für Discovery und Service-Mapping aus ServiceNow® Storeinstallieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Geben Sie Anmeldeinformationen für die Erkennung des Hosts an

Identifizieren Sie die Server, die eine Cassandra -Datenbank hosten, und stellen Sie die Anmeldeinformationen bereit, die für die Horizontal-Discovery dieser Server erforderlich sind. Weitere Informationen finden Sie unter Für die Hosterkennung erforderliche Anmeldeinformationen.

Stellen Sie sicher, dass die Store-App „CMDB CI Class Models“ aktuell ist

Stellen Sie sicher, dass Ihre -Instanz die CI-Klassenmodelle Cassandra unterstützt, indem Sie Version 1.14.0 der Store-App CMDB CI-Klassenmodelle aus ServiceNow Storebereitstellen.

Berechtigungen für Cassandra -Befehle für UNIXverifizieren

Die Liste der Cassandra -Befehle finden Sie im Abschnitt Cassandra (für UNIX) in Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern.

Verifizieren Sie den Lesezugriff auf cassandra.yaml

Mögliche Speicherorte für die Datei „cassandra.yaml“:

- `$config_directory + „/cassandra.yaml“`
- `$process.environmentVariables.CASSANDRA_CONF.value + "/cassandra.yaml"`
- `$install_directory + „/conf/cassandra.yaml“`

Daten, die von Discovery für die Datenbank Cassandra gesammelt wurden

Discovery füllt die Daten in CMDB aus, wenn das verteilte Cassandra-DB-Muster ausgeführt wird.

Cassandra-Cluster [cmdb_ci_cassandra_cluster]

Feld	Beschreibung
Name [name]	Der Name des Clusters dient auch als Anzeigename.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cassandra-Clusterknoten [cmdb_ci_cassandra_cluster_node]

Feld	Beschreibung
Cluster [cluster]	Referenz des CI im Cluster Cassandra, zu dem dieser Knoten gehört.
Clustername [cluster_name]	Name des Clusters.
IP-Adresse [ip_address]	IP-Adresse des Clusterknotens (Hostcomputer)
Name [name]	Anzeigename im folgenden Format: cluster_name@hostname
Betriebsstatus [operational_status]	Betriebsstatus des Clusterknotens
Server [Server]	Referenz des Server-CI (Hostcomputer)

Cassandra-Instanz [cmdb_ci_cassandra_instance]

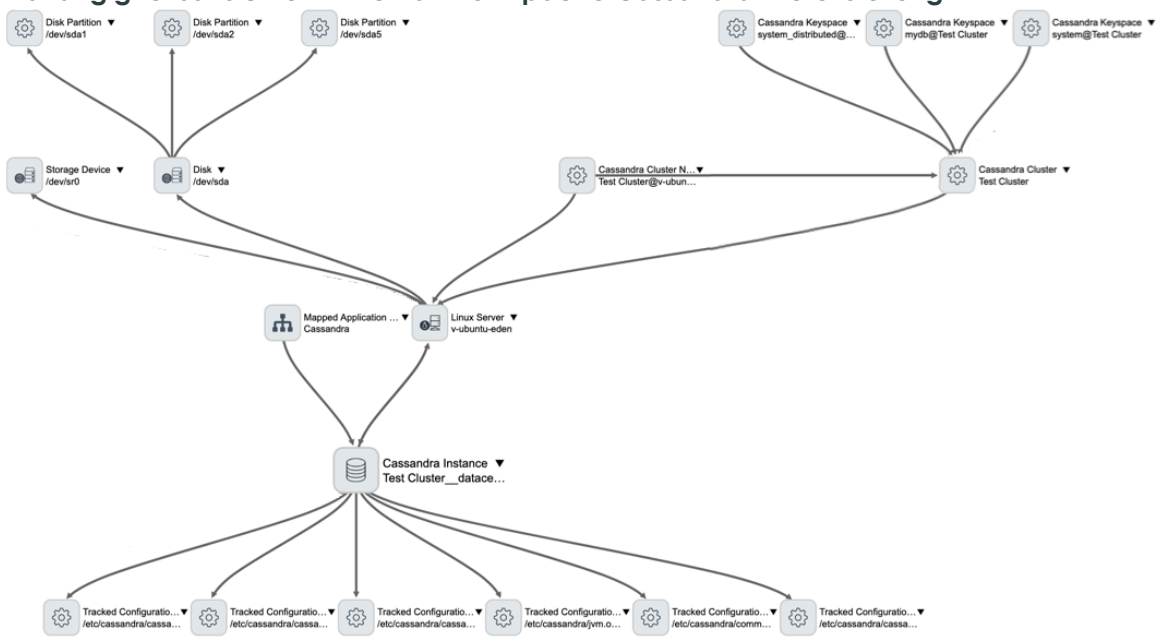
Feld	Beschreibung
Clustername [cluster_name]	Name des Clusters.
Konfigurationsverzeichnis [config_directory]	Verzeichnispfad, in dem Konfigurationsdateien verfügbar sind
Konfigurationsdatei [config_file]	Dateipfad der BaseInit-Konfigurationsdatei, in der andere konfigurationsbezogene Pfade konfiguriert werden können
Rechenzentrum [data_center]	Rechenzentrum, in dem der Clusterknoten Teil eines Clusters ist
Installationsverzeichnis [install_directory]	Der Installationspfad
IP-Adresse [ip_address]	IP-Adresse des Hostcomputers, auf dem der Prozess ausgeführt wird
Name [name]	Anzeigename, der mit der <uid> identisch ist
PID [pid]	Prozess-ID, die auf dem Hostcomputer ausgeführt wird
Rack [Rack]	Die Rack-Informationen, zu denen der Clusterknoten gehört
Beschreibung [short_description]	Eine Kurzbeschreibung der Instanz
TCP-Port(s) [tcp_port]	Liste der TCP-Ports, die wie in der Konfigurationsdatei „cassandra.yaml“ konfiguriert sind (Format: „:port1:port2:port3:“)
UID [uid]	Die eindeutige ID zum Identifizieren der Instanz (Format: <cluster_name> __ <data_center> __ <rack> @hostname)
Anbieter [vendor]	Lieferantenname für Referenz aus der Tabelle „core_company“, falls bereits verfügbar. Wenn er nicht verfügbar ist, wird logisch ein neuer Eintrag mit dem Namen „Apache“ oder „DataStax“ erstellt.
Auslastung wird ausgeführt [workload_running]	Der Name der Workload, die auf der Instanz ausgeführt wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cassandra-Keyspace [cmdb_ci_cassandra_keyspace]

Feld	Beschreibung
Cluster [cluster]	Die Referenz des Cluster-CI Cassandra, zu der der Keyspace gehört.
Clustername [cluster_name]	Name des Clusters, zu dem der Keyspace gehört
Keyspace-Name [keyspace_name]	Name des Keyspace
Name [name]	Der Anzeigename im folgenden Format:<keyspace_name> @<cluster_name> .

Abhängigkeitsansichten mit erkannter Apache Cassandra -Bereitstellung



CI-Beziehungen

Discovery erstellt diese Beziehungen, um die Datenbank-Discovery Apache Cassandra von zu unterstützen.

CI	Beziehung	CI
Cassandra-Instanz [cmdb_ci_cassandra_instance]	Wird ausgeführt auf::Wird ausgeführt	Server [cmdb_ci_server]
Cassandra-Clusterknoten [cmdb_ci_cassandra_cluster_node]	Gehostet auf::Hostet	Server [cmdb_ci_server]
	Cluster von::Cluster	Cassandra-Cluster [cmdb_ci_cassandra_cluster]
Cassandra-Keyspace [cmdb_ci_cassandra_keyspace]	Gehostet auf::Hostet	Cassandra-Cluster [cmdb_ci_cassandra_cluster]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Service Mapping führt die Top Down-Discovery von Cassandradurch, das normalerweise als verteilte Datenbank auf einem Cluster von Serverknoten ausgeführt wird. Bei der Top Down-Discovery erkennt Service-Mapping Instanzen, die auf -Knoten ausgeführt werden, und zeigt sie in der Anwendungsservice-Zuordnung an.

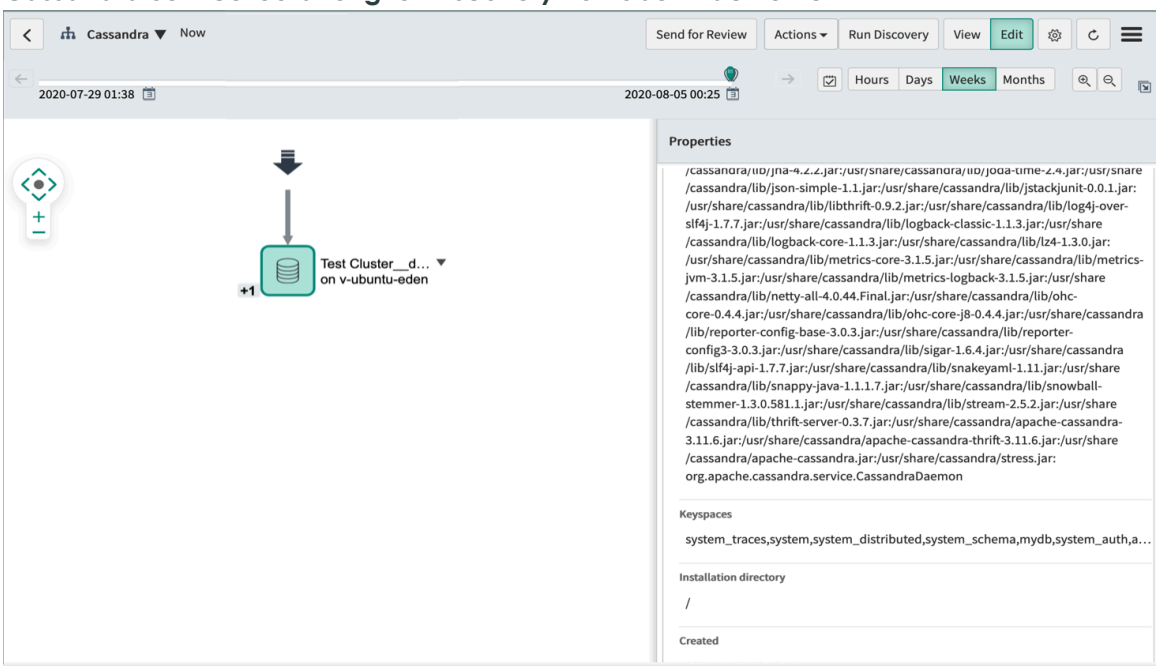
Zusätzlich zu den während der horizontalen Erkennung erkannten Tabellen und Feldern werden bei der Erkennung von oben nach unten auch die in der folgenden Tabelle aufgeführten Felder erkannt.

Cassandra-Instanz [cmdb_ci_cassandra_instance]

Feld	Beschreibung
Schlüsselbereiche [keyspaces]	Keyspace(s), auf die die Instanz zugreifen kann (nur in Erkennung von oben nach unten ausgefüllt)

Bei eingehenden Verbindungen wird die Instanz erkannt, wie im folgenden Bild dargestellt.

Cassandra Servicezuordnung für Discovery von oben nach unten



Zugehörige Informationen

Discovery-Berichte von Database Administrator (DBA).

Erkennung von Apache Kafka und Apache Zookeeper

ServiceNow Discovery verwendet das Erkennungsmuster „Kafka and Zookeeper“, um Kafka-Daten zu finden, die für den Zookeeper-Synchronisierungsservice erstellt wurden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Store-App „CMDB CI Class Models“

Stellen Sie sicher, dass die Store-App CMDB CI Class Models (Version 1.20.0) installiert ist.

Store-App Discovery and Service Mapping Patterns

Stellen Sie sicher, dass die Store-App Discovery and Service Mapping Patterns (Version 1.0.72) installiert ist.

Zertifizierungsstellen-Prozess

Stellen Sie sicher, dass auf dem Hostcomputer der CA-Prozess ausgeführt wird.

Discovery-Anmeldeinformationen

Stellen Sie sicher, dass Sie über die Anmeldeinformationen für die Ausführung von Discovery auf dem Host-Computer verfügen, auf dem der CA-Prozess ausgeführt wird.

Die Kafka- und Zookeeper-Prozesse müssen auf dem Host ausgeführt werden.

Hinweis: Die Discovery des Kafka-Brokers muss zuerst ausgeführt werden, gefolgt von Zookeeper. In der Zookeeper-Konfigurationsdatei muss die Reihenfolge der Knoten, die das Cluster bilden, für alle Knoten im Cluster einheitlich sein.

Von Discovery während der horizontalen Erkennung erfasste Daten

In der Tabelle [cmdb_ci_appl_kafka_connect] erkannte Ressourcen

Felder	Beschreibung
name	Name des CI
node	Knoten, auf dem Zookeeper installiert ist
tier	Stufe von Zookeeper
install_directory	Pfad des Installationsverzeichnisses
config_file	Pfad der Konfigurationsdatei
config_directory	Pfad des Konfigurationsverzeichnisses

In der Tabelle [cmdb_ci_appl_kafka_topic] erkannte Ressourcen

Felder	Beschreibung
name	Name des CI
isr	Synchronisiertes Replikat
replicas	Anzahl der Replikate des Themas
partition_count	Anzahl der Partitionen des Themas
replication_factor	Replikationsfaktor des Themas

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Tabelle [cmdb_ci_appl_zoo_keeper] erkannte Ressourcen

Felder	Beschreibung
name	Name des CI
node	Knoten, auf dem Zookeeper installiert ist
tier	Stufe von Zookeeper
config_file	Pfad der Konfigurationsdatei
install_directory	Pfad der Installation

In der Tabelle [cmdb_ci_kafka_cluster] erkannte Ressourcen

Felder	Beschreibung
Cluster_id	Eindeutige clusterspezifische ID

In der Tabelle [cmdb_ci_zoo_keeper_cluster] erkannte Ressourcen

Felder	Beschreibung
Cluster_id	Eindeutige clusterspezifische ID

In der Tabelle [cmdb_ci_kafka_cluster_node] erkannte Ressourcen

Felder	Beschreibung
Name	Name des Knotens
Clustername	Name des Clusters, zu dem der Knoten gehört

In der Tabelle [cmdb_ci_zoo_keeper_cluster_node] erkannte Ressourcen

Felder	Beschreibung
Name	Name des Knotens
clustername	Name des Clusters, zu dem der Knoten gehört

CI-Beziehungen

Das Muster „Kafka and Zookeeper“ erstellt keine CI-Beziehungen.

Erkennung von Apigee Edge Enterprise Edition

Die Anwendung ServiceNow Discovery verwendet das APIGee-Muster, um Apigee Edge Enterprise Edition-Versionen 4.xx zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Das APIGee-Muster verwendet einen integrierten Cache-Mechanismus, der Daten von jedem API-Service in einer lokalen Cache-Datei sammelt. Service-Mapping führt eine Erkennung von oben nach unten für diese Cache-Dateien durch, um ausgehende Apigee Edge-Verbindungen zu finden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Linux-Benutzer

Gewähren Sie einem Benutzer des Linux-Betriebssystems erhöhte Rechte für die Ausführung der Befehle cat, ls, netstat und stat. Weitere Informationen finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern.

Erteilen Sie diesem Linux-Benutzer außerdem die Berechtigung, die folgenden Befehle im Home-Ordner des Betriebssystembenutzers auszuführen:

Befehl	Beschreibung
"date +%s"	Ruft das aktuelle Datum ab
"ls -d $HOME/APIGee_Cache/ cache_folder*"	Ruft den letzten Cache-Ordner ab
"mkdir-p $HOME/APIGee_Cache/ cache_folder_" + $today + ";ls -d$HOME/APIGee_Cache/ cache_folder_" + $today	Erstellt die Cache-Datei, wenn die Cache-Datei leer ist
"ls -d $HOME/APIGee_Cache/ cache_folder*"	Überprüft, ob die Cache-Datei erstellt wurde
"echo `expr " + $today + " -" + $current_date+ "`"	Berechnet die Lücke zwischen dem Zeitpunkt der Ordnererstellung und dem aktuellen Datum
"if [" + $diff + " -ge" + $week_seconds+ "]; then echo true; fi"	Prüft, ob der Ordner neu erstellt werden muss
"ls" + $cache_folder+ "/* | sort | xargsgrep -l " + $entry_point.source_url	Überprüft, ob vorhandene Cache-Dateien die Quell-URL enthalten, die Sie als Einstiegspunkt für den Service eingeben
"rm-rf" + $cache_folder+ ";mkdir-p $HOME/APIGee_Cache/ cache_folder_" + $today + ";ls -d $HOME/APIGee_Cache/ cache_folder_" + $today	Entfernt alte Cache-Dateien
“curl -k -X GETurl-H '<ClientID>: <Token>’”	Ruft die API-Antwort für das angegebene Token ab
"ls" + $cache_folder+ "/* | sort | xargsgrep -l " + $entry_point.source_url	Ruft die URL-Definition aus der Cache-Datei ab

Applicative-Anmeldeinformationen

Konfigurieren Sie die Applicative-Anmeldeinformationen wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Applicative-Anmeldeinformationen“

Feld	Beschreibung
Name	Der Name der Anmeldeinformationen, z. B. „Apigee-Token“
Aktiv	Kontrollkästchen zum Aktivieren dieser Anmeldeinformationen für die Erkennung
Benutzername	Der Name des Benutzers dieser Applicative-Anmeldeinformationen. Sie können einen beliebigen Benutzer für die Anmeldeinformationen für dieses Muster verwenden, da die Informationen aus einem lokalen Cache extrahiert werden.
Passwort	Das tatsächliche Benutzerpasswort für diese Applicative-Anmeldeinformationen.
CI-Typ	Der CI-Typ, für den diese Anmeldeinformationen verwendet werden: APIGee-Service [cmdb_ci_appl_apigee_srv]. **Hinweis:** ServiceNow -Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Configuration Items (CIs) umfassen.
Betrifft	Wählen Sie aus, ob diese Anmeldeinformationen für **Alle MID-Server** in Ihrem Netzwerk oder für einen oder mehrere **Spezielle MID-Server** angewendet werden sollen. Geben Sie im Feld **MID-Server** die MID-Server an, die diese Anmeldeinformationen verwenden sollen.
Reihenfolge	Geben Sie die Reihenfolge (Reihenfolge) ein, in der die Plattform diese Berechtigungsnachweise versucht, während sie versucht, sich an Geräten anzumelden. Je kleiner die Zahl, desto höher wird der Berechtigungsnachweis in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Applicative-Anmeldeinformationen“ (Fortsetzung)

Feld	Beschreibung
	Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge.

Curl-Befehl

Stellen Sie sicher, dass der Befehl „curl“ auf dem Linux-Server installiert ist, der Apigee Edge hostet.

Systemeigenschaften konfigurieren

- Zum Erstellen von ausgehenden Apigee Edge-Verbindungen von oben nach unten konfigurieren Sie die Systemeigenschaft Apigee-URLs (apigee.urls) mit der folgenden Syntax:

  ```
  01#DVL#https://<url1>.com/dashboard/v1/targetServers/dvl###
  02#QA#https://<url2>.com/dashboard/v2/targetServers/qa###
  ```

  Wobei

  01 die URL-Nummer ist.

  DVL der Umgebungstyp ist, wie z. B. Entwicklung.

  # das Trennzeichen zwischen den Attributen ist. Platzieren Sie es genau an der Stelle wie im Beispiel oben.

  ### das Trennzeichen zwischen URLs ist.

- Konfigurieren Sie die Systemeigenschaft „Apigee-API-Client-ID“ (apigee.api.client.id), indem Sie die ID des Apigee-API-Clients in das Feld „Wert“ eingeben. Das Muster verwendet diese Eigenschaft als Header für den Befehl „curl“ mit dem Token:

  ```
  curl -k -X GET " + url + " -H ' apigee.api.client.id: " + token
  ```

Das Muster füllt diese beiden Systemeigenschaften mithilfe des *Apigee-URLs und Apigee API Client-ID hinzufügen* sa_pre_task_script aus.

Von Discovery für die Enterprise-Edition von Apigee Edge gesammelte Daten

Discovery füllt die Daten in CMDB aus, wenn das APIGee-Muster ausgeführt wird.

APIGee-Service [cmdb_ci_appl_apigee_srv]

Feld	Beschreibung
Name [name]	Der Name des Servers, der Apigee Edge hostet
Version [version]	Die Version von Apigee Edge
Installationsverzeichnis [install_directory]	Der Ordner mit allen Apigee Edge-Bibliotheken und ausführbaren Dateien

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

APIGee-Service [cmdb_ci_appl_apigee_srv] (Fortsetzung)

Feld	Beschreibung
Konfigurationsverzeichnis [config_directory]	Der Ordner mit allen Apigee Edge-Konfigurationsdateien

CI-Beziehungen

Das APIGee-Muster erstellt keine CI-Beziehungen.

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Das APIGee-Muster identifiziert Verbindungen von Apigee Edge zu anderen CIs basierend auf der URL, die Sie im Verbindungsabschnitt des Musters konfigurieren.

Avi Vantage-Lastenausgleicherkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping verwenden die Muster für die Avi-Lastenausgleicherkennung, um die Komponenten des Avi Vantage-Lastenausgleichsmoduls zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery verwendet das Muster „Avi Load Balancer Controller“ und sowie das Muster „Avi Load Balancer Controller - Session-based“, um die horizontale Erkennung auszuführen. Von beiden Mustern werden REST-APIs dazu verwendet, die Lastenausgleichsmodule zu finden. Sie unterscheiden sich nur in der Art der Authentifizierung, die beim Ausführen der API-Abfragen verwendet wird.

Für die Erkennung von oben nach unten verwendet Service-Mapping das Muster „Avi Load Balancer VIP“.

Die Muster unterstützen Avi-Infrastrukturen unter AWS und VMware. Sie verknüpfen die erkannten CIs nur mit der Infrastruktur, wenn sie unter VMware ausgeführt werden. Die Muster unterstützen auch Global Server Load Balancing (GSLB).

Sie können diese Muster auf der Now Platform® mit Release Madrid Patch 5, New York oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass Ihre Instanz die CI-Klassenmodelle des Avi-Lastenausgleichsmoduls unterstützt, indem Sie die neueste Version der Store-App CMDB CI Class Models bereitstellen. Installieren Sie die Anwendung aus dem ServiceNow Store.
- Für das Muster „Avi Load Balancer Controller“:
  - Stellen Sie im Avi-Controller sicher, dass Standardauthentifizierung zulässig ist.
  - Konfigurieren Sie die folgenden Anmeldeinformationen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Discovery** > **Anmeldeinformationen**
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **Basisanmeldedaten**, füllen Sie das Formular aus, und klicken Sie dann auf **Senden**.

Formular für Anmeldeinformationen

Feld	Beschreibung
Name	Name der Anmeldeinformationen
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Betrifft	Wählen Sie **Alle MID Server**.
Reihenfolge	Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten verwendet. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist 100.
Benutzername	Name des Benutzers für die Ausführung der Avi-Lastenausgleicherkennung
Passwort	Passwort für diesen Benutzer

4. Schnell-Discovery ausführen auf der IP-Adresse des Avi Controller-Clusters.

- Für das Muster „Avi Load Balancer Controller - Session-based“:
  - Erstellen Sie Anmeldeinformationen für die Standardauthentifizierung mit einem Alias:
    1. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
    2. Klicken Sie auf **Neu**.
    3. Geben Sie einen eindeutigen Namen für den Alias ein, und wählen Sie **Anmeldeinformationen** als Alias-Typ aus.
    4. Klicken Sie auf **Absenden**.
    5. Öffnen Sie den neuen Alias.
    6. Klicken Sie auf der Registerkarte Anmeldeinformationen auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie **Basisanmeldedaten** für den Anmeldeinformationstyp aus, und füllen Sie das Formular aus.

Formular für Anmeldeinformationen

Feld	Beschreibung
Name	Name der Anmeldeinformationen
Benutzername	Name des Benutzers für die Ausführung der Avi-Lastenausgleicherkennung
Passwort	Passwort für diesen Benutzer

8. Klicken Sie auf **Aktualisieren**.

◦ Erstellen Sie einen Zeitplan für eine Erkennung ohne Server.

Führen Sie dann folgende Schritte aus:

1. Klicken Sie im Zeitplaner auf die Registerkarte **Ausführungsmuster ohne Server**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus, und klicken Sie dann auf **Senden**.

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Muster	Wählen Sie das Muster „Avi Load Balancer Controller - Session-based“ aus.

4. Öffnen Sie den in den vorherigen Schritten erstellten Datensatz, und konfigurieren Sie diese Parameter:

Parameter	Beschreibung
IP-Adresse	Die Avi-IP-Adresse
Anmeldeinformationsalias	Den Namen des oben erstellten Anmeldeinformationsalias

- Für das Muster „Avi Load Balancer Controller“ und das Muster „Avi Load Balancer Controller - Session-based“ erteilen Sie einem Benutzer Berechtigungen zum Senden der folgenden API-Abfragen.
  - /api/cluster
  - /api/serviceengine
  - /api/pool
  - /api/vimgrvmruntime?controller_vm=true
  - /api/cloud
  - /api/virtualservice
  - /api/serviceenginegroup

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- /api/gslbservice
- /api/tenant

- Für das Muster „Avi Load Balancer VIP“:
  - Erstellen Sie eine für Service .
  - Vor der Verwendung des Musters „Avi Load Balancer VIP“ verwenden Sie eines der Muster für die horizontale Avi-Lastenausgleicherkennung, um die Avi-Infrastruktur zu finden.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

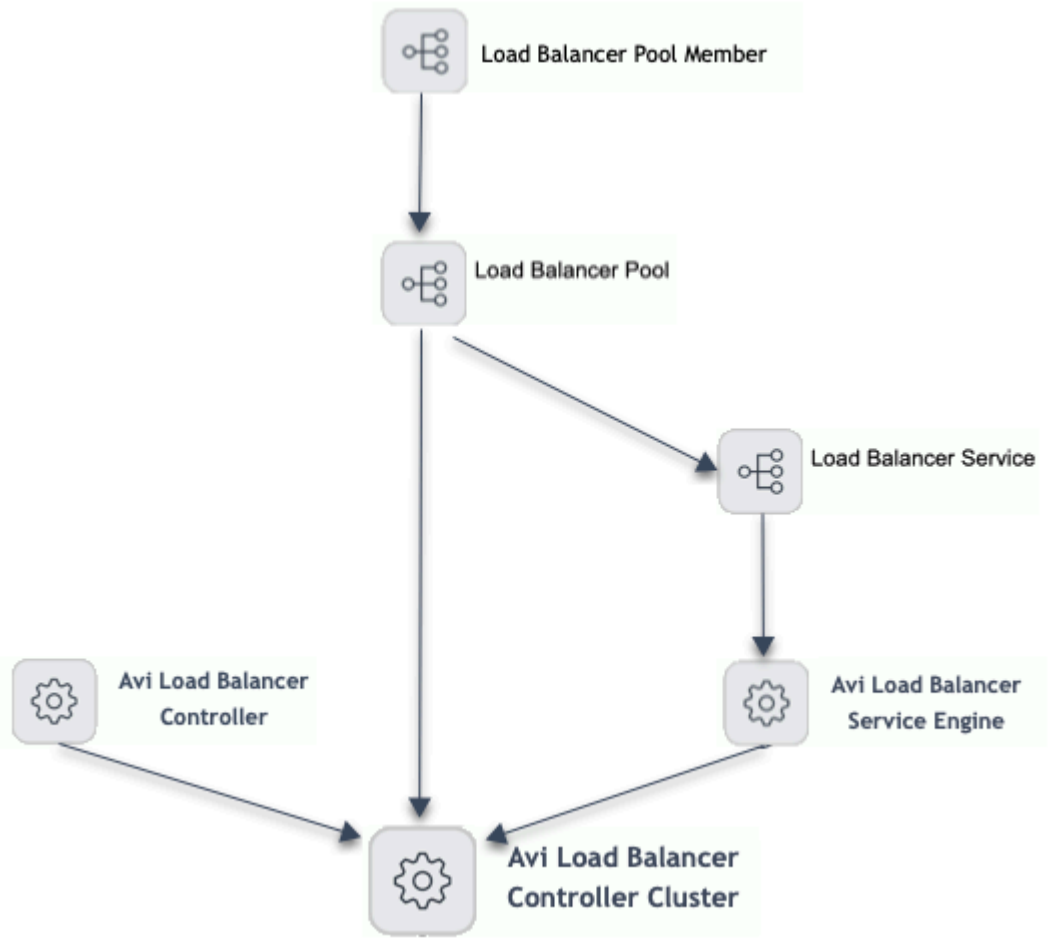
Tabelle und Feld	Beschreibung
Avi Controller [cmdb_ci_avi_controller]	
Name [name]	Name des Avi-Controllers
Vollständig qualifizierter Domänenname [fqdn]	Hostname des virtuellen Computers (VM)
IP-Adresse [ip_address]	IP-Adresse des FQDN
Avi-Service-Engine [cmdb_ci_avi_service_engine]	
Name [name]	Name der Avi-Service-Engine
IP-Adresse [ip_address]	IP-Adresse der Avi-Service-Engine
Version [version]	Version der Avi-Service-Engine
Objekt-ID [object_id]	Eindeutiger Bezeichner der Avi-Service-Engine
Avi-Controller-Cluster [cmdb_ci_avi_controller]	
Cluster-ID [cluster_id]	Eindeutiger Bezeichner des Avi Controller-Clusters
Name [name]	Name des Avi-Controller-Clusters
IP-Adresse [ip_address]	IP-Adresse des Hosts des Avi-Controller-Clusters
Load Balancer-Pool [cmdb_ci_lb_pool]	
Name [name]	Name des Pools von Lastenausgleichsmodulen
Server-ID [server_id]	Eindeutiger Bezeichner des Pools von Lastenausgleichsmodulen
Lastenausgleichsmethode [load_balancing_method]	Methode, die Avi Vantage zur Entscheidung über den Lastenausgleich verwendet. Das Muster übersetzt die Algorithmen wie folgt: • „LB_ALGORITHM_LEAST_CONNECTIONS“: „wenigste Verbindungen“ • „LB_ALGORITHM_ROUND_ROBIN“: „Round-Robin“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
	• „LB_ALGORITHM_FASTEST_RESPONSE“: „schnellste Antwort“ • „LB_ALGORITHM_CONSISTENT_HASH“: „konsistenter Hash“ • „LB_ALGORITHM_LEAST_LOAD“: „geringste Last“ • „LB_ALGORITHM_FEWEST_SERVERS“: „wenigste Server“ • „LB_ALGORITHM_RANDOM“: „zufällig“ • „LB_ALGORITHM_FEWEST_TASKS“: „wenigste Aufgaben“ • „LB_ALGORITHM_NEAREST_SERVER“: „nächstgelegener Server“
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	
Name [name]	Name des Poolmitglieds @ Name des Pools
IP-Adresse [ip_address]	IP-Adresse des Hosts des Poolmitglieds
Load Balancer-Service [cmdb_ci_lb_service]	
Name [name]	Name der virtuellen IP (VIP)
IP-Adresse [ip_address]	IP-Adresse der VIP
Objekt-ID [object_id]	Eindeutiger Bezeichner der VIP
Port [port]	Port der Host-VM
Avi-Mandant [cmdb_ci_avi_tenant]	
name	Name des Mandanten
object_id	object_id des Mandanten
tenant_url	URL zum Mandanten

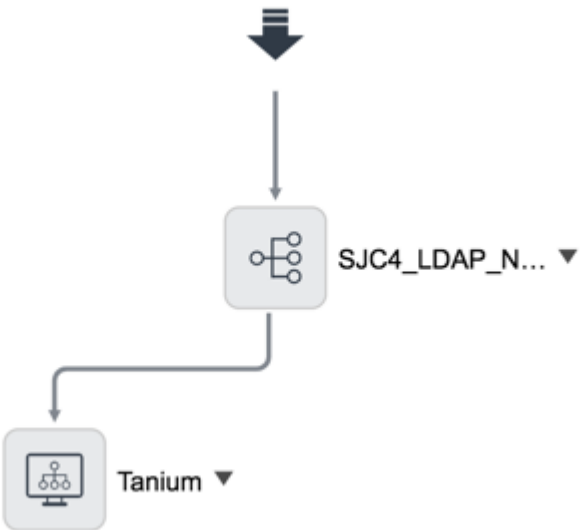
Die Dependency Views-Zuordnung zeigt die erkannten Lastenausgleichsmodul-CIs und deren Beziehung untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die folgende Abbildung zeigt die Ergebnisse einer Erkennung von oben nach unten, die das Muster „Avi Load Balancer VIP“ verwendet.

Erkennung von oben nach unten mithilfe des Musters „Avi Load Balancer VIP“



CI-Beziehungen

Die folgenden Beziehungen werden zur Unterstützung der Avi-Lastenausgleicherkennung erstellt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Avi-Controller-Cluster [cmdb_ci_avi_controller]	Cluster von::Cluster	Avi Controller [cmdb_ci_avi_controller]
Avi-Mandant [cmdb_ci_avi_tenant]	Gehostet auf::Hostet	Avi-Controller-Cluster [cmdb_ci_avi_controller]
	Enthält::Enthalten in	Load Balancer-Service [cmdb_ci_lb_service]
Load Balancer-Pool [cmdb_ci_lb_pool]	Verwendet von::Verwendet	Load Balancer-Service [cmdb_ci_lb_service]
	Gehostet auf::Hostet	Avi-Controller-Cluster [cmdb_ci_avi_controller]
	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Avi-Service-Engine [cmdb_ci_avi_service_engine]	Gehostet auf::Hostet	Avi-Controller-Cluster [cmdb_ci_avi_controller]
Avi Controller [cmdb_ci_avi_controller]	Enthält::Enthalten in	Avi-Service-Engine [cmdb_ci_avi_service_engine]
Load Balancer-Service [cmdb_ci_lb_service]	Verwendet von::Verwendet	Avi-Service-Engine [cmdb_ci_avi_service_engine]
	Wird ausgeführt auf::Wird ausgeführt	Avi-Controller-Cluster [cmdb_ci_avi_controller]
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	Nur Referenz	Avi-Controller-Cluster [cmdb_ci_avi_controller]

Problembehandlung

Wenn die Erkennung von oben nach unten des Avi-Lastenausgleichsmoduls fehlschlägt, finden Sie eine Problemumgehung im KB-Artikel KB0824019 .

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
		Hinweis: Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter *sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Amazon AWS Application ELB Service-Erkennung

Discovery verwendet das Erkennungsmuster „Amazon AWS application ELB Service“, um alle Lastenausgleichsmodule in Ihrer Umgebung in einer Zuordnung anzuzeigen.

Elastic Load Balancing (ELB) verteilt eingehenden Anwendungsdatenverkehr automatisch auf mehrere Ziele.

Das Erkennungsmuster „Amazon AWS application ELB Service“ unterstützt die Erkennung von oben nach unten. Dieses Muster erkennt alle Lastenausgleichsmodule mit diesen Eigenschaften:

- Ultrahochleistung, skaliertes TLS-Offloading und zentralisierte Zertifikatbereitstellung verwenden
- Unterstützung von UDP und statischen IP-Adressen für Ihre Anwendung

Für die Erkennung von oben nach unten lautet der Einstiegspunkt HTTP(s)-Endpunkt. Ausgehende Beziehungen bestehen zu Amazon EC2-Instanzen.

Von der Now Platform werden Amazon Commercial Cloud Services (C2S) für Discovery und Cloud-Governance unterstützt. C2S ist das Regierungsprogramm, das AWS für die Intelligence Community verfügbar macht.

Sie können dieses Muster auf der ServiceNow-Plattform mit Version Kingston oder höher verwenden.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

- Führen Sie eine horizontale Erkennung mithilfe der Cloud-API (CAPI) aus. Dies ist erforderlich, da dieses Erkennungsmuster nur die Erkennung von oben nach unten unterstützt. Für Cloud-Discovery können Sie die horizontale Erkennung wie gewohnt ausführen.
- Wenn die Daten des Lastenausgleichsmoduls in der Configuration Management Database (CMDB) gespeichert wurden, erstellen Sie einen Anwendungsservice für jedes Lastenausgleichsmodul.
- Legen Sie schreibgeschützte Berechtigungen für diese REST APIs fest:
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeLoadBalancers&LoadBalancerArns.member.1=<LB_ARN>&Version=2015-12-01
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeLoadBalancers&Version=2015-12-01
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeListeners&LoadBalancerArn=<LB_ARN>&Version=2015-12-01
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeRules&ListenerArn=<LISTENER_ARN>&Version=2015-12-01
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeTargetHealth&TargetGroupArn=<TARGET_GROUP_ARN>&Version=2015-12-01
  - https://ec2.<REGION>.amazonaws.com/?Action=DescribeInstances&Version=2016-11-15&Filter.1.Name=instance-state-name&Filter.1.Value=running&Filter.2.Name=instance-id&Filter.2.Value=<INSTANCE_ID>
- Laden Sie für Cloud-Discovery das Muster „Discovery and Service Mapping“ aus dem ServiceNow Store herunter.
- Stellen Sie bei der Installation von MID-Serversicher, dass der Hostcomputer die auf der Dokumentationswebsite ServiceNow veröffentlichten Systemanforderungen für den MID-Server erfüllt oder überschreitet.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Load Balancer-Services [cmdb_ci_lb_service]	
Vollständig qualifizierter Domänenname [fqdn]	Vollständig qualifizierte Domänenname (FQDN) des Lastenausgleichsmoduls. Der DNS-Name
Name [name]	Name des Lastenausgleichsmoduls im folgenden Format: <LB-Name>:<LB-Port>
Seriennummer [serial_number]	Seriennummer des Lastenausgleichsmoduls im folgenden Format: ##Object_ID=<LB_ARN>
Port [port]	Port des Lastenausgleichsmoduls
Objekt-ID [object_id]	Eindeutiger Bezeichner des Lastenausgleichsmoduls
IP-Adresse [ip_address]	IP-Adresse des FQDN

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon AWS Classic ELB-Service-Erkennung

Discovery verwendet das Erkennungsmuster „Amazon AWS Classic ELB Service“, um alle Lastenausgleichsmodule zu finden, die HTTP- und HTTPS-Datenverkehr verwenden.

Elastic Load Balancing (ELB) verteilt eingehenden Anwendungsdatenverkehr automatisch auf mehrere Ziele.

Das Erkennungsmuster „Amazon AWS Classic ELB Service“ unterstützt die Erkennung von oben nach unten. Die zwei möglichen Einstiegspunkte für die Erkennung von oben nach unten sind der HTTP(s)-Endpunkt und der TCP-Endpunkt. Ausgehende Beziehungen bestehen zu Amazon EC2-Instanzen.

Von der Now Platform werden Amazon Commercial Cloud Services (C2S) für Discovery und Cloud-Governance unterstützt. C2S ist das Regierungsprogramm, das AWS für die Intelligence Community verfügbar macht.

Sie können dieses Muster auf der ServiceNow-Plattform mit Version Jakarta oder höher verwenden.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Führen Sie eine horizontale Erkennung mithilfe der Cloud-API (CAPI) aus. Dies ist erforderlich, da dieses Erkennungsmuster nur die Erkennung von oben nach unten unterstützt. Für die Cloud-Erkennung können Sie die horizontale Erkennung wie gewohnt ausführen.
- Wenn die Daten des Lastenausgleichsmoduls in der Configuration Management Database (CMDB) gespeichert wurden, erstellen Sie einen Anwendungsservice für jedes Lastenausgleichsmodul.
- Legen Sie schreibgeschützte Berechtigungen für diese REST APIs fest:
  - https://elasticloadbalancing.<REGION>.amazonaws.com/?Action=DescribeLoadBalancers&Version=2012-06-01&LoadBalancerNames.member.1=<LB_NAME>
  - https://ec2.<REGION>.amazonaws.com/?Action=DescribeInstances&Version=2016-11-15&Filter.1.Name=instance-state-name&Filter.1.Value=running&Filter.2.Name=instance-id&Filter.2.Value=<INSTANCE_ID> (to create relation between LB and EC2 instance)
- Laden Sie für Cloud-Discovery das Muster „Discovery and Service Mapping“ aus dem ServiceNow Store herunter.
- Stellen Sie bei der Installation von MID-Serversicher, dass der Hostcomputer die auf der Dokumentationswebsite ServiceNow veröffentlichten Systemanforderungen für den MID-Server erfüllt oder überschreitet.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Load Balancer-Services [cmdb_ci_lb_service]	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Vollständig qualifizierter Domänenname [fqdn]	Vollständig qualifizierte Domänenname (FQDN) des Lastenausgleichsmoduls. Der DNS-Name
Name [name]	Name des Lastenausgleichsmoduls im folgenden Format: <LB-Name>:<LB-Port>
Back-End-Port [back_end_port]	Port der Instanz
Server-Port [server_port]	Port der Instanz
Port [port]	Port des Lastenausgleichsmoduls
Front-End-Port [front_end_port]	Port des Lastenausgleichsmoduls
Objekt-ID [object_id]	LB-Port
IP-Adresse [ip_address]	IP-Adresse des FQDN
Serverprotokoll [server_protocol]	Protokoll der Instanz.
IP-Adresse [cmdb_ci_ip_address]	
IP-Adresse [ip_address]	Die IP-Adresse des Lastenausgleichsmodul-FQDN
Name [name]	Name des Lastenausgleichsmoduls im folgenden Format: <LB-Name>:<LB-Port>
Netzmaske [netmask]	0.0.0.0

Amazon AWS Cloud-Komponentenerkennung mithilfe von Mustern

Muster für Discovery und Service-Mapping verwendet Muster, um Komponenten der Bereitstellung Amazon AWS Cloud während der Horizontal-Discovery zu erkennen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle
- Visibility Content

Methode für Punkterkennung für AWS CFT-Stapel aktualisieren

Wenn Sie Cloud Provisioning and Governanceverwenden, müssen Sie die Methode *getOperationGR(type)* aktualisieren. Diese Aktualisierung stellt sicher, dass die Punkterkennung die Ressourcen für den AWS CloudFormation Template (CFT)-Stapel nach der Bereitstellung korrekt auflistet. Weitere Informationen zu

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

den Schritten, die zum Aktualisieren dieser Methode erforderlich sind, finden Sie im Knowledge Base-Artikel KB0858437 .

Servicekonto in der AWS-Verwaltungskonsole

Eine AWS-Organisation ist eine Sammlung von AWS-Konten unter einem einzelnen Konto. Cloud-Discovery verweist auf AWS-Organisationen im Assistenten als Verwaltungskonten. Die Mitgliedskonten, die zu einem Verwaltungskonto gehören, werden als Unterkonten bezeichnet.

Hinweis: Cloud-Discovery für AWS-Organisationen wird in einer isolierten GovCloud -Region nicht vollständig unterstützt.

Die Verwendung von Verwaltungskonten hat folgende Vorteile:

Einfaches Füllen von Unterkonten

Nachdem Sie das Verwaltungskonto konfiguriert und die erforderlichen Anmeldeinformationen angegeben haben, können Sie die Verbindung mit dem Konto testen. Wenn der Test erfolgreich ist, gibt Discovery eine Liste der Mitgliedskonten in diesem Verwaltungskonto zurück. In dieser Liste können Sie mindestens ein Unterkonto auswählen, das in die Discovery des Verwaltungskontos aufgenommen werden soll.

(Optional für die Erkennung der gesamten AWS-Organisation) Erkennung von Unterkontenressourcen mithilfe dynamisch bezogener Anmeldeinformationen

Wenn Sie Discovery für Ihre Cloud-Ressourcen ausführen, benötigen Sie keine separaten Anmeldeinformationen für jedes Unterkonto. Der Prozess Cloud-Discovery verarbeitet Anmeldeinformationen automatisch, indem für jeden Unteraccount temporäre Anmeldeinformationen über eine AWS -API abgerufen werden. Sie können die Standardkonfiguration verwenden oder den MID-Server anpassen, um andere Rollen für zusätzliche Steuerungen und Sicherheitseinstellungen zu übernehmen.

IAM-Benutzerrichtlinie in der AWS-Verwaltungskonsole

Zur Verwendung der IAM-Benutzerrichtlinie anstelle von Anmeldeinformationen während der Erkennung konfigurieren Sie den MID Server für AWS IAM-Rollen.

Normalerweise erstellen Sie die IAM-Benutzerrichtlinie für die Bereitstellung von AWS-Ressourcen in Cloud Provisioning and Governance, wie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern beschrieben. Stellen Sie sicher, dass die IAM-Benutzerrichtlinie die folgenden AWS-Ressourcen abdeckt:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
        "elasticloadbalancing:DescribeLoadBalancerPolicyTypes",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeLoadBalancerPolicies",
        "elasticloadbalancing:DescribeInstanceHealth",
        "elasticloadbalancing:DescribeTags",
        "elasticloadbalancing:DescribeLoadBalancerAttributes",
        "account:ListRegions",
        "elasticloadbalancing:Describe*",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "ec2:Describe*",
            "ec2:DescribeNetworkInterfaceAttribute",
            "ec2:DescribeInstanceStatus",
            "ec2:DescribeCustomerGateways",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeHosts",
            "ec2:DescribeImages",
            "ec2:DescribeVpcs",
            "ec2:DescribeAccountAttributes",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeInstanceCreditSpecifications",

                ],
                "Effect": "Allow",
                "Resource": "*"
            }
        ]
}
```

Zugriff auf AWS-Ressourcen konfigurieren

Um ein einzelnen Konto zu erkennen, erstellen Sie in der AWS-Verwaltungskonsole ein IAM-Konto und stellen Sie sicher, dass die Richtlinie „ReadOnlyAccess“ darauf angewendet ist. Um mehrere Mitgliedskonten/untergeordnete Konten zu erkennen, konfigurieren Sie die Anmeldeinformationen wie in Zugriff für AWS-Servicekonten einrichten beschrieben.

Store-App CMDB CI Class Models

Ihre Instanz muss AWS CI-Klassenmodelle durch Bereitstellen der jüngsten Version der Store-App CMDB CI Class Models aus dem ServiceNow Store unterstützen.

Cloudbezogenen CI-Beziehungen aktivieren

Um erkannte Komponenten in Serviceinstanzen aufzunehmen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von Service-Mappingverwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Konfiguration der Tag-basierten Discovery.

Konfigurieren Sie einen Discovery-Zeitplan

Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Unterstützung für AWS -Services in der Region China

Die neueste Version von Muster für Discovery und Service-Mapping unterstützt die Erkennung von AWS -Services in der Region China. Sie können diese Services in den Instanzen Now Platformab Xanadu Patch 3 und Washington DC Patch 9 erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Erkennung von AWS -Services in der Region China erfordert die Verwendung einer Rechenzentrums-URL beim Einrichten eines AWS -Service-Accounts. Beispiel: `https://organizations.cn-northwest-1.amazonaws.com.cn`.

- Weitere Informationen zur Unterstützung von Master-Accounts und Unteraccounts AWS in der Region China finden Sie unter KB1704526 .
- Informationen zum Identifizieren von AWS -Mustern, die in der Region China unterstützt werden, finden Sie in der Tabelle mit Cloud-Discovery-Mustern. Die Spalte **„AWS-Support für die Region China“** enthält für unterstützte Muster einen Wert „Ja“.

Von Discovery während der horizontalen Erkennung erfasste Daten

Ressourcen, die mithilfe des Musters „Amazon AWS - ACL (LP)“ erkannt wurden

Netzwerk-ACL [cmdb_ci_network_acl]

Feld	Beschreibung
Name [name]	Name der Netzwerk-Zugriffssteuerungsliste (ACL)
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird

ACL-Endpunkt [cmdb_ci_endpoint_acl]

Feld	Beschreibung
Name [name]	Name des Endpunkts.
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird

Ressourcen, die mithilfe des Musters „Amazon AWS - Application and Network LB (LP)“ erkannt wurden

Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Feld	Beschreibung
Name [name]	Name des Lastenausgleichsmoduls
Vollständig qualifizierter Domänenname [fqdn]	IP-Adresse des vollständig qualifizierten Domänennamens des Lastenausgleichsmoduls.
Objekt-ID [object_id]	Der Amazon-Ressourcenname (ARN) des Lastenausgleichsmoduls
DNS-Name [dns_name]	Der öffentliche DNS-Name des Lastenausgleichmoduls
Name der kanonischen gehosteten Zone [canonical_hosted_zone_name]	Name der gehosteten Amazon Route 53-Zone, die dem Lastenausgleichsmodul zugeordnet ist.
ID der kanonischen gehosteten Zone [canonical_hosted_zone_id]	ID der gehosteten Amazon Route 53-Zone, die dem Lastenausgleichsmodul zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Load Balancer [cmdb_ci_cloud_load_balancer] (Fortsetzung)

Feld	Beschreibung
Status [state]	Der Status des Lastenausgleichsmoduls
Kurzbeschreibung [short_description]	Eine Verkettung einer Reihe von Attributen für die Lastenausgleichsmodule wie LB ARN, VPC ID, Typ und Zone
Kommentare [comments]	Bezeichner zur internen Verwendung (Löschungsstrategie)

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
IP-Adresse [ip_address]	IP-Adresse des DNS.
Objekt-ID [object_id]	Name des Domain Name System (DNS)
Kommentare [comments]	Bezeichner zur internen Verwendung (Löschungsstrategie)

Ressourcen, die mithilfe des Musters „Amazon AWS - Availability Zone (LP)“ erkannt wurden

Verfügbarkeitszone [cmdb_ci_av availability_zone]

Feld	Beschreibung
Name [name]	Name der Verfügbarkeitszone
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Status [state]	Der Status der Verfügbarkeitszone. Mögliche Werte: available, information, impaired und unavailable.

Ressourcen, die mithilfe des Musters „Amazon AWS - Classic LB (LP)“ erkannt wurden

Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Feld	Beschreibung
Name [name]	Der Name des Lastenausgleichsmoduls
Vollständig qualifizierter Domänenname [fqdn]	Der DNS-Name des Lastenausgleichmoduls
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
DNS-Name [dns_name]	Der DNS-Name des Lastenausgleichmoduls

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Load Balancer [cmdb_ci_cloud_load_balancer] (Fortsetzung)

Feld	Beschreibung
Name der kanonischen gehosteten Zone [canonical_hosted_zone_name]	Der DNS-Name des Lastenausgleichmoduls
ID der kanonischen gehosteten Zone [canonical_hosted_zone_id]	ID der gehosteten Amazon Route 53-Zone für das Lastenausgleichsmodul.

Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]

Feld	Beschreibung
Name [name]	IP-Adresse des Lastenausgleichsmoduls.
Objekt-ID [object_id]	IP-Adresse des Lastenausgleichsmoduls.
IP-Adresse [ip_address]	IP-Adresse des Lastenausgleichsmoduls.
Kommentare [comments]	Kommentare im Zusammenhang mit dem Configuration Item (CI).

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
IP-Adresse [ip_address]	IP-Adresse des DNS.
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Name [name]	Der Name des Pools von Lastenausgleichsmodulen
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]

Feld	Beschreibung
Name [name]	Der Name des Mitglieds des Lastenausgleichsmodul-Pools
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Load Balancer-Service [cmdb_ci_lb_service]

Feld	Beschreibung
Name [name]	Name des Lastenausgleichsmodul-Services
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Port [port]	Der Port, den das Lastenausgleichsmodul abhört
Serviceport [service_port]	Der Port, den die Instanz abhört
Serverprotokoll [service_protocol]	Das für die Weiterleitung von Datenverkehr an Instanzen zu verwendende Protokoll: HTTP, HTTPS, TCP oder SSL
Listener-Protokoll [service_protocol]	Das Transportprotokoll des Lastenausgleichsmoduls, das zur Weiterleitung verwendet wird: HTTP, HTTPS, TCP oder SSL
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Ressourcen, die mithilfe des Musters „Amazon AWS - Customer Gateway (LP)“ erkannt wurden

Kunden-Gateway [cmdb_ci_customer_gateway]

Feld	Beschreibung
Name [name]	Name oder ID, wenn beim Kunden-Gateway kein Name angegeben ist
Objekt-ID [object_id]	ID des Kunden-Gateways
Verbindungstyp [connection_type]	Typ der vom Kunden-Gateway unterstützten VPN-Verbindung

Kunden-Gateway-Endpunkt [cmdb_ci_endpoint_custom_gateway]

Feld	Beschreibung
Name [name]	Name oder ID, wenn beim Kunden-Gateway kein Name angegeben ist
Objekt-ID [object_id]	ID des Kunden-Gateways

Ressourcen, die mithilfe des Musters „Amazon AWS - Executable Template (LP)“ erkannt wurden

Image [cmdb_ci_os_template]

Feld	Beschreibung
Name [name]	Name des Image. Zum Beispiel: CentOS 7.0-64 Minimal for VSI

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Image [cmdb_ci_os_template] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Image-Typ [image_type]	Typ des Betriebssystem-Image
Root-Gerätetyp [root_device_type]	Gerätename des Root-Gerätevolumes (beispielsweise / dev/sda1)
Image-Quelle [image_source]	Quelle des Betriebssystem-Image
Gast-Betriebssystem [guest_os]	Betriebssystem, das sekundär zum Betriebssystem ist
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktiviert die Discovery von Cloud-BS-Images.

Im Abschnitt „Mustererweiterung“ erkennen Sie die Bring Your Own License (BYOL) oder die enthaltenen Lizenzen für virtuelle Windows-Computer (VMs) und RHEL-VMs.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Der Schlüssel ist eine der Optionen: • Windows_OS_License_Type_automatic • RHEL_OS_License_Type_automatic • SQL_Server_Lizenz_Typ_automatisch
Wert [value]	Der Wert ist eine der Optionen: • BYOL • Lizenz enthalten
CI [ci]	Verweis auf den Datensatz der VM-Instanz.
Klasse	Die Klasse ist *Image* oder *Cloud Image*.

Ressourcen, die mithilfe des Musters „Amazon AWS - Hardware Type (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hardwaretyp [cmdb_ci_compute_template]

Feld	Beschreibung
Name [name]	Name dieses Image
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Kern [core]	Die Standardanzahl der Kerne für den Instanztyp
Arbeitsspeicher – MB [memory_mb]	Speichergröße, die dieser Vorlage zugewiesen ist
vCPIs [vCPUs]	Anzahl der dieser Vorlage zugewiesenen CPU-Kerne
Lokaler Speicher – GB [local_storage_gb]	Speicher, der dieser Vorlage zugewiesen ist

Hinweis: Unter bestimmten Umständen stellen Sie möglicherweise eine ungewöhnlich große Anzahl von Datensätzen in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] fest. In solchen Fällen können Sie die erkannten Hardwaretypen in der Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type] speichern. Weitere Informationen finden Sie unter Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren.

Ressourcen, die mithilfe des Musters „Amazon AWS - Host (LP)“ erkannt wurden

Cloud-Host [cmdb_ci_cloud_host]

Feld	Beschreibung
Name [name]	Name dieses Hosts
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Anzahl CPU-Kerne [cpu_core_count]	Anzahl der Hostkerne
Status [state]	Aktueller Status des Hosts
Hosttyp [host_type]	Typ des Hosts (instanceFamily)
Cloud-Anbieter [cloud_vendor]	Anbieter der Cloud: AWS
Virtuell [virtual]	Virtueller Host: False

Ressourcen, die mithilfe des Musters „Amazon AWS - Internet Gateway (LP)“ erkannt wurden

Internet-Gateway [cmdb_ci_internet_gateway]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das Internet-Gateway kein Name angegeben ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Internet-Gateway [cmdb_ci_internet_gateway] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	ID des Internet-Gateways

Internet-Gateway-Endpunkt [cmdb_ci_endpoint_intgateway]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das Internet-Gateway kein Name angegeben ist.
Objekt-ID [object_id]	ID des Internet-Gateways

Ressourcen, die mithilfe des Musters „Amazon AWS - IP Address (LP)“ erkannt wurden

IP-Adresse [cmdb_ci_cloud_ip_address]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für die Netzwerkschnittstelle kein Name angegeben ist
IP-Adresse [ip_address]	Die Adresse der Elastic IP-Adresse, die an die Netzwerkschnittstelle gebunden ist (falls verfügbar), andernfalls die Private IP
Objekt-ID [object_id]	Die ID der Netzwerkschnittstelle
Öffentlicher DNS [public_dns]	Der öffentliche DNS-Name, falls verfügbar
Private IP-Adresse [private_ip]	Die IPv4-Adresse der Netzwerkschnittstelle im Subnetz
Instanz-ID [instance_id]	Die ID der Instanz

Ressourcen, die mithilfe des Musters „Amazon AWS - Key Pair (LP)“ erkannt wurden

Cloud-Schlüsselpaar [cmdb_ci_cloud_key_pair]

Feld	Beschreibung
Name [name]	Der Name des Schlüsselpaars
Objekt-ID [object_id]	Die ID des Schlüsselpaars
Fingerabdruck [finger_print]	Wenn Sie das Schlüsselpaar mit CreateKeyPair erstellt haben, ist dies der SHA-1-Digest des DER-codierten privaten Schlüssels. Wenn Sie ImportKeyPair verwendet haben, um AWS den öffentlichen Schlüssel bereitzustellen, ist dies

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Schlüsselpaar [cmdb_ci_cloud_key_pair] (Fortsetzung)

Feld	Beschreibung
	der Fingerabdruck des öffentlichen MD5-Schlüssels, wie in Abschnitt 4 von RFC 4716 angegeben.

Ressourcen, die mithilfe des Musters „Amazon AWS - LB Pool (LP)“ erkannt wurden

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Name [name]	Der Name des Pools von Lastenausgleichsmodulen
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Ressourcen, die mithilfe des Musters „Amazon AWS - LB Service (LP)“ erkannt wurden

Load Balancer-Service [cmdb_ci_lb_service]

Feld	Beschreibung
Name [name]	Name des Lastenausgleichsmodul-Services
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Port [port]	Der Port, den das Lastenausgleichsmodul abhört
Serviceport [service_port]	Der Port, den die Instanz abhört
Serverprotokoll [service_protocol]	Das für die Weiterleitung von Datenverkehr an Instanzen zu verwendende Protokoll: HTTP, HTTPS, TCP oder SSL
Listener-Protokoll [service_protocol]	Das Transportprotokoll des Lastenausgleichsmoduls, das zur Weiterleitung verwendet wird: HTTP, HTTPS, TCP oder SSL
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Ressourcen, die mithilfe des Musters „Amazon AWS - NAT Gateway (LP)“ erkannt wurden

NAT-Gateway [cmdb_ci_nat_gateway]

Feld	Beschreibung
Name [name]	Name des NAT-Gateways
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Installationsstatus [install_status]	Bereitstellungsstatus des NAT-Gateway.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

NAT-Endpunkt [cmdb_ci_endpoint_nat]

Feld	Beschreibung
Name [name]	Der Name des NAT-Endpunkts
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird

Ressourcen, die mithilfe des Musters „Amazon AWS - Network (LP)“ erkannt wurden

Cloud-Netzwerk [cmdb_ci_network]

Feld	Beschreibung
Name [name]	Name des VPC-Netzwerks (Virtual Private Cloud)
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Status [state]	Der aktuelle Status der VPC: ausstehend (pending) oder verfügbar (available).
CIDR [cidr]	CIDR-Darstellung des Subnetzes. Beispiel: 10.0.0.0/24
Installationsstatus [install_status]	Bereitstellungsstatus der Ressource

Ressourcen, die mithilfe des Musters „Amazon AWS - NIC (LP)“ erkannt wurden

Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für die Netzwerkschnittstelle kein Name angegeben ist
Objekt-ID [object_id]	Die ID der Netzwerkschnittstelle
Status [state]	Der Status der Netzwerkschnittstelle Gültige Werte: verfügbar (available), zugeordnet (associated), hängt an (attaching), in Gebrauch (in-use) oder trennt (detaching).
Private IP [private_ip]	Die IPv4-Adresse der Netzwerkschnittstelle im Subnetz
IP-Adresse [ip_address]	Die Adresse der Elastic IP-Adresse, die an die Netzwerkschnittstelle gebunden ist (falls verfügbar), andernfalls die Private IP
Öffentliche IP [public_ip]	Die Adresse der Elastic IP-Adresse, die an die Netzwerkschnittstelle gebunden ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]

Feld	Beschreibung
Name [name]	IP-Adresse des Lastenausgleichsmoduls.
Objekt-ID [object_id]	Die Adresse der Elastic IP-Adresse, die an die Netzwerkschnittstelle gebunden ist (falls verfügbar), andernfalls die Private IP
IP-Adresse [ip_address]	Die Adresse der Elastic IP-Adresse, die an die Netzwerkschnittstelle gebunden ist (falls verfügbar), andernfalls die Private IP
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

VNIC-Endpunkt [cmdb_ci_endpoint_vnic]

Feld	Beschreibung
Name [name]	Der Name des VNIC-Endpunkts (Virtual Network Machine Interface)
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
IP-Adresse [ip_address]	Die Adresse der Elastic IP-Adresse, die an die Netzwerkschnittstelle gebunden ist (falls verfügbar), andernfalls die Private IP
Host [host]	Die ID der Instanz

Ressourcen, die mithilfe des Musters „Amazon AWS - Owned Template (LP)“ erkannt wurden

Image [cmdb_ci_os_template]

Feld	Beschreibung
Name [name]	Name des Image. Zum Beispiel: CentOS 7.0-64 Minimal for VSI
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Image-Typ [image_type]	Typ des Betriebssystem-Image
Root-Gerätetyp [root_device_type]	Der Typ des vom AMI verwendeten Root-Geräts. Das AMI kann ein EBS-Volume oder ein Instanzspeichervolume verwenden.
Image-Quelle [image_source]	Quelle des Betriebssystem-Image
Gast-Betriebssystem [guest_os]	Betriebssystem, das sekundär zum Betriebssystem ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Image [cmdb_ci_os_template] (Fortsetzung)

Feld	Beschreibung
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktiviert die Discovery von Cloud-BS-Images.

Im Abschnitt „Mustererweiterung“ erkennen Sie die Bring Your Own License (BYOL) oder die enthaltenen Lizenzen für Windows-VMs und RHEL-VMs.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Der Schlüssel ist eine der Optionen: • Windows_OS_License_Type_automatic • RHEL_OS_License_Type_automatic • SQL_Server_Lizenz_Typ_automatisch
Wert [value]	Der Wert ist eine der Optionen: • BYOL • Lizenz enthalten
CI [ci]	Verweis auf den Datensatz der VM-Instanz.
Klasse	Die Klasse ist *Image* oder *Cloud Image*.

Ressourcen, die mithilfe des Musters „Amazon AWS - Public IP Address (LP)“ erkannt wurden

Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]

Feld	Beschreibung
Name [name]	Der Name oder die Zuteilungs-ID, wenn für die öffentliche IP-Adresse kein Name angegeben ist
Objekt-ID [object_id]	Die ID, die die Zuordnung der Adresse für die Verwendung mit EC2-VPC darstellt
Öffentliche IP-Adresse [public_ip]	Die Elastic IP-Adresse

Ressourcen, die mithilfe des Musters „Amazon AWS - Route Table (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weiterleitungstabelle [cmdb_ci_route_table]

Feld	Beschreibung
Name [name]	Die ID der Weiterleitungstabelle
Status [state]	Wenn die Weiterleitungstabelle erkennbar ist, ist der Wert verfügbar.
Objekt-ID [object_id]	Name oder ID, wenn für die Weiterleitungstabelle kein Name angegeben ist

Endpunkt der Weiterleitungstabelle [cmdb_ci_route_table]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für die Weiterleitungstabelle kein Name angegeben ist
Objekt-ID [object_id]	Die ID der Weiterleitungstabelle

Ressourcen, die mithilfe des Musters „Amazon AWS - Security Group (LP)“ erkannt wurden

Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Feld	Beschreibung
Name [name]	Der Name der Sicherheitsgruppe
Objekt-ID [object_id]	Die ID der Sicherheitsgruppe

Ressourcen, die mithilfe des Musters „Amazon AWS - Storage (LP)“ erkannt wurden

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Status [state]	Der Volumestatus. Die folgenden Werte sind gültig: wird erstellt (creating), verfügbar (available), in Gebrauch (in-use), löscht (deleting), gelöscht (deleted) oder Fehler (error).
Speichertyp [storage_type]	Beispiel: hartcodierter Wert „Block“.
Volume-ID [volume_id]	Der Volumetyp. Beispiel: gp2 für Allzweck-SSD, io1 für bereitgestellte IOPS-SSD, st1 für durchsatzoptimierte Festplatte, sc1 für kalte Festplatte oder „Standard“ für magnetische Volumes.
Name [name]	Name oder ID, wenn für das Volume kein Name angegeben ist
Größe in Byte [size_bytes]	Die Größe des Volumes (Byte)
Objekt-ID [object_id]	Die ID des Volumes

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Block-Endpunkt [cmdb_ci_endpoint_block]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das Volume kein Name angegeben ist
Objekt-ID [object_id]	Die ID des Volumes

Ressourcen, die mit dem Muster Amazon AWS - Sub Account (LP) erkannt wurden

Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Feld	Beschreibung
Konto-ID [account_id]	Eindeutiger Bezeichner (ID) des Accounts.
Objekt-ID [object_id]	Eindeutiger Bezeichner (ID) des Accounts.
Rechenzentrumstyp [datacenter_type]	Hartcodierter Wert: cmdb_ci_aws_datacenter.
Name [name]	Anwenderfreundlicher Name des Accounts.
Ist Master-Konto [is_master_account]	Boolesches Attribut, das angibt, ob dies der Verwaltungsaccount ist oder nicht.
Account-E-Mail [account_email]	E-Mail-Adresse des Service-Accounts AWS.

Ressourcen, die mithilfe des Musters „Amazon AWS - Subnet (LP)“ erkannt wurden

Cloud-Subnetz [cmdb_ci_cloud_subnet]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das Subnetz kein Name angegeben ist
Objekt-ID [object_id]	Die ID des Subnetzes
CIDR [cidr]	Der IPv4 CIDR-Block, der dem Subnetz zugewiesen ist
Verfügbare IP-Anzahl [available_ip_count]	Die Anzahl der nicht verwendeten privaten IPv4-Adressen im Subnetz. Die IPv4-Adressen für angehaltene Instanzen gelten als nicht verfügbar.
Status [state]	Der aktuelle Status des Subnetzes. Die folgenden Werte sind gültig: ausstehend (pending) oder verfügbar (available).

Ressourcen, die mithilfe des Musters „Amazon AWS – Virtual Server (LP)“ erkannt wurden

VM-Instanz [cmdb_ci_vm_instance]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für die Instanz kein Name angegeben ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VM-Instanz [cmdb_ci_vm_instance] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	Die ID der Instanz
Arbeitsspeicher [memory]	Für die Instanz verfügbare Arbeitsspeicher (MBs)
CPUs [cpus]	Anzahl der für die Instanz verfügbaren CPUs
Datenträger [disks]	Anzahl der Datenträger, die an die Instanz angeschlossen sind
ID der VM-Instanz [vm_inst_id]	Die ID der Instanz
Status [state]	Der aktuelle Status der Instanz
IP-Adresse [ip_address]	ID-Adresse der VM-Instanz
Netzwerkadapter [network_adapters]	Anzahl der für die Instanz verfügbaren NICs

Hinweis:

Wenn Sie eine stillgelegte VM erneut aktiviert haben und möchten, dass ihr aktiver Status in den Feldern **„Betriebsstatus“** und **„Installationsstatus“** in der Tabelle „VM-Instanz“ [cmdb_ci_vm_instance] genau angezeigt wird, legen Sie die Eigenschaft *sn_itom_pattern.discover_aws_instance_statuses* MID-Server auf **true**fest. Beachten Sie, dass diese Einstellung zusätzliche API-Aufrufe umfasst – einen für jede Seite der Musterausführung – was sich auf die Leistung auswirken kann, wenn Sie eine große Anzahl von VMs verwalten.

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
IP-Adresse [ip_address]	IP-Adresse des DNS.
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Subnetzendpunkt [cmdb_ci_endpoint_subnet]

Feld	Beschreibung
Name [name]	Der Name des Subnetzendpunkts
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird

Image [cmdb_ci_os_template]

Feld	Beschreibung
Name [name]	Name des Image. Zum Beispiel: CentOS 7.0-64 Minimal for VSI

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Image [cmdb_ci_os_template] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von Amazon AWS Cloud für diese Ressource zugewiesen wird
Image-Typ [image_type]	Typ des Betriebssystem-Image
Root-Gerätetyp [root_device_type]	Der Typ des vom AMI verwendeten Root-Geräts. Das AMI kann ein EBS-Volume oder ein Instanzspeichervolume verwenden.
Image-Quelle [image_source]	Quelle des Betriebssystem-Image
Gast-Betriebssystem [guest_os]	Betriebssystem, das sekundär zum Betriebssystem ist
Kommentare [comments]	Kommentare im Zusammenhang mit dem CI.

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktiviert die Discovery von Cloud-BS-Images.

Speicherzuordnung [cmdb_ci_storage_mapping]

Feld	Beschreibung
Name [name]	Die ID des Volumes
Objekt-ID [object_id]	Die ID des Volumes
Bereitstellungspunkt [mount_point]	Der Gerätename, z. B. /dev/sdh oder xvdh
Host [host]	Die öffentliche IPv4-Adresse, die der Instanz zugewiesen wurde, falls zutreffend
Zuordnungstyp [mapping_type]	Der Typ des vom AMI verwendeten Root-Geräts Das AMI kann ein EBS-Volume oder ein Instanzspeichervolume verwenden.

Ressourcen, die mithilfe des Musters „Amazon AWS - VPN Connections (LP)“ erkannt wurden

VPN-Verbindung [cmdb_ci_vpn_connection]

Feld	Beschreibung
Name [name]	Name des Projekts, das für die Erkennung verwendet wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VPN-Verbindung [cmdb_ci_vpn_connection] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	Name oder ID, wenn für die VPN-Verbindung kein Name angegeben ist
Status [state]	Der aktuelle Status der VPN-Verbindung. Die folgenden Werte sind gültig: ausstehend (pending), verfügbar (available), löscht (deleting) oder gelöscht (deleted).

Ressourcen, die mithilfe des Musters „Amazon AWS - VPN Gateway (LP)“ erkannt wurden

Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das VPN-Gateway kein Name angegeben ist
Objekt-ID [object_id]	Die ID des Virtual Private Gateway
Verbindungstyp [connection_type]	Der Typ der vom Virtual Private Gateway unterstützten VPN-Verbindung

Virtual Private Gateway-Endpunkt [cmdb_ci_endpoint_vpg]

Feld	Beschreibung
Name [name]	Name oder ID, wenn für das VPN-Gateway kein Name angegeben ist
Objekt-ID [object_id]	Die ID des Virtual Private Gateway
Verbindungstyp [connection_type]	Der Typ der vom Virtual Private Gateway unterstützten VPN-Verbindung

Ressourcen, die mit Amazon AWS erkannt wurden – Organisationsmuster erkennen

Cloud-Organisationen [cmdb_ci_cloud_org]

Feld	Beschreibung
Name [name]	Der eindeutige Bezeichner (ID) einer Organisation.
Objekt-ID [object_id]	Der Amazon-Ressourcenname (ARN) des Accounts, der als Verwaltungsaccount für die Organisation festgelegt ist.
Stamm-ID [root_id]	Der eindeutige Bezeichner (ID) einer Organisation.
Master-E-Mail [master_email]	Die E-Mail-Adresse, die dem Account AWS zugeordnet ist, der als Verwaltungsaccount für die Organisation festgelegt ist.
Installationsstatus [install_status]	Der Installationsstatus der Organisation basierend auf dem Status der verfügbaren Richtlinientypen
Betriebsstatus [operational_status]	Der Betriebsstatus der Organisation basierend auf dem Status der verfügbaren Richtlinientypen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen, die mit dem Muster Amazon AWS - Organisationseinheiten (LP) erkannt wurden

AWS-Organisationseinheit [cmdb_ci_aws_org_unit]

Feld	Beschreibung
Name [name]	Der anwenderfreundliche Name der Organisationseinheit (OE).
Objekt-ID [object_id]	Der eindeutige Bezeichner (ID), der dieser OE zugeordnet ist. Die ID ist für die Organisation eindeutig.
Organisations-ID [aws_org_id]	Der eindeutige Bezeichner (ID), der dieser OE zugeordnet ist. Die ID ist für die Organisation eindeutig.
ID der übergeordneten Org.-Einheit [org_unit_parent_id]	Die ID des Stamms oder der unmittelbar übergeordneten OE.

Events, die während der horizontalen Erkennung mithilfe von Discovery erkannt wurden

Discovery verwendet Muster, um Events zu suchen, die für Amazon AWS Cloud-Komponenten erstellt wurden. Wenn Events vorhanden sind, die auf eine Statusänderung in einer der Amazon AWS Cloud-Komponenten hinweisen, wird die Erkennung von Amazon AWS Cloud-Komponenten anhand der Muster ausgelöst.

Muster, die für die Event-Erkennung verwendet wurden

Muster	CI
Amazon AWS Virtual Server Events	VM-Instanz [cmdb_ci_vm_instance]
Amazon AWS Security Group Events	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]
Amazon AWS Subnet Events	Cloud-Subnetz [cmdb_ci_cloud_subnet]
Amazon AWS Storage Events	Speichervolume [cmdb_ci_storage_volume]
Amazon AWS Network Events	Cloud-Netzwerk [cmdb_ci_network]
Amazon AWS Classic LB Events	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Amazon AWS Application and Network LBs Events	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

CI-Beziehungen

Beziehungen, die mithilfe des Musters „Amazon AWS - ACL (LP)“ erkannt wurden

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Enthält::Enthalten in	Netzwerk-ACL [cmdb_ci_network_acl]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Netzwerk-ACL [cmdb_ci_network_acl]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Netzwerk-ACL [cmdb_ci_network_acl]	Endpunkt implementieren in::Endpunkt implementieren von	Netzwerk-ACL [cmdb_ci_network_acl]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Endpunkt verwenden an::Endpunkt verwenden von	Netzwerk-ACL [cmdb_ci_network_acl]

Beziehungen, die mithilfe des Musters „Amazon AWS - Application and Network (LP)“ erkannt wurden

CI	Beziehung	CI
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Enthält::Enthalten in	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Enthält::Enthalten in	DNS-Name [cmdb_ci_dns_name]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Enthält::Enthalten in	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Beziehungen, die mithilfe des Musters „Amazon AWS - Availability Zone (LP)“ erkannt wurden

CI	Beziehung	CI
AWS-Rechenzentrum [cmdb_ci_aws_datacenter]	Enthält::Enthalten in	Verfügbarkeitszone [cmdb_ci_av availability_zone]

Beziehungen, die mithilfe des Musters „Amazon AWS - Classic LB (LP)“ erkannt wurden

CI	Beziehung	CI
Load Balancer-Service [cmdb_ci_lb_service]	Gehostet auf::Hostet	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Enthält::Enthalten in	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Load Balancer-Pool [cmdb_ci_lb_pool]	Gehostet auf::Hostet	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Load Balancer-Pool [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Enthält::Enthalten in	DNS-Name [cmdb_ci_dns_name]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Eigentümer von::Eigentum von	Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Enthält::Enthalten in	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Beziehungen, die mithilfe des Musters „Amazon AWS - Customer Gateway (LP)“ erkannt wurden

CI	Beziehung	CI
Kunden-Gateway [cmdb_ci_customer_gateway]	Gehostet auf::Hostet	VM-Instanz [cmdb_ci_instance]
Kunden-Gateway [cmdb_ci_customer_gateway]	Endpunkt implementieren in::Endpunkt implementieren von	Kunden-Gateway [cmdb_ci_endpoint_cust_gateway]

Beziehungen, die mithilfe des Musters „Amazon AWS - Executable Template (LP)“ erkannt wurden

CI	Beziehung	CI
Image [cmdb_ci_os_template]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Hardware Type (LP)“ erkannt wurden

CI	Beziehung	CI
Hardwaretyp [cmdb_ci_compute_template]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Host (LP)“ erkannt wurden

CI	Beziehung	CI
Host [cmdb_ci_cloud_host]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
VM-Instanz [cmdb_ci_vm_instance]	Wird ausgeführt auf::Wird ausgeführt	Host [cmdb_ci_cloud_host]

Beziehungen, die mithilfe des Musters „Amazon AWS - Internet Gateway (LP)“ erkannt wurden

CI	Beziehung	CI
Internet-Gateway [cmdb_ci_internet_gateway]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Internet-Gateway [cmdb_ci_internet_gateway]	Endpunkt implementieren in::Endpunkt implementieren von	Internet-Gateway - EP [cmdb_ci_endpoint_intgateway]
Cloud-Netzwerk [cmdb_ci_network]	Endpunkt verwenden an::Endpunkt verwenden von	Internet-Gateway - EP [cmdb_ci_endpoint_intgateway]

Beziehungen, die mithilfe des Musters „Amazon AWS - IP Address (LP)“ erkannt wurden

CI	Beziehung	CI
Cloud-Schlüsselpaar [cmdb_ci_cloud_key_pair]	Enthält::Enthalten in	IP-Adresse [cmdb_ci_cloud_ip_address]

Beziehungen, die mithilfe des Musters „Amazon AWS - Key Pair (LP)“ erkannt wurden

CI	Beziehung	CI
Server [cmdb_ci_server]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - LB Pool (LP)“ erkannt wurden

CI	Beziehung	CI
Load Balancer-Pool [cmdb_ci_lb_pool]	Gehostet auf::Hostet	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Beziehungen, die mithilfe des Musters „Amazon AWS - LB Service (LP)“ erkannt wurden

CI	Beziehung	CI
Load Balancer-Service [cmdb_ci_lb_service]	Gehostet auf::Hostet	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Beziehungen, die mithilfe des Musters „Amazon AWS - NAT Gateway (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
NAT-Gateway [cmdb_ci_nat_gateway]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
NAT-Gateway [cmdb_ci_nat_gateway]	Endpunkt implementieren in::Endpunkt implementieren von	NAT-EP [cmdb_ci_endpoint_nat]
Netzwerk [cmdb_ci_network]	Endpunkt verwenden an::Endpunkt verwenden von	NAT-EP [cmdb_ci_endpoint_nat]

Beziehungen, die mithilfe des Musters „Amazon AWS - Network (LP)“ erkannt wurden

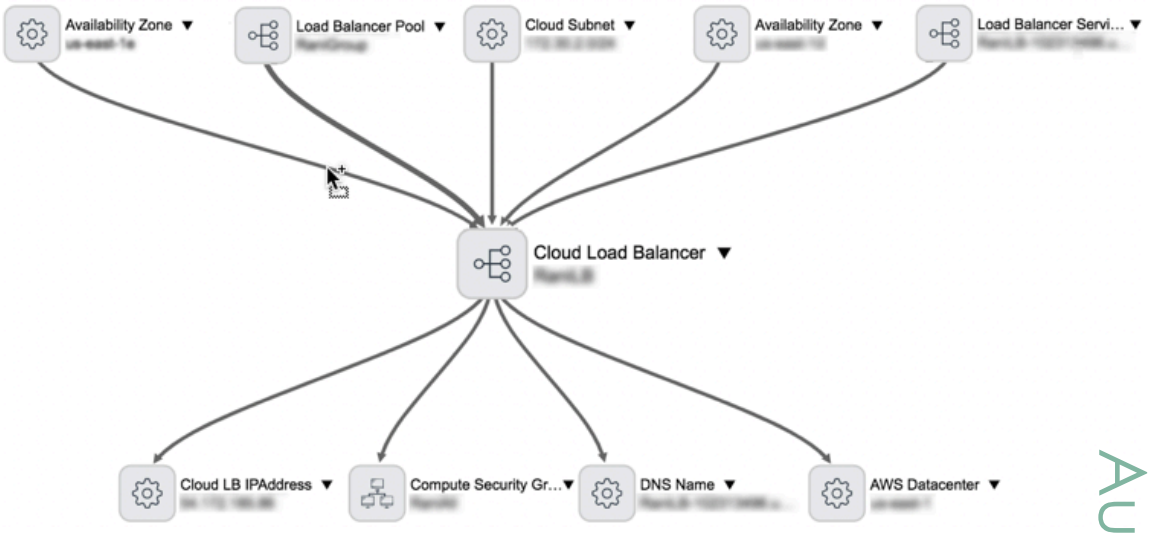
CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - NIC (LP)“ erkannt wurden

CI	Beziehung	CI
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Eigentümer von::Eigentum von	Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]
VM-Instanz [cmdb_ci_vm_instance]	Endpunkt verwenden an::Endpunkt verwenden von	VNIC-Endpunkt [cmdb_ci_endpoint_vnic]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Enthält::Enthalten in	NIC [cmdb_ci_nic]
VNIC-Endpunkt [cmdb_ci_endpoint_vnic]	Endpunkt implementieren in::Endpunkt implementieren von	NIC [cmdb_ci_nic]
NIC [cmdb_ci_nic]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängigkeitsansichten, die das Cloud-Lastenausgleichsmodul und die verbundene Komponenten anzeigen



Beziehungen, die mithilfe des Musters „Amazon AWS - Owned Template (LP)“ erkannt wurden

CI	Beziehung	CI
Image [cmdb_ci_os_template]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Public IP Address (LP)“ erkannt wurden

CI	Beziehung	CI
Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Route Table (LP)“ erkannt wurden

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Enthält::Enthalten in	Weiterleitungstabelle [cmdb_ci_route_table]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Endpunkt verwenden an::Endpunkt verwenden von	Endpunkt der Weiterleitungstabelle [cmdb_ci_route_table]
Weiterleitungstabelle [cmdb_ci_route_table]	Endpunkt implementieren in::Endpunkt implementieren von	Endpunkt der Weiterleitungstabelle [cmdb_ci_route_table]

Beziehungen, die mithilfe des Musters „Amazon AWS - Security Group (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Enthält::Enthalten in	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]
Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Storage Volume (LP)“ erkannt wurden

CI	Beziehung	CI
VM-Instanz [cmdb_ci_instance]	Endpunkt verwenden an::Endpunkt verwenden von	Block-Endpunkt [cmdb_ci_endpoint_block]
Block-Endpunkt [cmdb_ci_endpoint_block]	Endpunkt implementieren in::Endpunkt implementieren von	Speichervolume [cmdb_ci_storage_volume]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Speichervolume [cmdb_ci_storage_volume]
Speichervolume [cmdb_ci_storage_volume]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - Subnet (LP)“ erkannt wurden

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Enthält::Enthalten in	Cloud-Subnetz [cmdb_ci_cloud_subnet]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	Cloud-Subnetz [cmdb_ci_cloud_subnet]

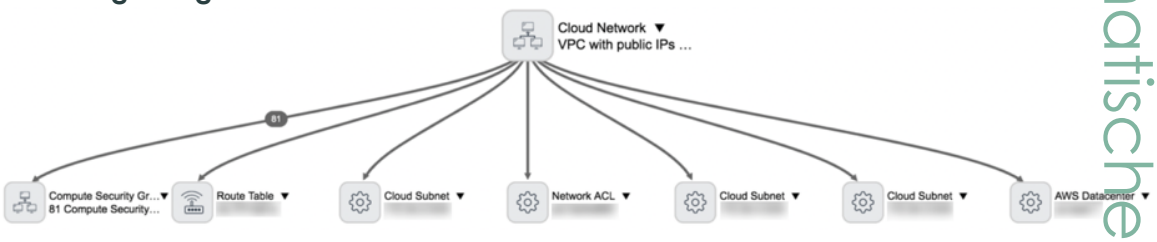
Beziehungen, die mithilfe des Musters „Amazon AWS – Virtual Server (LP)“ erkannt wurden

CI	Beziehung	CI
Netzwerk [cmdb_ci_network]	Enthält::Enthalten in	Cloud-Subnetz [cmdb_ci_cloud_subnet]
Cloud-Subnetz [cmdb_ci_cloud_subnet]	Endpunkt implementieren in::Endpunkt implementieren von	Subnetzendpunkt [cmdb_ci_endpoint_subnet]
Verfügbarkeitszone [cmdb_ci_av availability_zone]	Enthält::Enthalten in	VM-Instanz [cmdb_ci_vm_instance]
VM-Instanz [cmdb_ci_vm_instance]	Endpunkt verwenden	Subnetzendpunkt [cmdb_ci_endpoint_subnet]

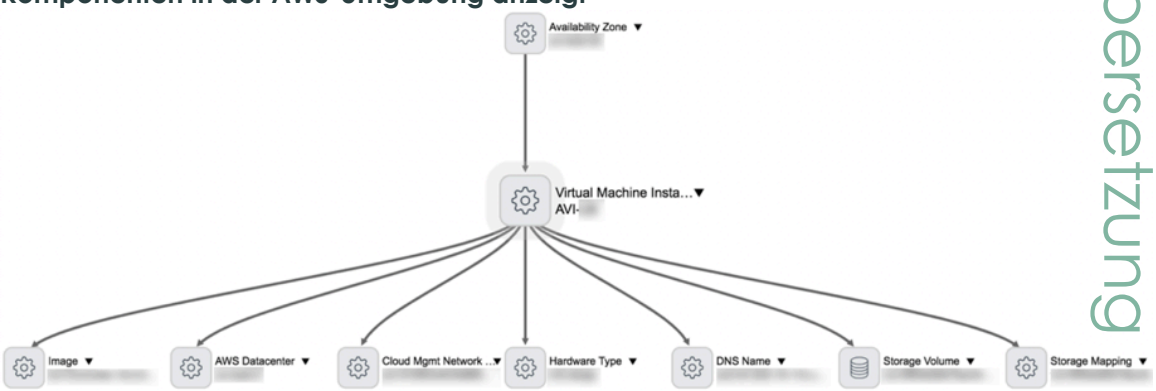
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
	an::Endpunkt verwenden von	
VM-Instanz [cmdb_ci_vm_instance]	Enthält::Enthalten in	Speicherzuordnung [cmdb_ci_storage_mapping]
VM-Instanz [cmdb_ci_vm_instance]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
VM-Instanz [cmdb_ci_vm_instance]	Bereitgestellt von::Bereitgestellt	Hardwaretyp [cmdb_ci_compute_template]
VM-Instanz [cmdb_ci_vm_instance]	Bereitgestellt von::Bereitgestellt	Image [cmdb_ci_os_template]
VM-Instanz [cmdb_ci_vm_instance]	Enthält::Enthalten in	DNS-Name [cmdb_ci_dns_name]
Image [cmdb_ci_os_template]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Abhängigkeitsansichten, die Komponenten anzeigen, die in der AWS-Umgebung mit dem Cloud-Netzwerk verbunden sind



Abhängigkeitsansichten, die die VM und die verbundenen Komponenten in der AWS-Umgebung anzeigt



Beziehungen, die mithilfe des Musters „Amazon AWS - VPN Connections (LP)“ erkannt wurden

CI	Beziehung	CI
Kunden-Gateway [cmdb_ci_customer_gateway]	Enthält::Enthalten in	VPN-Verbindung [cmdb_ci_vpn_connection]
Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]	Enthält::Enthalten in	VPN-Verbindung [cmdb_ci_vpn_connection]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
VPN-Verbindung [cmdb_ci_vpn_connection]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Beziehungen, die mithilfe des Musters „Amazon AWS - VPN Gateway (LP)“ erkannt wurden

CI	Beziehung	CI
Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]	Endpunkt implementieren in::Endpunkt implementieren von	Virtual Private Gateway-Endpunkt [cmdb_ci_endpoint_vpg]
Netzwerk [cmdb_ci_network]	Endpunkt verwenden an::Endpunkt verwenden von	Virtual Private Gateway-Endpunkt [cmdb_ci_endpoint_vpg]

Beziehungen, die mit dem Muster Amazon AWS - Organisationseinheiten (LP) erkannt wurden

CI	Beziehung	CI
Cloud-Organisation [cmdb_ci_cloud_org]	Enthält::Enthalten in	AWS-Organisationseinheit [cmdb_ci_aws_org_unit]
AWS-Organisationseinheit [cmdb_ci_aws_org_unit]	Enthält::Enthalten in	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
Schlüsselwert [cmdb_key_value]	Nur Referenz	AWS-Organisationseinheit [cmdb_ci_aws_org_unit]

Services, die mithilfe von Mustern erkannt wurden

Bei der horizontalen Erkennung werden EC2- und VPC-Services gefunden, die auf AWS-Ressourcen ausgeführt werden.

Services, die von Discovery mithilfe von Mustern erkannt wurden

Servicename	CI-Klasse	Muster
AWS::EC2::SecurityGroup	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]	Amazon AWS Security Group Events
AWS::EC2::Subnet	Cloud-Subnetz [cmdb_ci_cloud_subnet]	Amazon AWS Subnet Events
AWS::EC2::VPC	Cloud-Netzwerk [cmdb_ci_network]	Amazon AWS Network Events
AWS::EC2::Instance	VM-Instanz [cmdb_ci_vm_instance]	Amazon AWS Virtual Server Events

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Services, die von Discovery mithilfe von Mustern erkannt wurden (Fortsetzung)

Servicename	CI-Klasse	Muster
EQS::EC2::Volume	Speichervolume [cmdb_ci_storage_volume]	Amazon AWS Elastic Block Storage
AWS::ElasticLoadBalancingV2::LoadBalancer	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Amazon AWS Application und Network LBs Events
AWS::ElasticLoadBalancing::LoadBalancer	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Amazon AWS Classic LBs Events

Daten, die von Service-Mapping während der tagbasierten Erkennung erfasst wurden

Service-Mapping verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren

Aktivieren Sie die Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type], um die vordefinierten VM-Hardwaretyp-Datensätze für Amazon AWS Cloud, Microsoft Azure Cloud und Google Cloud Platform (GCP)zu speichern. Diese Klassenerweiterung trägt dazu bei, die Duplizierung der VM-Hardwaretyp-Datensätze in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] zu verhindern, was wiederum die Leistung von Discovery und anderer zugehöriger Flows verbessert.

Vorbereitungen

- Stellen Sie sicher, dass das Plugin Muster für Discovery und Service-Mapping (com.sn_itom_pattern) Version 1.0.75 installiert ist.
- Stellen Sie sicher, dass Version 1.24.0 des Plugins CMDB CI-Klassenmodelle – Store-App (sn_cmdb_ci_class) installiert ist.
- Vergewissern Sie sich, dass der Anwendungsbereich Discovery und die Anwendung Service-Mapping ist.

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Jeder Cloud-Service Provider bietet mehrere vordefinierte VM-Hardwaretypen, z. B. t1.micro (AWS), usw. Sie können auch Ihren eigenen VM-Hardwaretyp erstellen. Standardmäßig werden die erkannten VM-Hardwaretypen von Discovery in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] gespeichert. Diese Tabelle ist eine abhängige Klasse der Klasse cmdb_ci_logical_datacenter. Dieses Modell führt wie folgt zur Erstellung einer Reihe von doppelten Datensätzen für jeden erkannten VM-Hardwaretyp:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anzahl der Datensätze für jeden erkannten VM-Hardwaretyp = Anzahl der Servicekonten * Anzahl der logischen Rechenzentren.

Daher kann Discovery, wenn Ihre Organisation Hunderte von Servicekonten hat, möglicherweise Tausende von VM-Hardwaretyp-Datensätzen erstellen, was wiederum die Erkennung und andere zugehörige Flows verlangsamt.

Beispiel: Das AWS-Konto einer Organisation enthält eine t1.micro-VM. Die Organisation verfügt über 3.000 Servicekonten und 10 LRZ (z. B. West-USA). Während des nächsten Scans erkennt Discovery den VM-Hardwaretyp und erstellt 30.000 t1.micro-VM-Datensätze in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template].

Sie können diese Probleme vermeiden, indem Sie die vordefinierten VM-Hardwaretypen AWS und GCP in der Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type] speichern. Die vorhandene Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] wird von dieser Tabelle erweitert. Sie ist jedoch nicht an ein LRZ oder ein Servicekonto gebunden. Daher wird der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] von Discovery auch dann keine große Anzahl von VM-Hardwaretyp-Datensätzen hinzugefügt, wenn Sie über mehrere Servicekonten verfügen. Bei dieser Tabelle werden die Felder „object_id“ und „Provider“ in der Identifizierungsregel verwendet.

Informationen zur Erkennung des Hardwaretyps Azure finden Sie unter Erkennung von Microsoft Azure-Cloud-Komponenten mithilfe von Mustern

Hinweis: Wenn Sie Muster für Discovery und Service-Mapping Version 1.6.0 haben, fahren Sie mit dem folgenden Verfahren fort. Wenn Sie eine frühere Version haben, lesen Sie den Artikel Knowledge BaseKB0955939 .

Prozedur

1. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen Sie nach dem folgenden Systemeigenschaftsdatensatz und öffnen Sie ihn.
   sn_itom_pattern.use a single hardware type for cloud datacenters
3. Ändern Sie im Formular das Feld **Wert** in **true**.
4. Wählen Sie **Aktualisieren**.

Nächste Maßnahme

1. Bereinigen Sie die Hardwaretyp-Datensätze. Weitere Informationen finden Sie im Knowledge Base -Artikel KB1285337 .

   Wichtig: Bei der Bereinigung werden alle vorhandenen Computing-Profile aus der CMDB entfernt. Daher müssen Sie, wenn Sie der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] manuell eine Hardwarevorlage hinzugefügt haben, diese manuell der Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type] hinzufügen.

2. Führen Sie Cloud-Discovery erneut aus.

Aktiviert die Discovery von Cloud-BS-Images

Aktivieren Sie die Tabelle „Cloud-BS-Image“ [cmdb_ci_cloud_os_image], um die Cloud-BS-Image-Datensätze für Amazon AWS Cloud, Microsoft Azure Cloud, und Google Cloud Platform (GCP)zu speichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass die aktuelle Version Muster für Discovery und Service-Mapping installiert ist.
- Stellen Sie sicher, dass die neueste Version von CMDB CI-Klassenmodelle installiert ist.
- Vergewissern Sie sich, dass der Anwendungsbereich Discovery und die Anwendung Service-Mapping ist.

Hinweis: Cloud Provisioning and Governance (CPG) unterstützt die Tabelle „Neues Cloud-Image“ (cmdb_ci_cloud_os_image) nicht. Wenn Sie derzeit CPG-Bereitstellungs-Flows verwenden oder dies beabsichtigen, migrieren Sie nicht zum neuen Image-Modell.

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Jeder Cloud-Service Provider bietet Betriebssystem-Images zum Starten einer Compute-/VM-Instanz an. Cloud-Discovery speichert die erkannte Tabelle „Image“ [cmdb_ci_os_template]. Diese Tabelle ist eine abhängige Klasse von [cmdb_ci_logical_datacenter] oder [cmdb_ci_cloud_service_account]. Das neue Image-Modell erstellt unabhängig vom Servicekonto einen Datensatz für jedes öffentliche Image (Objekt-ID), und füllt sie in die Tabelle „Cloud-Image“ [cmdb_ci_cloud_os_image] ein. Dafür reduziert das neue Modell die Anzahl der Datensätze in CMDB

Hinweis: Wenn Sie Muster für Discovery und Service-Mapping Version 1.10.0 – November 2023 haben, fahren Sie mit dem folgenden Verfahren fort. Wenn Sie eine frühere Version haben, lesen Sie den Artikel Knowledge BaseKB1000183 .

Prozedur

1. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen Sie nach dem folgenden Systemeigenschaftsdatensatz, und öffnen Sie ihn dann *sn_cmdb_ci_class.use_single_cloud_os_image*.
3. Ändern Sie im Formular das Feld **Wert** in **true**.
4. Wählen Sie **Aktualisieren**.

Nächste Maßnahme

1. Bereinigen Sie die Bilddatensätze. Weitere Informationen finden Sie im Knowledge Base -Artikel KB1537376 .
2. Führen Sie Cloud-Discovery erneut aus.

Amazon AWS ElastiCache-Erkennung

Von der Anwendung ServiceNow® Discovery wird das Amazon ElastiCache-Erkennungsmuster dazu verwendet, Redis-Cluster zu ermitteln, die als Teil des ElastiCache-Service bereitgestellt werden. ElastiCache ist sowohl mit Redis als auch mit Memcached kompatibel, mit dem Muster werden jedoch nur Informationen für Redis gesammelt.

Amazon ElastiCache ist ein vollständig verwalteter In-Memory Caching-Service, der in AWS verfügbar ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

- Installieren Sie die Anwendung „Discovery and Service Mapping Patterns“ aus dem ServiceNow Store.
- Konfigurieren Sie für die ServiceNow-Instanz ein AWS-Servicekonto mit gültigen Anmeldeinformationen sowie mit der Berechtigung zum Ausführen folgender APIs:
  - `https://elasticache.{region}.amazonaws.com?Action=DescribeReplicationGroups&Version=2015-02-02`
  - `https://tagging.{region}.amazonaws.com {"ResourceTypeFilters":[]}`

Von Discovery während der horizontalen Erkennung erfasste Daten

Replikationsgruppen werden in der Tabelle „Cloud-Datenbankcluster“ [cmdb_ci_cloud_db_cluster] gespeichert, und Knotengruppenmitglieder werden in der Tabelle „Cloud-Datenbanken“ [cmdb_ci_cloud_database] gespeichert.

Feld	Beschreibung
Amazon resource name (Amazon-Ressourcenname)	Name der Ressource für jede Replikationsgruppe und jedes Knotengruppenmitglied.
FQDN	Vollqualifizierter Domänenname für jedes Knotengruppenmitglied.
Port	Port, der von jedem Knotengruppenmitglied verwendet wird.

Amazon AWS Relational Database Service-Erkennung

Die Anwendung ServiceNow® Discovery verwendet das Erkennungsmuster „Amazon AWS Relational Database Service“, um AWS RDS-Komponenten zu finden.

Amazon Relational Database Service (RDS) ist ein verwalteter relationaler Datenbankservice von Amazon Web Services (AWS). Er ermöglicht Benutzern das einfache Erstellen und Verwalten von relationalen Datenbankinstanzen in der Cloud.

Discovery verwendet das Erkennungsmuster, um eine horizontale Erkennung, Event-Erkennung und Tag-Erkennung auszuführen. Das Muster verwendet eine Reihe von Amazon REST APIs, um die RDS-Komponenten zu finden.

Von der Now Platform werden Amazon Commercial Cloud Services (C2S) für Discovery und Cloud-Governance unterstützt. C2S ist das Regierungsprogramm, das AWS für die Intelligence Community verfügbar macht.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Installieren Sie die Anwendung „Muster für Discovery und Service-Mapping“ aus dem ServiceNow Store.
- Konfigurieren Sie auf der Now Platform die AWS-Anmeldeinformationen mithilfe eines geheimen Schlüssels und eines Zugriffsschlüssels.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie ein Servicekonto. Legen Sie die **Konto-ID** auf die Amazon-Konto-ID fest, zu der RDS gehört. Verwenden Sie die Konto-ID, wie sie in der AWS-Verwaltungskonsole angezeigt wird.
- Legen Sie schreibgeschützte Berechtigungen für diese REST APIs fest:
  - https://rds.<REGION>.amazonaws.com/?Action=DescribeDBInstances
  - https://rds.<REGION>.amazonaws.com/?Action=DescribeDBInstances&DBInstanceIdentifier=<input_object_id> for events discovery
  - https://tagging.<REGION>.amazonaws.com/ for tags discovery
- Der MID-Server muss in der Amazon-Cloud platziert sein.
- Laden Sie für Cloud-Discovery das Muster „Discovery and Service Mapping“ aus dem ServiceNow Store herunter.
- Stellen Sie bei der Installation von MID-Serversicher, dass der Hostcomputer die auf der Dokumentationswebsite ServiceNow veröffentlichten Systemanforderungen für den MID-Server erfüllt oder überschreitet.

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

Unterstützung für AWS -Services in der Region China

Die neueste Version von Muster für Discovery und Service-Mapping unterstützt die Erkennung von AWS -Services in der Region China. Sie können diese Services in den Instanzen Now Platformab Xanadu Patch 3 und Washington DC Patch 9 erkennen.

Die Erkennung von AWS -Services in der Region China erfordert die Verwendung einer Rechenzentrums-URL beim Einrichten eines AWS -Service-Accounts. Beispiel: `https://organizations.cn-northwest-1.amazonaws.com.cn`.

- Weitere Informationen zur Unterstützung von Master-Accounts und Unteraccounts AWS in der Region China finden Sie unter KB1704526 .
- Informationen zum Identifizieren von AWS -Mustern, die in der Region China unterstützt werden, finden Sie in der Tabelle mit Cloud-Discovery-Mustern. Die Spalte **„AWS-Support für die Region China“** enthält für unterstützte Muster einen Wert „Ja“.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Cloud-Datenbank [cmdb_ci_cloud_database]	
Kategorie [category]	Klasse der Datenbank. Enthält Vorlagen für CPU und Arbeitsspeicher

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Objekt-ID [object_id]	Eindeutige Ressourcen-ID, die jedes logische Rechenzentrum (LDC) identifiziert
Vollständig qualifizierter Domänenname [fqdn]	Adresse des Datenbankendpunkts Der DNS-Name
TCP-Port [tcp_port]	Port des Datenbankendpunkts
Name [name]	Name der Datenbank.
Version [version]	Version der Datenbank
Typ [type]	Typ der Datenbank. Kann Folgendes sein: Amazon Aurora, PostgreSQL, MySQL, MariaDB, Oracle-Datenbank, SQL Server.
Betriebsstatus [operational_status]	Status der Datenbank
IP-Adresse [ip_address]	IP-Adresse des vollständig qualifizierten Domänennamens (FQDN)
Anbieter [vendor]	Der Anbieter, Amazon
IP-Adresse [cmdb_ci_ip_address]	
IP-Adresse [ip_address]	IP-Adresse des Datenbankendpunkts
Name [name]	Name des Datenbankendpunkts
Vollständig qualifizierter Domänenname [fqdn]	Adresse des Datenbankendpunkts Der DNS-Name
Kategorie [category]	Klasse der Datenbank. Enthält Vorlagen für CPU und Arbeitsspeicher
Netzmaske [netmask]	IP-Netzmaske
Betriebsstatus [operational_status]	Status der IP-Adresse

Amazon AWS Service-Discovery anhand von Mustern

Die AnwendungMuster für Discovery und Service-Mapping verwendet Servicemuster Amazon AWS, um die Services Amazon AWS während der Horizontal-Discovery zu erkennen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Voraussetzungen

Überprüfen Sie die Discovery-Voraussetzungen für Amazon AWS .

Weitere Informationen finden Sie im Abschnitt über die Voraussetzungen in Amazon AWS Cloud-Komponentenerkennung mithilfe von Mustern.

Entfernen Sie Ressourcen aus der Tabelle „Ressourcenaufnahmeliste“.

Stellen Sie sicher, dass die relevante Ressource nicht in der Tabelle „Ressourcenaufnahmeliste“ [sa_cloud_inventory_resource_whitelist] aufgeführt ist, um eine doppelte Discovery zu vermeiden. Weitere Informationen zum Entfernen von Ressourcen aus der Ressourcenaufnahmeliste finden Sie unter Ressourcenbestand von Amazon Web Services (AWS).

Relevantes Muster aktivieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Aktivieren Sie ein deaktiviertes Muster. Beachten Sie, dass Muster für Discovery und Service-Mapping für diese Services standardmäßig deaktiviert sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die aktuelle Version von Muster für Discovery und Service-Mapping unterstützt die Discovery der folgenden Amazon AWS -Services.

- Athena-Arbeitsgruppe
- Sicherungsplan
- Backup Vault
- CloudFront-Verteilung
- CloudWatch-Protokolle
- CodeDeploy-Bereitstellung
- CodePipeline-Pipeline
- DMS-Endpunkte
- EMR-Cluster (wird auf EC2 ausgeführt)
- FSX-Sicherung
- FSx-Dateisystem
- Glide-Datenbank
- IAM-Richtlinie
- IAM-Rolle
- IAM-Benutzer
- KMS-Schlüssel
- MQ-Konfiguration
- S3-Gletscher-Vault
- Sage Maker-Notebook-Instanz
- Managergeheimnis für Geheimnisse
- SES-Identität (Simple Email Service)
- Systems Manager-Dokument
- Systems Manager-Parameterspeicher
- Familienserver übertragen
- VPC-Flow-Protokoll
- Von VPC verwaltete Präfixliste
- Regel für X-Ray-Stichprobennahme

CI-Beziehungen

Discovery erstellt diese Beziehungen, um die Erkennung von Amazon AWS -Services zu unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Regionale Services

CI	Beziehung	CI
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

Globale Services

CI	Beziehung	CI
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Amazon DynamoDB-Erkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping verwenden das DynamoDB-Muster Amazon AWS, um Komponenten von DynamoDB zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Das AWS DynamoDB-Muster stellt Amazon REST APIs zum Abrufen von Informationen zu DynamoDB bereit. Sie können auch Service-Mapping und Discovery konfigurieren, um AWS DynamoDB-Komponenten mithilfe von AWS -Ereignissen zu erkennen.

Von der Now Platform werden Amazon Commercial Cloud Services (C2S) für Discovery und Cloud-Governance unterstützt. C2S ist das Regierungsprogramm, das AWS für die Intelligence Community verfügbar macht.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Anwenderzugriff

Stellen Sie in der Konsole AWS einen Benutzer mit den folgenden Berechtigungen bereit: AmazonDynamoDBReadOnly-Zugriff und AWSLambdaInvocation-DynamoDB.

Cloud-Servicekonto

Richten Sie das Servicekonto auf der Now Platform® mit den folgenden Eigenschaften ein:

- Eine **Account-ID**, bei der es sich um die Account-ID Amazon handelt, zu der DynamoDB gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
- Die entsprechenden AWS -Anmeldeinformationen, die erforderlich sind, damit die -Account-ID die AWS -Cloud erreicht.

AWS Anmeldeinformationen

Konfigurieren Sie auf der Now Platform®die Anmeldeinformationen AWS mit einem geheimen Schlüssel und einem Zugriffsschlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstiegspunkt für einen Service, der DynamoDB enthält

Verwenden Sie den *AWS* **Ressourcennamensendpunkt** als Einstiegspunkttyp, wenn Sie einen Service erstellen, der DynamoDB enthält. Geben Sie den Amazon-Ressourcennamen (ARN) und den Host für den Einstiegspunkt an.

(Für Top Down-Discovery durch Service-Mapping) Führen Sie eine Horizontal-Discovery der logischen Rechenzentren durch.

Erkennen Sie logische Rechenzentren, von denen DynamoDB gehostet wird, wie unter „Discovery für ein AWS -Cloud-Servicekonto ausführen in der ServiceNow Cloud Provisioning and Governance -Dokumentation beschrieben.

Cloud-Discovery

Laden Sie für Cloud-Discovery das Muster für Discovery und Service-Mapping aus dem ServiceNow Store herunter.

MID-Server

Wenn Sie den MID-Server installieren, vergewissern Sie sich, dass der Hostcomputer die Systemanforderungen für den MID-Server erfüllt oder übertrifft.

Discovery-Zeitplan

Erstellen Sie einen Zeitplan für das relevante Servicekonto AWS wie unter „Discovery für ein Servicekonto planen“ in der Dokumentation ServiceNow Cloud Provisioning and Governance beschrieben.

Konfigurieren Sie den Ereignisservice AWS .

Zum Aktivieren der warnungsbasierten Discovery konfigurieren Sie den Ereignisservice AWS wie unter Einrichten AWS der Ereignisverarbeitung für Discovery und Service-Mapping in der ServiceNow Cloud Provisioning and Governance -Dokumentation beschrieben.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Globale DynamoDB-Tabelle [cmdb_ci_dynamodb_global_table]	
Objekt-ID [object_id]	Der Amazon-Ressourcenname (ARN) im folgenden Format: *arn:aws:dynamodb::xxxxxxxxxxxx:table:<table name>*
DynamoDB-Tabelle [cmdb_ci_dynamodb_table]	
Name [name]	Tabellenname.
Erstellungsdatum [creation date]	Erstellungsdatum der DynamoDB gemäß der Zeitzone des MID-Servers, der diese DynamoDB erkennt.
Cloud-Anbieter [cloud_provider]	Amazon AWS
Objekt-ID [object_id]	Der Amazon-Ressourcenname (ARN) im folgenden Format: *arn:aws:dynamodb:<region>:xxxxxxxxxxxx:table:<tab name>*

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

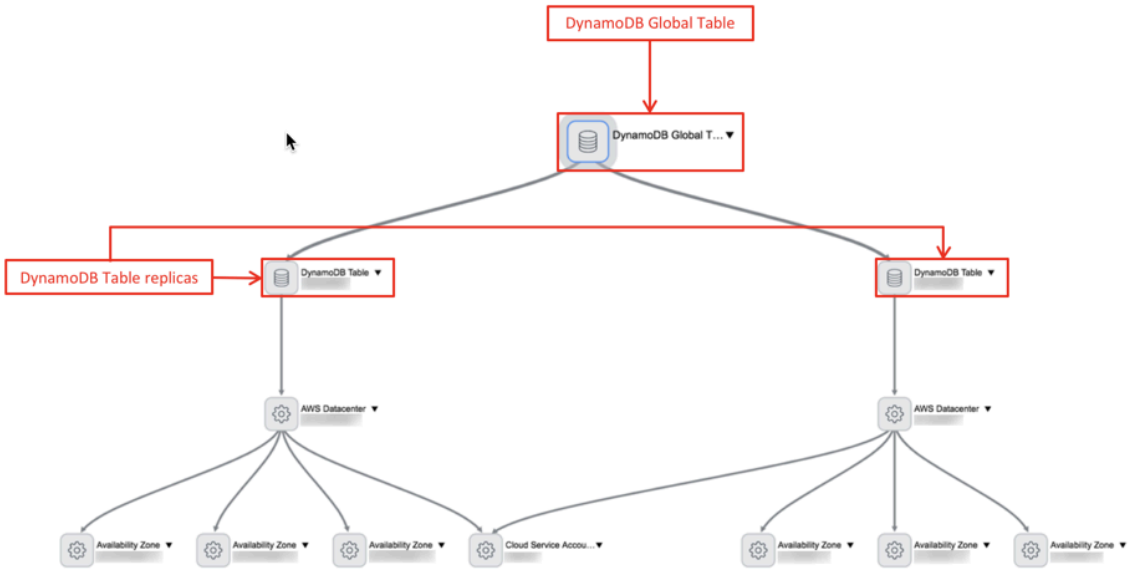
Tabelle und Feld	Beschreibung
Globale ARN [global_arn]	Die globale ARN der Tabelle für die globale DynamoDB-Tabelle. Dieses Feld ist leer, wenn die DynamoDB nicht global ist.
Stream-ARN [stream_arn]	Die Auswahlmöglichkeiten sind: • Stream-ARN • Deaktiviert
Servicename [service_name]	Standardmäßig auf **DynamoDB** festgelegt
Verschlüsselung [encryption]	Verschlüsselungskonfiguration auf der DynamoDB Die Auswahlmöglichkeiten sind: • Aktiviert • Deaktiviert
Replikationsgruppe [replication_group]	Tabellen-ARN der verbundenen globalen DynamoDB-Tabellen
Automatische Skalierung lesen [read_autoscaling]	Die Auswahlmöglichkeiten sind: • Aktiviert • Deaktiviert
Einheiten lesen [read_units]	Die Anzahl der gelesenen Einheiten in der DynamoDB-Tabelle
Max. Einheiten zum Lesen [read_max_units]	Die maximal zulässige Anzahl der gelesenen Einheiten in der DynamoDB-Tabelle
Min. Einheiten zum Lesen [read_min_units]	Die zulässige Mindestzahl an gelesenen Einheiten in der DynamoDB-Tabelle
Einheiten zum Schreiben [write_units]	Die Anzahl der zu schreibenden Einheiten in der DynamoDB-Tabelle
Max. Einheiten zum Schreiben [write_max_units]	Die maximal zulässige Anzahl der zu schreibenden Einheiten in der DynamoDB-Tabelle
Min. Einheiten zum Schreiben [write_min_units]	Die zulässige Mindestzahl der zu schreibenden Einheiten in der DynamoDB-Tabelle
Tabellengröße [table_size]	Die derzeit bereitgestellte Größe der DynamoDB-Tabelle in Byte
Automatische Skalierung schreiben [write_autoscaling]	Die Auswahlmöglichkeiten sind: • Aktiviert • Deaktiviert
Zeitpunkt [point_in_time]	Die Auswahlmöglichkeiten sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
	• Aktiviert • Deaktiviert

Die Grafik zeigt CIs, die Teil der DynamoDB-Erkennung sind.

Abhängigkeitsansichten mit DynamoDB-Komponenten



CI-Beziehungen

Das Muster „Amazon AWS DynamoDB“ erstellt die folgenden CI-Beziehungen:

CI	Beziehung	CI
Globale DynamoDB-Tabelle [cmdb_ci_dynamodb_global_table]	Cluster von::Cluster	DynamoDB-Tabelle [cmdb_ci_dynamodb_table]

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Das Muster „Amazon AWS DynamoDB“ identifiziert Verbindungen von der DynamoDB zu AWS Lambda-Funktionen.

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
die REST-Zeitüberschreitung verursacht wurde.	nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter *sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Zugehörige Informationen

Cloud-REST-Abfrage für Cloud-Computing-Geräte definieren

Cloud-REST-Abfrage für Cloud-Computing-Geräte definieren

Als Teil der Erstellung oder Änderung eines Erkennungsmusters können Sie den Vorgang **Cloud-REST-Abfrage** verwenden, um Informationen aus Konfigurationselementen (CIs) des PaaS-Typs (Platform as a Service) zu extrahieren, z. B. Microsoft Azure oder Amazon Web Services.

Vorbereitungen

- Überprüfen Sie, ob das Betriebssystem des CI, für das Sie den Vorgang „Cloud-REST-Aufruf“ verwenden möchten, den Betriebssystemtyp des logischen Datenzentrums [cmdb_ci_logical_datacenter] erweitert:
  1. Navigieren zu **Musterdesigner** > **Discovery-Muster**.
  2. Doppelklicken Sie auf das relevante Muster, um es im Musterdesigner zu öffnen.
  3. Klicken Sie auf die Registerkarte **Standard**.
  4. Beachten Sie das Betriebssystem für dieses CI.
  5. Navigieren zu **Systemdefinition** > **Tabellen**.
  6. Legen Sie das Suchfeld auf **Bezeichnung** fest und geben Sie den Namen des Betriebssystems ein, wie auf der Registerkarte **Standard** des Musters angegeben.
  7. Suchen Sie das Betriebssystem in der Liste, und stellen Sie sicher, dass das logische Rechenzentrum in der Spalte **Erweitert Tabelle** angezeigt wird.

- Navigieren Sie zu dem entsprechenden Pattern-Schritt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wählen Sie auf dem Musterformular den entsprechenden Identifikationsteil für aus Discovery .

   Alternativ wählen Sie den entsprechenden Identifikations- oder Verbindungsabschnitt für aus Service-Mapping .

2. Wählen Sie den entsprechenden Musterschritt aus, oder klicken Sie auf das Symbol **Schritt darüber hinzufügen**, um einen Schritt hinzufügen.

Grundkenntnisse in der Programmierung sind wünschenswert.

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird

Stellen Sie den Cloud-REST-Aufrufvorgang in Mustern für die Erkennung von PaaS-CIs bereit. Dieser auf Java-Skript basierende benutzerdefinierte Vorgang ist nur verfügbar, nachdem Musterversion 1.0.24 oder höher aus dem ServiceNow Store heruntergeladen wurde. Verwenden Sie diesen Vorgang anstelle des im Standardsystem verfügbaren Cloud-REST-Aufrufvorgangs.

In der offiziellen Dokumentation der API-Hersteller finden Sie die Abfragesyntax für das Gerät, das Sie mit dem Vorgang Cloud-REST-Abfrage abfragen möchten. Beispiel:

- http://docs.aws.amazon.com/AWSEC2/latest/APIReference/Welcome.html
- https://docs.microsoft.com/en-us/rest/api/apimanagement/

Prozedur

1. Wählen Sie **Cloud-REST-Abfrage** aus der Liste **Vorgang** aus.
2. Definieren Sie Abfrageparameter nach Bedarf:

   Hinweis: Wenn Sie diesen Vorgang angepasst haben, können die Abfrageparameter unterschiedlich sein.

Feld	Beschreibung
URL	Geben Sie die URL wie in der offiziellen Microsoft Azure- oder Amazon Web Services-Dokumentation beschrieben an. Sie können Variablen verwenden. Sie können auch einen Wert aus einem bestimmten Feld in einer tabellarischen Variable eingeben.
Methode	Geben Sie den Methodenwert als Zeichenfolge in Großbuchstaben ein, z. B. „GET“. Unterstützte Methoden: ◦ GET ◦ POST ◦ PUT Weitere Informationen finden Sie im entsprechenden API-Leitfaden. Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

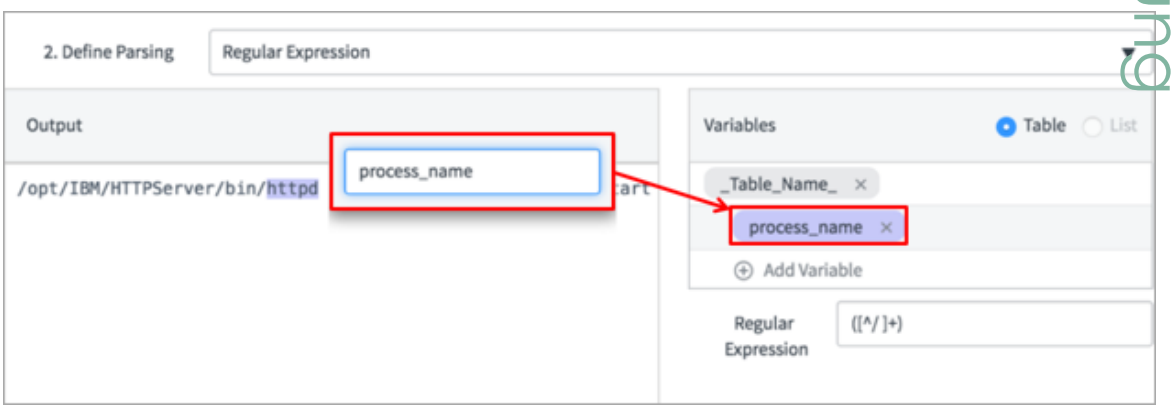
Feld	Beschreibung
	die HTTP-Abfragemethode in der API-Dokumentation nicht ausdrücklich erwähnt wird, verwenden Sie die GET-Methode.
Textkörper	(Optional) Geben Sie einen Anforderungstext als Zeichenfolge ein. Wenn die Zeichenfolge Anführungszeichen enthält, verwenden Sie den umgekehrten Schrägstrich vor den Anführungszeichen, um anzugeben, dass die Zeichenfolge nicht bei den Anführungszeichen endet.
Header	(Optional) Wenn die relevante API-Dokumentation besagt, dass HTTP-Header gesendet werden müssen, geben Sie diese Header im folgenden Format ein: Header_name1:header_value1,header_name2:header_valu Zum Beispiel: `Content-Type:xml`.
Formatiert	JSON formatiert oder nicht

3. Wenn Sie die gesamte Befehlsausgabe als Variable speichern möchten, klicken Sie in der Liste **Analyse definieren** auf `KEINE`, und definieren Sie die Variable.
4. Wählen Sie die Parsing-Strategie aus der Liste **Analyse definieren** aus.
5. Wenn Sie im Debug-Modus arbeiten, definieren Sie die Analysekriterien wie folgt:

   a. Klicken Sie auf **Vorgang ausführen**, um das Ergebnis im Bereich **Ausgabe** anzuzeigen.

   b. Im Feld **Ausgabe** markieren Sie Text oder Symbole, der/die eine Variable enthalten soll/sollen.

   c. Geben Sie im Feld Variablenname den Namen für die neue Variable ein, beispielsweise 'process_name'.



   d. Drücken Sie die **Eingabetaste**.
   Die neue Variable wird im Feld **Variablen** hinzugefügt.

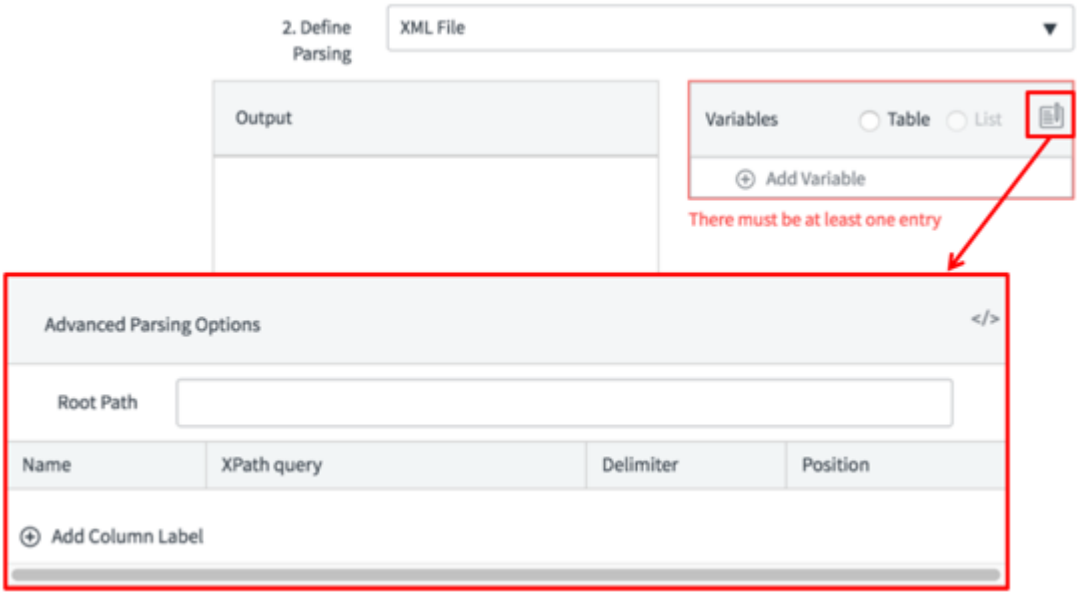
6. Wenn Sie nicht im Debug-Modus arbeiten, definieren Sie die Analysekriterien wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie im Variablenbereich auf **Variable hinzufügen**, und geben Sie den Namen für die neue Variable ein.

b. Klicken Sie auf das Symbol **Erweitert**.



c. Klicken Sie auf **Spaltenbezeichnung hinzufügen**.

d. Geben Sie die Analyse-Abfrage ein.

e. Geben Sie einen Wert für das Trennzeichen ein.

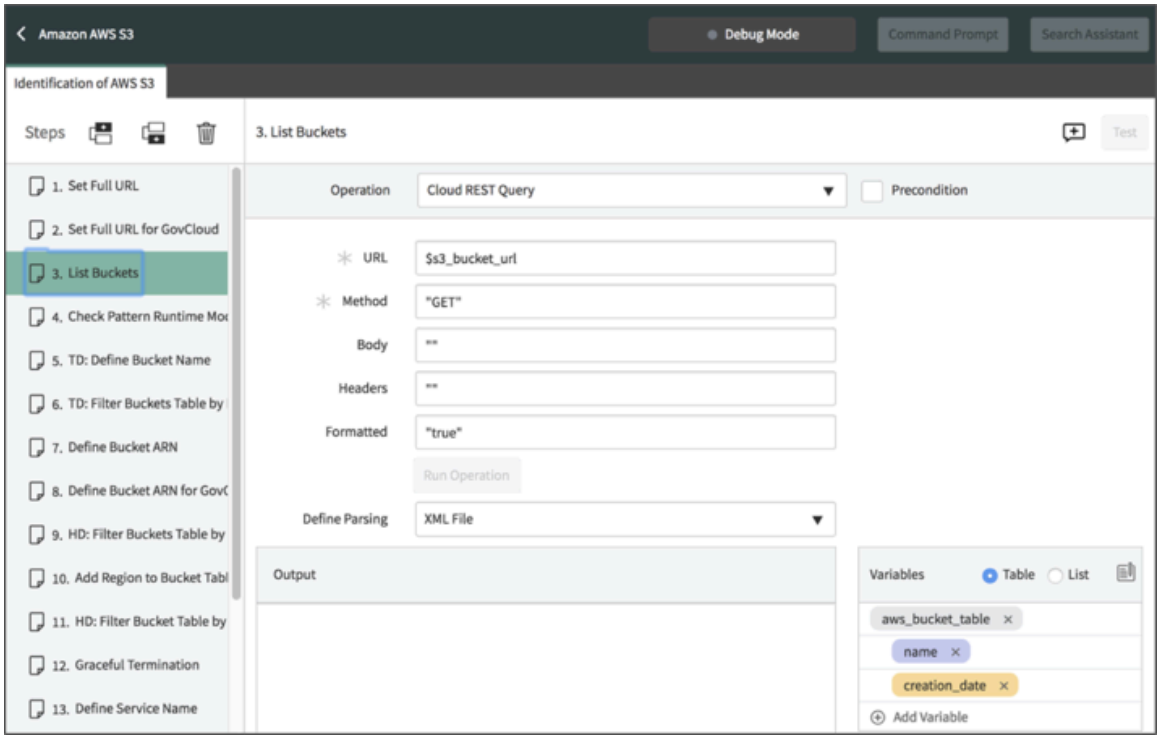
f. Geben Sie einen Wert für die Position ein.

7. Wählen Sie **Beenden**, um die Erkennung zu stoppen, wenn keine Ergebnisse gefunden werden.

Example:

Diese Operation wird verwendet in	Dieses Objekt
Hierarchie	Applikation
CI-Typ	Cloud-Objektspeicher [cmdb_ci_cloud_object_storage]
Muster	Amazon AWS S3
Abschnitt	Identifizierung von AWS S3
Schrittnummer und -Name	3. Buckets auflisten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Verwenden Sie den Cloud-REST-Abfragevorgang, um Informationen zu AWS-Buckets, deren Namen und Erstellungsdaten zu extrahieren.

Amazon Kinesis-Discovery

Die Anwendung ServiceNow® Discovery verwendet das Discovery-Muster Kinesis Amazon, um Kinesis-Services zu finden, die unter Amazon Web Services (AWS) verfügbar sind.

Kinesis ist ein verwalteter, skalierbarer AWS cloudbasierter Service, der die Echtzeitverarbeitung von Streaming großer Datenmengen pro Sekunde ermöglicht. AWS Kinesis enthält vier Arten von Services:

- Kinesis-Videostreams – erfassen, verarbeiten und speichern Videostreams für Analysen und maschinelles Lernen.
- Kinesis Data Streams: ein vollständig verwalteter Streaming-Datenservice.
- Kinesis Data Firehose – lädt Datenströme in AWS-Datenspeicher.
- Kinesis Data Analytics: Verarbeiten und analysieren Sie Streaming-Daten.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Installieren Sie die Anwendung „Discovery and Service Mapping Patterns“ aus dem ServiceNow Store.
- Überprüfen Sie die folgenden Plugin-Versionen:
  - Discovery and Service Mapping Patterns 1.0.93 oder höher (sn_itom_pattern)
  - CMDB CI Class Models Version 1.40.0 oder höher (sn_cmdb_ci_class)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Felder in der Tabelle „-Cloud-Datenbank“ [cmdb_ci_aws_kingesis].

Feld	Beschreibung
Objekt-ID	Name der Streamressource.
Name	Der Name des Streams. • Kinesis-Daten: cmdb_ci_aws_kinsis_data • Kinesis-Video: cmdb_ci_aws_kinsis_video • Kinesis Firehose – cmdb_ci_aws_kinsis_firehose • Analytics für Kinesis-Daten – cmdb_ci_aws_kinsis_data_analytics
Status	Der Status des Streams.

Beziehungen von Configuration Item (CI)

CI	Beziehung	CI
AWS Kinesis-Daten	Gehostet auf::Hostet	AWS-Rechenzentrum
AWS Kinesis Video	Gehostet auf::Hostet	AWS-Rechenzentrum
AWS Kinesis Firehose	Gehostet auf::Hostet	AWS-Rechenzentrum
Analytics für AWS Kinesis-Daten	Gehostet auf::Hostet	AWS-Rechenzentrum

Amazon Keyspaces-Erkennung

Von der Anwendung ServiceNow® Discovery wird das Amazon Keyspaces-Erkennungsmuster dazu verwendet, den mit Amazon Keyspaces verwalteten Apache Cassandra-kompatiblen Datenbankservice zu ermitteln.

Amazon Keyspaces ist ein verwalteter Apache Cassandra-kompatibler Datenbankservice. Von einem Keyspace werden zugehörige Tabellen gruppiert, die für mindestens eine Anwendung relevant sind. Der Keyspace enthält mindestens eine Tabelle und definiert die Replikationsstrategie für alle enthaltenen Tabellen.

Voraussetzungen

- Installieren Sie die Anwendung „Discovery and Service Mapping Patterns“ aus dem ServiceNow Store.
- Konfigurieren Sie für die ServiceNow-Instanz ein AWS-Servicekonto mit gültigen Anmeldeinformationen sowie mit der Berechtigung zum Ausführen folgender APIs:
  - `https://cassandra.{region}.amazonaws.com {Content-Type:application/x-amz-json-1.0, , X-Amz-Target: KeyspacesService.ListKeyspaces}`
  - `https://tagging.{region}.amazonaws.com {"ResourceTypeFilters":[]}`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Keyspaces werden in der Tabelle „Cloud-Datenbanken“ [cmdb_ci_cloud_database] gespeichert.

Feld	Beschreibung
Amazon resource name (Amazon-Ressourcenname)	Name des Keyspace
FQDN	Vollqualifizierter Domänenname der Region, in der sich der Keyspace befindet.
Port	Port für eingehende TLS-Verbindungen (9142).

Amazon OpenSearch-Erkennung

Von der Anwendung ServiceNow® Discovery wird das Amazon OpenSearch-Erkennungsmuster dazu verwendet, Amazon OpenSearch-Servicedomänen zu ermitteln.

OpenSearch ist eine Such- und Analyse-Engine auf Open-Source-Basis für Anwendungsfälle wie Protokollanalysen, Echtzeit-Anwendungsüberwachung und Clickstream-Analysen. OpenSearch funktioniert als Cluster von Knoten, die vom Endbenutzer abstrahiert werden. Eine OpenSearch-Servicedomäne ist gleichbedeutend mit einem OpenSearch-Cluster. Domänen sind Cluster mit Einstellungen, Instanztypen, Instanzanzahlen und Speicherressourcen.

Voraussetzungen

- Installieren Sie die Anwendung „Discovery and Service Mapping Patterns“ aus dem ServiceNow Store.
- Konfigurieren Sie für die ServiceNow-Instanz ein AWS-Servicekonto mit gültigen Anmeldeinformationen sowie mit der Berechtigung zum Ausführen folgender APIs:
  - `https://es.{region}.amazonaws.com/2021-01-01/domain`
  - `https://es.{region}.amazonaws.com/2021-01-01/opernsearch/domain-info{"Domänennamen":[]}`
  - `https://tagging.{region}.amazonaws.com {"ResourceTypeFilters":[]}`

Von Discovery während der horizontalen Erkennung erfasste Daten

OpenSearch-Servicedomänen werden in der Tabelle „Cloud-Datenbanken“ [cmdb_ci_cloud_database] gespeichert.

Feld	Beschreibung
Amazon resource name (Amazon-Ressourcenname)	Name der Servicedomäne.
FQDN	Vollqualifizierter Domänenname der Region, in der sich der Keyspace befindet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon Redshift-Erkennung

Von der Anwendung ServiceNow® Discovery wird das Amazon Redshift-Erkennungsmuster dazu verwendet, in Amazon Web Services (AWS) verfügbare Redshift Data Warehouse-Services zu ermitteln.

Redshift wird als Cluster von Compute-Knoten mit einem zusätzlichen Leader-Knoten ausgeführt. Der Leader-Knoten fungiert als Schnittstelle zu Clientanwendungen und wird dazu eingesetzt, die Kommunikation zwischen den Compute-Knoten zu koordinieren.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Installieren Sie die Anwendung „Discovery and Service Mapping Patterns“ aus dem ServiceNow Store.
- Konfigurieren Sie für die ServiceNow-Instanz ein AWS-Servicekonto mit gültigen Anmeldeinformationen sowie mit der Berechtigung zum Ausführen folgender APIs:
  - `https://redshift.{region}.amazonaws.com?Action=DescribeClusters`
  - `https://redshift.{region}.amazonaws.com?Action=DescribeTags`

Von Discovery während der horizontalen Erkennung erfasste Daten

Die ermittelten Daten umfassen die folgenden Felder in der Tabelle „Cloud-Datenbank“ [cmdb_ci_cloud_database].

Feld	Beschreibung
Startdatum	Zeitpunkt, zu dem der Redshift-Cluster erstellt wurde.
Name	Name des Redshift-Clusters.
VPC-ID	Bezeichner der Virtual Private Cloud, die den Cluster enthält.
Cluster availability status (Verfügbarkeitsstatus des Clusters)	Status des Clusters, z. B.: • Verfügbar • Nicht verfügbar • Wartung • Wird geändert • Fehlgeschlagen
Knotenanzahl	Anzahl der Knoten im Cluster.
Verfügbarkeitszone	AWS-Verfügbarkeitszone, in der der Cluster bereitgestellt wird.
Knotentyp	Typ der Knoten im Cluster, z. B.:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• dc2 • ds2 • ra3
FQDN	Vollqualifizierter Domänenname des Clusters.
TCP-Port	Port, der vom Cluster zum Abhören verwendet wird.

Erkennung von Amazon Simple Storage Service (AWS S3)

Die ServiceNow Discovery-Anwendung verwendet das Muster „Amazon AWS S3“, um Buckets von öffentlichem und nicht öffentlichem Speicher des Amazon Simple Storage Service zu suchen. Das Muster verwendet eine Reihe von REST API-Aufrufen, um diese Ressourcen zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Zusätzlich zum Erkennungszeitplan löst die ServiceNow-Instanz das Muster „Amazon AWS S3“ aus, wenn AWS Config ein Event an die ServiceNow-Instanz sendet. Config ist ein Service, der AWS-Ressourcen kontinuierlich überwacht und jedes Mal Events an ServiceNow sendet, wenn erkannt wird, dass sich eine Ressourcenkonfiguration geändert hat.

Das Muster „Amazon AWS S3“ kann auch AWS S3-Buckets erkennen, die sich in der Region AWS GovCloud (US) befinden. Für AWS S3 in AWS GovCloud (SU) kann das Muster ausgehende AWS S3-Verbindungen zu anderen Cloud-Ressourcen wie der Lambda-Funktion nicht erkennen. Die Erkennung ausgehender Verbindungen für AWS S3 wird in zukünftigen Versionen unterstützt.

Sie können dieses Muster auf der ServiceNow-Plattform mit Jakarta Patch 10, Kingston Patch 8 oder London Patch 1 verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Wenn Sie Identity and Access Management (IAM) verwenden, um Benutzer auf der AWS-Plattform (Amazon Web Services) zu verwalten, stellen Sie sicher, dass Sie eine Benutzerrichtlinie für den AWS-Benutzer erstellt haben. Weitere Informationen finden Sie im Abschnitt zur Erstellung einer IAM-Benutzerrichtlinie für Cloud Provisioning and Governance in der ServiceNow Cloud Provisioning and Governance-Dokumentation.
- Konfigurieren Sie das AWS-Servicekonto.
- Konfigurieren Sie die AWS-Anmeldeinformationen mithilfe eines geheimen Schlüssels und eines Zugriffsschlüssels.
- Benutzerberechtigungen für die AmazonS3ReadOnlyAccess-Richtlinie
- Erkennen Sie logische Rechenzentren, die S3-Buckets hosten, wie unter „Erkennung für ein AWS Cloud-Servicekonto ausführen“ in der ServiceNow Cloud Provisioning and Governance-Dokumentation beschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie einen Zeitplan für das relevante AWS-Servicekonto, wie im Abschnitt zum Planen der Erkennung für ein Servicekonto in der ServiceNow Cloud Provisioning and Governance-Dokumentation beschrieben.
- Zum Aktivieren der alarmbasierten Erkennung konfigurieren Sie den AWS Event-Service wie im Abschnitt zum Einrichten der AWS Event-Verarbeitung für Discovery und Service-Mapping in der ServiceNow Cloud Provisioning and Governance-Dokumentation beschrieben.
- Laden Sie für Cloud-Discovery das Muster „Discovery and Service Mapping“ aus dem ServiceNow Store herunter.
- Stellen Sie bei der Installation von MID-Serversicher, dass der Hostcomputer die auf der Dokumentationswebsite ServiceNow veröffentlichten Systemanforderungen für den MID-Server erfüllt oder überschreitet.

Von Discovery während der horizontalen Erkennung erfasste Daten

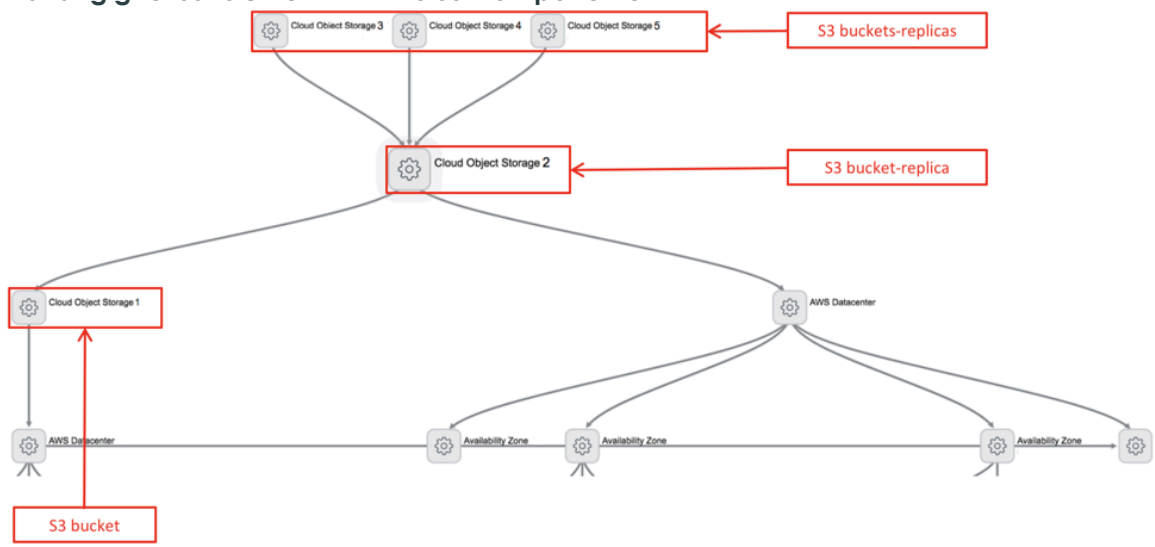
Tabelle und Feld	Beschreibung
Cloud-Objektspeicher [cmdb_ci_cloud_object_storage]	
Bucket-Name [bucket_name]	Der Name des AWS S3-Bucket. Sie können alle in einem logischen Rechenzentrum gehosteten Buckets während eines Erkennungsprozesses erkennen.
Erstellungsdatum [creation date]	Erstellungsdatum des AWS S3-Bucket
Cloud-Anbieter [cloud_provider]	Amazon AWS
Objekt-ID [object_id]	Der Amazon-Ressourcenname (ARN) im folgenden Format: *arn:aws:s3:::<bucket name>*
Servicename [service_name]	Standardmäßig auf **S3** festgelegt
Eigentümer [owner]	Der Name des Eigentümers des AWS S3-Bucket
Verschlüsselungstyp [encryption_type]	Typ der Verschlüsselung für diesen Bucket. Die Auswahlmöglichkeiten sind: • Keine • AES-256 • AWS-KMS
ACL-Zugriffstyp [acl_access_type]	Auswahlmöglichkeiten für Zugriffssteuerungstypen: • Öffentlich • Nicht öffentlich
Richtlinie Zugriffstyp [policy_access_type]	Auswahlmöglichkeiten für Richtlinien-Zugriffstypen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
	• Öffentlich • Nicht öffentlich
Replikationsziel [replication_destination]	Bucket-ARN des Bucket am Replikationsziel

In der Übersicht Abhängigkeitsansichten sehen Sie alle erkannten S3-Buckets in Ihrer Organisation, einschließlich S3-Buckets, die Sie als Repliken konfiguriert haben. In diesem Beispiel replizieren Cloudobjektspeicher 1, Cloudobjektspeicher 2 und Cloudobjektspeicher 3 Cloudobjektspeicher 2. Cloudobjektspeicher 2 wiederum repliziert Cloudobjektspeicher 1.

Abhängigkeitsansichten mit AWS S3-Komponenten



CI-Beziehungen

Diese Beziehungen sollen die Erkennung von AWS S3 unterstützen:

CI	Beziehung	CI
cmdb_ci_cloud_object_storage	Repliziert zu::Repliziert von	cmdb_ci_cloud_object_storage
cmdb_ci_cloud_object_storage	Gehostet auf::Hostet	cmdb_ci_logical_datacenter

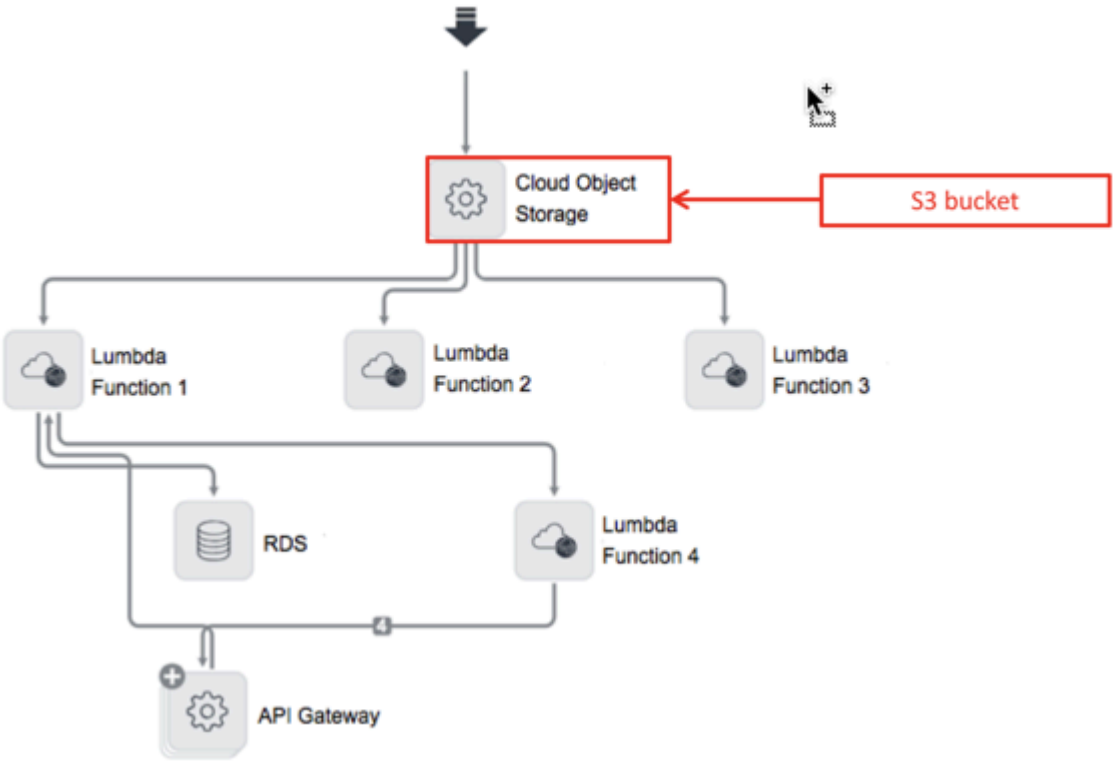
Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Service-Mapping kann ausgehende AWS S3-Verbindungen zu Cloud-Ressourcen erkennen, z. B. die Lambda-Funktion.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservicezuordnung mit einem S3-Bucket-CI



Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim	Standardmäßig ist der Parameter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Muster-Debugging auf (und nicht während der Discovery).	*sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Ressourcenbestand von Amazon Web Services (AWS)

Die Anwendungen ServiceNow Discovery und Service-Mapping können die über den AWS-Konfigurationsservice verfügbaren AWS-Ressourcen finden und zuordnen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery verwendet das Muster „AWS Resource Inventory“, um die über AWS verfügbaren Ressourcen zu erkennen. Verwenden Sie dieses Muster für AWS-Ressourcen, die kein eigenes Muster haben, z. B. AWS Lambda oder EC2. Dieses Muster ist auf Ressourcen beschränkt, die über den AWS-Konfigurationsservice verfügbar sind, wie im AWS Config Developer Guide beschrieben.

Sie können dieses Muster auf der ServiceNow-Plattform mit der Version London (Patch 8), Madrid (Patch 2) oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Erstellen Sie AWS-Anmeldeinformationen.
- Erstellen Sie ein AWS-Cloud-Servicekonto.

  Für die Erkennung können Sie nur das AWS-Verwaltungsservicekonto verwenden, nicht aber dessen Unterkonten.

  Hinweis: Die Cloud Discovery-Benutzeroberfläche bezeichnet Mitgliedskonten als Unterkonten.

- AWS-Rechenzentren (LDC) erkennen
- Vollständige AWS Discovery planen oder bestimmtes Bestandsmuster verwenden
- Optimieren Sie die Erkennung von AWS-Ressourcen mithilfe der Aufnahmeliste für Ressourcen.

  Wenn Ihre Bereitstellung benutzerdefinierte Muster für die AWS Discovery aufweist, stellen Sie sicher, dass Sie AWS-Ressourcen nicht zweimal erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Stellen Sie sicher, dass der Anwendungsbereich „Discovery and Service Mapping Patterns“ ist:
   a. Navigieren zu **Einstellungen** > **Entwickler**.
   b. Wählen Sie `Discovery and Service Mapping Patterns` aus der Liste **Anwendung** aus.
2. Navigieren zu **Systemdefinitionen** > **Tabellen**.
3. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].
4. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.
5. Wählen Sie Ressourcentypen aus, für die Sie benutzerdefinierte Muster haben, und wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option `Löschen` aus.

Die Aufnahmeliste für Cloud-Bestandsressourcen ist mit allgemeinen Services vordefiniert. Sie können die Liste um zusätzliche Ressourcentypen erweitern, die das Muster erkennen soll. Die Namen dieser Ressourcentypen müssen den Benennungskonventionen der entsprechenden Anbieter entsprechen.

Hinweis: Wenn Sie die sofort einsatzbereite Aufnahmeliste ändern, wird sie in Anwendungsupdates nicht mehr automatisch aktualisiert. Sie müssen die benutzerdefinierte Liste selbst verwalten.

1. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
Cloud-Anbieter	Der Anbieter des Ressourcentyps: AWS
Ressourcentyp	Der Wert des AWS-Ressourcentyps. Zum Beispiel: AWS::CloudWatch::Alarm.
Applikation	Der Anwendungsbereich: Discovery and Service Mapping Patterns

Die Änderungen werden beim nächsten Ausführen des Musters angewendet.

- Zum Erkennen der Ressourcen, von denen der AWS-Konfigurationsservice unterstützt wird, wird vom Muster folgende API verwendet: `https://config.[AWS region].amazonaws.com`. Vom Muster wird der Ressourcentyp in der API-Anforderung im folgenden Format angegeben: `{"resourceType":"AWS::[RESOURCE]::[TYPE]"}`.

  Die POST-Methode erfordert die folgenden Header:

  - X-Amz-Target - StarlingDoveService.ListDiscoveredResources
  - Accept - application/json
  - Content-Type - application/x-amz-json-1.1

- Zum Erkennen der Ressourcen-Tags für Ressourcen, die Tags unterstützen, wird vom Muster folgende API verwendet: `https://tagging.[AWS region].amazonaws.com`. Vom

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Muster wird der Ressourcentyp in der API-Anforderung im folgenden Format angegeben: `{"ResourceTypeFilters": ["[resource]:[type]"]}`.

Die POST-Methode erfordert die folgenden Header:

- X-Amz-Target - ResourceGroupsTaggingAPI_20170126.GetResources
- Accept - application/json
- Content-Type - application/x-amz-json-1.1

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Haupt-CI [cmdb_ci_cmp_resource]	
object_id	Die ID des Elements. Dies ist normalerweise der Amazon-Ressourcenname (Amazon Resource Name, ARN).
name	Name der Ressource
resource_type	Der Asset-Ressourcentyp, basierend auf dem Inhalt der JSON-Datei
Beschreibung	Kurzbeschreibung, wie das CI mit Daten gefüllt wird

CI-Beziehungen

Das Muster „AWS Resource Inventory“ erstellt die folgenden CI-Beziehung:

CI	Beziehung	CI
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]

Im Folgenden finden Sie eine Abhängigkeitsansicht des gesammelten Daten-Flows.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS Resource Inventory –Abhängigkeitsansicht

AWS API-Gateway-Erkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping können AWS API-Gateways und Verbindungen zu anderen Entitäten finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery und Service-Mapping verwenden das Muster *Amazon AWS API Gateway*, um eine horizontale Erkennung und eine Erkennung von oben nach unten auszuführen.

Dieses Muster können Sie auf der ServiceNow-Plattform in Version Kingston oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

AWS-Servicekonto mit Anmeldeinformationen

Richten Sie auf der Now Platform® das Servicekonto wie folgt ein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Eine **Konten-ID**, bei der es sich um die Amazon Konten-ID handelt, zu der das API-Gateway gehört. Verwenden Sie die Konto-ID, wie sie in der AWS-Verwaltungskonsole angezeigt wird. Sie können eine Erkennung über das Servicekonten-Formular ausführen.
- Die entsprechenden AWS-Anmeldeinformationen, die erforderlich sind, damit die Konten-ID die AWS-Cloud erreicht.

Weitere Informationen zu Servicekonten für Discovery und Service-Mapping finden Sie in der Produktdokumentation.

Update Set

Wenn Ihre Instanz die Version Jakarta oder Istanbul hat, importieren Sie das Update Set, das in „KB0679927 : AWS Lambda top-down discovery update set (Update Set für AWS Lambda-Erkennung von oben nach unten)“ bereitgestellt wird. Dieses Update Set ist für Service-Mapping erforderlich.

Benutzerzugriff

Erteilen Sie einem Benutzer auf der AWS-Konsole Berechtigungen zum Ausführen der Funktion `apigateway:GET` nur für die GET-Aktion in API Gateway.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Zusätzliche Informationen
Cloud-Gateway [cmdb_ci_cloud_gateway]	
Objekt-ID	Die ID des Gateways
Kurzbeschreibung	Eine Kurzbeschreibung des Gateways
DNS-Name [cmdb_ci_dns_name]	
Name	Der eindeutige Name oder die IP-Adresse des DNS-Hosts
IP-Adresse	Die IP-Adresse des Hosts des DNS-Hosts
AWS-Ressourcenname des Endpunkts [cmdb_ci_endpoint_arn]	
Host	Der Host-Name oder die IP-Adresse des Endpunkts
ARN	Die ID (Amazon-Ressourcenname) anderer AWS-Entitäten, mit denen das Gateway eine Verbindung herstellt

Beziehungen von Konfigurationselementen

Diese Beziehungen sollen die AWS API Gateway-Erkennung unterstützen:

CI	Beziehung	CI
Cloud-Gateway [cmdb_ci_cloud_gateway]	Verwendet::Verwendet von	DNS-Name [cmdb_ci_dns_name]
	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
		Das AWS-Rechenzentrum hat Beziehungen zu anderen AWS-CIs, z. B. Verfügbarkeitszonen, Servicekonten usw. Weitere Details finden Sie unter AWS- und Azure Cloud-Erkennung in der Produktdokumentation.

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping führt die Erkennung von oben nach unten der AWS API-Gateways im Kontext von Anwendungsservices durch. Es erkennt ausgehende Verbindungen der AWS API-Gateways:

- AWS Lambda – ARN
- VPC-Link für Virtual Private Cloud
- HTTP-Endpunkt, der als konfigurierte URL auf dem API-Gateway definiert ist

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim	Standardmäßig ist der Parameter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Muster-Debugging auf (und nicht während der Discovery).	*sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Zugehörige Informationen

Testmuster für die Erkennung von AWS API Gateway und AWS Lambda

Testmuster für die Erkennung von AWS API Gateway und AWS Lambda

Führen Sie die horizontale Erkennung und die Erkennung von oben nach unten mithilfe der Muster „Amazon AWS API Gateway“ [cmdb_ci_cloud_gateway] und „Amazon AWS Lambda“ [cmdb_ci_cloud_function] aus. Überprüfen Sie, ob das Ergebnis den Erwartungen entspricht.

Vorbereitungen

Stellen Sie sicher, dass Ihre Bereitstellung alle Voraussetzungen für AWS API-Gateway-Erkennung und AWS Lambda-Erkennung erfüllt.

Erforderliche Rolle: admin

Prozedur

1. Erstellen Sie einen Anwendungsservice mit den folgenden Eigenschaften für seinen Einstiegspunkt.

Feld	Beschreibung
CI-Typ	HTTPS
URL	Die URL zum Aufruf von API Gateway Normalerweise hat API GW das folgende Format: https://{restapi_id}.execute-api.{region}.amazonaws.com/{stage_name}/ Beispiel: https://k40o0l3af6.execute-api.us-east-1.amazonaws.com/prod/. Informationen zum URL-Format finden Sie unter https://docs.aws.amazon.com/apigateway/latest/developerguide/how-to-call-api.html . **Hinweis:** Der Standardwert für den Parameter stage_name lautet *prod*.

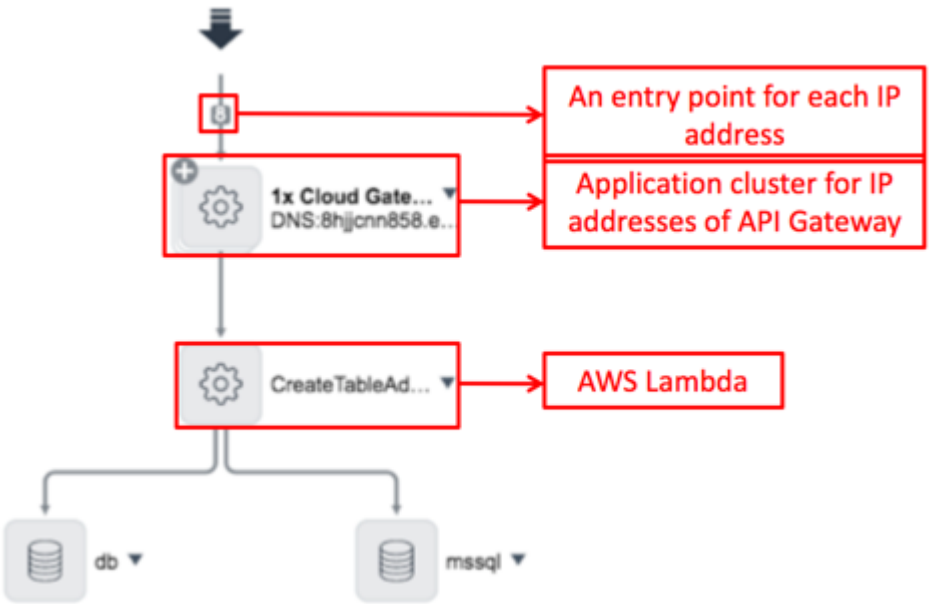
2. Klicken Sie auf **Erkennen**.
   Service-Mapping führt die Erkennung von oben nach unten mit dem Muster „Amazon AWS API Gateway“ [cmdb_ci_cloud_gateway] aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nachdem Service-Mapping die Identifizierung des API Gateway-Konfigurationselements (CI) abgeschlossen hat, führt es den Verbindungsabschnitt **Connection to APIs (Verbindung zu APIs)** aus und erkennt die Verbindung zu AWS Lambda. Anschließend wird das Muster „Amazon AWS Lambda“ [cmdb_ci_cloud_funktion] ausgeführt und das AWS Lambda-CI identifiziert.

3. Nachdem dieser Anwendungsservice von Service-Mapping erkannt wurde, überprüfen Sie, ob AWS-Komponenten richtig erkannt und identifiziert wurden.
Überprüfen Sie, ob die folgenden Aktionen ausgeführt werden:

   - Service-Mapping die URL korrekt auflöst, alle zugehörigen IP-Adressen findet und einen Einstiegspunkt für jede IP-Adresse erstellt.



   - Service-Mapping identifiziert das AWS API Gateway und erstellt ein Anwendungscluster für die IP-Adresse.
   - Im Bereich **Eigenschaften** werden die Eigenschaften für das AWS API Gateway angezeigt: Cloud-Gateway [cmdb_ci_cloud_gateway].
   - Service-Mapping erkennt AWS Lambda, das mit dem Anwendungscluster für API Gateway verbunden ist.
   - Service-Mapping erkennt die mit AWS Lambda verbundenen Datenbanken.

AWS Discovery von Auto Scaling-Gruppen

Die Anwendung ® Discovery verwendet das Muster AWS „ Auto Scaling-Gruppen“ und Auto Scaling-Erweiterungen, um AWS Auto Scaling-Gruppen zu finden. Das Erkennen einiger dieser Ressourcen erfordert die Installation der Anwendung Muster für Discovery und Service-Mapping aus dem ® Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Konfigurierte AWS Anmeldeinformationen

Konfigurieren Sie in Ihrer -Instanz Anmeldeinformationen vom Typ **AWS-Anmeldeinformationen**, und legen Sie für auf **Aktiv**fest. Weitere Informationen finden Sie unter Zugriffseinrichtung für AWS-Servicekonten.

Konfigurierter Cloud-Serviceaccount

Konfigurieren Sie den Service-Account AWS, der in der Instanz ServiceNow gültig ist. Weitere Informationen finden Sie unter AWS-Servicekonten einrichten.

Es wurden Anwenderberechtigungen für die Ausführung des API-Aufrufs für die Liste der AWS Auto Scaling-Gruppen konfiguriert

Erteilen Sie die Benutzerberechtigung zum Ausführen der folgenden API: https://autoscaling.amazonaws.com/?Action=DescribeAutoScalingGroups&Version=2011-01-01

Weitere Informationen hierzu finden Sie unter Erkennung von Amazon AWS-Cloud-Komponenten mithilfe von Mustern.

Konfigurierter Cloud-Discovery-Zeitplan

Erstellen Sie einen Cloud-Anwendungszeitplan zum Erkennen von AWS Auto Scaling-Gruppen, und konfigurieren Sie die Attribute. Legen Sie **Discovery** auf **Cloud-Anwendung**fest. Weitere Informationen finden Sie unter Zeitpläne für die Erkennung von Cloud-Ressourcen im Discovery-Arbeitsbereicherstellen

Konfigurationen für AWS Auto Scaling-Gruppen

Navigieren Sie zur Tabelle „Haupt-CI“ (Instanzskalierungssatz), und vergewissern Sie sich, dass die Konfigurationen wie folgt festgelegt sind:

Neue Felder für Tabelle – [cmdb_ci_instance_scale_set]

Elementname	Typ	Bezeichnung	Max. Länge
gewünschte_Kapazität	Ganzzahl	Gewünschte Kapazität	32
min_size	Ganzzahl	Mindestgröße	32
max_size	Ganzzahl	Maximale Größe	32
health_check_type	Zeichenfolge	Integritätsprüfungstyp	128

AWS Auto Scaling-Gruppen-Tags.

Die Mustererweiterung wird automatisch angezeigt und sammelt die Tags der automatischen Skalierung (ab Release November 2022, Version 1.0.95).

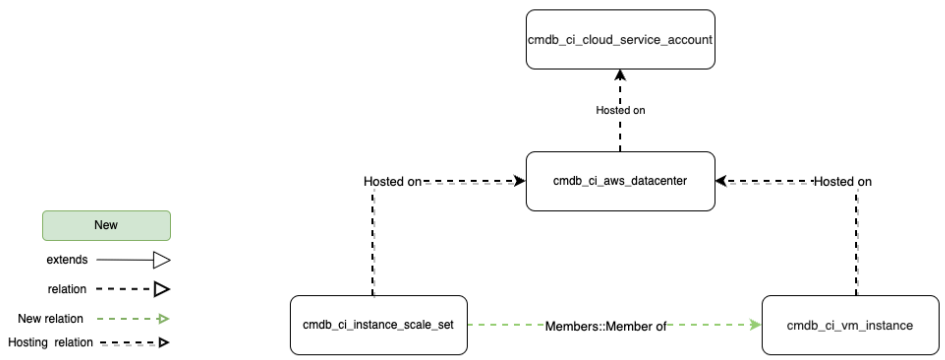
Daten, die während der Horizontal-Discovery von AWS Auto Scaling-Gruppen erfasst wurden

Feld	Beschreibung
Haupt-CI (Instanzskalierungssatz) [cmdb_ci_instance_scale_set]	
object_id	Der Amazon-Ressourcenname (ARN) der Auto Scaling-Gruppe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
name	Der Amazon-Ressourcenname (ARN) der Auto Scaling-Gruppe.
install_status	Der Installationsstatus der Auto Scaling-Gruppe (installiert).
operational_status	Der Betriebsstatus der Auto Scaling-Gruppe (funktionsfähig).
gewünschte_Kapazität	Gewünschte Größe der Gruppe
max_size	Die maximale Größe der Gruppe.
min_size	Die Mindestgröße der Gruppe.
VM-Instanz [cmdb_ci_vm_instance]	
object_id	Die Instanz-ID der VM.
Schlüsselwert [cmdb_key_value]	
Key	Der Schlüssel des Ressourcen-Tags.
Wert	Der Wert des Ressourcen-Tags.

AWS Automatische EC2-Skalierung – Klassenmodell



Musterbeziehungen

CI	Beziehungstyp	CI
AWS-Rechenzentrum [cmdb_ci_aws_datacenter]	Gehostet auf::Hostet	Service-Account [cmdb_ci_cloud_service_account]
Instanzskalierungssatz [cmdb_ci_instance_scale_set]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Instanzskalierungssatz [cmdb_ci_instance_scale_set]	Mitglieder::Mitglied von	VM-Instanz [cmdb_ci_vm_instance]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Musterbeziehungen (Fortsetzung)

CI	Beziehungstyp	CI
		Hinweis: EC2-VM
Schlüsselwert [cmdb_key_value]	Nur Referenz (configuration_item)	Instanzskalierungssatz [cmdb_ci_instance_scale_set]

Zugehörige Informationen

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Amazon AWS Cloud-Komponentenerkennung mithilfe von Mustern

AWS Cognito-Erkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping verwenden das Muster „Amazon AWS Cognito“, um Authentifizierungs-, Autorisierungs- und Benutzerverwaltungsfunktionen für AWS-Kunden bereitzustellen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Sie können dieses Muster auf der Now Platform mit London Patch 8, Madrid Patch 2 oder spätere Releases verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Benutzerberechtigungen

Gewähren Sie einem Benutzer eine Leseberechtigung, um die folgende API auszuführen:

- https://cognito-idp.<region>.amazonaws.com
- Methode: POST
- Body: {\"MaxResults\": 10}
- Headers: X-Amz-Target:AWSCognitoIdentityProviderService.ListUserPools,Content-Type:application/x-amz-json-1.0

AWS-Anmeldeinformationen

Konfigurieren Sie auf Ihrer Instanz Anmeldeinformationen des Typs **AWS-Anmeldeinformationen**, und setzen Sie sie auf **Aktiv**.

Cloud-Servicekonto

Konfigurieren Sie auf Ihrer Instanz das Cloud-Servicekonto vom Typ **AWS-Rechenzentrum**, und setzen Sie es auf **AWS-Konto-ID** . Verwenden Sie die zuvor in **AWS-Anmeldeinformationen** definierten Anmeldeinformationen.

Discovery Zeitplan

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Cloud-Anwendungszeitplan für die Erkennung von AWS Cognito, und konfigurieren Sie die Attribute. Legen Sie Erkennung auf **Cloud-Anwendung** fest.

Ausführungsmuster

Erstellen und definieren Sie das Ausführungsmuster ohne Server für die Erkennung von Cloud-Anwendungen.

1. Erstellen Sie neue **Cloud-Ausführungsmuster**.
2. Definieren Sie den **Namen**.
3. Stellen Sie sicher, dass **Aktiv** auf „true“ gesetzt ist.
4. Stellen Sie sicher, dass die **Domäne** global ist.
5. Wählen Sie das **AWS-Muster** aus, das Sie ausführen möchten.
6. Erstellen Sie mehrere Datensätze, wenn Sie mehrere Muster ausführen möchten.

Erkennungszeitplan für vollständige AWS Discovery

Erstellen Sie einen Erkennungszeitplan aus dem **Cloud-Servicekonto**, das im vorherigen Verfahren erstellt wurde.

1. Klicken Sie auf **Discover Datacenter (Rechenzentren erkennen)**, und warten Sie, bis der Vorgang abgeschlossen ist.
2. Klicken Sie auf **Discovery Zeitplan erstellen**.
3. Dieser neue Zeitplan wird unter dem Discovery-Zeitplan erstellt und führt alle AWS-Muster aus.

Von Discovery und Service-Mapping während der horizontalen Erkennung und der Erkennung von oben nach unten erfasste Daten

Das Muster „AWS Cognito“ sammelt Daten.

Vom Muster „AWS Cognito“ gesammelte Informationen

Feld	Beschreibung
Haupt-CI: cmdb_ci_cloud_authentication	
name	Ein beschreibender Name, der zur Identifizierung des Benutzer-Pools verwendet wird
object_id	Sie entspricht der account_id und wird von IRE-Identifizierungsregeln verwendet.
Fqdn	Beispiel für eine ARN: arn:aws:cognito-idp:eu-west-1:751200741520:userpool/eu-west-1_fim5E2mix

Tags werden auch von einem Erweiterungsabschnitt gesammelt, der dem Muster entsprechend ausgeführt wird. Die Tagging-API für AWS gibt den Ressourcentyp Cognito an.

Gesammelte Informationen aus den AWS Cognito-Tags

Feld	Beschreibung
cmdb_key_value	
key	Der tatsächliche Tag-Schlüssel

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gesammelte Informationen aus den AWS Cognito-Tags (Fortsetzung)

Feld	Beschreibung
Wert	Der Tag-Wert
configuration_item	Die eindeutige Ressourcen-ID (ARN), die die Ressource in der AWS-Konsole identifiziert

CI-Beziehungen

Das Muster „AWS Cognito“ erstellt die folgenden CI-Beziehungen:

CI	Beziehung	CI
Cloud-Authentifizierung [cmdb_ci_cloud_authentication]	Hostet::Gehostet auf	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter *sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennung von AWS-DB-Clustern

ServiceNow Discovery verwendet das Erkennungsmuster für AWS-DB-Cluster, um Aurora-DB-Cluster, serverlose Aurora-Ressourcen, Amazon Neptune-DB-Instanzen und Amazon DocumentDB-Instanzen zu suchen und zuzuordnen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Die erkannten DB-Cluster bilden neue Beziehungen mit den DB-Instanzen, die mit dem Muster „AWS Relational Database Service“ erkannt wurden. Daher wird das Muster für AWS-DB-Cluster während der Erkennung nach dem Muster „AWS Relational Database Service“ ausgelöst. Weitere Informationen finden Sie unter Amazon AWS Relational Database Service-Erkennung.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Installieren Sie die Anwendung Discovery and Service Mapping Patterns (Version 1.0.75) aus dem ServiceNow Store.
- Konfigurieren Sie auf der Now Platform die AWS-Anmeldeinformationen mithilfe eines geheimen Schlüssels und eines Zugriffsschlüssels.
- Erstellen Sie ein Servicekonto. Legen Sie die **Konto-ID** auf die Amazon-Konto-ID fest, zu der RDS gehört. Verwenden Sie die Konto-ID, die in der AWS-Managementkonsole angezeigt wird.
- Legen Sie schreibgeschützte Berechtigungen für diese REST APIs fest:
  - https://rds.<REGION>.amazonaws.com/?Action=DescribeDBInstances
  - https://rds.<REGION>.amazonaws.com/?Action=DescribeDBClusters
  - https://rds.<REGION>.amazonaws.com/?Action=DescribeDBInstances&DBInstanceIdentifier=<input_object_id> for events discovery
  - https://tagging.<REGION>.amazonaws.com/ for tags discovery
- Laden Sie für Cloud-Discovery das Muster „Discovery and Service Mapping“ aus dem ServiceNow Store herunter.
- Stellen Sie bei der Installation von MID-Serversicher, dass der Hostcomputer die auf der Dokumentationswebsite ServiceNow veröffentlichten Systemanforderungen für den MID-Server erfüllt oder überschreitet.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Cloud-Datenbankcluster [cmdb_ci_cloud_db_cluster]	
Cluster-ID [cluster_id]	Enthält einen vom Benutzer angegebenen Bezeichner für das DB-Cluster. Dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
	Bezeichner ist der eindeutige Schlüssel, der ein DB-Cluster identifiziert.
Name [name]	Enthält den Namen der ursprünglichen Datenbank des DB-Clusters, die bei der Erstellung angegeben wurde. Wenn kein Name angegeben wurde, wird der Clusterbezeichner als Name verwendet. Dieser Name wird für die Lebensdauer des DB-Clusters zurückgegeben.
FQDN [fqdn]	Gibt den Verbindungsendpunkt für die primäre Instanz des DB-Clusters an.
TCP-Port [tcp_port]	Port des Datenbankendpunkts
Anbieter [vendor]	Der Anbieter, Amazon
Clusterstatus [cluster_status]	Gibt den aktuellen Status dieses DB-Clusters an.
Betriebsstatus [operational_status]	Status der Datenbank; „Verfügbar“, wenn betriebsbereit.
Cloud-Datenbank [cmdb_ci_cloud_database]	
Objekt-ID [object_id]	Der Instanzbezeichner für dieses Mitglied des DB-Clusters. **Hinweis:** Für Datenbankinstanzen wird diese Tabelle nur mit dem Attribut object_id gefüllt. Dieses Attribut ist für die Identifizierung von CIs der Cloud-Datenbank erforderlich, um sicherzustellen, dass Beziehungen zwischen den CIs und den Cloud-Datenbankclustern hergestellt werden können.
Name [name]	Enthält den Namen der ursprünglichen Datenbank des DB-Clusters, die bei der Erstellung angegeben wurde. Wenn kein Name angegeben wurde, wird der Clusterbezeichner als Name verwendet. Dieser Name wird für die Lebensdauer des DB-Clusters zurückgegeben.
FQDN [fqdn]	Gibt den Verbindungsendpunkt für die primäre Instanz des DB-Clusters an.
TCP-Port [tcp_port]	Port des Datenbankendpunkts
Anbieter [vendor]	Der Anbieter, Amazon
Betriebsstatus [operational_status]	Status der Datenbank; „Verfügbar“, wenn betriebsbereit.
IP-Adresse [cmdb_ci_ip_address]	
IP-Adresse [ip_address]	IP-Adresse des Cloud DB Cluster Writer-Endpunkts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Name [name]	IP-Adresse.
Vollständig qualifizierter Domänenname [fqdn]	Adresse des Datenbankendpunkts Der DNS-Name
Netzmaske [netmask]	IP-Netzmaske [0.0.0.0].

CI-Beziehungen

CI	Beziehung	CI
cmdb_ci_cloud_db_cluster	Cluster aus::Cluster	cmdb_ci_cloud_database
cmdb_ci_cloud_database	Gehostet auf::Hostet	cmdb_ci_aws_datacenter
cmdb_ci_cloud_db_cluster	Eigentümer von::Eigentum von	cmdb_ci_ip_address
cmdb_ci_cloud_database	Eigentümer von::Eigentum von	cmdb_ci_ip_address
cmdb_key_value	Nur Referenz	cmdb_ci_cloud_db_cluster
cmdb_key_value	Nur Referenz	cmdb_ci_cloud_database

Discovery von Amazon-ECS-Ressourcen

Die Anwendung ServiceNow Discovery verwendet das Muster Amazon AWS - ECS, um nach Ressourcen zu suchen, die vom Amazon Elastic Container Service (Amazon ECS) verwaltet werden. Dies umfasst Ressourcen, die beim Starttyp Fargate ausgeführt werden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Amazon ECS ist ein hoch skalierbarer, schneller Containerverwaltungsservice, der das Ausführen, Anhalten und Verwalten von Docker -Containern vereinfacht. AWS Fargate ist eine Rechen-Engine für Amazon ECS, mit der AWS Kunden Container ausführen können, ohne Server oder Cluster verwalten zu müssen.

Discovery verwendet das Muster Amazon AWS - ECS, um eine horizontale Discovery auszuführen.

Ab Muster für Discovery und Service-Mapping Version 1.18.0 unterstützt das Muster Amazon AWS - ECS die Discovery von Amazon Elastic Container Registry-Images (Amazon ECR).

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Erstellen Sie AWS -Anmeldeinformationen mit Anzeigeberechtigungen für ECS-Ressourcen

Erstellen Sie in der Konsole AWS Anmeldeinformationen vom AWS Typ mit Berechtigungen zum Anzeigen von ECS-Ressourcen. Weitere Informationen finden Sie unter: https://docs.aws.amazon.com/en_pv/AmazonECS/latest/userguide/get-set-up-for-amazon-ecs.html .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die API-Anforderungen verwenden AWS die Signaturversion 4 zur Authentifizierung. Wenn die richtigen Anmeldeinformationen angegeben sind, erfolgt die Authentifizierung intern für die Musterschritte „Cloud API Call“.

Erstellen Sie AWS Cloud-Anmeldeinformationsdatensätze, oder verwenden Sie temporäre Anmeldeinformationen

Erstellen Sie in Now Platformdie Anmeldeinformationsdatensätze AWS. Sie können auch temporäre Anmeldeinformationen verwenden, die vom AWS Security Token Service (AWS STS) für IAM-Rollen generiert wurden. Weitere Informationen finden Sie unter Cloud-Anmeldeinformationen

Erstellen Sie AWS Cloud-Service-Accounts

- Erstellen Sie in Now PlatformCloud-Service-Accounts für AWS mit permanenten oder temporären AWS -Anmeldeinformationen. Weitere Informationen finden Sie unter AWS-Servicekonten einrichten.
- Wählen Sie im Datensatz „Cloud-Servicekonto“ **die Option Rechenzentren erkennen aus**, um AWS Rechenzentren (LDCs) für das konfigurierte Cloud-Servicekonto AWS zu suchen.

Planen Sie eine Discovery AWS .

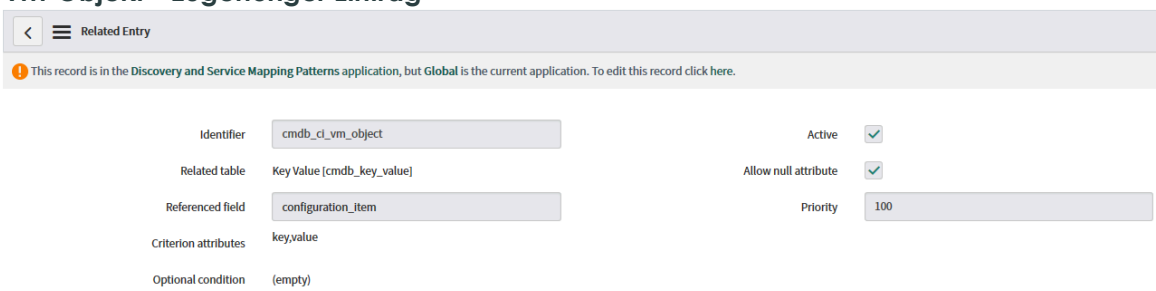
Planen Sie in Now Platformentweder eine vollständige AWS -Discovery oder nur eine ECS-Muster-Discovery. Weitere Informationen zum Planen einer Discovery finden Sie unter Horizontale Erkennung planen.

Überprüfen Sie die Konfiguration des VM-Objektdatensatzes, um die Ressourcen-Tags zu finden

Damit das Muster die Ressourcen-Tags finden kann, muss die übergeordnete ECS-Tabelle (VM-Objekt) über einen zugehörigen Eintrag für die Tabelle cmdb_key_value verfügen:

1. Navigieren Sie in der Navigationsleiste Now Platform zu **Alle** > **Konfiguration** > **Identifikation/Abgleich**und wählen Sie **CI-Bezeichner**.
2. Suchen Sie den Datensatz VM-Objekt, und öffnen Sie ihn.
3. Wählen Sie die Registerkarte **Zugehörige Einträge** aus, und vergewissern Sie sich, dass sie wie in der Abbildung „Zugehöriger Eintrag des VM-Objekts“ gezeigt konfiguriert ist. Ist dies nicht der Fall, geben Sie einen neuen zugehörigen Eintrag an: Wählen Sie in der zugehörigen Liste Zugehörige Einträge **Neu**aus, füllen Sie das Formular aus, und wählen Sie **Absenden aus**.

VM-Objekt – zugehöriger Eintrag



Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das Muster Amazon AWS - ECS ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]

Feld	Beschreibung
Objekt-ID [object_id]	Der Ressourcenname (ARN) Amazon, der den Cluster identifiziert.
Name [name]	Eine vom Benutzer generierte Zeichenfolge zur Identifizierung des Clusters
Anzahl der registrierten Containerinstanzen [registered_container_instances_count]	Die Anzahl der im Cluster registrierten Container-Instanzen. Der Status dieser Container-Instanzen kann entweder „ACTIVE“ oder „DRAINING“ sein.

AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]

Feld	Beschreibung
Objekt-ID [object_id]	Die vollständige ARN der Aufgabendefinition
Name [name]	Der Name der Familie, für die diese Aufgabendefinition registriert ist.
Überarbeitung [revision]	Die Überarbeitung der Aufgabe in einer bestimmten Familie. Dies ist die Versionsnummer der Aufgabendefinition in einer Familie.
Netzwerkmodus [network_mode]	Der Netzwerkmodus Docker, der für die Container in der Aufgabe verwendet werden soll. Gültige Werte: none, bridge, awsvpc, host.
CPU [CPU]	Die Anzahl der von der Aufgabe verwendeten CPU-Einheiten
Arbeitsspeicher [memory]	Die Menge des von der Aufgabe verwendeten Arbeitsspeichers in Megabyte (MiB).

AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]

Feld	Beschreibung
Objekt-ID [object_id]	Die ARN, die die Aufgabe identifiziert
Name [name]	Eine vom Benutzer generierte Zeichenfolge, um die Aufgabe zu identifizieren
Starttyp [launch_type]	Der Starttyp, für den die Aufgabe ausgeführt wird
Betriebsstatus [operation_status]	Der Integritätsstatus der Aufgabe, der von der Integrität der darin enthaltenen wesentlichen Container bestimmt wird
CPU [CPU]	Die Anzahl der von der Aufgabe verwendeten CPU-Einheiten, wie in der Aufgabendefinition angegeben
Arbeitsspeicher [memory]	Die von der Aufgabe verwendete Speichermenge in MiB, wie in der Aufgabendefinition angegeben

AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]

Feld	Beschreibung
Objekt-ID [object_id]	Die ARN, die den Service identifiziert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service] (Fortsetzung)

Feld	Beschreibung
Name [name]	Der Name des Services
Starttyp [launch_type]	Der Starttyp, für den der Service ausgeführt wird
Zeitplanungsstrategie [scheduling_strategy]	Die für den Service zu verwendende Zeitplanstrategie

Docker-Container [cmdb_ci_docker_container]

Feld	Beschreibung
Container ID [container_id]	Die ARN des Containers
Name [name]	Der Name des Containers
Status [status]	Der zuletzt bekannte Status des Containers
Betriebsstatus [operational_status]	Der Integritätsstatus des Containers
CPU [CPU]	Die Anzahl der für den Container festgelegten CPU-Einheiten
Arbeitsspeicher [memory]	Die feste Grenze des Arbeitsspeichers in MiB, die für den Container festgelegt ist

VM-Instanz [cmdb_ci_vm_instance]

Feld	Beschreibung
Objekt-ID [object_id]	Der ARN, der die VM-Instanz identifiziert. **Hinweis:** Vollständige Informationen zur VM-Instanz werden in einem anderen EC2-Cloudmuster erkannt. Bei der ECS-Ressourcen-Discovery Amazon wird nur die object_id analysiert, um die eindeutige Identifizierung des CI zu unterstützen.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Der Tag-Schlüssel
Wert [value]	Der Tag-Wert

Docker-Image [cmdb_ci_docker_image]

Feld	Beschreibung
Name [name]	Name des Docker Bildes.
Bildauszug [image_digest]	Eindeutiger Bezeichner für das Docker -Image.
Image-ID [image_id]	Eindeutiger Bezeichner mit 12 Zeichen für das Bild Docker.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Container-Repository [cmdb_ci_container_repository]

Feld	Beschreibung
Name [name]	Vollqualifizierter Name des Repositorys, das das Image Docker enthält.

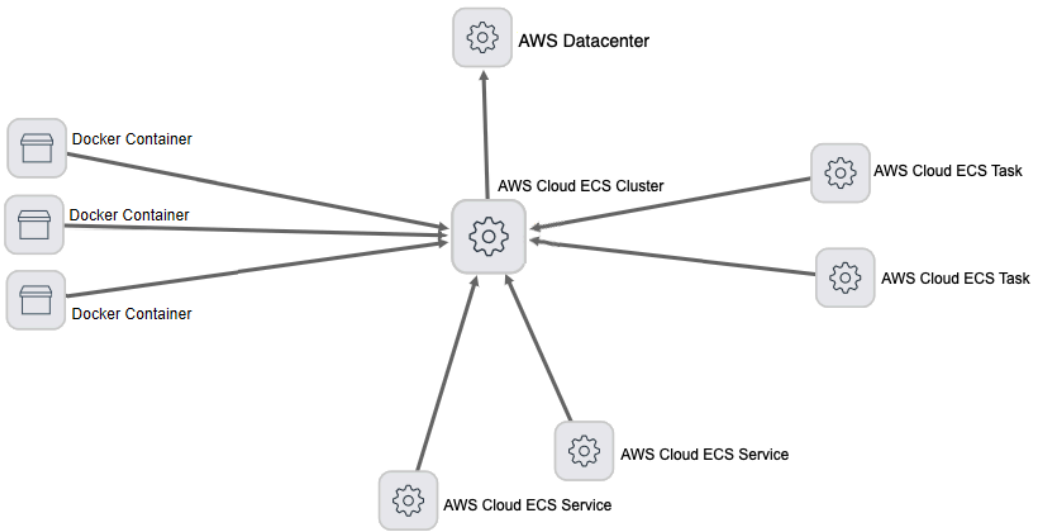
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]

Feld	Beschreibung
Name [name]	Das Image-Tag Docker.
Kategorie [category]	Vollqualifizierter Name des Repositorys, das das Image Docker enthält.

In der Zuordnung der Abhängigkeitsansichten können Sie alle erkannten Ressourcen in Ihrer Organisation anzeigen, die von Amazon ECS verwaltet werden, sowie die Beziehungen zwischen ihnen.

In diesem Beispiel wird das Cloud-ECS-Cluster-CI AWS in einem Rechenzentrum AWS gehostet. Es führt zwei AWS Cloud-ECS-Aufgaben und zwei AWS Cloud-ECS-Services aus und verwendet drei Docker Container.

Dependency Views-Beispielzuordnung



CI-Beziehungen

Diese Beziehungen werden erstellt, um die Erkennung von Amazon ECS-Ressourcen zu unterstützen.

CI	Beziehung	CI
AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]	Verwendet::Verwendet von	VM-Instanz [cmdb_ci_vm_instance]
AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]	Wird ausgeführt:Wird ausgeführt auf	AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]
AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]	Wird ausgeführt:Wird ausgeführt auf	AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]	Gehostet auf::Hostet	AWS-Rechenzentren
AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]	Erweitert::Erweitert um	VM-Objekt [cmdb_ci_vm_object]
AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]	Verwendet::Verwendet von	AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]
AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]	Gehostet auf::Hostet	AWS-Rechenzentren
AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]	Wird ausgeführt auf::Wird ausgeführt	AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]
AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]	Erweitert::Erweitert um	VM-Objekt [cmdb_ci_vm_object]
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Wird ausgeführt auf::Wird ausgeführt	VM-Instanz [cmdb_ci_vm_instance]
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Wird ausgeführt auf::Wird ausgeführt	Docker-Container [cmdb_ci_docker_container]
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Verwendet::Verwendet von	AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Gehostet auf::Hostet	AWS-Rechenzentren
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Wird ausgeführt auf::Wird ausgeführt	AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]
AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]	Erweitert::Erweitert um	VM-Objekt [cmdb_ci_vm_object]
AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]	Verwendet von::Verwendet	AWS Cloud ECS-Service [cmdb_ci_cloud_ecs_service]
AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]	Verwendet von::Verwendet	AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]
AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]	Gehostet auf::Hostet	AWS-Rechenzentren
AWS Cloud ECS-Aufgabendefinition [cmdb_ci_cloud_ecs_task_definition]	Erweitert::Erweitert um	VM-Objekt [cmdb_ci_vm_object]
Container-Repository [cmdb_ci_container_repository]	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter]
Container-Repository-Eintrag [cmdb_ci_container_repository_entry]	Gehostet auf::Hostet	Container-Repository [cmdb_ci_container_repository]
Docker-Container [cmdb_ci_docker_container]	Gehostet auf::Hostet	AWS-Rechenzentren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Docker-Container [cmdb_ci_docker_container]	Wird ausgeführt:Wird ausgeführt auf	AWS Cloud ECS-Aufgabe [cmdb_ci_cloud_ecs_task]
Docker-Container [cmdb_ci_docker_container]	Verwendet von::Verwendet	AWS Cloud ECS-Cluster [cmdb_ci_cloud_ecs_cluster]
Docker-Image [cmdb_ci_docker_image]	Bereitgestellt von::Bereitgestellt	Container-Repository-Eintrag [cmdb_ci_container_repository_entry]
Docker-Image [cmdb_ci_docker_image]	Instanziiert::Instanziiert von	Docker-Container [cmdb_ci_docker_container]

AWS Lambda-Erkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping können Lambda-Funktionen suchen und zuordnen, die in Ihrer AWS-Cloud ausgeführt werden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery und Service-Mapping verwenden das Muster „Amazon AWS Lambda“, um eine horizontale Erkennung und eine Erkennung von oben nach unten auszuführen. Wenn Sie die Cloud-Erkennung ausführen, fragt Ihre Instanz Ihr AWS-Servicekonto mit den erforderlichen Anmeldeinformationen ab und führt dann eine Abfrage aus, um Lambda-Informationen zu erhalten. Das Muster analysiert diese Informationen, die dann in der CMDB gespeichert werden.

Sie können dieses Muster auf der ServiceNow-Plattform mit Jakarta Patch 10, Kingston Patch 8 oder London Patch 1 verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Update Set

Wenn Ihre Instanz die Version Jakarta oder Istanbul hat, importieren Sie das Update Set, das in „KB0679927 : AWS Lambda top-down discovery update set (Update Set für AWS Lambda-Erkennung von oben nach unten)“ bereitgestellt wird. Dieses Update Set ist für Service-Mapping erforderlich.

Benutzerrichtlinie für AWS-Benutzer

Wenn Sie Identity and Access Management (IAM) verwenden, um Benutzer auf der AWS-Plattform (Amazon Web Services) zu verwalten, stellen Sie sicher, dass Sie eine Benutzerrichtlinie für den AWS-Benutzer erstellt haben. Weitere Informationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern in der Dokumentation zu ServiceNow Cloud Provisioning and Governance.

AWS-Servicekonto mit Anmeldeinformationen

Sie müssen Ihr Servicekonto mit den entsprechenden AWS-Anmeldeinformationen einrichten. Sie führen die Erkennung über das Servicekonten-Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu Servicekonten für Discovery und Service-Mapping finden Sie in der Produktdokumentation.

Servicekonto

Erstellen Sie ein Servicekonto auf der ServiceNow-Plattform. Legen Sie die Konto-ID auf die Amazon-Konto-ID fest, zu der AWS Lambda gehört. Verwenden Sie die Konto-ID, wie sie in der AWS-Verwaltungskonsole angezeigt wird. Stellen Sie sicher, dass der MID-Server auf der virtuellen Maschine platziert wird, die Teil des zu erkennenden Servicekontos ist.

Logische Rechenzentren mithilfe der horizontalen Erkennung erkennen

Klicken Sie im Formular „Cloud-Servicekonto“ unter **Zugehörige Links** auf **Rechenzentren erkennen**.

Benutzerberechtigungen

Gewähren Sie einem Benutzer die Berechtigung zum Ausführen der ListFunctions-API mit der Ressource: arn:aws:lambda:region:account-id: function:function-name. Gewähren Sie einem Benutzer die Berechtigung zum Ausführen der GetFunction-API mit der Ressource: „*“.

Amazon-Ressourcenname (ARN)

(Optional für Anwendungsservices, die ARN als Einstiegspunkt verwenden) Stellen Sie sicher, dass Sie den ARN für das zu erkennende AWS Lambda kennen. ARNs dienen als Ressourcenbezeichner für Amazon Web Services.

Host

Wenn Ihre Instanz die Version Jakarta oder Istanbul hat, verwenden Sie den folgenden Host: 127.0.0.1.

Cloud-Discovery

Laden Sie für Cloud-Discovery das Muster „Discovery and Service Mapping“ aus dem ServiceNow Store herunter.

MID-Server

Stellen Sie bei der Installation von MID-Serversicher, dass der Hostcomputer die auf der Dokumentationswebsite ServiceNow veröffentlichten Systemanforderungen für den MID-Server erfüllt oder überschreitet.

Von Discovery während der horizontalen Erkennung erfasste Daten

Horizontale Erkennung trägt diese Daten in die CMDB ein:

Tabelle und Feld	Beschreibung
Cloud-Funktion [cmdb_ci_cloud_function]	
Name [name]	Der Name der Funktion
Objekt-ID [object_id]	Die ID (Amazon-Ressourcenname) der AWS Lamdba-Funktion, z. B. `arn:aws:lambda:{datacenter}1:751200741520:function:{function-name}`
Version [version]	Die Version der Funktion. Beispielsweise steht `$Latest` für die neueste veröffentlichte Version.
Sprache [language]	Die Laufzeitumgebung oder Sprache und Version, in der die Funktion geschrieben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
	ist, z. B. `Node.js6.10` für JavaScript Version 6.10.
Code-Speicherort-URL [code_location_url]	Die URL der Funktion, die Sie über die API Gateway-Konsole erstellt haben
CodeSha256 [codesha256]	Die kryptografische Hash-Signatur für die Funktion
Codegröße [code_size]	Die Größe des Funktionscodes in MB
Letzte Änderung an der Funktion [function_last_modified]	Das Datum, an dem die Funktion in Ihrer AWS Lamdba-Umgebung zuletzt geändert wurde

Hinweis: Um alle diese Felder anzuzeigen, müssen Sie das Formularlayout wie in der Produktdokumentation beschrieben konfigurieren.

CI-Beziehungen

Diese Beziehungen sollen die AWS Lambda-Erkennung unterstützen:

CI	Beziehung	CI
Cloudfunktion [cmdb_ci_cloud_function]	Verwendet::Verwendet von	Cloud-Datenbank [cmdb_ci_cloud_database]
	Gehostet auf::Hostet	AWS-Rechenzentrum [cmdb_ci_aws_datacenter] Das AWS-Rechenzentrum hat Beziehungen zu anderen AWS-CIs, z. B. Verfügbarkeitszonen, Servicekonten usw. Weitere Informationen finden Sie unter AWS und Azure Cloud-Erkennung in der Produktdokumentation.
	Stellt bereit::Bereitgestellt von	Cloud Event-Quelle [cmdb_ci_cloud_event_source] Dieses CI kann eine beliebige Event-Quelle sein, die die Cloud-Funktion oder das API-Gateway auslöst.

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping führt die Erkennung von oben nach unten von AWS Lambda im Kontext von Anwendungsservices durch. Es erkennt ausgehende Verbindungen von AWS Lambda:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- AWS API-Gateway
- Amazon Relational Database Service (RDS)
- Weitere Instanz von AWS Lambda innerhalb oder außerhalb der aktuellen Region, die ARN verwendet

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter *sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Zugehörige Informationen

Testmuster für die Erkennung von AWS API Gateway und AWS Lambda

Cloud-REST-Abfrage für Cloud-Computing-Geräte definieren

AWS MemoryDB für Redis

Die Anwendung ® Discovery verwendet das Muster AWS MemoryDB for Redis und Erweiterungen, um AWS MemoryDB for Redis zu finden. Das Erkennen einiger dieser Ressourcen erfordert die Installation der Anwendung Muster für Discovery und Service-Mapping aus dem ® Store.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Konfigurierte AWS Anmeldeinformationen

Konfigurieren Sie in Ihrer -Instanz Anmeldeinformationen vom Typ **AWS-Anmeldeinformationen**. Weitere Informationen finden Sie unter Zugriffseinrichtung für AWS-Servicekonten.

Konfigurierter Cloud-Serviceaccount

Konfigurieren Sie den Service-Account AWS, der in der Instanz ServiceNow gültig ist. Weitere Informationen finden Sie unter AWS-Servicekonten einrichten.

Konfigurierte Anwenderberechtigungen zum Ausführen der Liste AWS MemoryDB for Redis API-Aufrufe

Erteilen Sie die Benutzerberechtigung zum Ausführen der folgenden API:

- https://memory-db.{region}.amazonaws.com?Action=DescribeClusters&ShowShardDetails=wahr
- https://Speicher-DB.{Region}.amazonaws.com?Aktion=ListTags&ResourceArn={arn}

Weitere Informationen hierzu finden Sie unter Erkennung von Amazon AWS-Cloud-Komponenten anhand von Mustern.

Konfigurierter Cloud-Discovery-Zeitplan

Erstellen Sie einen Cloud-Anwendungszeitplan zum Erkennen von AWS -Rechenzentren. Legen Sie **Discovery** auf **Cloud-Discovery**fest. Weitere Informationen finden Sie unter: Zeitpläne für die Erkennung von Cloud-Ressourcen im Cloud-Discovery-Arbeitsbereich erstellen

Daten, die während der Horizontal-Discovery von AWS MemoryDB für Redis erfasst wurden

Feld	Beschreibung
Haupt-CI [cmdb_ci_cloud_database]	
ARN	Amazon-Ressourcenname eines einzelnen Knotens im Cluster. Die Werte werden in die Spalte „Objekt-ID“ [object_id] eingetragen.
Name	Der Name eines einzelnen Knotens im Cluster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
FQDN	Der vollständig qualifizierte Domänenname jedes Knotens im Cluster
TCP _Port	Der TCP-Port, von dem ein einzelner Knoten im Cluster Datenverkehr erhält.
Typ	Der Typ der Datenbank ist MemoryDB.
Datenbank-Cluster [cmdb_ci_cloud_db_cluster]	
ARN	Der Amazon-Ressourcenname des Clusters. Die Werte werden in die Spalte „Objekt-ID“ [object_id] eingetragen.
Name	Name des Clusters
FQDN	Der vollständig qualifizierte Domänenname des Clusters.
TCP _Port	Der TCP-Port, von dem der Cluster Datenverkehr erhält.

Musterbeziehungen

CI	Beziehungstyp	CI
[cmdb_ci]	Erweitert::Erweitert	[cmdb_ci_appl]
[cmdb_ci_appl]	Erweitert::Erweitert	[cmdb_ci_cloud_database]
[cmdb_ci_cloud_db_cluster]	Cluster::Cluster von	[cmdb_ci_cloud_db_cluster]
[cmdb_ci_cloud_db_cluster]	Nur Referenz (configuration_item)	[cmdb_key_value]

Zugehörige Informationen

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Amazon AWS Cloud-Komponentenerkennung mithilfe von Mustern

AWS Tag-Erkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping können Muster verwenden, um die Tags für AWS-Ressourcen und CI-Typen (Konfigurationselemente) zu erkennen und die CMDB dann mit diesen Erkennungen zu füllen. Um einige dieser Ressourcen zu erkennen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Dieses Tag-spezifische Erkennungsmuster ist zusätzlich zu den anderen im ServiceNow Store verfügbaren AWS-Mustern vorhanden. Dieses Muster erweitert die Muster, die zum Erkennen der jeweiligen AWS-Ressourcen verwendet werden.

Sie können dieses Muster verwenden, um Tags in Now Platform® mit dem Release New York oder höherzu erkennen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

AWS-Anmeldeinformationen

- Konfigurieren Sie auf der Now Platform AWS-Anmeldeinformationen mithilfe eines geheimen Schlüssels und eines Zugriffsschlüssels.
- Besorgen Se sich eine Amazon- **Konto-ID**. Verwenden Sie die Konto-ID, wie sie in der AWS-Verwaltungskonsole angezeigt wird. Sie können Discovery über das Servicekonten-Formular ausführen.
- Legen Sie schreibgeschützte Berechtigungen für die folgende URL fest: `https//tagging.<region>.amazonaws.com.`

Discovery Zeitplan

Erstellen Sie einen Zeitplan für das relevante AWS-Servicekonto, wie im Abschnitt zum Planen der Erkennung für ein Servicekonto in der ServiceNow® Cloud Provisioning and Governance-Dokumentation beschrieben.

Die CMDB wird mit Tags für die folgenden AWS-Ressourcen und CI-Typen (Konfigurationselement) gefüllt:

- API Gateway [cmdb_ci_cloud_gateway]
- Cognito [cmdb_ci_cloud_authentication]
- DynamoDB [cmdb_ci_dynamodb_table]
- Lambda [cmdb_ci_cloud_function]
- RDS (Relational Database Service) [cmdb_ci_cloud_database]
- S3 [cmdb_ci_cloud_object_storage]

Hinweis: Weitere Informationen zu Tags und Mustern für jede dieser Ressourcen finden Sie in der Dokumentation der jeweiligen AWS-Ressource.

Bei der Erkennung von AWS-Tags führt das Muster die folgenden allgemeinen Aufgaben aus:

- Legt den Filter für Ressourcentypen fest: Filtert die Tags nur nach Tags, die mit dem Muster-CI-Typ in Verbindung stehen.
- Initiiert den Cloud API-Aufruf: Der API-Aufruf der Cloud-Umgebung, die die Tags sammelt und ihre Attribute in der Tag-Tabelle analysiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Analysiert den Ressourcennamen aus dem Amazon-Ressourcennamen (ARN). Jeder Amazon-Ressource wird ein Name und ein eindeutiger Bezeichner zugewiesen.

  Hinweis: Das Analysieren des Ressourcennamens ist nur für Muster erforderlich, bei denen der Hauptidentifizierungsabschnitt nicht die ARN der AWS-Ressource verwendet. Wenn dies der Fall ist, muss ein Beziehungsattribut aus der AWS ARN analysiert werden.

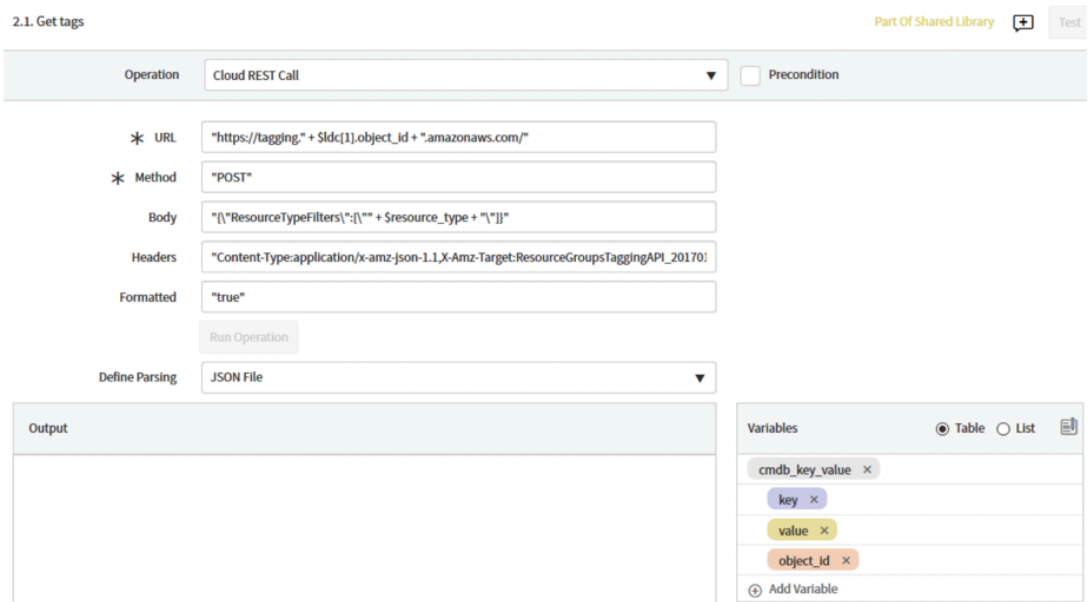
- Enthält Verweise auf den Cloud-Ressourcentyp. Stellt die Beziehung zwischen dem Tag und dem Cloud-Ressourcentyp her.

Das Muster enthält eine API mit dem Namen „Cloud Rest Call“ Post Call, die zum Sammeln der folgenden Daten verwendet wird:

- API-URL, die zum Abrufen der Daten verwendet wird — "https://tagging." + $ldc[1].object_id + ".amazonaws.com/“
- API-Hauptteil — "{\"ResourceTypeFilters\":[\"" + $resource_type + "\"]}“
- Header — "Content-Type:application/x-amz-json-1.1,X-Amz-Target:ResourceGroupsTaggingAPI_20170126.GetResources"

Diese Daten werden wie im folgenden Fenster angezeigt.

Daten aus dem Cloud REST-Aufruf



Dieses Muster sammelt die folgenden Daten während der horizontalen Erkennung:

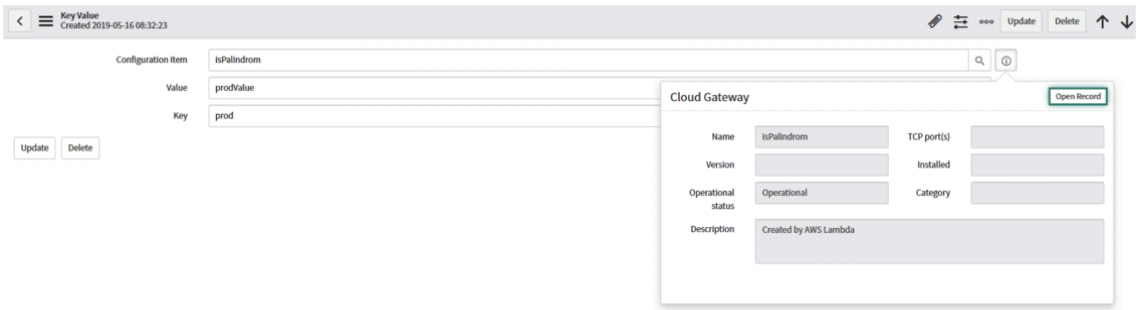
Tabelle und Feld	Zusätzliche Informationen
CI-Typ [cmdb_key_value]	
Schlüssel	Tag-Schlüssel
Wert	Tag-Wert
Object_id	Die eindeutige Ressourcen-ID, die die Ressource in der AWS-Konsole identifiziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Zusätzliche Informationen
Klassenmodell [cmdb_key_value]	
Erweitert Tabelle	Nicht zutreffend
Bezeichner – Object_id	Zugehörige Einträge zu den Cloud-Ressourcen
Metadatenregeln	Nicht zutreffend

Diese Daten werden wie im folgenden Fenster angezeigt:

Während der horizontalen Erkennung erfasste Daten



AWS Discovery-Muster verwenden den folgenden EVAL:

```
var rtrn;
var name = ${cmdb_key_value[].object_id}
name = name.substring(name.lastIndexOf("restapis/")+9,name.lastIndex);
name = name.substring(0,name.indexOf("/"));
rtrn = name;
```

Ähnliche EVALS sind für Muster verfügbar, bei denen der Hauptidentifizierungsabschnitt keine ARN-Informationen in der Tabelle des Haupt-CI-Typs enthält. Wenn diese Informationen nicht verfügbar sind, muss der Tag-Erweiterungsabschnitt eine eindeutige ARN analysieren, die zum Herstellen der Beziehung zur zugehörigen Cloud-Ressource verwendet wird.

Erkennung von Cisco Switch Wireless Access Point (WAP)

Die Anwendung ServiceNow Discovery verwendet die Cisco WAP-Erweiterung, um Wireless Access Points (WAPs) zu finden, die von einem Cisco-Netzwerk-Switch gesteuert werden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Diese Erweiterung erweitert das Erkennungsmuster „Network Switch“. Weitere Informationen finden Sie unter Erkennung von Routern und Switches.

Discovery verwendet die Cisco WAP-Erweiterung zum Ausführen der horizontalen Erkennung.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Voraussetzungen im Zusammenhang mit der Erkennung von Netzwerk-Switches finden Sie unter Erkennung von Routern und Switches.

Darüber hinaus müssen diese Voraussetzungen für die Cisco WAP-Erweiterung erfüllt sein:

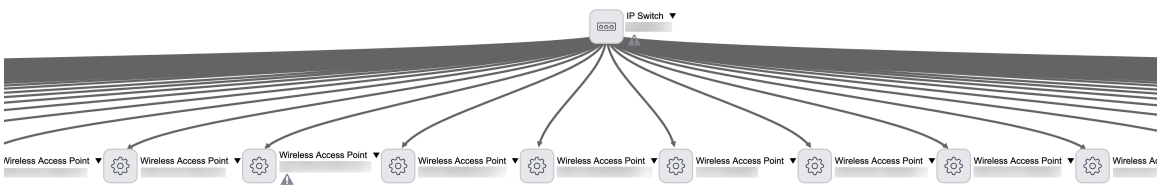
- Berechtigung zum Abfragen der OID: 1.3.6.1.4.1.14179.2.2.1.1.
- Der Client muss in der Lage sein, Erkennungsmuster auszuführen.
- Der Client muss einen Cisco-Netzwerk-Switch verwenden.
- Der Client muss SNMP-Zugriff auf den Cisco-Netzwerk-Switch haben, der die WAP-Geräte steuert.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die von der Cisco WAP-Erweiterung erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabellen und Felder	Beschreibung
Haupt-CI-Klasse [cmdb_ci_wap_network]	
Name [name]	Name, der dem WAP zugewiesen wurde. Gesammelt von bsnAPName.
MAC-Adresse [mac_address]	Die MAC-Adresse des WAP. Gesammelt von bsnAPDot3MacAddress.
IP-Adresse [ip_address]	Die IP-Adresse des WAP. Gesammelt von bsnApIpAddress.
Firmware-Version [Firmware-Version]	IOS-Version des IOS Cisco WAP. Gesammelt von bsnAPIOSVersion.
Seriennummer [serial_number]	WAP-Seriennummer Gesammelt von bsnAPSerialNumber.
Modellnummer [model_number]	WAP-Modell. Gesammelt von bsnAPModel.
snmp_sys_location	Benutzerdefinierter Speicherort des WAP. Gesammelt von bsnAPLocation.
Hersteller [manufacturer]	Hersteller des WAP (Cisco)

Die Dependency Views-Zuordnung zeigt alle erkannten Cisco WAP-CIs und deren Beziehungen untereinander.



CI-Beziehungen

Diese Beziehungen sollen die Cisco WAP-Erkennung unterstützen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_ip_switch	Controller für::Gesteuert von	cmdb_ci_wap_network

Erkennung von Citrix NetScaler SDX

Die Anwendung ServiceNow Discovery kann Citrix NetScaler SDX-Geräte mithilfe des Musters „Citrix NetScaler SDX“ erkennen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Sie können dieses Muster auf der Now Platform® mit dem Release Quebec oder höher verwenden.

Der in Quebec eingeführte neue Klassifizierungsmechanismus löst das Muster aus. Der Klassifizierungsmechanismus verhindert, dass die gesamte Probe ausfällt, wenn eine untergeordnete Probe in einer Mehrfachprobe ausfällt.

Der Klassifizierungsmechanismus enthält eine neue Tabelle „trigger_probe_m2m“, die definiert, welche Klassifizierungs-Probe in Bezug auf das relevante Protokoll ausgelöst werden soll. Für dieses Muster wird die interaktive Probe Shell über das Protokoll *ssh* ausgelöst.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass die Store-Apps CMDB CI Class Models (Version 1.0.20) und Discovery and Service Mapping Patterns (Version 1.0.72) installiert sind.
- Stellen Sie sicher, dass SSH-Anmeldeinformationen für das Citrix NetScaler SDX-Gerät festgelegt sind.
- Stellen Sie sicher, dass der in der Now Platform-Instanz hinzugefügte Discovery-Benutzer die folgenden Befehle ausführen kann:

Befehl	Beschreibung
vmdevice anzeigen	Ruft VM-Instanzen (virtueller Computer) ab.
sysctl -a	Bietet einen schnellen Überblick über alle konfigurierbaren Einstellungen für Citrix NetScaler SDX-Geräte

Von Discovery während der horizontalen Erkennung erfasste Daten

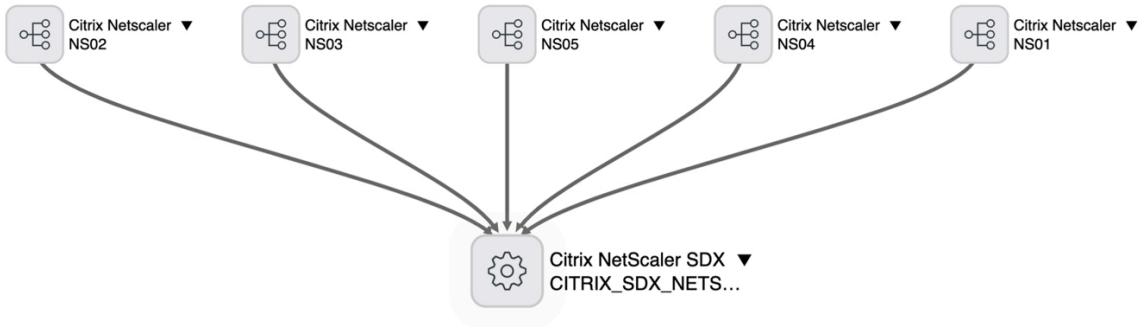
Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Hauptkonfigurationselement [cmdb_ci_citrix_netscaler_sdx]	
name	Name des Citrix NetScaler SDX-Geräts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
serial_number	Seriennummer des Citrix NetScaler SDX-Geräts
ip_address	IP-Adresse des Citrix NetScaler SDX-Geräts
object_id	CI-Bezeichner des Citrix NetScaler SDX-Geräts, der die Seriennummer und die IP-Adresse enthält
short_description	Beschreibung des Citrix NetScaler SDX-Geräts
os_version	Version des Citrix NetScaler SDX-Geräts
[cmdb_ci_lb_netscaler]	
name	Name des Citrix NetScaler-Lastenausgleichsmoduls
serial_number	Seriennummer des Citrix NetScaler-Lastenausgleichsmoduls
ip_address	IP-Adresse des Citrix NetScaler-Lastenausgleichsmoduls

Die Dependency Views-Zuordnung zeigt alle erkannten Citrix NetScaler SDX-Ressourcen in Ihrer Organisation und die Beziehungen zwischen ihnen an.



CI-Beziehungen

Die folgenden Beziehungen werden zur Unterstützung der Erkennung von Citrix NetScaler SDX erstellt:

CI	Beziehung	CI
cmdb_ci_lb_netscaler	Registriert auf::Hat sich registriert	cmdb_ci_citrix_netscaler_sdx

Citrix Xen Hyper-V-Erkennung

ServiceNow Discovery verwendet das Citrix Xen Hyper-V-Muster, um Instanzen zu suchen und zuzuordnen. Erkennen Sie diese Ressourcen, indem Sie die Musteranwendungen aus dem ServiceNow Store installieren und Citrix Xen Hyper-V zum Erweiterungsabschnitt des Linux-Server-Musters hinzufügen.

Verwenden Sie die Befehle Xen (XE) und (XL), um Citrix Xen Hyper-V, seine Komponenten und entsprechenden Attribute zu erkennen. Suchen Sie Informationen zu Hyper-V-Server, zugeordneten Pools, VMs, Netzwerk und Speicher und deren Beziehungen zu neuen und vorhandenen CIs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Stellen Sie sicher, dass die folgenden Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Überprüfen Sie die RBAC-Rolle des Pooladministrators

Diese Rolle ist für den SSH-Zugriff auf den Linux-Server, der den Hypervisor hostet, und für die Ausführung aller erforderlichen Befehle zum Extrahieren von Informationen aus der Hypervisor-Umgebung erforderlich. Weitere Informationen zu RBAC-Rollenberechtigungen oder zum Hinzufügen von Citrix-Benutzern zu einer Domäne und zum Zuweisen von Rollen finden Sie in der Citrix-Dokumentation .

Überprüfen Sie die Erreichbarkeit von MID-Server .

Stellen Sie sicher, dass MID-Server für das Zielgerät erreichbar ist.

Erstellen Sie SSH-Anmeldeinformationen mit Zugriff auf den Zielhost Linux .

Weitere Informationen finden Sie unter SSH-Anmeldeinformationen

Erstellen Sie einen Erweiterungsabschnitt nach dem Linux Server-Muster

Erstellen Sie einen Erweiterungsabschnitt nach dem Linux-Server-Muster, und ordnen Sie das **Citrix Xen HyperV** -Muster zu, das nach der Ausführung des Linux-Server-Discovery-Musters ausgelöst werden soll. Weitere Informationen zum Erstellen von Erweiterungsabschnitten finden Sie unter Muster verbessern, ohne ihre Identifizierungsabschnitte zu ändern.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB bei Ausführung des Citrix Xen HyperV-Musters aus.

Hyper-V-Ressourcenpool [cmdb_ci_hyper_v_resource_pool]

Feld	Beschreibung
object_id	UUID des Hyper-V-Ressourcenpools
name	Name des Hyper-V-Ressourcenpools
default_sr	Im Standardspeicher-Repository werden die VDIs standardmäßig gespeichert

Hyper-V-Server [cmdb_ci_hyper_v_server]

Feld	Beschreibung
object_id	UUID des Hyper-V-Servers

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hyper-V-Server [cmdb_ci_hyper_v_server] (Fortsetzung)

Feld	Beschreibung
name	Name des Hyper-V-Servers im Format NAME@Hyper-V-Server
serial_number	Seriennummer des Linux-Servers, auf dem der Citrix Xen Hyper-V-Server ausgeführt wird, im Format SERIEN-NUMBER_Hyper_v_Server zur Unterscheidung vom Linux-Server
manufacturer	Lieferant des Hyper-V-Servers
model_id	Modell-ID des Hyper-V-Servers
short_description	Beschreibung des Hyper-V-Servers
os	Betriebssystem des Hyper-V-Servers
os_version	Version des Betriebssystems des Hyper-V-Servers
host_name	Hostname des Hyper-V-Servers
ip_address	IP-Adresse des Hyper-V-Servers
virtual	Legen Sie den Wert auf „falsch“ fest, da dieser Wert von Rechnern verwendet wird, um die Kennzeichnung „IsVirtual“ im Dashboard (SAM) auszufüllen.
free_memory	Verfügbarer Arbeitsspeicher des Hyper-V-Servers
total_memory	Gesamtarbeitsspeicher des Hyper-V-Servers
Edition	Edition des Hyper-V-Servers
cpu_core_count	Die Anzahl der Kerne pro physische CPU
cpu_count	Anzahl der Gesamt-CPUs
ram	Gesamter RAM-Arbeitsspeicher in MB
cpu_speed	CPU-Geschwindigkeit in MHz
cpu_manufacturer	Hersteller der CPU
cpu_type	Typ der CPU
cpu_core_thread	Die Anzahl der Threads pro CPU-Kern

Hyper-V-VM-Instanz [cmdb_ci_hyper_v_instance]

Feld	Beschreibung
object_id	UUID des Hyper-V-Servers
name	Name des Hyper-V-Servers
state	Status der Hyper-V-Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hyper-V-VM-Instanz [cmdb_ci_hyper_v_instance] (Fortsetzung)

Feld	Beschreibung
ip_address	IP-Adresse der Hyper-V-Instanz
host_id	Die UUID des Hosts, auf dem sich die Instanz befindet
baseboard_serial	UUID der Hyper-V-Instanz
chassis_serial	UUID der Hyper-V-Instanz
bios_serial	UUID der Hyper-V-Instanz

Virtuelles Hyper-V-Netzwerk [cmdb_ci_hyper_v_network]

Feld	Beschreibung
object_id	UUID des virtuellen Hyper-V-Netzwerks
pif_uuid	UUID der physischen NIC
name	Name des virtuellen Hyper-V-Netzwerks
Bridge	Typ des Netzwerk-Setups: entweder überbrückt oder nicht

Komponente des virtuelles Hyper-V-Netzwerks [cmdb_ci_hyper_v_network_comp]

Feld	Beschreibung
object_id	UUID der Hyper-V-Netzwerkkomponente
mac_address	MAC-Adresse der Hyper-V-Netzwerkkomponente
VM	UUID der Hyper-V-Instanz, der die Netzwerkkomponente zugeordnet ist
name	Name der Hyper-V-Netzwerkkomponente

Hyper-V-Speicher [cmdb_ci_hyper_v_storage]

Feld	Beschreibung
object_id	LUN des Hyper-V-Speichers
name	Name des Hyper-V-Speichers
description	Beschreibung des Hyper-V-Speichers
Typ	Typ des Speichers (SR)
vm_object_id	UUID der Hyper-V-Instanz, der der Speicher zugeordnet ist
vm_id	UUID der Hyper-V-Instanz, der der Speicher zugeordnet ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hyper-V-Speicherkomponente [cmdb_ci_hyper_v_storage_comp]

Feld	Beschreibung
object_id	UUID des virtuellen Datenträgerbilds (VDI)
name	Name des virtuellen Datenträgerbilds (VDI)
description	Beschreibung des virtuellen Datenträgerbilds (VDI)
Typ	Typ der Speicherkomponente (VDI)
Kapazität	Gesamtkapazität des virtuellen Datenträgerbilds (VDI)
location_id	Speicherort des virtuellen Datenträgerbilds (VDI)
is_a_snapshot	Angabe, ob das virtuelle Datenträgerbild (VDI) ein Snapshot ist oder nicht
Snapshot_of	Angabe des VDI-Snapshots der Datenträger
Snapshot_Zeit	Zeitpunkt der Snapshot-Erstellung
sr_object_id	UUID des Speicher-Repositorys, dem das virtuelle Datenträger-Image (VDI) zugeordnet ist
vm_object_id	UUID der VM, die dem virtuellen Datenträgerbild zugeordnet ist

CI-Beziehungen

Von Citrix Xen Hyper-V-Erkennung erstellte Beziehungen

Übergeordnet	Beziehung	Untergeordnetes Element
cmdb_ci_hyper_v_resource_pool	Enthält :: Enthalten in	cmdb_ci_hyper_v_server
cmdb_ci_hyper_v_server	Wird ausgeführt auf :: Wird ausgeführt	cmdb_ci_linux_server
cmdb_ci_hyper_v_network	Stellt :: Bereitgestellt von bereit	cmdb_ci_hyper_v_server
CMDB_CI_Hyper_v_network_comp	Stellt :: Bereitgestellt von bereit	cmdb_ci_hyper_v_server
cmdb_ci_hyper_v_instance	Verbunden durch :: Verbindet	CMDB_CI_Hyper_v_network_comp
cmdb_ci_hyper_v_resource_pool	Referenz	cmdb_ci_hyper_v_storage
cmdb_ci_hyper_v_instance	Enthält :: Enthalten in	cmdb_ci_hyper_v_storage
CMDB_CI_Hyper_v_storage_comp	Verwaltet von :: Verwaltet	cmdb_ci_hyper_v_storage
CMDB_CI_Hyper_v_storage_comp	Referenz	cmdb_ci_hyper_v_instance
cmdb_ci_hyper_v_server	Ressourcen für definieren :: Erhält Ressourcen von	cmdb_ci_hyper_v_resource_pool

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übergeordnet	Beziehung	Untergeordnetes Element
cmdb_ci_hyper_v_instance	Registriert am :: Hat sich registriert	cmdb_ci_hyper_v_server

Cloudian-Speicher-Erkennung

Das Erkennungsmuster Cloudian Storage wird von ServiceNow Discovery dazu verwendet, Cloudian-Server und zugehörige Laufwerke zu finden. Um diese Ressourcen zu erkennen, müssen Sie die Patterns-Anwendung aus dem ServiceNow Store installieren.

Cloudian Storage System-Muster werden von Discovery dazu verwendet, Cloudian Storage-Systemdaten zu finden. Zur Erkennung dieser Ressourcen müssen die Anwendungen „Muster für Discovery und Service-Mapping“ und „CMDB CI-Klassenmodelle“ aus dem ServiceNow Store installiert werden, da die Anwendungen voneinander abhängig sind. Sie können die Muster zur Erkennung von Cloudian Storage-Komponenten auf der Now Platform mit dem Paris-Release oder höher verwenden.

Cloudian ist ein Unternehmen im Bereich softwaredefinierter Datenspeicher. Cloudian bietet sofort einsatzbereite, verteilte, softwaredefinierte, S3-kompatible Objektspeicherlösungen.

Cloudian Hyperstore-Software : Stellen Sie das CentOS-Betriebssystem, zugehörige Pakete und Binärdateien der Hyperstore-Software auf dem Hyperstore-Knoten bereit.

Cloudian Hyperstore-Knoten: Dies ist ein unabhängiger Hardwareserver, auf dem Cloudian Hyperstore-Software auf einem Server nach Branchenstandard oder einer VM bereitgestellt oder auf einer Cloudian Hyperstore-Appliance vorinstalliert ist.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Damit ein Gerät als Cloudian-Server erkannt wird, muss der Befehl **/bin/systemctl status cloudian-s3** gültige Antworten zurückgeben und das **Cloudian HyperStore-Speichersystem** enthalten. Wenn dies nicht der Fall ist, wird das Gerät als Linux-Server erkannt.

- Vergewissern Sie sich, dass der Client Discover-Muster verwendet.
- Legen Sie **SSH**-Anmeldeinformationen für den Cloudian Storage-Server fest.
- Stellen Sie sicher, dass der MID Server Zugriff auf das Zielgerät hat.
- Stellen Sie sicher, dass der Discovery-Benutzer über die richtigen Berechtigungen zum Ausführen von Befehlen verfügt.
- Installieren Sie die folgenden Plugins:

- ◦ Plugin „CMDB CI Class Models“ (Version 1.31.0 oder höher)
  - ◦ Plugin „Discovery and Service Mapping Patterns“ (Version 1.0.84 oder höher)
  - ◦ Discovery and Service Mapping Patterns: (sn_itom_pattern) Version 1.0.84 und abhängiges Plugin **CMDB CI Class Models** (sn_cmdb_ci_class) Version 1.31.0 (Content-Release von Oktober)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Berechtigungen

Stellen Sie sicher, dass die Cloudian Hyperstore-Software auf CentOS- oder RHEL-Servern bereitgestellt wird. Die Konfigurationen der Anmeldeinformationen sind dieselben wie für einen Linux-Server.

Konfigurieren Sie **SSH**-Anmeldeinformationen für den Cloudian Storage-Server.

Discovery ausführen

Um das Cloudian Storage-System zu erkennen, erstellen Sie einen Discovery-Zeitplan mit der IP-Adresse des Cloudian Storage-Servers als Ziel. Stellen Sie sicher, dass die von Ihnen konfigurierten **SSH**-Anmeldeinformationen auf den Cloudian-Server zugreifen können.

Von Discovery während der horizontalen Erkennung erfasste Daten

Speicherserver [cmdb_ci_storage_server]

Feld	Beschreibung
name	
serial_number	
ip_address	
manufacturer	
model_id	
short_description	
os_version	
os	
ram	
cpu_manufacturer	
CPU-Name	
cpu_core_count	
cpu_type	

Datenträger [cmdb_ci_disk]

Feld	Beschreibung
name	
device_id	
storage_type	
size_bytes	
manufacturer	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenträger [cmdb_ci_disk] (Fortsetzung)

Feld	Beschreibung
model_id	
computer [Reference cmdb_ci_storage_server]	

Dateisystem [cmdb_ci_file_system]

Feld	Beschreibung
name	
size_bytes	
free_space_bytes	
file_system	
mount_point	
computer [Reference cmdb_ci_storage_server]	
provided_by [Reference cmdb_ci_disk]	

Netzwerkadapter [cmdb_ci_network_adapter]

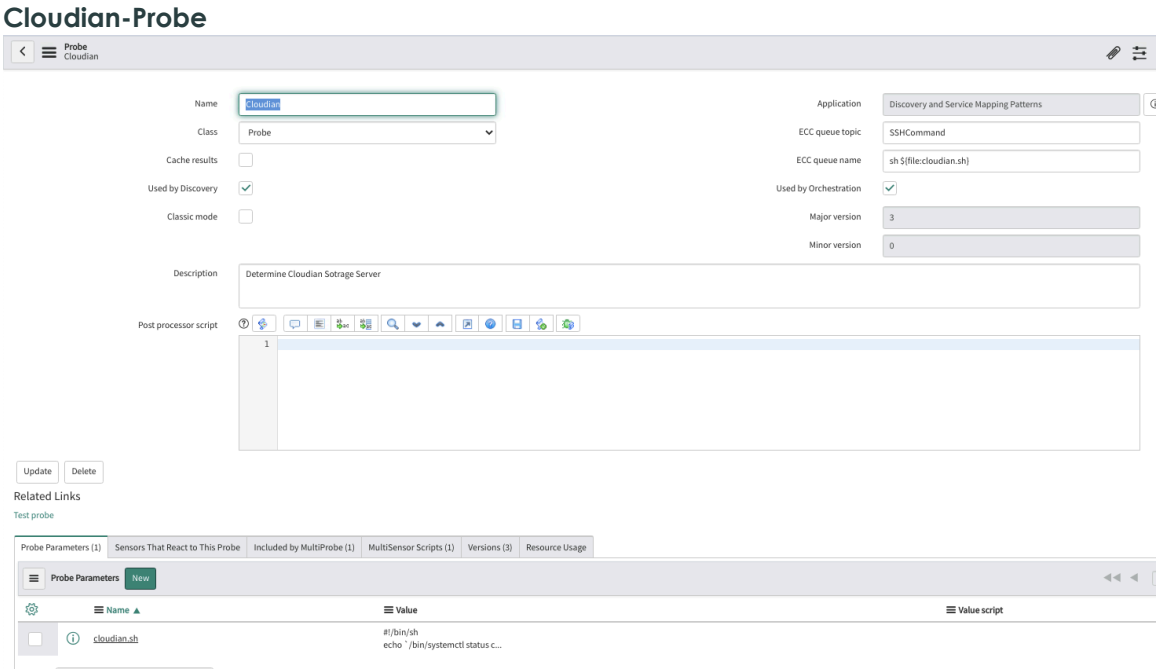
Feld	Beschreibung
name	
ip_address	
netmask	
mac_address	
cmdb_ci [Reference cmdb_ci_storage_server]	

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
ip_address	
netmask	
nic [Reference cmdb_ci_network_adapter]	

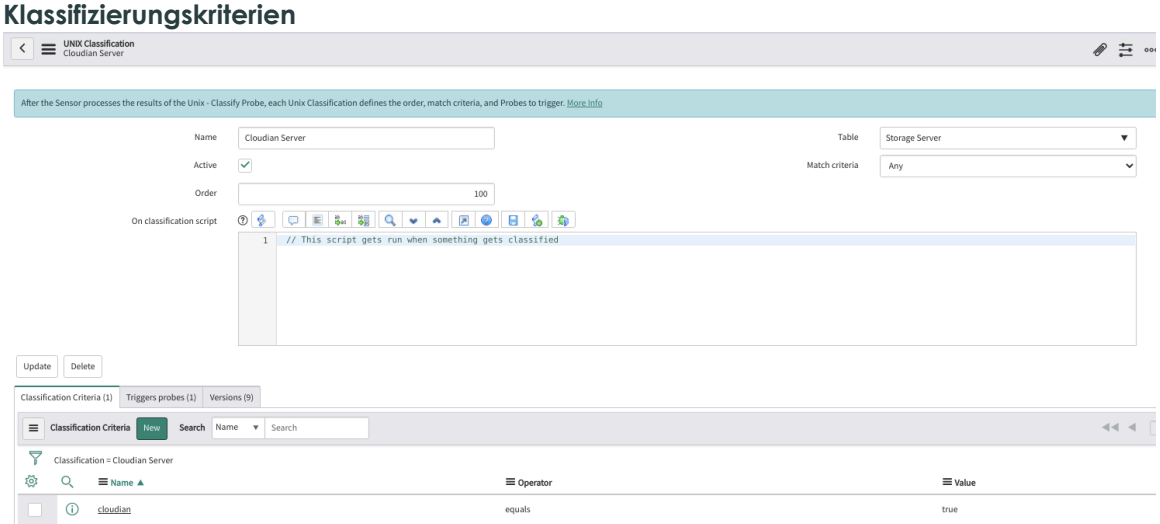
Die **Cloudian**-Probe wird in der Multi-Probe **Unix-Classify** erstellt. Die Probe **Cloudian** führt den Befehl **bin/systemctl status cloudian-s3** aus und prüft, ob die Ausgabe das **Cloudian HyperStore-Speichersystem** enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Bei der Unix-Klassifizierung wird der Klassifizierer **Cloudian-Server** vor dem **Linux-Klassifizierer** ausgeführt. Vom Cloudian-Klassifizierer werden Datensätze in der Tabelle [cmdb_ci_storage_server] erstellt. Von diesem Klassifizierer wird das Cloudian Storage System-Muster aufgerufen.

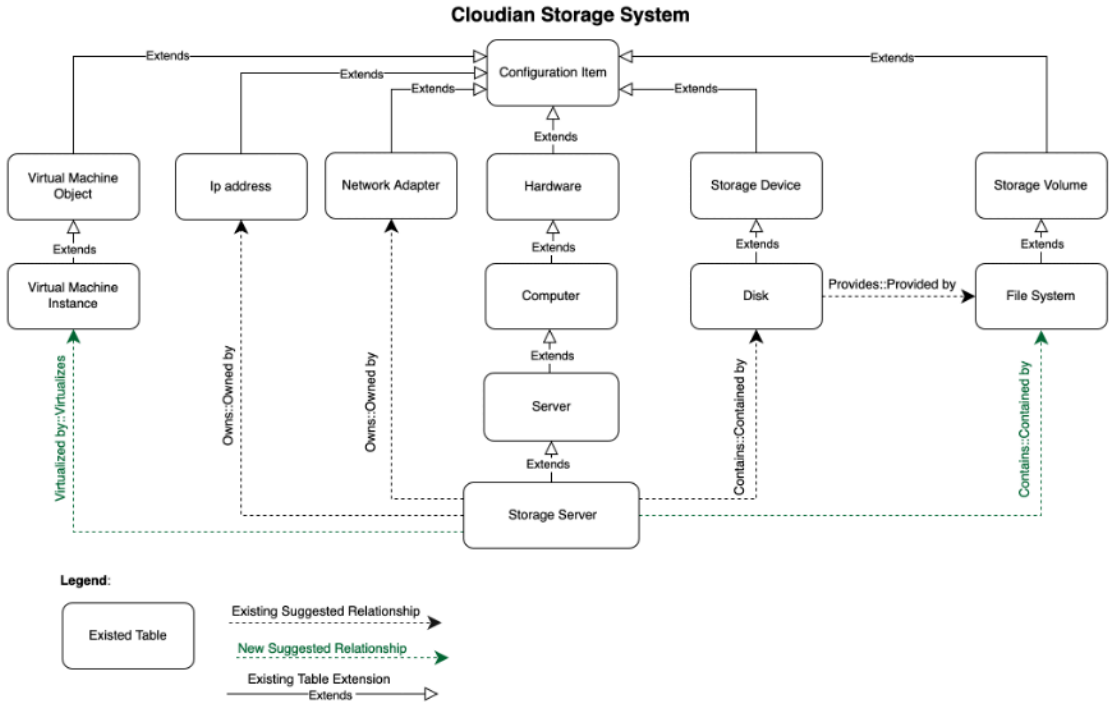
Klassifizierungskriterien



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

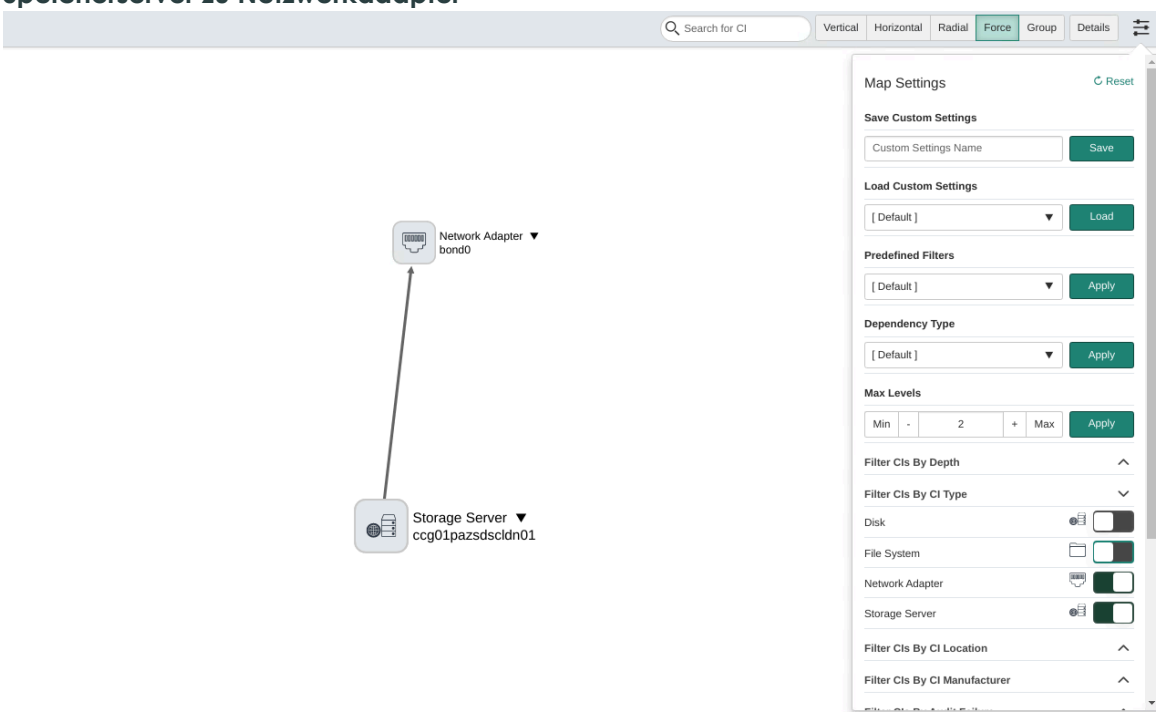
CMDB-Datenmodell

CMDB-Datenmodell



Speicherserver zu Netzwerkadapter

Speicherserver zu Netzwerkadapter

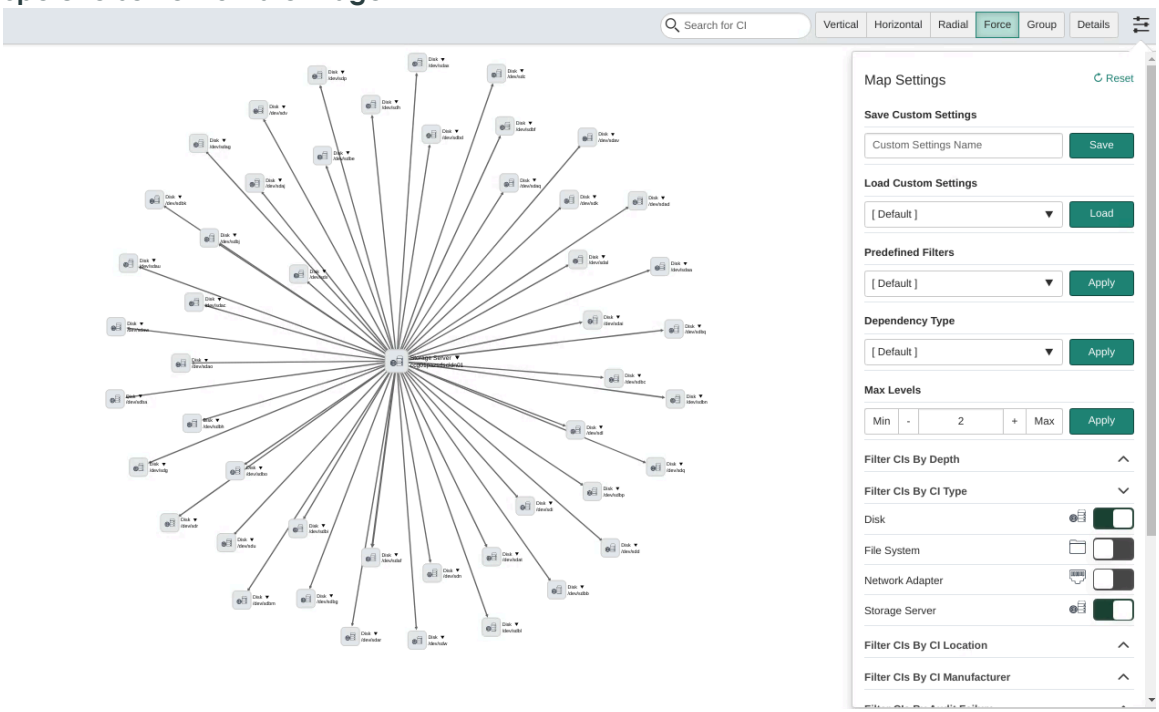


Speicherserver zu Datenträger

Automatische Übersetzung

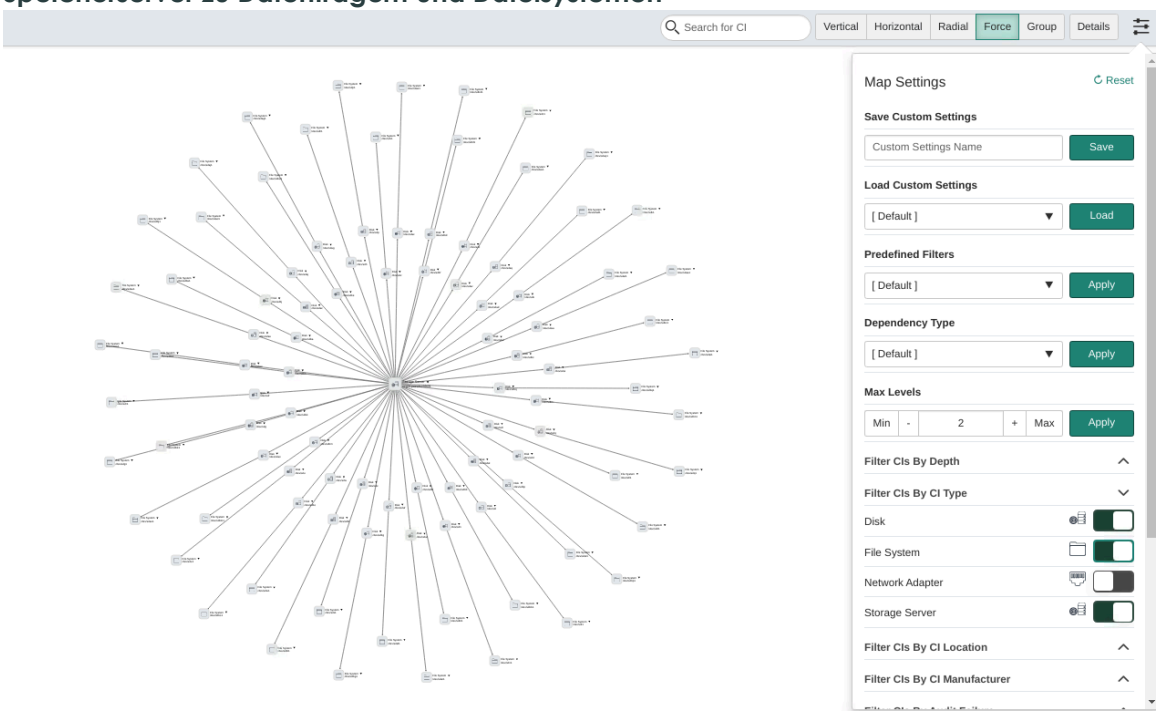
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherserver zu Datenträger



Speicherserver zu Datenträgern und Dateisystemen

Speicherserver zu Datenträgern und Dateisystemen



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Vom Cloudian Storage-Muster erstellte Beziehungen

Übergeordnet	Beziehung	Untergeordnetes Element
cmdb_ci_storage_server	Eigentümer von::Eigentum von	cmdb_ci_network_adapter
cmdb_ci_storage_server	Eigentümer von::Eigentum von	cmdb_ci_ip_address
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_disk
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_file_system
cmdb_ci_storage_server	Virtualisiert von::Virtualisiert	cmdb_ci_vm_instance
cmdb_ci_disk	Stellt bereit::Bereitgestellt von	cmdb_ci_file_system

Discovery des Cohesity-Speichersystems

Die Anwendung Muster für Discovery und Service-Mapping verwendet das Cohesity Storage System-Muster, um Cluster, Knoten und Chassis für die Cohesity DataPlatform zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Cohesity entwickelt Software, die zur Konsolidierung und Vereinfachung der Datenverwaltung verwendet wird, und enthält Analysefunktionen. Die Software von Incident löst auch das Problem der Massendatenfragmentierung bei Daten, die sich über mehrere Systeme oder Cloud-Anbieter erstrecken.

Das Hauptprodukt des Unternehmens, DataPlatform, ist eine hochkonvergente Software, mit der Unternehmen eine Vielzahl von Arbeitsauslastungen, einschließlich Backups, Archivierung, Test-, Entwicklungs- und Analysedaten, auf einer einzigen nativen Cloud-Plattform konsolidieren können. Es funktioniert sowohl mit physischen Servern als auch mit virtuellen Maschinen.

Cohesity erweitert Sicherungsfunktionen auf verteilte NoSQL-Arbeitsauslastungsdatenbanken wie MongoDB, Apache Cassandra, Couchbase und Apache HBase sowie Apache Hadoop-Daten in HDFS-Datenspeichern (Hadoop Distributed File System).

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

- CMDB CI-Klassenmodelle, ab Version 1.37.0
- Muster für Discovery und Service-Mapping, ab Version 1.0.91

Überprüfen Sie die Konfiguration MID-Server .

Stellen Sie sicher, dass MID-Server auf Aktiv festgelegt und für den Cohesity-Speichercluster erreichbar ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verifizieren Sie die API-Berechtigungen

Stellen Sie sicher, dass Sie ein Standardauthentifizierungskonto mit den richtigen Berechtigungen für die folgenden API-Aufrufe konfiguriert haben:

- `https://" + ${cluster_ip} + "/irisservices/api/v1/public/cluster?fetchStats=wahr`
- `https://" + ${cluster_ip} + "/irisservices/api/v1/nexus/cluster/status`
- `https://" + ${cluster_ip} + "/irisservices/api/v1/public/nodes?fetchStats=wahr`
- `https://" + nodeIp + "/irisservices/api/v1/nexus/node/hardware_info`

Erstellen Sie einen Alias für die Anmeldeinformationen für die Standardauthentifizierung

Weitere Informationen finden Sie unter Erstellen Sie einen Alias für die Anmeldeinformationen für die Standardauthentifizierung für die Discovery des Cohesity-Speichersystems.

Zeitplan für Erkennung ohne Server erstellen

Weitere Informationen finden Sie unter Erstellen Sie einen Zeitplan ohne Server für die Discovery des Cohesity-Speichersystems.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das Cohesity Storage System-Muster ausgeführt wird.

Cohesity-Cluster [cmdb_ci_cohesity_cluster]

Bezeichnung	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Clusters.
Vollständig qualifizierter Domänenname [fqdn]	Vollständig qualifizierter Domänenname (FQDN) des Clusters.

Cohesity-Knoten [cmdb_ci_cohesity_node]

Bezeichnung	Feldname
Hersteller [manufacturer]	Hersteller des Clusterknotens, bei dem es sich um Cohesity oder eine Drittpartei handeln kann.
Vollständig qualifizierter Domänenname [fqdn]	FQDN des Knotens innerhalb des Clusters.
Betriebsstatus [operational_status]	Betriebsstatus. Standardwert: Installiert.
Beschreibung [short_description]	Beschreibung des Cluster-Knotens: Cohesity Backup Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gehäuse [cmdb_ci_chassis]

Bezeichnung	Feldname
Hersteller [manufacturer]	Hersteller des Gehäuses.
Beschreibung [short_description]	Beschreibung des Chassis: Cohesity Chassis.
Seriennummer [serial_number]	Seriennummer des Gehäuses.

IP-Adresse [cmdb_ci_ip_address]

Bezeichnung	Feldname
Name [name]	Name des Cohesity-Knotens.
IP-Adresse [ip_address]	IP-Adresse des Cohesity-Knotens.
IP-Version [ip_version]	IP-Version des Cohesity-Knotens.

CI-Beziehungen

Discovery erstellt diese Beziehungen, um die Discovery des Cohesity-Speichersystems zu unterstützen.

CI	Beziehungstyp	CI
Cohesity-Knoten [cmdb_ci_cohesity_node]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Cohesity-Knoten [cmdb_ci_cohesity_node]	Cluster von::Cluster	Cohesity-Cluster [cmdb_ci_cohesity_cluster]
Cohesity-Knoten [cmdb_ci_cohesity_node]	Gehostet auf::Hostet	Gehäuse [cmdb_ci_chassis]

Erstellen Sie einen Alias für die Anmeldeinformationen für die Standardauthentifizierung für die Discovery des Cohesity-Speichersystems

Erstellen Sie einen Alias, und fügen Sie ihn den Anmeldeinformationen für die Standardauthentifizierung hinzu, um Cohesity-Speichersysteme zu erkennen.

Vorbereitungen

Vergewissern Sie sich, dass ein Account für die Standardauthentifizierung mit den entsprechenden Berechtigungen konfiguriert ist. Weitere Informationen finden Sie im Abschnitt Verifizieren Sie die API-Berechtigungen in Discovery des Cohesity-Speichersystems.

Erforderliche Rolle: discovery_admin

Prozedur

1. Erstellen Sie einen Alias.
   a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
   b. Wählen Sie **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Geben Sie einen eindeutigen Namen für den Alias ein, und wählen Sie im Feld **TypAnmeldeinformationen** für den Aliastyp aus.

d. Wählen Sie **Absenden**.

2. Konfigurieren Sie Anmeldeinformationen für die Standardauthentifizierung für den neuen Alias.

a. Navigieren zu **Discovery** > **Anmeldeinformationen**.

b. Wählen Sie **Neu**.

c. Klicken Sie auf **Basisanmeldedaten**.

d. Entsperren Sie das Feld **Alias für Anmeldeinformationen**, und wählen Sie den von Ihnen erstellten Alias aus.

e. Konfigurieren Sie die restlichen Felder des Formulars **„Anmeldeinformationen für Standardauthentifizierung“**.

f. Wählen Sie **Absenden**.
Weitere Informationen zu den Feldern des Formulars „Anmeldeinformationen für Standardauthentifizierung“ finden Sie unter Virtual Server Interface .

Nächste Maßnahme

Erstellen Sie einen Zeitplan für eine Erkennung ohne Server. Weitere Informationen finden Sie unter Erstellen Sie einen Zeitplan ohne Server für die Discovery des Cohesity-Speichersystems.

Zugehörige Informationen

Discovery des Cohesity-Speichersystems

Erstellen Sie einen Zeitplan ohne Server für die Discovery des Cohesity-Speichersystems

Erstellen Sie einen serverlosen Discovery-Zeitplan, um Cohesity-Speichersysteme zu erkennen.

Vorbereitungen

- Stellen Sie sicher, dass MID-Server auf Aktiv festgelegt und für den Cohesity-Speicher-Cluster erreichbar ist.
- Erstellen Sie einen Alias für die Anmeldeinformationen für die Standardauthentifizierung. Weitere Informationen finden Sie unter Erstellen Sie einen Alias für die Anmeldeinformationen für die Standardauthentifizierung für die Discovery des Cohesity-Speichersystems.

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Zeitpläne**.
2. Wählen Sie **Neu**.
3. Konfigurieren Sie das Formular „Discovery-Zeitplan“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Neuer Datensatz des Discovery-Zeitplans“.

Feld	Beschreibung
Name	Eindeutiger Name für diesen Discovery-Zeitplan.
Discovery	Scantyp, der „Serverlos“ sein muss.
MID-Server	Name von MID-Server, der für diesen Zeitplan verwendet werden soll.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

4. Wählen Sie **Absenden**.
5. Wählen Sie auf der Seite „Discovery-Zeitpläne“ den von Ihnen erstellten Datensatz aus.
6. Wählen Sie auf der Registerkarte **Ausführungsmuster ohne ServerNeu**.
7. Füllen Sie die Felder des Formulars aus.

Formular „Neuer Datensatz“ für serverlose Ausführungsmuster

Feld	Beschreibung
Name	Beschreibender Name für diesen Datensatz.
Muster	Muster, das für diesen Zeitplan verwendet werden soll; muss das Cohesity Storage System-Muster sein.
Proxyhost	Vollqualifizierter Domänenname des Computers, auf dem ggf. ein Proxy-Server installiert ist. Dieses Feld muss leer bleiben.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

8. Wählen Sie **Absenden**.
9. Wählen Sie auf der Registerkarte **Startprogrammparameter für Discovery-Muster** den von Ihnen erstellten Datensatz aus.
10. Konfigurieren Sie die folgenden Parameter mit den relevanten Werten.

Parameter	Wert
cluster_ip	Die URL oder IP-Adresse des Cohesity-Clusters.
Anmeldeinformationsalias	Name des von Ihnen erstellten Anmeldeinformationsalias.

11. Wählen Sie **Absenden**.

Nächste Maßnahme

Führen Sie Discovery entweder sofort aus, indem **Sie Jetzt erkennen** auswählen, oder warten Sie, bis der vordefinierte Zeitplan die Discovery auslöst.

Zugehörige Informationen

Discovery des Cohesity-Speichersystems

ColdFusion-Erkennung

Die ServiceNow Discovery-Anwendung findet Adobe ColdFusion-Server und die Instanzen der auf ihnen ausgeführten ColdFusion-Anwendungen. Nur die ColdFusion-Version 2016 wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

unterstützt. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Komponenten

Discovery und Service-Mapping verwenden die Muster *`ColdFusion Application`* und *`ColdFusion Application Server`*, um eine horizontale Erkennung und eine Erkennung von oben nach unten auszuführen. Das Muster *`ColdFusion Application Server`* wird vom Prozessklassifizierer ColdFusion Application Server für die horizontale Erkennung ausgelöst.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Berechtigungen

Konfigurieren Sie die folgenden Anmeldeinformationen, je nachdem, auf welchem Typ von Hostcomputer der ColdFusion-Server installiert ist:

- Windows-Anmeldeinformationen
- SSH-Anmeldeinformationen (für Linux-Computer)

Dateizugriff

Das Muster muss auf diese ColdFusion-Dateien zugreifen können:

Datei	Beschreibung
`neo-runtime.xml`	Diese Datei stellt die Zuordnung zwischen der URL und dem Arbeitsverzeichnispfad der Anwendung bereit.
`application.cfc` und `application.cfm`	Diese Dateien enthalten die Anwendungsnamen.
`neo-datasource.xml`	Diese Datei enthält den Namen der Datenquelle, die in der Konfiguration der ColdFusion-Anwendung verwendet wird. Die Datenquellenreferenz ist in den Dateien `application.cfc` und `application.cfm` konfiguriert. **Hinweis:** Die Datenquelle wird nur für die Erkennung von oben nach unten verwendet.

Eingabepunkt

Für die Erkennung von oben nach unten verwenden Sie die vollständige URL oder IP-Adresse der Webanwendung als HTTP(S)-Endpunkt. Beispiel: `https://my-website-on-coldfusion/path` oder `https:10.120.255.2555:8500/path`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
ColdFusion-Server [cmdb_ci_coldfusion_server]	
Installationsverzeichnis [installation_directory]	Der Name und die Version des ColdFusion-Servers sowie das Verzeichnis, in dem er installiert ist.
Name [name]	
Version [version]	
Installationsverzeichnis [installation_directory]	Der Name der Anwendung sowie das Verzeichnis, in dem sie installiert ist.
Name [name]	

Hinweis: Cold-Fusion-Anwendungen [cmdb_ci_cf_application] sind benutzerdefinierte Anwendungen, die dieses Muster nicht erkennt.

CI-Beziehungen

CI	Beziehung	CI
cmdb_ci_cf_application	Enthält::Enthalten in	cmdb_ci_coldfusion_server
cmdb_ci_coldfusion_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_linux_server cmdb_ci_win_server cmdb_ci_osx_server

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping führt die Erkennung von Adobe ColdFusion von oben nach unten im Kontext von Anwendungsservices durch. Service-Mapping erkennt die ausgehenden Datenquellenverbindungen von ColdFusion-Servern zu Datenbankinstanzen.

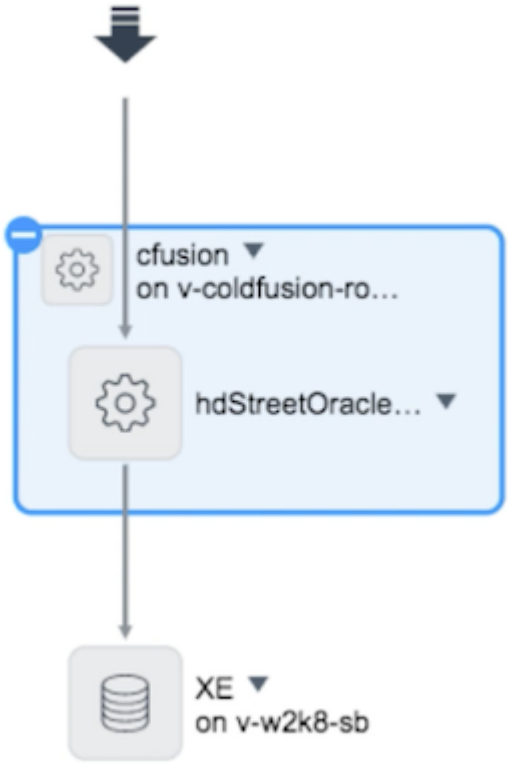
Beispiel

In diesem Beispiel zeigt die Anwendungsservicezuordnung die Ergebnisse einer Erkennung von oben nach unten des ColdFusion-Webanwendungsservices. Der Anwendungsservice besteht aus drei CIs:

- Der ColdFusion-Anwendungsserver heißt **cfusion**.
- Die ColdFusion-Anwendung **hdStreetOracle**.
- Eine Datenbank namens **XE**, mit der die ColdFusion-Anwendung eine Verbindung herstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ColdFusion-Servicezuordnung



Couchbase-Datenbankerkennung

Von der ServiceNow Discovery-Anwendung wird das Erkennungsmuster „Couchbase-Instanz“ dazu verwendet, Couchbase-Datenbankinstanzen und ihre Cluster zu finden und zuzuordnen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Die Couchbase-Datenbank ist eine verteilte Open Source-Datenbank, mit der JSON-Dokumente verwaltet werden. Mindestens eine Instanz eines Couchbase-Servers bildet einen Cluster. Daten und Services werden im gesamten Cluster gemeinsam genutzt.

Das Erkennungsmuster „Couchbase-Instanz“ wird von Discovery dazu verwendet, eine horizontale Erkennung und eine Erkennung von oben nach unten auszuführen. Sie können dieses Muster auf der Now Platform® mit Quebec-Release oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Die Couchbase-Datenbank muss auf einem Linux-Server installiert sein: Red Hat 7.9 oder Ubuntu 20.
- Stellen Sie sicher, dass auf den Servern CLI-Tools installiert sind.
- Konfigurieren Sie auf der Now Platform die SSH-Anmeldeinformationen . Konfigurieren Sie Anmeldeinformationen mit den folgenden Berechtigungen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Discovery-Berechtigungen
- Berechtigungen zum Auflisten von Dateien wie VERSION.txt in den Couchbase-Installationsordnern auf dem Linux-Server.
- Berechtigungen zum Ausführen des Befehls `systemctl status couchbase-server` auf dem Linux-Server.

Konfigurieren Sie auf der Now Platform Applicative-Anmeldeinformationen für die Tabelle cmdb_ci_couchbase_instance. Die Anmeldeinformationen müssen über ausreichende Berechtigungen verfügen, damit die folgenden Befehle auf dem Couchbase-Server ausgeführt werden können:

- `<couchbase install dir>/bin/curl -u <username>:'<password>' http://"<couchbase server>:<access_port>/pools/`
- `<couchbase install dir>/bin/curl -u <username>:'<password>' http://"<couchbase server>:<access_port>/pools/<default Pool name>`
- `<couchbase install dir>/bin/curl -u <username>:'<password>' http://"<couchbase server>:<access_port>/pools/<default Pool name>/buckets`
- `<couchbase install dir>/bin/curl -u <username>:'<password>' http://"<couchbase server>:<access_port>/pools/<default Pool name>/remoteClusters`

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Haupt-CI (Couchbase-Instanz) [cmdb_ci_couchbase_instance]	
name	Name der Couchbase-Instanz.
install_directory	Der Installationsordner oder das Verzeichnis der Couchbase-Instanz.
config_file	Die Hauptkonfigurationsdatei der Couchbase-Instanz.
Version	Version der Couchbase-Instanz.
tcp_port	Der für den Zugriff auf die Befehlszeile und die REST-API verwendete Port.
Edition	Entweder die Basic- oder Enterprise-Edition der Couchbase-Instanz.
start_date	Das Datum, seit dem die Couchbase-Instanz aktiv ist.
Couchbase Cluster [cmdb_ci_couchbase_cluster]	
name	Name des Couchbase-Clusters.
cluster_id	ID des Couchbase-Clusters.
install_status	Installationsstatus, festgelegt auf „1“/ „installiert“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
cluster_type	Betriebsstatus, festgelegt auf „1“/ „funktionsfähig“.
Couchbase-Clusterknoten [cmdb _ci_couchbase_ cluster_node]	
name	Name des Clusterknotens.
install_status	Installationsstatus, festgelegt auf „1“/ „installiert“.
operational_status	Betriebsstatus, festgelegt auf „1“/ „funktionsfähig“.
node_status	Der Integritätsstatus des Clusterknotens.
node_encryption	Feld, das angibt, ob der Knoten verschlüsselt ist.
configured_host_name	Der konfigurierte Hostname des Clusterknotens.
host_name	Tatsächlicher Hostname des Clusterknotens.
total_memory	Der gesamte Speicher.
free_memory	Der freie Speicher.
mcd_reserved_memory	Der reservierte MCD-Speicher.
mcd_allocated_memory	Der zugeteilte MCD-Speicher.
couch_api_base	Die Couchbase-Basis-API-URL.
couch_api_base_https	Die Couchbase-HTTPS-API-URL.
recovery_type	Der Wiederherstellungstyp.
otpnode	Der OTP-Knoten.
node_uuid	Die UUID des Clusterknotens.
cluster_compatibility	Die Clusterkompatibilität des Clusterknotens.
Version	Die Version des Clusterknotens.
os	Das Betriebssystem des Clusterknotens.
cpu_count	Die CPU-Anzahl des Clusterknotens.
Edition	Die Clusterknoten-Edition. Die Edition ist die gleiche wie die der Couchbase-Instanz.
Couchbase-Bucket [cmdb_ci_couchbase_bucket]	
name	Der Name des Couchbase-Buckets.
Cluster	Verweis auf das Couchbase-Cluster.
install_status	Installationsstatus, festgelegt auf „1“/ „installiert“.
Couchbase-Clusterressource [cmdb_ci_couchbase_cluster_resource]	
name	Der Name des Couchbase-Service.
install_status	Installationsstatus, festgelegt auf „1“/ „installiert“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
operational_status	Betriebsstatus, festgelegt auf „1“/ „funktionsfähig“.
Cluster	Verweis auf das Couchbase-Cluster.

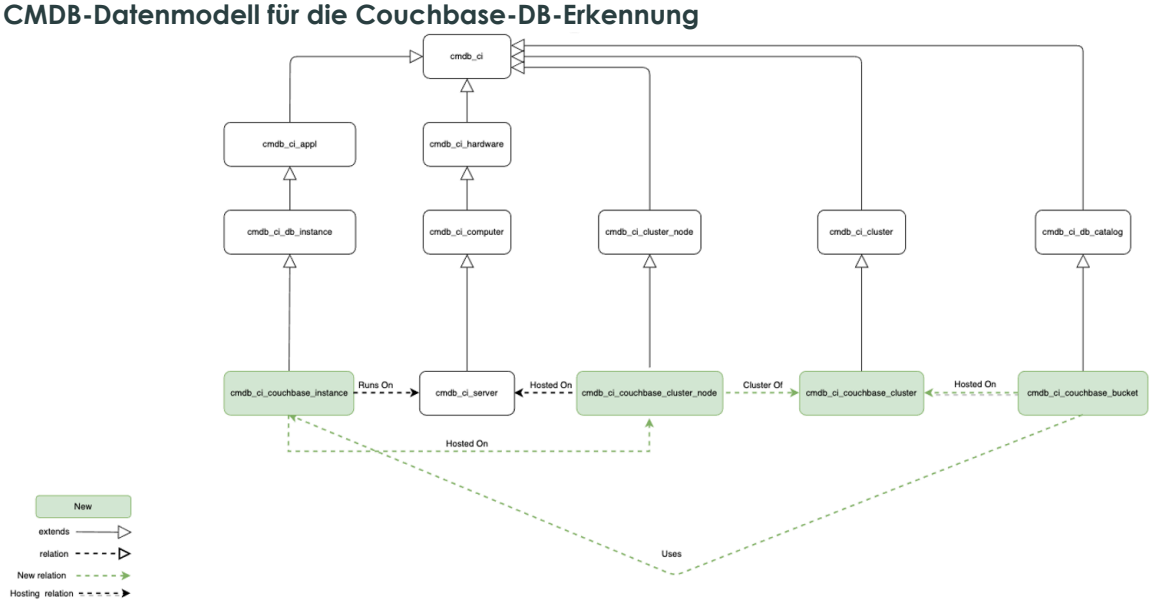
CI-Beziehungen

Diese Beziehungen sollen die Couchbase-DB-Erkennung unterstützen.

CI	Beziehung	CI
Couchbase-Instanz [cmdb_ci_couchbase_instance]	Wird ausgeführt auf::Wird ausgeführt Referenz	Linux-Server [cmdb_ci_linux_server]
Couchbase-Clusterknoten [cmdb _ci_couchbase_ cluster_node]	Cluster von::Cluster Referenz	Couchbase Cluster [cmdb_ci_couchbase_cluster]
Couchbase-Clusterknoten [cmdb _ci_couchbase_ cluster_node]	Gehostet auf::Hostet Referenz	Linux-Server [cmdb_ci_linux_server]
Couchbase-Bucket [cmdb_ci_couchbase_bucket]	Verwendet::Verwendet von Referenz	Couchbase-Instanz [cmdb_ci_couchbase_instance]
Couchbase-Bucket [cmdb_ci_couchbase_bucket]	Gehostet auf::Hostet Referenz	Couchbase Cluster [cmdb_ci_couchbase_cluster]
Couchbase Cluster [cmdb_ci_couchbase_cluster]	Repliziert zu::Repliziert von	Couchbase Cluster [cmdb_ci_couchbase_cluster]

CMDB-Datenmodell

CMDB-Datenmodell für die Couchbase-DB-Erkennung



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dell EMC XtremIO-Speicher-Array Discovery

ServiceNow Discovery verwendet das Muster Dell EMC XtremIO-Speicher-Array, um Dell EMC XtremIO-Speicher-Array -Komponenten zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Store-App Muster für Discovery und Service-Mapping

Stellen Sie sicher, dass die Store-App Muster für Discovery und Service-Mapping, Version 1.0.96, installiert ist.

Stellen Sie sicher, dass CMDB CI-Klassenmodelle, Version 1.42.0, installiert ist.

Hinweis: Die Store-Version Dell EMC XtremIO-Speicher-Array Muster 1.0.96 wurde nur für den Clustertyp XtremIO X2 getestet.

Anmeldeinformationen

Erteilen Sie Berechtigungen für Standardauthentifizierung, indem Sie Anmeldeinformationen für Standardauthentifizierung für die RESTful-API konfigurieren. Speichern Sie die Administrator-Anmeldeinformationen als Anmeldeinformationen für die Standardauthentifizierung, um einen ordnungsgemäßen Zugriff zu gewährleisten.

Ausführen Discovery

Führen Sie eine Schnell-Discovery nach Ziel-IP aus. Geben Sie die IP des XMS an (das den Speicher verwaltet).

Berechtigungen für REST API-Abfragen

Während der Erkennung verwendet das Muster folgende API-Abfragen. Der Anwender, der den Anmeldeinformationen in der Instanz hinzugefügt wird, muss berechtigt sein, diese Abfragen auszuführen.

- Details von XMS nach index_id https:// abrufen<IP> /api/json/v2/types/xms/<index_id>
- Details des Speicherservers (Cluster) nach index_id https:// abrufen<IP> /api/json/v2/types/clusters/<index_id>
- Details des Speicherknotenelements (Steine) nach index_id https:// abrufen<IP> /api/json/v2/types/bries/<index_id>
- Details zu Speicherdatenträgern (SSDs) nach index_id https:// abrufen<IP> /api/json/v2/types/ssds/<index_id>
- Details des Speichergehäuses (DAEs) nach index_id https:// abrufen<IP> /api/json/v2/types/daes/<index_id>
- Details zu Speicher-Switches (Infiniband-Switches) nach index_id https:// abrufen<IP> /api/json/v2/types/infiniband-Switches/<index_id>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Details zu Batterie-Backup-Einheiten (BBUs) nach index_id https:// abrufen<IP> /api/json/v2/types/bbus/<index_id>
- Details zu Speichercontrollern nach index_id https:// abrufen<IP> /api/json/v2/types/storage-controllers/<index_id>
- Details zu Speicherports (Ziele) nach index_id https:// abrufen<IP> /api/json/v2/types/targets/<index_id>
- Details von Datenträgern (lokale Datenträger) nach index_id https:// abrufen<IP> /api/json/v2/types/local-disks/<index_id>
- Details der Initiatorgruppen nach index_id https:// abrufen<IP> /api/json/v2/types/initiator-groups/<index_id>
- Details der Fibre Channel-Ports (Initiatoren) nach index_id https:// abrufen<IP> /api/json/v2/types/initiators/<index_id>
- Details von Fibre Channel-Datenträgern (Volumes) nach index_id https:// abrufen<IP> /api/json/v2/types/volumes/<index_id>

Das neue Configuration Item (CI), das wie folgt klassifiziert ist:

Initiatorgruppe

Von Discovery während der horizontalen Erkennung erfasste Daten

Das erkannte Element Dell EMC XtremIO-Speicher-Array Configuration Management Database (CMDB) enthält die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Haupt-CI [cmdb_ci_linux_server]	
name	Der Name des Linux-/XMS-Servers
ip_address	Die IP-Adresse des Linux-/XMS-Servers
host_name	Der Hostname des Linux-/XMS-Servers
object_id	Das Bezeichnerattribut des Linux/XMS-Servers
ram	Der insgesamt verfügbare RAM des Linux-/XMS-Servers
Speicherserver [cmdb_ci_storage_server]	
name	Der Name des Speicherservers (Cluster)
object_id	Die IP-Adresse des Speicherservers (Cluster)
serial_number	Die Seriennummer des Speicherservers (Cluster)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Speicherknotenelement [cmdb_ci_storage_node_element]	
name	Der Name des Speicherknotenelements (X-Bric)
object_id	Das Bezeichnerattribut des Speicherknotenelements (X-Bric)
serial_number	Die Seriennummer des Speicherknotenelements (X-Bric).
Speichercontroller [cmdb_ci_storage_controller]	
name	Der Name des Speichercontrollers
device_id	Die ID des Speichercontrollers
serial_number	Die Seriennummer des Speichercontrollers
model_number	Die Modellnummer des Speichercontrollers
model_id	Die Modell-ID des Speichercontrollers
Speicheranschluss [cmdb_ci_storage_port]	
wwpn	Der WWPN
name	Der Name des Speicherports (Ziel)
correlation_id	Die Korrelations-ID des Speicherports (Ziel).
speed	Die Geschwindigkeit des Speicherports (Ziel)
port_type	Der Speicherporttyp (Ziel).
Speicher-Switch [cmdb_ci_storage_switch]	
object_id	Das Bezeichnerattribut des Speicher-Switches (Infiniband-Switch)
name	Der Name des Speicher-Switches (Infiniband-Switch)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
serial_number	Die Seriennummer des Speicher-Switches (Infiniband-Switches)
model_id	Die Modell-ID des Speicher-Switches (Infiniband-Switch)
Speichergehäuse [cmdb_ci_storage_enclosure]	
name	Der Name des Speichergehäuses (Disk-Array-Gehäuse)
object_id	Das Bezeichnerattribut des Speichergehäuses (Disk-Array-Gehäuse)
serial_number	Die Seriennummer des Speichergehäuses (Disk-Array-Gehäuse)
model_number	Die Modellnummer des Speichergehäuses (Disk-Array-Gehäuse)
UPS [cmdb_ci_ups]	
name	Der Name des Batterie-Backup-Geräts (BBU)
serial_number	Die Seriennummer des Batterie-Backup-Geräts (BBU)
model_number	Die Modellnummer des Batterie-Backup-Geräts (BBU)
model_id	Die Modell-ID des Batterie-Backup-Geräts (BBU)
Schätzung_Gebühr_verbleibend	Die geschätzte verbleibende Ladung für das Batterie-Backup-Gerät (BBU)
battery_voltage	Die Batteriespannung des Batterie-Backup-Geräts (BBU)
Initiatorgruppe [cmdb_ci_initiator_group]	
object_id	Das Bezeichnerattribut der Initiatorgruppe
name	Der Name der Initiatorgruppe
number_of_initiators	Die Anzahl der Initiatoren in der Gruppe
number_of_volumes	Die Anzahl der Volumes
Fibre Channel-Datenträger [cmdb_ci_fc_disk]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
name	Der Name des Fibre Channel-Datenträgers (Volume)
device_id	Die ID des Fibre Channel-Datenträgers (Volume)
size	Die verfügbare Speichergröße des Fibre Channel-Datenträgers (Volume)
Fibre Channel-Port [cmdb_ci_fc_port]	
wwpn	Der WWPN
wwnn	WWNN.
name	Der Name des Fibre Channel-Ports (Initiator)
port_type	Der Porttyp des Fibre Channel-Ports (Initiator)

CI-Beziehungen

CI	Beziehungstyp	CI
cmdb_ci_linux_server	Verwalten::Verwaltet von	cmdb_ci_storage_server
cmdb_ci_storage_switch	Verbindet mit::Verbunden mit	cmdb_ci_storage_server
cmdb_ci_storage_server	Zugeordnet zu::Zugeordnet von	cmdb_ci_storage_node_element
cmdb_ci_storage_enclosure	Enthält::Enthalten in	cmdb_ci_storage_node_element
cmdb_ci_disk	Enthält::Enthalten in	cmdb_ci_storage_node_element
cmdb_ci_storage_controller	Enthält::Enthalten in	cmdb_ci_storage_node_element
cmdb_ci_storage_controller	Enthält::Enthalten in	cmdb_ci_storage_port
cmdb_ci_ups	Verbindet mit::Verbunden mit	cmdb_ci_storage_node_element
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_Initiator_group

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehungstyp	CI
cmdb_ci_Initiator_group	Mitglied::Mitglied von	cmdb_ci_fc_port
cmdb_ci_Initiator_group	Verbindet mit::Verbunden mit	cmdb_ci_fc_disk

Zugehörige Informationen

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Dell EMC Istilon-Discovery

Die Anwendung ServiceNow Discovery verwendet das Muster Istilon Dell EMC, um nach Komponenten von Istilon Dell EMC zu suchen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Eine vollständige Liste der Geräte und Anwendungen, die von ITOM Visibility erkannt werden können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

SNMP-Community

Erstellen Sie SNMP-Community-Anmeldeinformationen für den Istilon-Cluster. Der Erkennungsprozess beginnt mit der Verwendung von SNMP-basierten Abfragen zur Klassifizierung einer Anwendung als Isilon-Cluster. Weitere Informationen finden Sie unter Anmeldeinformationen für die SNMP-Community in SNMP-Anmeldeinformationen .

Dell EMC isilon-Benutzer

Sobald die Anwendung als Isilon-Cluster klassifiziert ist, verwendet der Erkennungsprozess REST-Abfragen, um Informationen darüber zu finden. Stellen Sie dem Isar-Benutzer Dell EMC die folgenden REST-Fähigkeiten zur Verfügung:

- "https://" + $host + ":8080/platform/3/cluster/config"
- "https://" + $host + ":8080/platform/3/network/interfaces"
- "https://" + $host_ip + ":8080/platform/3/cluster/nodes/"
- "https://" + $host + ":8080/platform/3/zones"
- "https://" + $host + ":8080/platform/3/network/pools"
- "https://" + $host + ":8080/platform/3/storagepool/nodepools"
- "https://" + $host + ":8080/platform/3/storagepool/storagepools"
- "https://" + $host + ":8080/platform/3/protocols/nfs/exports"
- "https://" + $host + ":8080/platform/3/protocols/smb/shares"

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzlich zu diesen Fähigkeiten muss dieser Isar-Benutzer Dell EMC über die folgenden Berechtigungen verfügen:

- ISI_PRIV_LOGIN_PAPI
- ISI_PRIV_AUTH
- ISI_PRIV_DEVICES
- ISI_PRIV_NETWORK
- ISI_PRIV_NFS
- ISI_PRIV_SMARTPOOLS
- ISI_PRIV_SMB

Standardauthentifizierung

Erstellen Sie im Modul „Anmeldeinformationen“ der Plattform ServiceNow Anmeldeinformationen für die Standardauthentifizierung für denselben Istilon-Benutzer Dell EMC. Weitere Informationen finden Sie unter Virtual Server Interface .

ServiceNow-Plattform aktualisieren

Aktualisieren Sie die ServiceNow-Plattform auf den entsprechenden Patch: Jakarta Patch 10, Kingston Patch 8 oder London Patch 1.

Hinweis: Die neuesten Patches enthalten Metadatenregeln für Isilon und seine Komponenten.

Von Discovery für Dell EMC Istilon gesammelte Daten

Discovery füllt die Daten in CMDB bei der Ausführung des EMC Istilon-Musters aus.

Tabelle und Feld	Beschreibung
Speicherserver [cmdb_ci_storage_server]	Der Server, der den Isilon-Cluster hostet
short_description	Die während der Isilon-Serverinstallation konfigurierte Beschreibung
firmware_version	Die Version der auf dem Isilon-Server installierten Firmware
ip_address	Die IP-Adresse des Isilon-Servers
manufacturer	Das Unternehmen, das das Gerät hergestellt hat: EMC
model_id	Vorkonfigurierte Identifizierungszeichenfolge des Geräts
host_name	Der Hostname des Isilon-Servers
Speichercluster [cmdb_ci_storage_cluster]	Der Name der IP-Adresse des Clusters, den Isilon-Server bilden
name	
ip_address	
Speicherclusterknoten [cmdb_ci_storage_cluster_node]	Der Name und andere Attribute des Knotens, der Teil des Isilon-Speicherclusters ist
name	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Cluster	
operational_status	
Speicherknotenelement [cmdb_ci_storage_node_element]	Der Name und andere Attribute des physischen Knotens, der vom Speicherclusters gehostet wird
name	
manufacturer	
cpu_type	
model_id	
Netzwerkadapter [cmdb_ci_network_adapter]	Das Attribut, das anzeigt, ob der auf dem Clusterknoten installierte Netzwerkadapter aktiv ist
active	
name	
ip_address	
netmask	
IP-Adresse [cmdb_ci_ip_address]	Die Attribute der IP-Adresse des Clusterknotens
name	
netmask	
Datenträger [cmdb_ci_disk]	Der auf dem Isilon-Server installierte Speicherdatenträger
device_id	
name	
model_id	
Schnittstelle	
disk_interface	
Speicherdateifreigabe [cmdb_ci_storage_fileshare]	Die Serverattribute für die Dateifreigabe
Pfad	
name	
fileshare_id	
correlation_id	
Speichervolume [cmdb_ci_storage_volume]	Die Attribute des Speichervolume, das zum Speichercluster gehört
media_type	
object_id	
size_bytes	
free_space_bytes	
Speicherpool [cmdb_ci_storage_pool]	
pool_id	Die Attribute des Speicher-Pools, zu dem der Speichercluster gehört

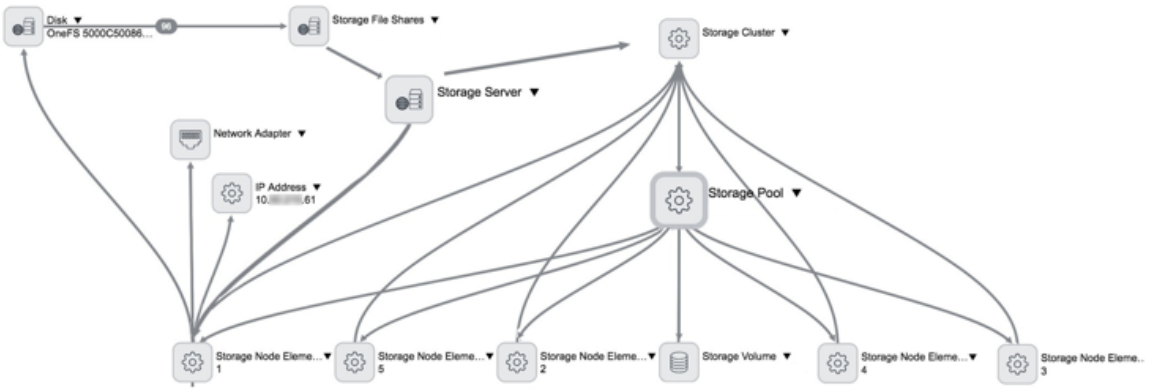
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
free_space_bytes	
size_bytes	
name	
object_id	
Seriennummer [cmdb_serial_number]	Die Attribute der Seriennummer des Speicherknotens
serial_number	
serial_number_type	
valid	

Die Grafik zeigt CIs, die Teil der Isilon-Erkennung sind.

Hinweis: Diese Abhängigkeitsansichten-Zuordnung wurde der Übersichtlichkeit halber vereinfacht. Ihre Isilon-Bereitstellungen können viele weitere CIs enthalten.

Abhängigkeitsansichten mit Isilon-Komponenten



CI-Beziehungen

CI	Beziehung/Referenz	CI
cmdb_ci_storage_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_storage_cluster
cmdb_ci_storage_server	Zugeordnet zu::Zugeordnet von	cmdb_ci_storage_node_element
cmdb_ci_storage_cluster_node	Cluster von::Cluster	cmdb_ci_storage_cluster (Referenz-*cluster*)
cmdb_ci_storage_cluster_node	Gehostet auf::Hostet	cmdb_ci_storage_node_element (Referenz-*server*)
cmdb_ci_storage_node_element	Verwaltet von::Verwaltet	cmdb_ci_storage_cluster
cmdb_ci_network_adapter	Eigentümer von::Eigentum von	cmdb_ci_storage_node_element (Referenz-*cmdb_ci*)
cmdb_ci_network_adapter	Verwendet von::Verwendet	cmdb_ci_storage_server (Referenz-*cmdb_ci*)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung/Referenz	CI
cmdb_ci_ip_address	Eigentümer von::Eigentum von	cmdb_ci_storage_node_element
cmdb_ci_ip_address	Verwendet von::Verwendet	cmdb_ci_storage_server
cmdb_ci_disk	Enthält::Enthalten in	cmdb_ci_storage_node_element (Referenz-*computer*)
cmdb_ci_storage_fileshare	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_server
cmdb_ci_storage_fileshare	Zugeordnet von::Zugeordnet zu	cmdb_ci_storage_volume
cmdb_ci_storage_volume	Verwendet::Verwendet von	cmdb_ci_storage_server
cmdb_ci_storage_volume	Eigentümer von::Eigentum von	cmdb_ci_storage_cluster
cmdb_ci_storage_pool	Eigentümer von::Eigentum von	cmdb_ci_storage_cluster (Referenz-*hosted_by*)

Dell EMC PowerMax-Speicher-Discovery mit Mustern

ServiceNow Discovery verwendet die Muster **EMC PMax Phase 1** und **EMC PMax Phase 2**, um Dell EMC PowerMax-Speicherkomponenten zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Informationen zu den PowerMax-Speicherkomponenten und ihren Versionen, die erkannt werden können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

Muster für Discovery und Service-Mapping

CMDB CI-Klassenmodelle

Überprüfen Sie die Erstellung des Alias für Anmeldeinformationen

1. Legen Sie für den Bereich Folgendes fest: **Global**.
2. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**
3. Wählen Sie **Neu**.
4. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für den Alias ein. Beispiel: `Powermax_discovery_ceredential_alias`. Notieren Sie sich den Aliasnamen, um ihn für die Konfiguration der Anmeldeinformationen für die **Standardauthentifizierung** zu verwenden.
Typ	Wählen Sie in der Liste **Anmeldeinformationen**aus.
ID	Das **ID-** Feld wird beim Senden des Formulars automatisch ausgefüllt. Notieren Sie sich die Alias-ID, um sie zum Konfigurieren der Parameter für das **EMC PMax Phase 1-** Muster zu verwenden. Beispiel: `Powermax_credential_alias_id`.

5. Wählen Sie **Absenden**.

Überprüfen Sie die Konfiguration der Anmeldeinformationen **für die Standardauthentifizierung**

Konfigurieren Sie die Anmeldeinformationen **für die Standardauthentifizierung**, um die Verbindung zur PowerMax-REST-API zu aktivieren. Das Verfahren finden Sie unter Erstellen Sie Anmeldeinformationen für die Standardauthentifizierung.

Füllen Sie das Formular aus.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für die Anmeldeinformationen ein. Beispiel: `Powermax_discovery_basic_auth_credentials`.
Anwendername	Geben Sie den Anwendernamen ein, der auf PowerMax zugreifen kann. Der Anwender muss über minimale schreibgeschützte Berechtigungen verfügen.
Passwort	Geben Sie das Passwort ein, das auf PowerMax zugreifen kann.

Überprüft die Konfiguration eines Zeitplans ohne Server Discovery .

Achten Sie darauf, `Serverlos` im Feld **Erkennen** auszuwählen. Informationen zum Verfahren finden Sie unter: Horizontale Erkennung planen

Ordnen Sie das Muster **EMC PMax Phase 1** dem Zeitplan ohne Server Discovery zu

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**
2. Wählen Sie den von Ihnen konfigurierten Zeitplan aus.
3. Wählen Sie die Registerkarte **Ausführungsmuster ohne Server**.
4. Wählen Sie **Neu**.
5. Füllen Sie die Felder im Formular wie folgt aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
IP-Adresse [emc_ip_address]	Die IP-Adresse der Navisphere, die als EMC-Verwaltungskonsole dient und mehrere Speicher verwalten kann.
Alias [credential_alias]	Die Alias-ID, die für die EMC PowerMax-Anmeldeinformationen konfiguriert ist. Beispiel: `Powermax_credential_alias_id`.

6. Wählen Sie **Absenden**.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB bei der Ausführung der **EMC PowerMAX-** Muster aus.

Speicherserver [cmdb_ci_storage_server]

Feld	Beschreibung
Name [name]	Der vom Anwender zugewiesene Bezeichner oder die Bezeichnung für ein bestimmtes Speicher-Array oder eine bestimmte Komponente im System.
Modell-ID [model_id]	Die jeweilige Variante oder das bestimmte Modell des Speicher-Arrays.
Seriennummer [serial_number]	Die Seriennummer, die jede einzelne Speicher-Array-Einheit eindeutig identifiziert.
BS [os]	Die auf dem Speicher-Array gehostete Betriebssystemumgebung. Zum Beispiel eingebettete Verwaltungssoftware oder Betriebssysteme.
BS-Version [os_version]	Die auf dem Speicher-Array installierte Softwareversion, einschließlich Core-Betriebssystem und Verwaltungssoftware.
Firmware-Version [firmware _version]	Die in den Hardwarekomponenten des Speicher-Arrays eingebettete Software, einschließlich Controllern, Laufwerken und anderen Subsystemen.
Hersteller [manufacturer]	Das Unternehmen, das für die Entwicklung, Produktion und den Support des PowerMax-Speicher-Arrays verantwortlich ist: Dell EMC.
Verwendete physische Kapazität [used_physical_capacity]	Die Menge des derzeit im PowerMax-System zugewiesenen und verwendeten Speicherplatzes. Sie gibt an, wie viele der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherserver [cmdb_ci_storage_server] (Fortsetzung)

Feld	Beschreibung
	verfügbaren physischen Speicherressourcen aktiv Daten oder andere Inhalte speichern.
Physische Kapazität [physical_capacity]	Die maximale Kapazität, die zum Speichern von Daten oder anderen Inhalten verwendet werden kann.

Speicherclusterknoten [cmdb_ci_storage_cluster_node]

Feld	Beschreibung
Name [name]	Der Name des Clusterknotens.
Cluster [cluster]	Die Hostgruppe, die diesem Clusterknoten in der PowerMax-Umgebung zugeordnet ist.
Hersteller [manufacturer]	Der Herstellername (Dell EMC) .

Speichercluster [cmdb_ci_storage_cluster]

Feld	Beschreibung
Name [name]	Der Name des Speicher-Clusters.
Korrelations-ID [correlation_id]	Kombiniert den Clusternamen und die Seriennummer des Speichers, um einen eindeutigen Bezeichner zu erstellen.

Speichercontroller [cmdb_ci_storage_controller]

Feld	Beschreibung
Name [name]	Die Kombination aus Asset und Asset-Tag.
Zugewiesen [assigned]	Der Verfügbarkeitsstatus.
Asset [asset]	Die Nummer des Direktor-Slots.
Asset-Tag [asset_tag]	Die Direktorennummer.
Geräte-ID [device_id]	Eine eindeutige Bezeichnung für den Controller.
Kurzbeschreibung [short_description]	Den Slot und die Nummer des Direktors.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichercontroller [cmdb_ci_storage_controller] (Fortsetzung)

Feld	Beschreibung
Hersteller [manufacturer]	Der Herstellername (Dell EMC) .

Speicheranschluss [cmdb_ci_storage_port]

Feld	Beschreibung
WWPN [wwpn]	Der World Wide Port Name (WWPN) des Speicherports.
Name [name]	Der Port-Bezeichner.
Bestellnummer [po_number]	Die Portnummer.
Status [state]	Der Portstatus.
Geschwindigkeit [speed]	Die Übertragungsgeschwindigkeit des Ports.
Hersteller [manufacturer]	Der Herstellername (Dell EMC) .
Kurzbeschreibung [short_description]	Eine Liste der IP-Adressen des Ports.
IP-Adresse [ip_address]	Die verbundene IP-Adresse.

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Objekt-ID [object_id]	Eindeutiger Bezeichner des World Wide Name (WWN).
Status [state]	Der aktuelle Betriebsstatus des Volumes. Beispiel: **Schreiben deaktiviert** oder **Bereit**.
Größe [size]	Die Kapazität in Gigabyte (GB).

Datenträger [cmdb_ci_disk]

Feld	Beschreibung
Name [name]	Die ID der -Spalte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenträger [cmdb_ci_disk] (Fortsetzung)

Feld	Beschreibung
Hersteller [manufacturer]	Der Datenträgerhersteller.
Modell-ID [model_id]	Das Datenträgermodell.
Größe [size]	Die Datenträgerkapazität in Gigabyte (GB).
Geräte-ID [device_id]	Die Kombination aus der Seriennummer des Speichersystems und dem Datenträgernamen, die jeden Datenträger in der PowerMax-Umgebung eindeutig identifiziert.

FC-Export [cmdb_ci_fc_export]

Feld	Beschreibung
Export-ID [export_id]	Der Fibre Channel-Bezeichner.
Initiator-WWPN [initiator_wwpn]	Ein eindeutiger Bezeichner, der die Direktor-ID, die Portnummer und die Initiator-ID kombiniert.
Bestellnummer [po_number]	Die Portnummer.
Zugewiesen an [assigned_to]	Der spezifische Host, der dem Export zugewiesen ist und die Fibre Channel-Verbindung verwaltet.
Attribute [attributes]	Die Direktor-ID, die den spezifischen Direktor identifiziert, der für die Verwaltung der Fibre Channel-Exporte verantwortlich ist.
Name [name]	Die ID des Initiators.
Hersteller [manufacturer]	Der Herstellername (Dell EMC) .
Lun [lun]	Die Anzahl der logischen Einheiten (Logical Unit Number, LUN), die in PowerMax-Systemen verbunden ist, und gibt die spezifische Speichereinheit an, die für den Fibre Channel-Export zugeordnet ist.
Asset-Tag [asset_tag]	Eine Kombination aus der Direktor-ID und der Portnummer, die das Asset innerhalb der Fibre Channel-Exporte eindeutig identifiziert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

iSCSI-Export [cmdb_ci_isci_export]

Feld	Beschreibung
Export-ID [export_id]	Der eindeutige Bezeichner für einen iSCSI-Export in PowerMax-Systemen. Er erleichtert die Verwaltung und Nachverfolgung von iSCSI-Verbindungen.
Initiator-WWPN [initiator_wwpn]	Kombination aus Direktor-ID, Portnummer und Initiator-ID, die innerhalb der iSCSI-Exporte einen eindeutigen Bezeichner für den Initiator darstellt
Name [name]	Die Initiator-ID in PowerMax-Systemen, die als eindeutiger Bezeichner für den Initiator im Kontext von iSCSI-Exporten dient.
Bestellnummer [po_number]	Die Portnummer, die den spezifischen Port identifiziert, der für den iSCSI-Export verwendet wird.
Attribute [attributes]	Die Direktor-ID, die den spezifischen Direktor identifiziert, der für die Verwaltung des iSCSI-Exports verantwortlich ist.
Zugewiesen an [assigned_to]	Der Host, der dem iSCSI-Export in der PowerMax-Umgebung zugewiesen ist und gibt das jeweilige Hostsystem an, das mit dem Export verbunden ist.

Speicherpool [cmdb_ci_storage_pool]

Feld	Beschreibung
Name [name]	Der Name des Pools.

CI-Beziehungen

Diese Beziehungen werden von Discovery erstellt, um die PowerMax-Discovery mit dem **EMC PMax Phase2-** Muster zu unterstützen.

CI	Beziehungstyp	CI
cmdb_ci_disk	Enthält::Enthalten in	cmdb_ci_storage_server
cmdb_ci_fc_export	Zugeordnet von::Zugeordnet zu	cmdb_ci_storage_volume
cmdb_ci_fc_export	Exportieren nach::Importieren von	cmdb_ci_storage_cluster_node
cmdb_ci_isci_export	Gehostet::Hosts	cmdb_ci_storage_server
cmdb_ci_isci_export	Zugeordnet von::Zugeordnet zu	cmdb_ci_storage_volume

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehungstyp	CI
cmdb_ci_isci_export	Exportieren nach::Importieren von	cmdb_ci_storage_cluster_node
cmdb_ci_storage_cluster_node	Cluster von::Cluster	cmdb_ci_storage_cluster
cmdb_ci_storage_controller	Enthält::Enthalten in	cmdb_ci_storage_server
cmdb_ci_storage_controller	Enthält::Enthalten in	cmdb_ci_storage_port
cmdb_ci_storage_port	Eigentümer von::Eigentum von	cmdb_ci_fc_export
cmdb_ci_storage_port	Eigentümer von::Eigentum von	cmdb_ci_isci_export
cmdb_ci_storage_port	Eigentümer von::Eigentum von	cmdb_ci_isci_export
cmdb_ci_storage_port	Eigentümer von::Eigentum von	cmdb_ci_fc_export
cmdb_ci_storage_server	Eigentümer von::Eigentum von	cmdb_ci_storage_port
cmdb_ci_storage_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_storage_cluster
cmdb_ci_storage_server	Zugeordnet von::Zugeordnet zu	cmdb_ci_storage_cluster_node
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_storage_pool

Dell EMC Data Domain-Speicher-Discovery mit Mustern

Discovery und Service-Mapping verwenden das Muster ohne Server **von Dell EMC Data Domain**, um die Data Domain-Speichersysteme zu finden, die im Data Domain Management Center (DDMC) registriert sind. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zu Datendomänenkomponenten und ihren Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

Muster für Discovery und Service-Mapping

CMDB CI-Klassenmodelle

Überprüfen Sie die Erstellung des Alias für Anmeldeinformationen

Rolle: DDMC-Administrator.

1. Legen Sie für den Bereich Folgendes fest: **Global**.
2. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
3. Wählen Sie **Neu**.
4. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für den Alias ein. Beispiel: `ddmc_discovery_ceredential_alias`. Notieren Sie sich den Aliasnamen, um ihn für die Konfiguration der Anmeldeinformationen für die **Standardauthentifizierung** zu verwenden.
Typ	Wählen Sie in der Liste **Anmeldeinformationen**aus.
ID	Das **ID-** Feld wird beim Senden des Formulars automatisch ausgefüllt. Notieren Sie sich die Alias-ID, um sie zum Konfigurieren der Parameter für das **Dell EMC Data Domain** -Muster zu verwenden. Beispiel: `ddmc_credential_alias_id`.

5. Wählen Sie **Absenden**.

Überprüfen Sie die Konfiguration der Anmeldeinformationen **für die Standardauthentifizierung**

Rolle: DDMC-Administrator.

Hinweis: Zum Ausführen einer Discovery mit Mustern können Sie nur jeweils eine Anmeldeinformation pro Alias erstellen.

1. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Suchen Sie in der Liste nach dem eindeutigen Aliasnamen, und öffnen Sie den Datensatz.
3. Wählen Sie in der Liste Anmeldeinformationen **für Standardauthentifizierung** aus.
4. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Namen für die Anmeldeinformationen ein. Beispiel: `ddmc_discovery_basic_auth_ceredentials`.
Anwendername	Geben Sie den Anwendernamen ein, der auf die DDMC zugreifen kann. Dieser Anwender wird in der DDMC erstellt. Der Anwender muss über minimale schreibgeschützte Berechtigungen verfügen. Alternativ können Sie die REST API-Schnittstelle für die DDMC ausfüllen.
Passwort	Geben Sie das Passwort ein, das auf die DDMC zugreifen kann. Dieses Passwort wird in der DDMC erstellt.
Aktiv	Standardmäßig aktiviert.
Anmeldeinformationsalias	Wenn Sie über den Alias auf das Formular zugegriffen haben, müssen Sie dieses Feld nicht konfigurieren.

5. Wählen Sie **Absenden**.

Überprüft die Konfiguration eines Zeitplans ohne Server Discovery .

Rolle: Discovery_admin.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie den Namen Ihrer Wahl ein.
Erkannt	Wählen Sie in der Liste `Serverlos`aus.
MID-Server	Wählen Sie die Suchschaltfläche, um die Liste der MID-Server zu öffnen, und wählen Sie den MID-Server aus, der über Netzwerkzugriff auf die DDMC verfügt.
Aktiv	Standardmäßig aktiviert.
Anmeldeinformationsalias	Dieses Feld muss nicht konfiguriert werden.

Weitere Informationen zum Festlegen der Felder **Max. Laufzeit**, **Ausführung**und **Zeit** finden Sie unter: Horizontale Erkennung planen

4. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ordnen Sie das Muster **„Dell EMC Data Domain“** dem Zeitplan ohne Server Discovery zu

Rolle: Discovery_admin.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
2. Wählen Sie den von Ihnen konfigurierten Zeitplan aus.
3. Wählen Sie die Registerkarte **Ausführungsmuster ohne Server**.
4. Wählen Sie **Neu**.
5. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Name	Geben Sie den Namen Ihrer Wahl ein. Beispiel: `dell_emc_data_domain_serverless_discovery`
Muster	Wählen Sie die Suchschaltfläche aus, um die Liste der Muster zu öffnen, und wählen Sie das Muster **Dell EMC Data Domain** aus.
Proxyhost	Dieses Feld muss nicht konfiguriert werden.
Erweiterte Parameter	Dieses Feld muss nicht konfiguriert werden.

6. Wählen Sie **Absenden**.

Konfigurieren Sie die Parameter für das **Dell EMC Data Domain** -Muster

Rolle: Discovery_admin.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
2. Wählen Sie den von Ihnen konfigurierten Zeitplan aus.
3. Wählen Sie die Registerkarte **Ausführungsmuster ohne Server**.
4. Wählen Sie den für das **Dell EMC Data Domain-** Muster erstellten Datensatz aus.
5. Legen Sie auf der Registerkarte **mit den Parametern des Discovery-Muster-Startprogramms** die Werte für die Felder wie folgt fest:

Feld	Beschreibung
Anmeldeinformationsalias	Füllen Sie die für DDMC konfigurierte Alias-ID aus. Sie finden den Alias in der Liste **„Aliasse für Verbindungen und Anmeldeinformationen“**. Beispiel: `ddmc_credential_alias_id`.
DDMC-Port	(Optional) Standardmäßig verwendet das Muster Port 3009.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
DDMC-IP-Adresse	Geben Sie den Hostnamen oder die IP-Adresse der DDMC ein. Diese Details können vom DDMC-Administrator bereitgestellt werden. Beispiel: `101.10.10.101` oder `ddmc.demo.local`.

6. Um die Erkennung auszuführen, können Sie **Jetzt erkennen** über **Zugehörige Links** auswählen oder die Ausführungszeit abwarten.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB bei Ausführung der **Dell EMC Data Domain** -Muster aus.

Speicherserver [cmdb_ci_storage_server]

Feld	Beschreibung
Name [name]	Der eindeutige Bezeichner des Speicherservers. Der Name ist normalerweise der DNS-Hostname (Domain Name System) oder der Computername, der dem Attribut **host_name** entspricht.
Hostname [host_name]	Der DNS-Hostname des Data Domain-Systems. Der Host, der zur Registrierung des Systems beim Data Domain Management Center (DDMC) verwendet wird.
FQDN [fqdn]	Der vollständig qualifizierte Domänenname des Data Domain-Systems. Der vollständige Domänenname, der zur Registrierung des Systems bei der DDMC verwendet wird.
IP-Adresse [ip_address]	Die IP-Adresse des Data Domain-Speicherservers. Der Name ist die spezifische IP-Adresse, die zur Registrierung des Data Domain-Systems bei der DDMC verwendet wird.
BS-Version [os_version]	Die Version des Betriebssystems, das auf dem Data Domain-System ausgeführt wird. Unterstützte Versionen beginnen bei DD OS 7.3.
Modell [model]	Das spezifische Modell des Data Domain-Systems (DD). Der Name für die virtuelle DD-Edition (VE) lautet beispielsweise **DELL EMC DD VE**.
Hersteller [manufacturer]	Der Hersteller ist Dell EMC.
Seriennummer [serial_number]	Die dem DD-System zugewiesene eindeutige Seriennummer.
Betriebssystem [os]	Das Datendomänen-BS ist: **DD OS**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichercluster [cmdb_ci_storage_cluster]

Feld	Beschreibung
Name [name]	Der Name der DDMC, die dem Speicher-Cluster zugeordnet ist.
Cluster-ID [cluster_id]	Universally Unique Identifier (UUID) der DDMC, die den Cluster eindeutig identifiziert.
Clusterversion [cluster_version]	Die Softwareversion der DDMC, die derzeit im Cluster installiert ist.
Seriennummer [serial_number]	Die eindeutige Seriennummer, die dem Virtual Data Domain Management Center-System (VDDMC) zugewiesen ist.
Modell-ID [model_id]	Das spezifische Modell des verwendeten Data Domain-Systems. Für die DDMC lautet die Modell-ID „DELL EMC DD Management Center“.
Hersteller [manufacturer]	Der Hersteller ist Dell EMC.

Datenträger [cmdb_ci_disk]

Feld	Beschreibung
Name [name]	Der dem Datenträgergerät im Speichersystem zugewiesene Name.
Geräte-ID [device_id]	Der eindeutige Bezeichner für das Datenträgergerät, der mit dem Gerätenamen identisch ist.
Modell-ID [model_id]	Das Modell des Datenträgergeräts. Beispiel: **VMware Virtual_disk**.
Größe [size]	Die Kapazität des Datenträgergeräts, gemessen in Gigabyte (GB).

Die Datenbank für das Gehäuse des Festplattenregals wird nur für physische DD-Systeme gefüllt, die Festplattenerweiterungsregale unterstützen.

Gehäuse für Festplattenregal [cmdb_ci_diskshelf_chassis_cluster]

Feld	Beschreibung
Name [name]	Der Name des Festplatten-Erweiterungsfachs.
Seriennummer [serial_number]	Die eindeutige Seriennummer des Festplatten-Erweiterungsfachs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seriennummer [cmdb_ci_serial_number]

Feld	Beschreibung
Seriennummer [serial_number]	Die eindeutige Seriennummer des Dell EMC Data Domain-Speichersystems, wie in DDMC registriert.
Seriennummerntyp [serial_number_type]	Das Format der Seriennummer für das Dell EMC Data Domain-Speichersystem, das angibt, ob es sich um eine System-Seriennummer oder einen Universally Unique Identifier (UUID) handelt.
Gültig [valid]	Die Gültigkeit der Daten, wobei der Wert „ **true**“ bestätigt, dass die Seriennummer erfolgreich verifiziert wurde.

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
Name [name]	Der Bezeichner oder die Bezeichnung des Netzwerkadapters, z. B. **eth1**.

Die DDMC-REST-API stellt nicht die MAC-Adresse von Netzwerkadaptern bereit. Daher bleibt das MAC-Adressfeld für Netzwerkadapter leer.

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	Die dem Gerät zugewiesene IP-Adresse.
Netzmaske [netmask]	Die der IP-Adresse zugeordnete Netzmaske, die das Subnetz definiert, zu dem die IP-Adresse gehört.

CI-Beziehungen

Muster für Discovery und Service-Mapping erstellen diese Beziehungen zur Unterstützung der Datendomänen-Discovery.

CI	Beziehungstyp	CI
cmdb_ci_storage_server	Verwaltet von::Verwaltet	cmdb_ci_storage_cluster
cmdb_ci_storage_server	Enthält::Enthalten in	cmdb_ci_disk
cmdb_ci_disk_shelf_chassis	Gehostet auf:: Hosts	cmdb_ci_storage_server
cmdb_ci_serial_number	Referenz	cmdb_ci_storage_server

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehungstyp	CI
cmdb_ci_storage_server	Eigentümer von::Eigentum von	cmdb_ci_network_adapter
cmdb_ci_storage_server	Eigentümer von::Eigentum von	cmdb_ci_ip_address

Erkennung von F5-Zertifikaten

Die Anwendung ServiceNow® Discovery verwendet **die Mustererweiterung „F5-SSH-SSL-Zertifizierung“,** um alle zugeordneten Zertifikate auf F5-Lastenausgleichsmodulen zu finden, die IPv4-Adressen und/oder IPv6-Adressen verwenden.

Die Mustererweiterung **„F5-SSH-SSL-Zertifizierung“** ist Teil der SSH-Muster für **F5-Lastenausgleichsmodul** und **F5-Lastenausgleichsmodul,** mit denen das F5-BIG-IP-Load Balancererkannt wird. Die Mustererweiterung **F5-SSH-SSL-Zertifizierung** erkennt F5-Lastenausgleichsmodul-Instanzen, die auf den Hosts über SNMP/SSH ausgeführt werden, und erkennt dann Zertifizierungen, die vom laufenden Knoten des Lastenausgleichsmoduls verwendet werden.

Hinweis: Für IPv6-Lastenausgleichsmodule wird nur SSH unterstützt.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Weitere Informationen zu Systemanforderungen und Familienkompatibilität finden Sie in der Anwendungsliste auf der Website des ServiceNow Store .

Einschränkungen der IPv6-Unterstützung

- F5-SNMP wird nicht unterstützt.
- *MID-Server* kann REST APIs mit IPv6 nicht ausführen.

  Informationen zum Ausführen einer Discovery mit F5 REST finden Sie unter KB0864769 .

Voraussetzungen

Stellen Sie sicher, dass die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Verifiziert die Konfiguration des F5-Lastenausgleichsmoduls

- Stellen Sie sicher, dass Instanzen des F5-Lastenausgleichsmoduls ausgeführt werden.
- Stellen Sie sicher, dass der Host (auf dem die F5-Instanz ausgeführt wird) mit den Anmeldeinformationen des Discovery-Benutzers erfolgreich erkennen kann.

Überprüfen Sie die Konfiguration von Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass der in der Now Platform-Instanz hinzugefügte Discovery-Benutzer die folgenden Befehle ausführen kann:

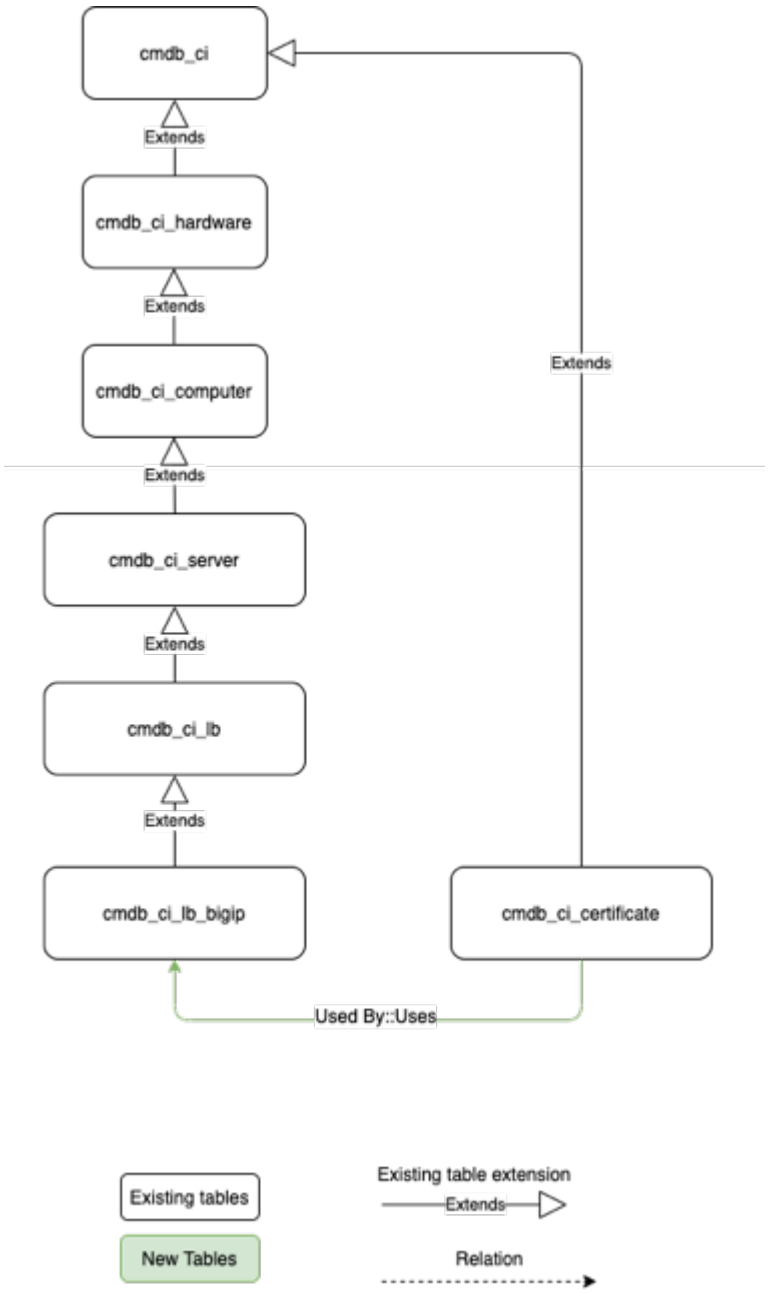
Befehl	Beschreibung
modify	Ändert die TMSH-Komponenten. Sie können eine oder mehrere Eigenschaftseinstellungen in mehreren Komponenten ändern. Der Befehl *modify* verwendet die folgende Option: *display-threshold pager*.
display_threshold	Ermöglicht Ihnen, einen *display-threshold* in Ihrem Skript erneut zu aktivieren
list	Zeigt Komponenten an, zu deren Anzeige Sie berechtigt sind oder die als Argumente übergeben werden. Der Befehl *list* sucht nach den folgenden Argumenten: • *ssl-cert* • *certificate-key-size* • *checksum* • *create-time* • *expiration-string* • *issuer* • *subject* • *Version* • *fingerprint* • *serial-number* • *subject-alternative-name* • *size*

Überprüfen Sie die Konfiguration der Muster

Stellen Sie sicher, dass die gemeinsame Bibliothek **„F5-SSH-SSL-Zertifizierung“** dem Erweiterungsabschnitt der SSH-Muster für **F5-Lastenausgleichsmodul** und **F5-Lastenausgleichsmodul** hinzugefügt wird, um die Zertifizierungsattribute zu sammeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassenmodell für die Erkennung von F5-Zertifikaten



Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Basiskonfigurationselement-Cluster [cmdb]	
Seriennummer	Seriennummer, die dem CI zugeordnet ist
Konfigurationselement [cmdb_ci]	
operational_status	Betriebsstatus des Clusterknotens
Eindeutiges Zertifikat [cmdb_ci_unique_certificate]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
fingerprint	Hashwert des Zertifikats
Fingerabdruck-Algorithmus	Algorithmus, der zum Hashen des Zertifikats verwendet wird
Allgemeiner Antragstellername	Identifiziert den dem Zertifikat zugeordneten Hostnamen/ die Domäne
Eindeutiger Antragstellername	Identifizierende Informationen des Antragstellers
Eindeutiger Ausstellername	Eindeutiger Name des Ausstellers
Anmerkungen	
Verlängerungsnachverfolgung	Gibt an, ob Aufgaben mit Priorität 1 oder Priorität 3 für ablaufende Zertifikate erstellt werden sollen
Allgemeiner Ausstellername	Allgemeiner Name des Ausstellers
gültig ab	Gültigkeitsstartzeitraum des Zertifikats
Seriennummer	Seriennummer, die dem CI zugeordnet ist
Antragstellerland	Der zweistellige Ländercode des Antragstellers.
Antragstellerorganisation	Organisation des Antragstellers
Version	X.509-Version des Zertifikats
Aussteller	Entität, die das Zertifikat signiert und ausgestellt hat
Antragsteller-Organisationseinheit	Organisationseinheit des Antragstellers
Alternativer Antragstellername	Liste vollqualifizierter Domänennamen, die durch das Zertifikat gesichert werden
gültig bis	Gültigkeitsendzeitraum des Zertifikats
name	
Status	Lebenszyklusstatus des Zertifikats
Stammaussteller	Stammentität, die das Zwischenzertifikat signiert und ausgestellt hat
Schlüsselgröße	Größe des vom Signaturalgorithmus verwendeten Schlüssels
Antragsteller-Ort	Ort des Antragstellers
Antragstellerstatus	Status des Antragstellers

CI-Beziehungen

Die Mustererweiterung **„F5-SSH-SSL-Zertifizierung“** erstellt keine CI-Beziehungen.

Fortinet Firewall und FortiGate VDOM REST-basierte Discovery

Die Anwendung Muster für Discovery und Service-Mapping verwendet das Muster „Next Generation Fortinet Network Firewall – REST“, um Fortinet -Firewalls über REST-API-Aufrufe zu finden. Darüber hinaus sucht die Mustererweiterung VDOM Discovery nach FortiGate Virtual Domains (VDOMs). Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Muster „Next Generation Fortinet Network Firewall – REST“ verwendet eine Reihe von REST-API-Aufrufen, um die Fortinet -Firewalls zu finden. Discovery verwendet das Muster für die Horizontal-Discovery.

Hinweis: Nur die REST-basierte Firewall-Discovery-Methode Fortinet findet FortiGate-VDOMs. Die SNMP-basierte Fortinet -Firewall-Discovery-Methode erkennt sie nicht. Informationen zur standardmäßigen SNMP-basierten Firewall-Discovery Fortinet finden Sie unter SNMP-basierte Discovery der Netzwerk-Firewall der nächsten Generation Fortinet ..

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Informationen zu Fortinet Firewalls und den Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

API-Token erstellen

Erstellen Sie ein API-Token in Fortinet. Anweisungen zum Erstellen eines API-Tokens finden Sie in der Fortinet-Dokumentbibliothek , und suchen Sie in der Produktfamilie „FortiConverter Tool“ nach dem Artikel „FortiGate-Gerät über API-Token verbinden – Online-Hilfe“.

Verifizieren Sie den API-Zugriff und die Berechtigungen

- Vergewissern Sie sich, dass MID-Server auf die APIs Fortinet zugreifen kann.
- Vergewissern Sie sich, dass das API-Token über ausreichende Berechtigungen zum Abrufen der erforderlichen Informationen von den Fortinet -Geräten verfügt.

Erforderliche Fortinet APIs:

- `v2/cmdb/system/global`
- `api/v2/monitor/system/status`
- `api/v2/cmdb/system/ha`
- `api/v2/cmdb/router/static`
- `/api/v2/cmdb/firewall/policy`
- `api/v2/cmdb/system/vdom-property`
- `api/v2/cmdb/system/interface`
- `/api/v2/monitor/system/interface/select`

SNMP-basierte Fortinet -Firewall-Discovery deaktivieren

Weitere Informationen finden Sie unter SNMP-basierte Fortinet -Firewall-Discovery deaktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Alias für die API Key-Anmeldeinformationen

Weitere Informationen finden Sie unter Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen für die REST-basierte Discovery der Firewall Fortinet ..

Zeitplan für Erkennung ohne Server erstellen

Weitere Informationen finden Sie unter Erstellen Sie einen serverlosen Zeitplan für die REST-basierte Discovery der Firewall Fortinet ..

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das Muster „Next Generation Fortinet Network Firewall – REST“ ausgeführt wird.

Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]

Feld	Beschreibung
Name [name]	Feld**„Hostname“** des Geräts Fortinet
Seriennummer [serial_number]	Seriennummer des Geräts Fortinet.
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname des Fortinet -Geräts.
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät Fortinet im Status „Aktiv“ befindet.
IP-Adresse [ip_address]	IP-Adresse des Fortinet -Geräts.
Hersteller [manufacturer]	Fortinet Gerätehersteller.
Beschreibung [short_description]	Kurze Beschreibung des Geräts Fortinet.
Modellnummer [model_number]	Fortinet Modellnummer des Geräts.
Firmware-Version [Firmware-Version]	Fortinet Firmware-Version des Geräts.
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet]

Feld	Beschreibung
Name [name]	Feld**„Hostname** “ des Firewall-Clusters Fortinet
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname des Firewall-Clusters.
IP-Adresse [ip_address]	IP-Adresse des Firewall-Clusters.
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurze Beschreibung des Firewall-Clusters.
Modellnummer [model_number]	Modellnummer des Geräts
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
Alias [alias]	Vom Anwender zugewiesener Name für den Netzwerkadapter.
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
Name [name]	Name des Netzwerkadapters
Konfigurationselement [cmdb_ci]	Referenziert die Fortinet-Firewall-Gerätetabelle [cmdb_ci_firewall_device_fortinet].

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse der Fortinet -Firewall.
Netzmaske [netmask]	Netzmaske der Fortinet -Firewall.

Seriennummer [cmdb_serial_number]

Feld	Beschreibung
Konfigurationselement [cmdb_ci]	Referenziert die Fortinet-Firewall-Gerätetabelle [cmdb_ci_firewall_device_fortinet].

Discovery füllt die Daten in CMDB aus, wenn die Mustererweiterung „Next Generation Fortinet Network Firewall – REST“-Mustererweiterung VDOM-Discovery ausgeführt wird.

Virtuelle Fortinet-Domäne [cmdb_ci_fortinet_vdom]

Feld	Beschreibung
VDOM-Index [vdom_index]	Index des VDOM in der Liste.
Name [name]	Name des VDOM.
Beschreibung [short_description]	Beschreibung der VDOM-Eigenschaft, die zusätzlichen Kontext oder zusätzliche Informationen zum Zweck der Eigenschaft bietet.

Fortinet-Firewall-Schnittstelle [cmdb_ci_fortinet_firewall_interface]

Feld	Beschreibung
ID [id]	Eindeutiger Bezeichner für die Schnittstelle. Beispiel: port1.
Name [name]	Name der Schnittstelle. Beispiel: LAN
IP-Adresse [ip_address]	Der Schnittstelle zugewiesene IP-Adresse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fortinet-Firewall-Schnittstelle [cmdb_ci_fortinet_firewall_interface] (Fortsetzung)

Feld	Beschreibung
Beschreibung [short_description]	Beschreibung der Schnittstelle, wird häufig zu Dokumentations- oder Identifizierungszwecken verwendet. Beispiel: Haupt-LAN-Schnittstelle.
MAC-Adresse [mac_address]	MAC-Adresse der Schnittstelle.
Zugriffstyp [access_type]	Typ der Schnittstelle. Beispiel: physisch, VLAN oder Aggregat.

Netzwerktopologie [cmdb_ci_network_topology]

Feld	Beschreibung
Name [name]	Virtual LAN(VLAN)-ID, die der Schnittstelle zugeordnet ist, falls zutreffend. Das Format lautet: `VLAN-{Vlan ID}`. Beispiel: VLAN-310.

Fortinet-Firewall-Richtlinie [cmdb_ci_fortinet_firewall_policy]

Feld	Beschreibung
Richtlinien-ID [policy_id]	Eindeutige ID, die der Richtlinie auf VDOM- oder Geräteebene zugewiesen ist.
UUID [uuid]	Globaler eindeutiger Identifier (GUID) für die Firewallrichtlinie.
Name [name]	Name der Richtlinie
source_interface	Netzwerkschnittstelle, von der der Datenverkehr stammt.
target_interface	Netzwerkschnittstelle, an die der Datenverkehr geleitet wird.
Quelladresse [source_address]	Quelladresse oder Adressgruppe, von der der Datenverkehr stammt.
Zieladresse [destination_address]	Zieladresse oder Adressgruppe, an die der Datenverkehr geleitet wird.
Internetservice [internet_service]	Von der Richtlinie verwalteter Service oder Anwendung, häufig dargestellt durch eine Servicegruppe oder einen Namen.

CI-Beziehungen

Discovery erstellt diese Beziehungen, um die Firewall-Discovery Fortinet von zu unterstützen.

CI	Beziehung	CI
Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet]	Gehostet auf::Hostet	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Verwendet::Verwendet von	Routerschnittstelle [dscy_router_interface]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Routerschnittstelle [dscy_router_interface]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Seriennummer [cmdb_serial_number]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]

Discovery erstellt diese Beziehungen zur Unterstützung der FortiGate VDOM-Discovery.

CI	Beziehung	CI
Fortinet-Firewall-Schnittstelle [cmdb_ci_fortinet_firewall_interface]	Erweitert::Erweitert um	Netzwerkschnittstelle [cmdb_ci_ni_interface]
Fortinet-Firewall-Richtlinie [cmdb_ci_fortinet_firewall_policy]	Erweitert::Erweitert um	Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_sec_policy]
Virtuelle Fortinet-Domäne [cmdb_ci_fortinet_vdom]	Enthält::Enthalten in	Fortinet-Firewall-Schnittstelle [cmdb_ci_fortinet_firewall_interface]
Virtuelle Fortinet-Domäne [cmdb_ci_fortinet_vdom]	Enthält::Enthalten in	Fortinet-Firewall-Richtlinie [cmdb_ci_fortinet_firewall_policy]
Virtuelle Fortinet-Domäne [cmdb_ci_fortinet_vdom]	Erweitert::Erweitert um	IP-Firewall [cmdb_ci_ip_firewall]
Virtuelle Fortinet-Domäne [cmdb_ci_fortinet_vdom]	Gehostet auf::Hostet	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Netzwerktopologie [cmdb_ci_network_topology]	Mitglieder::Mitglied von	Fortinet-Firewall-Schnittstelle [cmdb_ci_fortinet_firewall_interface]

SNMP-basierte Fortinet -Firewall-Discovery deaktivieren

Deaktivieren Sie die standardmäßige SNMP-basierte Fortinet -Firewall-Discovery, und verwenden Sie stattdessen die REST-basierte Discovery, um FortiGate Virtual Domains (VDOMs) zu erkennen.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery-Definition** > **CI-Klassifizierung** > **SNMP**.
2. Suchen Sie im Feld **Name** nach `Fortinet Firewall`.
3. Wählen Sie den Fortinet-Firewall-Datensatz aus.
4. Deaktivieren Sie das Kontrollkästchen **Aktiv**.
5. Wählen Sie **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Erstellen Sie einen Alias, und fügen Sie ihn den API-Schlüssel-Anmeldeinformationen hinzu. Weitere Informationen finden Sie unter Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen für die REST-basierte Discovery der Firewall Fortinet ..

Zugehörige Informationen

Fortinet Firewall und FortiGate VDOM REST-basierte Discovery

Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen für die REST-basierte Discovery der Firewall Fortinet .

Erstellen Sie einen Alias, und fügen Sie ihn den API-Schlüssel-Anmeldeinformationen hinzu, um Fortinet -Firewalls und FortiGate Virtual Domains (VDOMs) über REST-basierte Discovery zu erkennen.

Vorbereitungen

Erstellen Sie ein API-Token in Fortinet. Weitere Informationen finden Sie unter Voraussetzungen API-Token erstellen in Fortinet Firewall und FortiGate VDOM REST-basierte Discovery.

Erforderliche Rolle: discovery_admin

Prozedur

1. Erstellen Sie einen Alias.
   a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Aliasse für Verbindungen und Anmeldeinformationen**.
   b. Wählen Sie **Neu**.
   c. Geben Sie einen eindeutigen Namen für den Alias ein, und wählen Sie im Feld **TypAnmeldeinformationen** für den Aliastyp aus.
   d. Wählen Sie **Absenden**.
2. Konfigurieren Sie API-Schlüssel-Anmeldeinformationen für den neuen Alias.
   a. Navigieren zu **Discovery** > **Anmeldeinformationen**.
   b. Wählen Sie **Neu**.
   c. Wählen Sie **API Key-Anmeldeinformationen**aus.
   d. Entsperren Sie das Feld **Alias für Anmeldeinformationen**, und wählen Sie den von Ihnen erstellten Alias aus.
   e. Konfigurieren Sie die restlichen Formularfelder für **API-Schlüssel-Anmeldeinformationen**.
   f. Wählen Sie **Absenden**.
   Weitere Informationen zu den Feldern des Formulars mit Anmeldeinformationen für API-Schlüssel finden Sie unter Anmeldeinformationen für API-Keys .

Nächste Maßnahme

Erstellen Sie einen serverlosen Zeitplan für die REST-basierte Discovery der Fortinet -Firewall. Weitere Informationen finden Sie unter Erstellen Sie einen serverlosen Zeitplan für die REST-basierte Discovery der Firewall Fortinet ..

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Fortinet Firewall und FortiGate VDOM REST-basierte Discovery

Erstellen Sie einen serverlosen Zeitplan für die REST-basierte Discovery der Firewall Fortinet .

Erstellen Sie einen serverlosen Discovery-Zeitplan, um Fortinet -Firewalls und FortiGate Virtual Domains (VDOMs) über REST-basierte Discovery zu erkennen.

Vorbereitungen

- Stellen Sie sicher, dass Sie die IP-Adresse für das Firewall-Gerät Fortinet haben.
- Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen. Weitere Informationen finden Sie unter Erstellen Sie einen Alias für die API-Schlüssel-Anmeldeinformationen für die REST-basierte Discovery der Firewall Fortinet ..

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Zeitpläne**.
2. Wählen Sie **Neu**.
3. Konfigurieren Sie das Formular „Discovery-Zeitplan“.

Formular „Neuer Datensatz des Discovery-Zeitplans“.

Feld	Beschreibung
Name	Eindeutiger Name für diesen Discovery-Zeitplan.
Discovery	Scantyp, der „Serverlos“ sein muss.
MID-Server	Name von MID-Server, der für diesen Zeitplan verwendet werden soll.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

4. Wählen Sie **Absenden**.
5. Wählen Sie auf der Seite „Discovery-Zeitpläne“ den von Ihnen erstellten Datensatz aus.
6. Wählen Sie auf der Registerkarte **Ausführungsmuster ohne ServerNeu**.
7. Füllen Sie die Felder des Formulars aus.

Formular „Neuer Datensatz“ für serverlose Ausführungsmuster

Feld	Beschreibung
Name	Beschreibender Name für diesen Datensatz.
Muster	Muster, das für diesen Zeitplan verwendet werden soll; muss das Muster „Next Generation Fortinet Network Firewall – REST“ sein.
Proxyhost	Vollqualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren; muss global sein.
Aktiv	Aktiviert diesen Zeitplan für die Discovery.

8. Wählen Sie **Absenden**.
9. Wählen Sie auf der Registerkarte **Startprogrammparameter für Discovery-Muster** den von Ihnen erstellten Datensatz aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Konfigurieren Sie die folgenden Parameter mit den relevanten Werten.

Parameter	Wert
ip_address	IP-Adresse des Firewall-Geräts.
Anmeldeinformationsalias	Name des von Ihnen erstellten Anmeldeinformationsalias.

11. Wählen Sie **Absenden**.

Nächste Maßnahme

Führen Sie Discovery entweder sofort aus, indem **Sie Jetzt erkennen** auswählen, oder warten Sie, bis der vordefinierte Zeitplan die Discovery auslöst.

Zugehörige Informationen

Fortinet Firewall und FortiGate VDOM REST-basierte Discovery

Erkennung des GCP-Assetbestands (Google Cloud Platform)

Die Anwendung ServiceNow Discovery verwendet das Asset-Bestandsmuster Google Cloud Platform (GCP), um Ressourcen und Richtlinien GCP von zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Das Muster bietet Sichtbarkeit für Services, die von der Asset Inventory-API unterstützt werden, sowie zum Sammeln von Bestandsdaten zu den bereitgestellten GCP-Services und zum Aktualisieren der CMDB.

Das Muster sammelt Bestandsdaten entweder für alle von GCP unterstützte Ressourcen oder für eine vorkonfigurierte Aufnahmeliste von Ressourcen. Die Aufnahmeliste für Ressourcen des Cloud-Bestands enthält alle Ressourcentypen, die vom Bestand von GCP-Cloud-Assets unterstützt werden, mit Ausnahme von Compute Engine-Ressourcen und IAM-Richtlinien. Ihren Anforderungen entsprechend können Sie die Aufnahmeliste um zusätzliche Ressourcentypen erweitern. Weitere Informationen zu Google Cloud-Assets finden Sie unter https://cloud.google.com/resource-manager/docs/cloud-asset-inventory/overview .

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Ab Muster für Discovery und Service-Mapping Version 1.18.1 können Sie den Speicher GCP durch zwei Discovery-Arten erkennen: ohne Server und Cloud-Discovery. Durch das Ausführen von Cloud-Discovery-Zeitplänen können Sie einen Zeitplan für alle Ihre GCP -Projekte ausführen, ohne manuell separate Zeitpläne zu konfigurieren. Sie können die serverlose Discovery auch wie zuvor verwenden.

Das erweiterte Asset-Bestandsmuster Google Cloud Platform (GCP) führt Abfragen aus, um die Konfigurationen in Ihrem System zu überprüfen und eine Discovery entsprechend Ihren Konfigurationen auszulösen. Die Abfragen nach Reihenfolge:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wenn Sie die **Startprogrammparameter für Discovery-Muster** konfiguriert haben, löst das Muster einen Discovery-Zeitplan ohne Server aus.

2. Wenn die vorherige Abfrage keine Ergebnisse liefert, fragt das Muster weiterhin ab, ob Sie die Eigenschaft *mid.gcp_resource_inventory_bucketpath* MID-Server konfiguriert haben. Wenn Sie dies tun, führt das Muster einen Cloud-Discovery-Zeitplan nach Cloud-Accounts aus.

3. Wenn die vorherige Abfrage keine Ergebnisse liefert, fragt das Muster weiterhin ab, ob Sie die Eigenschaft *mid.gcp_resource_inventory_bucketpath.default* MID-Server konfiguriert haben. Wenn Sie dies tun, löst das Muster einen standardmäßigen Cloud-Discovery-Zeitplan aus.

4. Wenn keine dieser Eigenschaften konfiguriert ist, wird das Muster ordnungsgemäß beendet.

Voraussetzungen

Stellen Sie sicher, dass die Store-Apps auf dem neuesten Stand sind

- Muster für Discovery und Service-Mapping
- Visibility Content

GCP Autorisierung für Discovery zur Verwendung der Cloud Asset API

- API-Endpunkt: *https://cloudasset.googleapis.com/v1/projects/*<account_id> :exportAssets
- Mindestens eine der folgenden IAM-Berechtigungen für das angegebene übergeordnete Ressourcenelement erforderlich:
  - cloudasset.assets.exportResource
  - cloudasset.assets.exportIamPolicy

Service-Account-Anwender für die Cloud-Speicher-API

Der Cloud-Service-Account ServiceNow benötigt eine schreibgeschützte Berechtigung von GCP, um auf den API-Endpunkt – https://www.googleapis.com/storage/v1 zuzugreifen.

Hinweis: Mit den Headern auf der Verschlüsselungsseite können Sie Folgendes tun:

- Laden Sie ein Objekt herunter, das mit einem vom Kunden bereitgestellten Verschlüsselungsschlüssel verschlüsselt ist.
- Rufen Sie Objektmetadaten mit Inhalts-Hashes ab.

Berechtigung zum Lesen und Schreiben in einem Cloud Storage-Bucket

- Speicherobjektersteller
- Speicherobjekt-Viewer
- Speicherobjektadministrator

Erstellen Sie mit der Google Cloud Console einen Cloud Storage-Bucket

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Rufen Sie die **Google Cloud Console**auf.
2. Wählen Sie im **Navigationsmenü**die Option aus **Cloud Storage** > **Buckets**.
3. Um einen neuen Bucket zu erstellen, wählen Sie **+ Erstellen aus**.
4. Füllen Sie auf der Seite **Bucket erstellen** die Bucket-Informationen aus.

Feld	Beschreibung
Benennen Sie Ihren Bucket	Geben Sie einen global eindeutigen Namen für Ihren Bucket ein.
Wählen Sie aus, wo Ihre Daten gespeichert werden sollen	Wählen Sie einen Ortstyp und einen Ort aus, an dem die Bucket-Daten dauerhaft gespeichert werden. ◦ Standorttyp: Multiregional, für globalen Speicher (z. B. us, eur, asien). ◦ Speicherort: Liste der Cloud Storage-Speicherorte, die zum Speichern Ihrer Daten verfügbar sind.
Wählen Sie eine Speicherklasse für Ihre Daten	Wählen Sie die Speicherklasse aus, die Ihren Anforderungen entspricht (z. B. „Standard“, „Nearline“, „Coldline“ oder „Archive“).
Wählen Sie aus, wie der Zugriff auf Objekte gesteuert werden soll	Wählen Sie aus, ob Ihr Bucket die Verhinderung des öffentlichen Zugriffs erzwingt.
Wählen Sie aus, wie Objektdaten geschützt werden sollen	Konfigurieren Sie bei Bedarf Schutztools.

5. Wählen Sie **Erstellen** aus.

Hinweis: Weitere Informationen finden Sie in der Dokumentation zu Google Cloud Storage .

Aufbewahrungsrichtlinie für den Speicher-Bucket

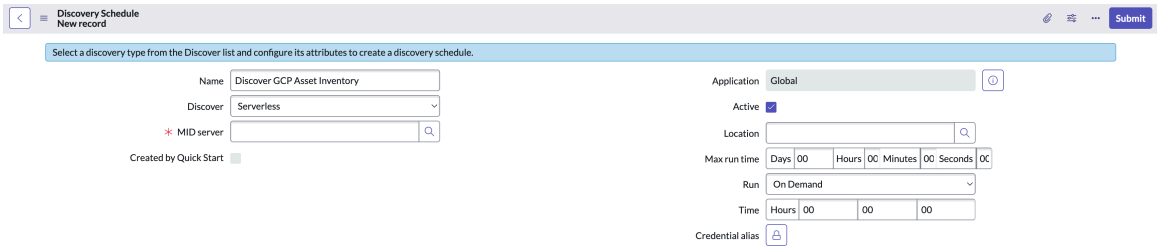
Stellen Sie sicher, dass die Aufbewahrungsrichtlinie für den Speicher-Bucket nicht aktiv ist. Wenn die Aufbewahrungsrichtlinie aktiv ist, kann die automatisch generierte Bestandsdatendatei nicht nach dem Muster gelöscht werden.

Erstellen Sie einen Discovery-Zeitplan ohne Server

Erstellen Sie einen Discovery-Zeitplan, um eine gezielte Erkennung des Asset-Bestands GCP durchzuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular

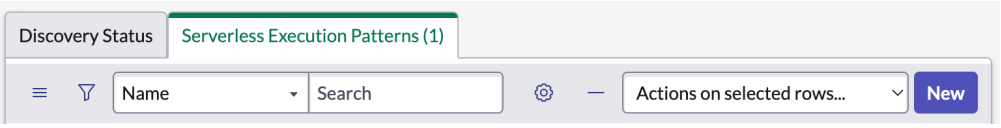


aus.

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Name des Discovery-Zeitplans. Beispiel: `GCP-Asset-Bestand erkennen`.
Erkannt	Erkennungstyp. Wählen Sie **Ohne Server** aus.
MID-Server	Name des MID-Servers
Ausführen	Option zum Auswählen, wann die nächste Discovery ausgeführt werden soll.

3. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.
4. Klicken Sie auf die Registerkarte **Ausführungsmuster ohne Server**, **Neu**, und füllen Sie das Formular aus.



Formular „Ausführungsmuster ohne Server“

Feld	Beschreibung
Name	Name dieses serverlosen Ausführungsmusters. Beispiel: `GCP-Asset-Bestand erkennen`.
Muster	Wählen Sie das Muster **Ressourcenbestand für Google Cloud Platform (GCP)** aus.
Proxyhost	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. Geben Sie **Global** an.
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie **Absenden**.
6. Konfigurieren Sie auf der Registerkarte **Parameter des Discovery-Muster-Startprogramms** die folgenden Parameter mit den relevanten Werten:

Parameter	Wert
cloud_account_id	Projekt-ID in GCP
full_path_file	Der vollständige Dateipfad des Speicher-Buckets. Beispiel: `gs://<bucketname>` .
cloud_cred_id	Sysid der GCP-Anmeldeinformationen
cloud_datacenter_type	`cmdb_ci_google_datacenter`

Speicher-Discovery-Konfigurationen mit den Eigenschaften MID-Server

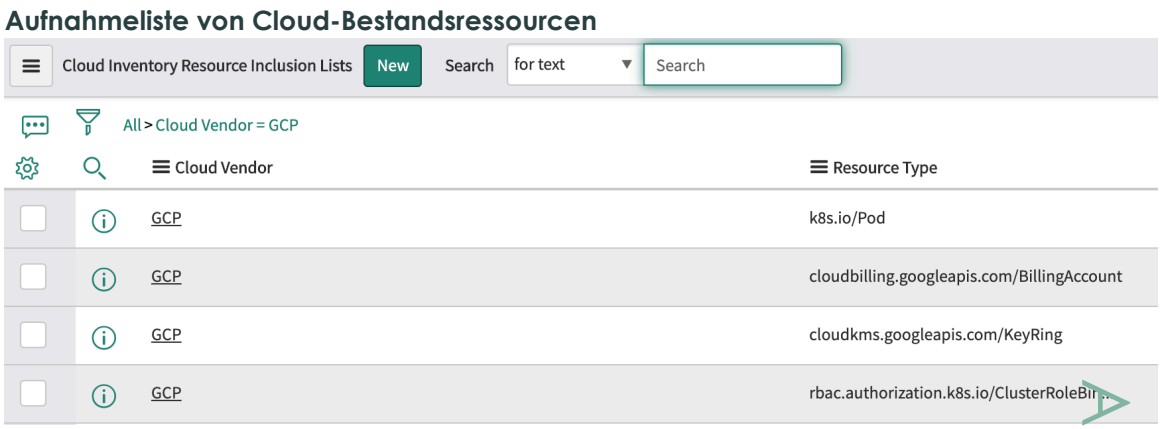
1. Konfigurieren Sie die Eigenschaft *`mid.gcp_resource_inventory_bucketpath`*.
   a. Navigieren zu **Alle** > **MID-Server** > **Eigenschaften** und filtern Sie die Liste nach `Name beginnend mit mid.gcp`.
   b. Wählen Sie *`mid.gcp_resource_inventory_bucketpath`*.
   c. Füllen Sie das Formular aus.
      i. Konfigurieren Sie das Feld **Name** der Eigenschaft so, dass Ihre Account-ID wie folgt aufgenommen wird: `mid.gcp_resource_inventory_bucketpath.`<Cloud Account Id> .
      ii. Füllen Sie das Feld **„Wert“** mit dem Bucket-URI aus. Dies ist der vollständige Dateipfad des Speicher-Buckets. Beispiel: `gs://`<bucketname> .
      iii. Lassen Sie das Feld **MID-Server** leer, um eine MID-Server -Eigenschaft festzulegen, die sich auf alle MID-Server auswirkt. Zum Festlegen der Eigenschaft MID-Server für ein bestimmtes ElementMID-Serverwählen Sie den gewünschten Server aus.
      iv. Wählen Sie **Aktualisieren**.
2. Konfigurieren Sie die Eigenschaft *`mid.gcp_resource_inventory_bucketpath.default`*.
   a. Navigieren zu **Alle** > **MID-Server** > **Eigenschaften** und filtern Sie die Liste nach `Name beginnend mit mid.gcp`.
   b. Wählen Sie *`mid.gcp_resource_inventory_bucketpath.default`*.
   c. Füllen Sie das Feld **„Wert“** mit dem Bucket-URI aus. Dies ist der vollständige Dateipfad des Speicher-Buckets. Beispiel: `gs://`<bucketname> .
   d. Wählen Sie **Aktualisieren**.

Weitere Informationen finden Sie unter Asset-Metadaten von einem Projekt in ein anderes exportieren

Aufnahmeliste für Cloud-Bestandsressourcen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um Bestandsdaten für von GCPunterstützte Ressourcen zu sammeln, navigieren Sie in Now Platformzu **Cloud-Bestandsressourceneinschlussliste**, und löschen Sie alle Datensätze der Tabelle GCP.



- Feintunen Sie die Erkennung von GCP-Ressourcen mithilfe der Aufnahmeliste von Cloud-Bestandsressourcen.

  Wenn Ihre Bereitstellung benutzerdefinierte Muster für die GCP-Erkennung hat, stellen Sie sicher, dass Sie GCP-Ressourcen nicht zweimal entdecken:

  1. Stellen Sie sicher, dass der Anwendungsbereich „Discovery and Service Mapping Patterns“ ist:
     a. Navigieren zu **Einstellungen** > **Entwickler**.
     b. Wählen Sie `Discovery and Service Mapping Patterns` aus der Liste **Anwendung** aus.
  2. Navigieren zu **Systemdefinitionen** > **Tabellen**.
  3. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].
  4. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.
  5. Wählen Sie Ressourcentypen aus, für die Sie benutzerdefinierte Muster haben, und wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option `Löschen` aus.

  Die Aufnahmeliste für Cloud-Bestandsressourcen ist mit allgemeinen Services vordefiniert. Sie können die Liste wie folgt mit zusätzlichen Ressourcentypen erweitern, die vom Muster erkannt werden sollen:

  Hinweis: Wenn Sie die im Basissystem bereitgestellte Liste ändern, wird sie bei Anwendungsupdates nicht mehr automatisch aktualisiert. Sie müssen anwenderdefinierte Listen selbst pflegen.

  1. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].
  2. Klicken Sie auf **Neu**.
  3. Füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

  Hinweis: Die Namen der zusätzlichen Ressourcentypen müssen den entsprechenden Namenskonventionen der Lieferanten entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Cloud-Anbieter	Der Lieferant des Ressourcentyps: GCP
Ressourcentyp	Wert des GCP-Ressourcentyps
Anwendung	Der Anwendungsbereich: Discovery and Service Mapping Patterns

Die Änderungen werden beim nächsten Ausführen des Musters angewendet.

Von Discovery während der horizontalen Erkennung erfasste Daten

Dieses Muster erkennt Daten, die Sichtbarkeit für alle GCP-Services in Ihrer Organisation bieten. Die erkannten Daten umfassen die folgenden Tabellen und Felder.

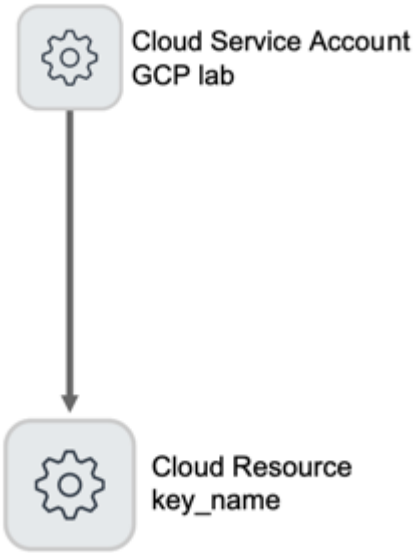
Tabelle und Feld	Beschreibung
Haupt-CI [cmdb_ci_cmp_resource]	
object_id	Die ID des Elements. Das Element wird mit dieser URL aufgerufen.
name	Der Name der Ressource
resource_type	Der Asset-Ressourcentyp gemäß den Daten in der JSON-Datei
Schlüsselwert [cmdb_key_value]	
Key	Der GCP-Tag-Schlüsselname.
Wert	Der GCP-Tag-Wertname.

Die Dependency Views-Zuordnung zeigt die erkannten Konfigurationselemente (CIs) in Ihrer Organisation und die Beziehungen zwischen ihnen an. Hier ist die einzige bedeutungsvolle Beziehung zwischen den CIs die, mit der Discovery sie identifizieren kann.

Jedes GCP-Bestand-CI ist entweder einem Logischen Datenzentrum (LDC)-CI oder einem Cloud-Servicekonto-CI zugeordnet. In diesem Beispiel bezieht sich das Bestand-CI auf ein Cloud-Servicekonto-CI.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dependency Views-Zuordnung mit Cloud-Servicekonto-CI



CI-Beziehungen

Diese Beziehungen sollen die GCP-Asset-Bestandserkennung unterstützen:

CI	Beziehung	CI
Für globale Ressourcen:		
Haupt-CI [cmdb_ci_cmp_resource]	Enthalten in::Enthält	Cloud-Servicekonten
Für regionale Ressourcen:		
Haupt-CI [cmdb_ci_cmp_resource]	HostedOn::Hosts	Logisches Rechenzentrum (LDC)

Google Cloud Platform (GCP)-Organisationserkennung

Die Anwendung ServiceNow Discovery verwendet das Google Cloud Platform (GCP)-Organisationserkennungsmuster, um GCP-Organisationsprojekte und -ressourcen zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Weitere Informationen zu Systemanforderungen und Familienkompatibilität finden Sie in der Anwendungsliste auf der Website des ServiceNow Store .

GCP-Organisationsstruktur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergewissern Sie sich, dass eine GCP-Organisationsressource ordnungsgemäß strukturiert ist und sich die Projekte in einer anderen Hierarchie darunter befinden.

Stellen Sie sicher, dass für alle Projekte unter der GCP-Organisationsressource die Compute Engine-API aktiviert ist.

Servicekonto-Benutzereinstellungen

Überprüfen Sie, ob Benutzer des Servicekontos Zugriff auf den Ressourcenknoten der GCP-Organisation haben.

Stellen Sie sicher, dass Servicekonto-Benutzer Mitglieder aller anderen Projekte sind, die sich unter dem GCP -Organisationsressourcenknoten befinden.

Stellen Sie sicher, dass Servicekonto-Benutzer über die folgenden Cloud-Identitäts- und Zugriffsverwaltungs-Anmeldeinformationen für Projekte unter der GCP-Organisationsressource verfügen:

- resourcemanager.folders.list
- resourcemanager.organizations.get
- resourcemanager.projects.get
- resourcemanager.projects.list

Anmeldeinformationen für API-Elemente

Während der Erkennung verwendet das Muster folgende API-Elemente. Der Benutzer, der den Anmeldeinformationen in der Instanz hinzugefügt wurde, muss über Berechtigungen zum Senden dieser Abfragen verfügen.

- https://cloudresourcemanager.googleapis.com/v1/{name=organizations/*}
- https://cloudresourcemanager.googleapis.com/v1/projects
- https://cloudresourcemanager.googleapis.com/v2/folders:search

Anmeldeinformationen für die Erstellung eines Erkennungszeitplans

Konfigurieren Sie die folgenden Anmeldeinformationen:

1. Erstellen Sie GCP-Anmeldeinformationen.
2. Erstellen Sie ein GCP-Servicekonto:
   a. Anmeldeinformationen: Die GCP-Anmeldeinformationen
   b. Konto-ID: Die Google-Servicekonto-ID
   c. Rechenzentrumstyp: Wählen Sie **cmdb_ci_google_datacenter** aus.
3. Erstellen Sie einen Erkennungszeitplan.

(Optional) Erkennungszeitplan ohne Server erstellen

Erstellen Sie einen Erkennungszeitplan, um eine gezielte Erkennung von GCP-Organisationsressourcen durchzuführen.

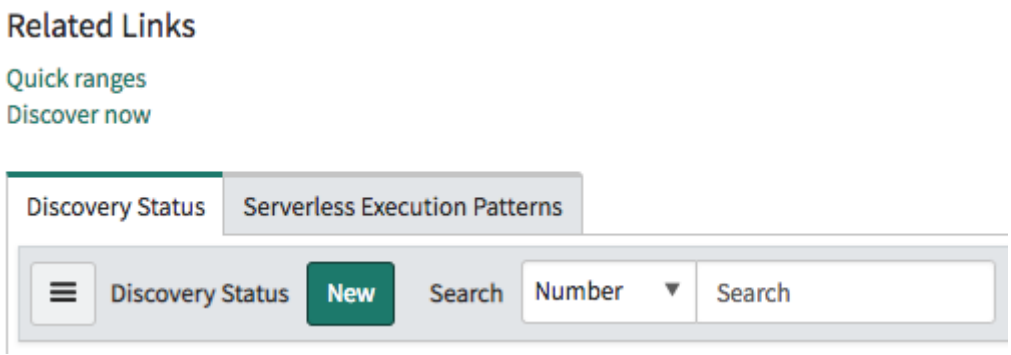
1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Name des Discovery-Zeitplans. Beispielsweise `GCP-Organisation erkennen`.
Erkennen	Erkennungstyp. Wählen Sie **Ohne Server** aus.
MID-Server	Name des MID-Servers
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

3. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.
4. Klicken Sie auf die Registerkarte **Ausführungsmuster ohne Server**, **Neu**, und füllen Sie das Formular aus.



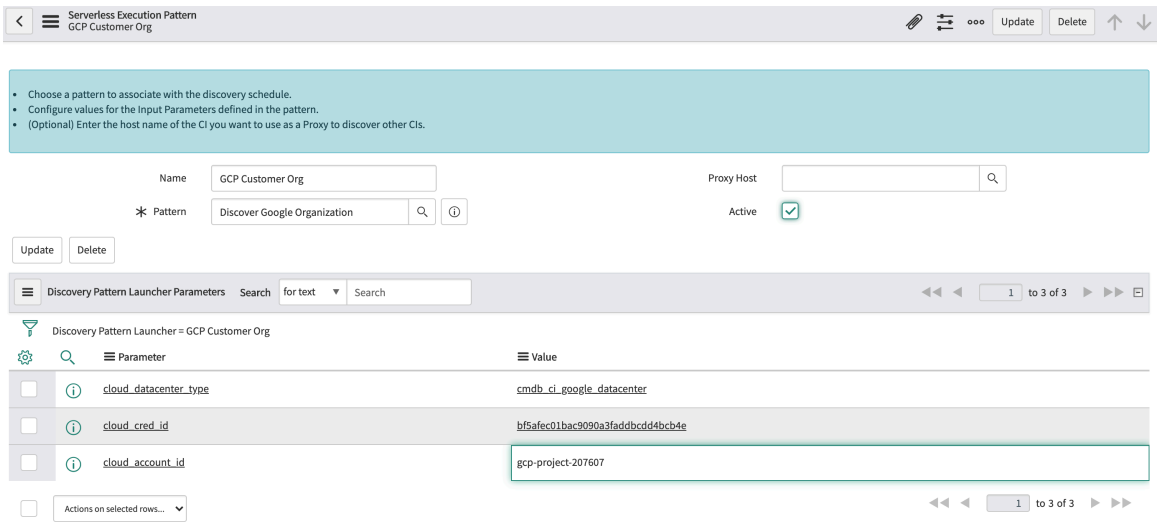
Formular „Ausführungsmuster ohne Server“

Feld	Beschreibung
Name	Name dieses serverlosen Ausführungsmusters. Beispielsweise `GCP-Organisation erkennen`.
Muster	Name des auszuführenden Musters: GCP Organization.
Proxy-Host	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. Geben Sie **Global** an.
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

5. Konfigurieren Sie unter **Startprogrammparameter für Discovery-Muster** die folgenden Parameter mit den entsprechenden Werten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert
cloud_account_id	Projekt-ID in GCP
cloud_cred_id	Sysid der GCP-Anmeldeinformationen
cloud_datacenter_type	`cmdb_ci_google_datacenter`



Kunden mit frühem Zugriff auf das Muster „GCP Organization“

Stellen Sie sicher, dass die geplante Aufgabe „Discover-GCP-SubAccounts“ in Ihrer Instanz nicht aktiviert ist.

1. Navigieren zu **Systemdefinition** > **Geplante Aufgaben**.
2. Klicken Sie auf die geplante Aufgabe „Discover-GCP-SubAccounts“.
3. Deaktivieren Sie das Kontrollkästchen **Aktiv**, und klicken Sie auf **Aktualisieren**.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Organisation [cmdb_ci_cloud_org]	
name	Der Name der Organisationsressource
object_id	Die ID der Organisationsressource
time	Die Zeit, zu der die Organisationsressource in GCP erstellt wurde
operational_status	Aktueller Betriebsstatus. Eine der folgenden Möglichkeiten: • Operativ • Nicht funktionsfähig • Reparatur in Arbeit • DR-Standby • Bereit • Stillgelegt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Ordner [cmdb_ci_gcp_folder]	
name	Der Name des Organisationsordners
parent_id	Die ID der übergeordneten Ressource
parent_type	Der Typ der übergeordneten Ressource. Kann `Organisation` oder `Ordner` sein.
time	Die Zeit, zu der die Ressource in GCP erstellt wurde
Status	Der Status des Ordners gemäß dem `Lebenszyklusstatus` in GCP
object_id	Die ID des Organisationsordners
Projekt [cmdb_ci_gcp_project]	
name	Der Name des Projekts
project_id	Die ID des Projekts
parent_id	Die ID der übergeordneten Ordnerressource
parent_type	Der Typ der übergeordneten Ressource. Kann `Organisation` oder `Ordner` sein.
time	Die Zeit, zu der die Ressource in GCP erstellt wurde
operational_status	Der Status des Ordners gemäß dem `Lebenszyklusstatus` in GCP
object_id	Die ID des Projekts
discovery_credentials	GCP-Kontoanmeldeinformationen
Ressource [cmdb_key_value]	
key	Der Schlüssel oder die Bezeichnung, die dem GCP-Projekt zugeordnet ist. Beispiel: `Land`.
Wert	Der dem GCP-Projekt zugewiesene Projektbezeichnungswert. Beispiel: `ca`.
configuration_item	Die URL oder der Pfad des CI.

CI-Beziehungen

CI	Beziehung	CI
Cloud-Organisation [cmdb_ci_cloud_org]	Enthalten in::Enthält	Google-Projekt [cmdb_ci_gcp_project]
Cloud-Organisation [cmdb_ci_cloud_org]	Enthalten in::Enthält	Servicekonto
Cloud-Organisation [cmdb_ci_cloud_org]	Enthalten in::Enthält	Google-Ordner [cmdb_ci_gcp_folder]
Servicekonto	Eigentümer von::Eigentum von	Google-Projekt [cmdb_ci_gcp_project]
Google-Ordner [cmdb_ci_gcp_folder]	Enthalten in::Enthält	Google-Projekt [cmdb_ci_gcp_project]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Google-Ordner [cmdb_ci_gcp_folder]	Enthalten in::Enthält	Untergeordneter Google-Ordner
Untergeordneter Google-Ordner	Enthalten in::Enthält	Google-Projekt [cmdb_ci_gcp_project]

HAProxy Lastenausgleichsmodul-Discovery mit Mustern

Die Anwendung Muster für Discovery und Service-Mapping verwendet das HA-Proxy-Muster, um das Community-Lastenausgleichsmodul HAProxy zu finden, das auf einem Server Linux vom Typ ausgeführt wird. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

HAProxy Community-Edition ist ein Open-Source-Lastenausgleichsmodul, das entweder im TCP- oder HTTP-Modus ausgeführt werden kann. Beachten Sie, dass HAProxyDiscovery zwar den HTTP-Lastenausgleich unterstützt, der TCP-Lastenausgleich jedoch nicht.

Ab Muster für Discovery und Service-Mapping Version 1.15.0 ist die musterbasierte Discovery die Standardmethode zur Erkennung von HAProxy -Lastenausgleichsmodulen. Informationen zur probebasierten Erkennung HAProxy finden Sie unter HAProxy Lastenausgleichsmodul-Discovery mit Probes.

Hinweis: HAProxy Die Discovery von unterstützt 1:1-Beziehungszuordnungen zwischen einem Front-End-Port und einem Back-End-Port. Wenn mehrere Front-Ends mit demselben Back-End verbunden sind, ordnet der Discovery-Prozess nur die Beziehung von der niedrigsten Front-End-Portnummer in einem definierten Bereich zum Back-End-Port zu.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Informationen zu den Lastenausgleichsmodulen HAProxy und den Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- Visibility Content

Stellen Sie sicher, dass HAProxy auf dem Server Linux installiert ist

Stellen Sie sicher, dass die Software HAProxy auf einem Server Linux installiert ist und ausgeführt wird.

Überprüfen Sie die Berechtigung zum Ausführen des Befehls HAProxy .

Vergewissern Sie sich, dass Sie zum Ausführen des folgenden Befehls berechtigt sind:<HAproxy Installation Path> `/haproxy -v`.

Verifizieren Sie den Lesezugriff auf die Konfigurationsdatei HAProxy .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass Sie Lesezugriff auf die Datei `haproxy.cfg` haben.

SSH-Anmeldeinformationen erstellen

Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Horizontale Erkennung planen

Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das HA-Proxy-Muster ausgeführt wird.

HAProxy Load Balancer [cmdb_ci_lb_haproxy]

Feld	Beschreibung
Name [name]	Name des Lastenausgleichsmoduls HAProxy.
Version [version]	Version des Lastenausgleichsmoduls HAProxy.
Beschreibung [short_description]	Beschreibung des Prozesses HAProxy, die durch Ausführen des folgenden Befehls abgerufen wird: `haproxy -version`.

Load Balancer-Service [cmdb_ci_lb_service]

Feld	Beschreibung
Name [name]	Name des Lastenausgleichsmoduls im folgenden Format:<LB name> `:`<LB port> .
Port [port]	Port, den das Lastenausgleichsmodul abhört.
IP-Adresse [ip_address]	IP-Adresse des Lastenausgleichsmodul-Services.
Letzter Port [last_port]	Höchste vom Lastenausgleichsmodul-Service verwendete Portnummer.
Load Balancer [load_balancer]	Referenziert die Tabelle „HAProxy-Lastenausgleichsmodul“ [cmdb_ci_lb_haproxy].

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Name [name]	Name des Pools von Lastenausgleichsmodulen
Load Balancer [load_balancer]	Referenziert die Tabelle „HAProxy-Lastenausgleichsmodul“ [cmdb_ci_lb_haproxy].
Lastenausgleichsmethode [load_balancing_method]	Methode für den Lastenausgleich des Pools, z. B. Round-Robin.
Neueste Discovery [last_discovered]	Zeitstempel der neuesten Discovery.
Installationsstatus [install_status]	Installationsstatus des Lastenausgleichsmodul-Pools, z. B.: Installiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]

Feld	Beschreibung
Name [name]	Name des Mitglieds des Lastenausgleichsmodul-Pools.
Serviceport [service_port]	Vom Poolmitglied verwendeter Port
IP-Adresse [ip_address]	IP-Adresse des Hosts des Poolmitglieds
Pool [pool]	Referenziert die Tabelle „Lastenausgleichsmodul-Pool“ [cmdb_ci_lb_pool].
Load Balancer [load_balancer]	Referenziert die Tabelle „HAProxy-Lastenausgleichsmodul“ [cmdb_ci_lb_haproxy].

CI-Beziehungen

Discovery erstellt diese Beziehungen, um die Erkennung des Lastenausgleichsmoduls HAProxy zu unterstützen.

CI	Beziehung	CI
Load Balancer-Pool [cmdb_ci_lb_pool]	Zugeordnet zu::Zugeordnet von	Load Balancer-Service [cmdb_ci_lb_service]
Load Balancer-Pool [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Load Balancer-Pool [cmdb_ci_lb_pool]	Referenzen	HAProxy Load Balancer [cmdb_ci_lb_haproxy]
Load Balancer-Pool [cmdb_ci_lb_pool]	Referenzen	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]	Referenzen	HAProxy Load Balancer [cmdb_ci_lb_haproxy]
Load Balancer-Service [cmdb_ci_lb_service]	Referenzen	HAProxy Load Balancer [cmdb_ci_lb_haproxy]
Load Balancer-Service [cmdb_ci_lb_service]	Wird ausgeführt auf::Wird ausgeführt	Hardware [cmdb_ci_hardware]

Erkennung „HPE BladeSystem Enclosure“

ServiceNow Discovery verwendet das Erkennungsmuster „HPE BladeSystem Enclosure“, um BladeSystem-Muster zu erkennen. Das BladeSystem ist eine Reihe von Hewlett Packard Enterprise Blade-Server-Computern.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

- Stellen Sie sicher, dass Sie verwenden Muster für Discovery und Service-Mapping
- SNMP-Anmeldeinformationen für das Gehäuse festlegen (zur Verwendung durch den Klassifizierer)
- Legen Sie die SSH-Anmeldeinformationen für die Standardauthentifizierung für den Onboard-Administrator des Gehäuses fest (zu verwenden vom Muster Discovery).
- Die Erkennung wird anhand der IP-Adresse von Onboard Administrator ausgeführt.
- Stellen Sie sicher, dass der Hostcomputer vom MID-Serveraus erreichbar ist.

Authentifizierung und Autorisierung

Konfigurieren Sie die Anmeldeinformationen für die **Standardauthentifizierung** von Onboard Administrator für das Gehäuse. Das für den Zugriff auf Onboard Administrator verwendete Konto muss über Berechtigungen zum Anzeigen aller Einschübe des Gehäuses verfügen, damit die Informationen der Blade-Server erfasst werden können.

Highlights und Einschränkungen

Das Muster wurde getestet anhand von:

- HPE BladeSystem c7000-Gehäuse G2 und G3
- HPE BladeSystem-Blades: HPE ProLiant BL460c
  - Generation 8, 9 und 10
  - ROM-Versionen: I31, I36, I41 (2014-2021)
  - Von einem Virtual Connect Manager/Virtual Connect Enterprise Manager (VCM/VCEM) verwaltete Blades haben eine logische Seriennummer. In diesem Fall ist die Seriennummer, die beispielsweise von WMI verfügbar gemacht wird, die logische und nicht die physische Nummer, wie es normalerweise der Fall ist. Beim Erstellen der Beziehung zwischen dem Blade- und dem BS-Server versucht das System, die physische und die logische Seriennummer mit denen des BS-Servers abzugleichen.
  - Bei der Erkennung von Blade-Servern mit logischen Seriennummern werden ihre logischen Seriennummern in **cmdb_serial_number** mit dem Typ **logisch** eingefügt. Dies ist ein neuer Seriennummerntyp, der zur Unterstützung dieser von HP eingeführten neuen Seriennummern erstellt wurde.

    Hinweis: Die WMI stellt die logische Seriennummer als Bios-Seriennummer bereit. ESXi-Server werden von Probes erkannt. Das ESXiserver-CI erhält die logische Seriennummer als **Gehäuse**.

Von Discovery während der horizontalen Erkennung erfasste Daten

Das Erkennungsmuster „HPE BladeSystem Enclosure“ füllt die folgenden CIs:

Haupt-CI [cmdb_ci_hpe_bladesystem_enclosure]

Feld	Beschreibung
Name [name]	Name des Gehäuses.
UUID [uuid]	Eindeutiger Bezeichner des Gehäuses (proprietärer Bezeichner von HPE).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Haupt-CI [cmdb_ci_hpe_bladesystem_enclosure] (Fortsetzung)

Feld	Beschreibung
IP-Adresse [ip_address]	Management-IP des Gehäuses (Onboard Administrator-Adresse).
Modell-ID [model_id]	Typ des Gehäuses (Modell).
Hersteller [manufacturer]	Herstellername des Gehäuses („HP“ oder „HPE“, je nach Modell).
Seriennummer [serial_number]	Generierte Seriennummer gemäß der folgenden Konvention: **<Originalseriennummer des Gehäuses>::<UUID des Gehäuses>**.
Asset-Tag [asset_tag]	Asset-Tag, extrahiert aus den Daten des Gehäuses.
Modellnummer [model_number]	Teilenummer des Gehäuses (proprietär von HPE).
Midplane-Ersatzteilnummer [midplane_spare_part_number]	Ersatzteilnummer (proprietär von HPE) der Mittelebene.
PDU-Typ [pdu_type]	Typ der Stromverteilungseinheit.
PDU-Ersatzteilnummer [pdu_spare_part_number]	Ersatzteilnummer der Stromverteilungseinheit (proprietär von HPE).
Ablagetyp für Onboard-Administrator [onboard_admin_tray_type]	Typ des Onboard Administrator-Tray.
Onboard-Administrator – Ablage-Ersatzteilnummer [onboard_admin_tray_spare_part_number]	Ersatzteilnummer des Onboard Administrator-Tray (proprietär von HPE).
Onboard-Administrator – Ablageseriennummer [onboard_admin_tray_serial_number]	Seriennummer des Onboard Administrator-Tray.

Haupt-CI: [cmdb_ci_hpe_bladesystem_blade]

Feld	Beschreibung
Name [name]	Generierter Wert gemäß der folgenden Konvention: **<Name des Gehäuses>/bay-<Positionsnummer>**
UUID [uuid]	Eindeutiger Bezeichner des Blade-Servers (proprietärer HPE-Bezeichner).
Logische UUID [uuid_logical]	Der logische eindeutige Bezeichner des HPE Server Blade (proprietärer Bezeichner von HPE).
Modell-ID [model_id]	Produktname des Blade-Servers (Modell).
Hersteller [manufacturer]	Herstellername des Blade-Servers („HP“ oder „HPE“, je nach Modell).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Haupt-CI: [cmdb_ci_hpe_bladesystem_blade] (Fortsetzung)

Feld	Beschreibung
Seriennummer [serial_number]	Generierte Seriennummer gemäß der folgenden Konvention: **<Originalseriennummer des Blade>::<UUID des Blade>**.
Logische Seriennummer [serial_number_logical]	Die logische Seriennummer des HPE Server Blade (proprietärer Bezeichner von HPE).
Asset-Tag [asset_tag]	Asset-Tag, extrahiert aus den Daten des Blade
Modellnummer [model_number]	Teilenummer des Blade (proprietär von HPE).
RAM (MB) [ram]	RAM-Größe des Blade.
ROM-Version [rom_version]	Version des ROM des Blade.
Ersatzteilnummer der Hauptplatine [system_board_spare_part_number]	Ersatzteilnummer der Hauptplatine des Blade-Systems (proprietär von HPE).
Startmodus [boot_mode]	Startmodus des Blade.
Status des sicheren Starts [secure_boot_status]	Sicherer Platinenstatus des Blade.
Typ des Verwaltungsprozessors [management_processor_type]	Verwaltungsprozessortyp des Blade (iLO-Version).
Name des Verwaltungsprozessors [management_processor_name]	Hostname des Verwaltungsprozessors des Blade.
Firmware-Version des Verwaltungsprozessors [management_processor_firmware_version]	Version der Verwaltungsprozessor-Firmware des Blade.
IP-Adresse des Verwaltungsprozessors [amanagement_processor_ip_address]	IP-Adresse des Verwaltungsprozessors des Blade.
MAC-Adresse des Verwaltungsprozessors [management_processor_mac_address]	MAC-Adresse des Verwaltungsprozessors des Blade.
Version des Energieverwaltungs-Controllers [power_management_controller_version]	Version des Energieverwaltungs-Controllers des Blade.
iLO Federation-fähig [olo_federation_capable]	iLofederation-Fähigkeit aktiviert/deaktiviert.
Schachtnummer [bucht_nummer]	Positionsnummer des Gehäuses, in dem das Blade installiert ist.

Netzwerkadapter- und IP-Adressdatensätze für jeden im Gehäuse installierten Blade-Server:

Gesammelte Informationen (cmdb_ci_network_adapter)

Feld	Beschreibung
MAC-Adresse [mac_address]	Ethernet-Adresse des Blade-Verwaltungsprozessors (= MAC-Adresse der iLOnetwork-Schnittstelle).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gesammelte Informationen (cmdb_ci_network_adapter) (Fortsetzung)

Feld	Beschreibung
Name [name]	Hostname des Verwaltungsprozessors des Blade.
IP-Adresse [ip_address]	IP-Adresse des Verwaltungsprozessors des Blade.

Gesammelte Informationen (cmdb_ci_ip_address)

Feld	Beschreibung
Name [name]	IPv4-IP-Adresse des Verwaltungsprozessors (iLO) des Blade.
IP-Adresse [ip_address]	IP-Adresse des Verwaltungsprozessors des Blade.

Seriennummerndatensatz für das Gehäuse und jeden im Gehäuse installierten Blade-Server.

Gesammelte Informationen (cmdb_serial_number)

Feld	Beschreibung
Seriennummer [serial_number]	Gehäuse-/Blade-Seriennummer, extrahiert aus Onboard Administrator.
Seriennummerntyp [serial_number_type]	Typ der Seriennummer.
Gültig [valid]	Immer auf „true“ setzen.

Die Implementierung des HPE BladeSystem Enclosure CMDB-Modells umfasst drei neue CI-Klassen:

CMDB-Modell: (Neue CI-Klassen)

Feld	Beschreibung
Gehäuse [cmdb_ci_enclosure]	Allgemeine Klasse zur Darstellung einer beliebigen Gehäuseentität. Erweitert die HardwareCI-Klasse.
HPE BladeSystem-Gehäuse [cmdb_ci_hpe_blattsystem_enclosure]	CI-Klasse zur Darstellung der Gehäuse-Entität.
HPE BladeSystem-Blade [cmdb_ci_hpe_blattsystem_blatt]	CI-Klasse zur Darstellung der Blade-Serverentität.

CMDB-Modellbeziehungen und Referenzen

Das Muster „HPE BladeSystem Encloser“ erstellt die folgenden Beziehungen:

CI	Beziehung	CI
cmdb_ci_hpe_bladesystem_enclosure	Enthält::Enthalten in	cmdb_ci_hpe_bladesystem_blade

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_hpe_bladesystem_blade	Eigentümer von::Eigentum von	cmdb_ci_network_adapter
cmdb_ci_hpe_bladesystem_blade	Eigentümer von::Eigentum von	cmdb_ci_ip_address
cmdb_ci_server	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_hpe_bladesystem_blade
cmdb_ci_ip_address	Referenz auf	cmdb_ci_network_adapter
cmdb_serial_number	Referenz auf	cmdb_ci_hpe_bladesystem_enclosure
cmdb_serial_number	Referenz auf	cmdb_ci_hpe_bladesystem_blade

Zugehörige Informationen

SNMP-basierte Abfragen

IBM Cloud Platform-Erkennung

Die ServiceNow Discovery-Anwendung findet IBM Cloud Platform-Komponenten (Softlayer API v3 und v3.1 und Bluemix-API v2) mithilfe der IBM Cloud Platform-Muster. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Sie können die Muster auf Now Platform mithilfe der Versionen London Patch 7, Madrid Patch 2 oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

MID-Server

Verwenden Sie zur Cloud-Erkennung einen dedizierten MID-Server. Der MID-Server muss über 16 Kerne und 8 GB mit 4 GB Java Memory Model (JVM)-Speicherzuweisung verfügen.

Stellen Sie den dedizierten MID-Server mit Internetzugang bereit und stellen Sie die Verbindung her.

Berechtigungen

Die Cloud-Ressourcen befinden sich in einer IBM-Cloud. Erstellen Sie die IBM-Anmeldeinformationen für den Zugriff auf Ihr IBM-Konto.

1. Navigieren zu **Discovery** > **Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **IBM-Anmeldeinformationen**, und füllen Sie das Formular aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Anmeldeinformationen

Feld	Beschreibung
Name	Name der Anmeldeinformationen Ein Beispiel ist `ibm-cred`.
Reihenfolge	Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten verwendet. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist 100.
SoftLayer-API-Benutzer	Benutzername für die Softlayer-API. Verwenden Sie den Softlayer-API-Benutzernamen, der in der Softlayer-Konsole definiert ist.
SoftLayer-API-Schlüssel	Schlüssel für die Softlayer-API. Verwenden Sie den Softlayer-API-Schlüssel, der in der Softlayer-Konsole definiert ist.
Bluemix-API-Schlüssel	Schlüssel für die Bluemix-API. Verwenden Sie den in der IBM Cloud-Konsole definierten Bluemix-API-Schlüssel.

4. Klicken Sie auf **Absenden**.

IBM Cloud-Servicekonto erstellen

Verwenden Sie die im vorherigen Verfahren definierten Anmeldeinformationen, um das IBM Cloud-Servicekonto zu erstellen.

1. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Name der Anmeldeinformationen Ein Beispiel ist `ibm-snow`.
Konto-ID	IBM Konto-ID-Name. Geben Sie die IBM-Konto-ID ein.
Discovery Anmeldeinformationen	Discovery-Anmeldeinformationen, die Sie zuvor definiert haben
Datencenter-Typ	Datencenter-Typ. Beispiel: `IBM Datacenter [cmdb_ci_ibm_datacenter]`

4. Klicken Sie auf **Absenden**.

Discovery-Zeitplan ohne Server erstellen

Konfigurieren Sie eine Discovery ohne Server.

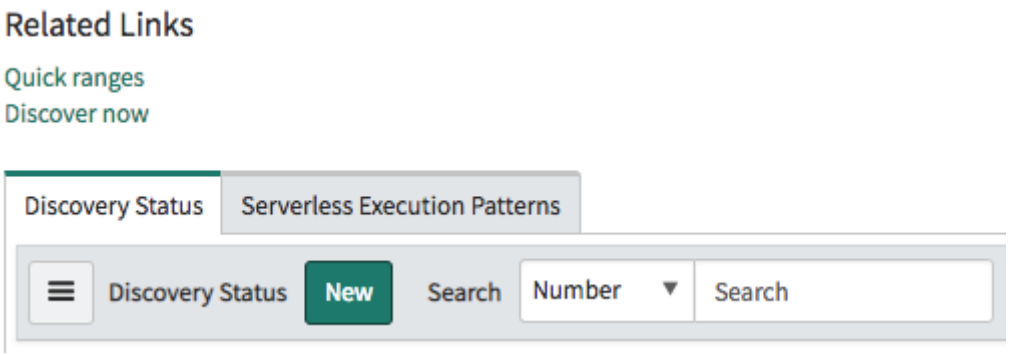
1. Navigieren Sie im Now Platformzu **Discovery** > **Discovery-Zeitpläne**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular aus:

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Name für diesen Discovery-Zeitplan. Beispiel: `Muster ohne Server`
Erkennen	Erkennungstyp. Wählen Sie **Ohne Server** aus.
MID-Server	Name des MID-Servers Beispiel: `Discovery_Server`
Aktiv	Option zur Aktivierung dieses Zeitplans für Discovery. Aktivieren Sie dieses Kontrollkästchen, um Discovery zu aktivieren.
Ausführen	Gibt an, wie häufig der Discovery-Zeitplan ausgeführt werden soll

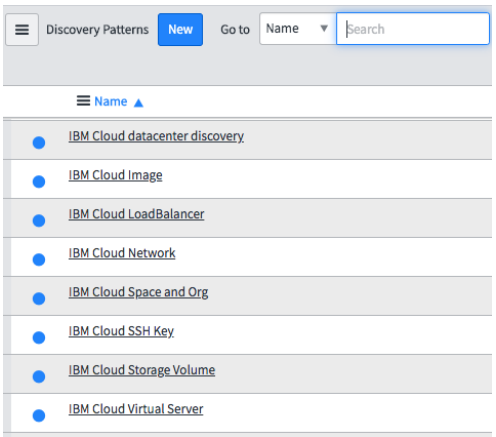
4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf die Registerkarte **Ausführungsmuster ohne Server**.
6. Klicken Sie auf **Neu**.
7. Füllen Sie die Felder im Formular aus:

Formular „Ausführungsmuster ohne Server“

Feld	Beschreibung
Name	Name dieses serverlosen Ausführungsmusters. Beispiel: `IBM1`.
Muster	Name des Musters, das Sie ausführen möchten.  Wenn Sie mehrere Muster ausführen möchten, erstellen Sie mehrere Datensätze.
Proxy-Host	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. Geben Sie **Global** an.
Aktiv	Option zur Aktivierung dieses Zeitplans für Discovery. Aktivieren Sie dieses Kontrollkästchen, um Discovery zu aktivieren.

8. Konfigurieren Sie die Parameter, die vom IBM Cloud Platform-Muster erforderlich sind, wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Startprogrammparameter für Discovery-Muster

Parameter	Beschreibung
cloud_cred_id	Die sys_id der IBM-Anmeldeinformationen, die in der Konfiguration angegeben ist.
cloud_account_id	Die IBM-Konto-ID
cloud_datacenter_type	cmdb_ci_ibm_datacenter

9. **Führen Sie eine Aktualisierung durch**.
10. Um Discovery zu starten, navigieren Sie zur Discovery-Definition ohne Server, und klicken auf **Discovery starten**.

IBM Flow – horizontale Erkennung

- Wenn Sie die Erkennung mithilfe eines Zeitplans ohne Server ausführen möchte, werden die ausgewählten IBM Cloud-Platform-Muster ausgeführt und IBM Cloud-Platform-Ressourcen erkannt.
- Wenn Sie die Erkennung mit einem Servicekonto durchführen möchten, wird ein vollständiger IBM Cloud Platform-Discovery-Zeitplan ausgeführt, der alle unterstützten IBM Cloud Platform-Ressourcen erkennt.

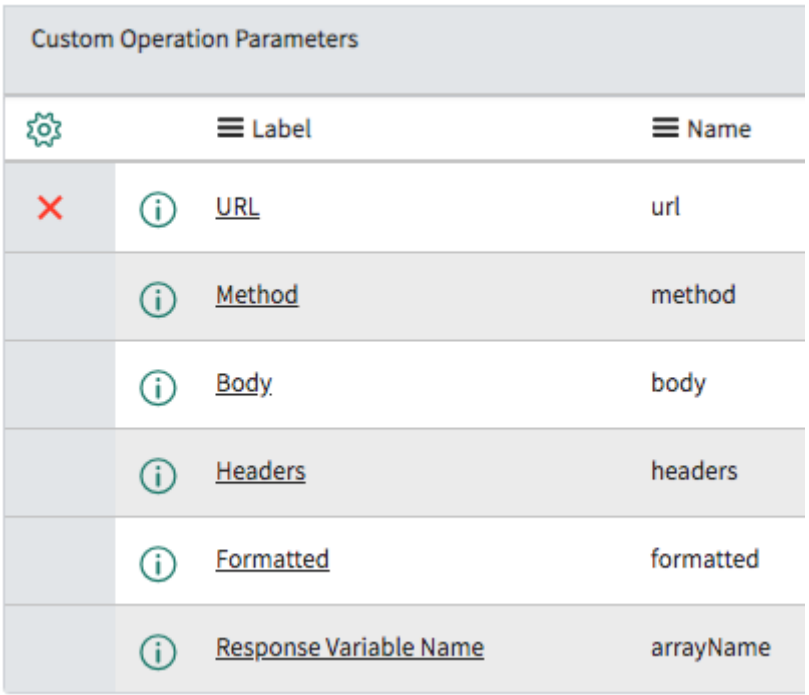
Benutzerdefinierter Cloud-Vorgang

Cloud-REST – Antwort zu Kontext hinzufügen

Vorgang für Cloud-REST-Abfragen, der umfangreiche Antworten und eine bessere Speichernutzung unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

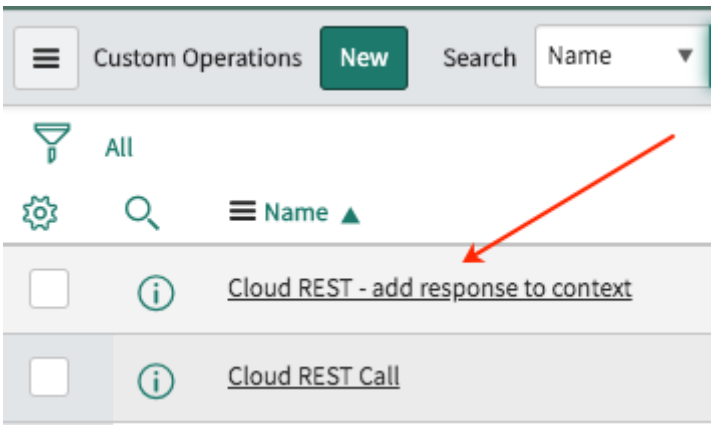
- Geben Sie alle Felder mit denselben Werten wie im benutzerdefinierten Vorgang „Cloud-REST-Abfrage“ an, mit Ausnahme der Tabelle für die Antwort, die im Feld **Name der Antwortvariablen** festgelegt ist.



- Legen Sie **Analyse definieren** als „Keine“ fest.

Methoden zum Abrufen von Daten für das IBM-Konto

1. Navigieren zu **Musterdesigner** > **Anwenderdefinierte Vorgänge**.



2. Klicken Sie auf **Cloud-REST – Antwort zu Kontext hinzufügen**.

Methode: Get-Aufruf

API-URLs, die zum Abrufen der Daten verwendet werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Lastenausgleichsmodul *https://api.softlayer.com/rest<api_version>/SoftLayer_Network_LBaaS_LoadBalancer/getAllObjects?objectMask=mask[listeners[defaultPool],members,healthMonitors]*
- Netzwerk *https://api.softlayer.com/rest/<API_VERSION>/SoftLayer_Account/getNetworkVlans?objectMask=mask[primaryRouter.datacenter,name,id,vlanNumber,networkSpace]*
- Netzwerk *https://api.softlayer.com/rest/<API_VERSION>/SoftLayer_Account/getSubnets?objectMask=mask[datacenter]*
- Netzwerk *https://api.softlayer.com/rest/<API_VERSION>/SoftLayer_Account/getSecurityGroups?objectMask=mask[rules]*
- Organisationen und Bereiche *https://api.<region>.bluemix.net/v2/organizations*
- *https://api.<region>.bluemix.net/v2/spaces*
- SSH-Schlüssel *https://api.softlayer.com/rest/v3/SoftLayer_Account/SoftLayer_Account/getSshKeys*
- Speicher *https://api.softlayer.com/rest/<api_version>/SoftLayer_Account/getNetworkStorage*
- Virtueller Server *https://api.softlayer.com/rest/v3.1/SoftLayer_Account/getSecurityGroups*
- *http://api.softlayer.com/rest/v3.1/SoftLayer_Account/getSecurityGroups?objectMask=mask[id,name,networkComponentBindings[networkComponentId,networkCompon*
- *https://api.softlayer.com/rest/v3.1/SoftLayer_Account/getVirtualGuests?objectMask=mask[hostname,domain,powerState,fullyQualifiedDomainName,notes,id,sta*

EVAL-Funktionen

Verwenden Sie die folgende EVAL-Funktion, um die Lastenausgleichsmodul-API-Antwort in ein vollständiges JSON-Format umzuwandeln. Die Standardantwort hat das Format „[<resource objects>]".

```
var cloud_lb_response = ${cloud_lb_response};
for (var i = 0; i < cloud_lb_response.size(); i++){
      cloud_lb_response.set(i, '{"result":[' +
 cloud_lb_response.get(i) + ']}');
}
CTX.setAttribute("cloud_lb_response", cloud_lb_response;
```

Verwenden Sie die folgende EVAL-Funktion, um die Netzwerk-API-Antwort in ein vollständiges JSON-Format umzuwandeln. Die Standardantwort hat das Format „[<resource objects>]".

```
var network_response = ${network_response};
for (var i = 0; i < network_response.size(); i++){
      network_response.set(i, '{"result":[' +
 network_response.get(i) + ']}');
}
CTX.setAttribute("network_response", network_response);
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die folgende EVAL-Funktion, um die IBM-Region aus der LB-Verfügbarkeitszone (Rechenzentrum) abzurufen. Dieselbe Funktion wird für andere Ressourcen im Muster verwendet.

```
var res = "";
res =
 IbmCloudDcToRegion.convertDctoRegion(${cloud_lb[].cloud_lb_az_
short_name});
```

Verwenden Sie die folgende EVAL-Funktion, um den erforderlichen Algorithmus im Muster auszuwählen.

```
var rtrn
var lb_algorithm = ${cloud_lb_pools[].lb_algorithm}.toString();
switch (lb_algorithm){
   case "ROUNDROBIN":
      lb_algorithm = "round-robin";
      break;
   case "WEIGHTED_RR":
      lb_algorithm = "round-robin";
      break;
   case "LEASTCONNECTION":
      lb_algorithm = "least-connections";
      break;
   default: break;
```

Verwenden Sie die folgende EVAL-Funktion, um die eindeutige Region für das Konto zu analysieren, das die Organisationen und die entsprechenden Bereiche hostet.

```
var tableWithoutDuplicates = '';
tableWithoutDuplicates =
 DuplicateRemover.removeDuplicates(${account_region},["region_n
ame"]);
CTX.setAttribute("account_region_unique",
 tableWithoutDuplicates);
```

Verwenden Sie die folgende EVAL-Funktion, um Informationen für alle Organisationen abzurufen, die dem IBM Cloud-Konto zugewiesen sind, bei dem die Iteration zum Abrufen der eindeutigen Region durchgeführt wird.

```
var cloudcall = new CloudRestAPIClient();
var resourceTable = ${account_region_unique[*].region_name};
var tableSize = resourceTable.size();
var tmp_response = new Packages.java.util.ArrayList();
var all_organizations_response = new
 Packages.java.util.ArrayList();
for (var i = 0; i < tableSize ; i++){
   if  (!resourceTable.get(i)) continue;
   var url =
 "https://api."+resourceTable.get(i)+".bluemix.net/v2/organizat
ions";
   tmp_response =
 cloudcall.arrayListExecute(${service_account}, null, url,
 null, 'GET', null, 'true', CTX);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
   for (var j = 0; j < tmp_response.size(); j++){
      all_organizations_response.add('{"result":[' +
 tmp_response.get(j) + ']}');
   }
}
CTX.setAttribute("all_organizations_response",
 all_organizations_response);
```

Verwenden Sie die folgende EVAL-Funktion, um Informationen für alle Bereiche abzurufen, die dem IBM Cloud-Konto zugewiesen sind, bei dem die Iteration zum Abrufen der eindeutigen Region durchgeführt wird.

```
var rtrn = '';
var cloudcall = new CloudRestAPIClient();
var resultList = new Packages.java.util.ArrayList();
var rest = '';
var resourceTable = ${account_region_unique[*].region_name};
var result = new Packages.java.util.ArrayList();
var all_organizations_response = ${all_organizations_response}
for (var i = 0; i < resourceTable.size() ; i++){
   var url =
 "https://api."+resourceTable.get(i)+".bluemix.net/v2/spaces";
   result = cloudcall.arrayListExecute(${service_account},
 null, url, null, 'GET', null, 'true', CTX);
   for (var z = 0; z < all_organizations_response.size(); z++){
      var jsonObj = JSON.parse(result.get(z));
      ms.log("length "+jsonObj.resources.length);
for(var j=0;j<jsonObj.resources.length;j++){
         var guid = jsonObj.resources[j].metadata.guid;
         var url = jsonObj.resources[j].metadata.url;
         var name = jsonObj.resources[j].entity.name;
         var organization_guid =
 jsonObj.resources[j].entity.organization_guid;
         var allow_ssh =
 jsonObj.resources[j].entity.allow_ssh ? "true" : "false";
         var row = new Packages.java.util.HashMap();
 Packages.com.snc.sw.log.DiscoLog.getLogger("IBM Cloud Space
 and Org").debug(">>>>>>>>>>>>>||||||||||>>>>>> region
 alias=" + resourceTable.get(i));
         Packages.com.snc.sw.log.DiscoLog.getLogger("IBM Cloud
 Space and Org").debug(">>>>>>>>>>>>>||||||||||>>>>>> region
 full name=" +
 IbmCloudDcToRegion.regionNamebyAlias(resourceTable.get(i)));
         row.put("region",
 IbmCloudDcToRegion.regionNamebyAlias(resourceTable.get(i)));
         row.put("space_guid",guid);
         row.put("space_url",url);
         row.put("space_name",name);
         row.put("space_organization_guid",organization_guid);
         row.put("space_allow_ssh",allow_ssh);
         row.put("rest", rest);
         resultList.add(row);
      }
   }
   CTX.setAttribute('spaces_table', resultList);
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die folgende EVAL-Funktion, um alle Bereiche nach eindeutiger Region zu filtern.

```
var space_region = ${spaces_table[].region};

Packages.com.snc.sw.log.DiscoLog.getLogger("IBM Cloud Space and
 Org").debug("filtering space according to LDC. space_region="
 + space_region);
var regions = ${cmdb_ci_ibm_datacenter[*].region};
Packages.com.snc.sw.log.DiscoLog.getLogger("IBM Cloud Space and
 Org").debug("input regions list=" + regions.toString());

var rtrn = "false";
if(regions.contains(space_region)) {
    rtrn = "true";
}
rtrn;
```

Verwenden Sie die folgende EVAL-Funktion, um alle Bereiche nach Speichererkennung zu filtern.

```
var storage_response = ${storage_response};
for (var i = 0; i < storage_response.size(); i++){
      storage_response.set(i, '{"result":[' +
 storage_response.get(i) + ']}');
}
CTX.setAttribute("storage_response", storage_response);
```

Verwenden Sie die folgende EVAL-Funktion, um die API-Antwort in das vollständige JSON-Format zu konvertieren, da die unberührte Antwort als „[<resource objects>]" formatiert ist.

```
var ssh_key = ${ssh_key_json};
for(var i = 0; i < ssh_key.size(); i++){
   ssh_key.set(i,'{"result\" : ' + ssh_key.get(i) + "}");
}
CTX.setAttribute("ssh_key_json", ssh_key);
```

Verwenden Sie die folgende EVAL-Funktion, um die Verfügbarkeitszone in die Speichervolume-Tabelle einzufügen.

```
var rtrn;
var resource_group = ${network_storage[].resource_name};
var regex = /.*-(\w{3}\d{2}).*/;
var az_name = regex.exec(resource_group);
if (az_name) {
   rtrn = az_name[1];
} else {
   rtrn;
}
```

Verwenden Sie die folgende EVAL-Funktion, um die Region in die Speichervolume-Tabelle einzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
var res = "";
res =
 IbmCloudDcToRegion.convertDctoRegion(${network_storage[].avail
ability_zone});
```

Verwenden Sie die folgende EVAL-Funktion, um die Größe der Speicher von Gigabyte in Byte zu konvertieren.

```
var rtrn = '';

var size = ${network_storage[].size};

rtrn = (parseInt(size) * 1073741824) + ‘’;
```

Verwenden Sie die folgende EVAL-Funktion, um die Größe der Speicher von Gigabyte in Byte zu konvertieren.

```
var cloudcall = new CloudRestAPIClient();
var resourceTable = ${network_storage[*].storage_object_id};
var tableSize = resourceTable.size();
var allResources = new Packages.java.util.ArrayList();
var response = new Packages.java.util.ArrayList();
for (var i = 0; i < tableSize ; i++){
   if  (!resourceTable.get(i)) continue;
   var url =
 "https://api.softlayer.com/rest/"+${api_version}+"/SoftLayer_N
etwork_Storage/"+resourceTable.get(i)+"/getObject?objectMask=ma
sk[snapshots]";
   // the commented out code is to call the "Cloud Rest Call"
 API

   allResources =
 cloudcall.arrayListExecute(${service_account}, null, url,
 null, 'GET', null, 'true', CTX);
   for (var j = 0; j < allResources.size(); j++){
      response.add('{"result":[' + allResources.get(j) + ']}');
   }
}
CTX.setAttribute("all_snapshots_response", response);
```

Verwenden Sie den folgenden EVAL-Abschluss, der die von der API empfangene JSON-Datei in ein Format umwandelt, mit dem der JSON-Parser arbeiten kann. Die Standard-JSON wird unter `$vm_json_array` gespeichert, die neue JSON unter `$vm_json`.

```
var vm_json = new Packages.java.util.ArrayList();
vm_json.addAll(${vm_json_array});

for (var i = 0 ; i < vm_json.size(); i++){
      vm_json.set(i, '{\"result\":[' + vm_json.get(i) + ']}');
}

CTX.setAttribute("vm_json", vm_json);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie den folgenden EVAL-Abschluss, der „on“ zurückgibt, wenn der Stromversorgungsstatus aktiv ist. Der Wert „off“ wird zurückgegeben, wenn der Stromversorgungsstatus deaktiviert ist.

```
var power = ${cmdb_ci_vm_instance[].state};
var rtrn = '';

if (power == 'Running'){
   rtrn = "on";
}
else {
   rtrn = "off"
}
```

Verwenden Sie den folgenden EVAL-Abschluss, der die Region des CI basierend auf dem angegebenen Verfügbarkeitszonennamen zurückgibt.

```
var az = ${cmdb_ci_vm_instance[].avail_zone};
var rtrn = '';
rtrn = IbmCloudDcToRegion.convertDctoRegion(az);
```

Verwenden Sie den folgenden EVAL-Abschluss, der eine HashMap aus HashSets erstellt und VMs mit ihren Netzwerkspeichern verbindet. Der folgende Schlüssel wird verwendet:

- P = Seite
- V = VM
- N = Netzwerkspeicher

```
var rtrn = '';
var vmJson = ${vm_json_array};
var VMtoStorageHashMap = new Packages.java.util.HashMap();

for (var p = 0 ; p < vmJson.size(); p++){
   var page = JSON.parse(vmJson.get(p));
   for (var now_V in page){
      if (page[v].allowedNetworkStorage.length > 0){
         var vm_id = page[v].id + '';
         var storageSet = new Packages.java.util.HashSet();
         for (var n in page[v].allowedNetworkStorage){
            storageSet.add(page[v].allowedNetworkStorage[n].id
 + '');
         }
         VMtoStorageHashMap.put(vm_id,storageSet);
      }
   }
}
CTX.setAttribute("VMStorageCache", VMtoStorageHashMap);
```

Verwenden Sie den folgenden EVAL-Abschluss, um doppelte Einträge aus Tabellen zu entfernen.

```
var tableWithoutDuplicates = '';
tableWithoutDuplicates =
 DuplicateRemover.removeDuplicates(${cmdb_ci_os_template},["obj
ect_id"]);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
CTX.setAttribute("cmdb_ci_os_template",
 tableWithoutDuplicates);
```

Verwenden Sie den folgenden EVAL-Abschluss, der eine Liste von VM-IDs erstellt, die sich auf die aktuelle Sicherheitsgruppen-ID beziehen.

```
var rtrn = '';
//get the Security Group ID of the current record in the table
 for comparison
var current_table_id = ${security_groups[].sec_group_id};
var current_table_id_string = current_table_id + '';

// get the list of instance's ID that will be then added to
 Security Group table
var needed_value_id_list =
 ${sec_group_network_components[*].vm_instance_id};
//get the list of Security Group IDs in the Network Component
 table, which will then be compared one by one to the current
 record of the security_groups table
var compare_id_list =
 ${sec_group_network_components[*].sec_group_id};

var beforeReturn = '';
var separator = '';
for (var i = 0; i <  compare_id_list.size(); i++)   {

   if   (current_table_id_string == compare_id_list.get(i)){

      beforeReturn += separator + needed_value_id_list.get(i);
      separator = ',';
   }
}
rtrn = beforeReturn;
```

Verwenden Sie den folgenden EVAL-Abschluss, der eine HashMap von HashSets zwischen Sicherheitsgruppen und den VMs erstellt, die für ihre Verwendung konfiguriert sind.

```
rtrn = '';
var secGroupTable = ${cmdb_ci_endpoint_comp_security};
var secToVMHashSet = new Packages.java.util.HashMap();

// this loop worst case O(N*M) M = security groups, N = VMs
for(var i=0; i<secGroupTable.size(); i++){
   var securityTableId = secGroupTable.get(i).get('object_id');
   var vmListStr = secGroupTable.get(i).get('instance_list');
   var vmList = vmListStr.split(",");

   var vmSet = new Packages.java.util.HashSet();
   for (var j in vmList){
      vmSet.add(vmList[j]);
   }

   secToVMHashSet.put(securityTableId,vmSet);
}
CTX.setAttribute("securityVMCache",  secToVMHashSet);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie den folgenden EVAL-Abschluss, der „true“ zurückgibt, wenn die aktuelle VM die aktuelle Sicherheitsgruppen-ID verwendet.

```
var rtrn = '';
var vm_id = ${cmdb_ci_vm_instance[].object_id};
var vmHashSet =
 ${securityVMCache}.get(${cmdb_ci_endpoint_comp_security[].obje
ct_id});
rtrn = vmHashSet.contains(vm_id);
```

Verwenden Sie den folgenden EVAL-Abschluss, der „true“ zurückgibt, wenn die aktuelle VM das aktuelle Speichervolume verwendet.

```
var rtrn = '';
var vm_id = ${cmdb_ci_vm_instance[].object_id};
var vol_id = ${cmdb_ci_endpoint_iscsi[].object_id};
var vmHashSet = ${VMStorageCache}.get(vm_id);
if (vmHashSet){
   rtrn = vmHashSet.contains(vol_id);
}
else {
   rtrn = 'false'
}
```

Verwenden Sie die folgende EVAL-Funktion, um die API-Antwort in das vollständige JSON-Format zu konvertieren, da die unberührte Antwort als „[<resource objects>]” formatiert ist.

```
var cloud_response = ${location_groups_response}
for (var i = 0; i < cloud_response.size(); i++){
    cloud_response.set(I, '{"result":[' + cloud_response.get(i)
 + ']}');
}
CTX.setAttribute("location_groups_response", cloud_response);
```

Analysiert die eindeutigen Standortgruppen in der Tabelle „location_groups_az“ in der Spalte „lg_id“ und erstellt eine neue Tabelle „location_groups_az_unique“, die das Ergebnis enthält

```
var tableWithoutDuplicates= '';
tableWithoutDuplicates =
 DuplicateRemover.removeDuplicates(${location_groups_az},["lg_i
d"]);
CTX.setAttribute("location_groups_az_unique",
 tableWithoutDuplicates);
```

Erstellt eine Liste von Verfügbarkeitszonen pro Standortgruppe, die in einer neuen Spalte in „llocation_groups_az_uniquetable“ gespeichert ist. Die Listendatensätze sind absichtlich durch Kommas unterteilt, sodass im nachfolgenden Schritt eindeutige Beziehungen hergestellt werden können.

```
var current_table_id= ${location_groups_az_unique[].lg_id};
var current_table_id_string = current_table_id+ '';
var needed_v alue_id_list = ${location_groups_az[*].lg_az_id};
var compare_id_list= ${location_groups_az[*].lg_id};
var beforeReturn= '';
var separator = ',';
for (var i= 0; i< compare_id_list.size(); i++)  {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    if (current_table_id_string == compare_id_list.get(i)){
    beforeReturn += separator + needed_v alue_id_list.get(i) +
 separator;
  }
}
rtrn = beforeReturn;
```

Cloudbezogenen CI-Beziehungen aktivieren

Um erkannte Komponenten in Serviceinstanzen aufzunehmen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von Service-Mappingverwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Konfiguration der Tag-basierten Discovery.

Von Discovery während der horizontalen Erkennung erfasste Daten

Daten werden mithilfe der folgenden Muster gesammelt:

- IBM Cloud-Lastenausgleichsmodul
- IBM Cloud-Standortgruppen
- IBM Cloud-Netzwerk
- IBM Cloud-Organisationen und -Bereiche
- IBM Cloud-Ressourcengruppen
- IBM Cloud-SSH-Schlüssel
- IBM Cloud-Speicher
- IBM Cloud virtueller Server

Daten, die für IBM-Komponenten erfasst wurden:

Vom IBM Cloud-Lastenausgleichsmodul erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_cloud_load_balancer	
name	Name des Lastenausgleichmoduls
object_id	Eindeutiger Bezeichner des Lastenausgleichmoduls
fqdn	Lastenausgleichsmoduladresse (Hostname)
dns_name	Domänenservername des Lastenausgleichmoduls
short_description	Beschreibung des Lastenausgleichmoduls, das Sie zur einfachen Identifizierung angeben
operational_status	Status des Lastenausgleichmoduls, einer der folgenden: • ONLINE • OFFLINE
location	Standort des Rechenzentrums
state	Bereitstellungsstatus des Lastenausgleichmoduls
Zugehöriges CI: cmdb_ci_lb_service	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
name	Name für Mustererstellung, bestehend aus: • Name des Lastenausgleichmoduls • Typ des Protokolls • Ressourcentyp-Listener
object_id	Eindeutiger Bezeichner des Lastenausgleichmoduls
port	Portnummer des Listeners
front_end_port	Protokollportnummer des Listeners
listener_protocol	Protokoll des Listeners Eines der folgenden Protokolle: • TCP • HTTP • HTTPS
operational_status	Bereitstellungsstatus des Listeners
Zugehöriges CI: cmdb_ci_lb_pool	
name	Name für Mustererstellung, bestehend aus: • Name des Lastenausgleichmoduls • Typ des Protokolls • port • Ressourcentyp „Pool“
object_id	Eindeutiger Bezeichner des Lastenausgleichmodulpools
port	Protokoll-Port des Back-End
pool_status	Pool-Bereitstellungsstatus des Lastenausgleichmoduls
load_balancing_method	Lastenausgleichsmethode. Einer der folgenden Algorithmen: • "ROUNDROBIN" • "WEIGHTED_RR" • "LEASTCONNECTION"
Zugehöriges CI: cmdb_ci_lb_pool_member	
name	Name für Mustererstellung, bestehend aus: • Name des Lastenausgleichmoduls • Typ des Protokolls • IP-Adresse des Poolmitglieds

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
object_id	Eindeutiger Bezeichner des Lastenausgleichmodul-Poolmitglieds, bestehend aus: • Mitglieds-ID • Listener-ID
ip_address	IP-Adresse des Lastenausgleichsmodulmitglieds
server_id	ID des Mitglieds in IBM Cloud
load_balancer	Name des zugehörigen Lastenausgleichmoduls
Zugehöriges CI: cmdb_ci_lb_health_service	
name	Name für Mustererstellung, bestehend aus: • Name des Lastenausgleichmoduls • Typ des Protokolls • Ressourcentyp: **Integritätsprüfung** • resource ID
object_id	Eindeutiger Bezeichner der Integritätsdienstprüfung
monitor_type	Integritätsprüfungstyp Eine der folgenden Möglichkeiten: • TCP • HTTP • HTTPS
timeout_sec	Zeit in Sekunden, die auf die Antworten der Integritätsprüfung gewartet wird
check_interval_sec	Intervall in Sekunden zum Ausführen der Integritätsprüfung

Von den IBM Cloud-Standortgruppen erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_cloud_location_group	
name	Ein beschreibender Name zur Identifizierung einer Standortgruppe
object_id	Die ID des Standortgruppen-Datensatzes
locationGroupType Name	Der Name des Standortgruppentyps
short_description	Ein kleiner Hinweis zu einer Standortgruppe, den Sie nach Belieben verwenden können.
locationGroup Type ID	Die ID des Standortgruppentyps

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vom IBM Cloud-Netzwerk erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_network	
name	VLAN-Nummer
object_id	Eindeutiger Netzwerk-Bezeichner
access_port_vlan	VLAN-Nummer
is_external	Netzwerkspeicherplatzwert. Der Wert ist entweder: • „true“, wenn network_space „PUBLIC“ ist • „false“, wenn network_space „PRIVATE“ ist
state	Status hat den Wert „verfügbar“.
Zugehöriges CI: cmdb_ci_cloud_subnet	
name	Name, bestehend aus: „network_identifier/cidr“
object_id	Eindeutiger Subnetz-Bezeichner
subnet_mask	Netzmaske des Subnetzes
gateway	Gateway-IP-Adresse
cidr	Methode für die Zuweisung von IP-Adressen und IP-Routing: „network_identifier/cidr“
Kategorie	Subnetztyp
broadcast_address	Broadcast-Adresse des Subnetzes
available_ip_count	Anzahl der IP-Adressen, die im Subnetz verfügbar sind
Zugehöriges CI: cmdb_ci_compute_security_group	
name	Name der Sicherheitsgruppe
object_id	Eindeutiger Bezeichner der Sicherheitsgruppe
short_description	Beschreibung der Sicherheitsgruppe, die Sie zur einfachen Identifizierung angeben
Zugehörige CI: cmdb_ci_compute_security_group_rule	
name	Feld mit demselben Wert wie das Feld „object_id“ der Sicherheitsgruppenregel
object_id	Eindeutiger Bezeichner der Sicherheitsgruppenregeln
erstellt	Datum, an dem das CI erstellt wurde
direction	Richtung der Informationen. Eine der folgenden Möglichkeiten: • eingehend • ausgehend
EtherType	EtherType Eine der folgenden Möglichkeiten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• IPv4 • IPv6
port_range_min	Der erste Port des Bereichs, für den die Regel gilt
port_range_max	Der letzte Port des Bereichs, für den die Regel gilt
protocol	Protokoll, auf das die Regel angewendet wird
remote_group_id	Sicherheitsgruppen-ID für die Quell-/Ziel-Sicherheitsgruppe. Dies bedeutet, dass diese Regel für alle IP-Adressen gilt, die in dieser Sicherheitsgruppe konfiguriert wurden.

Von IBM Cloud-Organisationen und -Bereichen erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_cloud_org	
name	Name der Cloud-Organisation
guid	Eindeutiger Bezeichner der Organisation
url	Eindeutige URL der Organisation
billing_enabled	Von der Organisation verwendete Abrechnungsmethode. Eine der folgenden: • Aktiviert / (TRUE) • Deaktiviert / (FALSE)
quota_definition_url	Ressourcen, die einer Organisation zur Verfügung stehen
spaces_url	Eindeutige URL des Speicherplatzes, der einer Organisation zugewiesen ist
operational_status	Betriebsstatus der Organisation
Zugehöriges CI: cmdb_ci_cloud_space	
name	Eindeutiger Name des Bereichs
object_id	Eindeutiger Bereichsbezeichner (GUID)
allow_ssh	Zugriff auf die Anwendung über SSH ist entweder erlaubt oder nicht erlaubt. Boolesch, einer der folgenden Werte: • WAHR • FALSCH
URL	URL des Bereichs aus der Metadatenbeschreibung

Von den IBM Cloud-Ressourcengruppen erkannte Ressourcen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Haupt-CI: cmdb_ci_resource_group	
name	Name der Ressourcengruppe
object_id	Eindeutiger Bezeichner der Ressourcengruppe
quota_id	Wert, der die der Ressourcengruppe zugeordnete Kontingent-ID angibt

Vom IBM Cloud-SSH-Schlüssel erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_cloud_key_pair	
name	Name zur Identifizierung eines SSH-Schlüssels
object_id	ID des SSH-Schlüsseldatensatzes
key	SSH-Schlüsseldatensatz
finger_print	Kurze Sequenz von Bytes, die zur Authentifizierung oder zum Nachschlagen eines längeren SSH-Schlüssels verwendet wird. Dieser Wert wird automatisch generiert, wenn der SSH-Schlüssel hinzugefügt oder bearbeitet wird. Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
created _date	Datum, an dem der SSH-Schlüssel hinzugefügt wurde. Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
modify_date	Datum, an dem der SSH-Schlüssel modifiziert wurde. Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
short_description	Beschreibung des SSH, die Sie zur einfachen Identifizierung angeben
Zugehöriges CI: cmdb_ci_ibm_datacenter	
name	Name des Rechenzentrums
region	Region, in der sich das Rechenzentrum befindet
discovery_status	Statusinformationen zum IBM-Rechenzentrum
sys_class_name	Klasse des Rechenzentrums
Zugehöriges CI: cmdb_ci_cloud_service_account	
name	Name des Cloud-Servicekontos
account_id	Konto-ID für dieses Cloud-Servicekonto
discovery_credentials	Anmeldeinformationen für dieses Cloud-Servicekonto
datacenter_url	URL zum Ausfüllen der logischen Rechenzentren (LDCs)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
datacenter_type	Typ des Rechenzentrums Beispiel: IBM Datacenter [cmdb_ci_ibm_datacenter]
datacenter_discovery_status	Status der letzten Ausführung von „Rechenzentren erkennen“

Vom IBM Cloud-Speicher erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_storage_volume	
name	Benutzername für folgende Aktionen: • Zugriff auf ein Nicht-EVault-Speichervolume • Registrierung des EVault-Server-Agent mit dem Vault-Sicherungssystem
object_id	Eindeutiger Bezeichner für Speicherkonto
size	Kapazität des Speicherkontos, gemessen in Gigabyte
size_bytes	Kapazität des Speicherkontos, gemessen in Byte
Bezeichnung	Name der Speichernetzwerkressource
storage_type	Beschreibung des Speichertyps. Beispiel: NAS
fqdn	IP-Adresse einer Speicherressource oder vollqualifizierter Domänenname
Gerät	Eindeutige Identifikationsnummer des Geräts, das dem Speichervolume zugeordnet ist
Zugehöriges CI: cmdb_ci_storage_vol_snapshot	
name	Name der Speicher-Netzwerkressource
object_id	Eindeutiger Speicher-Bezeichner
Kapazität	Kapazität des Snapshot-Volume in Gigabyte
fqdn	IP-Adresse einer Speicherressource oder vollqualifizierter Domänenname
location	Eindeutige Verfügbarkeitszone, in der sich das Speichervolume befindet
Zugehöriges CI: cmdb_ci_ibm_datacenter	
name	Name des Rechenzentrums
region	Region, in der sich das Rechenzentrum befindet
discovery_status	Statusinformationen zum IBM-Rechenzentrum
sys_class_name	Klasse des Rechenzentrums
Zugehöriges CI: cmdb_ci_cloud_service_account	
name	Name des Cloud-Servicekontos

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
account_id	Konto-ID für dieses Cloud-Servicekonto
discovery_credentials	Anmeldeinformationen für dieses Cloud-Servicekonto
datacenter_url	URL zum Ausfüllen der LDCs
datacenter_type	Typ des Rechenzentrums Beispiel: IBM Datacenter [cmdb_ci_ibm_datacenter]
datacenter_discovery_status	Status der letzten Ausführung von „Rechenzentren erkennen“
Zugehöriges CI: cmdb_ci_availability_zone	
name	Name der Verfügbarkeitszone (AZ)
object_id	Eindeutiger Bezeichner für diese Ressource
short_description	Verfügbarkeitszonenbeschreibung, die Sie angeben

Vom IBM Cloud virtuellen Server erkannte Ressourcen

Feld	Beschreibung
Haupt-CI: cmdb_ci_vm_instance	
name	Name der VM
object_id	Eindeutiger Bezeichner der VM
dns_domain	Name des VM-Domänenservers
fqdn	VM-IP-Adresse
short_description	Beschreibung in einer Notiz, die der VM auf der IBM-Konsole angehängt wird
CPUs	Anzahl der CPU-Kerne, die dieser VM zugewiesen sind
memory	Speichergröße, die dieser VM zugewiesen ist
disks	Anzahl der Datenträger, die dieser VM zugewiesen sind
state	Der Ausführungsstatus der VM. • On – Wird von der API als „ausgeführt“ zurückgegeben • Off – Wird von der API als „angehalten“ zurückgegeben
placement_group_id	Platzierungsgruppen-ID
nics	Anzahl der NICs
Zugehöriges CI: cmdb_ci_nic	
name	Name, bestehend aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Name des Lastenausgleichmoduls • Port
object_id	Eindeutiger Bezeichner der NIC
ip_address	IP, die auf der NIC konfiguriert ist
mac_address	NIC-MAC-Details
netmask	Maske zur Unterteilung der IP-Adresse in Subnetze und zur Angabe der verfügbaren Hosts im Netzwerk
Status	Status der NIC
Zugehörige CI: cmdb_ci_endpoint_vnic	
name	Name für den VNIC-Endpunkt
object_id	Eindeutiger Bezeichner des VNIC-Endpunkts
host	Bezeichner des Hosts
Zugehöriges CI: cmdb_ci_storage_volume	
name	Benutzername für folgende Aktionen: • Zugriff auf ein Nicht-EVault-Speichervolume • Registrierung des EVault-Server-Agent mit dem Vault-Sicherungssystem
object_id	Eindeutiger Bezeichner für Speicherkonto
size	Kapazität des Speicherkontos, gemessen in Gigabyte
size_bytes	Kapazität des Speicherkontos, gemessen in Byte
Bezeichnung	Name der Speichernetzwerkressource
storage_type	Beschreibung des Speichertyps. Beispiel: NAS
fqdn	IP-Adresse einer Speicherressource oder vollqualifizierter Domänenname
Gerät	Eindeutige Identifikationsnummer des Gastes, der dem Speichervolume zugeordnet ist
Zugehöriges CI: cmdb_ci_endpoint_nfs	
name	Name für den NFS-Endpunkt
host	Bezeichner des Hosts
protocol	Angewendetes Protokoll
Typ	NFS-Endpunkttyp
erstellt	Datum, an dem der NFS-Endpunkt erstellt wurde
aktualisiert	Datum, an dem der NFS-Endpunkt aktualisiert wurde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
discovery_source	Quelle der Erkennung. Beispiel: ServiceWatch
host_name	Hostname des NFS-Endpunkts
Zugehöriges CI: cmdb_ci_endpoint_iscsi	
host	Host-Bezeichner für den ISCSI-Endpunkt
port	Port, um festzulegen, wie GCP-ISCSI Kontakt zu den VMs herstellt
protocol	Angewendetes Protokoll
Typ	ISCSI-Endpunkttyp
erstellt	Datum, an dem der ISCSI-Endpunkt erstellt wurde
aktualisiert	Datum, an dem der ISCSI-Endpunkt aktualisiert wurde
discovery_source	Quelle der Erkennung. Beispiel: ImportSet
host_name	Hostname des ISCSI-Endpunkts
Zugehörige CI: cmdb_ci_endpoint_block	
name	Name für den Block-Endpunkt
object_id	Eindeutiger Bezeichner des Block-Endpunkts
host	Bezeichner des Hosts
Zugehöriges CI: cmdb_ci_os_template	
name	Name des Image. Zum Beispiel: CentOS 7.0-64 Minimal for VSI
object_id	Eindeutiger Bezeichner des Images
guest_os	Vom Image verwendetes Betriebssystem Beispiel: Linux
root_device_type	Typ des von Root verwendeten Geräts
image_source	Image-Quelle
image_type	Image-Typ
infuse_key	Schlüssel, der zur Eingabe des Image verwendet wird
update_host_name	Update-Hostname für das Image
Anmeldeinformationen	Anmeldeinformationen für das Image
Version	Version des Betriebssystems. Beispiel: „7.0-64 Minimal for VSI“
Zugehöriges CI: cmdb_ci_cloud_key_pair	
name	Name zur Identifizierung eines Schlüssels (Schlüsselbezeichnung)
object_id	ID des Schlüsseldatensatzes
key	Schlüsseldatensatz

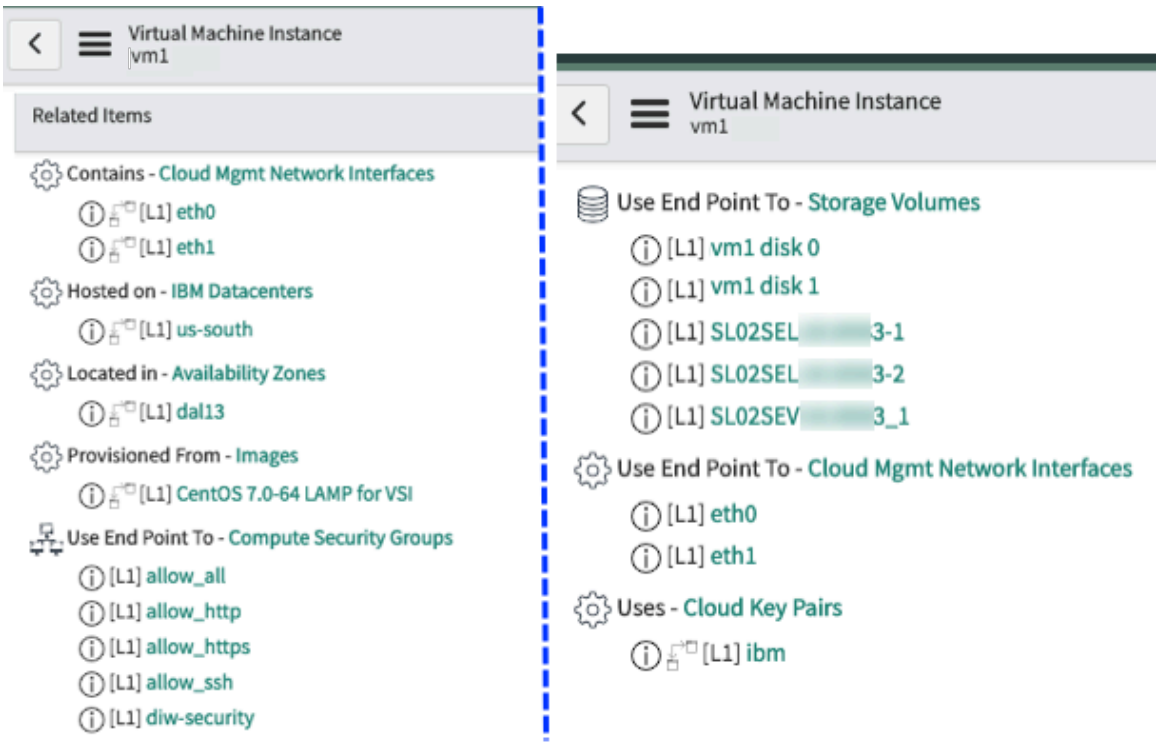
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
finger_print	Kurze Sequenz von Bytes, die zum Authentifizieren oder Nachschlagen eines Schlüssels verwendet wird. Dieser Wert wird automatisch generiert, wenn der Schlüssel hinzugefügt oder bearbeitet wird. Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
created _date	Datum, an dem der Schlüssel hinzugefügt wurde Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
modify_date	Datum, an dem der Schlüssel modifiziert wurde Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
short_description	Beschreibung, die Sie zur einfachen Identifizierung angeben
Zugehöriges CI: cmdb_ci_compute_security_group	
name	Name der Sicherheitsgruppe
object_id	Eindeutiger Bezeichner der Sicherheitsgruppe
short_description	Beschreibung der Sicherheitsgruppe, die Sie zur einfachen Identifizierung angeben
Zugehöriges CI: cmdb_ci_endpoint_comp_security	
host	Host-Bezeichner des Sicherheitsendpunkts der Berechnung
port	Eindeutiger Host-Bezeichner des Sicherheitsendpunkts der Berechnung
protocol	Angewendetes Protokoll
Typ	Typ des Sicherheitsendpunkts der Berechnung
erstellt	Datum, an dem der Sicherheitsendpunkt der Berechnung hinzugefügt wurde Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
aktualisiert	Datum, an dem der Sicherheitsendpunkt der Berechnung geändert wurde Schreibgeschützt. Vorgenommene Änderungen werden ignoriert.
discovery_source	Quelle der Erkennung. Beispiel: Manuelle Eingabe
host_name	Host-Name des Sicherheitsendpunkts der Berechnung
Zugehöriges CI: cmdb_ci_ibm_datacenter	
name	Name des Rechenzentrums
region	Region, in der sich das Rechenzentrum befindet
discovery_status	Statusinformationen zum IBM-Rechenzentrum
sys_class_name	Klasse des Rechenzentrums

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zugehöriges CI: cmdb_ci_availability_zone	
name	Name der Verfügbarkeitszone (AZ)
object_id	Eindeutiger Bezeichner für diese Ressource
short_description	Verfügbarkeitszonenbeschreibung, die Sie angeben
Zugehöriges CI: cmdb_ci_cloud_service_account	
name	Name des Cloud-Servicekontos
account_id	Konto-ID für dieses Cloud-Servicekonto
discovery_credentials	Anmeldeinformationen für dieses Cloud-Servicekonto
datacenter_url	URL zum Ausfüllen der LDCs
datacenter_type	Typ des Rechenzentrums Beispiel: IBM Datacenter [cmdb_ci_ibm_datacenter]
datacenter_discovery_status	Status der letzten Ausführung von „Rechenzentren erkennen“

IBM Cloud virtueller Server – Ansicht „Zugehörige Elemente“



CI-Beziehungen

Diese Beziehungen sollen die IBM Cloud Plattform-Erkennung unterstützen.

Beziehungen für vom IBM Cloud-Lastenausgleichsmodul erkannte Ressourcen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
Zugehöriges CI: cmdb_ci_cloud_load_balancer		
cmdb_ci_cloud_load_balancer	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_cloud_load_balancer	Enthält::Enthalten in	cmdb_ci_lb_health_service
Zugehöriges CI: cmdb_ci_availability_zone		
cmdb_ci_availability_zone	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_lb_service
Zugehöriges CI: cmdb_ci_lb_service		
cmdb_ci_lb_service	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_service	Enthält::Enthalten in	cmdb_ci_lb_pool
Zugehöriges CI: cmdb_ci_lb_pool		
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_pool	Eigentümer von::Eigentum von	cmdb_ci_lb_pool_member
Zugehöriges CI: cmdb_ci_lb_health_service		
cmdb_ci_lb_health_service	Enthält::Enthalten in	cmdb_ci_cloud_load_balancer

Beziehungen für von den IBM Cloud-Standortgruppen erkannte Ressourcen

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
Zugehörige CI: cmdb_ci_cloud_location_group		
cmdb_ci_cloud_location_group	Gehostet auf::Hostet	cmdb_ci_cloud_service_account

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_cloud_location_group	Enthält::Enthalten in	cmdb_ci_availability_zone

Beziehungen für vom IBM Cloud-Netzwerk erkannte Ressourcen

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
Zugehöriges CI: cmdb_ci_network		
cmdb_ci_network	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_network	Enthält::Enthalten in	cmdb_ci_cloud_subnet
Zugehöriges CI: cmdb_ci_compute_security_group		
cmdb_ci_compute_security_group	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_compute_security_group	Enthält::Enthalten in	cmdb_ci_compute_security_group_rule

Beziehungen für von den IBM Cloud-Ressourcegruppen erkannte Ressourcen

CI	Beziehung	CI
Zugehörige CI: cmdb_ci_resource_group		
cmdb_ci_resource_group	Gehostet auf::Hostet	cmdb_ci_cloud_service_account

Beziehungen für vom IBM Cloud-SSH-Schlüssel erkannte Ressourcen

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
Zugehöriges CI: cmdb_ci_cloud_key_pair		
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_cloud_service_account

Beziehungen für vom IBM Cloud-Speicher erkannte Ressourcen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
Zugehöriges CI: cmdb_ci_storage_volume		
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_volume	Bereitgestellt::Bereitgestellt von	cmdb_ci_storage_vol_snapshot
Zugehöriges CI: cmdb_ci_storage_vol_snapshot		
cmdb_ci_storage_vol_snapshot	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_vol_snapshot	Positioniert in Zone::Zone beinhaltet	cmdb_ci_availability_zone
Zugehöriges CI: cmdb_ci_availability_zone		
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_storage_volume

Beziehungen für vom IBM Cloud virtuellen Server erkannte Ressourcen

CI	Beziehung	CI
Zugehöriges CI: cmdb_ci_ibm_datacenter		
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_accoun
cmdb_ci_ibm_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
cmdb_ci_ibm_datacenter	Gehostet auf::Hostet	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_vm_instance		
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_vm_instance	Standort::Häuser	cmdb_ci_availability_zone
cmdb_ci_vm_instance	Verwendet::Verwendet von	cmdb_ci_cloud_key_pair
cmdb_ci_vm_instance	Enthält::Enthalten in	cmdb_ci_nic
cmdb_ci_vm_instance	endpoint	cmdb_ci_nic
Zugehöriges CI: cmdb_ci_availability_zone		
cmdb_ci_availability_zone	Gehostet auf::Hostet	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_nic		
cmdb_ci_nic	Gehostet auf::Hostet	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_os_template		
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_cloud_service_accoun
cmdb_ci_os_template	Bereitgestellt::Bereitgestellt von	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_compute_security_group		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_compute_security_group	Gehostet auf::Hostet	cmdb_ci_cloud_service_accoun
cmdb_ci_compute_security_group	Implementieren::Implementiert von	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_storage_volume		
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_ibm_datacenter
cmdb_ci_storage_volume	Implementieren::Implementiert von	cmdb_ci_vm_instance
Zugehöriges CI: cmdb_ci_cloud_key_pair		
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_cloud_service_accoun

Für die VM-Instanz erkannte Beziehungen

CI	Beziehung	CI
Server [cmdb_ci_server]	Virtualisiert von::Virtualisiert	VM-Instanz [cmdb_ci_instance]

Daten, die von Service-Mapping während der tagbasierten Erkennung erfasst wurden

Service-Mapping verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout*	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Ursache	Lösung
	gesteuerte Zeitbegrenzung überschritten wird.	und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter *sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

Erkennung von IBM DB2-Datenbanken unter Linux

ServiceNow Discovery verwendet das Erkennungsmuster „Db2 on Linux“, um IBM DB2-Instanzen auf Linux-Servern zu finden.

Discovery verwendet dieses Muster zum Ausführen einer horizontalen Erkennung. Sie können das Muster auf der Now Platform mit Release Istanbul oder höher verwenden.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Vor Release Yokohama wurde DB2 unter Linux durch eine Probe erkannt. Ab Release Yokohama wird das Muster automatisch durch die Klassifizierung mit diesen DB2-Bezeichnern ausgelöst: tcp_port, name, installed_dir.

Voraussetzungen

Konfigurieren Sie SSH-Anmeldeinformationen für den Linux-Server

Stellen Sie außerdem sicher, dass der Benutzer über die Berechtigungen zum Ausführen der folgenden Befehle verfügt:

Identifikation für die DB2-UDB-Einstiegspunkttypen

```
". /" + $process.environmentVariables.HOME.value + "/sqllib/
db2profile; " + $process.environmentVariables.HOME.value +
"/sqllib/bin/db2level"

"source " + $installed_dir + "db2profile"

"db2 list database directory | grep |"Database name|" | grep -i
|"" + $entry_point.instance + "|" | head -1"

"db2level | grep |"DB2 v|""
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identifikation für die Db2-UDB-Einstiegspunkttypen – NONE

```
"cat " + $installed_dir + "/db2dump/db2diag.log | grep
|"INSTANCE:|" | grep " + $entry_point.instance + " | head -1"

"db2level | grep |"DB2 v|""
```

Identifikation für DB2 unter z/OS

```
"netstat -a | grep " + $entry_point.port

"ls -d /*/* |grep " + $id
```

Von Discovery während der horizontalen Erkennung erfasste Daten

In **Identifikation für DB2 UDB-Einstiegspunkttypen** und **Identifikation für DB2 UDB-Einstiegspunkttypen – NONE** werden die folgenden Tabellen und Felder erfasst:

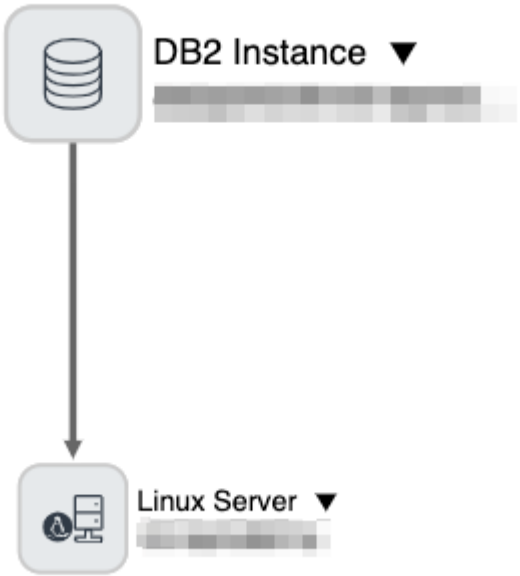
Tabelle und Feld	Beschreibung
name	Name der DB2-Instanz
tcp_port	TCP-Port
installed_dir	Installationsverzeichnis
Version	DB2-Version

In „Identifikation für DB2 unter z/OS“ werden die folgenden Tabellen und Felder erfasst:

Tabelle und Feld	Beschreibung
name	Name der DB2-Instanz
tcp_port	TCP-Port
installed_dir	Installationsverzeichnis

Die Dependency Views-Zuordnung zeigt alle erkannten IBM DB2-Instanzen in Ihrer Organisation und die Beziehungen zwischen ihnen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CI-Beziehungen

Das Muster „IBM Db2 on Linux“ erstellt keine CI-Beziehungen.

Erkennung von IBM DB2-Datenbanken unter Windows

ServiceNow Discovery verwendet das Erkennungsmuster „Db2 on Windows“, um IBM DB2-Instanzen auf Windows-Servern zu finden.

Discovery verwendet dieses Muster zum Ausführen einer horizontalen Erkennung. Sie können das Muster auf der Now Platform mit Release Istanbul oder höher verwenden.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Vor Release Yokohama wurde DB2 unter Windows durch eine Probe erkannt. Ab Release Yokohama wird das Muster automatisch durch die Klassifizierung mit diesen DB2-Bezeichnern ausgelöst: tcp_port, name, installed_dir.

Voraussetzungen

Stellen Sie sicher, dass der Benutzer über die Berechtigungen zum Ausführen der folgenden Befehle verfügt:

- *"|"" + $installed_dir + "|bin|db2cmd|" /c /w /i db2 list database directory"*
- *"|"" + $installed_dir + "|bin|db2cmd|" /c /w /i db2 list database directory | findstr |"Database name|" | findstr /i " + $entry_point.instance*
- *"|"" + $installed_dir + "|bin|db2level|""*

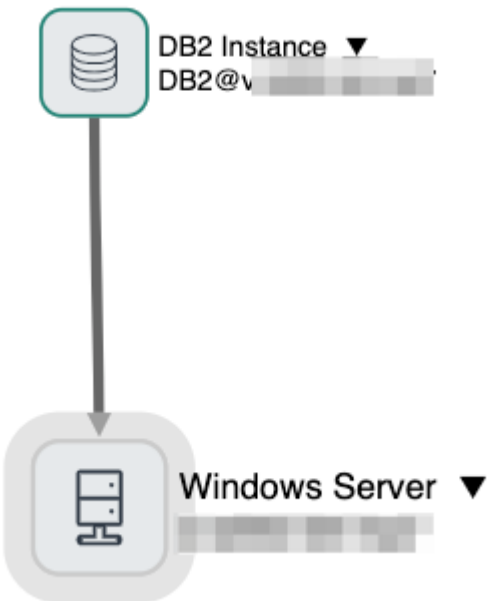
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
name	Name der DB2-Instanz
tcp_port	TCP-Port
installed_dir	Installationsverzeichnis
Version	DB2-Version
db_name	Name der Datenbank.
pid	Prozess-ID der DB2-Instanz

Die Dependency Views-Zuordnung zeigt alle erkannten IBM DB2-Instanzen in Ihrer Organisation und die Beziehungen zwischen ihnen an.



CI-Beziehungen

Das Muster „IBM Db2 on Windows“ erstellt keine CI-Beziehungen.

IBM Informix Dynamic Server-Erkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping können den Informix Dynamic Server finden und zuordnen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Anwender

Gewähren Sie dem Benutzer die Berechtigungen zum Ausführen der folgenden Befehle ohne erhöhte Rechte:

- `$install_directory/bin/onstat -g dis`

  Dieser Befehl ruft den Status und die Konfiguration des Informix Dynamic Servers ab.

- `$install_directory/bin/dbaccess sysmaster`

  Dieser Befehl führt eine SQL-Abfrage für das Master-Schema aus.

Derselbe Benutzer muss Leseberechtigung für die folgenden Verzeichnisse haben:

- install_directory + "/etc/sqlhosts

  Zugriff auf dieses Verzeichnis ist erforderlich, um Informationen über die Port-, Host- und Servicedefinition des Informix Dynamic Servers zu erhalten.

- /etc/services

  Zugriff auf dieses Verzeichnis ist erforderlich, um Informationen über die Host-Servicedefinition zu erhalten.

Berechtigungen

Konfigurieren Sie SSH-Anmeldeinformationen im Modul für Anmeldeinformationen der ServiceNow-Plattform für den Zugriff auf den Server, auf dem der Informix Dynamic Server gehostet wird.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Informix-Instanz [cmdb_ci_db_informix_instance]	Die Informix-Instanzattribute
tcp_port	
running_process	
Version	
install_directory	
config_file	
name	
Informix-Katalog [cmdb_ci_db_informix_catalog]	Die in der Informix-Instanz enthaltene Datenbank
Datenbank	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

CI	Beziehung/Referenz	CI
Informix-Instanz [cmdb_ci_db_informix_instance]	Enthält::Enthalten in	Informix-Katalog [cmdb_ci_db_informix_catalog]

Von oben nach unten

Während der Erkennung von oben nach unten erkennt Service-Mapping Verbindungen zwischen der Informix-Instanz und den Informix-Katalogen, die die Instanz enthält, und zeigt sie als Aufnahme in die Anwendungsservicezuordnung an.

Erkennung von IBM PowerHA Cluster (HACMP)

Die Anwendung ServiceNow Discovery verwendet das Muster IBM PowerHA Cluster (HACMP), um die Hochverfügbarkeits-Cluster IBM PowerHA SystemMirror for AIX (früher HACMP) auf den AIX-Systemplattformen UNIX und Linux for IBM zu suchen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery verwendet dieses Muster zum Ausführen einer horizontalen Erkennung.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Store-AppMuster für Discovery und Service-Mapping : Stellen Sie die neueste Version aus ServiceNow® Storebereit.
- Unter **CI-Klassifizierung** > **UNIX** > **AIX** Stellen Sie in der zugehörigen Liste **„Auslösertests“** sicher, dass dieses Muster in der Liste enthalten ist, als eine Erkundung, die nach dem Betriebssystemmuster, AIX dem Servermusterausgeführt wird. Weitere Informationen zur Erkennung des Servers AIX finden Sie unter Erkennung von AIX-Servern
- Stellen Sie sicher, dass MID-Server Zugriff auf den Zielhost hat und alle im Muster implementierten Befehle ausführen kann.
- Stellen Sie sicher, dass das Muster so konfiguriert ist, dass es für die IP-Adresse oder den Hostnamen des Servers ausgeführt wird.
- Konfigurieren Sie einen UNIX-Benutzer mit Berechtigungen zum Ausführen aller in der offiziellen IBM-Dokumentation definierten Befehle und den folgenden Befehlen unter AIX:

Befehl	Beschreibung
`lssrc -s clstrmgrES`	Überprüft, dass der clstrmgrES-Prozess ausgeführt wird
`lslpp -l cluster.license`	Ruft die Lizenz- und Versionsdaten des Clusters ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
`lslpp -l cluster.license | awk '{$1=$2=$3=\"\"; print $0}' |sed -e 's/^[[:space:]]*//'`	Ruft die Softwarebezeichnungs-Versionsdaten des Clusters ab
`/usr/es/sbin/cluster/utilities/clRGinfo -a | awk „{print $1,$2}“ | grep -E -v 'verweigert|Fehler'`	Rufen Sie den Namen und Typ der Ressourcengruppe ab
`/usr/es/sbin/cluster/utilities/clRGinfo -s | grep -E -v 'verweigert|Fehler'`	Rufen Sie weitere Informationen zu Ressourcengruppen ab
`/usr/es/sbin/cluster/utilities/clfindres -s | grep -E -v 'verweigert|Fehler'`	Alternativer Befehl zum Abrufen weiterer Informationen zu Ressourcengruppen
`/usr/es/sbin/cluster/utilities/clshowres | grep -E 'Ressourcengruppenname|Volume' | grep -E -v 'Gleichzeitig|Automatisch|Fehler|Verweigert' | sed 's/Volumegruppen/Namen der Volumegruppen/' | awk '{print substr($0, index($0,$4))}' | sed 'N;s/\n/ /'`	Rufen Sie Volumegruppen ab, die Ressourcengruppen zugeordnet sind
`/usr/es/sbin/cluster/clstat -o | grep 'Ressourcengruppe' | grep -E -v 'Fehler|Verweigert' | awk '{print $3, $5, $6}'`	Status der Ressourcengruppe(n) abrufen
`/usr/es/sbin/cluster/utilities/cltopinfo -c`	Rufen Sie den Clusternamen ab
`/usr/es/sbin/cluster/utilities/cllscf`	Alternativer Befehl zum Abrufen des Clusternamens
`lssrc -ls clstrmgrES`	Rufen Sie den aktuellen Clusterstatus ab
`/usr/es/sbin/cluster/clstat -o |awk '{$1=$2=\"\"; print $0}' |sed -e 's/^[[:space:]]*//'`	Rufen Sie die Cluster-ID ab
`/usr/es/sbin/cluster/utilities/cllsclstr | grep -E -v 'Fehler| Verweigert' | awk „{print $1}“`	Alternativer Befehl zum Abrufen der Cluster-ID
`/usr/bin/odmget HACMP-Cluster| grep -w id | grep -E -v 'Fehler| Abgelehnt'`	Alternativer Befehl zum Abrufen der Cluster-ID
`/usr/es/sbin/cluster/utilities/cltopinfo -n | grep -E -v 'Fehler| Abgelehnt'`	Name(n) des Clusterknotens abrufen
`/usr/es/sbin/cluster/utilities/cllsnode | grep -E -v 'Fehler| Abgelehnt'`	Alternativer Befehl zum Abrufen der Namen von Cluster-Knoten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Beschreibung
`/usr/es/sbin/cluster/clstat -o | grep -i 'Knoten:' | awk „{print $2, $4}"`	Status der Cluster-Knoten abrufen
`lscluster -m | grep -E 'Knotenname| Status des Knotens' | grep -E -v 'FEHLER|lscluster' | awk '{print $2, $3, $4}' | sed 'N;s/\n/ /'`	Alternativer Befehl zum Abrufen der Status von Clusterknoten
`/usr/es/sbin/cluster/utilities/ cllsif | grep -E -v 'Fehler| Verweigert' | awk '{print $1, $2, $6, $7}'`	Ruft Informationen zu Netzwerkschnittstellen ab
`lspv | grep -E -v 'Fehler|Abgelehnt'`	Ruft Informationen zu physischen Volumes ab
`lsvg | grep -E -v 'Fehler|Abgelehnt'`	Ruft Informationen zu Volumegruppen ab
`lsvg -o | grep -E -v 'Fehler| Abgelehnt'`	Rufen Sie Informationen zu den aktiven Volumegruppen ab
`/usr/es/sbin/cluster/utilities/ clshowres | grep 'Concurrent Volume Group' | awk '{$1=$2=$3=\"\"; print $0}' |sed -e 's/^[[:space:]]*//'`	Rufen Sie Informationen zu den gleichzeitigen Volumegruppen ab
`hostname`	Ruft den aktuellen Knotenhostnamen ab
`nslookup-Hostname`	Konvertieren Sie den Hostnamen in einen FQDN

Von Discovery während der horizontalen Erkennung erfasste Daten

Das Muster erkennt Daten, die Ihnen helfen, die Clustertopologie Ihrer Organisation und die Beziehungen zwischen ihren Komponenten zu verstehen. Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group]	
name	Der Name der Ressourcengruppe, die im Clusterkontext konfiguriert ist.
Server	Der Name des PowerHA/HACMP-Clusters.
resource_group_status	Der Status der Ressourcengruppe im Clusterkontext. Beispiel: Online
resource_group_type	Typ der Ressourcengruppe. Beispiele: Gleichzeitig, nicht gleichzeitig
Cluster	Der Name des PowerHA/HACMP-Clusters, zu dem die Ressourcengruppe gehört.
UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	
name	Der Name der Volumegruppe im Clusterkontext.
resource_type	Der Ressourcentyp (Volumegruppe)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

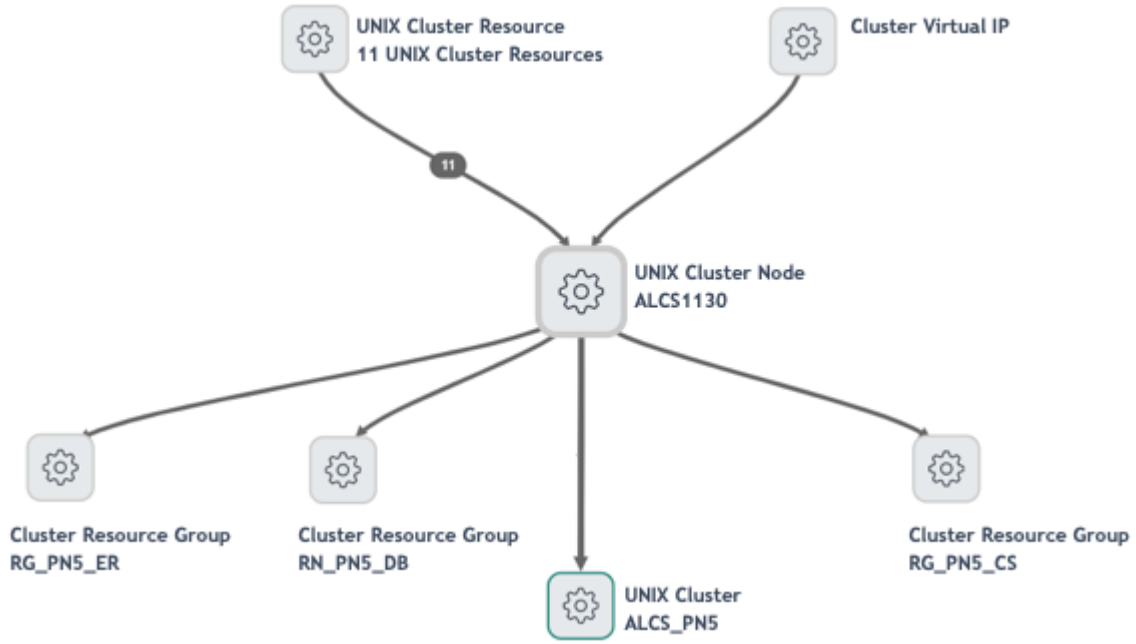
Tabelle und Feld	Beschreibung
resource_status	Der Status der Volumegruppe. Beispiele: Online, Offline
Cluster	Der Name des PowerHA/HACMP-Clusters, zu dem die Volumegruppe gehört.
UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]	
name	Der Name des Knoten, der am Cluster teilnimmt
node_state	Status des Clusterknotens im Kontext des CI-Status. Beispiel: UP, DOWN, UNKNOWN
ip_address	Die dem Knoten zugewiesenen IP-Adressen
node_status	Der Status des Knotens im Kontext der Ressourcengruppe, zu der er gehört
Cluster	Der Name des Clusters, zu dem der Clusterknoten gehört.
AIX-Server [cmdb_ci_aix_server]	
name	Name des AIX-Servers, der den Clusterknoten im Kontext des PowerHA/HACMP-Clusters darstellt.
UNIX-Cluster [cmdb_ci_unix_cluster]	
name	Der Name des PowerHA/HACMP-Clusters.
cluster_id	Die ID des PowerHA/HACMP-Clusters. Beispiel: 0123456789
cluster_status	Der aktuelle Status des PowerHA/HACMP-Clusters. Beispiele: ST_STABLE, NOT_CONFIGURED
cluster_version	Die Version des PowerHA/HACMP-Clusters. Beispiele: 5.5; 6.1; 7.2
cluster_type	Der Typ des PowerHA/HACMP-Clusters. Nur relevant für Versionen 7.2 und höher. Beispiel: Gestreckt
short_description	Beschreibung des PowerHA/HACMP-Clusters (Version, ID).
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	
name	Der Schnittstellenname des Clusterknotens
ip_address	Hostname oder IP-Adresse, wobei der Hostname den Namen der Netzwerkschnittstelle des Clusterknotens und die IP-Adresse die IPv4-Adresse darstellt, die dem Namen der Netzwerkschnittstelle zugeordnet ist. (Da das IBM PowerHA/HACMP-Cluster keine dedizierte VIP-Adresse hat).
Cluster	Der Name des PowerHA/HACMP-Clusters.

Die Dependency Views-Zuordnung zeigt alle erkannten Cluster-CIs in Ihrer Organisation und die Beziehungen zwischen ihnen an.

In diesem Beispiel stellt der Clusterknoten UNIX einen Cluster von UNIX Clustern dar. UNIX Clusterknoten ruft Ressourcen von UNIX Clusterressource ab und verwendet virtuelle Cluster-IP. UNIX Der Clusterknoten enthält drei Clusterressourcengruppen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dependency Views-Beispielzuordnung



CI-Beziehungen

Die folgenden Beziehungen werden erstellt, um die Erkennung von IBM HACMP/PowerHA-Clustern zu unterstützen:

CI	Beziehung	CI
UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]	Cluster von::Cluster	UNIX-Cluster [cmdb_ci_unix_cluster]
UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]	Enthält::Enthalten in	Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group]
Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group]	Enthält::Enthalten in	UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]
UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]
UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für::Erhält Ressourcen von	UNIX-Cluster [cmdb_ci_unix_cluster]
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	Verwendet von::Verwendet	UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]
UNIX-Cluster [cmdb_ci_unix_cluster]	Virtualisiert von::Virtualisiert	Virtuelle Cluster-IP [cmdb_ci_cluster_vip]
UNIX-Cluster [cmdb_ci_unix_cluster]	Enthält::Enthalten in	Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group]
UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]	Gehostet auf::Hostet	AIX-Server [cmdb_ci_aix_server]

Erkennung der IBM-Virtualisierung und Hardware Management Console

Die Anwendung Muster für Discovery und Service-Mapping verwendet das IBM HMC Server-Muster, um Informationen zu Hardware Management Console (HMC), Frame- und LPAR-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servern zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery unterstützt die folgenden CIs:

- HMC-Server
- IBM-Frame
- LPAR-Instanz (Logische Partition)

  Eine LPAR ist das Äquivalent von IBM zu einem virtuellen Computer.

- LPAR-Ressource

Discovery wird auf dem HMC-Server und den einzelnen AIX-Maschinen (LPARs) verwendet.

Das IBM HMC Server-Muster wird über SSH ausgeführt. Die Ausführung unter IBM AIX OS für LPAR- und Linux für HMC-Server wird nur unterstützt.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Verifizieren Sie die Berechtigungen für HMC- und AIX-Server

- Stellen Sie sicher, dass Sie für die folgenden HMC-Befehle berechtigt sind:
  - `lssyscfg`
  - `lshmc`
  - `lshwres`
- Vergewissern Sie sich, dass Sie für den folgenden AIX-Befehl (LPAR) berechtigt sind: `lparstat -i`.

  Hinweis: Der Befehl „`lparstat -i`“ ist zusätzlich zu den für die AIX-Server-Discovery erforderlichen Befehlen erforderlich. Weitere Informationen zur AIX-Server-Discovery finden Sie unter Erkennung von AIX-Servern. Eine Liste der AIX-Befehle finden Sie unter Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern.

Konfigurieren Sie die SSH-Anmeldeinformationen

Konfigurieren Sie SSH-Anmeldeinformationen für Now Platform. Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Führen Sie eine Horizontal-Discovery für HMC-Server und LPARs aus

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Führen Sie eine Discovery für die HMC-IP-Adresse aus.
2. Führen Sie nur dann eine Discovery für die LPARs unter Verwendung der IP-Adresse des AIX-Computers aus, wenn die HMC-Server-Discovery erfolgreich abgeschlossen wurde.

Weitere Informationen zum Ausführen einer Erkennung finden Sie unter Horizontale Erkennung planen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das IBM HMC Server-Muster ausgeführt wird.

IBM HMC-Server [cmdb_ci_hmc_server]

Feld	Beschreibung
Name [name]	Name der HMC.
Frame-Anzahl [frame_count]	Anzahl der für die HMC verwalteten Frames. Ein Frame ist der physische Computer, auf dem sich die LPARs befinden. Ein Frame entspricht einem ESX-Computer.
Seriennummer [serial number]	Seriennummer des HMC-Servers.
IP-Adresse [ip_address]	IP-Adresse der HMC.
BS-Version [os_version]	Betriebssystemversion.
CPU-Typ [cpu_type]	CPU-Typ
CPU-Geschwindigkeit (MHz) [cpu_speed]	CPU-Geschwindigkeit
CPU-Anzahl [cpu_count]	CPU-Anzahl.
Anzahl der CPU-Kerne [cpu_core_count]	Anzahl der CPU-Cores.
RAM (MB) [ram]	Arbeitsspeicher RAM

IBM Frame [cmdb_ci_ibm_frame]

Feld	Beschreibung
Name [name]	Name des Frames.
Seriennummer [serial number]	Seriennummer des Frame-Servers.
Aktuell verfügbare Prozessoreinheiten [curr_avail_sys_proc_units]	Aktuell verfügbare Prozessoreinheiten.
Konfigurierbare Prozessoreinheiten [configurable_sys_proc_units]	Konfigurierbare Prozessoreinheiten.
Installierte Prozessoreinheiten [installed_sys_proc_units]	Installierte Prozessoreinheiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM Frame [cmdb_ci_ibm_frame] (Fortsetzung)

Feld	Beschreibung
Aktuell verfügbare Arbeitsspeichereinheiten [curr_avail_sys_mem]	Aktuell verfügbare Arbeitsspeichereinheiten.
Konfigurierbare Speichereinheiten [configurable_sys_mem]	Konfigurierbare Arbeitsspeichereinheiten.
Installierte Speichereinheiten [installed_sys_mem]	Installierte Arbeitsspeichereinheiten.

IBM LPAR-Instanz [cmdb_ci_lpar_instance]

Feld	Beschreibung
Name [name]	Name der LPAR-Instanz.
Status [state]	Betriebsstatus. • Wird ausgeführt: bedeutet „Ein“. • Nicht aktiviert und nicht verfügbar: in Aus übersetzen.
Seriennummer [serial_number]	Seriennummer der LPAR.
Objekt-ID [object_id]	Eindeutiger Objektbezeichner. Dieser Bezeichner wird aus der Seriennummer des Frames und dem LPAR-Bezeichner verkettet.
Ist VIO [is_vio]	Identifiziert die LPAR als VIO-Server Ein VIO-Server ist die LPAR, die die physischen Komponenten für andere LPARs wie Netzwerkschnittstellenkarten (NICs) und optische Laufwerke verwaltet.
VIO-Server [vio_servers]	• Client-LPARs: Gibt die VIO-Server an, die die Client-LPARs verwalten. • VIO-Server: Identifiziert die Client-LPARs, die von den VIO-Servern verwaltet werden.
Aktuelle Mindestprozessoreinheiten [curr_min_proc_units]	Mindestanzahl an Verarbeitungseinheiten, die der Partition dynamisch zugewiesen werden können
Laufende Verarbeitungseinheiten [run_proc_units]	Anzahl der Verarbeitungseinheiten, die für die Partition geändert werden
Aktueller Arbeitsspeicher [curr_mem]	Die Menge des Arbeitsspeichers in Megabyte (MB), die der Partition zugewiesen ist.
Arbeitsspeicher [run_mem]	Aktuelle Speichermenge in MB, an die die Partition angehängt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

LPAR-Ressource [cmdb_ci_lpar_resource]

Feld	Beschreibung
Hohe Wasserzeichen-VCPU [high_watermark_vcpu]	Höchster aufgezeichneter Wert des Felds **„Virtuelle Online-CPUs“**, wie vom Befehl `„lparstat-i“` erfasst. Da der Wert dynamisch ist, können sich die Ergebnisse einer Discovery auf den Wert auswirken: • Wenn der Wert des Felds **Virtuelle Online-CPUs** niedriger ist als der mit dem Befehl `„lparstat-i“` erfasste Wert, ändert sich der Wert nicht. • Wenn der Wert des Felds **Virtuelle Online-CPUs** höher ist als der mit dem Befehl `lparstat-i` gesammelte Wert, wird der höhere Wert verwendet.
Knotenname [node_name]	Name der Instanz zusammen mit dem Feld, das auf das CI der LPAR-Instanz verweist.

Seriennummer [cmdb_serial_number]

Feld	Beschreibung
Seriennummer [serial_number]	Seriennummer des CI

CI-Beziehungen

Discovery erstellt diese Beziehungen, um die Virtualisierungs- und HMC-Erkennung IBM von zu unterstützen.

CI	Beziehung	CI
IBM HMC-Server [cmdb_ci_hmc_server]	Definiert Ressourcen für::Erhält Ressourcen von	IBM HMC-Prozessorpool [cmdb_ci_processor_pool]
IBM LPAR-Instanz [cmdb_ci_lpar_instance]	Virtualisiert von::Virtualisiert	IBM Frame [cmdb_ci_ibm_frame]
IBM Frame [cmdb_ci_ibm_frame]	Verwaltet von::Verwaltet	IBM HMC-Server [cmdb_ci_hmc_server]
IBM HMC-Prozessorpool [cmdb_ci_processor_pool]	Mitglieder::Mitglied von	IBM LPAR-Instanz [cmdb_ci_lpar_instance]

IBM WebSEAL Discovery

Die Anwendung ® Discovery verwendet die Muster IBM WebSEAL, um WebSEAL -Anwendungen, Webanwendungsserver und Verbindungen in Ihrer Infrastruktur zu finden. Das Erkennen einiger dieser Ressourcen erfordert die Installation der Anwendung Muster für Discovery und Service-Mapping aus dem ® Store.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Detaillierte Informationen zu IBM WebSEAL

Weitere Informationen finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Authentifizierung

Der Authentifizierungsprozess WebSEAL umfasst eine HTTP-Header-Authentifizierung mit Standardanmeldeinformationen Virtual Server Interface .

Wenn Sie Discovery zum ersten Mal ausführen, konfigurieren Sie die Berechtigungsaffinität für Discovery und Orchestration Anmeldeinformationsaffinität für Discovery und Orchestration .

Hinweis: Anmeldeinformationsaffinität ist im Debug-Modus nicht verfügbar.

Konfiguriert MID-Server

Stellen Sie sicher, dass MID-Server über Zugriff und Berechtigungen zum Senden von HTTPS-Anforderungen an die Anwendung WebSEAL verfügt.

Konfigurierte Anwenderberechtigungen zum Ausführen von API-Aufrufen

Stellen Sie sicher, dass der Benutzer über die Berechtigung zum Ausführen der folgenden API verfügt:

- `/net/general`
- `/net/dns`
- `/wga/reverseproxy`
- `/wga/reverseproxy/<reverse_proxy_id> /configuration/stanza/jonction/entry_name/match-vhj-first`
- `/wga/reverseproxy/<reverse_proxy_id> /Junctions`
- `/wga/reverseproxy/"<reverse_proxy_id> /Junctions?Junctions_id=<junction_id>`
- `/wga/widgets/health.json`

HTTP-Klassifizierung aktiviert

Das Muster IBM WebSEAL wird ausgelöst, wenn Sie die Discovery auf dem Server ausführen, auf dem sich das WebSEAL Muster befindet. Stellen Sie sicher, dass die HTTP-Klassifizierung in der Instanz vorhanden ist. Weitere Informationen finden Sie unter HTTP-Klassifizierung erstellen und Erkennung über einen HTTP- oder HTTPS REST-Aufruf ausführen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Während der horizontalen Erkennung erfasste Daten

Feld	Beschreibung
ISAM-Server [cmdb_ci_isam_server]	
name	Der Name des Servers, wie vom API-Aufruf „`/net/general`“ zurückgegeben. Wenn das Feld leer ist, wird `durch nslookup` nach der IP-Adresse versucht, dieses Feld auszufüllen.
IP-Adresse [ip_address]	Die IP-Adresse gemäß Discovery-Zeitplan/ Konfiguration.
fqdn	Die vom`/net/dns-` API-Aufruf zurückgegebene `search_domain`.
WebSEAL [cmdb_ci_app_server_websear]	
name	Der Name des WebSEAL -Servers, wie von der API zurückgegeben.
IP-Adresse [ip_address]	Die IP-Adresse gemäß Discovery-Zeitplan/ Konfiguration.
fqdn	Die vom`/net/dns-` API-Aufruf zurückgegebene `search_domain`.
install_status	Der Status ist standardmäßig auf **„Installiert“** festgelegt.
operation_status	Der Status ist standardmäßig auf **„Funktionsfähig“** festgelegt.
install_directory	Gemäß der Identifizierungsanforderung wird dieses Feld mit dem FQDN des Servers gefüllt.
WebSEAL-Reverse-Proxys [cmdb_ci_websear_reverse_proxy]	
name	Der Name der Ressource gemäß der API-Antwort.
object_id	Die ID der Ressource für die API-Antwort.
install_status	Gibt an, ob die Installation aktiviert ist.
operational_status	Gibt an, ob der Vorgang gestartet wurde.
service_type: hartcodiert	Der Status ist standardmäßig auf `WebSEAL Reverse Proxy`festgelegt.
webSEAL_Health_Status	Der von WebSEAL gemeldete Integritätsstatus in Bezug auf den API-Aufruf „`/wga/widgets/health.json`“.
WebSEAL-Verbindungen [cmdb_ci_webSEAL_Junction]	
name	Der Name der Ressource gemäß der API-Antwort.
object_id	Die ID der Ressource, erstellt als eindeutige Hash-Nummer, die dem Namen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	der Ressource, bei dem die Groß-/Kleinschreibung beachtet wird, entspricht. **Hinweis:** Die Nichtberücksichtigung von Groß-/Kleinschreibung bei den Abfragen kann zu doppelten Feldern führen, wenn der **Namenswert** mit dem **Objekt-ID-** Wert identisch ist. Eines der Identifizierungsattribute muss geändert werden, um einen eindeutigen Wert anzuweisen.
install_status	Auf Status „Installiert“ hartcodiert
operational_status	Hartcodiert auf Betriebsstatus
Stateful_Junction	Boolescher Wert, der angibt, ob es sich um eine statusbehaftete Verbindung handelt
transparent_path_übergang	Boolescher Wert, der angibt, ob es sich um eine transparente Pfadverbindung handelt
connection_type	Liste für den Typ der Verbindung
WebSEAL-Back-End-Server [cmdb_ci_websear_backend_server]	
name	Der Name der Ressource gemäß API-Antwort
object_id	Die ID der Ressource gemäß API-Antwort
install_status	Der Status der Ressource gemäß dem Wert „enabled“ in der API-Antwort
operational_status	den Status der Ressource gemäß dem Wert „Betriebsstatus“.
server_id	Die zur Identifizierung des Verbindungs-Webservers verwendete UUID
http_port	HTTP-Port des Back-End-Drittparteiservers. Anwendbar, wenn der Verbindungstyp „TCP“ ist.
service_port	TCP-Port des Back-End-Drittpartei-Servers. Der Standardwert ist 80 für TCP-Verbindungen und 443 für SSL-Verbindungen
Priorität	Die Priorität des Servers (1–9). Der Standardwert ist 9.

Musterbeziehungen

CI	Beziehungstyp	CI
Webseal [cmdb_ci_app_server_webseal]	Wird ausgeführt auf::Wird ausgeführt	ISAM-Server [cmdb_ci_isam_server]
WebSEAL-Reverse-Proxy [cmdb_ci_websear_reverse_proxy]	Gehostet auf::Hostet	Webseal [cmdb_ci_app_server_webseal]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Musterbeziehungen (Fortsetzung)

CI	Beziehungstyp	CI
	Referenz [load_balancer]	
WebSEAL-Reverse-Proxy [cmdb_ci_websear_reverse_proxy]	Wird ausgeführt auf::Wird ausgeführt Referenz [isam_server]	ISAM-Server [cmdb_ci_isam_server]
WebSEAL-Verbindung [cmdb_ci_webSEAL_Junction]	Zugeordnet an::Zuordnen Referenz [service]	WebSEAL-Reverse-Proxy [cmdb_ci_websear_reverse_proxy]
WebSEAL-Verbindung [cmdb_ci_webSEAL_Junction]	Eigentümer von::Eigentum von Referenz [pool]	Mitglied des Lastenausgleichsmodul-Pools [cmdb_ci_websear_backend_server]
WebSEAL-Verbindung [cmdb_ci_webSEAL_Junction]	Nur Referenz [load_balancer]	Webseal [cmdb_ci_app_server_webseal]

Hinweis: Derzeit ist die Beziehung zwischen den Back-End-Servern und tatsächlichen Server-CIs in der CMDB für HD nicht möglich.

IBM WebSphere Application Server-Discovery anhand von Mustern

Die Anwendung Muster für Discovery und Service-Mapping verwendet die Muster „Websphere On Windows“ und „Websphere On Unix“, um IBM WebSphere Application Server zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Der IBM WebSphere Application Server ist ein Software-Framework mit Middleware, das Java-basierte Webanwendungen hostet. Discovery identifiziert und klassifiziert Informationen über den WebSphere Application Server IBM auf den Computern Windows und Linux.

Hinweis: Ab Visibility Content Version 6.1.0 ist die musterbasierte Discovery die Standardmethode zur Erkennung von IBM WebSphere Application Server. Die WebSphere-Proben sind standardmäßig deaktiviert. Weitere Informationen finden Sie unter IBM WebSphere-Server-Discovery mithilfe von Probes.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen für die Discovery Windows von [].

Stellen Sie sicher, dass die folgenden Anwendungen aktuell sind:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Muster für Discovery und Service-Mapping
- Visibility Content

Aktivieren Sie PowerShell auf der MID-Server

Weitere Informationen finden Sie unter MID Server zur Verwendung von PowerShell einrichten.

Verifiziert den Zugriff auf Dateien und Verzeichnisse

Verifizieren Sie den Zugriff auf die folgenden Dateien und Verzeichnisse:

- Installationsverzeichnis des Produkts
- Konfigurationsverzeichnis des Produkts
- `versionInfo.bat`
- `WAS.Produkt`
- `BASE.product`
- `Profil.Version`
- `Express.Produkt`
- `application.xml`
- `server.xml`
- `cell.xml`

Erstellen Sie Windows -Anmeldeinformationen

Weitere Informationen finden Sie unter Windows-Anmeldeinformationen .

Horizontale Erkennung planen

Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Voraussetzungen für die Discovery Linux von [].

Stellen Sie sicher, dass die folgenden Anwendungen aktuell sind:

- Muster für Discovery und Service-Mapping
- Visibility Content

Aktivieren Sie SSH auf dem WebSphere Application Server

Weitere Informationen finden Sie im Artikel „SSH auf Linux- oder UNIX-Servern einrichten“ im Abschnitt „WebSphere Automation“ in der IBM - Dokumentation (https://www.ibm.com/docs/en/products).

Verifiziert den Zugriff auf Dateien und Verzeichnisse

Verifizieren Sie den Zugriff auf die folgenden Dateien und Verzeichnisse:

- Installationsverzeichnis des Produkts
- Konfigurationsverzeichnis des Produkts
- `oeconsol`
- `WAS_HOME`
- `CONFIG_ROOT`
- `versionInfo.sh`
- `WAS.Produkt`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `BASE.product`
- `Profil.Version`
- `Express.Produkt`
- `application.xml`
- `server.xml`
- `cell.xml`

SSH-Anmeldeinformationen erstellen

Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Verifiziert die erweiterten Rechte für IBM WebSphere Application Server-Befehle

Weitere Informationen finden Sie unter Tabelle IBM WebSphere Application Server (unter UNIX) in Service-Mapping-Befehle, die einen privilegierten Benutzer erfordern.

Horizontale Erkennung planen

Weitere Informationen finden Sie unter Horizontale Erkennung planen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn die Muster „Websphere On Windows“ und „Websphere On Unix“ ausgeführt werden.

IBM Websphere [cmdb_ci_app_server_websphere]

Feld	Beschreibung
Name [name]	Name des WebSphere-Anwendungsservers.
Version [version]	Aktuelle Version des WebSphere Application Servers.
Knoten [node]	Name des Knotens, der den WebSphere Application Server bzw. die WebSphere Application Server gruppiert.
Zelle [zelle]	Name der Zelle, die einen oder mehrere Knoten des WebSphere Application Server gruppiert.

Websphere EAR [cmdb_ci_app_server_ws_ear]

Feld	Beschreibung
Name [name]	Name der EAR-Datei (Enterprise Application Archive).
Installationsverzeichnis [install_directory]	Installationsverzeichnis der EAR-Datei.

Webservice [cmdb_ci_web_service]

Feld	Beschreibung
Name [name]	Name des Webservice.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Webservice [cmdb_ci_web_service] (Fortsetzung)

Feld	Beschreibung
Service-ID [service_id]	ID des Webservice.
Attribute [attributes]	Zusätzliche Attribute des Webservice.

Websphere-Zelle [cmdb_ci_websphere_zelle]

Feld	Beschreibung
Name [name]	Name der WebSphere-Zelle.
Zellen-ID [zelle_id]	ID der WebSphere-Zelle
Zellentyp [Zellentyp]	Typ der WebSphere-Zelle.
Zellen-Discovery-Protokoll [zelle_discovery_protocol]	Zellen-Discovery-Protokoll.
Beschreibung [short_description]	Beschreibung der Zelle, falls angegeben. Dieses Feld wird nur in der Discovery Linux ausgefüllt.

CI-Beziehungen

Discovery erstellt diese Beziehungen, um die WebSphere Application Server-Discovery für die Systeme Windows und Linux zu unterstützen.

CI	Beziehung	CI
IBM Websphere [cmdb_ci_app_server_websphere]	Enthält::Enthalten in	Websphere-Zelle [cmdb_ci_websphere_zelle]
IBM Websphere [cmdb_ci_app_server_websphere]	Enthält::Enthalten in	Websphere EAR [cmdb_ci_app_server_ws_ear]
Webservice [cmdb_ci_web_service]	Wird ausgeführt auf::Wird ausgeführt	IBM Websphere [cmdb_ci_app_server_websphere]

InfiniBox-Erkennung

ServiceNow Discovery verwendet das InfiniBox-Muster, um Instanzen zu suchen und zuzuordnen. Um diese Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Store installieren.

Die Erkennung verwendet mehrere Muster, um InfiniBox-Speichersystemdaten zu finden. Um diese Ressourcen zu erkennen, müssen Sie die Anwendungen Muster für Discovery und Service-Mapping und CMDB CI Class Models aus dem ServiceNow Store installieren, da die beiden Anwendungen voneinander abhängig sind. Sie können die Muster zur Erkennung von InfiniBox-Komponenten auf der Now Platform mit Paris-Release oder höher verwenden.

Das InfiniBox Enterprise-Speicher-Array bietet eine schnellere Performance, hohe Verfügbarkeit und eine Multi-Petabyte-Skalierung für gemischte Anwendungs-Arbeitsauslastung. Das Hardware-Redundanzdesign von InfiniBox ermöglicht eine schnelle Wiederherstellung nach Komponentenfehlern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Hinweis: Die Erkennung von „Hosts“ und „Clustern“, die dem InfiniBox-System zugeordnet sind, wird ab Version 1.0.83 des Plugins „Muster für Discovery und Service-Mapping“ (sn_itom_pattern) nicht unterstützt.

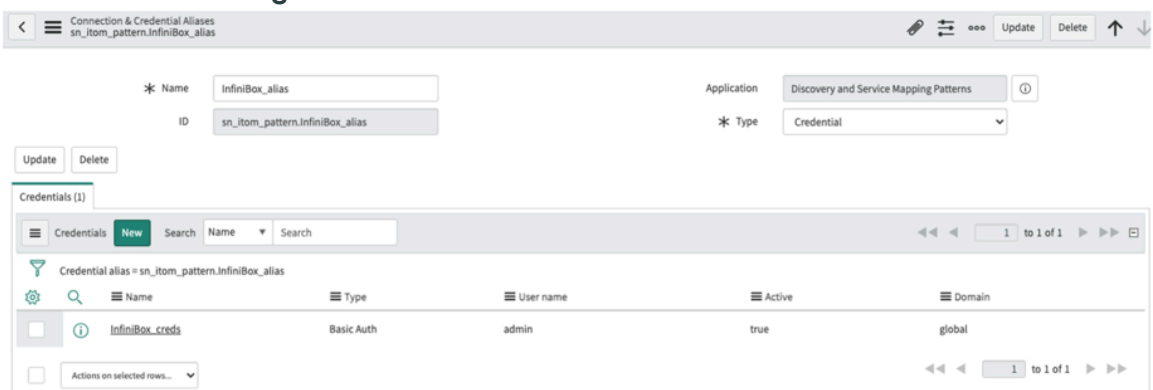
- Installieren Sie die folgenden Plugins:
  - Plugin „CMDB CI Class Models“ (Version 1.28.0 oder höher)
  - Plugin „Discovery and Service Mapping Patterns“ (Version 1.0.81 oder höher)
- Legen Sie Anmeldeinformationen für die Standardauthentifizierung für das InfiniBox-Speichersystem fest.
- Legen Sie einen Anmeldeinformationsalias fest, und ordnen Sie ihn dem Anmeldedatensatz des InfiniBox-Systems zu.
- Setzen Sie den Erkennungszeitplantyp auf „Serverlos“.
- Stellen Sie sicher, dass der MID Server Zugriff auf das Zielgerät hat.

Authentifizierung

Konfigurieren Sie die Anmeldeinformationen der Standardauthentifizierung für die Authentifizierung der REST API-Aufrufe. Sie werden für die Erkennung der CI-Typen verwendet, die dem InfiniBox-Speichersystem zugeordnet sind.

1. Navigieren Sie zu **Aliasse für Verbindungen und Anmeldeinformationen**.
2. Erstellen Sie einen neuen **Anmeldeinformationsdatensatz**.
3. Erstellen Sie im Formular der zugehörigen Liste „Anmeldeinformationen“ einen neuen Anmeldeinformationendatensatz für die **Standardauthentifizierung**. Konfigurieren Sie die Parameter für die **Standardauthentifizierung**:

Aliasse für Verbindungen und Anmeldeinformationen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

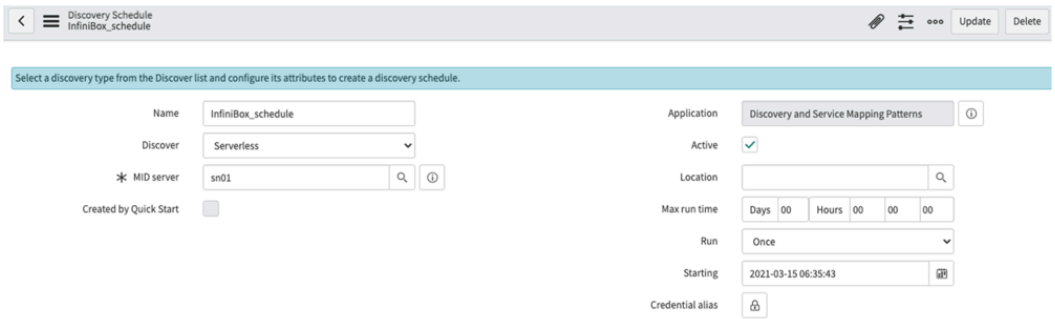
Konfigurieren Sie die Anmeldeinformationen des Typs **Standardauthentifizierung** und den dem Anmeldeinformationsdatensatz zugeordneten Anmeldeinformationsalias.

Sie können dieselbe Konfiguration über das Anmeldeinformationsdatensatzformular vornehmen, in dem Sie zuvor den Anmeldeinformationsalias erstellt haben. Ordnen Sie die Datensätze Aliasse für Verbindungen und Anmeldeinformationen zu.

Basisanmeldedaten

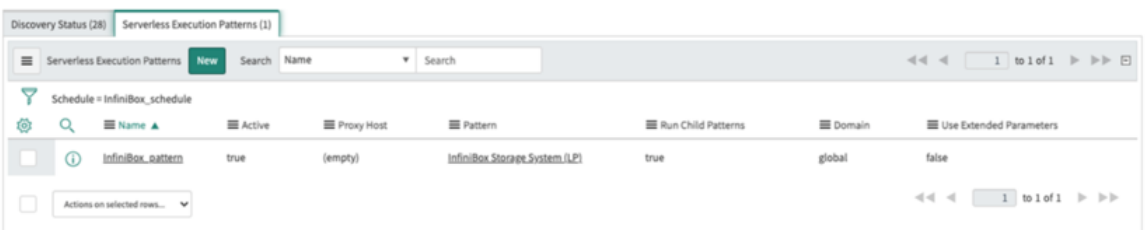
Discovery Zeitplan

1. Erstellen Sie den Erkennungszeitplan mit dem Typ „Serverlose Erkennung“.



2. Für den Erkennungszeitplan mit dem Typ „Serverlose Erkennung“ konfigurieren Sie das InfiniBox-Speichersystem-LP-Muster auf der Registerkarte „Ausführungsmuster ohne Server“.
3. Legen Sie die Option „Untergeordnete Muster ausführen“ auf „True“ fest.

   Dadurch kann das System alle untergeordneten Muster auslösen, die dem InfiniBox-Speichersystem (LP) zugeordnet sind. Dies ist aufgrund des Large Payload (LP) -Mechanismus erforderlich. Dies wird für die Erkennung des InfiniBox-Speichersystems und aller entsprechenden CI-Typen verwendet.

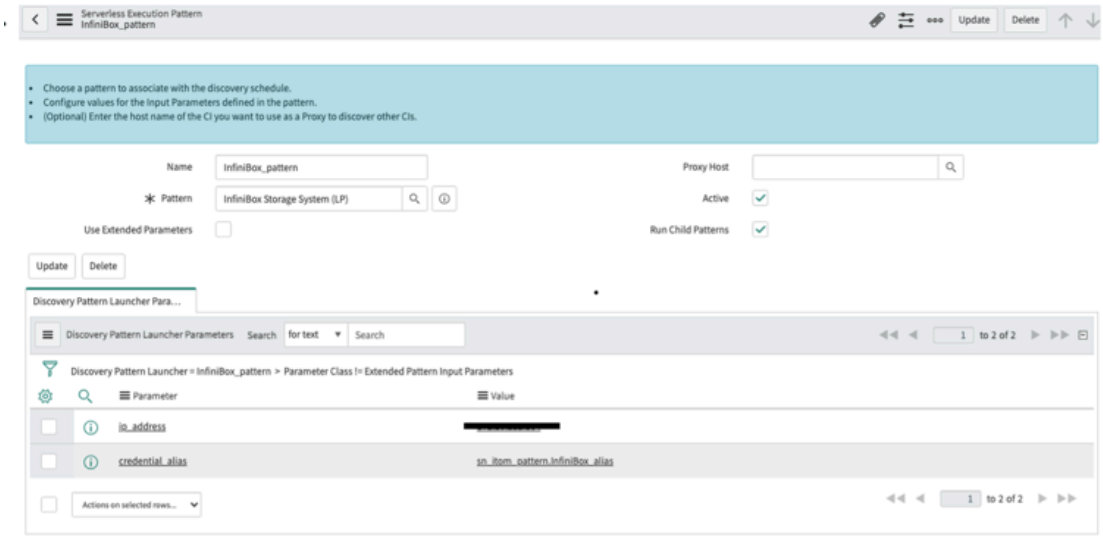


Übernehmen Sie die Werte für **ip_address** und **credential_alias** aus dem zugehörigen Abschnitt „Ausführungsmuster ohne Server“. Diese dienen als Eingabeparameter zum Auslösen des Erkennungszeitplans und des zugehörigen InfiniBox-Erkennungsmusters.

Wenden Sie die IP-Adresse des InfiniBox-Systems und die ID des zuvor erstellten Datensatzes für Aliasse für Verbindungen und Anmeldeinformationen an. Diese beziehen sich auf die InfiniBox-Anmeldedaten für den Datensatz vom Typ **Standardauthentifizierung**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausführungsmuster ohne Server



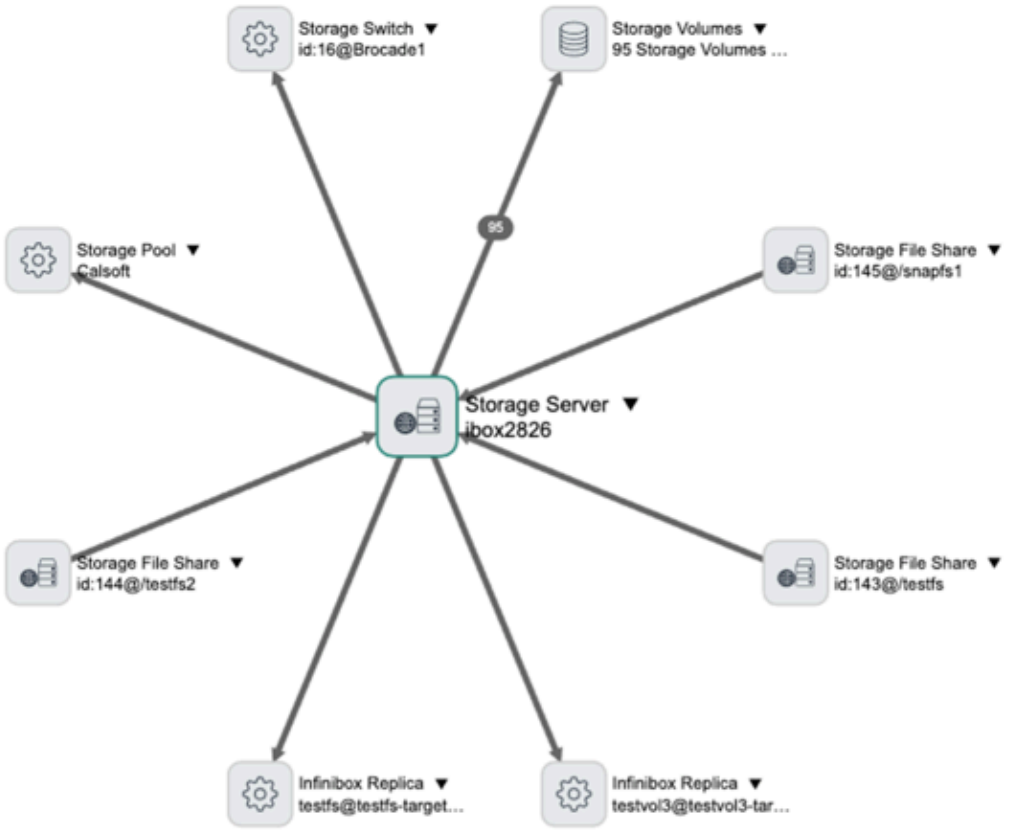
Von Discovery während der horizontalen Erkennung erfasste Daten

Speicherserver [cmdb_ci_storage_server]

Feld	Beschreibung
ip_address	IP-Adresse des InfiniBox-Systems.
Name	Name des InfiniBox-Systems.
os_version	Aktuelle Version des InfiniBox-Systems.
model_id	Modell-ID des InfiniBox-Systems.
manufacturer	Produktbezeichnung des InfiniBox-Systems.
serial_number	Seriennummer des InfiniBox-Systems.
operational_status	Betriebszustand des InfiniBox-Systems.
physical_capacity	Physische Gesamtkapazität des InfiniBox-Systems in Gigabyte.
virtual_capacity	Virtuelle Gesamtkapazität des InfiniBox-Systems in Gigabyte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherserver-Ansichtszuordnung



Datenträger [cmdb_ci_disk]

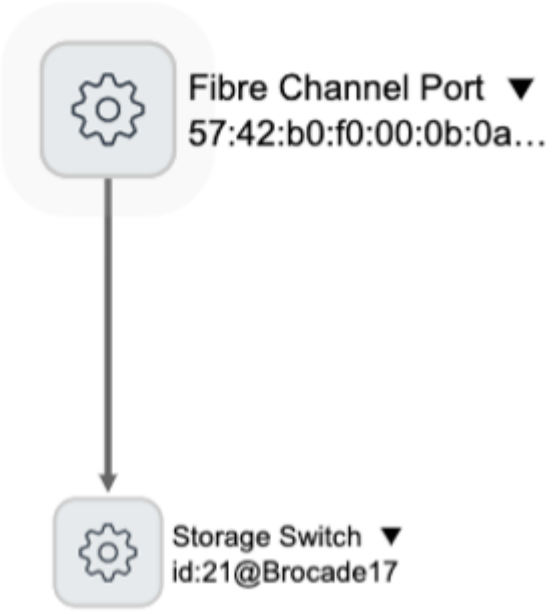
Feld	Beschreibung
device id	ID des physischen Datenträgers, Kombination aus NODE_ID@DISK_ID.
Name	Name des physischen Datenträgers, Kombination aus INFINIBOX_NAME:NODE_ID@DISK_ID
drive_type	Laufwerkstyp des physischen Datenträgers.
model_id	Modell-ID des physischen Datenträgers.
manufacturer	Anbieter des physischen Datenträgers.
operational_status	Betriebsstatus des physischen Datenträgers.
serial_number	Seriennummer des physischen Datenträgers.
Computer	Verweis auf einen der physischen Knoten des InfiniBox-Systems.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fibre-Channel-Port [cmdb_ci_fc_port]

Feld	Beschreibung
wwpn	Weltweiter Port-Name des Fibre Channel-Ports.
name	Name des Fibre Channel-Ports (wwpn).
speed	Geschwindigkeitswert des Fibre Channel-Ports in Gigabit pro Sekunde, falls angewendet.
wwnn	Weltweiter Knotenname des Fibre Channel-Ports.
port_role	Rolle des Fibre Channel-Ports.
state	Status des Fibre Channel-Ports.
link_state	Verbindungsstatus des Fibre Channel-Ports.
manufacturer	Anbieter des Fibre Channel-Ports.
model_id	Modell-ID des Fibre Channel-Ports.
Computer	Verweis auf einen der physischen Knoten des InfiniBox-Systems.

Fibre Channel-Ansichtszuordnung



Speicher-Switch [cmdb_ci_storage_switch]

Feld	Beschreibung
object_id	ID des Speicher-Switches.
name	Name des Speicher-Switches, Kombination aus id:SWITCH_ID@SWITCH_NAME.

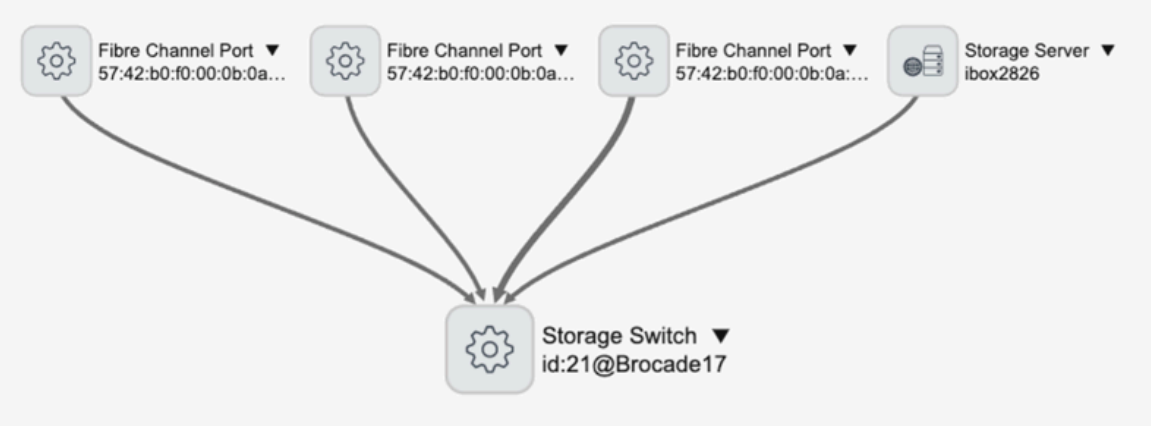
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicher-Switch [cmdb_ci_storage_switch] (Fortsetzung)

Feld	Beschreibung
wwnn	Weltweiter Knotenname des Speicher-Switches.
manufacturer	Anbieter des Speicher-Switches.

Speicher-Switch-Ansichtszuordnung

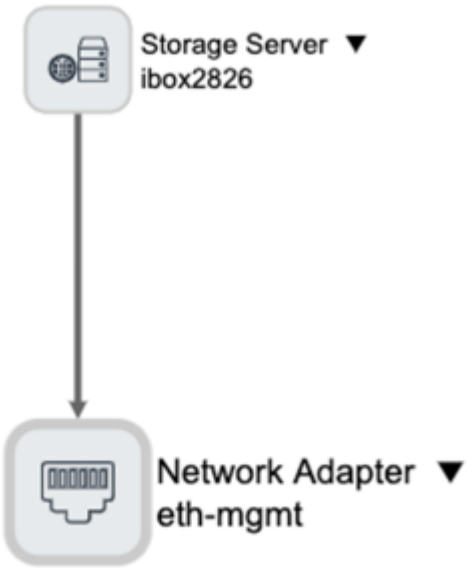


Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
mac_address	Ethernet-Adresse des Netzwerkadapters.
name	Ethernet-Name des Netzwerkadapters.
operational_status	Ethernet-Verknüpfungsstatus des Netzwerkadapters.
manufacturer	Ethernet-Anbieter des Netzwerkadapters.
model_id	Ethernet-Modell-ID des Netzwerkadapters.
ip_address	IPv4-IP-Adresse, die dem Ethernet-Netzwerkadapter zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkadapter-Ansichtszuordnung



IP-Adresse [cmdb_ci_ip_address]

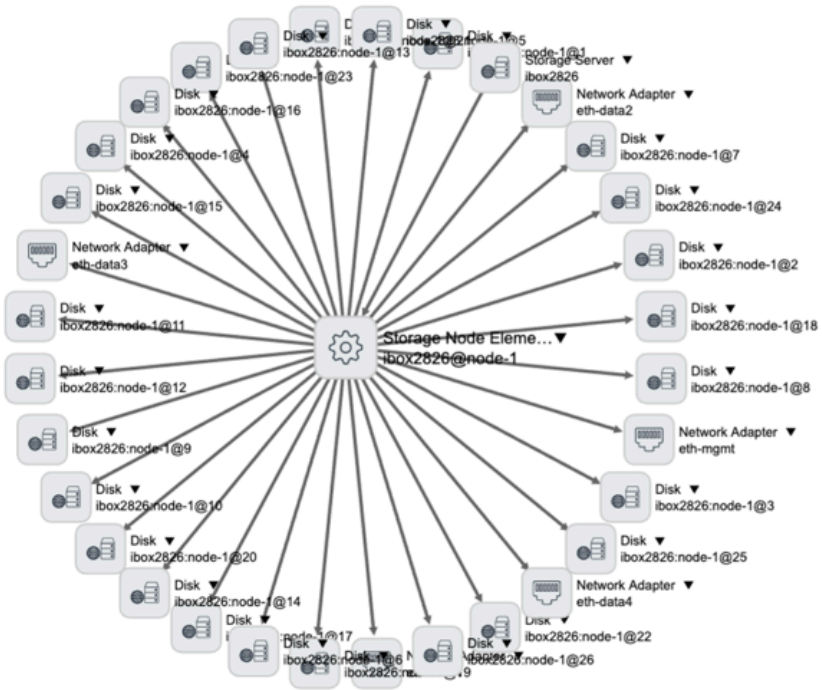
Feld	Beschreibung
netmask	Dem InfiniBox-Speichersystem zugeordnete Netzmaske.
name	IPv4-IP-Adresse eines der InfiniBox-Knoten oder des InfiniBox-Speichersystems.
ip_address	IPv4-IP-Adresse eines der InfiniBox-Knoten.

Speicherknotenelement [cmdb_ci_storage_node_element]

Feld	Beschreibung
object_id	Name des InfiniBox-Speicherknotens, Kombination aus id:NODE_ID@NODE_NAME.
name	Name des InfiniBox-Speicherknotens, Kombination aus INFINIBOX_NAME@NODE_NAME.
node_state	Betriebszustand des InfiniBox-Speicherknotens.
manufacturer	Anbieter des InfiniBox-Speicherknotens.
model_id	Modell des InfiniBox-Speicherknotens.
ip_address	Dem InfiniBox-Speicherknoten zugewiesene IPv4-Adresse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherknotenelement-Ansichtszuordnung



Seriennummer [cmdb_serial_number]

Feld	Beschreibung
serial_number	Dem InfiniBox-Speichersystem zugeordnete Seriennummer.
serial_number_type	Seriennummerntyp des InfiniBox-Speichersystems.
valid	Seriennummergültigkeitstyp des InfiniBox-Speichersystems.

Speichervolume [cmdb_ci_storage_volume]

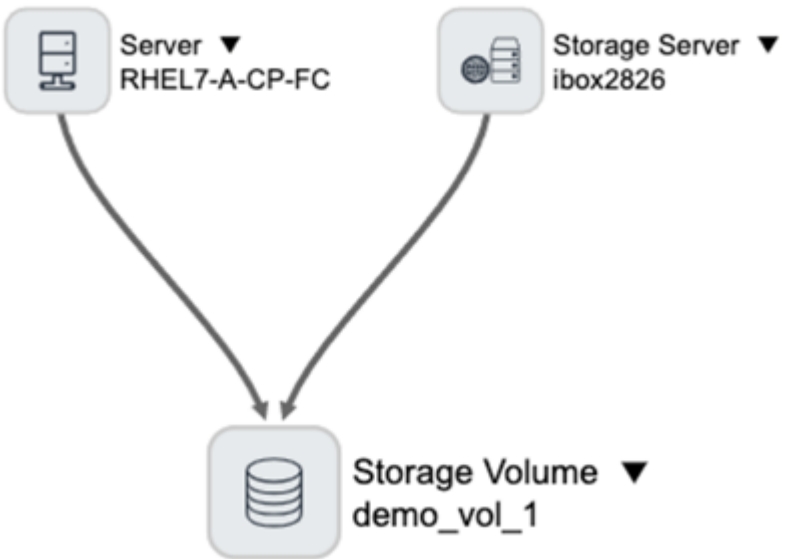
Feld	Beschreibung
object_id	ID des Speichervolume, Kombination aus id:VOLUME_ID@VOLUME_NAME.
volume_id	ID des Speichervolume, Kombination aus id:VOLUME_ID@VOLUME_NAME.
name	Name des Speichervolume.
storage_type	Rolle des Speichervolume.
size_bytes	Gesamtkapazität des Speichervolume in Byte.
serial_number	Seriennummer des Speichervolume.
pool_id	ID des Pools, dem das Speichervolume zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichervolume [cmdb_ci_storage_volume] (Fortsetzung)

Feld	Beschreibung
state	Sperrstatus des Speichervolume.
provisioning_type	Art der Bereitstellung des Speichervolume.
size	Gesamtkapazität des Speichervolume in Gigabyte
provided_by	Verweis zum Speicher-Pool, dem das Speichervolume zugeordnet ist.

Speichervolume-Ansichtszuordnung



Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]

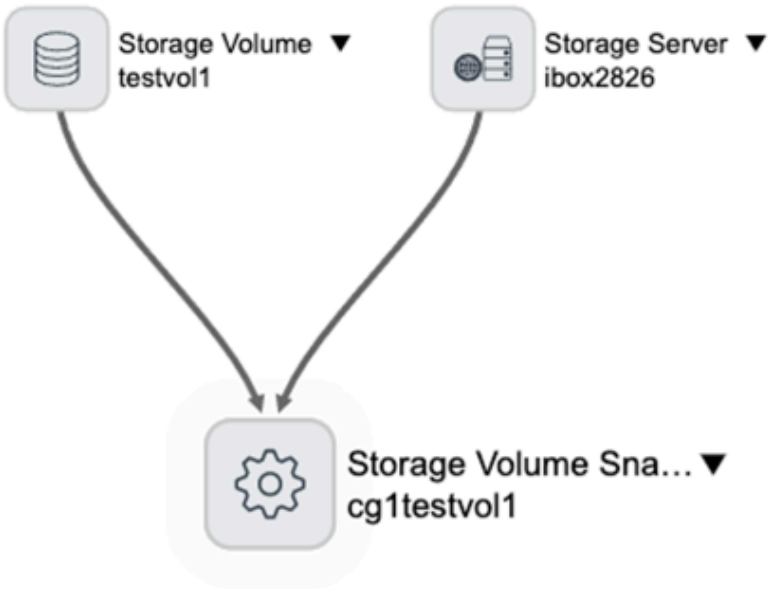
Feld	Beschreibung
object_id	ID des Speichervolume-Snapshot, Kombination aus id:VOLUME_ID@VOLUME_NAME.
storage_server	Name des InfiniBox-Systems, dem der Volume-Snapshot zugeordnet ist.
name	Name des Speichervolume-Snapshots.
size_bytes	Gesamtkapazität des Speichervolume-Snapshots in Byte.
size	Gesamtkapazität des Speichervolume-Snapshots in Gigabyte.
serial_number	Seriennummer des Speichervolume-Snapshots.
pool_id	ID des Pools, dem der Speichervolume-Snapshot zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot] (Fortsetzung)

Feld	Beschreibung
parent_id	ID des Speichervolume, das dem Snapshot des Speichervolume übergeordnet ist.
state	Sperrstatus des Speichervolume-Snapshots.
provisioning_type	Art der Bereitstellung des Speichervolume-Snapshots.
provided_by	Verweis zum Speicher-Pool, dem das Speichervolume zugeordnet ist.

Speichervolume-Snapshot



Speicherpool [cmdb_ci_storage_pool]

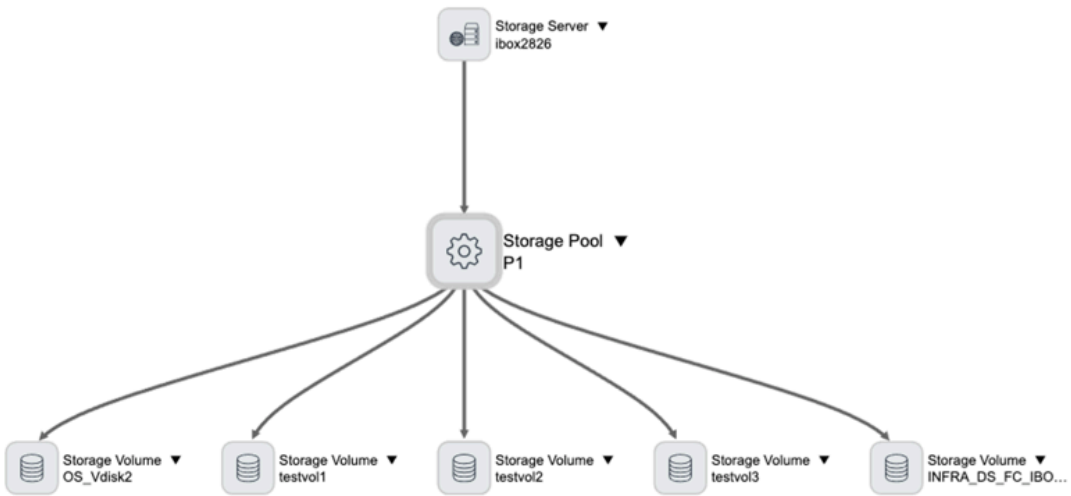
Feld	Beschreibung
object_id	ID des Speichervolume, Kombination aus id:POOL_ID@POOL_NAME.
Name	Name des Speicherpools.
physical_capacity	Physische Gesamtkapazität des Speicherpools in Gigabyte.
virtual_capacity	Virtuelle Gesamtkapazität des Speicherpools in Gigabyte.
free_phys_capacity	Verfügbare physische Kapazität des Speicherpools in Gigabyte.
free_virt_capacity	Verfügbare virtuelle Kapazität des Speicherpools in Gigabyte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherpool [cmdb_ci_storage_pool] (Fortsetzung)

Feld	Beschreibung
num_vols	Anzahl der am Speicherpool beteiligten Volumes.
num_file_sys	Anzahl der am Speicherpool beteiligten Dateisysteme.
num_file_sys_snap	Anzahl der am Speicherpool beteiligten Dateisystem-Snapshots.
num_vol_snap	Anzahl der am Speicherpool beteiligten Volume-Snapshots.
pool_id	ID des Speicherpools.
pool_state	Status des Speicherpools.

Speicherpool-Ansichtszuordnung



Dateisystem [cmdb_ci_file_system]

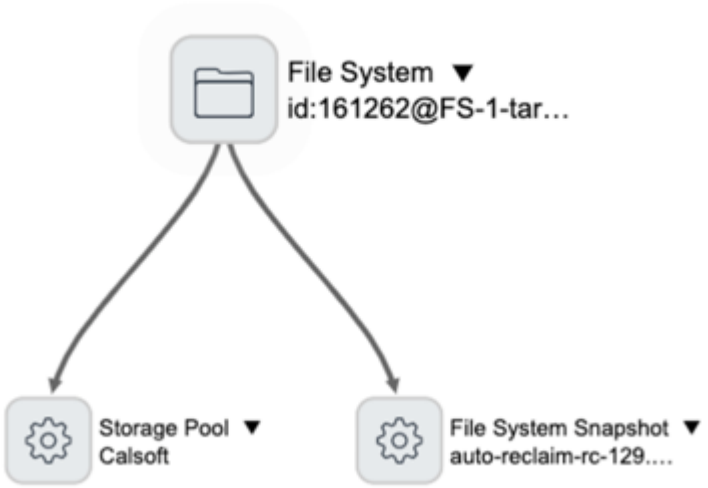
Feld	Beschreibung
object_id	ID des primären Dateisystems, Kombination aus id:FILE_SYSTEM_ID.
server_name	Name des InfiniBox-Systems, dem das primäre Dateisystem zugeordnet ist.
name	Name des primären Dateisystems, Kombination aus id:FILE_SYSTEM_ID@FILE_SYSTEM_NAME.
size_bytes	Gesamtgröße des primären Dateisystems in Byte.
size	Gesamtgröße des primären Dateisystems in Gigabyte.
free_space_bytes	Freier Speicher des primären Dateisystems in Byte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateisystem [cmdb_ci_file_system] (Fortsetzung)

Feld	Beschreibung
serial_number	Seriennummer des primären Dateisystems.
storage_type	Art des primären Dateisystems.
pool_id	ID des Pools, dem das primäre Dateisystem zugeordnet ist.
provisioning_type	Art der Bereitstellung des primären Dateisystems.
provided_by	Verweis auf den Speicherpool, dem das primäre Dateisystem zugeordnet ist.

Dateisystem-Ansichtszuordnung



Dateisystem-Snapshot [cmdb_ci_file_system_snapshot]

Feld	Beschreibung
object_id	ID des Snapshot-Dateisystems, Kombination aus id:FILE_SYSTEM_ID@FILE_SYSTEM_NAME.
volume_id	ID des Snapshot-Dateisystems, Kombination aus id:FILE_SYSTEM_ID@FILE_SYSTEM_NAME.
server_name	Name des InfiniBox-Systems, dem das Snapshot-Dateisystem zugeordnet ist.
name	Name des Snapshot-Dateisystems.
size_bytes	Gesamtgröße des Snapshot-Dateisystems in Byte.
free_space_bytes	Freier Speicher des Snapshot-Dateisystems in Byte.
serial_number	Seriennummer des Snapshot-Dateisystems.
storage_type	Typ des Snapshot-Dateisystems.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateisystem-Snapshot [cmdb_ci_file_system_snapshot] (Fortsetzung)

Feld	Beschreibung
pool_id	ID des Pools, dem das Snapshot-Dateisystem zugeordnet ist.
parent_id	ID des primären Dateisystems, dem das Snapshot-Dateisystem zugeordnet ist.
provisioning_type	Art der Bereitstellung des Snapshot-Dateisystems.

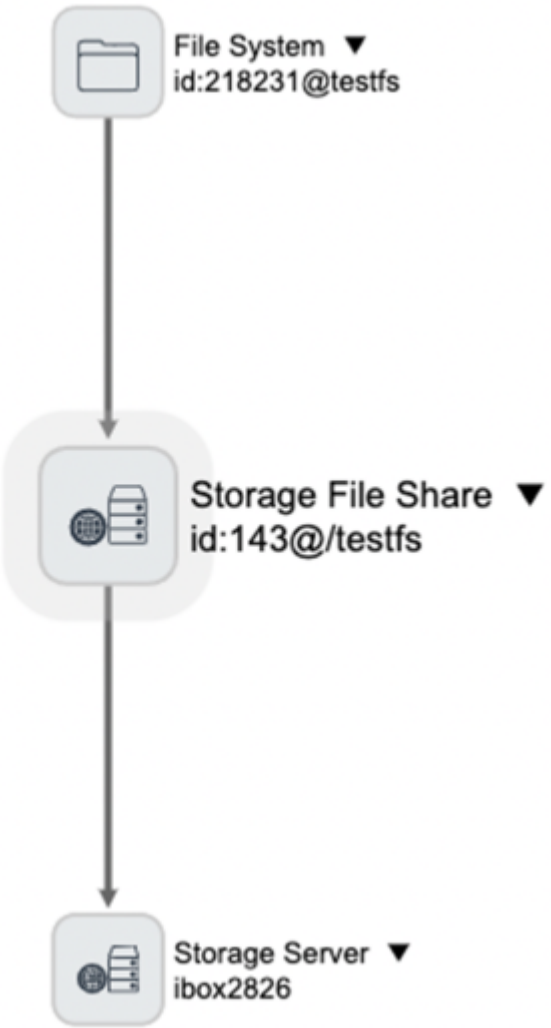
Dateisystem-Snapshot-Ansichtszuordnung

Speicherdateifreigabe [cmdb_ci_storage_fileshare]

Feld	Beschreibung
Pfad	Exportpfad der InfiniBox-Exportentität.
Name	Name der InfiniBox-Exportentität, Kombination aus id:EXPORT_ID@EXPORT_PATH.
fileshare_id	ID der Exportentität im Kontext des InfiniBox-Systems.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Export-Ansichtszuordnung



Primäre InfiniBox-Konsistenzgruppe [cmdb_ci_infinibox_cg]

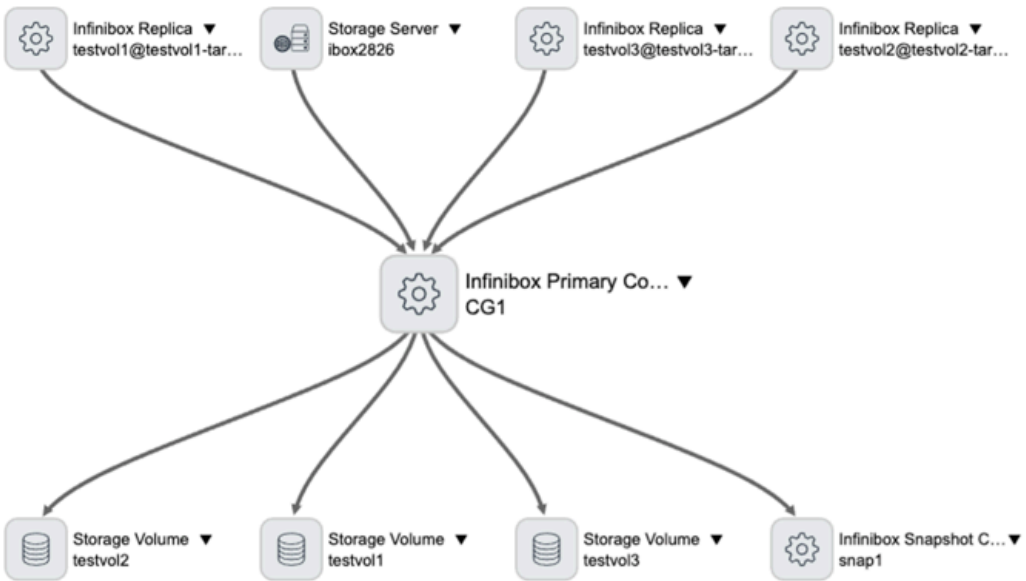
Feld	Beschreibung
object_id	ID der primären InfiniBox-Konsistenzgruppe, Kombination aus id:CONSISTENCY_GROUP_ID@ CONSISTENCY_GROUP_NAME.
created_time	Erstellungszeit der primären InfiniBox-Konsistenzgruppe im Format JJ-MM-TT HH:mm::SS.
updated_time	Aktualisierte Zeit der primären InfiniBox-Konsistenzgruppe im Format JJ-MM-TT HH:mm::SS.
name	Name der primären InfiniBox-Konsistenzgruppe.
type	Typ der primären InfiniBox-Konsistenzgruppe.
members_count	Anzahl der Entitäten, die an der primären InfiniBox-Konsistenzgruppe teilnehmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Primäre InfiniBox-Konsistenzgruppe [cmdb_ci_infinibox_cg] (Fortsetzung)

Feld	Beschreibung
pool_id	ID des Pools, dem die primäre InfiniBox-Konsistenzgruppe zugeordnet ist.
lock_state	Sperrstatus der primären InfiniBox-Konsistenzgruppe.

Primäre Konsistenzgruppe – Ansichtszuordnung



Snapshot der InfiniBox-Konsistenzgruppe[cmdb_ci_infinibox_snapshot_cg]

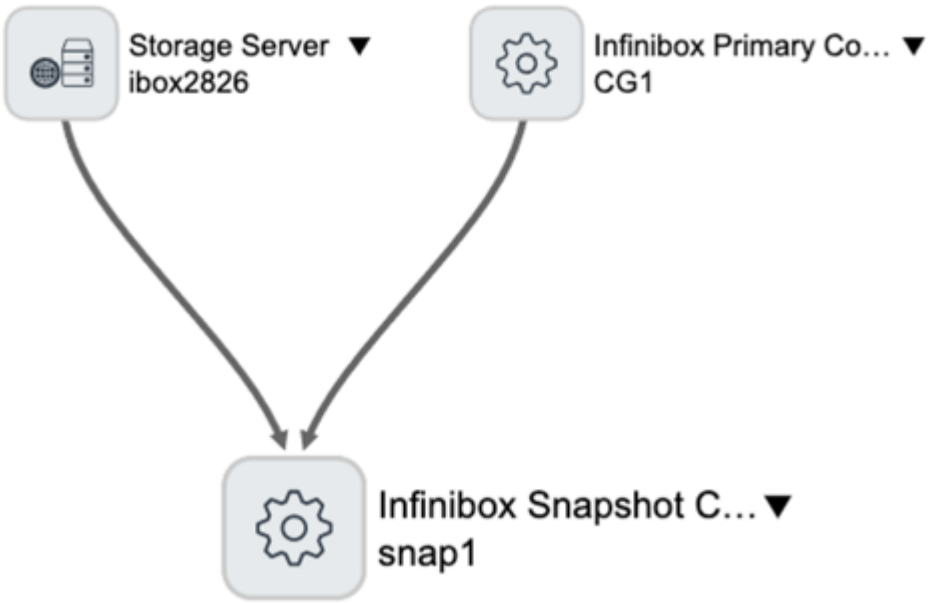
Feld	Beschreibung
object_id	ID des Snapshot der InfiniBox-Konsistenzgruppe, Kombination aus id:CONSISTENCY_GROUP_ID@ CONSISTENCY_GROUP_NAME.
created_time	Erstellungszeit für den Snapshot der InfiniBox-Konsistenzgruppe im Format JJ-MM-TT HH:mm::SS.
updated_time	Aktualisierte Zeit für den Snapshot der InfiniBox-Konsistenzgruppe im Format JJ-MM-TT HH:mm::SS.
name	Snapshot-Name der InfiniBox-Konsistenzgruppe.
type	Snapshot-Typ der InfiniBox-Konsistenzgruppe.
members_count	Anzahl der Entitäten, die an der Snapshot-InfiniBox-Konsistenzgruppe teilnehmen.
pool_id	ID des Pools, dem der Snapshot der InfiniBox-Konsistenzgruppe zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Snapshot der InfiniBox-Konsistenzgruppe[cmdb_ci_infinibox_snapshot_cg] (Fortsetzung)

Feld	Beschreibung
lock_state	Sperrstatus der Snapshot-InfiniBox-Konsistenzgruppe.

Ansichtszuordnung – Snapshot-Konsistenzgruppe



InfiniBox-Verknüpfung [cmdb_ci_infinibox_link]

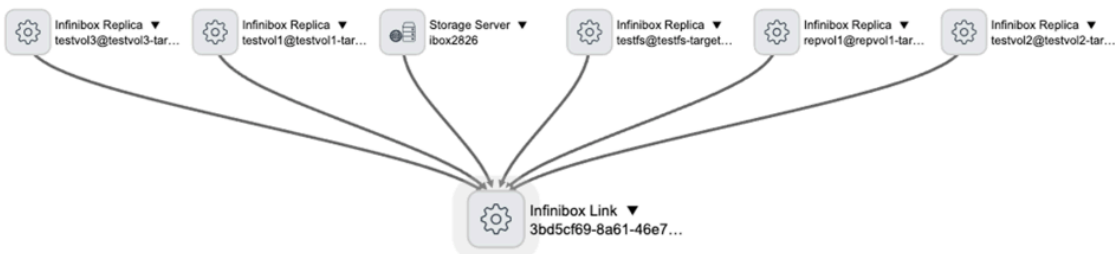
Feld	Beschreibung
object_id	ID der InfiniBox-Verknüpfung.
name	Name der InfiniBox-Verknüpfung.
remote_version	Version des InfiniBox-Remote-Speichersystems.
remote_host	Hostname oder die IP-Adresse des InfiniBox-Remote-Speichersystems.
remote_ip	IP-Adresse des InfiniBox-Remote-Speichersystems.
remote_link_id	Verknüpfungs-ID des InfiniBox-Remote-Speichersystems.
remote_serial_number	Seriennummerntyp des InfiniBox-Remote-Speichersystems.
remote_sys_name	Systemname des InfiniBox-Remote-Speichersystems.
link_state	Verknüpfungsstatus zwischen den InfiniBox-Speichersystemen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

InfiniBox-Verknüpfung [cmdb_ci_infinibox_link] (Fortsetzung)

Feld	Beschreibung
link_config_id	ID der Verknüpfungskonfiguration des InfiniBox-Remote-Speichersystems im GUID-Format.
link_mode	Verknüpfungsmodus zwischen den InfiniBox-Speichersystemen.
resiliency_mode	Resilienzmodus zwischen den InfiniBox-Speichersystemen.
local_witness_state	Lokaler Zeugenstatus des InfiniBox-Speichersystems.
witness_address	Lokale Zeugenadresse des InfiniBox-Speichersystems, wenn zugewiesen.
last_connection_time	Zeitstempel der eingerichteten Verbindung zwischen den InfiniBox-Speichersystemen im Format JJ-MM-TT HH: MM::SS.
local_replica_net_space_id	ID des lokalen Replikat-Netzwerkspeichers des InfiniBox-Speichersystems.
link_replication_type	Replikationstyp der Verknüpfung zwischen den InfiniBox-Speichersystemen.

Verknüpfung-Ansichtszuordnung



InfiniBox-Replikat [cmdb_ci_infinibox_replica]

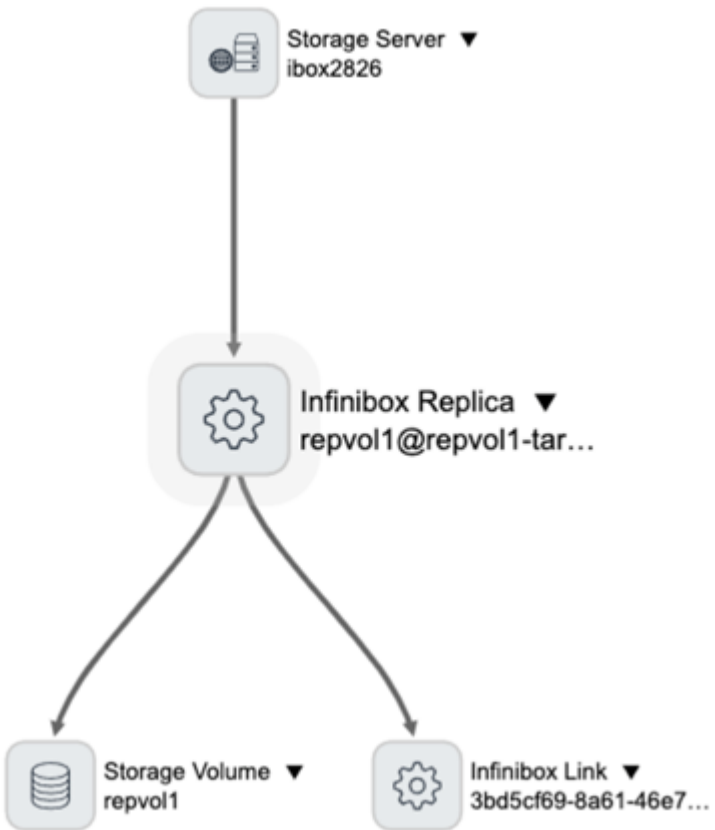
Feld	Beschreibung
object_id	ID des InfiniBox-Replikats, Kombination aus LOCAL_ENTITY_NAME@REMOTE_ENTITY_NAME@replica:REPLICA_ID.
name	ID des InfiniBox-Replikats, Kombination aus LOCAL_ENTITY_NAME@REMOTE_ENTITY_NAME@replica:REPLICA_ID.
replica_role	Rolle des InfiniBox-Speichersystem-Replikats.
entity_type	Typ der replizierten Entität im Kontext des InfiniBox-Speichersystems.
replica_state	Status des Replikats im Kontext des InfiniBox-Speichersystems.
replication_type	Typ der Replizierung des Kontexts des InfiniBox-Speichersystems, wenn angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

InfiniBox-Replikat [cmdb_ci_infinibox_replica] (Fortsetzung)

Feld	Beschreibung
sync_state	Synchronisierungsstatus des InfiniBox-Speichersystem-Replikats.
link_id	ID der Verknüpfung, die dem Replikat im Kontext des InfiniBox-Speichersystems zugeordnet ist.
entity_id	ID der replizierten Entität im Kontext des InfiniBox-Speichersystems.
remote_entity_id	ID der replizierten Remote-Entität des InfiniBox-Speichersystems.
entity_name	Name der lokalen replizierten Entität im Kontext des InfiniBox-Speichersystems.
remote_entity_name	Name der replizierten Remote-Entität im Kontext des InfiniBox-Speichersystems.
dataset_type	Lokaler Datensatztyp im Kontext des InfiniBox-Speichersystems.

Replikat-Ansichtszuordnung



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Beziehungen

Vom InfiniBox-Speichersystem (LP)-Muster erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_storage_switch
cmdb_ci_fc_port	Verbunden mit::Verbunden von	cmdb_ci_storage_switch
cmdb_ci_storage_server	Verwendet::Verwendet von	cmdb_ci_network_adapter
cmdb_ci_storage_node_element	Besitzt::Eigentum von	cmdb_ci_network_adapter
cmdb_ci_ip_address	Referenz nach Spaltennamen-NIC	cmdb_ci_network_adapter
cmdb_ci_storage_node_element	Besitzt::Eigentum von	cmdb_ci_fc_port
cmdb_ci_storage_server	Besitzt::Eigentum von	cmdb_ci_ip_address
cmdb_ci_storage_node_element	Besitzt::Eigentum von	cmdb_ci_ip_address
cmdb_ci_storage_node_element	Enthält::Enthalten von	cmdb_ci_disk
cmdb_serial_number	Referenz	cmdb_ci_storage_server
cmdb_ci_storage_server	Zugeordnet zu::Zugeordnet von	cmdb_ci_storage_node_element

Vom InfiniBox-Speichervolume (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_volume	Bereitgestellt von::Bereitgestellt	cmdb_ci_storage_vol_snapshot
cmdb_ci_storage_pool	Referenz nach Spaltenname bereitgestellt von	cmdb_ci_storage_volume
cmdb_ci_storage_server	Enthält::Enthalten in und Verweis auf Spaltennamencomputer	cmdb_ci_storage_volume
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_storage_vol_snapshot
cmdb_ci_infinibox_cg	Enthält::Enthalten von	cmdb_ci_storage_volume
cmdb_ci_infinibox_snapshot_cg	Enthält::Enthalten von	cmdb_ci_storage_vol_snapshot

Vom InfiniBox-Speicherpool (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_storage_pool

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vom InfiniBox-Speicherexport (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_fileshare	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_server

Vom InfiniBox-Speicherdateisystem (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_file_system
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_file_system_snapshot
cmdb_ci_file_system	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_pool
cmdb_ci_file_system_snapshot	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_pool
cmdb_ci_file_system	Bereitgestellt von::Bereitgestellt	cmdb_ci_file_system_snapshot
cmdb_ci_file_system	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_fileshare
cmdb_ci_file_system_snapshot	Bereitgestellt von::Stellt bereit	cmdb_ci_storage_fileshare

Vom InfiniBox-Speicherkonsistenzgruppen (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_infinibox_cg
cmdb_ci_infinibox_cg	Bereitgestellt von::Bereitgestellt	cmdb_ci_infinibox_snapshot_cg
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_infinibox_snapshot_cg
cmdb_ci_infinibox_cg	Enthält::Enthalten von	cmdb_ci_storage_pool
cmdb_ci_infinibox_snapshot_cg	Enthält::Enthalten von	cmdb_ci_storage_pool

Vom InfiniBox-Speicherreplikat (LP)-Muster erstellte Beziehungen

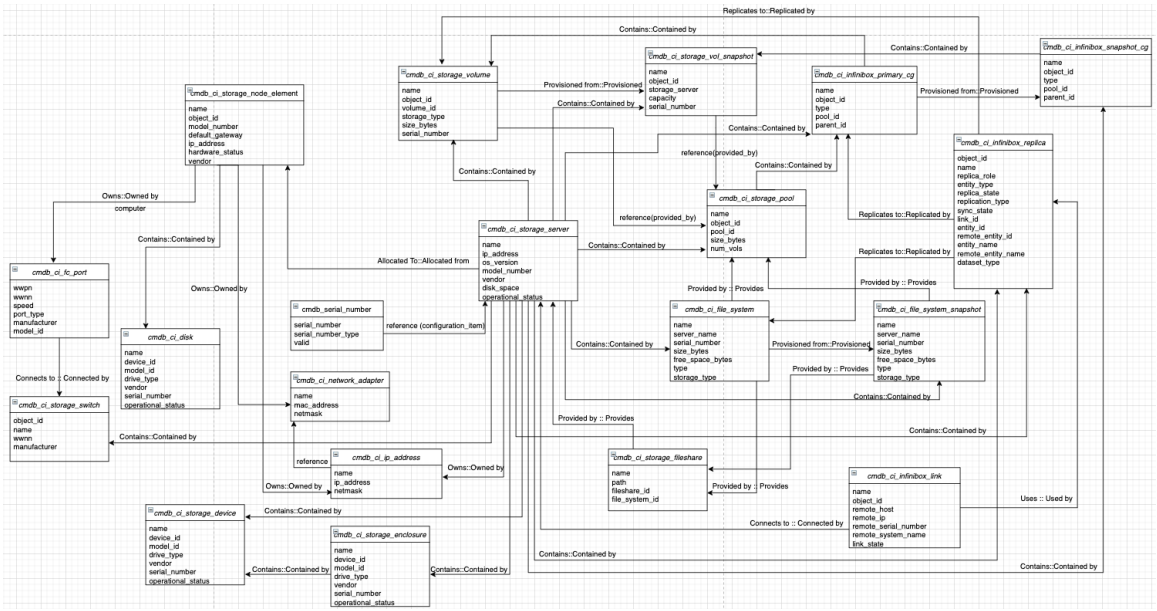
CI	Beziehungen	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_infinibox_replica
cmdb_ci_infinibox_replica	Repliziert zu::Repliziert von	cmdb_ci_infinibox_cg
cmdb_ci_infinibox_replica	Verwendet::Verwendet von	cmdb_ci_infinibox_link
cmdb_ci_infinibox_replica	Repliziert zu::Repliziert von	cmdb_ci_storage_volume
cmdb_ci_infinibox_replica	Repliziert zu::Repliziert von	cmdb_ci_file_system

Vom InfiniBox-Speicherverknüpfungs (LP)-Muster erstellte Beziehungen

CI	Beziehungen	CI
cmdb_ci_storage_server	Enthält::Enthalten von	cmdb_ci_infinibox_link

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Infinibox-Klassenmodell



Linux Pacemaker Cluster-Erkennung

Die ServiceNow Discovery-Anwendung verwendet das Linux Pacemaker Cluster-Erkennungsmuster, um Clusterdaten mit hoher Verfügbarkeit zu finden und CMDB mit den erkannten Informationen auszufüllen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Dieses Muster ist ein Erweiterungsabschnitt des Linux-Server-Musters. Discovery verwendet das Muster zum Ausführen der horizontalen Erkennung.

Sie können dieses Muster auf der Now Platform® mit Madrid -Release oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Konfigurieren Sie SSH-Anmeldeinformationen für den Linux-Server
- Gewähren Sie einem Benutzer die Berechtigung zum Lesen dieser Dateien:
  - `/etc/hosts`
  - `/etc/corosync/corosync.conf`
  - `/var/lib/heartbeat/crm/cib.xml` oder `/var/lib/pacemaker/cib/cib.xml` von Linux SP3
- Erteilen Sie einem Benutzer Berechtigungen zum Ausführen der folgenden Befehle:

```
ps -ef | grep corosync | grep -v grep

ps -ef | grep pacemaker | grep -v grep

ifconfig | grep 'inet addr:' |awk '{print $1, $2 }'
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
hostname -s
```

```
hostname -f
```

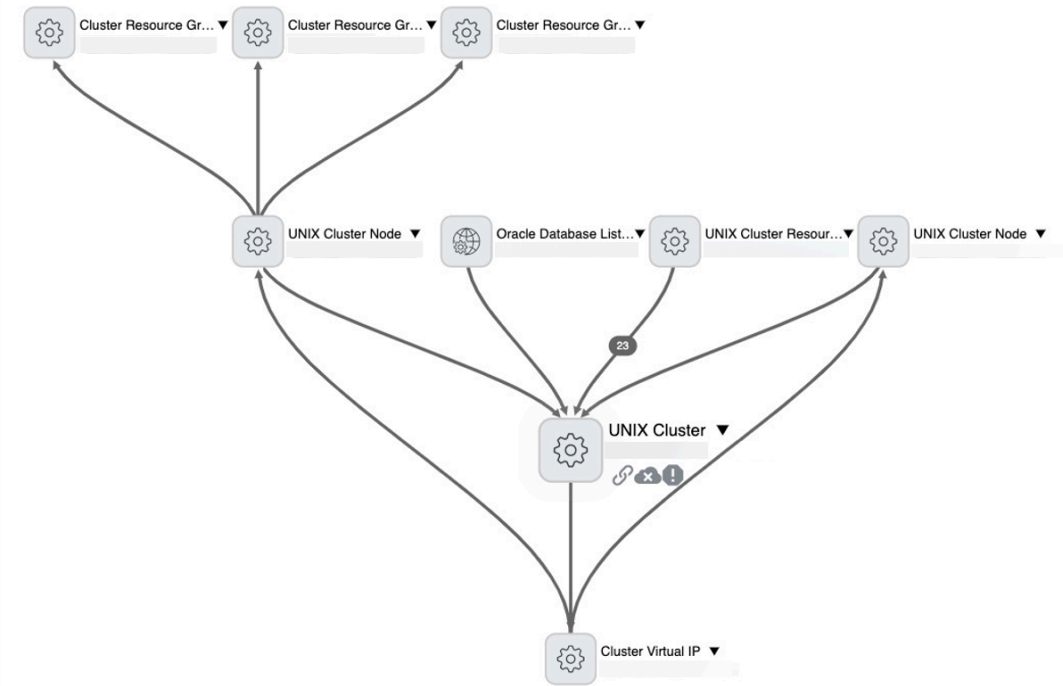
Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Haupt-CI – UNIX-Cluster [cmdb_ci_unix_cluster]	
name	Clustername
cluster_id	Cluster-ID. Enthält die Knoten-ID.
cluster_type	Clustertyp
cluster_status	Cluster-Status: Online / Offline
cluster_version	Clusterversion
UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	
name	Ressourcenname
resource_type	Ressourcentyp
resource_status	Ressourcenstatus. Beispiel: Gestartet
ip_address	IP-Adresse des Computers, auf dem die Ressource ausgeführt wird
fqdn	FQDN des Computers, auf dem die Ressource ausgeführt
Virtuelle Cluster-IP [cmdb_ci_cluster_vip]	
name	Cluster-VIP-Name
ip_address	IP-Adresse der VIP
Cluster-Ressourcengruppe [cmdb_ci_cluster_resource_group]	
name	Ressourcengruppenname
Knoten	Ressourcengruppenknoten
resource_group_status	Ressourcengruppenstatus
Server	Ressourcengruppenserver
fqdn	FQDN des Computers, auf dem die Ressourcengruppe läuft
UNIX-Clusterknoten [cmdb_ci_unix_cluster_node]	
name	Knotenname und Knoten-ID
node_status	Knotenstatus
node_state	Knotenstatus
fqdn	FQDN des Computers, auf dem der Knoten ausgeführt wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Karte Abhängigkeitsansichten zeigt entdeckte Lastenausgleichsmodul-CIs und die Beziehungen untereinander.



CI-Beziehungen

Diese Beziehungen sollen die Linux Pacemaker Cluster-Erkennung unterstützen:

CI	Beziehung	CI
cmdb_ci_unix_cluster	Hostet::Gehostet auf	cmdb_ci_linux_server
cmdb_ci_unix_cluster_node	Gehostet auf::Hostet	cmdb_ci_linux_server
	Cluster von::Cluster	cmdb_ci_unix_cluster
cmdb_ci_cluster_vip	Verwendet::Verwendet von	cmdb_ci_unix_cluster_node
	Virtualisiert von::Virtualisiert	cmdb_ci_unix_cluster
cmdb_ci_unix_cluster_resource	Definiert Ressourcen für::Erhält Ressourcen von	cmdb_ci_unix_cluster
	Definiert Ressourcen für::Erhält Ressourcen von	cmdb_ci_unix_cluster_node
cmdb_ci_cluster_resource_group	Enthält::Enthalten in	cmdb_ci_unix_cluster
	Enthält::Enthalten in	cmdb_ci_unix_cluster_node
	Enthält::Enthalten in	cmdb_ci_unix_cluster_resource

Erkennung von Microsoft Azure-Cloud-Komponenten mithilfe von Mustern

Discovery verwendet mehrere Muster, um Komponenten der Bereitstellung Microsoft Azure Cloud während der Horizontal-Discovery zu erkennen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind.

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle
- Visibility Content

Konfiguration von Cloud-Discovery für Microsoft Azureüberprüfen

- Verwenden Sie Arbeitsbereich für Cloud-Vorgänge, um Cloud-Discoveryeinzurichten. Weitere Informationen finden Sie unter Cloud-Discovery Setup mit Arbeitsbereich für Cloud-Vorgänge
- Aktivieren Sie Cloud-Discovery für den Zugriff auf Ihre Azure -Umgebung. Weitere Informationen finden Sie unter Erkennung von Azure-Clouds

Cloudbezogenen CI-Beziehungen aktivieren

Um erkannte Komponenten in Serviceinstanzen aufzunehmen, aktivieren Sie CI-Beziehungen, die in der Tag-basierten Discovery von Service-Mappingverwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar. Schritte zur Ausführung finden Sie unter Konfiguration der Tag-basierten Discovery.

Azure-Verfügbarkeitssatz

Warten Sie auf den **Bereinigungsauftrag für die Verfügbarkeitszone, um den Zeitplanauftrag für den Verfügbarkeitssatz-Datensatz zu löschen** und alle Konfigurationselemente (CI) des vorab ausgefüllten Verfügbarkeitssatzes in der Tabelle **„cmdb_ci_availability_zone“** zu löschen.

Azure-Verfügbarkeitszone

Um eine Discovery mit der Azure-Verfügbarkeitszone auszuführen, registrieren Sie die Abonnement-ID für die Funktion **„AvailabilityZonePeering“** mit AZ CLI mithilfe von `az Feature Register -n AvailabilityZonePeering --namespace Microsoft.Resources`, um die Check Zone Peering-API zu verwenden. Überprüfen Sie den Status mit `der az-Funktion show -n AvailabilityZonePeering --namespace Microsoft.Resources`, bevor Sie Discovery ausführen.

Verifizieren Sie die REST API-Berechtigungen

Laden Sie die herunter Cloud-Discovery Tabelle mit Mustern , damit Sie Anwenderberechtigungen erteilen können, die zum Ausführen der Discovery -Muster erforderlich sind. Neben Berechtigungen enthält die Tabelle auch nützliche Informationen wie Musternamen, Typen, CI-Klassen und Links zur Lieferantendokumentation. Neue Muster sind vierteljährlich verfügbar. Überprüfen Sie daher regelmäßig, ob Sie über die aktuelle Version der Tabellenkalkulation verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Discovery von -Ressourcen nach Rechenzentren

Azure verfügt über Dutzende von Rechenzentren auf der ganzen Welt. Ihre Ressourcen wie Lastenausgleichsmodule und virtuelle Computer befinden sich normalerweise nicht in allen Rechenzentren, sondern nur in einigen von ihnen. Das **Azure Datacenter Discovery-** Muster wird vor allen anderen Azure -Mustern ausgeführt, um die Rechenzentren zu identifizieren, die über Ressourcen im Zusammenhang mit Ihrem Servicekonto verfügen („aktiv"), und die Rechenzentren, die nicht über Ihre Ressourcen verfügen („passiv"). Dieses Modell verbessert die Leistung der Discovery Azure. Dieses Ausführungsmodell ist effizienter als das vorherige, in dem alle Rechenzentren unabhängig davon erkannt wurden, ob sie relevante Ressourcen enthalten.

Nach der Identifizierung der „aktiven" und „passiven" Rechenzentren führt der Zeitplan Discovery weiterhin alle Azure -Muster nur für die „aktiven" Rechenzentren aus, um Ihre Azure -Cloud-Ressourcen zu erkennen. Die „passiven" Rechenzentren werden bei der Ausführung des Zeitplans ignoriert.

Je nach Servicekonto und MID-Server -Eigenschaftseinstellungen können Sie Unterschiede im Discovery-Protokoll Azure, in der Discovery-Zeit und in CMDBfeststellen.

Rechenzentren, die bereits vor Muster für Discovery und Service-Mapping Version 1.15.0 erkannt wurden, verbleiben in der Tabelle **„Azure-Rechenzentren"**. Das Laufzeitverhalten der Discovery wird jedoch jetzt durch den Wert der MID-Server Eigenschaft [] *`mid.cloud.discovery.sonar.discover_all_azure_datacenters`*bestimmt. Die Eigenschaft ist standardmäßig auf **„false"** festgelegt, um die Discovery-Ausführung auf die „aktiven" Rechenzentren und nicht auf alle Rechenzentren zu beschränken. Sie können alle Rechenzentren für ein Servicekonto erkennen, einschließlich der „passiven", indem Sie die Eigenschaft auf **true**festlegen. Weitere Informationen finden Sie unter: MID-Server-Eigenschaften erstellen

Unterschiede gemäß der Service-Account-Discovery nach der Bereitstellung von Muster für Discovery und Service-Mapping Version 1.15.0:

- Für neu erkannten Service-Account:
  - Wenn die Eigenschaft MID-Server auf **„false"** (Standard) festgelegt ist, sammelt Discovery die Azure -Ressourcen nur für „aktive" Rechenzentren. Die Tabelle **„Azure-Rechenzentren"** enthält nur Datensätze zu „aktiven" Rechenzentren für den Serviceaccount. Im Discovery-Protokoll (Registerkarte „Geräte") werden nur „aktive" Rechenzentren angezeigt.
  - Wenn die Eigenschaft MID-Server auf **true**festgelegt ist, sammelt Discovery die Azure -Ressourcen für alle Rechenzentren. Die Tabelle „Rechenzentren" Azure enthält alle Rechenzentrumsdatensätze für den Serviceaccount. Im Discovery-Protokoll (Registerkarte „Geräte") werden alle Rechenzentren („aktiv" und „passiv") angezeigt.
- Für einen Serviceaccount, der vor Muster für Discovery und Service-Mapping Version 1.15.0 erkannt wurde:
  - Wenn die Eigenschaft MID-Server auf **„false"** (Standard) festgelegt ist, sammelt Discovery die Azure -Ressourcen nur für „aktive" Rechenzentren. Die Tabelle **„Azure-Rechenzentren"** enthält alle Rechenzentrumsdatensätze für den Serviceaccount. Im Discovery-Protokoll (Registerkarte „Geräte") werden nur „aktive" Rechenzentrenangezeigt.
  - Wenn die Eigenschaft MID-Server auf **true**festgelegt ist, sammelt Discovery die Azure -Ressourcen für alle Rechenzentren. Die Tabelle **„Azure-Rechenzentren"** enthält alle Rechenzentrumsdatensätze für den Serviceaccount. Im Discovery-Protokoll (Registerkarte „Geräte") werden alle Rechenzentren („aktiv" und „passiv") angezeigt.

Für Verwaltungsgruppen erkennt Azure Cloud-Discovery alle Azure -Rechenzentren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Discovery des Hardwaretyps

Die Hardwaretyp-Discovery hat in den letzten Jahren drei Modelländerungen erfahren. Das Modell 1.15.0 löst das **Hardwaretypmuster** und das **VM-** Muster nach dem **Azure Datacenter Discovery-** Muster aus. Ab Muster für Discovery und Service-Mapping Plugin-Version 1.15.0 erkennt Cloud-Discovery, welches Hardwaretyp-Modell verwendet wird, und startet nur eines der beiden Muster: **Hardwaretyp (LP)** oder **Cloud-Hardwaretyp (LP)**.

Migration zum neuen Azure Hardwaretyp-Discovery-Modell – Anwendungsfälle

Muster für Discovery und Service-Mapping **Version**	**Status der Hardwaretyp-Migration**	**Welches Muster führtsaus?**	**Discovery-Ergebnis**
Vor 1.0.75	Nicht zum neuen Modell migriert	**Hardware Type (LP)** -Muster	Der erstellte CI-Typ: [cmdb_ci_compute_template]
Muster für Discovery und Service-Mapping Version 1.0.75	Die Migration zum neuen Modell erfolgt per Migrationsskript. Siehe KB0955939	**Hardware Type (LP)** -Muster	Der erstellte CI-Typ: [cmdb_ci_cloud_hardware_type]
Muster für Discovery und Service-Mapping Version 1.6.0	Der Hardwaretyp für das neue Modell wird standardmäßig bereitgestellt und mit der folgenden Systemeigenschaft aktiviert: *sn_itom_pattern.use a single hardware type for cloud datacenters*. Weitere Informationen finden Sieunter KB1285337 .	Gemäß KB1285337- Flow-Diagramm	Der erstellte CI-Typ: Gemäß KB1285337
Muster für Discovery und Service-Mapping 1.15.0	Der Hardwaretyp „Neues Modell“ wird OOB-fähig mit der folgenden Systemeigenschaft bereitgestellt: *sn_itom_pattern.use a single hardware type for cloud datacenters*. Weitere Informationen finden Sieunter KB1285337 .	Der Flow entspricht der Beschreibung in KB1285337 . Es wird jedoch nur ein Muster ausgeführt. Das Muster, das zum ordnungsgemäßen Beenden von verwendet wurde, wird nicht ausgeführt.	Entweder **das Hardware Type-Muster (LP)** oder **das Cloud-Hardware Type-Muster (LP)** führtsaus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Lizenz-Discovery für verwaltete SQL-Instanzen

Die Azure DataBase (LP)-Mustererweiterung für **die Azure SQL Managed Instance-Lizenz** erkennt Lizenzinformationen für Azure SQL Managed Instance und füllt den Lizenztyp in der Tabelle „Schlüsselwert“ [cmdb_key_value] des Clouddatenbank-CI [cmdb_ci_cloud_database] aus.

Erforderliche Plugins und Anwendungen

- Software Asset Management Professional für Microsoft
- Visibility Content

Erkannte Ressourcen und Beziehungen

Ressourcen, die mit der Lizenz für die Mustererweiterung Azure DataBase (LP) Azure SQL Managed Instanceerkannt wurden

Beziehungen, die mit der Mustererweiterung Azure SQL Managed Instances-Lizenz fürAzure DataBase (LP) erkannt wurden

Azure Marketplace-Discovery

Das Muster „Azure - Marketplace LB (LP)“ erkennt die folgenden Azure Marketplace-Produkte:

- SaaS
- Azure-Anwendung
- Virtuelle Maschine

Hinweis: Das Muster erkennt nur virtuelle Computer (VMs), die aus Images von Drittanbietern oder Commercial Marketplace erstellt wurden.

Erkannte Ressourcen und Beziehungen

Ressourcen, die vom Muster „Azure – Marktplatz LB (LP)“ erkannt werden

Beziehungen, die mit dem Muster „Azure – Marktplatz LB (LP)“ erkannt wurden

Von Discovery während der horizontalen Erkennung erfasste Daten

Ressourcen, die mithilfe des Musters „Microsoft Azure - Application LB (LP)“ erkannt wurden

Feld	Beschreibung
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für das Lastenausgleichsmodul kein Name angegeben ist
location	Pfad des Lastenausgleichsmoduls
state	Aktueller Status des Lastenausgleichsmoduls
install_status	Bereitstellungsstatus der Ressource
ip_address	IP-Adresse des Lastenausgleichsmoduls.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
fqdn	Der vollqualifizierte Domänenname des Lastenausgleichsmoduls.
dns_name	Der DNS-Name des Lastenausgleichmoduls
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
IP-Adresse des Cloud-Lastenausgleichsmoduls [cmdb_ci_cloud_lb_ipaddress]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
lb_id	Ein eindeutiger Bezeichner für das Lastenausgleichsmodul.
ip_address	IP-Adresse des Lastenausgleichsmoduls
ip_address_type	Der Typ der IP-Adresse, die privat oder öffentlich sein kann.
fqdn	Der vollqualifizierte Domänenname des Lastenausgleichsmoduls.
Kommentare	Bezeichner zur internen Verwendung (Löschungsstrategie)
install_status	Bereitstellungsstatus der Ressource
Load Balancer-Pool [cmdb_ci_lb_pool]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für den Pool des Lastenausgleichsmoduls kein Name angegeben ist
location	Pfad des Pools des Lastenausgleichsmoduls
install_status	Bereitstellungsstatus der Ressource
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
Load Balancer-Service [cmdb_ci_lb_service]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für den Service des Lastenausgleichsmoduls kein Name angegeben ist
location	Pfad des Services des Lastenausgleichsmoduls
port	TCP-Port, den der Service des Lastenausgleichsmoduls abhört
install_status	Bereitstellungsstatus der Ressource
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)

Ressourcen, die mithilfe des Musters „Microsoft Azure - Availability Set (LP)“ erkannt wurden

Feld	Beschreibung
Verfügbarkeitssatz [cmdb_ci_availability_set]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
name	Name oder ID, wenn für die Verfügbarkeitszone kein Name angegeben ist
install_status	Bereitstellungsstatus der Ressource

Vom Muster Microsoft Azure - Verfügbarkeitszonen (LP) erkannte Ressourcen

Feld	Beschreibung
Verfügbarkeitszone [cmdb_ci_av availability_zone]	
object_id	{Ort} + "-" + {ZoneNum}
name	{Ort} + "-" + {ZoneNum}

Ressourcen, die mithilfe des Musters „Microsoft Azure - Classic LB (LP)“ erkannt wurden

Feld	Beschreibung
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für das Lastenausgleichsmodul kein Name angegeben ist
location	Pfad des Lastenausgleichsmoduls
state	Aktueller Status des Lastenausgleichsmoduls
install_status	Bereitstellungsstatus der Ressource
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
IP-Adresse des Cloud-Lastenausgleichsmoduls [cmdb_ci_cloud_lb_ipaddress]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
lb_id	Ein eindeutiger Bezeichner für das Lastenausgleichsmodul.
ip_address	IP-Adresse des Lastenausgleichsmoduls
ip_address_type	Typ der IP-Adresse, kann privat oder öffentlich sein
fqdn	Der vollqualifizierte Domänenname des Lastenausgleichsmoduls.
Kommentare	Bezeichner zur internen Verwendung (Löschungsstrategie)
install_status	Bereitstellungsstatus der Ressource
Load Balancer-Service [cmdb_ci_lb_service]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für den Service des Lastenausgleichsmoduls kein Name angegeben ist
location	Pfad des Services des Lastenausgleichsmoduls

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
port	TCP-Port, den der Service des Lastenausgleichsmoduls abhört
install_status	Bereitstellungsstatus der Ressource
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
Load Balancer-Pool [cmdb_ci_lb_pool]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für den Pool des Lastenausgleichsmoduls kein Name angegeben ist
location	Pfad des Pools des Lastenausgleichsmoduls
install_status	Bereitstellungsstatus der Ressource
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)

Ressourcen, die mithilfe des Musters „Microsoft Azure - Hardware Type (LP)“ erkannt wurden

Feld	Beschreibung
Hardwaretyp [cmdb_ci_hardware_type]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für den Hardwaretyp kein Name angegeben ist
local_storage_gb	Speicher, der dieser Vorlage zugewiesen ist
cores	Die Standardanzahl der Kerne für den Instanztyp
memory_mb	Speichergröße, die dieser Vorlage zugewiesen ist
vcpus	Anzahl der dieser Vorlage zugewiesenen CPU-Kerne

Ressourcen, die mithilfe des Musters „Microsoft Azure - Host (LP)“ erkannt wurden

Feld	Beschreibung
Host [cmdb_ci_cloud_host]	
name	Name oder ID, wenn für den Host kein Name angegeben ist
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
host_type	Typ des Hosts
cloud_vendor	Anbieter der Cloud: Microsoft Azure
virtual	Virtueller Host: False

Ressourcen, die mithilfe des Musters „Microsoft Azure - Image (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Image-Tabelle [cmdb_ci_os_template]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für das Image kein Name angegeben ist
location	Pfad des Image
guest_os	Betriebssystem, das sekundär zum Betriebssystem ist
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
image_source	Quelle des Betriebssystem-Image

Hinweis: Wenn Sie die Tabelle „Image“ [cmdb_ci_os_template] zum Speichern von Cloud-BS-Images verwenden, können Sie eine ungewöhnlich große Anzahl von Datensätzen feststellen. Um dieses Problem zu vermeiden, können Sie die erkannten BS-Images in der Tabelle „Cloud-Image“ [cmdb_ci_cloud_os_image] speichern. Weitere Informationen finden Sie unter Aktiviert die Discovery von Cloud-BS-Images.

Ressourcen, die mithilfe des Musters „Microsoft Azure - Network and Subnet (LP)“ erkannt wurden

Feld	Beschreibung
Cloud-Netzwerk [cmdb_ci_network]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für das Cloud-Netzwerk kein Name angegeben ist
location	Pfad des Netzwerks
state	Aktueller Status des Netzwerks
install_status	Bereitstellungsstatus der Ressource
cidr	CIDR-Darstellung des Netzwerks Beispiel: 10.0.0.0/24
Cloud-Subnetz [cmdb_ci_cloud_subnet]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für das Cloud-Subnetz kein Name angegeben ist
location	Bezeichner zur internen Verwendung (Löschungsstrategie)
state	Der aktuelle Status des Subnetzes.
install_status	Bereitstellungsstatus der Ressource
cidr	CIDR-Darstellung des Subnetzes. Beispiel: 10.0.0.0/24

Ressourcen, die mithilfe des Musters „Microsoft Azure - NIC (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für die Netzwerkschnittstelle kein Name angegeben ist
location	Pfad der Netzwerkschnittstelle
install_status	Bereitstellungsstatus der Ressource
state	Aktueller Status der Netzwerkschnittstelle
public_ip	Die Adresse der Elastic IP-Adresse, die an die Netzwerkschnittstelle gebunden ist
private_ip	Die IPv4-Adresse der Netzwerkschnittstelle im Subnetz
Primär	True/False. Definiert, ob die Netzwerkschnittstelle die primäre Netzwerkschnittstelle ist oder nicht
mac_address	MAC-Adresse der Netzwerkschnittstelle
public_dns	Öffentlicher DNS-Name der Netzwerkschnittstelle

Ressourcen, die mithilfe des Musters „Microsoft Azure - Private Gateway (LP)“ erkannt wurden

Feld	Beschreibung
Virtual Private Gateway [cmdb_ci_virtual_pvt_gateway]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für das private Gateway kein Name angegeben ist
location	Pfad des privaten Gateway
connection_type	Typ der vom Gateway unterstützten VPN-Verbindung
operational_status	Status der Ressource
install_status	Bereitstellungsstatus der Ressource
Virtual Private Gateway-Endpunkt [cmdb_ci_endpoint_vpg]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für den Endpunkt kein Name angegeben ist
location	Pfad des Endpunkts
connection_type	Typ der vom Gateway unterstützten VPN-Verbindung

Ressourcen, die mithilfe des Musters „Microsoft Azure - Public IP (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für die IP-Adresse kein Name angegeben ist
location	Pfad der IP-Adresse
state	Aktueller Status der IP-Adresse
public_ip_address	Adresse der Elastic IP-Adresse
public_dns	Öffentlicher DNS-Name
install_status	Bereitstellungsstatus der Ressource

Ressourcen, die mithilfe des Musters „Microsoft Azure - Resource Group (LP)“ erkannt wurden

Feld	Beschreibung
Ressourcengruppe [cmdb_ci_resource_group]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für die Ressourcengruppe kein Name angegeben ist
location	Pfad der Ressourcengruppe
state	Aktueller Status der Ressourcengruppe
install_status	Bereitstellungsstatus der Ressource

Ressourcen, die mithilfe des Musters „Microsoft Azure - Route Table (LP)“ erkannt wurden

Feld	Beschreibung
Weiterleitungstabelle [cmdb_ci_route_table]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für die Weiterleitungstabelle kein Name angegeben ist
location	Pfad der Weiterleitungstabelle
install_status	Bereitstellungsstatus der Ressource
state	Aktueller Status der Weiterleitungstabelle

Ressourcen, die mithilfe des Musters „Microsoft Azure - Security Group (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für die Sicherheitsgruppe kein Name angegeben ist
location	Pfad der Sicherheitsgruppe
state	Aktueller Status der Sicherheitsgruppe
install_status	Bereitstellungsstatus der Ressource

Ressourcen, die mithilfe des Musters „Microsoft Azure - SQL Server (LP)“ erkannt wurden

Feld	Beschreibung
VM-Instanz [cmdb_ci_vm_instance]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
location	Pfad der VM-Instanz

Ressourcen, die mithilfe des Musters „Microsoft Azure - Storage Account (LP)“ erkannt wurden

Feld	Beschreibung
Cloud-Speicherkonto [cmdb_ci_cloud_storage_account]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für das Speicherkonto kein Name angegeben ist
location	Pfad des Speicherkontos
sku_name	Name der SKU (für Sicherungshäufigkeit)
install_status	Bereitstellungsstatus der Ressource
state	Aktueller Status des Speicherkontos

Ressourcen, die mithilfe des Musters „Microsoft Azure - Storage Containers (LP)“ erkannt wurden

Feld	Beschreibung
Speichervolume [cmdb_ci_storage_volume]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für das Speichervolume kein Name angegeben ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
location	Pfad des Speichervolume
volume_id	Bezeichner, der die Volume-ID als Wert enthält
volume_container	Name des Containers
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
Status	Status der Ressource
Block-Endpunkt [cmdb_ci_endpoint_block]	
name	Name oder ID, wenn für den Block-Endpunkt kein Name angegeben ist
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.

Ressourcen, die mithilfe des Musters „Microsoft Azure - Storage Volume (LP)“ erkannt wurden

Feld	Beschreibung
Speichervolume [cmdb_ci_storage_volume]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für das Speichervolume kein Name angegeben ist
volume_id	Der Volumetyp. Beispiel: • `gp2` für Allzweck-SSD • `io1` für bereitgestellte IOPS-SSD • `st1` für durchsatzoptimierte HDD • `sc1` für Cold-HDD • `standard` für magnetische Volumes
location	Pfad des Speichervolume
state	Aktueller Status des Speichervolume
install_status	Bereitstellungsstatus der Ressource
size	Größe des Volume
size_bytes	Die Größe des Volumes (Byte)
storage_type	Beispiel: der hartcodierte Wert „block“.
Kommentare	Bezeichner zur internen Verwendung (Löschungsstrategie)

Ressourcen, die mithilfe des Musters „Microsoft Azure - Sub Account (LP)“ erkannt wurden

Feld	Beschreibung
Cloud-Servicekonto [cmdb_ci_cloud_service_account]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
account_id	Der eindeutige Bezeichner (ID) des Kontos
name	Name oder ID, wenn für das Servicekonto kein Name angegeben ist
datacenter_type	cmdb_ci_azure_datacenter
discovery_credentials	Referenzfeld zu den zugehörigen Microsoft Azure-Anmeldeinformationen.
datacenter_url	URL des Rechenzentrums
parent_account	Verweis auf das Primärkonto, falls vorhanden
is_master_account	Boolesches Attribut, das angibt, ob es sich hierbei um das Primärkonto handelt oder nicht

Ressourcen, die mithilfe des Musters „Microsoft Azure - Virtual Machine (LP)“ erkannt wurden

Feld	Beschreibung
VM-Instanz [cmdb_ci_vm_instance]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für die Instanz kein Name angegeben ist
location	Pfad der Instanz
install_status	Bereitstellungsstatus der Ressource
state	Der aktuelle Status der Instanz
vm_inst_id	Die ID der Instanz
nics	Anzahl der für die Instanz verfügbaren NICs
disks	Anzahl der Datenträger, die an die Instanz angeschlossen sind
disks_size	Gesamtgröße der angehängten Datenträger
memory	Für die Instanz verfügbare Arbeitsspeicher (MBs)
CPUs	Anzahl der für die Instanz verfügbaren CPUs
Block-Endpunkt [cmdb_ci_endpoint_block]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für den Endpunkt kein Name angegeben ist
location	Pfad des Endpunkts
host	Die öffentliche IPv4-Adresse, die der Instanz zugewiesen wurde, falls zutreffend
Speichervolume [cmdb_ci_storage_volume]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für das Speichervolume kein Name angegeben ist
location	Pfad des Speichervolume
Anmerkungen	Bezeichner zur internen Verwendung (Löschungsstrategie)
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
location	Pfad der Netzwerkschnittstelle
VNIC-Endpunkt [cmdb_ci_endpoint_vnic]	
object_id	Ein eindeutiger Bezeichner, der von Microsoft Azure für diese Ressource zugewiesen wird.
name	Name oder ID, wenn für den Endpunkt kein Name angegeben ist
location	Pfad des Endpunkts

Im Abschnitt „Mustererweiterung“ erkennen Sie die Bring Your Own License (BYOL) oder die enthaltenen Lizenzen für Windows-VMs und RHEL-VMs.

Feld	Beschreibung
Schlüsselwert [cmdb_key_value]	
Schlüssel [key]	Der Schlüssel ist eine der Optionen: • Windows_OS_License_Type_automatic • RHEL_OS_License_Type_automatic • SQL_Server_Lizenz_Typ_automatisch
Wert [value]	Der Wert ist eine der Optionen: • BYOL • Lizenz enthalten
CI [ci]	Verweis auf den Datensatz der VM-Instanz.
Klasse	Die Klasse ist *`Virtual Machine Instance`*.

Vom Muster Microsoft Azure WebSite (LP) und vom Muster Microsoft Azure WebSite erkannte Ressourcen

Feld	Beschreibung
Cloud-Ressource [cmdb_ci_cloud_webserver]	
Name [name]	Der Name des Azure Webservers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Objekt-ID [object_id]	Die ID des Azure Webservers.
IP-Adresse [ip_address]	Die IP-Adresse des Webservers.
FQDN [fqdn]	Der vollqualifizierte Domänenname (FQDN) des Webservers.
Anbieter [vendor]	Der Lieferant ist MicrosoftMicrosoft Azure Event Hubs.
Installationsstatus [install_status]	Der Installationsstatus des Webservers.
Status [state]	Der Betriebsstatus des Webservers.
Betriebsstatus [operational_status]	Der Betriebsstatus des Webservers.
IP-Adresse [cmdb_ci_ip_address]	
Name [name]	Die IP-Adresse des Webservers.
IP-Adresse [ip_address]	Die IP-Adresse des Webservers.
FQDN [fqdn]	Der vollqualifizierte Domänenname (FQDN)
Anbieter [vendor]	Der Lieferant ist MicrosoftMicrosoft Azure Event Hubs.
Installationsstatus [install_status]	Der Installationsstatus.
Betriebsstatus [operational_status]	Der Betriebsstatus.
Schlüsselwert [cmdb_key_value]	
Schlüssel [key]	Der Azure Schlüsselwertname.
Wert [value]	Der Schlüsselwertwert Azure

Ressourcen, die mit dem Muster Azure DataBase (LP) erkannt wurden

Cloud-Datenbank [cmdb_ci_cloud_database]

Feld	Beschreibung
Vollständig qualifizierter Domänenname [fqdn]	Der FQDN, den Microsoft Azure Ihrer Datenbank zugewiesen hat.
Name [name]	Der Name der Datenbank, die Sie in Microsoft Azure erstellt haben.
Objekt-ID [object_id]	Der Identifikationsname der Datenbank.
Betriebsstatus [operational_status]	Der Betriebsstatus der Datenbank.
Typ [type]	Der Typ der von Ihnen erstellten Datenbank.
Status [state]	Der Status der Datenbank: Verfügbar oder Beendet.
Anbieter [vendor]	Der Lieferantenname lautet Azure.
Version [version]	Die Version der Datenbank.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud-Datenbank [cmdb_ci_cloud_database] (Fortsetzung)

Feld	Beschreibung
Kategorie [category]	Die SKU-Familie (Lagerhaltungseinheit).

Cloud-Hardwaretyp [cmdb_ci_cloud_hardware_type]

Feld	Beschreibung
Objekt-ID [object_id]	Ein eindeutiger Bezeichner für den Hardwaretyp.
Name [name]	Name für den Hardwaretyp.
vCPUs [vcpus]	Anzahl der virtuellen CPU-Kerne.
Anbieter [provider]	Anbieter für den Hardwaretyp: Azure.

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
Netzmaske [netmask]	Netzmaske der Datenbank Azure.

Ressourcen, die mit der Lizenz für die Mustererweiterung Azure DataBase (LP) **Azure SQL Managed Instance**erkannt wurden

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	SQL_Server_PaaS_Managed_Instance_License_Type_automatic
Wert [value]	Lizenztyp. Folgendes ordnet die Portallizenz Azure den Werten ServiceNow zu: • **Azure-Hybridvorteil**: BYOL • **Pay-as-y-go**: Lizenz enthalten • **Hybrid-Failover-Rechte**: Hybrid-Failover
Konfigurationselement [configuration_item]	cmdb_ci_cloud_database

Serverlose Hardware [cmdb_ci_serverless_hardware]

Feld	Beschreibung
Objekt-ID [object_id]	Objekt-ID der Cloud-Datenbank Azure.
Name [name]	SKU-Name.
Cloud-Anbieter [cloud_vendor]	Cloud-Anbieter der serverlosen Hardware: MS Azure.
Anzahl der CPU-Kerne [cpu_core_count]	Anzahl der virtuellen Kerne (vCores).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Serverlose Hardware [cmdb_ci_serverless_hardware] (Fortsetzung)

Feld	Beschreibung
CPU-Core-Thread [cpu_core_thread]	Anzahl der vCores.
CPU-Anzahl [cpu_count]	Anzahl der vCores.
Kategorie [category]	vCore-Einkaufsmodell.
Unterkategorie [Unterkategorie]	SKU-Stufe.
Hosttyp [host_type]	Hosttyp: PaaS

Ressourcen, die vom Muster „Azure – Marktplatz LB (LP)“ erkannt werden

Bereitgestelltes Marktplatzprodukt [cmdb_ci_deployed_marketplace_product]

Feld	Beschreibung
Name [name]	Name der Cloud-Ressource, normalerweise das Marktplatzangebot oder der SKU-Name.
Objekt-ID [object_id]	Eine eindeutige Ressourcen-ID der Cloud-Ressource.
Ressourcentyp [resource_type]	Service im Cloud-Marketplace. Beispiel: Microsoft.compute/virtualmaschines.
Planname [plan_name]	Abrechnungs- oder SKU-Plan für eine Ressource aus dem Cloud Marketplace. Beispiel: Pay-as-Du-Go.
Markt [market]	ISO-Code (International Organization for Standardization) des geografischen Marktes, in dem die Ressource im angegebenen Markt verkauft wird. Beispiel: US oder EU.
Organisations-ID [organization_id]	Ein eindeutiger Bezeichner für die Organisation oder den Herausgeber, die bzw. der die Marketplace-Ressource besitzt.

Marketplace – Produktdetails [marketplace_product_details]

Feld	Beschreibung
Produktcode [product_code]	Ein eindeutiger Produktcode der Ressource im Cloud Marketplace.
Herausgebername [publisher_name]	Organisation oder Person, die für die Erstellung und Bereitstellung des Produkts oder Services verantwortlich ist.
Version [version]	Release-Nummer oder Iteration des Produkts.
Bereitgestellt am [deployed_on]	Referenziert die Tabelle „Bereitgestelltes Marktplatzprodukt“ [cmdb_ci_deployed_marketplace_product].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Schlüssel [key]	Azure Schlüsselwertname.
Wert [value]	Azure Schlüsselwertwert.

CI-Beziehungen

Beziehungen, die mithilfe des Musters „Microsoft Azure - Application LB (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_load_balancer	Eigentümer von::Eigentum von	cmdb_ci_cloud_lb_ipaddress
cmdb_ci_cloud_load_balancer	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_lb_service	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_cloud_subnet	Enthält::Enthalten in	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_cloud_load_balancer

Beziehungen, die mithilfe des Musters „Microsoft Azure - Availability Set (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_availability_set
cmdb_ci_azure_datacenter	Enthält::Enthalten in	cmdb_ci_availability_set

Mit dem Muster Microsoft Azure - Verfügbarkeitszone (LP) erkannte Beziehungen

CI	Beziehung	CI
cmdb_ci_azure_datacenter	Enthält::Enthalten in	cmdb_ci_availability_zone
cmdb_ci_availability_zone	Enthält::Enthalten in	cmdb_ci_vm_instance

Beziehungen, die mithilfe des Musters „Microsoft Azure - Classic LB (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_load_balancer	Eigentümer von::Eigentum von	cmdb_ci_cloud_lb_ipaddress

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_cloud_load_balancer	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_lb_service	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_lb_service
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_cloud_load_balancer

Beziehungen, die mithilfe des Musters „Microsoft Azure - Hardware Type (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_compute_template	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

Beziehungen, die mithilfe des Musters „Microsoft Azure - Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_host	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_cloud_host
cmdb_ci_vm_instance	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_cloud_host

Beziehungen, die mithilfe des Musters „Microsoft Azure - Image (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_os_template

Beziehungen, die mithilfe des Musters „Microsoft Azure - Network and Subnet (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_network	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_network	Enthält::Enthalten in	cmdb_ci_cloud_subnet
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_network

Beziehungen, die mithilfe des Musters „Microsoft Azure - NIC (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_nic	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_nic
cmdb_ci_cloud_subnet	Enthält::Enthalten in	cmdb_ci_nic

Beziehungen, die mithilfe des Musters „Microsoft Azure - Private Gateway (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_endpoint_vpg	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_virtual_pvt_gateway
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_virtual_pvt_gateway
cmdb_ci_virtual_pvt_gateway	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_network	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_vpg

Beziehungen, die mithilfe des Musters „Microsoft Azure - Public IP (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_public_ipaddress	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_nic	Enthält::Enthalten in	cmdb_ci_cloud_public_ipaddress
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_cloud_public_ipaddress

Beziehungen, die mithilfe des Musters „Microsoft Azure - Resoure Group (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_azure_datacenter	Enthält::Enthalten in	cmdb_ci_resource_group

Beziehungen, die mithilfe des Musters „Microsoft Azure - Route Table (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_route_table	Enthält::Enthalten in	cmdb_ci_route

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_route_table	Enthält::Enthalten in	cmdb_ci_network
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_route_table
cmdb_ci_azure_datacenter	Enthält::Enthalten in	cmdb_ci_route_table

Beziehungen, die mithilfe des Musters „Microsoft Azure - Security Group (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_subnet	Verwendet::Verwendet von	cmdb_ci_compute_security_group
cmdb_ci_network	Enthält::Enthalten in	cmdb_ci_compute_security_group
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_compute_security_group
cmdb_ci_compute_security_group	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

Beziehungen, die mithilfe des Musters „Microsoft Azure - Storage Account (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_cloud_storage_account
cmdb_ci_cloud_storage_account	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

Beziehungen, die mithilfe des Musters „Microsoft Azure - Storage Containers (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_endpoint_block	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_storage_volume
cmdb_ci_cloud_storage_account	Enthält::Enthalten in	cmdb_ci_storage_volume
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_storage_volume
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

Beziehungen, die mithilfe des Musters „Microsoft Azure - Storage Volume (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_storage_volume
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_azure_datacenter

Beziehungen, die mithilfe des Musters „Microsoft Azure - Sub Account (LP)“ erkannt wurden

Mit dem Muster „Microsoft Azure - Sub Account (LP)“ werden keine Beziehungen erkannt.

Beziehungen, die mithilfe des Musters „Microsoft Azure - Virtual Machine (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_vm_instance	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_vnic
cmdb_ci_endpoint_vnic	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_nic
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_compute_template
cmdb_ci_resource_group	Enthält::Enthalten in	cmdb_ci_vm_instance
cmdb_ci_vm_instance	Endpunkt verwenden an::Endpunkt verwenden von	cmdb_ci_endpoint_block
cmdb_ci_endpoint_block	Endpunkt implementieren in::Endpunkt implementieren von	cmdb_ci_storage_volume
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_os_template
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_availability_set	Enthält::Enthalten in	cmdb_ci_vm_instance

Beziehungen, die anhand der Muster Microsoft Azure WebSite (LP) und Microsoft Azure WebSite erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_webserver	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_cloud_webserver	Besitzt::Eigentum	cmdb_ci_ip_address

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_key_value	Nur Referenz	cmdb_ci_cloud_webserver

Mit dem Azure DataBase (LP) Pattern erkannte Beziehungen.

CI	Beziehung	CI
cmdb_ci_cloud_database	Besitzer: Im Besitz von	cmdb_ci_ip_address
cmdb_ci_cloud_database	Enthält::Enthalten in	cmdb_ci_database
cmdb_ci_cloud_database	Gehostet auf::Gehostet	cmdb_ci_azure_datacenter
cmdb_ci_database	Bereitgestellt von::Bereitgestellt	cmdb_ci_compute_template
cmdb_ci_database	Bereitgestellt von::Bereitgestellt	cmdb_ci_cloud_hardware_type
cmdb_ci_compute_template	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_ci_compute_template	Gehostet auf::Hostet	cmdb_ci_cloud_hardware_type

Beziehungen, die mit der Mustererweiterung **Azure SQL Managed Instances-Lizenz für**Azure DataBase (LP) erkannt wurden

CI	Beziehung	CI
cmdb_ci_cloud_database	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_serverless_hardware
cmdb_ci_serverless_hardware	Gehostet auf::Hostet	cmdb_ci_azure_datacenter
cmdb_key_value	Nur Referenz	cmdb_ci_cloud_database

Beziehungen, die mit dem Muster „Azure – Marktplatz LB (LP)“ erkannt wurden

CI	Beziehung	CI
Bereitgestelltes Marketplace-Produkt [cmdb_ci_deployed_marketplace_product]	Erweitert::Erweitert um	VM-Objekt [cmdb_ci_vm_object]
Bereitgestelltes Marketplace-Produkt [cmdb_ci_deployed_marketplace_product]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_sevice_account]
Bereitgestelltes Marketplace-Produkt [cmdb_ci_deployed_marketplace_product]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]
Marketplace – Produktdetails [marketplace_product_details]	Referenzen	Bereitgestelltes Marketplace-Produk [cmdb_ci_deployed_marketplace_

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Bereitgestelltes Marketplace-Produk [cmdb_ci_deployed_marketplace_

Events, die während der horizontalen Erkennung mithilfe von Discovery erkannt wurden

Discovery verwendet Muster, um Events zu suchen, die für Microsoft Azure-Komponenten erstellt wurden. Wenn Events vorhanden sind, die auf eine Statusänderung in einer der Microsoft Azure-Komponenten hinweisen, wird die Erkennung von Microsoft Azure-Komponenten anhand der Muster ausgelöst.

Muster, die für die Event-Erkennung verwendet wurden

Muster	CI-Klasse
Azure Availability Set Event	Verfügbarkeitssatz [cmdb_ci_availability_set]
Azure Application LB Event	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Azure NIC Event	Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]
Azure Security Group Event	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]
Azure Public IP Event	Öffentliche Cloud-IP-Adresse [cmdb_ci_cloud_public_ipaddress]
Azure Resource Group Event	Ressourcengruppe [cmdb_ci_resource_group]

Von Discovery während der horizontalen Erkennung erfasste Tag-Informationen

Beim Ausführen der Muster werden Tag-Informationen erfasst, um die Tabelle „cmdb_key_value“ zu füllen. Jedes Tag bezieht sich auf ein CI, das während der Erkennung erkannt wurde. Die Tag-Erkennung erfolgt im Erweiterungsabschnitt jedes Musters.

Daten, die von Service-Mapping während der tagbasierten Erkennung erfasst wurden

Service-Mapping verwendet die Tag-basierte Discovery, um Serviceinstanzzuordnungen einschließlich der Cloud-Komponenten zu erstellen. Im Lieferumfang von Service-Mapping befinden sich folgende vorkonfigurierte CI-Beziehungen, die für Tag-basierte Discovery verwendet werden. Diese CI-Beziehungen sind im ServiceNow Store ab Version 1.0.68 verfügbar.

CI	Beziehung	CI
Konfigurationselement [cmdb_ci]	Gehostet auf::Hostet	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
Logisches Rechenzentrum [cmdb_ci_logical_datacenter]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]

MicrosoftMicrosoft Azure Event Hubs Azure Application Gateway-Erkennung

Die ServiceNow Discovery-Anwendung verwendet das Azure Application Gateway HD-Muster für die Erkennung dieses Produkts, während die Service-Mapping-Anwendung das

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Application Gateway mithilfe des Azure Application Gateway TD-Musters (LBS) erkennt. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Azure-Prinzipal-Anmeldeinformationen

Erstellen Sie auf der ServiceNow Platform ein Servicekonto für die Cloud-Erkennung. Legen Sie für die Konto-ID den Azure-Service-Prinzipal fest, der in der Microsoft Azure-Konsole angezeigt wird.

Berechtigungen

Weisen Sie in der Microsoft Azure-Konsole einem Benutzer die Leserrolle zu.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Zusätzliche Informationen
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	
name	Name des Azure Application Gateway
Fqdn	Vollqualifizierter Domänenname des Azure Application Gateway
Object_id	Die ID des Gateways
Install_status	Installationsstatus des Azure Application Gateway
state	Status des Azure Application Gateway
Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]	
name	IP-Adresse des Azure Application Gateway
Object_id	ID des Azure Application Gateway
ipaddress _type	Typ der IP-Adresse, kann privat oder öffentlich sein
ip_address	IP-Adresse des Azure Application Gateway
state	Status der IP-Adresse des Azure Application Gateway
operational_state	Betriebsstatus der IP-Adresse des Azure Application Gateway
install_status	Installationsstatus der IP-Adresse des Azure Application Gateway
Load Balancer-Service [cmdb_ci_lb_service]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Zusätzliche Informationen
Seriennummer	ID des Azure Application Gateway-Service
port	TCP-Port, den der Azure Application Gateway-Service abhört
name	FQDN mit der Portnummer des Azure Application Gateway-Service gemäß dieser Syntax: <fqdn>:<port>.
ip_address	IP-Adresse des Azure Application Gateway, auf dem der Service ausgeführt wird
object_id	ID des Azure Application Gateway-Service
operational_state	Betriebsstatus des Azure Application Gateway-Service

CI-Beziehungen

Diese Beziehungen sollen die Azure Application Gateway-Erkennung unterstützen:

CI	Beziehung	CI
Load Balancer-Service [cmdb_ci_lb_service]	Gehostet auf::Hostet	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]
Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]	Eigentümer von::Eigentum von	Cloud LB-IP-Adresse [cmdb_ci_cloud_lb_ipaddress]
Ressourcengruppe [cmdb_ci_resource_group]	Enthält::Enthalten in	Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Verbindungen, die Service-Mapping bei der Erkennung von oben nach unten erkennt

Service-Mapping führt die Erkennung von oben nach unten des Azure Application Gateway im Kontext von Anwendungsservices durch. Service-Mapping erkennt die ausgehenden http-Verbindungen vom Azure Application Gateway-Service zu Poolmitgliedern, z. B. virtuellen Computern.

Zugehörige Informationen

Cloud-REST-Abfrage für Cloud-Computing-Geräte definieren

MicrosoftMicrosoft Azure Event Hubs Azure Bestands-Discovery

Die Anwendung ServiceNow Discovery verwendet das Muster Azure Inventar, um nach Ressourcen zu suchen, die über Azureverfügbar sind. Verwenden Sie dieses Muster für Azure -Ressourcen, die kein dediziertes Muster haben, wie z. B. Azure -Funktionen oder Azure Application Gateway. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Mit dem Muster Azure Bestand können Sie bis zu 10.000 Ressourcen erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Azure Serviceprinzipal

Vergewissern Sie sich, dass der Serviceprinzipal Azure konfiguriert ist. Weitere Informationen finden Sie unter Erkennung von Azure-Clouds

Berechtigungen

Für Versionen 1.3.0 und höher:

Gewähren Sie in der Microsoft Azure-Konsole einem Benutzer mit der Rolle „API Management Service-Leser“ Berechtigungen zum Ausführen der folgenden REST POST-Anforderung:

```
„https://management.<resource url> /providers/
microsoft.resourcegraph/resources?api-version=2022-10-01“
```

<resource url>– Die URL variiert je nach Azure-Kontotyp, z. B. „azure.com“ oder Adresse eines Behördenstandorts.

Für Versionen 1.0.99 und früher:

Stellen Sie in der Microsoft Azure-Konsole einem Benutzer die Rolle „API Management Service-Leser“ mit Berechtigungen zum Ausführen der folgenden REST GET-Anforderung zur Verfügung:

```
"https://management.azure.com/subscriptions/<subscription id>/
resources"
```

Cloud Discovery-Zeitplan erstellen

Erstellen Sie einen Zeitplan für das relevante Azure-Service-Account wie in beschrieben Zeitpläne zur Erkennung von Cloud-Ressourcen in Cloud-Discovery erstellen

Erkennung des Azure-Bestands mithilfe der Aufnahmeliste für Ressourcen feintunen

Wenn Ihre Bereitstellung über anwenderdefinierte Muster für die Azure-Discovery verfügt, stellen Sie sicher, dass Sie Azure-Ressourcen nicht zweimal erkennen.

Hinweis: Wenn Sie die Tabelle [pre_resource_whitelist] leer lassen, werden alle Ressourcen vom Muster gefüllt, was zu Leistungsproblemen führen kann.

1. Stellen Sie sicher, dass der Anwendungsbereich „Discovery and Service Mapping Patterns“ ist:
   a. Navigieren zu **Einstellungen** > **Entwickler**.
   b. Wählen Sie `Discovery and Service Mapping Patterns` aus der Liste **Anwendung** aus.
2. Navigieren zu **Systemdefinitionen** > **Tabellen**.
3. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie unter **Zugehörige Links**auf **Liste anzeigen**.
5. Wählen Sie Ressourcentypen aus, für die Sie benutzerdefinierte Muster haben, und wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option `Löschen` aus.

Die Aufnahmeliste für Cloud-Bestandsressourcen ist mit allgemeinen Services vordefiniert. Sie können die Aufnahmeliste um zusätzliche Ressourcentypen erweitern, die das Muster erkennen soll. Die Namen dieser Ressourcentypen müssen den Benennungskonventionen der entsprechenden Anbieter entsprechen.

Hinweis: Wenn Sie die sofort einsatzbereite Aufnahmeliste ändern, wird sie in Anwendungsupdates nicht mehr automatisch aktualisiert. Sie müssen die anwenderdefinierte Liste selbst verwalten.

1. Öffnen Sie die Tabelle „Aufnahmeliste für Cloud-Bestandsressourcen“ [sa_cloud_inventory_resource_whitelist].
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
Cloud-Anbieter	Der Lieferant des Ressourcentyps: Azure.
Ressourcentyp	Der Wert des Ressourcentyps Azure.
Anwendung	Der Anwendungsbereich: Discovery and Service Mapping Patterns

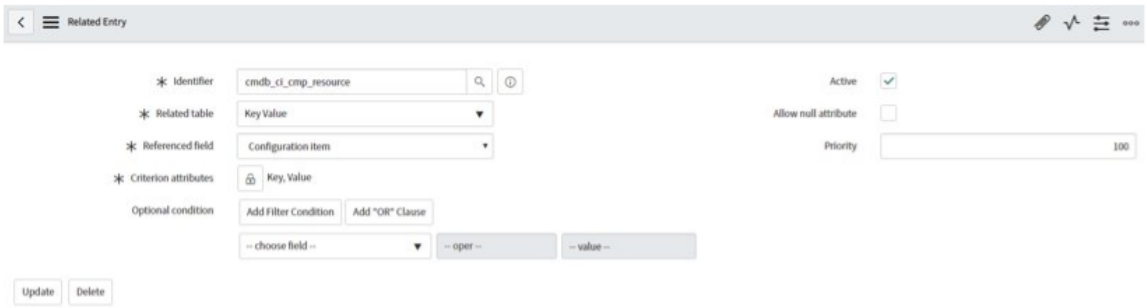
Die Änderungen werden beim nächsten Ausführen des Musters angewendet.

Ändern Sie die mit ServiceNow verbundenen Einträge.

1. Navigieren Sie zu **Zugehörige Einträge**.
2. Klicken Sie auf **Neu**.
3. Geben Sie als Bezeichner **cmdb_ci_cmp_resource** ein.
4. Wählen Sie für die zugehörige Tabelle **Schlüsselwert [cmdb_key_value]** aus.
5. Wählen Sie für das referenzierte Feld **Configuration Item** aus.
6. Fügen Sie für die Kriteriumsattribute **Schlüssel** und **Wert** hinzu.

   Möglicherweise müssen Sie auf das Schlosssymbol klicken, um die Kriteriumsattribute anzuzeigen und zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Zusätzliche Informationen
Cloud-Ressource [cmdb_ci_cmp_resource]	
Name	Ein beschreibender Name zum Erkennen der Azure-Ressource
Ressourcentyp	Der Typ der Ressource, z. B. Netzwerk, Lastenausgleichsmodul
Objekt-ID	Die ID der Azure-Ressource.
Beschreibung	Der während der Erkennung ausgefüllte Text, der angibt, dass diese Ressource in Azure verfügbar ist
Schlüsselwert [cmdb_key_value]	
Key	Der Azure-Tag-Schlüsselname.
Wert	Der Azure-Tag-Wertname.

CI-Beziehungen

Diese Beziehungen werden erstellt, um die Discovery von Azure Functions zu unterstützen:

CI	Beziehung	CI
Cloud-Ressource [cmdb_ci_cmp_resource]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]

Zugehörige Informationen

https://learn.microsoft.com/en-us/azure/governance/resource-graph/reference/supported-tables-resources

MicrosoftMicrosoft Azure Event Hubs Azure Functions-Erkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping verwenden die Muster Azure - Functions (LP) und Azure - Functions TD (LP), um Azure-Funktions-Apps zu erkennen und im Kontext von Anwendungsservices zuzuordnen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Azure Functions detaillierte Informationen

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Azure Service-Account

Konfigurieren Sie den Serviceaccount Azure. Weitere Informationen finden Sie unter Richten Sie ein Cloud-Konto für ein Azure

Azure-Prinzipal-Anmeldeinformationen

Erstellen Sie auf der Now Platform ein Servicekonto für die Cloud-Erkennung. Legen Sie für die Konto-ID den Azure-Service-Prinzipal fest, der in der Microsoft Azure-Konsole angezeigt wird. Weitere Informationen finden Sie unter: Anmeldeinformationen für Azure-Cloud erstellen

Berechtigungen

Weisen Sie in der Microsoft Azure-Konsole einem Benutzer die API-Management-Service-Leserrolle zu.

Führen Sie Azure die Cloud-Discovery aus

Ausführliche Informationen finden Sie unter: Erkennung von Azure-Clouds

Discovery-Zeitplan erstellen

Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Azure Function [cmdb_ci_cloud_function]	
name	Der Name der Funktions-App.
Object_id	Die ID der Funktions-App.
ip_address	Die IP-Adresse der Funktions-App.
fqdn	Der vollqualifizierte Domänenname (FQDN) der Funktions-App.
code_location_url	Die URL des Quellcodes der Funktions-App.
app_function_state	Der Status der Funktions-App.
operational_status	Der Betriebsstatus der Funktions-App.
install_status	Der Installationsstatus der Funktions-App.

CI-Beziehungen

Diese Beziehungen sollen die Azure Functions-Erkennung unterstützen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Azure Functions [cmdb_ci_cloud_function]	Gehostet auf::Hostet	Azure-Rechenzentrum [cmdb_ci_azure_datacenter]

Verbindungen, die von Service-Mapping während der Erkennung von oben nach unten gefunden werden

Service-Mapping kann die folgenden Verbindungen erkennen:

- Verbindungen mit den folgenden Datenbanken: MSSql, MySql, MongoDB und Documentum
- HTTP-Verbindungen, die zur Azure Functions-Umgebung gehören, z. B. https://scenario4-hop1-azure-funktion.azurewebsites.net

Hinweis: Service-Mapping durchsucht Java-Klassen/JAR-Dateien und Binärdateien nicht nach möglichen Informationen über ausgehende HTTP-Verbindungen von Azure Functions. Wenn Java-Klassen/JAR-Dateien und Binärdateien die einzige Informationsquelle zu einigen ausgehenden HTTP-Verbindungen sind, findet Service-Mapping diese HTTP-Verbindungen nicht.

Zugehörige Informationen

Cloud-REST-Abfrage für Cloud-Computing-Geräte definieren

Azure DNS Zonen-Discovery

Die Anwendung ServiceNow Discovery und Service-Mapping verwenden die Muster Azure - DNS-Zonen (LP) und Azure DNS-Zonen-Datensätze (LP), um Azure Domain Name System (DNS) -Definitionen (Zonen und ihre jeweiligen Datensätze) zu erkennen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Detaillierte Informationen zu Azure DNS Zonen

Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte

Azure Service-Account

Konfigurieren Sie den Serviceaccount Azure. Weitere Informationen finden Sie unter Richten Sie ein Cloud-Konto für ein Azure

Azure Anmeldeinformationen des Prinzipals

Erstellen Sie auf der Now Platform ein Servicekonto für die Cloud-Erkennung. Legen Sie die Account-ID auf den Serviceprinzipal Azure fest, wie er in der Microsoft Azure-Konsole angezeigt wird. Weitere Informationen finden Sie unter: Anmeldeinformationen für Azure-Cloud erstellen

Berechtigungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie in der Microsoft-Konsole Azure einen Benutzer mit der Rolle „API Management-Serviceleser“ bereit.

Führen Sie Azure die Cloud-Discovery aus

Ausführliche Informationen finden Sie unter: Erkennung von Azure-Clouds

Discovery-Zeitplan erstellen

Erstellen Sie einen Zeitplan für die relevanten Azure-Service-Accounts wie beschrieben in: Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge

Von Discovery während der horizontalen Erkennung erfasste Daten

Ressourcen, die vom Muster Azure - DNS Zones (LP) erkannt wurden

Tabelle und Feld	Zusätzliche Information
DNS-Zone [cmdb_ci_dns_zone]	
name	Der Name der DNS-Zone.
number_of_recordsets	Die Anzahl der in der DNS-Zone definierten Datensätze.
operational_status	Der Betriebsstatus der DNS-Zone.
state	Der Status der DNS-Zone.
install_status	Der Installationsstatus der DNS-Zone.
Kommentare	Das Feld für allgemeine Kommentare.

Ressourcen, die vom Muster Azure - DNS Zone Records (LP) erkannt wurden

Feld	Beschreibung
DNS - Alias [cmdb_ci_dns_alias]	
Name	Der Name des DNS-Alias-Datensatzes.
Kategorie	Die Kategorie des DNS-Alias.
Status	Der Status des DNS-Alias.

Feld	Beschreibung
DNS -Name [cmdb_ci_dns_name]	
name	Der Name des DNS-Namendatensatzes.
Fqdn	Der im DNS-Datensatz definierte vollständig qualifizierte Domänenname
ip_address	Die im DNS-Datensatz definierte IP-Adresse.
operational_status	Der Betriebsstatus des DNS-Datensatzes.
state	Der Status des DNS-Datensatzes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
install_status	Der Installationsstatus des DNS-Datensatzes.
Kommentare	Das Feld für allgemeine Kommentare.

CI-Beziehungen

Diese Beziehungen werden erstellt, um die Erkennung von Azure DNS Zonen (LP) zu unterstützen:

CI	Beziehung	CI
[cmdb_ci_resource_group]	Enthält :: Enthalten in	[cmdb_ci_dns_zone]

Diese Beziehungen werden erstellt, um die Discovery von Azure DNS Zone Recordsets (LP) zu unterstützen:

CI	Beziehung	CI
[cmdb_ci_dns_zone]	Enthält :: Enthalten in	[cmdb_ci_dns_name]
[cmdb_ci_dns_zone]	Enthält :: Enthalten in	[cmdb_ci_dns_alias]
[cmdb_ci_dns_name]	Verwendet von :: Verwendet	[cmdb_ci_dns_alias]

MicrosoftMicrosoft Azure Event Hubs Discovery von Zertifikaten einer Zertifizierungsstelle (Certificate Authority, CA).

Mit dem Muster „MicrosoftMicrosoft Azure Event Hubs CA – Certificate Management“ können von der Anwendung ServiceNow Discovery Zertifikate der MicrosoftMicrosoft Azure Event Hubs-Zertifizierungsstelle (Certificate Authority, CA) erkannt werden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

CMDB CI-Klassenmodelle und Muster für Discovery und Service-Mapping Store Apps

Stellen Sie sicher, dass die Store-Apps CMDB CI-Klassenmodelle und Muster für Discovery und Service-Mapping (neueste Versionen) installiert sind.

Zertifizierungsstellen-Prozess

Stellen Sie sicher, dass auf dem Hostcomputer der CA-Prozess ausgeführt wird.

Discovery-Anmeldeinformationen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass Sie über die Anmeldeinformationen für die Ausführung von Discovery auf dem Host-Computer verfügen, auf dem der CA-Prozess ausgeführt wird.

Zeitplan für Erkennung ohne Server erstellen

Erstellen Sie einen Erkennungszeitplan, um eine gezielte Erkennung von Zertifikaten von MicrosoftMicrosoft Azure Event Hubs CA durchzuführen. Das Muster „MicrosoftMicrosoft Azure Event Hubs CA – Certificate Management“ wird durch einen Zeitplan für serverlose Erkennung ausgelöst, bei dem der Host verwendet wird, auf dem der CA-Prozess ausgeführt wird.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
2. Wählen Sie **Neu** aus, und füllen Sie das Formular aus.

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Name des Discovery-Zeitplans. Zum Beispiel `Erkennung MS CA`
Erkannt	Der Typ des Produkts. Wählen Sie **Zertifikat**.
MID-Server	Name des MID-Servers
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

3. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.
4. Wählen Sie die Registerkarte **Ausführungsmuster ohne Server**, dann **Neu**, und füllen Sie das Formular aus.

Hinweis: Discovery verwendet jedes Ausführungsmuster, um bis zu 20.000 Zertifikate zu erkennen. Erstellen Sie für Bereitstellungen mit mehr als 20.000 Zertifikaten mehrere Ausführungsmuster.

Formular „Ausführungsmuster ohne Server“

Feld	Beschreibung
Name	Name dieses serverlosen Ausführungsmusters. Zum Beispiel `Erkennung MS CA`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Muster	Name des auszuführenden Musters: MicrosoftMicrosoft Azure Event Hubs CA Certificate Management.
Proxyhost	Vollständig qualifizierter Domänenname (FQDN) des Computers, auf dem Ihre Zertifizierungsstelle ausgeführt wird.
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

5. Konfigurieren Sie unter **Startprogrammparameter für Discovery-Muster** die Startparameter mit den entsprechenden Werten.

Formular „Startprogrammparameter für Discovery-Muster“

Feld	Beschreibung
template_list	OID-Wert einer einzelnen Zertifikatvorlage.
start_offset	Nummer des Zertifikats, ab dem die Erkennung gestartet werden soll. Wenn Sie mehrere serverlose Ausführungsmuster für Bereitstellungen mit mehr als 20.000 Zertifikaten erstellen, verwenden Sie `1` für das erste Ausführungsmuster, `20001` für das zweite Ausführungsmuster und so weiter. Dieses Feld ist relevant für Bereitstellungen mit mehr als 20.000 Zertifikaten.
ip	IP des Servers, auf dem die Zertifikate bereitgestellt werden.

Weitere Informationen finden Sie unter Serverlose Erkennung.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten CA-Konfigurationsdaten umfassen die folgenden Tabellen und Felder.

Feld	Beschreibung
Basiskonfigurationselement-Cluster [CMDB]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Seriennummer	Seriennummer, die dem CI zugeordnet ist
Konfigurationselement [cmdb_ci]	
operational_status	Betriebsstatus des Clusterknotens
Eindeutiges Zertifikat [cmdb_ci_certificate]	
Fingerabdruck	Hashwert des Zertifikats
Fingerabdruck-Algorithmus	Algorithmus, der zum Hashen des Zertifikats verwendet wird
Allgemeiner Antragstellername	Identifiziert den Hostnamen/die Domäne, der/die dem Zertifikat zugeordnet ist
Eindeutiger Antragstellername	Identifizierende Informationen des Antragstellers
Eindeutiger Ausstellername	Eindeutiger Name des Ausstellers
Kommentare	Enthält eine lesbare Beschreibung für Benutzer
Verlängerungsnachverfolgung	Gibt an, ob Aufgaben mit Priorität 1 oder Priorität 3 für ablaufende Zertifikate erstellt werden sollen
Zertifikatvorlage	Die Zertifikatvorlage, die die Richtlinien und Regeln definiert, die eine CA verwendet, wenn eine Anforderung für ein Zertifikat empfangen wird
Fingerabdruck des Zertifikats	Der eindeutige Bezeichner für Zertifikate in Anwendungen beim Treffen von Vertrauensentscheidungen, in Konfigurationsdateien und bei der Anzeige in Schnittstellen.
Allgemeiner Ausstellername	Allgemeiner Name des Ausstellers
Gültig ab	Gültigkeitsstartzeitraum des Zertifikats
Seriennummer	Seriennummer des Zertifikats
Antragstellerland	Ländercode des Antragstellers mit zwei Buchstaben.
Antragstellerorganisation	Organisation des Antragstellers
Bearbeiter	Entität, die das Zertifikat signiert und ausgestellt hat
Antragsteller-Organisationseinheit	Organisationseinheit des Antragstellers
Alternativer Antragstellername	Liste vollqualifizierter Domänennamen, die durch das Zertifikat gesichert werden
Gültig bis	Gültigkeitsendzeitraum des Zertifikats
Name	Name des CI
Status	Lebenszyklusstatus des Zertifikats.
Stammaussteller	Stammentität, die das Zwischenzertifikat signiert und ausgestellt hat
Antragsteller-Ort	Ort des Antragstellers
Antragstellerstatus	Status des Antragstellers

Zusätzliche Daten, die von der Store-Release-Version Muster für Discovery und Service-Mapping Februar 2024 erfasst wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Eindeutiges Zertifikat [cmdb_ci_certificate]	
Anforderungstyp [request_type]	Das Format, das zum Anfordern des Zertifikats verwendet wird.
Datum der Anforderungsübermittlung [request_submission_date]	Das Datum, an dem die Zertifikatanforderung übermittelt wurde.
Datum der Anforderungslösung [request_resolution_date]	Das Datum, an dem die Zertifikatanforderung von der Zertifizierungsstelle gelöst wurde.
Datum der Widerrufsanforderung [request_revocation_date]	Das Datum, an dem das Zertifikat widerrufen wurde. Dieses Feld wird nur für widerrufene Zertifikate ausgefüllt.
Gültigkeitsdatum des Widerrufs [effektive_revocation_date]	Das Datum, an dem das Zertifikat effektiv widerrufen wurde, indem es der CRL (Zertifikatwiderrufsliste) hinzugefügt wurde. Dieses Feld wird nur für widerrufene Zertifikate ausgefüllt.
Widerrufsgrund [revocation_reason]	Der Grund für das Widerrufen des Zertifikats. Dieses Feld wird nur für widerrufene Zertifikate ausgefüllt.
Name der anfordernden Person [requester_name]	Der Name der Person, die das Zertifikat angefordert hat.
Registrierungskennzeichnungen für Vorlage [template_enrollment_flags]	Informationen zum Zertifikat, auf die von der Zertifizierungsstelle oder dem Besitzer des Zertifikats reagiert werden muss. Um weitere Informationen zu erhalten, suchen Sie auf der offiziellen Microsoft-Dokumentationswebsite nach dem Fehlercode.

CI-Beziehungen

Mit dem Muster MicrosoftMicrosoft Azure Event Hubs CA – Zertifikatverwaltung werden keine CI-Beziehungen erstellt.

Erkennung des NetApp SolidFire-Speichersystems

ServiceNow Discovery verwendet das Erkennungsmuster „NetApp SolidFire storage system“, um Cluster und Knoten im SolidFire-Speichersystem zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Voraussetzungen

Store-App Discovery and Service Mapping Patterns

Stellen Sie sicher, dass die Store-App Discovery and Service Mapping Patterns (Version 1.0.74) installiert ist.

Berechtigungen für Basisauthentifizierung

Stellen Sie sicher, dass zur Authentifizierung der Element-API-Aufrufe die Anmeldeinformationen für die Standardauthentifizierung konfiguriert sind. Speichern Sie die folgenden Anmeldeinformationen für den SolidFire Cluster-Administrator als Basisauthentifizierung, um einen ordnungsgemäßen Zugriff zu gewährleisten:

- „sys_user_group“
- clusterAdmins
- reporting
- drives

MID-Server

Stellen Sie sicher, dass der MID Server auf das Zielgerät zugreifen kann.

Discovery-Anmeldeinformationen

Stellen Sie sicher, dass Sie über die Anmeldeinformationen für die Ausführung von Discovery auf dem Hostcomputer verfügen, auf dem das SolidFire-Speichersystem ausgeführt wird.

Zeitplan für Erkennung ohne Server erstellen

Erstellen Sie einen Erkennungszeitplan, um eine gezielte Erkennung von SolidFire-Clustern und -Knoten durchzuführen.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

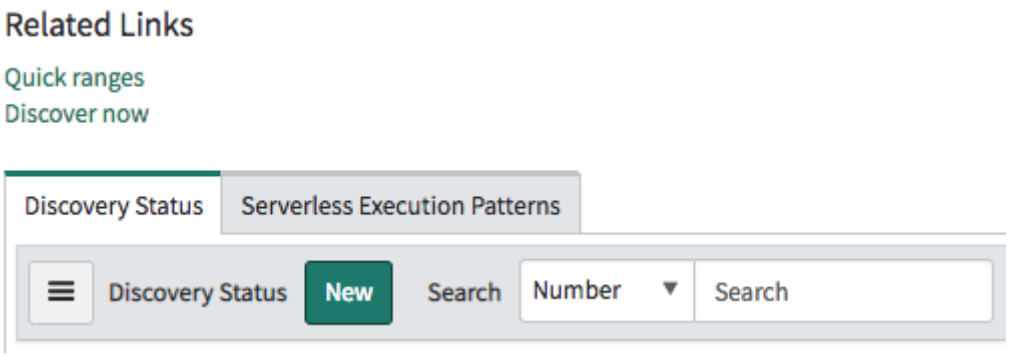
Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Name des Discovery-Zeitplans. Zum Beispiel: `Erkennung SolidFire`.
Erkennen	Erkennungstyp. Wählen Sie **Ohne Server** aus.
MID-Server	Name des MID-Servers
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

3. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf die Registerkarte **Ausführungsmuster ohne Server**, **Neu**, und füllen Sie das Formular aus.



Formular „Ausführungsmuster ohne Server“

Feld	Beschreibung
Name	Name dieses serverlosen Ausführungsmusters. Zum Beispiel: `Muster für SolidFire-Speicher`.
Muster	Name des auszuführenden Musters: NetApp SolidFire Storage System
Proxy-Host	Vollständig qualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. Geben Sie **Global** an.
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

5. Konfigurieren Sie unter **Startprogrammparameter für Discovery-Muster** die Startparameter mit den entsprechenden Werten. Stellen Sie sicher, dass die Management-IP des Clusters und der Alias für die Anmeldeinformationen definiert sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten SolidFire-Konfigurationsdaten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Hauptkonfigurationselement [cmdb_ci_storage_server]	
name	Name des CI
serial_number	Seriennummer, die dem CI zugeordnet ist
firmware_version	Firmwareversion des CI
ip_address	IP-Adresse für das CI
short_description	Kurze Textbeschreibung des CI
manufacturer	Hersteller des Geräts

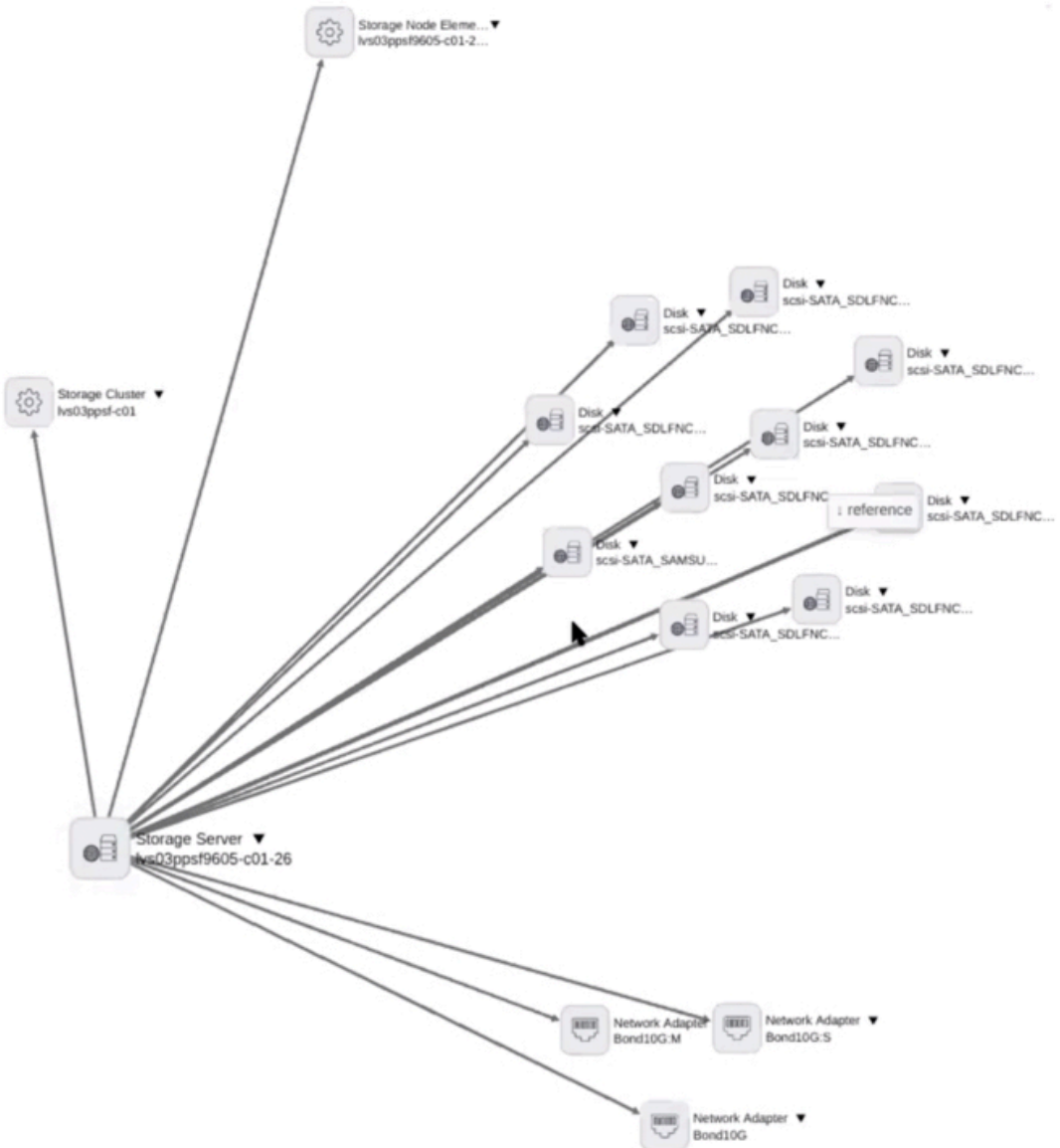
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
model_id	Modell-ID des Geräts
os_version	Version des auf dem CI ausgeführten Betriebssystems
os	Auf dem CI ausgeführtes Betriebssystem
Speichercluster [cmdb_ci_storage_cluster]	
ip_address	IP-Adresse des Speicherclusters
manufacturer	Hersteller des Geräts
short_description	Kurze Textbeschreibung des CI
cluster_version	Version der Element-OS-API, die im Cluster ausgeführt wird
name	Name des CI
Speicherclusterknoten [cmdb_ci_storage_cluster_node]	
name	Name des CI
operational_status	Gibt an, ob sich das Gerät im aktiven Status befindet
Cluster	Referenz für das Cluster-CI
Speicherknotenelement [cmdb_ci_storage_node_element]	
short_description	Kurze Textbeschreibung des CI
manufacturer	Hersteller des Geräts
serial_number	Seriennummer, die dem CI zugeordnet ist
model_id	Modell-ID des Geräts
chassis_type	Typ des Gehäuses, das den Server enthält
ram	Speichergröße des CI
cpu_type	CPU-Typ
cpu_manufacturer	Hersteller der CPU
Speicherdatenträger [cmdb_ci_disk]	
name	Name des CI
device_id	ID des Geräts
serial_number	Seriennummer, die dem CI zugeordnet ist
storage_type	Speichertyp
size_bytes	Verfügbare Speichergröße in Byte
manufacturer	Hersteller des Geräts
model_id	Modell-ID des Geräts
Computer	Referenz für den Speicherserver
Netzwerkadapter [cmdb_ci_network_adapter]	
name	Name des CI
ip_address	IP-Adresse für das CI
netmask	Netzmaske des Servers, der den Netzwerkadapter hostet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
mac_address	Die MAC-Adresse des Netzwerkadapters
IP-Adresse [cmdb_ci_ip_address]	
ip_address	IP-Adresse für das CI
netmask	Netzmaske des Servers, der das CI hostet

Die Dependency Views-Zuordnung zeigt alle erkannten Cluster und Knoten des SolidFire-Speichersystems in Ihrer Organisation und die Beziehungen zwischen ihnen an.



CI-Beziehungen

CI	Beziehung/Referenz	CI
Speichercluster	Cluster von::Cluster	Knoten des Speicherclusters
Knoten des Speicherclusters	Gehostet auf::Hostet	Element des Speicherknotens
Element des Speicherknotens	Verwaltet von::Verwaltet	Speichercluster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

CI	Beziehung/Referenz	CI
Speicherserver (Haupt-CI)	Zugeordnet zu::Zugeordnet von	Element des Speicherknotens
Speicherserver (Haupt-CI)	Wird ausgeführt auf::Wird ausgeführt	Speichercluster
Speicherserver (Haupt-CI)	Enthält::Enthalten in	Datenträger

Next-Generation Cisco Firewall-Erkennung

Die ServiceNow Discovery-Anwendung verwendet das Erkennungsmuster Next-Generation Cisco Firewall, um Cisco-Firewalls zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Das Erkennungsmuster verwendet eine Reihe von SNMP-Aufrufen, um die Cisco-Firewalls zu finden. Discovery verwendet das Muster zum Ausführen der horizontalen Erkennung.

Sie können dieses Muster auf der Now Platform® mit Madrid -Release oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass Ihr Netzwerkfirewallgerät über SNMP-Zugriff verfügt.
- Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow-Instanz.
- Fügen Sie den SNMP-System-OID-Datensatz für das Cisco-Gerät der Instanz ServiceNow hinzu. Aktualisieren Sie Folgendes:
  - Klassifizierer: Cisco-Firewall
  - Klasse: Cisco-Firewall-Gerät
- Stellen Sie das Muster wie folgt bereit:
  1. Laden Sie Firewall-Erweiterungsklassen aus ServiceNow Storeherunter, und installieren Sie sie. Die App fügt die neuen CMDB-Klassen hinzu, die für die Erkennung der Netzwerkfirewall erforderlich sind.
  2. Laden Sie die Anwendung Discovery and Service Mapping Patterns aus dem ServiceNow Store herunter, und installieren Sie sie.
  3. Synchronisieren Sie das Muster mit dem entsprechenden MID-Server.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
IP-Firewall [cmdb_ci_ip_firewall] – Enthält alle Netzwerk-Firewalls	
Name [name]	Hostname

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Seriennummer [serial_number]	Seriennummer des Geräts
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Firewall-Gerät [cmdb_ci_firewall_device] – Abstrakte Klasse für herstellerspezifische Firewalls	
Name [name]	Hostname
Seriennummer [serial_number]	Seriennummer des Geräts
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Cisco-Firewall-Gerät [cmdb_ci_firewall_device_cisco] - Enthält physische Cisco-Firewalls	
Name [name]	Hostname
Seriennummer [serial_number]	Seriennummer des Geräts
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardwarestatus [hardware_status]	Hardwarestatus
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

Diese Abhängigkeitsansichten-Zuordnung auf dem Cisco Firewall-CI zeigt das Cisco Firewall-Gerät.

CI-Beziehungen

Diese Beziehungen sollen die Cisco Firewall-Erkennung unterstützen:

CI	Beziehung	CI
Firewall-Gerät [cmdb_ci_firewall_device]	Erweitert::Erweitert um	IP-Firewall [cmdb_ci_ip_firewall]
	Enthält::Enthalten in	Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]
Cisco-Firewall-Gerät [cmdb_ci_firewall_device_cisco]	Erweitert::Erweitert um	Firewall-Gerät [cmdb_ci_firewall_device]
Firewall-Gerätegruppe [cmdb_ci_firewall_device_group]	Erweitert::Erweitert um	CMDB-CI [cmdb_ci]
	Mitglieder::Mitglied von	Firewall-Gerät [cmdb_ci_firewall_device]
	Enthält::Enthalten in	Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]
Firewall-Manager [cmdb_ci_firewall_manager]	Erweitert::Erweitert um	CMDB-CI [cmdb_ci]
	Verwaltet::Verwaltet von	Firewall-Gerät [cmdb_ci_firewall_device]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
	Enthält::Enthalten in	Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]
Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]	Erweitert::Erweitert um	CMDB-CI [cmdb_ci]

SNMP-basierte Discovery der Netzwerk-Firewall der nächsten Generation Fortinet .

Die Anwendung Muster für Discovery und Service-Mapping verwendet das Muster Next Generation Fortinet Network Firewall, um Fortinet -Firewalls über eine Reihe von SNMP-Aufrufen zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Das Muster der Fortinet-Netzwerkfirewall der nächsten Generation verwendet eine Reihe von SNMP-Aufrufen, um die Fortinet -Firewalls zu finden. Discovery verwendet das Muster für die Horizontal-Discovery.

Hinweis: Nur die REST-basierte Firewall-Discovery-Methode Fortinet findet FortiGate-VDOMs. Die SNMP-basierte Fortinet -Firewall-Discovery-Methode erkennt sie nicht. Informationen zur REST-basierten Fortinet -Firewall und zur Discovery von FortiGate Virtual Domains (VDOMs) finden Sie unter Fortinet Firewall und FortiGate VDOM REST-basierte Discovery.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Informationen zu den Firewalls Fortinet und den Versionen, die Sie erkennen können, finden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Voraussetzungen

Stellen Sie sicher, dass die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Stellen Sie den SNMP-Zugriff sicher

Stellen Sie sicher, dass Ihr Firewall-Gerät Fortinet über SNMP-Zugriff verfügt.

Konfigurieren Sie SNMP-Anmeldeinformationen

Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow-Instanz. Weitere Informationen finden Sie unter SNMP-Anmeldeinformationen .

Fügen Sie den SNMP-System-OID-Datensatz der Instanz ServiceNow hinzu

Fügen Sie der ServiceNow-Instanz den OID-Datensatz des SNMP-Systems für das Fortinet-Gerät hinzu. Aktualisieren Sie Folgendes:

- Klassifizierer: Fortinet-Firewall
- Klasse: Fortinet-Firewall-Gerät

Führen Sie eine Horizontal-Discovery aus

Weitere Informationen finden Sie unter Erkennungen im Netzwerk ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das Next Generation Fortinet Network Firewall-Muster ausgeführt wird.

Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet]

Feld	Beschreibung
Name [name]	Hostname
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung des Fortinet -Firewall-Clusters.
Modellnummer [model_number]	Modellnummer des Geräts
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]

Feld	Beschreibung
Name [name]	Hostname
Seriennummer [serial_number]	Seriennummer des Geräts
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurze Beschreibung des Geräts.
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse der Fortinet -Firewall.
Netzmaske [netmask]	Netzmaske der Fortinet -Firewall.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

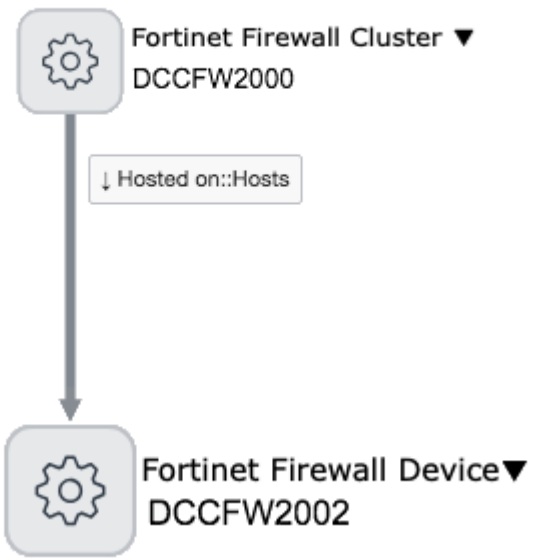
Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
Alias [alias]	Vom Anwender zugewiesener Name für den Netzwerkadapter.
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
Name [name]	Name des Netzwerkadapters

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	Name des Domain Name System (DNS)
IP-Adresse [ip_address]	IP-Adresse des DNS.

Diese Zuordnung Abhängigkeitsansichten auf dem CI des Firewall-Geräts Fortinet zeigt den Firewall-Cluster Fortinet, zu dem sie gehört.



CI-Beziehungen

Diese Beziehungen werden erstellt, um die Firewall-Discovery von Fortinet zu unterstützen.

CI	Beziehung	CI
Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet]	Erweitert::Erweitert um	Firewall-Cluster [cmdb_ci_firewall_cluster]
Fortinet-Firewall-Cluster [cmdb_ci_firewall_cluster_fortinet]	Gehostet auf::Hostet	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Erweitert::Erweitert um	Firewall-Gerät [cmdb_ci_firewall_device]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]	Verwendet::Verwendet von	Routerschnittstelle [dscy_router_interface]
IP-Adresse [cmdb_ci_ip_address]	Referenzen	Netzwerkadapter [cmdb_ci_network_adapter]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Routerschnittstelle [dscy_router_interface]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]
Seriennummer [cmdb_serial_number]	Referenzen	Fortinet-Firewall-Gerät [cmdb_ci_firewall_device_fortinet]

Next-Generation Juniper Network Firewall-Erkennung

Die ServiceNow Discovery-Anwendung verwendet das Erkennungsmuster Next-Generation Juniper Network Firewall, um Juniper-Firewalls zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Das Erkennungsmuster verwendet eine Reihe von SNMP-Aufrufen, um die Juniper-Netzwerk-Firewalls zu finden. Discovery verwendet das Muster zum Ausführen der horizontalen Erkennung.

Sie können dieses Muster auf der Now Platform® mit Madrid -Release oder höher verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass Ihr Netzwerkfirewallgerät über SNMP-Zugriff verfügt.
- Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow-Instanz.
- Fügen Sie den SNMP-System-OID-Datensatz für das Juniper-Gerät der Instanz ServiceNow hinzu. Aktualisieren Sie Folgendes:
  - Klassifizierer: Juniper-Firewall
  - Klasse: Juniper-Firewall-Gerät

Stellen Sie das Muster wie folgt bereit:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Laden Sie CMDB CI Class Models: Release 1.10.0 aus dem ServiceNow Store herunter, und installieren Sie es. Die App fügt die neuen CMDB-Klassen hinzu, die für die Erkennung der Netzwerkfirewall erforderlich sind. Weitere Informationen finden Sie unter Firewall-Erweiterungsklassen .
2. Laden Sie das Erkennungsmuster aus dem ServiceNow Store herunter, und installieren Sie es.
3. Synchronisieren Sie das Muster mit dem entsprechenden MID-Server.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
IP-Firewall [cmdb_ci_ip_firewall] – Enthält alle Netzwerk-Firewalls	
Name [name]	Hostname
Seriennummer [serial_number]	Seriennummer des Geräts
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Firewall-Gerät [cmdb_ci_firewall_device] – Abstrakte Klasse für herstellerspezifische Firewalls	
Name [name]	Hostname
Seriennummer [serial_number]	Seriennummer des Geräts
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem

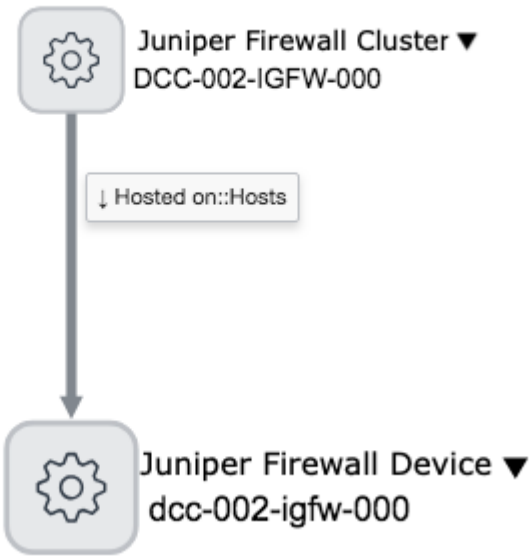
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Juniper-Firewall-Gerät [cmdb_ci_firewall_device_juniper] – Enthält physische Juniper-Firewalls	
Name [name]	Hostname
Seriennummer [serial_number]	Seriennummer des Geräts
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
Betriebsstatus [operational_status]	Gibt an, ob sich das Gerät im aktiven Status befindet
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Firmware [firmware_version]	Firmware-Version
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Firewall-Cluster [cmdb_ci_firewall_cluster] – Abstrakte Klasse für einen herstellerspezifischen Firewall-Cluster.	
Name [name]	Hostname
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Juniper-Firewall-Cluster [cmdb_ci_firewall_cluster_juniper] – Enthält Juniper-Firewall-Cluster	
Name [name]	Hostname
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname
IP-Adresse [ip_address]	IP-Adresse
Hersteller [manufacturer]	Gerätehersteller
Beschreibung [short_description]	Kurzbeschreibung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Modellnummer [model_number]	Modellnummer des Geräts
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems

Diese Abhängigkeitsansichtszuordnung auf dem Juniper-Firewall-Geräte-CI zeigt das Juniper-Firewall-Cluster, zu dem es gehört.



CI-Beziehungen

Diese Beziehungen sollen die Juniper-Netzwerk-Firewall-Erkennung unterstützen:

CI	Beziehung	CI
Firewall-Cluster [cmdb_ci_firewall_cluster]	Erweitert::Erweitert um	Cluster [cmdb_ci_cluster]
Juniper-Firewall-Cluster [cmdb_ci_firewall_cluster_juniper]	Erweitert::Erweitert um	Firewall-Cluster [cmdb_ci_firewall_cluster]
	Gehostet::Gehostet auf	Juniper-Firewall-Gerät [cmdb_ci_firewall_device]
Firewall-Gerät [cmdb_ci_firewall_device]	Erweitert::Erweitert um	IP-Firewall [cmdb_ci_ip_firewall]
	Enthält::Enthalten in	Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]
Juniper-Firewall-Gerät [cmdb_ci_firewall_device]	Erweitert::Erweitert um	Firewall-Gerät [cmdb_ci_firewall_device]
Firewall-Gerätegruppe [cmdb_ci_firewall_device_group]	Erweitert::Erweitert um	CMDB-CI [cmdb_ci]
	Mitglieder::Mitglied von	Firewall-Gerät [cmdb_ci_firewall_device]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
	Enthält::Enthalten in	Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]
Firewall-Manager [cmdb_ci_firewall_manager]	Erweitert::Erweitert um	CMDB-CI [cmdb_ci]
	Verwaltet::Verwaltet von	Firewall-Gerät [cmdb_ci_firewall_device]
	Enthält::Enthalten in	Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]
Firewall-Sicherheitsrichtlinie [cmdb_ci_firewall_security_policy]	Erweitert::Erweitert um	CMDB-CI [cmdb_ci]

Nutanix Acropolis-Discovery

Die Anwendung ServiceNow Discovery verwendet das Muster „Nutanix-Komponenten“, um nach Komponenten der Lösung Nutanix Acropolis zu suchen, die Nutanix Prism Central Version 5.10 oder Nutanix Prism Element 5.9 enthält. Das Muster „Nutanix-VM-Ereignis“ findet Ereignisse, die für virtuelle Maschinen (VMs) in der Bereitstellung Nutanix erstellt wurden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Sie können dieses Muster auf dem Now Platform mit Madrid , Patch 9 und höher verwenden.

Das Nutanix Components-Muster verwendet REST APIs, um Informationen über die Acropolis-Bereitstellungskomponenten zu sammeln.

Das Nutanix-VM-Event-Muster wird alle fünf Minuten ausgeführt. Wenn Ereignisse auftreten, die auf eine Statusänderung in einer der Nutanix -Komponenten hinweisen, wird die erneute Erkennung von Nutanix -Komponenten mithilfe des Nutanix-Komponentenmusters ausgelöst.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

MID-Server-Anforderungen

Stellen Sie ein dediziertes MID-Server Element bereit, und verbinden Sie es mit Netzwerkzugriff auf Prism Element und Prism Central.

Um Ereignisse im Zusammenhang mit VMs in der Bereitstellung Nutanix zu erkennen, legen Sie die Fähigkeit MID-Server auf **Alle** oder **Nutanix**fest.

Sichere Verbindung wird hergestellt

Installieren Sie Nutanix Endpunkt-SSL-Zertifikate für die MID-Server JRE.

Konfigurieren Sie vor der Installation der Nutanix -Endpunkt-SSL-Zertifikate Folgendes:

1. Sammeln Sie die Zertifikate, indem Sie die Prism-Konsole Nutanix in Internet Explorer durchsuchen.
2. Fügen Sie SSL-Zertifikate für MID-Serverhinzu (siehe Beschreibung unter SSL-Zertifikate für den MID Server hinzufügen) .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Verwenden Sie den folgenden JRE-Keytool-Befehl, um die SSL-Zertifikate im Schlüsselspeicher von MID-Serverzu importieren:<MID Installation> `/jre/bin/keytool -import -v -keystore`jre/lib/security/cacerts
4. Wenn Sie ein Passwort eingeben müssen, geben Sie das anwenderdefinierte Passwort oder das Standardpasswort „change“ ein.

Anmeldeinformationen

Konfigurieren Sie die folgenden Anmeldeinformationen:

1. Navigieren zu **Discovery** > **Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **Anmeldeinformationen für Standardauthentifizierung**, füllen Sie das Formular aus, und wählen Sie **Absenden**aus.

Formular für Anmeldeinformationen

Feld	Beschreibung
Name	Name der Anmeldeinformationen Ein Beispiel ist `Acropolis`.
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Betrifft	Wählen Sie **Alle MID Server**.
Reihenfolge	Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten verwendet. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist 100.
Benutzername	Name des Benutzers zum Ausführen der Acropolis-Erkennung
Passwort	Passwort für diesen Benutzer
Anmeldeinformationsalias	Der Anmeldeinformationsalias für diese Anmeldeinformationen zum Autorisieren von Aktionen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen für API-Elemente

Während der Erkennung verwendet das Muster folgende API-Elemente. Der Benutzer, der den Anmeldeinformationen in der Instanz hinzugefügt wurde, muss über Berechtigungen zum Senden dieser Abfragen verfügen.

- /PrismGateway/services/rest/v2.0/tasks/list
- /api/nutanix/v3/clusters/list
- /PrismGateway/services/rest/v2.0/hosts
- /PrismGateway/services/rest/v2.0/clusters
- /PrismGateway/services/rest/v1/vms
- /PrismGateway/services/rest/v1/storage_pools
- /PrismGateway/services/rest/v2.0/storage_containers
- /api/nutanix/v3/categories/list
- /api/nutanix/v3/categories/{category_keys}/list
- /api/nutanix/v3/category/query

Zeitplan für Erkennung ohne Server erstellen

Erstellen Sie einen Discovery-Zeitplan für die gezielte Erkennung von Nutanix -Komponenten. Weitere Informationen finden Sie unter Serverlose Erkennung.

(Optional) Aktivieren Sie die HTTP-Klassifizierung für die Verwendung von Schnell-Discovery.

Wenn Sie keinen serverlosen Discovery-Zeitplan erstellen möchten, können Sie die Discovery der Nutanix -Komponenten mit der HTTP-Klassifizierung auslösen. Diese Klassifizierung ermöglicht Ihnen, die Erkennung mithilfe von Schnell-Discovery auszuführen. In diesem Fall wird die Erkennung mit einer einzelnen IP-Adresse ausgeführt, ohne dass ein Zeitplan erforderlich ist.

Stellen Sie zum Aktivieren der HTTP-Klassifizierung sicher, dass der Anwendungsbereich Muster für Discovery und Service-Mappingist:

1. Navigieren zu **Einstellungen** > **Entwickler**.
2. Wählen Sie **Discovery and Service Mapping Patterns** aus der Liste **Anwendung** aus.

Da die HTTP-Klassifizierung Abfragen aller Server mit offenen HTTP-Ports auslöst, kann dies zu einer Überlastung des Netzwerks und einer Verlangsamung des Erkennungsprozesses führen.

1. Navigieren zu **Discovery** > **Discovery-Definition** > **CI-Klassifizierung** > **HTTP**.
2. Ändern Sie den Filter, um alle Klassifizierungen anzuzeigen, einschließlich nicht aktiver Klassifizierungen.
3. Suchen Sie die Klassifizierung **Nutanix HTTP**, und legen Sie das Attribut **Aktiv** als `true` fest.

Store-App CMDB CI-Klassenmodelle

Stellen Sie sicher, dass Ihre -Instanz die -CI-Klassenmodelle Nutanix unterstützt, indem Sie die neueste Version der Store-App CMDB CI-Klassenmodelle aus dem ServiceNow Storebereitstellen.

(Optional) VMware-Komponenten erkennen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um die Anzeige von Beziehungen zwischen Nutanix Acropolis und VMware zu ermöglichen, führen Sie die VMware-Discovery vor Nutanix der Acropolis-Discovery aus. Führen Sie die horizontale Erkennung für VMware Vcenter mit der Probe „VMware - vCenter Datacenters“ aus.

(Optional) CI-Tag-Erkennung deaktivieren

Das Muster „Nutanix-Komponenten“ erkennt Tags für Nutanix -Hosts und virtuelle Computer. Wenn Ihre Bereitstellung Dutzende von Tags aufweist, kann dies die Erkennung verlangsamen und zu Leistungsproblemen führen. So können Sie die Erkennung von CI-Tags deaktivieren:

1. Navigieren zu **Musterdesigner** > **Discovery-Muster**.
2. Klicken Sie auf das Muster **Nutanix Components**.
3. Klicken Sie unter **Erweiterungsabschnitt** auf das Kontrollkästchen **Kategorien (Tags)** und anschließend auf **Entfernen**.
4. Klicken Sie auf **Speichern**.

Passen Sie die Batchgröße zum Entfernen redundanter Beziehungsdaten an

Die Eigenschaft *sn_itom_pattern.nutanix_relations_deletion_batch_size* legt die Batchgröße zum Löschen von Beziehungen zwischen der VM-Instanz Nutanix und dem Host Nutanix fest. Der Standardwert ist 1000; können Sie diese Batchgröße nach Bedarf anpassen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das Muster „Nutanix-Komponenten“ ausgeführt wird.

Nutanix-Controller-VM [cmdb_ci_nutanix_controller_vm]

Feld	Beschreibung
Name [name]	Der Name der Nutanix Controller-VM.
VM-ID [vm_id]	Der Universally Unique Identifier (UUID) der Controller-VM Nutanix.
Objekt-ID [object_id]	Die ID der Controller-VM Nutanix.
Arbeitsspeicher (MB) [memory]	Die Größe des Arbeitsspeichers der Controller-VM Nutanix in Megabyte (MB).
Status [state]	Der Energiestatus der Nutanix Controller-VM (ein/aus).
Hypervisor-Typ [Hypervisor_type]	Der Typ des für die Controller-VM Nutanix verwendeten Hypervisors.
Beschreibung [short_description]	Die für die VM in der Konsole Nutanix definierte Beschreibung: Prism Central oder Prism Element.

Nutanix-Cluster [cmdb_ci_nutanix_cluster]

Feld	Beschreibung
Name [name]	Der Name des Nutanix -Clusters.
IP-Adresse [ip_address]	Die IP-Adresse des Nutanix -Clusters.
Cluster-ID [cluster_id]	Die ID des Nutanix -Clusters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutanix-Cluster [cmdb_ci_nutanix_cluster] (Fortsetzung)

Feld	Beschreibung
Objekt-ID [object_id]	Die Objekt-ID des Nutanix -Clusters.
Version [version]	Die Nutanix -Clusterversion.
Vollversion [full_version]	Die Vollversion des Nutanix -Clusters.
Internes Subnetz [internal_subnet]	Das Subnetz der internen IP-Adresse des Nutanix -Clusters.
Externes Subnetz [external_subnet]	Das Subnetz der externen IP-Adresse des Nutanix -Clusters.
Zeitzone [timezone]	Die Zeitzone des Nutanix -Clusters.
Hypervisor-Typen [hypervisor_types]	Der Typ des für den Nutanix -Cluster verwendeten Hypervisors.
NTP-Server [ntp_servers]	Die Network Time Protocol(NTP)-Server, die mit dem Cluster Nutanix verbunden sind.
Anzahl der Knoten [num_nodes]	Die Anzahl der mit dem Cluster Nutanix verbundenen Knoten.
NCC-Version [ncc_version]	Die Nutanix Cluster Check-Version (NCC-Version).
Block-Seriennummern [block_serial_numbers]	Die Seriennummern der Datenblöcke, die mit dem Cluster Nutanix verbunden sind.

Nutanix-Host [cmdb_ci_nutanix_host]

Feld	Beschreibung
Name [name]	Der Name des Nutanix -Hosts.
Objekt-ID [object_id]	Die ID des Nutanix -Hosts.
Anzahl der CPU-Kerne [cpu_core_count]	Die Anzahl von Nutanix Hostkernen.
CPU-Core-Thread [cpu_core_thread]	Die Anzahl der Threads des Hosts Nutanix
CPU-Geschwindigkeit (MHz) [cpu_speed]	Die CPU-Geschwindigkeit des Hosts Nutanix in MHz.
CPU-Anzahl [cpu_count]	Die Anzahl der CPU-Sockel auf dem Host Nutanix.
RAM (MB) [ram]	Der Arbeitsspeicher des Hosts in Megabyte (MB)

Nutanix-Speicherpool [cmdb_ci_storage_pool]

Feld	Beschreibung
Name [name]	Der Name des Speicher-Pools Nutanix.
Pool-ID [pool_id]	Die UUID des Speicher-Pools Nutanix.
Objekt-ID [object_id]	Die ID des Speicher-Pools Nutanix.
Größe [size]	Die Größe des Speicher-Pools Nutanix.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutanix-Speichercontainer [cmdb_ci_nutanix_storage_container]

Feld	Beschreibung
Objekt-ID [object_id]	Die ID des Nutanix -Containers.
Container-ID [container_id]	Die UUID des Nutanix -Containers.
Name [name]	Der Name des Nutanix -Containers.
Replikationsfaktor [replication_factor]	Die Anzahl der Kopien, die für die in diesem Nutanix Speichercontainer gespeicherten Daten erstellt wurden.
Deduplizierung [deduplication]	Die Deduplizierung wird für den Container Nutanix aktiviert oder deaktiviert.
Komprimierung [compression]	Die Komprimierung wird für den Container Nutanix aktiviert oder deaktiviert.
Löschcode [erasure_code]	Das Löschen von Code wird für den Container Nutanix aktiviert oder deaktiviert.
Größe [size]	Die Nutanix -Containergröße, die während der Discovery dynamisch berechnet wird.

Nutanix VM-Instanz [cmdb_ci_nutanix_vm_instance]

Feld	Beschreibung
Name [name]	Der Name der Nutanix Controller-VM.
ID der VM-Instanz [vm_inst_id]	Der Universally Unique Identifier (UUID) der Controller-VM Nutanix.
Objekt-ID [object_id]	Die ID der Controller-VM Nutanix.
CPUs [cpus]	Die Anzahl der CPUs der VM
Arbeitsspeicher (MB) [memory]	Die Größe des Arbeitsspeichers der Controller-VM Nutanix in Megabyte (MB).
Status [state]	Der Energiestatus der Nutanix Controller-VM (ein/aus).
Beschreibung [short_description]	Die für die VM in der Konsole Nutanix definierte Beschreibung: Prism Central oder Prism Element.

Nutanix Prism Central [cmdb_ci_nutanix_prism_central]

Feld	Beschreibung
Name [name]	Der Name des Nutanix Prism Central-Multi-Cluster-Managers. • **PrismCentral@**<IP_ADDRESS> : Wenn die IP-Adresse der Prism Central-Instanz zugeordnet ist. Dies gilt in den folgenden Szenarien: ◦ Während der Schnell-Discovery mit HTTP-Klassifizierung. ◦ Während der serverlosen Discovery, ob die IP-Adresse in den Parameterwert **„PRSM_Address“** eingegeben wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nutanix Prism Central [cmdb_ci_nutanix_prism_central] (Fortsetzung)

Feld	Beschreibung
	• **PrismCentral@**<DNS_NAME> : Wenn der DNS-Name der zentralen Prisma-Instanz zugeordnet ist. Dies gilt, wenn der DNS-Name während der serverlosen Discovery in den Parameterwert **„PRSM_Address“** eingegeben wurde.
Objekt-ID [object_id]	Die ID von Nutanix Prism Central. Dieses Feld hat den gleichen Wert wie das Feld **Name**. • **PrismCentral@**<IP_ADDRESS> : Wenn die IP-Adresse der Prism Central-Instanz zugeordnet ist. Dies gilt in den folgenden Szenarien: ◦ Während der Schnell-Discovery mit HTTP-Klassifizierung. ◦ Während der serverlosen Discovery, ob die IP-Adresse in den Parameterwert **„PRSM_Address“** eingegeben wurde. • **PrismCentral@**<DNS_NAME> : Wenn der DNS-Name der zentralen Prisma-Instanz zugeordnet ist. Dies gilt, wenn der DNS-Name während der serverlosen Discovery in den Parameterwert **„PRSM_Address“** eingegeben wurde.

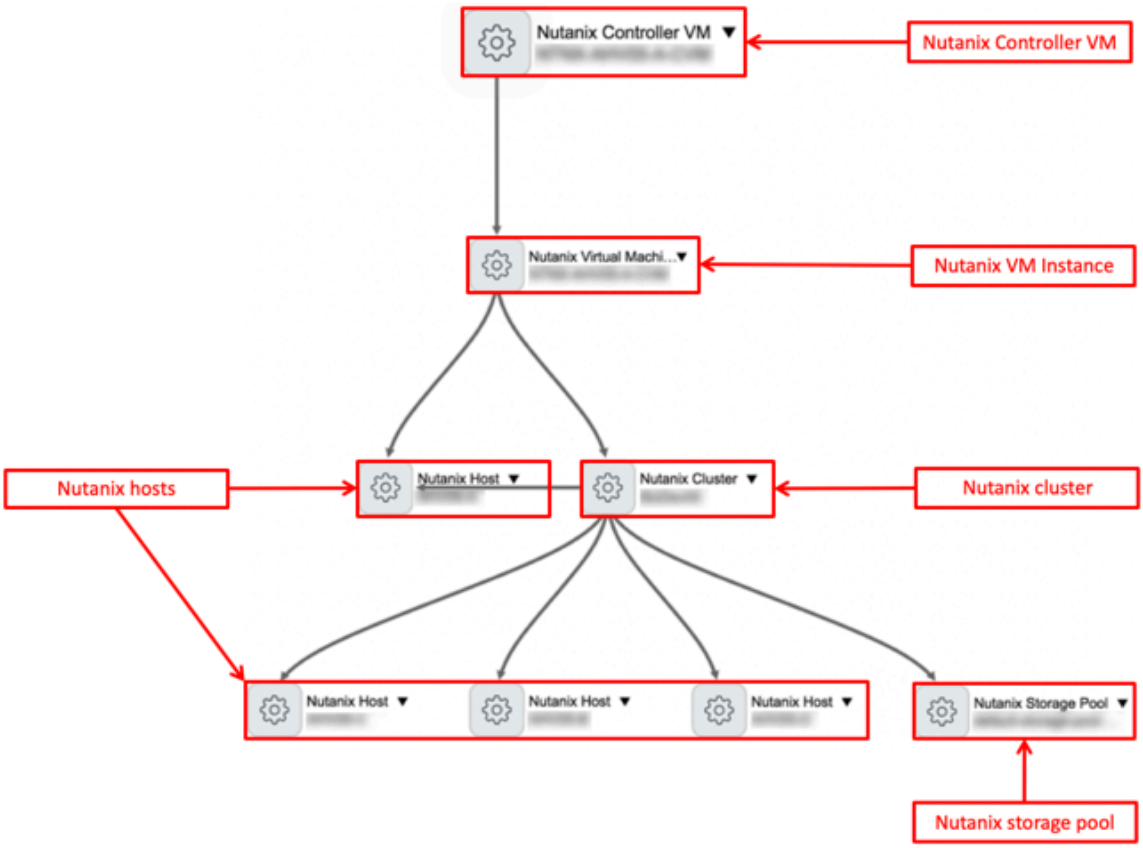
Schlüsselwert [cmdb_key_value]

Feld	Beschreibung
Konfigurationselement [configuration_item]	Der Verweis auf das CI, für das das Tag definiert ist
Schlüssel [key]	Der Kategorieschlüssel
Wert [value]	Der Kategoriewert
Objekt-ID [object_id]	Die Objekt-ID für den Nutanix -Host oder Nutanix die -VM.

Die Grafik zeigt CIs, die Teil der -Erkennung Acropolis in Bereitstellungen sind, die Nutanix AHV für die Virtualisierung verwenden.

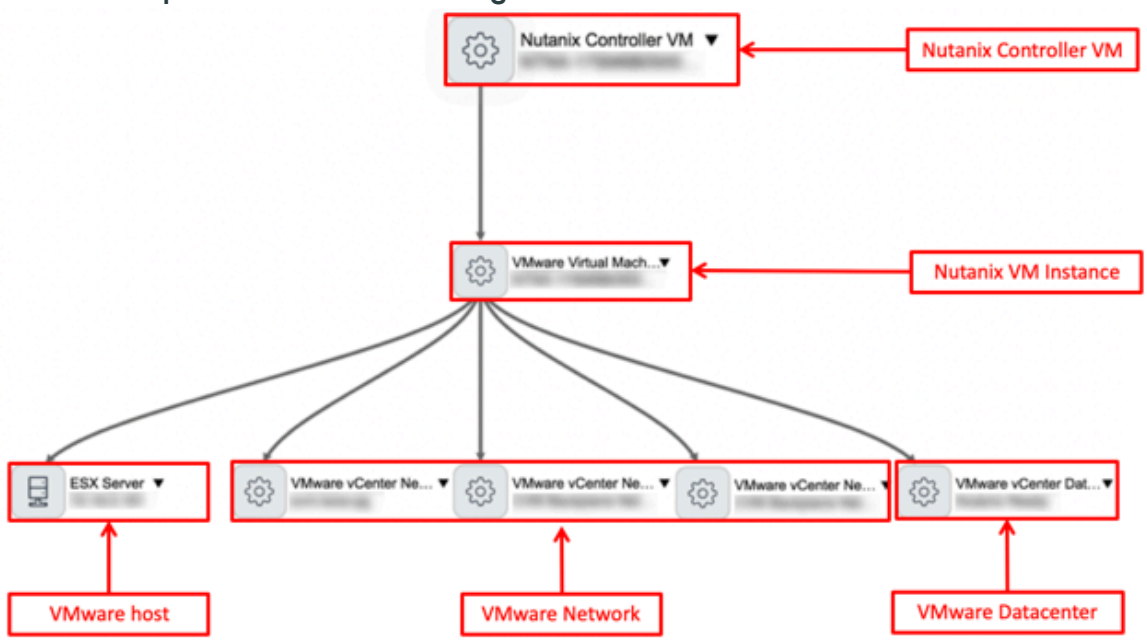
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten von Nutanix



Die Grafik zeigt CIs, die Teil der -Erkennung Acropolis in Bereitstellungen sind, die VMware-Software für die Virtualisierung verwenden.

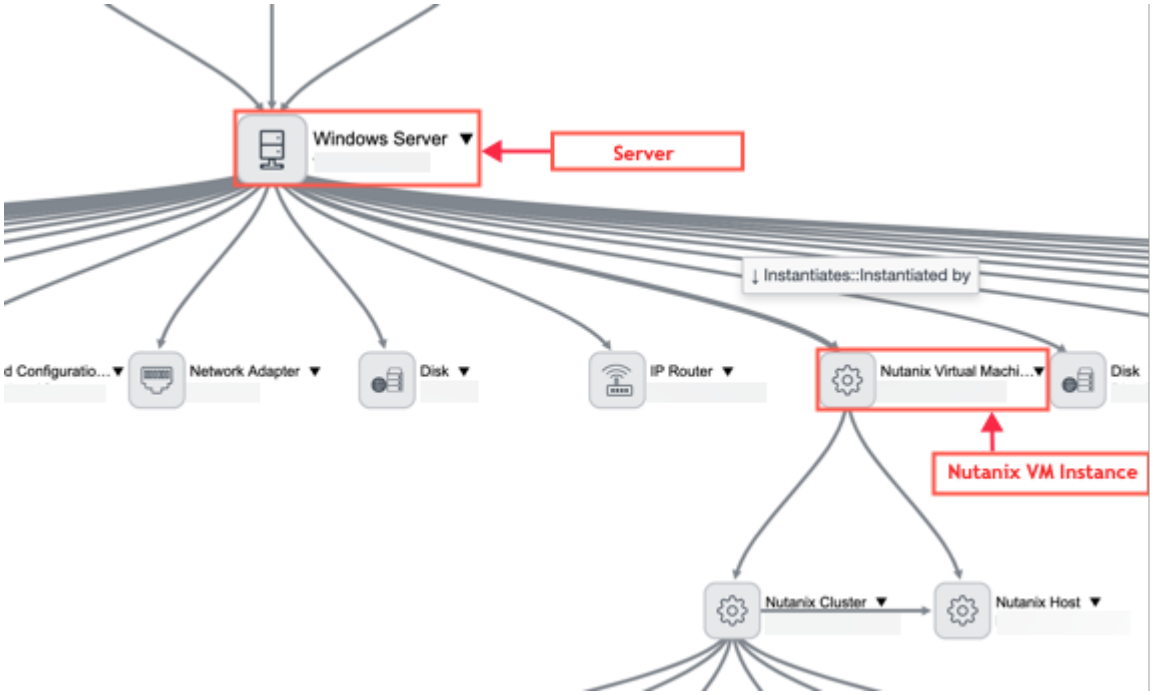
Nutanix Komponenten in -Bereitstellungen mithilfe von VM-Software



Die Grafik veranschaulicht die Beziehung zwischen Server und Nutanix VM-Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CI-Beziehungen

Diese Beziehungen werden erstellt, um die Discovery Nutanix von zu unterstützen:

CI	Beziehung	CI
Nutanix-Cluster [cmdb_ci_nutanix_cluster]	Definiert Ressourcen für::Erhält Ressourcen von	Nutanix-Speicherpool [cmdb_ci_storage_pool]
	Mitglieder::Mitglied von	Nutanix-Host [cmdb_ci_nutanix_host]
Nutanix VM-Instanz [cmdb_ci_nutanix_vm_instance]	Registriert::Hat sich registriert	Nutanix-Host [cmdb_ci_nutanix_host]
	Gehostet auf::Hostet	Nutanix-Cluster [cmdb_ci_nutanix_cluster]
Nutanix-Controller-VM [cmdb_ci_nutanix_controller_vm]	Wird ausgeführt auf::Wird ausgeführt	Nutanix VM-Instanz [cmdb_ci_nutanix_vm_instance]
	Wird ausgeführt auf::Wird ausgeführt	[cmdb_ci_vmware_instance]
	Gehostet auf::Hostet	Nutanix Prism Central [cmdb_ci_nutanix_prism_central]
Nutanix-Speicherpool [cmdb_ci_storage_pool]	Enthält::Enthalten in	Nutanix-Speichercontainer [cmdb_ci_nutanix_storage_container]
	Gehostet auf::Hostet	Nutanix Prism Central [cmdb_ci_nutanix_prism_central]
VMware-Cluster [cmdb_ci_vmware_cluster]	Definiert Ressourcen für::Erhält Ressourcen von	Nutanix-Speicherpool [cmdb_ci_storage_pool]
Server [cmdb_ci_server]	Instanziiert::Instanziiert von	Nutanix VM-Instanz [cmdb_ci_nutanix_vm_instance]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Nutanix-Cluster [cmdb_ci_nutanix_cluster]	Verwaltet von::Verwaltet	Nutanix Prism Central [cmdb_ci_nutanix_prism_central]

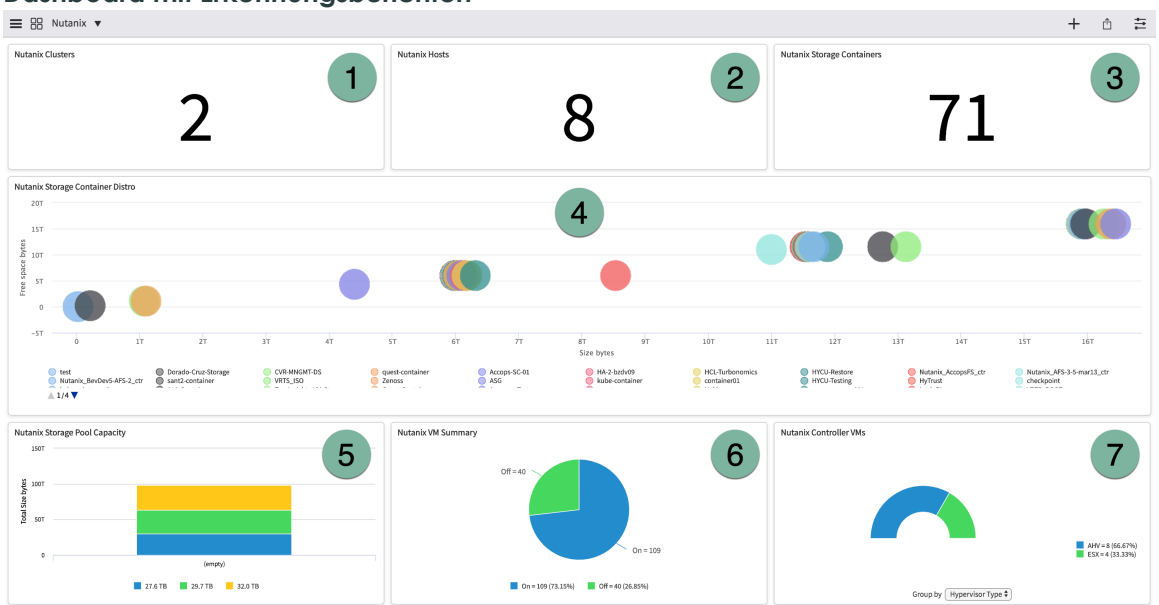
Dashboard

Das Dashboard enthält Berichte, die Anfragen an die Configuration Management Database (CMDB) stellen und die Ergebnisse anzeigen. Die Informationen werden erst angezeigt, nachdem das Muster die Infrastruktur erkannt hat.

Um das Dashboard anzuzeigen, navigieren Sie zu **Selfservice** > **Dashboards** > **Alle** > **Nutanix**.

Nach dem Upgrade auf Discovery-Administratorarbeitsbereich Version 1.3.1 (Store August 2024) können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** und verwenden Sie das erweiterte Dashboard.

Dashboard mit Erkennungsberichten



Die Berichte auf dem Dashboard enthalten die folgenden Informationen. Sie werden in der Tabelle anhand der in der Grafik angezeigten Nummern aufgelistet.

	Bericht	Beschreibung
1	Nutanix-Cluster	Anzahl oder Nutanix Cluster gefunden.
2	Nutanix-Hosts	Anzahl von Nutanix Hosts gefunden.
3	Nutanix-Speichercontainer	Anzahl von Nutanix Speichercontainern gefunden.
4	Nutanix-Speichercontainer-Verteilung	Die Verteilung von Nutanix freiem Speicherplatz und Kapazität der Speichercontainer in Byte.
5	Nutanix-Speicherpool-Kapazität	Kapazität des Speicher-Pools Nutanix in Byte.
6	Nutanix-VM-Zusammenfassung	Die Nutanix VMs nach Status gruppiert: Ein, Aus, Beendet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Bericht	Beschreibung
7	Nutanix-Controller-VMs	Die Controller-VMs Nutanix, gruppiert nach Hypervisor-Typ.

OpenStack-Ressourcenerkennung

Die ServiceNow Discovery-Anwendung verwendet OpenStack-Ressourcen-Erkennungsmuster, um OpenStack-Ressourcen über REST API-Aufrufe zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery verwendet Discovery-Muster für OpenStack-Ressourcen, um eine Horizontal-Discovery auszuführen.

Ab dem Store-Release Muster für Discovery und Service-Mapping von August 2024 unterstützen OpenStack-Ressourcen-Discovery-Muster sowohl Private als auch Public Cloud-Discovery.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

OpenStack-Anforderungen

- Suchen Sie im OpenStack Identity-Servicekatalog die Zugriffs-URL, die als OpenStack Identity-Service-Endpunkt verwendet wird. Beispiel: https://<openstack dns>:<port>.
- Konfigurieren Sie einen OpenStack-Anwender mit Berechtigungen zum Generieren eines Projektbereichstokens. Das Festlegen der Werte für Domänen-ID, Anwendername, Projektname und Passwort ist erforderlich, um ein Token zu generieren.

MID Server-Anforderungen

Stellen Sie einen dedizierten MID-Server für Cloud-Erkennung bereit und verbinden Sie ihn.

Der dedizierte MID-Server muss Zugriff auf OpenStack und einen offenen Port haben, damit jeder OpenStack-Service erkannt werden kann.

Anmeldeinformationen

Erstellen Sie auf der Seite Now Platformdie OpenStack-Anmeldeinformationen für das Cloud-Servicekonto ServiceNow. Geben Sie die Werte für Domänen-ID, Anwendername, Projektname und Passwort ein, die Sie in den OpenStack-Anforderungen konfiguriert haben. Weitere Informationen finden Sie unter Anmeldeinformationen erstellen und testen .

Servicekonto

Konfigurieren Sie auf der Now Platformein Cloud-Servicekonto ServiceNow unter Verwendung der erstellten OpenStack-Anmeldeinformationen und der OpenStack-Rechenzentrumsdetails. Geben Sie im Feld **„Account-ID“** die Projekt-ID des zu erkennenden OpenStack-Projekts an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennungszeitpläne erstellen

Weitere Informationen finden Sie unter Erstellen Sie in einen Discovery-Zeitplan Arbeitsbereich für Cloud-Vorgänge.

Erstellt einen Zeitplan für die automatische Erkennung von OpenStack-Servicekonten (nur für Private Cloud).

Erstellen Sie mit dem Muster „OpenStack – Service-Accounts erkennen“ einen Zeitplan für die automatische serverlose Discovery für OpenStack-Servicekonten. Weitere Informationen finden Sie im Artikel Zeitplan für automatische Cloud-Discovery für Open Stack [KB1638685] in der Now Support Knowledge Base.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB bei der Ausführung der OpenStack-Ressourcen-Discovery-Muster.

VM-Instanz [cmdb_ci_vm_instance]

Feld	Beschreibung
Objekt-ID [object_id]	Server-UUID
Name [name]	Servername
Status [status]	Serverstatus
Beschreibung [short_description]	(Optional) Serverbeschreibung
CPUs [cpus]	Anzahl der virtuellen CPUs (vCPUs) aus der Variante, mit der die VM-Instanz bereitgestellt wird.
Datenträger [disks]	Anzahl aller von ihr verwalteten Volumes, die von der VM-Instanz zurückgegeben werden.
Datenträgergröße (GB) [disk_size]	Gesamtmenge aller von CIder verwalteten Volumes, die von der VM-Instanz verwendet werden, gemessen in Gigabyte (GB).
Arbeitsspeicher (MB) [memory]	Der **RAM** -Wert der Variante, mit der die VM-Instanz bereitgestellt wird, gemessen in Megabyte (MB).
Netzwerkadapter [NICs]	Anzahl der in der VM-Instanz konfigurierten eindeutigen Schnittstellen.
Status [state]	Zugeordneter Statuswert, der für die VM-Instanz zurückgegeben wird. Die OpenStack Server-Status und die zugehörigen ServiceNow **Statuswerte** sind: • AKTIV: auf • GELÖSCHT: auf • PAUSED: angehalten • AUSGESETZT: aus • GEHALTEN: aus • Soft_deleteed: beendet • HARD_DELETED: beendet • GRÖSSE ÄNDERT: aus

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

VM-Instanz [cmdb_ci_vm_instance] (Fortsetzung)

Feld	Beschreibung
	• FEHLER: Fehler • INITIALISIERT: wird gestartet Für jeden nicht aufgeführten **Statuswert** ist der Standardwert Aus.

Cloud-Schlüsselpaare [cmdb_ci_cloud_key_pair]

Feld	Beschreibung
Objekt-ID [object_id]	Schlüsselpaar-UUID
Name [name]	Schlüsselpaarname, der zum Verweisen verwendet wird
Fingerabdruck [finger_print]	Schlüsselpaar-Fingerabdruck

Cloud-Load Balancer [cmdb_ci_cloud_load_balancer]

Feld	Beschreibung
Objekt-ID [object_id]	ID des Lastenausgleichsmoduls
Name [name]	Visuell lesbarer Ressourcenname
Beschreibung [short_description]	(Optional) Visuell lesbare Ressourcenbeschreibung
Installationsstatus [install_status]	Bereitstellungsstatus der Ressource
Betriebsstatus [operational_status]	Ressourcenvorgangsstatus

Lastenausgleichsmodul-Listener [cmdb_ci_lb_listener]

Feld	Beschreibung
Objekt-ID [object_id]	Listener-ID
Name [name]	Visuell lesbarer Name der Ressource
Installationsstatus [install_status]	Bereitstellungsstatus der Ressource
Listenerprotokoll [listener_protocol]	Protokoll für die Ressource. Entweder HTTP, HTTPS, TCP, TERMINATED_HTTPS oder UDP
Listenerport [listener_port]	Protokollportnummer für die Ressource
Betriebsstatus [operational_status]	Ressourcenvorgangsstatus
Beschreibung [short_description]	(Optional) Visuell lesbare Ressourcenbeschreibung

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Objekt-ID [object_id]	Pool-ID

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Load Balancer-Pool [cmdb_ci_lb_pool] (Fortsetzung)

Feld	Beschreibung
Name [name]	Visuell lesbarer Ressourcenname
Installationsstatus [install_status]	Bereitstellungsstatus der Ressource
Betriebsstatus [operational_status]	Ressourcenvorgangsstatus
Beschreibung [short_description]	(Optional) Visuell lesbare Ressourcenbeschreibung
Lastenausgleichsmethode [load_balancing_method]	Lastenausgleichsalgorithmus für den Pool. Einer der folgenden Werte: LEAST_CONNECTIONS, ROUND_ROBIN, SOURCE_IP oder SOURCE_IP_PORT

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]

Feld	Beschreibung
Objekt-ID [object_id]	Poolmitglieds-ID
Name [name]	Visuell lesbarer Ressourcenname
Installationsstatus [install_status]	Bereitstellungsstatus der Ressource
IP-Adresse [ip_address]	Back-End-Mitgliedsserver-IP-Adresse

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Objekt-ID [object_id]	Volume-UUID
Name [name]	Volumename
Status [status]	Volumestatus
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung
Speichertyp [storage_type]	Zugeordneter Volumetyp

Snapshot des Speichervolume [cmdb_ci_storage_vol_snapshot]

Feld	Beschreibung
Objekt-ID [object_id]	Volume-UUID
Name [name]	Volumename
Status [status]	Volumestatus
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung

Image [cmdb_ci_os_template]

Feld	Beschreibung
Objekt-ID [object_id]	Benutzerdefinierte Image-UUID

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Image [cmdb_ci_os_template] (Fortsetzung)

Feld	Beschreibung
Name [name]	Image-Name. Der Wert kann null sein (der JSON-Null-Datentyp).
Status [status]	Image-Status

Cloud-Netzwerk [cmdb_ci_network]

Feld	Beschreibung
Objekt-ID [object_id]	Netzwerk-ID
Name [name]	Visuell lesbarer Netzwerkname
Betriebsstatus [operational_status]	Netzwerkstatus. Mögliche Werte: ACTIVE, DOWN, BUILD oder ERROR
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung

Cloud-Subnetz [cmdb_ci_cloud_subnet]

Feld	Beschreibung
Objekt-ID [object_id]	Subnetz-ID
Name [name]	Visuell lesbarer Ressourcenname
DHCP aktiviert [is_dhcp_enabled]	Ob DHCP für das Subnetz aktiviert oder deaktiviert ist
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung

Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]

Feld	Beschreibung
Objekt-ID [object_id]	Sicherheitsgruppen-ID
Name [name]	Visuell lesbarer Ressourcenname
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung

Sicherheitsgruppenregel [cmdb_ci_compute_security_group_rule]

Feld	Beschreibung
Name [name]	Dieses Feld hat den gleichen Wert wie das Feld object_id.
Objekt-ID [object_id]	Sicherheitsgruppenregel-ID
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung
Ethertyp [ethertype]	EtherType Muss IPv4 oder IPv6 sein. In CIDR dargestellte Adressen müssen den Eingangs- oder Ausgangsregeln entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sicherheitsgruppenregel [cmdb_ci_compute_security_group_rule] (Fortsetzung)

Feld	Beschreibung
Portbereich max. [port_range_max]	Der letzte Port des Bereichs, für den die Regel gilt. Dieser Wert ist die maximale Portnummer in dem Bereich, der der Sicherheitsgruppenregel entspricht. • Wenn das Protokoll TCP, UDP, DCCP, SCTP oder UDP-Lite ist, muss dieser Wert größer oder gleich dem Attributwert port_range_min sein. • Wenn das Protokoll ICMP ist, muss dieser Wert ein ICMP-Code sein.
Portbereich min. [port_range_min]	Der erste Port des Bereichs, für den die Regel gilt. Dieser Wert ist die minimale Portnummer in dem Bereich, der der Sicherheitsgruppenregel entspricht. • Wenn das Protokoll TCP, UDP, DCCP, SCTP oder UDP-Lite ist, muss dieser Wert kleiner oder gleich dem Attributwert port_range_max sein. • Wenn das Protokoll ICMP ist, muss dieser Wert ein ICMP-Typ sein.

OpenStack-Domäne [cmdb_ci_cloud_openstack_domain]

Feld	Beschreibung
Objekt-ID [object_id]	Domänen-ID
Name [name]	Domänenname
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung
Aktiviert [enabled]	Definiert, ob die Domäne aktiviert oder deaktiviert ist • „True“ – Die Domäne ist aktiviert. • „False“ – Die Domäne ist deaktiviert.

OpenStack-Service [cmdb_ci_cloud_openstack_service]

Feld	Beschreibung
Objekt-ID [object_id]	Service-ID
Name [name]	Servicename
Beschreibung [short_description]	(Optional) Visuell lesbare Beschreibung
Typ [type]	Servicetyp. Beschreibt die vom Service implementierte API. Mögliche Werte: Berechnen, EC2, Identität, Image, Netzwerk oder Volume
Katalog aktiviert [enabled]	Definiert, ob der Service und seine Endpunkte im Servicekatalog angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

OpenStack-Service [cmdb_ci_cloud_openstack_service] (Fortsetzung)

Feld	Beschreibung
	• True – Der Service und seine Endpunkte werden im Servicekatalog angezeigt. • False – Der Service und seine Endpunkte werden nicht im Servicekatalog angezeigt.

OpenStack-Endpunkt [cmdb_ci_cloud_openstack_endpoint]

Feld	Beschreibung
Objekt-ID [object_id]	Endpunkt-ID
Name [name]	Servicename
Schnittstelle [interface]	Schnittstellentyp, der die Sichtbarkeit des Endpunkts beschreibt. Mögliche Werte: • Öffentlich – Für Endbenutzer auf einer öffentlich verfügbaren Netzwerkschnittstelle sichtbar • Intern – Für Endbenutzer auf einer nicht zertifizierten internen Netzwerkschnittstelle sichtbar • Administrator – Für Administratoren auf einer sicheren Netzwerkschnittstelle sichtbar
Katalog aktiviert [enabled]	Definiert, ob der Service und seine Endpunkte im Servicekatalog angezeigt werden. • True – Der Service und seine Endpunkte werden im Servicekatalog angezeigt. • False – Der Service und seine Endpunkte werden nicht im Servicekatalog angezeigt.

Cloud-Hardwaretyp [cmdb_ci_cloud_hardware_type]

Feld	Beschreibung
Name [name]	Das **Namensfeld** der OpenStack-Variante.
Objekt-ID [object_id]	Das **ID-** Feld der OpenStack-Variante.
vCPUs [vcpus]	Das Feld **„vcpus** “ der OpenStack-Variante.
MB Arbeitsspeicher [memory_mb]	Das **RAM-** Feld der OpenStack-Variante.
Lokaler Speicher – GB [local_storage_gb]	Das **Festplattenfeld** der OpenStack-Variante.

Die erkannten Daten enthalten die Tabelle „OpenStack-Hypervisor-Ansicht“ [cmdb_ci_openstack_hypervisor_view] und ihre Felder nur für Private Cloud.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder der Tabelle „OpenStack-Hypervisor-Ansicht“ [cmdb_ci_openstack_hypervisor_view].

Feld	Beschreibung
Name [name]	Verketteter Wert der Felder **„linker Bildschirmtyp“** und **„Hypervisor_Hostname“**. Beispiel: QEMU@host.acmecorp.com.
IP-Adresse [ip_address]	Der Wert des Felds **„host_ip“**.
Hypervisor-Technologie [hypervisor_technologie]	Der Wert des Felds **„Hypervisor_type** “.
Objekt-ID [object_id]	Der Wert des **ID** -Felds.
Status [state]	Der Wert des **Statusfelds**.
Version [version]	Der Wert des Felds **„Hypervisor_Version“**.

Die Zuordnung der Abhängigkeitsansichten zeigt alle erkannten OpenStack-Ressourcen in Ihrer Organisation, die über REST API-Aufrufe verfügbar sind, sowie die Beziehungen zwischen ihnen.

OpenStack-Netzwerkabhängigkeit

OpenStack-VM-Abhängigkeit

CI-Beziehungen

Die in der folgenden Tabelle aufgeführten Beziehungen werden zur Unterstützung der OpenStack-Ressourcen-Discovery erstellt.

CI	Beziehung	CI
cmdb_ci_openstack_datacenter	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_openstack_service	Gehostet auf::Hostet	cmdb_ci_cloud_service_account
cmdb_ci_cloud_openstack_endpoint	Endpunkt verwenden bis::Endpunkt verwenden ab	cmdb_ci_cloud_openstack_service
cmdb_ci_cloud_openstack_endpoint	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_cloud_openstack_domain	Eigentümer von::Eigentum von	cmdb_ci_cloud_service_account
cmdb_ci_network	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_network	Enthält::Enthalten in	cmdb_ci_cloud_subnet
cmdb_ci_compute_security_group	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_compute_security_group	Enthält::Enthalten in	cmdb_ci_compute_security_group_rule
cmdb_ci_cloud_load_balancer	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_cloud_load_balancer	Enthält::Enthalten in	cmdb_ci_lb_listener
cmdb_ci_lb_pool	Gehostet auf::Hostet	cmdb_ci_cloud_load_balancer

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_lb_pool	Eigentümer von::Eigentum von	cmdb_ci_lb_pool_member
cmdb_ci_storage_volume	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_vm_instance	Verwendet::Verwendet von	cmdb_ci_storage_volume
cmdb_ci_storage_vol_snapshot	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_storage_vol_snapshot	Bereitgestellt von::Bereitgestellt	cmdb_ci_storage_volume
cmdb_ci_vm_instance	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_cloud_key_pair	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_os_template	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_vm_instance	Bereitgestellt von::Bereitgestellt	cmdb_ci_os_template
cmdb_ci_vm_instance	Virtualisiert von::Virtualisiert	cmdb_ci_server

Die in der folgenden Tabelle aufgeführten Beziehungen werden erstellt, um die Erkennung von OpenStack-Ressourcen nur in der Private Cloud zu unterstützen.

CI	Beziehung	CI
cmdb_ci_vm_instance	Registriert auf::Hat sich registriert	cmdb_ci_openstack_hypervisor_view
cmdb_ci_openstack_hypervisor_view	Gehostet auf::Hostet	cmdb_ci_openstack_datacenter
cmdb_ci_openstack_hypervisor_view	Verwendet::Hosts Verwendet von	cmdb_ci_server

Oracle Katalog-Discovery

Die Anwendung Muster für Discovery und Service-Mapping verwendet die Mustererweiterung **„Kataloginformationen abrufen“** der Muster für Oracle DB unter Unix und Oracle DB unter Windows, um Oracle -Katalogobjekte zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery verwendet die Muster „Oracle DB on Unix“ und „Oracle DB on Windows“ sowie die Mustererweiterung „Kataloginformationen abrufen“, um eine Horizontal-Discovery auszuführen.

Sie können dieses Muster auf der Now Platform® mit Madrid -Release oder höher verwenden.

Informationen zur Erkennung der Datenbank Oracle finden Sie unter Erkennung von Oracle-Datenbanken.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Legen Sie die Benutzeranmeldeinformationen fest, und gewähren Sie Berechtigungen:

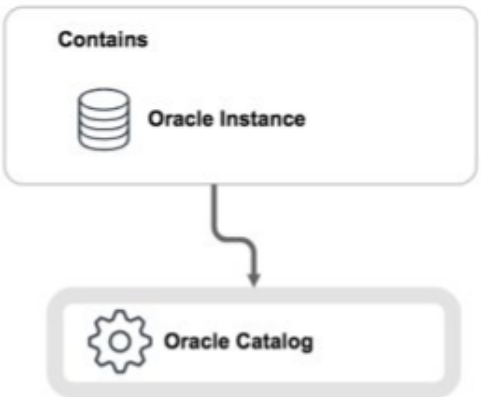
- Konfigurieren Sie Applicative-Anmeldeinformationen .
- Konfigurieren Sie für Windowsdie Windows-Anmeldeinformationen .
- Konfigurieren Sie für UNIXSSH-Anmeldeinformationen .
- Gewähren Sie einem Benutzer Berechtigungen zum Ausführen von Abfragen in der folgenden Tabelle: user_tables.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn die Erweiterung „Muster für Kataloginformationen abrufen“ ausgeführt wird.

Tabelle und Feld	Beschreibung
Oracle Catalog [cmdb_ci_db_ora_catalog]	
database_instance	Der Name der Datenbanksinstanz (SID)
name	Der Name des CI in der CMDB; Schema und SID
schema	Der Name des Katalogobjekts

Im Folgenden finden Sie eine Abhängigkeitsansicht der Beziehung zwischen einem Oracle Catalog und einer Oracle-Instanz.



CI-Beziehungen

Diese Beziehung wird erstellt, um die Katalog-Discovery von Oracle zu unterstützen.

CI	Beziehung	CI
Oracle Catalog [cmdb_ci_db_ora_catalog]	Enthält::Enthalten in	Oracle-Instanz [cmdb_ci_db_ora_instance]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennung der Oracle Database 12c

Die ServiceNow Discovery-Anwendung kann Pluggable-Datenbanken (PDBs) und Container-Datenbanken (CDBs) erkennen, die Funktionen von Oracle Database 12c sind. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Eine PDB ist eine portable Sammlung von Schemata, Schemaobjekten und Nicht-Schemaobjekten, die einem Oracle Net-Client als separate Datenbank angezeigt werden. Eine Sammlung von PDBs wird als Containerdatenbank (CDB) bezeichnet.

Weitere Informationen zu PDBs und CDBs finden Sie unter Was sind CDBs, PDBs und Container? .

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Legen Sie die Benutzeranmeldeinformationen fest, und gewähren Sie Berechtigungen:

- Konfigurieren Sie Applicative-Anmeldeinformationen .
- Für Windows konfigurieren Sie Windows-Anmeldeinformationen .
- Für Unix konfigurieren Sie SSH-Anmeldeinformationen .
- Konfigurieren Sie für die Oracle-Datenbank die Discovery von Oracle-Datenbanken.
- Gewähren Sie einem Benutzer Berechtigungen zum Ausführen von Abfragen in den folgenden Tabellen:
  - V$DATAFILE
  - V$TEMPFILE
  - V$LOG
  - DBA_FREE_SPACE
  - V$DATABASE
  - V$PDBS
  - V$PARAMETER

Hinweis: Legen Sie Applicative-Anmeldeinformationen auf der CDB-Ebene fest, um nur Beziehungen für PDBs und die CDB-Größe zu ermitteln. Legen Sie alternativ Applicative-Anmeldeinformationen auf der CDB/PDB-Ebene fest, um Beziehungen für PDBs und die CDB/PDB-Größe zu ermitteln. Wenn Sie auf der CDB-Ebene keine Applicative-Anmeldeinformationen festlegen, werden keine PDB-Attribute erkannt.

Daten, die während der Erkennung erfasst wurden

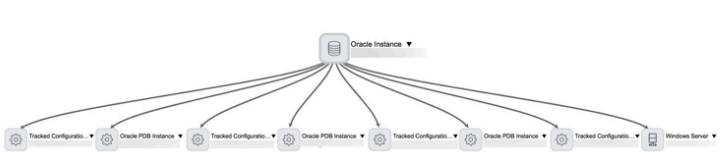
Discovery erfasst die folgenden Daten:

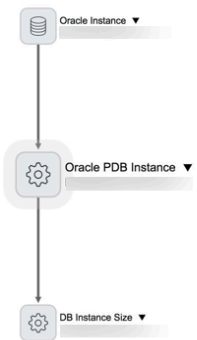
Tabelle und Feld	Beschreibung
cmdb_ci_db_ora_pdb_instance: Beziehungstyp: Verwaltet von	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
sid	Name der PDB-Instanz
name	Name des CI in CMDB Dies ist eine Kombination aus SID und dem Hostname.
Version	Version der PDB aus der CDB-Instanz
Edition	Ausgabe der PDB aus der CDB-Instanz
install_directory	Installationsverzeichnis der PDB aus der CDB-Instanz
oracle_home	Oracle Home der PDB aus der CDB-Instanz
cdb_name	Name der CDB-SID, die die PDB enthält. Dies bezieht sich auf das Configuration Item (CI) der Oracle-Datenbankinstanz ().
cmdb_ci_db_instance_size: Beziehungstyp: Aufgenommen von	
sid	Name der CDB-/PDB-Instanz der Oracle-Datenbank
name	Name des CI in CMDB Dies ist eine Kombination aus SID und dem Hostnamen.
db_size	Gesamtgröße, die der Datenbankinstanz zugewiesen ist
used_size	Von der Datenbankinstanz verwendete Größe
free_size	Größe des freien Speicherplatzes in der Datenbankinstanz

Im Folgenden finden Sie eine Abhängigkeitsansicht der Beziehung zwischen PDBs, CDBs und Containern.





Oracle Globale GLAS-Datensammlung (Global License Advisory Services)

Von der Anwendung ServiceNow Discovery wird das von Oracle geprüfte Muster „GLAS Data Collection“ zur Erkennung von Oracle GLAS-Daten verwendet. Diese Daten umfassen erkannte Oracle Datenbank-, Middleware- und Java-Konfigurationselemente.

Das Muster „Oracle GLAS Data Collection“ ist eine Erweiterung der folgenden Muster:

- Oracle Datenbank für UNIX - und Windows -Muster
- Oracle Middleware auf Linux für die folgenden Muster:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Oracle Tuxedo
- WebLogic
- Linux

- Oracle Java-on-Java-Installationsmuster

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Einzelheiten zum Anzeigen und Herunterladen der gesammelten Oracle GLAS-Daten finden Sie unter Oracle GLAS-Daten (Global License Advisory Services) herunterladen.

Voraussetzungen

Die Muster Datenbank Oracle und Middleware führen die Mustererweiterungen aus, und die gesammelten Daten werden in den Tabellen ServiceNow für GLAS-Daten gespeichert. Das Muster Oracle GLAS Data Collection Database kann ab Release [Now Platform in Paris verwendet werden. Das Muster für die GLAS Data Collection Middleware Oracle kann ab dem Release [Now Platform in Rome verwendet werden. Das Java-Muster Oracle kann für Now Platform ab Release Washington DC verwendet werden.

Unterstützte Versionen Oracle.

Informationen zu den unterstützten Versionen von Oraclefinden Sie unter Detailinformationen über die mittels ITOM-Transparenz erkannten Produkte.

Store-App Oracle Global Licensing and Advisory Services

Navigieren zu **Systemdefinition** > **Plugins** und installieren Sie das Plugin „Data Collection for Oracle Global Licensing and Advisory Services“.

- Die Mindestversion für die Datenbanksammlung ist 1.4.0
- Die Mindestversion für die Middleware-Sammlung ist 1.7.1
- Die Mindestversion für die Java-Sammlung ist 1.8.4

Hinweis: Voraussetzung für das Plugin „Data Collection for Oracle Global Licensing and Advisory Services“ ist, dass das Discovery-Plugin (com.snc.discovery) ordnungsgemäß funktioniert.

Andere bereitzustellende ServiceNow-Apps

- Muster für Discovery und Service-Mapping
- CMDB CI-Klassenmodelle

Anmeldeinformationen

Stellen Sie sicher, dass Sie über die folgenden Anmeldeinformationen verfügen:

- Windows und UNIX Discovery mit PowerShell/WMI/SSH.

Hinweis: PowerShell- und WMI-Anmeldeinformationen sind nur für die Datenbanksammlung erforderlich.

- Applicative-Anmeldeinformationen für die Oracle-Instanz (cmdb_ci_db_ora_instance)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- (Optional) Anmeldeinformationen für virtuelle Computer Stellen Sie sicher, dass Sie über die entsprechenden Anmeldeinformationen verfügen, um Hardwaredaten für Computer zu sammeln, die auf den folgenden virtuellen Providern gehostet werden:
  - VMware
  - Nutanix
  - IBM
  - Hyper-V

Berechtigungen im Betriebssystem

Stellen Sie sicher, dass Sie unter `/tmp`temporäre Dateien schreiben können. Verifizieren Sie außerdem, dass Sie die folgenden Betriebssystembefehle ausführen können:

- ls
- cat
- ps

Oracle-Berechtigungen

Vergewissern Sie sich, dass die Applicative-Anmeldeinformationen über die folgenden Berechtigungen verfügen:

- Leseberechtigungen für die Datei `tnsnames.ora`
- Berechtigungen zum Ausführen des Befehls *`sqlplus`*
- (Für Middleware-Sammlung) Sudo-Berechtigungen zum Ausführen des folgenden Befehls: `sudo Su - oracle -c "$ORACLE_INSTANCE/bin/opmnctl status"`

Vergewissern Sie sich außerdem, dass Sie über den Anwendernamen und das Passwort für die relevante Datenbank Oracle verfügen und über Leseberechtigungen für die folgenden Tabellen verfügen:

DBA_ADVISOR_TASKS	DBA_USERS	SYS.MODEL$
DBA_CPU_USAGE_STATISTICS	DMSYS.DM$MODEL	SYS.REGISTRY$HISTORY
DBA_ENCRYPTED_COLUMNS	DMSYS.DM$OBJECT	SYSMAN.MGMT_INV_CONTAINER
DBA_FEATURE_USAGE_STATISTICS	DMSYS.DM$P_MODEL	SYSMAN.MGMT_LICENSES
DBA_FLASHBACK_ARCHIVE_TABLES	DVSYS.DBA_DV_REALM	SYSMAN.MGMT_LICENSE_DEFINITIONS
DBA_INDEXES	GV$IM_SEGMENTS	SYSMAN.MGMT_TARGETS
DBA_LOBS	GV$INSTANCE	SYSMAN.MGMT_VERSIONS
DBA_LOB_PARTITIONS	GV$PARAMETER	V $ ARCHIVE_DEST_STATUS
DBA_LOB_SUBPARTITIONS	MDSYS.SDO_FEATURE_USAGE	V $BLOCK_CHANGE_TRACKING
DBA_OBJECTS	MDSYS.SDO_GEOM_METADATA_TABLE	V$CONTAINERS
DBA_RECYCLEBIN	MGMT$TARGET	V$DATABASE
DBA_REGISTRY	ODM.ODM_MINING_MODEL	V$DATAGUARD_CONFIG

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DBA_SQLSET	ODM_DOCUMENT	V$LICENSE
DBA_SQLSET_REFERENCES	ODM_RECORD	V$OPTION
DBA_SQL_PROFILES	REDACTION_POLICIES	V$PARAMETER
DBA_TABLES	SCHEMA_VERSION_REGISTRY	V$VERSION
DBA_TABLESPACES	SYS.CDC_CHANGE_SETS$	dba_aws
DBA_TAB_PARTITIONS	SYS.CDC_CHANGE_TABLES$	
DBA_TAB_SUBPARTITIONS	SYS.DBA_MINING_MODELS	

Datenbank-CI-Beziehungen

CI	Beziehung/Referenz	CI
cmdb_ci_orcl_vsession	Enthält::Enthalten in	cmdb_ci_db_ora_instance
cmdb_ci_ora_lms_detail	Enthält::Enthalten in	cmdb_ci_db_ora_instance
cmdb_ci_ora_lms_overview	Enthält::Enthalten in	cmdb_ci_db_ora_instance
cmdb_ci_orcl_options	Enthält::Enthalten in	cmdb_ci_db_ora_instance
cmdb_ci_orcl_dba_users	Enthält::Enthalten in	cmdb_ci_db_ora_instance
cmdb_ci_orcl_vlicense	Enthält::Enthalten in	cmdb_ci_db_ora_instance

Tuxedo-Middleware-Erweiterung

Tuxedo-Lizenzkonfiguration und erfasste Protokolldateien:

- *_InstallLog.log
- *ubbc*
- bdmconfig*
- comps.xml
- dmconfig*
- JSconfig.xml
- lic.txt
- registry.xml
- tuxconfig*
- tuxwsvr.ini

Hinweis: Das Sternchen steht für ein oder mehrere Zeichen im Dateinamen.

Erfasste Prozesse:

- BBL
- DBBL
- GWWS
- JSH
- JSL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- TMJAVASVR
- TMMETADATA

WebLogic-Middleware-Erweiterung

Erfasste Dateien:

- beahomelist
- biee-domain.xml
- cluster.properties
- comps.xml
- config.xml
- domain-registry.xml
- opmn.xml
- portalconfig.xml
- pthome.xml
- registry.xml
- server.xml
- sessions.xml
- setupinfo.txt

WebLogic-Prozesse und -Dateien, die für die folgenden Middleware-Produkte erfasst werden:

- WebLogic
- OAS
- SOA
- OBI
- WebCenter
- FormulareBerichte

Prozesse

WebLogic			OAS			OBI
startWebLogic	httpd	f90	iooomgrrmi	r30rbe32	rwrqm60	nqsserver
Java	Apache	frmweb	javaw	r30rqm32	rwrqm	sawserver
startWLS	Java	ifbld60	Java	r30run32	rwrun60	coreapplication_obijh1
nodemanager	opmn	ifbld90	jre	r30sxc32	rwserver	nqscheduler
beasvc	dis3	ifcgi60	oad	r30sxu32	rwsxc60	nqsclustercontroller
beasvc64	dis4	ifcmp60	odisrv	rwbld60	rwsxu60	essbase
beasvcX64	dis51pr	ifcmp90	ofcguard	rwbuilder	vdeserver	essvr
oraclesvc	dis51ws	ifctrl60	oidrepld	rwcgi60	webcachea	essbasestudio
opmn	dis51	ifdbg60	oidmon	rwcli60	webcached	hyperion

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozesse (Fortsetzung)

WebLogic		OAS				OBI
wlsvc	dwfde61	ifrun60	oidldapd	rwcon60	webcache	
wlsvc64	f45des	ifsrv60	opmn	rwconverter		
wlsvcX64	f45run	ifwdb60	r30cli32	rwisv60		
jmc	f50dbg32	ifweb60	r30con32	rwmts60		
httpd	f50run32	ifweb90	r30isv32	rwqmu60		
jrmc	f60	imapds	r30qmu32	rwrbe60		

Middleware-CI-Beziehungen

CI	Beziehung/Referenz	CI
cmdb_ci_ora_lms_overview	Enthält::Enthalten in	cmdb_ci_linux_server
cmdb_ci_config_file_tracked	Enthält::Enthalten in	cmdb_ci_linux_server

Diese Beziehungen werden von einer Containment-Regel erstellt, die die gültigen Objekte beschreibt, die in den Linux-CIs enthalten sein können.

Mit der Middleware-Datenerfassungsanwendung installierte Eigenschaften

Um auf die Eigenschaften der installierten Anwendung zuzugreifen, navigieren Sie zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**. Sie müssen über die Administratorrolle verfügen, um diese Eigenschaften zu ändern.

Systemeigenschaft	Standardwert	Beschreibung
sn_itom_oracleglas.isMaskingIp	wahr	Bestimmt, ob die IP-Adresse in nachverfolgten Middleware-Dateien Oracle maskiert werden soll, indem der Wert durch „text_removed“ ersetzt wird.
sn_itom_oracleglas.isMaskingUserName	wahr	Bestimmt, ob der Anwendername in nachverfolgten Middleware-Dateien Oracle maskiert werden soll, indem der Wert durch „text_removed“ ersetzt wird.
sn_itom_oracleglas.isMaskingPort	wahr	Bestimmt, ob der Port in nachverfolgten Middleware-Dateien Oracle maskiert werden soll, indem der Wert durch „text_removed“ ersetzt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Steuern Sie die Datensammlung der Middleware

Die folgende boolesche Systemeigenschaft kann die Middleware-Dateisammlung deaktivieren: *sn_itom_pattern.glas.disable_file_collection*

Steuern Sie die GLAS-Datenerfassung

Die folgende Eigenschaft MID-Server steuert die GLAS-Datensammlung: *sn_itom_pattern.disable_glas_data_collection*

Diese Eigenschaft ist standardmäßig auf **false** festgelegt.

Oracle Discovery des Java-Prozesses

ITOM-Transparenz kann Java-laufende Prozesse in Ihrer Infrastruktur erkennen, sodass Sie Oracle-Lizenzvereinbarungen einhalten und sich auf GLAS-Audits vorbereiten können. Sie können die Discovery entweder mit dem Muster *Java installation* (IP-basiert) oder mit Agent Client Collectordurchführen. Im Muster-Flow werden die Java-Prozesse von Application Dependency Mapping (ADM) erkannt. Wenn die -Prozesse erkannt werden, wird das Muster *Java installation* ausgelöst und die Daten werden gesammelt. Im ACC-Flow werden die Prozesse von ACC erkannt, was die ACC-Anwendungsmuster auslöst und die Daten sammelt. Weitere Informationen zu Mustern mit ACC finden Sie unter: Anwendungsmuster für Agent Client Collector

müssen Sie die folgenden Einstellungen haben:

- Alle Anwender müssen über die Store-App Oracle GLAS ab Version 1.8.4 verfügen.
- Agent Client Collector Anwender:
  - Muss das Store-Plugin Agent Client Collector Framework enthalten.
  - Für zusätzliche Daten kann das Store-Plugin Agent Client Collector Visibility – Inhalt Inhalt vorhanden sein.
  - Informationen zum Zugriff privilegierter Benutzer finden Sie unter KB1705845

Hinweis: Oracle Java-Discovery mit ACC gilt in allen Serverumgebungen. Derzeit wird sie jedoch für andere Desktopumgebungen teilweise unterstützt. Im folgenden KB-Artikel finden Sie ein Update Set für Windows Desktop. KB1705845

Erfasste Daten

Java-Audit [ora_java_audit]

Feld	Beschreibung
Name	Name des Datensatzes. Beispiel: Java@hostname
Name des physischen Computers	Name des Host-CI
Rechnertyp	Entweder Server(S) oder Desktop(D)
Java-Herausgeber/-Laufzeitanbieter	Java-Lieferantenname
Betriebssystem	Betriebssystem, in dem Java ausgeführt wird
Umgebungstyp	Produktions-, Entwicklungs- oder QA-Umgebung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Java-Audit [ora_java_audit] (Fortsetzung)

Feld	Beschreibung
Java-Release/-Version/-Build	Java-Version
Installationspfad	Absoluter Installationspfad der Java-Binärdatei
Installationsdatum (DateTime)	Datum und Uhrzeit der Erstellung der Java-Binärdatei im Dateisystem
Releasedatei (J/N)	Gibt an, ob eine *release.md*-Datei in der Installation vorhanden ist
Prozessormarke/-modell	Prozessormodellname
Sockets (Ganzzahl)	Anzahl der CPU-Sockel
Kerne (Ganzzahl)	Anzahl der CPU-Kerne
V6 und früher	Gibt an, ob Sie eine Java-Version 6 oder früher haben
Open Source	Gibt an, ob Sie über eine Open-Source-Java-Installation verfügen
Schalten Sie kommerzielle Funktionen frei	Gibt an, ob für Sie die gewerblichen Funktionen (wie JFR) aktiviert haben
Missionssteuerung	Gibt an, ob das Missionssteuerungs-Plugin aktiviert ist
AMC-Agent	Gibt an, ob das AMC-Agent-Plugin aktiviert ist
Nutzungs-Tracker	Gibt an, ob die Funktion „Nutzungstracker“ aktiviert ist
Objekt-ID der VM	Objekt-ID der VM-Instanz
PID	PID des laufenden Prozesses
IP-Adresse	IP-Adresse des Hosts/der VM
Zuerst erkannt	Das Datum der ersten Discovery
Neuester Discovery-Scan	Das Datum der neuesten Discovery
Discovery-Quelle	Die Discovery-Methode.
Anwendung	Verweis auf die Tabelle [cmdb_ci_appl].
Softwareinstallation	Verweis auf die Tabelle [cmdb_sam_sw_install].
Java-Beweis	Verweis auf die Tabelle [cmdb_ora_java_evidence].
Host	Verweis auf die Tabelle [cmdb_ci].

Java-Nachweis [ora_java_evidence]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

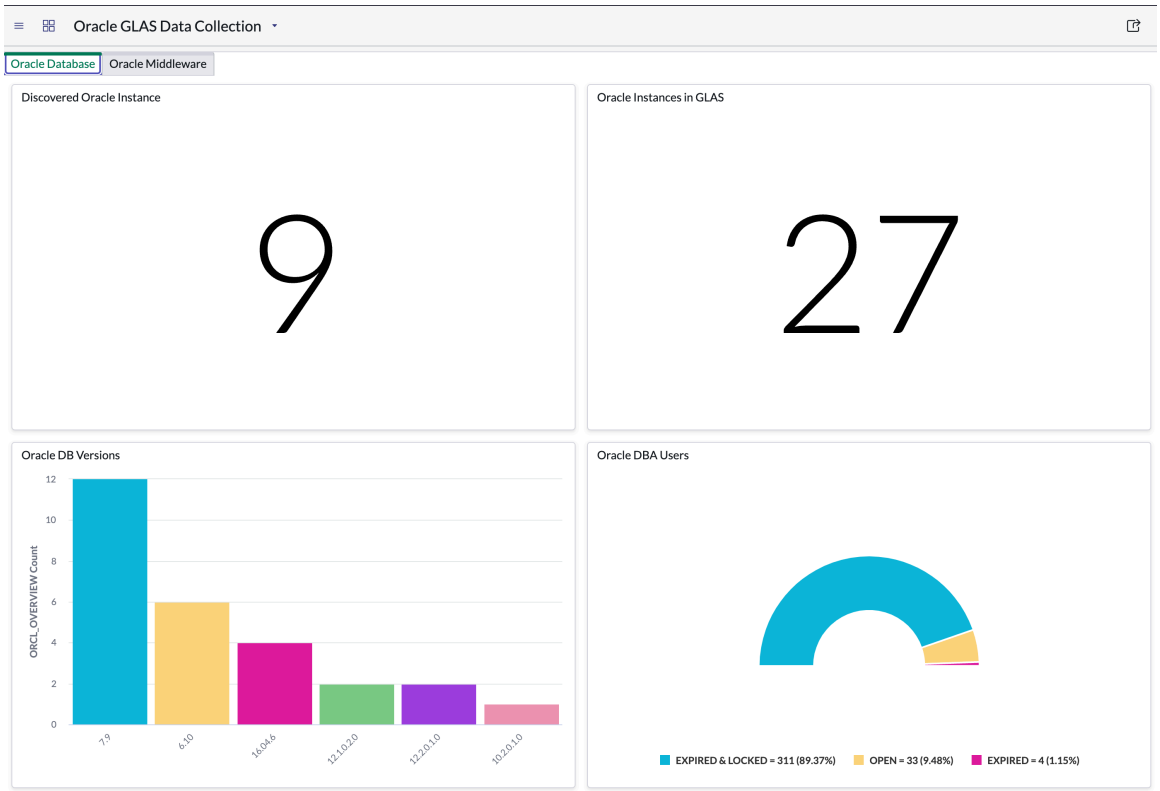
Feld	Beschreibung
Laufender Prozess	Verweis auf die Tabelle [cmdb_running_process].
Host-CI	Verweis auf die Tabelle [cmdb_ci_computer].
Datei-Informationen	Verweis auf die Tabelle [cmdb_file_information].

Laden Sie den Oracle GLAS-Bericht in Discovery-Administratorarbeitsbereich herunter. Weitere Informationen finden Sie unter Oracle GLAS-Daten (Global License Advisory Services) herunterladen.

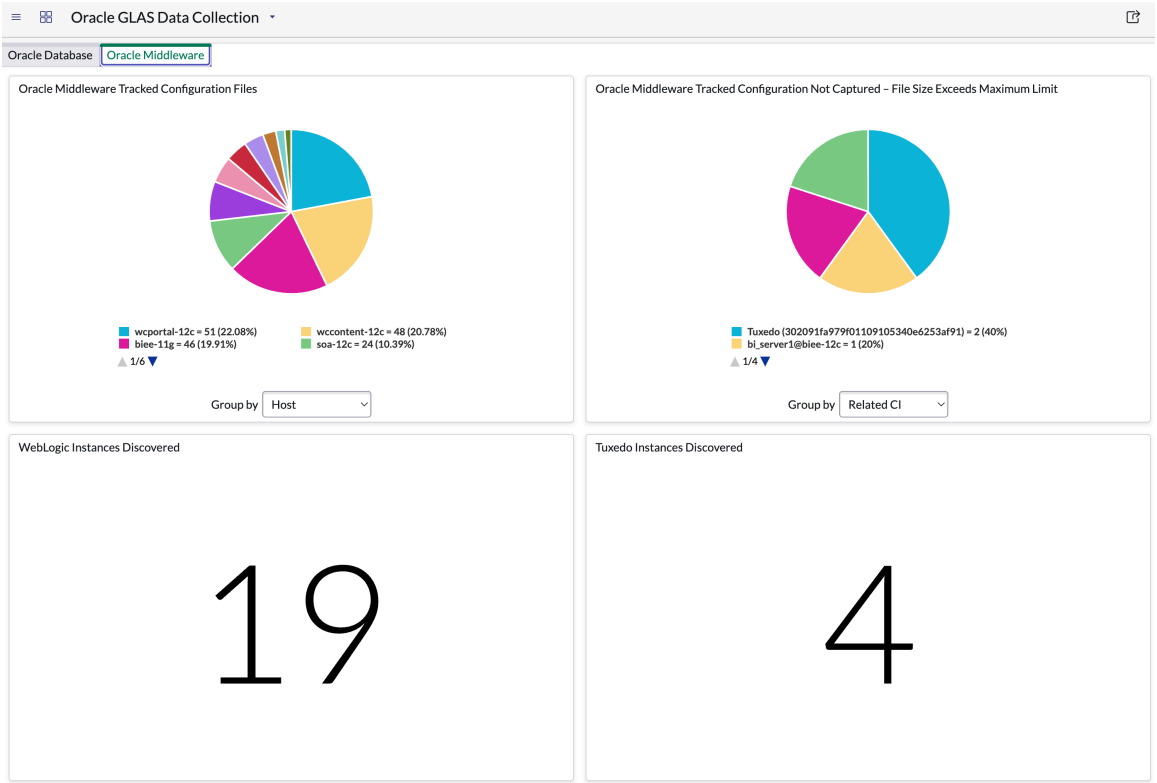
Oracle GLAS Data Collection – Dashboard

Nachdem Discovery die Erkennung der Komponenten Ihrer Datenbank- oder Middleware-Bereitstellung abgeschlossen hat, können Sie die relevanten Statistiken im Dashboard Oracle „ GLAS-Datensammlung anzeigen.

Nach dem Upgrade auf Discovery-Administratorarbeitsbereich Version 1.3.1 (Store August 2024) können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** und verwenden Sie das erweiterte Dashboard.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Oracle GLAS-Daten (Global License Advisory Services) herunterladen

Laden Sie Oracle GLAS-Daten im CSV-Format herunter, um detaillierte Informationen zu Mustern und Configuration Items zu erhalten. Sie können auch Berichte für Oracle Datenbank-, Middleware-, Oracle Java-, VM- und vCenter-Hardwareinformationen herunterladen.

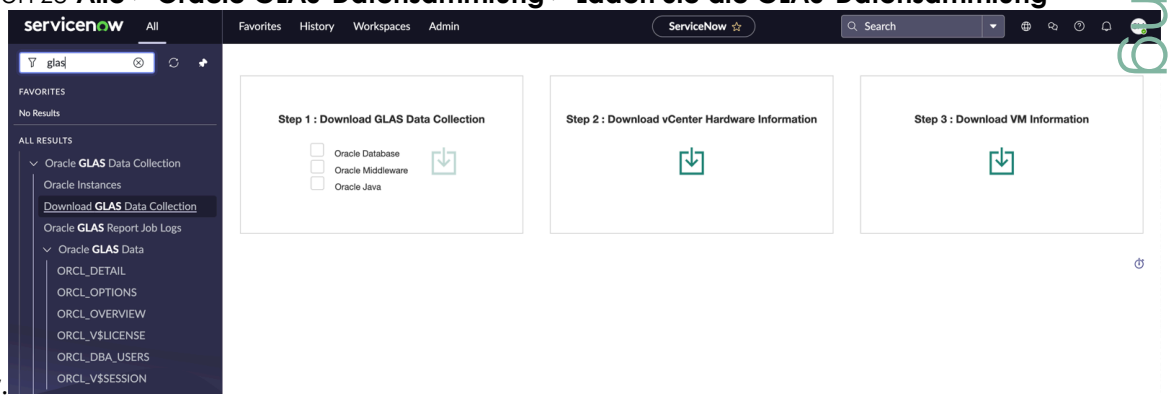
Vorbereitungen

Informationen zum Herunterladen des Oracle GLAS-Java-Berichts für Versionen vor Washington DC Patch 9 und Xanadu Patch 3 finden Sie unter KB1704359 .

Erforderliche Rolle: admin oder glas_admin

Prozedur

1. Navigieren zu **Alle** > **Oracle GLAS-Datensammlung** > **Laden Sie die GLAS-Datensammlung herunter.**



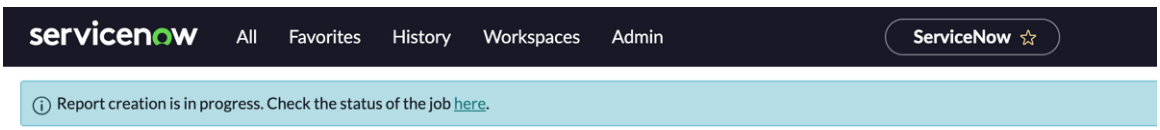
2. Laden Sie die folgenden Berichte für Oracle GLAS-Daten herunter:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um Oracle Datenbank-, Middleware- und Java-Berichte herunterzuladen, navigieren Sie zu **Schritt 1: GLAS-Datensammlung herunterladen**, und wählen Sie Ihre Datensammlungsoptionen aus.
- Um basierend auf dem Setup Ihrer Umgebung vCenter-Hardwareinformationen herunterzuladen, navigieren Sie zu **Schritt 2: vCenter-Hardwareinformationen herunterladen**.
- Um VM-Informationen herunterzuladen, navigieren Sie zu **Schritt 3: VM-Informationen herunterladen**.

3. Wählen Sie das Download-Symbol ( ).
4. Geben Sie im Dialogfeld „E-Mail-Adresse eingeben“ die E-Mail-Adresse ein, an die Sie eine Benachrichtigung erhalten möchten, wenn der Bericht fertig ist.
5. Wählen Sie **OK**.
   Nachdem die Statusmeldung für die Berichterstellung angezeigt wird, können Sie den Status des Downloadauftrags überprüfen, indem Sie den in der Meldung angegebenen Link auswählen.



   Die Tabelle „Oracle GLAS-Berichtsauftragsprotokoll“ [sn_itom_oraclefenster_job_log] wird in einem neuen Fenster geöffnet. Nachdem Ihr Bericht erfolgreich erstellt wurde, ändert sich der Status des Berichts in der Tabelle „Oracle GLAS-Berichtsauftragsprotokolle“ in „Abgeschlossen“.

6. Wählen Sie einen Aufgabenprotokolldatensatz aus, um die zugehörigen Details anzuzeigen, einschließlich der eindeutigen Nummer, des Namens, des Status, der Beschreibung sowie des Datums und der Uhrzeit, zu der das Aufgabenprotokoll erstellt und aktualisiert wird.
7. Laden Sie im Formular „Oracle GLAS-Berichtsauftragsprotokoll“, das sich öffnet, Ihren Bericht herunter, indem Sie zu **Anhänge verwalten** navigieren und **Download**auswählen.

   - Wenn Sie Oracle Datenbank auswählen, werden die folgenden CSV-Dateien heruntergeladen:
     - `ORCL_V$SESSION.csv`
     - `ORCL_OPTIONS.csv`
     - `ORCL_DBA_USERS.csv`
     - `ORCL_DETAIL.csv`
     - `ORCL_V$LICENSE.csv`
     - `ORCL_OVERVIEW.csv`
   - Wenn Sie Oracle Middleware auswählen, werden die folgenden Dateien in dem Format exportiert, das für den Servernamen und das installierte Produkt Oracle angezeigt wird:
     - ORCL_OVERVIEW.csv
     - `Collection-<Server Name>_<Oracle Product>.tar.bz` mit den Dateien und Verzeichnissen des Formats FMW/u01/app/oracle/config/domains/soa_domain/config/config.xml.
   - Wenn Sie Oracle Java auswählen, werden die folgenden Ordner heruntergeladen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Java-Ordner: Enthält Java-Installationsinformationen
- CPUQ-Ordner – Enthält Informationen zu CPUQ-Dateien, vCenter-Hardware und VM

Hinweis: Sie können die CSV-Dateien für Oracle die Datenbank auch herunterladen, indem Sie zu navigieren **Oracle GLAS-Datensammlung** > **Oracle GLAS-Daten**. Wählen Sie in der Liste, die sich öffnet, die Tabelle aus, die Sie herunterladen möchten, und wählen Sie dann **GLAS-Bericht herunterladen**aus.

Ergebnisse
Die heruntergeladenen Dateien werden an dem von Ihnen ausgewählten Speicherort angezeigt.

Trouble?

Wenn die Dateien leer sind oder eine Fehlermeldung enthalten, überprüfen Sie ihre Größe, um sicherzustellen, dass sie die in den folgenden Eigenschaften festgelegten Grenzwerte nicht überschritten haben. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften** um die folgenden Eigenschaften zu finden.

Wichtig: Wenden Sie sich an den Support von ServiceNow, bevor Sie diese Eigenschaften ändern.

Eigenschaft	Beschreibung
glide.discovery.file_tracking.max_file_size	Maximale Dateigröße für den Inhalt der verfolgten Konfigurationsdatei. Typ: Ganzzahl Standardwert: 500.000
glide.discovery.file_tracking.max_files_per_ci	Maximale Anzahl verfolgter Konfigurationsdateien pro CI. Typ: Ganzzahl Standardwert: 50
glide.discovery.file_tracking.change_limit_count	Anzahl der Changes, die für eine nachverfolgte Konfigurationsdatei im definierten Zeitfenster zulässig sind. Typ: Ganzzahl Standardwert: 4
glide.discovery.file_tracking.change_limit_days	Zeitfenster (in Tagen), das die Anzahl der Änderungen an einer verfolgten Konfigurationsdatei begrenzt. Typ: Ganzzahl Standardwert: 7

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie die Fehlermeldung `Fehler: Sensor für horizontales Muster aufgrund eines Fehlers in Nutzlast übersprungen: Nutzlastlänge 5056040 hat den Grenzwert von 300000 überschritten erhalten`, stellen Sie sicher, dass die Nutzlast das Systemlimit nicht überschritten hat. Navigieren zu **Alle** > **MID-Server** > **Eigenschaften** um die folgenden Eigenschaften zu finden.

Eigenschaft	Beschreibung
mid.discovery.max_payload_size	Definiert die maximale Gesamt-Payload-Größe für den Payload von Ergebnissen, die aus Mustern stammen. Typ: Ganzzahl (Bytes) Standardwert: 300000

Wenn ein SSH-Zeitüberschreitungsfehler auftritt, müssen Sie die folgenden Eigenschaften erstellen und festlegen. Weitere Informationen finden Sie unter „Eine MID-Server-Eigenschaft erstellen“ in Eigenschaften von MID-Servern .

Eigenschaft	Beschreibung
mid.ssh.command_timeout_ms	Anzahl der Millisekunden, die ein SSH-Befehl ausgeführt werden darf, bevor eine Zeitüberschreitung auftritt (Standardeinstellung ist per MID-Serverkonfigurierbar). Typ: Ganzzahl
mid.sa.ssh.timeout	Die SSH-Zeitüberschreitung in Millisekunden. Typ: Ganzzahl
channel_timeout_ms	Der Zeitraum in Millisekunden, der von einem MID-Server während der Verarbeitung eines SSH-Befehls auf Aktivität gewartet wird. Wenn MID-Server innerhalb des angegebenen Fensters keine Aktivität erkennt, beendet das System den Befehl. Typ: Ganzzahl

Oracle GoldenGate-Erkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping finden Oracle Golden Gate Version 12c-Komponenten mithilfe des Musters Oracle Golden Gate. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery verwendet das Muster Oracle Golden Gate, um eine horizontale Erkennung durchzuführen, um Daten in der Datei `$report_file` zu sammeln. Service-Mapping führt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eine Erkennung von oben nach unten für die Datei `$report_file` durch, um ausgehende Oracle Golden Gate-Verbindungen zu finden.

Das Muster „Oracle Golden Gate“ unterstützt die folgenden Plattformen: AIX, Linux Hewlett Packard und Solaris.

Sie können dieses Muster auf der Now Platform mithilfe von Kingston, London oder Madrid verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Berechtigungen

Konfigurieren Sie die SSH-Anmeldeinformationen für das Betriebssystem des Servers, auf dem der Oracle Golden Gate-Server gehostet wird.

Benutzerzugriff

Erteilen Sie dem UNIX-Betriebssystembenutzer die Berechtigung zum Lesen der `$report_file`. Die `$report_file` ist die Berichtsdatei, die aus dem Prozess Oracle Golden Gate `manager/replicat/extract`-Prozess mit der Erweiterung `.rpt` extrahiert wird. Beispiel:

Konfigurationsdatei:

```
/base/ggs_beta/oracle/bt01pims/ggs/dirprm/mgr.prm REPORTFILE
```

Berichtsdatei:

```
/base/ggs_beta/oracle/bt01pims/ggs/dirrpt/MGR.rpt PROCESSID MGR
```

Berechtigungen zum Ausführen von Befehlen

Der Betriebssystembenutzer muss über Berechtigungen zum Ausführen der relevanten Betriebssystembefehle für jede unterstützte Plattform verfügen.

Geben Sie dem UNIX-Betriebssystembenutzer Berechtigungen, die folgenden Befehle gegen den Oracle Golden Gate-Server auszuführen:

Befehl	Obligatorisch/Optional	Beschreibung
`$sudo + " ls -d " + $rpt_base_dir + "*.rpt | sort "`	Obligatorisch	Listet alle Berichtsdateien im Oracle Golden Gate-Berichtsbasisverzeichnis auf
`$sudo + " ls -d " + $prm_base_dir + "*.prm| sort "`	Obligatorisch	Listet alle Parameterdateien im Oracle Golden Gate-Parameterbasisverzeichnis auf

Daten abrufen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rufen Sie Daten ab, indem Sie folgende Elemente analysieren:

- Die Oracle Golden Gate Manager-Berichtsdatei (report_file) zum Abrufen zugehöriger Configuration Item-Namen (CI) und Zählerinformationen.
- Variablen in der Prozessbefehlszeile zum Abrufen des Installationsordners, des Manager-Prozessnamens, der Konfigurationsdatei und der Parameterdatei
- Variablen im Oracle Golden Gate-Installationsordner, um eine Liste von Parameter- und Konfigurationsdateien abzurufen

EVAL-Abschlussfunktionen

Verwenden Sie die folgenden EVAL-Abschlussfunktionen, um doppelte Einträge aus dem Extraktionsprozess und dem Replikationsprozess zu entfernen.

- var tableWithoutDuplicates = '';tableWithoutDuplicates = DuplicateRemover.removeDuplicates(${extracts}, ["name"]);CTX.setAttribute("extracts", tableWithoutDuplicates);
- var tableWithoutDuplicates = '';tableWithoutDuplicates = DuplicateRemover.removeDuplicates(${replicats}, ["name"]);CTX.setAttribute("replicats", tableWithoutDuplicates);

Verwenden Sie die folgenden EVAL-Abschlussfunktionen, um die Anzahl der Extraktionsprozesse und der Replikationsprozesse zu zählen.

```
return ${cmdb_ci_appl_ora_gg_replicat[*].config_file}.size()
return ${cmdb_ci_appl_ora_gg_extract[*].config_file}.size()
```

Verwenden Sie die folgende EVAL-Abschlussfunktion, um den privilegierten Befehl zurückzugeben.

```
return
 ${ctx}.getDiscoveryProvider(com.snc.sw.dto.ProviderType.SSH).g
etPrivilegedCommand();
```

Verwenden Sie die folgende EVAL-Abschlussfunktion, um den Erkennungstyp zurückzugeben.

```
ctx.getWork().getDiscoveryType();
```

Verwenden Sie die folgende EVAL-Abschlussfunktion, um die Version aus dem Installationsverzeichnispfad zu extrahieren, wenn sie leer ist.

```
inst_dir = ${install_directory}if(inst_dir.isEmpty()){return
 ${version}}if(inst_dir.startsWith('/')){return
 inst_dir.replaceAll('/.*/','')}if(!inst_dir.startsWith('/')
 && !inst_dir.isEmpty()){return
 inst_dir.replaceAll('.*\\\\',’’)}
```

Applicative-Anmeldeinformationen

1. Navigieren zu **Discovery** > **Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.
3. Klicken Sie auf **Applicative-Anmeldeinformationen**.
4. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Applicative-Anmeldeinformationen“

Feld	Beschreibung
Name	Name der Anmeldeinformationen Beispiel: oracle_db_user.
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Betrifft	Anmeldeinformationen, die Sie auf **Alle MID Server** in Ihrem Netzwerk oder auf einen oder mehrere **Spezielle MID Server** anwenden oder nicht anwenden möchten. Wählen Sie **Spezielle MID Server** aus.
MID Servers	MID Server, für die die Anmeldeinformationen gelten. Wählen Sie den erforderlichen MID Server aus. Dieses Feld wird angezeigt, wenn Sie **Spezielle MID Server** im Feld **Gilt für** auswählen.
Reihenfolge	Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten verwendet. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist **100**.
Benutzername	Name des Benutzers dieser Applicative-Anmeldeinformationen. Beispiel: oracle_db_user. Sie können einen beliebigen Benutzer für die Anmeldeinformationen für dieses Muster verwenden, da die Informationen aus einem lokalen Cache extrahiert werden.
Passwort	Nicht erforderlich. Sie können dieses Feld leer lassen oder einen beliebigen Wert eingeben.
CI-Typ	CI-Typ, für den diese Anmeldeinformationen verwendet wird: Speicherserver [cmdb_ci_storage_server] **Hinweis:** ServiceNow -Anwendungen beziehen sich auf Geräte und Anwendungen, die eine Serviceinstanz als Configuration Items (CIs) umfassen.

5. Klicken Sie auf **Absenden**.

Eingabepunkt

Verwenden Sie für die Erkennung von oben nach unten die Oracle Golden Gate-IP-Adresse, und geben Sie den MID Server an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery verwendet das Oracle Golden Gate-Muster zum Sammeln der in der folgenden Tabelle beschriebenen Daten.

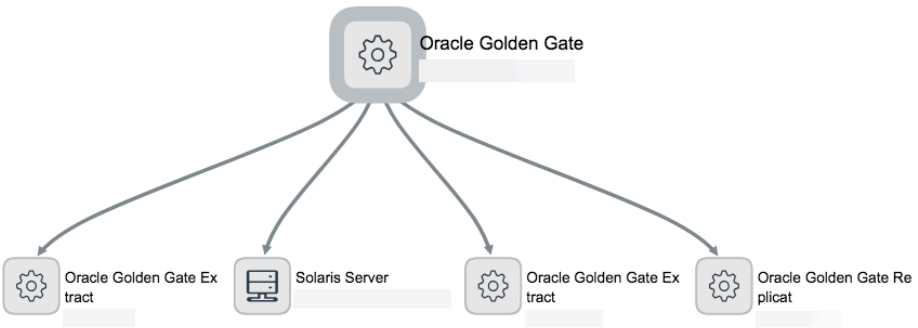
Tabelle und Feld	Beschreibung
Haupt-CI cmdb_ci_appl_oracle_golden_gate	
Name [name]	Name des CI in der CMDB (<process name>@<source db>).
Version [version]	Version der Installation von Oracle Golden Gate
Quell-DB [source_db]	Managerprozess-Quelldatenbanksystem-Bezeichner (SID)
Anzahl der Replikate [count_replicat]	Zähler der Replikatprozesse, die von der Oracle Golden Gate-Managerinstanz verwaltet werden
Anzahl der Extrakte [count_extract]	Zähler der Extraktprozesse, die von der Oracle Golden Gate-Managerinstanz verwaltet werden.
Konfigurationsdatei [config_file]	Parameterdatei des Oracle Golden Gate-Prozesses. Geben Sie den Pfad zur Konfigurationsdatei und den Dateinamen an, <name>.prm.
Berichtsdatei [report_file]	Berichtsdatei des Oracle Golden Gate-Prozesses. Geben Sie den Pfad zur Berichtsdatei und den Dateinamen an, <name>.rpt.
Typ [type]	Typ der Oracle Golden Gate-Installation. Geben Sie Oracle Golden Gate für Oracle-Technologien an.
Installationsverzeichnis [install_directory]	Ordner, der alle Setup-, Konfigurations-, Bibliotheks- und ausführbaren Dateien von Oracle Golden Gate enthält
Zugehöriges CI cmdb_ci_appl_ora_gg_replicat	
Name [name]	Name des CI in der CMDB (<process name>@<source db>).
Berichtsdatei [report_file]	Replikat-Prozessberichtsdatei. Geben Sie den Pfad zur Berichtsdatei und den Dateinamen an, <name>.rpt.
Konfigurationsdatei [config_file]	Parameterdatei des Replikatsprozesses. Geben Sie den Pfad zur Konfigurationsdatei und den Dateinamen an, <name>.prm.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Installationsverzeichnis [install_directory]	Ordner, der alle Setup-, Konfigurations-, Bibliotheks- und ausführbaren Dateien von Oracle Golden Gate enthält
Version [version]	Version der Installation von Oracle Golden Gate
Quell-DB [source_db]	Managerprozess-Quelldatenbanksystem-SID
Betriebsstatus [operational_status]	Betriebsstatus des CI. Wählen Sie **Funktionsfähig** aus.
Zugehöriges CI cmdb_ci_appl_ora_gg_extract	
Name [name]	Name des CI in der CMDB (<process name>@<source db>).
Berichtsdatei [report_file]	Berichtsdatei des Replikatprozesses
Konfigurationsdatei [config_file]	Parameterdatei des Extraktprozesses
Version [version]	Version der Installation von Oracle Golden Gate
Installationsverzeichnis [install_directory]	Ordner, der alle Setup-, Konfigurations-, Bibliotheks- und ausführbaren Dateien von Oracle Golden Gate enthält
Quell-DB [source_db]	Managerprozess-Quelldatenbanksystem-SID
Betriebsstatus [operational_status]	Betriebsstatus des CI. Wählen Sie **Funktionsfähig** aus.

Die Dependency Views-Zuordnung zeigt die erkannten Lastenausgleichsmodul-CIs und deren Beziehung untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CI-Beziehungen

Diese Beziehungen sollen die Oracle Golden Gate-Erkennung unterstützen.

CI	Beziehung	CI
Haupt cmdb_ci_appl_oracle_golden_gate		
cmdb_ci_appl_oracle_golden_gate	Verwaltet::Verwaltet von	cmdb_ci_appl_ora_gg_replicat cmdb_ci_appl_ora_gg_extract
cmdb_ci_appl_oracle_golden_gate	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_hardware
cmdb_ci_appl_oracle_golden_gate	Erweitert::Erweitert um	cmdb_ci_appl
Zugehöriges CI cmdb_ci_appl_ora_gg_replicat		
cmdb_ci_appl_ora_gg_replicat	Verwaltet von::Verwaltet	cmdb_ci_appl_oracle_golden_gate
cmdb_ci_appl_ora_gg_replicat	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_hardware
cmdb_ci_appl_ora_gg_replicat	Erweitert::Erweitert um	cmdb_ci_appl
Zugehöriges CI cmdb_ci_appl_ora_gg_extract		
cmdb_ci_appl_ora_gg_extract	Verwaltet von::Verwaltet	cmdb_ci_appl_oracle_golden_gate
cmdb_ci_appl_ora_gg_extract	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_hardware
cmdb_ci_appl_ora_gg_extract	Erweitert::Erweitert um	cmdb_ci_appl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Zum Erkennen des Oracle Golden Gate-Prozesses verwenden Sie den TCP-Einstiegspunkt mit dem richtigen Host und Port des Oracle Golden Gate-Prozesses.

Tabelle und Feld	Beschreibung
Haupt-CI cmdb_ci_appl_oracle_golden_gate	
Name [name]	Name des CI in der CMDB (<process name>@<source db>).
Version [version]	Version der Installation von Oracle Golden Gate
Installationsverzeichnis [install_directory]	Ordner, der alle Setup-, Konfigurations-, Bibliotheks- und ausführbaren Dateien von Oracle Golden Gate enthält
Konfigurationsdatei [config_file]	Parameterdatei des Oracle Golden Gate-Prozesses.
Berichtsdatei [report_file]	Berichtsdatei des Oracle Golden Gate-Replikatprozesses
Quelldatenbank [source_db]	Managerprozess-Quelldatenbanksystem-SID
Extraktprozesszähler [count_extract]	Zähler der Extraktprozesse, die von der Oracle Golden Gate-Managerinstanz verwaltet werden.
Replikatprozesszähler [count_replicat]	Zähler der Replikatprozesse, die von der Oracle Golden Gate-Managerinstanz verwaltet werden

Oracle Listener HD -Discovery

ServiceNow Discovery verwendet das Listener-HD-Muster Oracle, um Oracle echte Anwendungsclusterkomponenten zu finden und zuzuordnen. Um diese Ressourcen zu erkennen, installieren Sie die CMDB-CI-Klassenmodelle und Muster für Discovery und Service-Mapping aus dem ServiceNow Store.

Oracle RAC ermöglicht das Clustering einer Oracle -Datenbank. Oracle RAC verwendet Oracle Clusterware für die Infrastruktur, um mehrere Server so zu binden, dass sie wie ein einheitliches System arbeiten. MitOracle Clusterware können Sie einen gruppierten Speicherpool erstellen, der von einer beliebigen Kombination aus Nicht-Cluster-Datenbanken und Oracle RAC-Datenbanken verwendet werden kann. Discovery verwendet HD-Muster des Oracle Listeners, um Informationen über den Datenbank-Listener Oracle und die Komponenten in der RAC-Infrastruktur Oracle zu erkennen, wenn ein solches Setup konfiguriert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass die folgenden Plugins installiert sind:
  - Plugin „CMDB CI Class Models“ (Version 1.29.0 oder höher).
  - Muster für Discovery und Service-Mapping Plugin (Version 1.0.82 oder höher).
- Stellen Sie sicher, dass der Benutzer Discovery in der DBA-Gruppe Oracle ist oder über die richtigen Berechtigungen verfügt.
- Stellen Sie sicher, , dass der MID-Server Zugriff auf das Zielgerät hat.
- Stellen Sie sicher, dass die Clusterware-/Grid-Infrastruktur Oracle installiert und die RAC-Datenbank Oracle konfiguriert ist. Wenn ein Oracle Clusterware-Setup vorhanden ist.
- Stellen Sie sicher, dass der Listener-Prozess Oracle auf einem UNIX-BS-Host ausgeführt wird.
- Verwenden Sie Oracle Clusterware Mindestversion 12.2.XX (Oracle Database 12c Release 2) oder höher, Bei einem Oracle Clusterware-Setup.

Hinweis: Dieses Muster wird ab Release Paris aufunterstützt. Weitere UNIX-Betriebssystemtypen (AIX, Solaris, HPUX) werden ab Version 1.0.87 von den Plugins Muster für Discovery und Service-Mapping unterstützt.

Die folgenden Befehle werden während der Ausführung des Musters ausgeführt. Durch Ausführen der Befehle kann das Muster allerelevanten CMDB-Klassen mit den erforderlichen Informationen füllen:

- **Exportieren Sie TNS_ADMIN =**<oracle_home_directory> /network/admin : LegttORACLE_HOME auf die Umgebungsvariable TNS_ADMIN fest.
- **Export ORACLE_BASE ==**<oracle_home_directory> : Legt ORACLE_HOME auf die Umgebungsvariable ORACLE_BASE fest.
- **lsnrctl status LISTENER_NAME**: Überprüft den Status des Datenbank-Listeners .
- **ps -ef | grep 'd.bin'**: Sucht nach dem GRID_HOME-Pfad
- **CRSCTL Query Cluster Site -all**: Listet die Knoten und Datenträger auf, die die Sites enthalten
- **lsnrctl services LISTENER_NAME**: Listet die Services auf , die der Listener identifiziert.
- **scrtl stat res -f -w '((TYPE = ora.database.type))'**: Listet den Datenbanknamen, den zugehörigen Knoten, den Typ und den aktiven Statusauf.

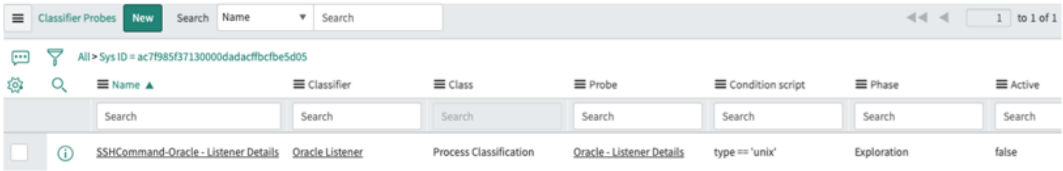
Hinweis: Wenn von **lsnrctl status LISTENER_NAME** keine Ausgabe abgerufen wird, wird das Muster **Oracle Listener HD** beendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einschränkungen

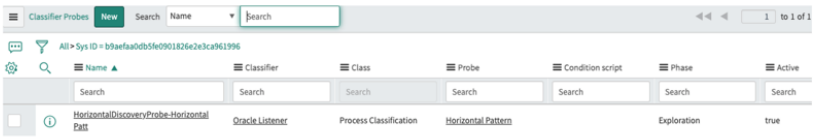
Das Oracle Clusterware-Setup wird nur für UNIX-Betriebssysteme unterstützt. Die **Klassifizierungsprobe „SSH-Befehl-Oracle – Listenerdetails“** des Basissystems ist inaktiv („Aktiv“ ist auf „Falsch“ festgelegt), wenn Sie CMDB CI Class Models Version 1.29.0 oder höher installieren.

Klassifizierungsprobes- Oracle-Listener-Details



Die **Oracle Listener-Prozessklassifizierung** löst das Muster „Oracle Listener HD“ aus.

Klassifizierungsprobes– Horizontales Muster



Von Discovery während der horizontalen Erkennung erfasste Daten

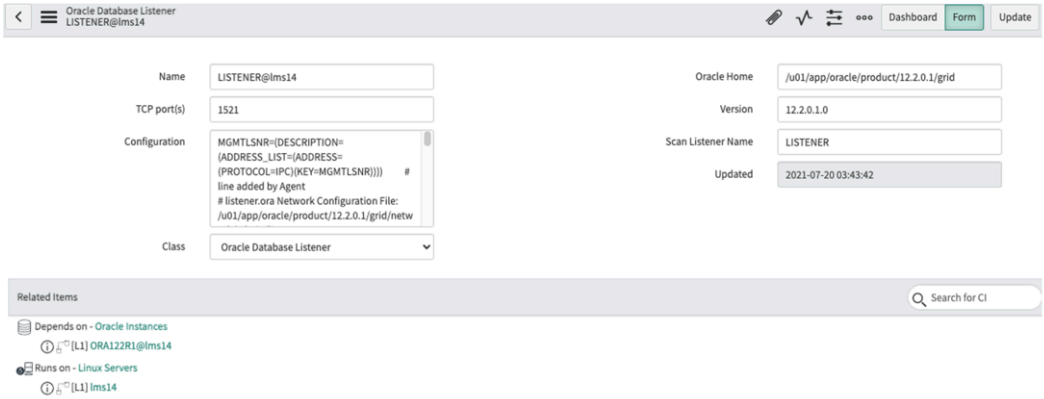
Das Muster „Oracle Listener HD“ füllt die folgenden CIs aus:

Haupt-CI (Oracle Database Listener) [cmdb_ci_db_ora_listener]

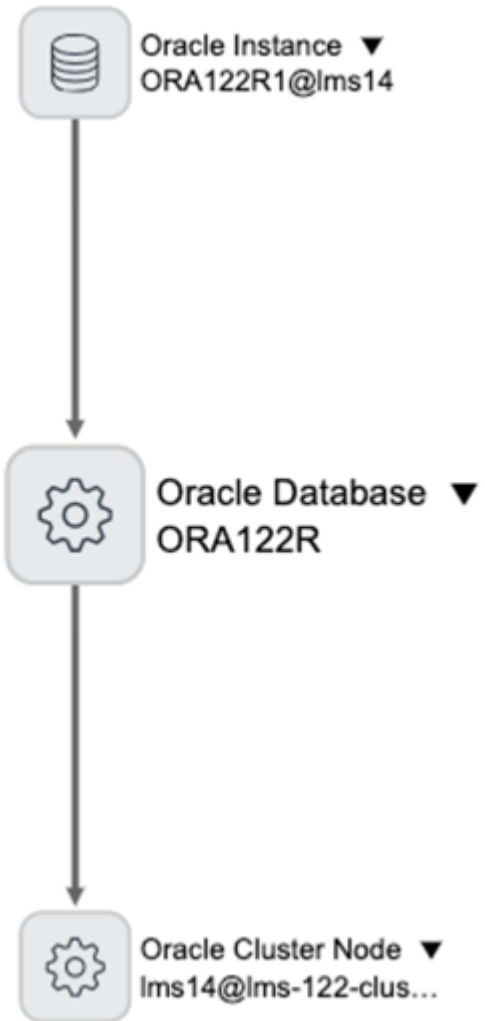
Feld	Beschreibung
name	Der Name des Oracle-Datenbanklisteners.
oracle_home	Das Oracle-Stammverzeichnis, in dem die Software installiert ist.
konfigurieren	Die Netzwerkkonfigurationsdatei listener.ora.
scan_listener_name	Der Name des SCAN LISTENER.
Version	Version des Oracle-Produkts.
tcp_port	Der Überwachungsport für Oracle-Client-Verbindungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Oracle-Datenbanklistener“



Oracle-Datenbanklistener-Ansichtszuordnung



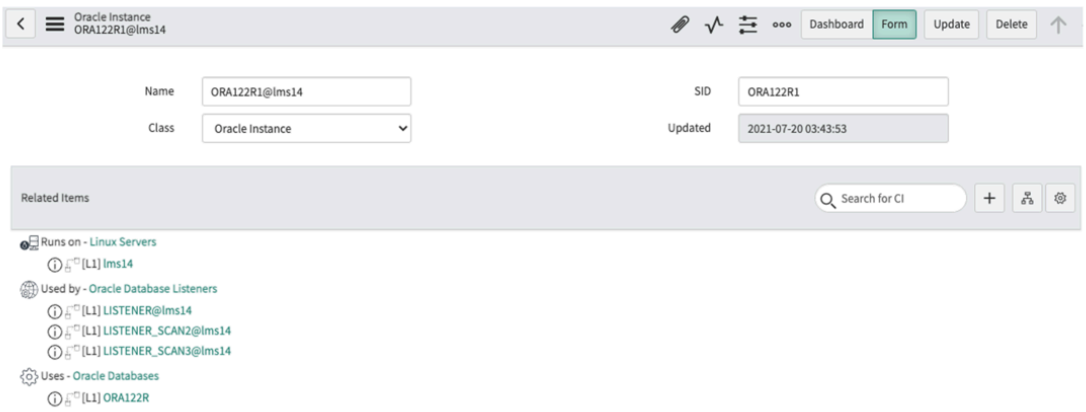
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

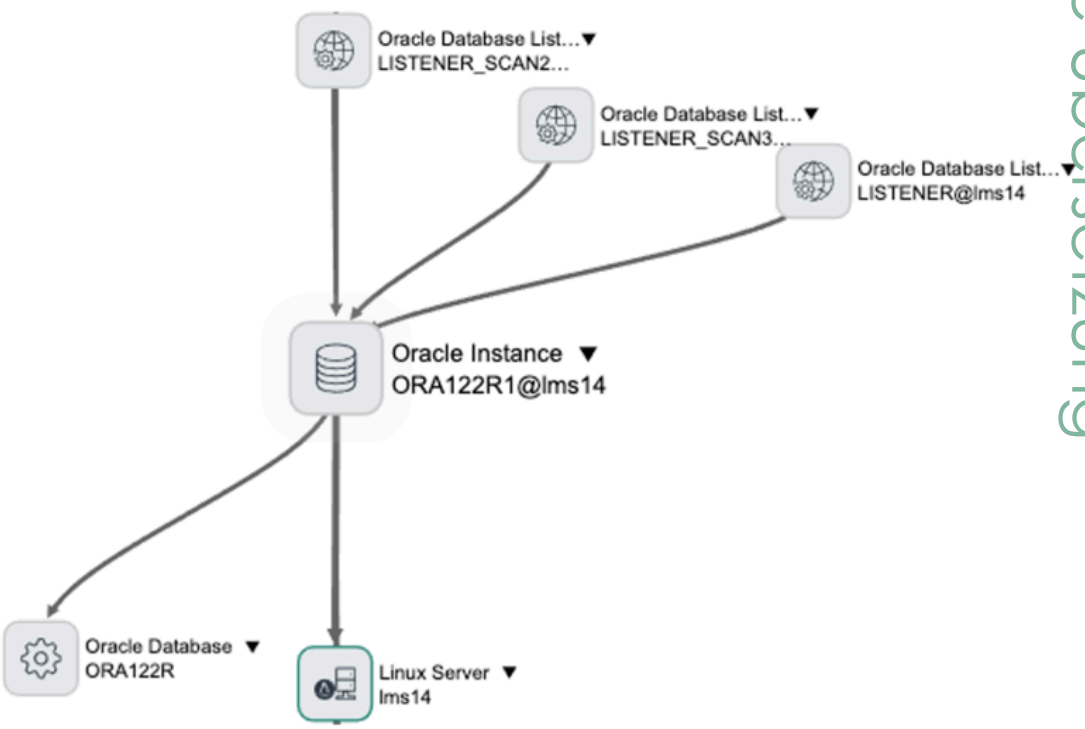
(Oracle-Instanz) cmdb_ci_db_ora_instance

Feld	Beschreibung
sid	Der spezifische Name, der speziell die Instanz identifiziert.
name	Der Name der Oracle-Instanzkombination von SID@HOST_NAME.

Formular „Oracle-Instanz“



Oracle-Instanz-Ansichtszuordnung



Automatische Übersetzung

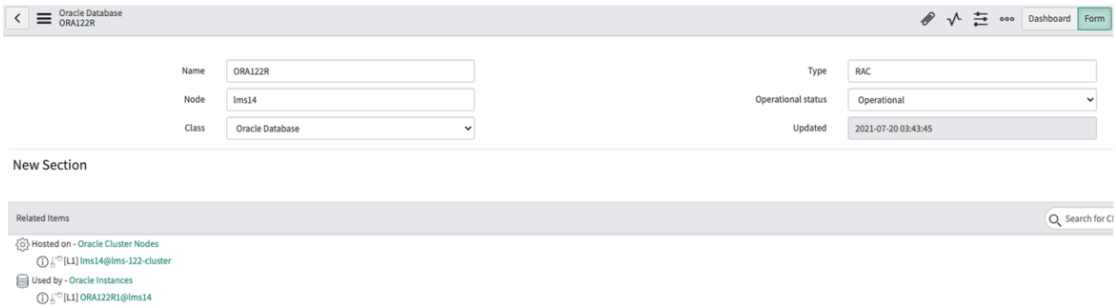
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Oracle-Datenbank) cmdb_ci_oracle_database

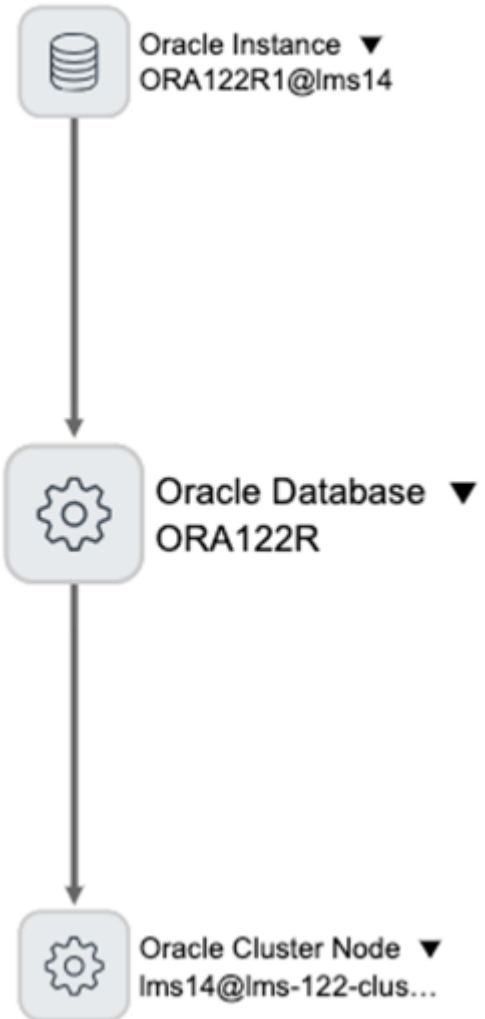
Feld	Beschreibung
name	Der eindeutige Name der Oracle-Datenbank.
Typ	Typ der Oracle-Datenbank
operational_status	Der aktive Status der Oracle-Datenbank.
Knoten	Der Hostname des Knotens, der die Oracle-Datenbank hostet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Oracle-Datenbank“



Oracle-Datenbank-Ansichtszuordnung



(Oracle-Cluster) cmdb_ci_oracle_cluster

Feld	Beschreibung
name	Der Name des Oracle-Datenbankclusters.
cluster_id	Die GUID des Oracle-Datenbankclusters.

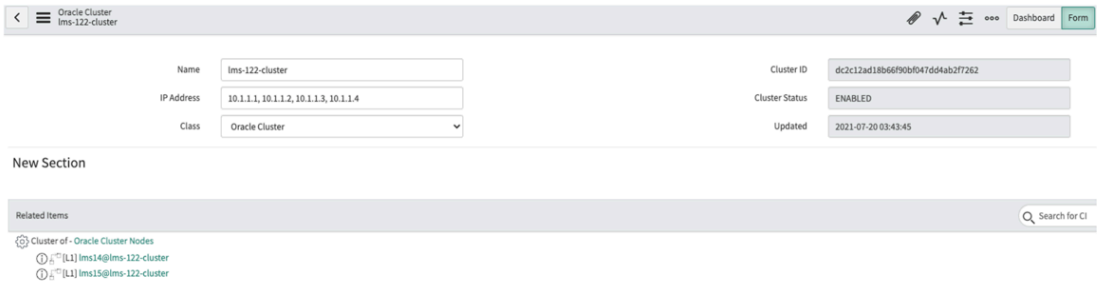
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

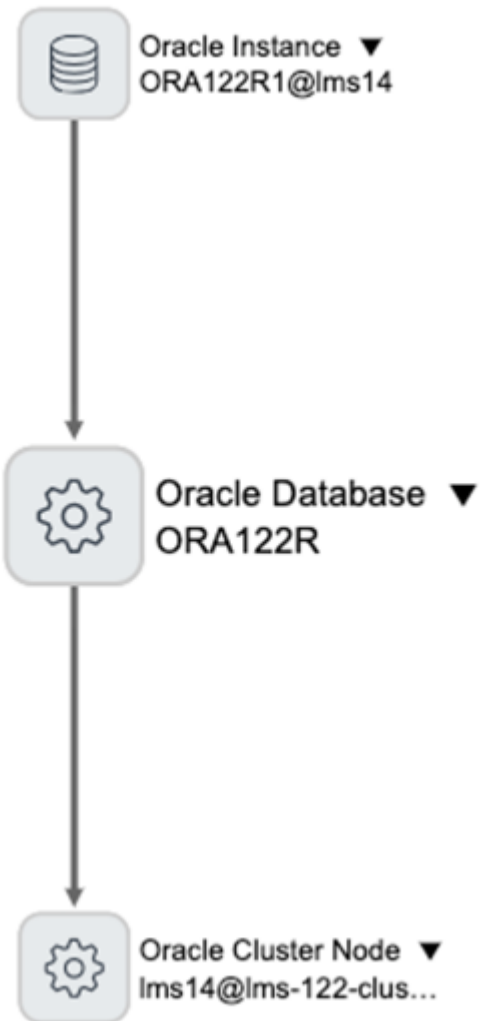
(Oracle-Cluster) cmdb_ci_oracle_cluster (Fortsetzung)

Feld	Beschreibung
cluster_status	Der aktive Status des Oracle-Datenbankclusters.
ip_address	Die IP-Adressen der am Cluster teilnehmenden Knoten.

Formular „Oracle-Cluster“



Oracle-Cluster-Ansichtszuordnung



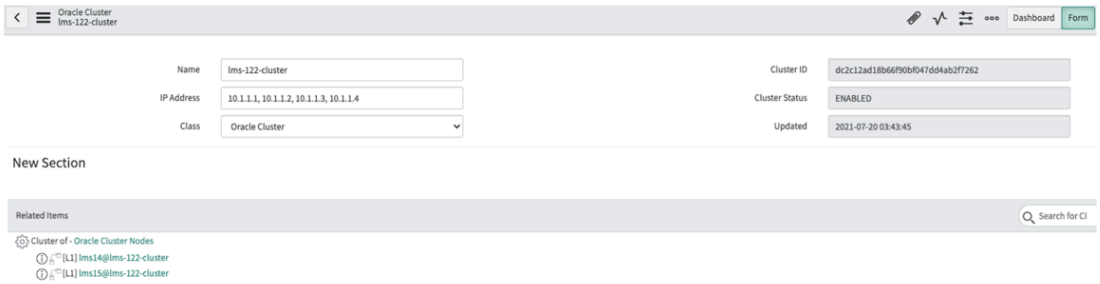
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Oracle-Clusterknoten) cmdb _ci_oracle_ cluster_node

Feld	Beschreibung
name	Der Hostname der Clusterknotenkombination HOSTNAME@CLUSTER_NAME.
ip_address	Die IP-Adresse des Clusterknotens, sofern durch DNS auflösbar.
Server	Der Hostname des Hosts, auf dem der Clusterknoten gehostet wird.
Cluster	Der Name des Clusters, dem der Clusterknoten zugewiesen ist.

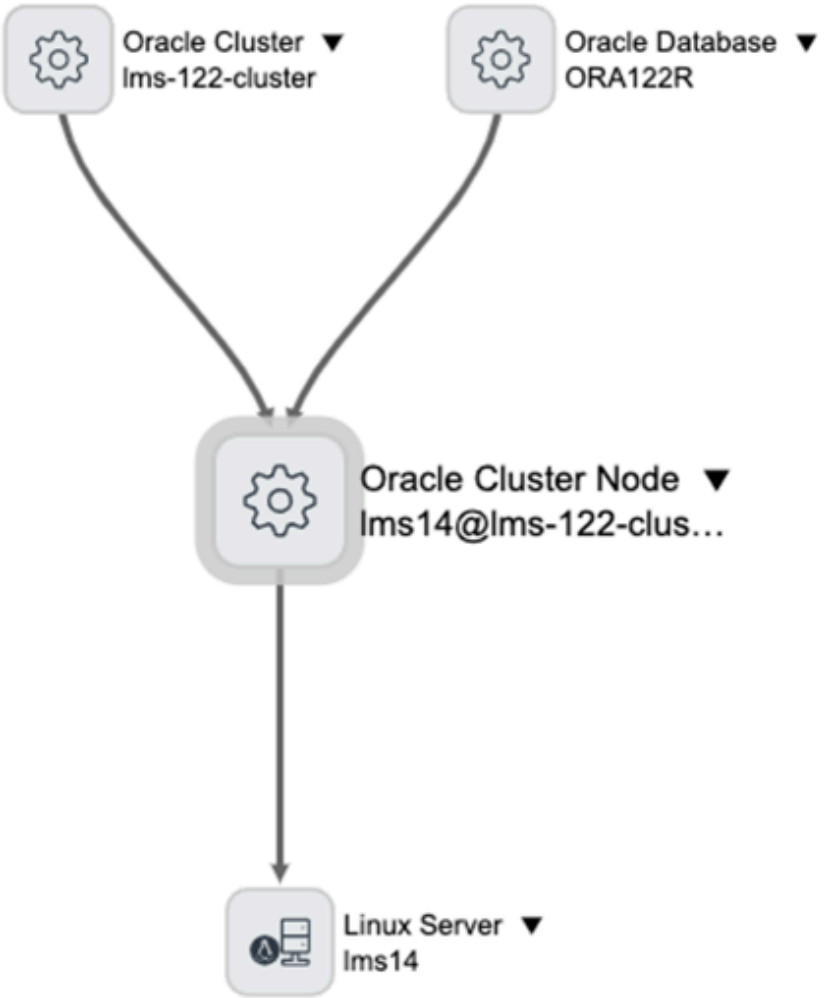
Formular „Oracle-Clusterknoten“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle-Clusterknoten-Ansichtszuordnung

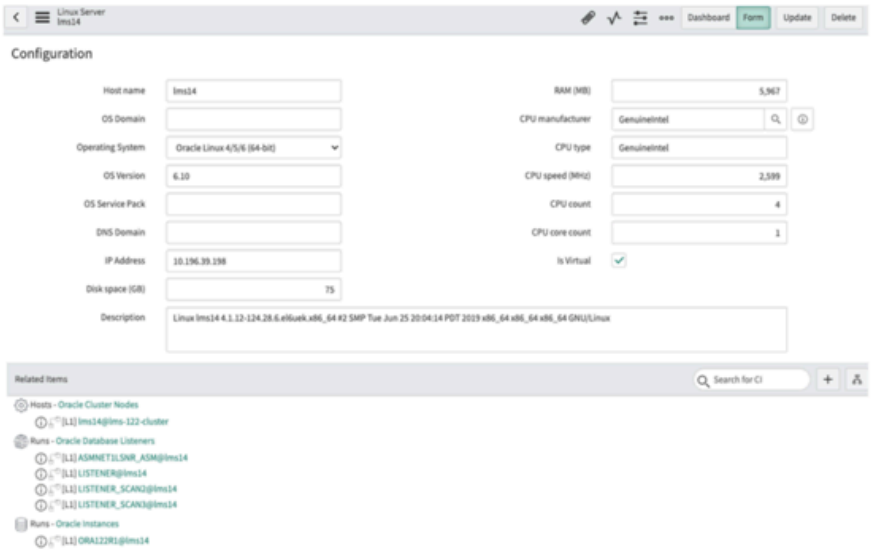


(Linux-Server) cmdb_ci_linux_server

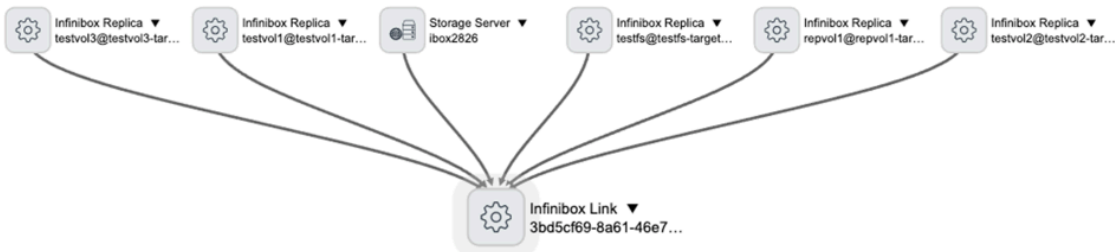
Feld	Beschreibung
name	Der Hostname des Linux-Servers, auf dem der Oracle Listener-Prozess gehostet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Linux-Server“



Linux-Server-Ansichtszuordnung



(AIX-Server) cmdb_ci_aix_server

Feld	Beschreibung
name	Der Hostname des AIX-Servers, auf dem der Oracle Listener-Prozess gehostet wird.

(HPUX Server) cmdb_ci_hpux_server

Feld	Beschreibung
name	Der Hostname des HPUX -Servers, der den Oracle Listener-Prozess hostet.

(Solaris-Server) cmdb_ci_solaris_server

Feld	Beschreibung
name	Der Hostname des Solaris-Servers, der den Oracle Listener-Prozesshostet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle DB-Service (cmdb_ci_db_ora_service)

Feld	Beschreibung
name	Der Name des Services
tcp_port	Der Port des Services.
listener_name	Der Name des Listeners, der den Service verwaltet.
version	Die Version des Service.

CI-Beziehungen

Vom Oracle Listener HD-Muster erstellte Beziehungen

CI	Beziehung	CI
cmdb_ci_oracle_cluster	„Cluster of :: Cluster“	cmdb_ci_oracle_cluster_node
cmdb_ci_oracle_cluster_node	„Hosted on :: Hosts“	cmdb_ci_linux_server
cmdb_ci_db_ora_instance	„Runs on :: Runs“	cmdb_ci_linux_server
cmdb_ci_db_ora_listener	„Depends on :: Used by“	cmdb_ci_db_ora_instance
cmdb_ci_db_ora_instance	Verwendet::Verwendet von	cmdb_ci_db_oracle_database
cmdb_ci_oracle_database	„Hosted on :: Hosts“	cmdb_ci_oracle_cluster_node
cmdb_ci_oracle_cluster_node	„Hosted on :: Hosts“	cmdb_ci_aix_server
cmdb_ci_db_ora_instance	„Runs on :: Runs“	cmdb_ci_aix_server
cmdb_ci_oracle_cluster_node	„Hosted on :: Hosts“	cmdb_ci_solaris_server
cmdb_ci_db_ora_instance	„Runs on :: Runs“	cmdb_ci_solaris_server
cmdb_ci_oracle_cluster_node	„Hosted on :: Hosts“	cmdb_ci_hpux_server
cmdb_ci_db_ora_instance	„Runs on :: Runs“	cmdb_ci_hpux_server
cmdb_ci_db_ora_service	Verwaltet von::Verwaltet	cmdb_ci_db_ora_listener
cmdb_ci_db_ora_instance	Verwendet::Verwendet von	cmdb_ci_db_ora_service

Erkennung von Oracle Solaris LDOM

Discovery verwendet das Muster für die LDOM-Infrastruktur (Solaris Logical Domain) und das Muster für die gemeinsam genutzte Solaris LDOM-Bibliothek, um alle LDOM-Daten zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery verwendet diese Muster zum Ausführen einer horizontalen Erkennung: Sie können die Muster auf der Now Platform mit Release Yokohama oder höher verwenden.

Das Muster für die Solaris LDOM-Infrastruktur wird bei der Solaris-Servererkennung automatisch ausgelöst. Das Muster überprüft, ob ein LDOM-Controller vorhanden ist, und stoppt die Ausführung, wenn kein Controller gefunden wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Muster für die gemeinsam genutzte Solaris LDOM-Bibliothek wird als Erweiterungsabschnitt zum Solaris-Servermuster ausgeführt. Das Muster ändert die Seriennummer (SN) auf LDOM-Computern, sodass sie mit der SN übereinstimmt, die vom Muster für die Solaris LDOM-Infrastruktur gefüllt wird. Weitere Informationen zum Solaris-Server finden Sie unter Solaris-Erkennung.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

LDOM-Befehle beim Ausführen des Musters für die Solaris LDOM-Infrastruktur

Stellen Sie sicher, dass die relevanten Benutzer berechtigt sind, die folgenden benötigten Befehle für das Muster für die Solaris LDOM-Infrastruktur auszuführen:

- *"sudo /usr/sbin/virtinfo -a"*
- *"sudo /usr/sbin/ldm -V"*
- *"hostname"*
- *"svcs ldmd"*
- *"sudo /usr/sbin/ldm list-rsrc-group -a"*
- *"sudo /usr/sbin/sneep -T | grep ChassisSerialNumber 2> /dev/null"*
- *"/usr/sbin/prtdiag -v | awk '/Chassis Serial/{getline; getline; print}'"*
- *"sudo /usr/sbin/ldm list"*

Hinweis: Einige dieser Befehle werden mit Bedingungen verwendet und nicht bei jeder Erkennung ausgeführt. Beispielsweise können Sie die SN für Server in der Regel mit dem Befehl *sneep* abrufen. Dieser ist jedoch auf Solaris-Servern standardmäßig nicht verfügbar, daher wird *prtdiag* als alternative Methode zum Abrufen der SN verwendet.

Wichtige LDOM-Befehle beim Ausführen des Musters für die gemeinsam genutzte Solaris LDOM-Bibliothek

Stellen Sie sicher, dass die relevanten Benutzer berechtigt sind, die folgenden benötigten Befehle für das Muster für die gemeinsam genutzte Solaris LDOM-Bibliothek auszuführen:

- *"sudo /usr/sbin/virtinfo -a"*
- *"sudo /usr/sbin/sneep -T | grep ChassisSerialNumber 2> /dev/null"*
- *"hostname"*

Stellen Sie sicher, dass die relevanten Benutzer über die Berechtigungen zum Ausführen des LDOM-Befehls *virtinfo* verfügen. Dieser Befehl stellt sicher, dass die richtige LDOM-Rolle eingerichtet werden kann.

Stellen Sie sicher, dass die relevanten Benutzer über die Berechtigungen zum Ausführen des LDOM-Befehls *"sudo /usr/sbin/ldm list"* verfügen, um Gast-VMs auf dem LDOM-Controller aufzulisten. Dies ist erforderlich, um Beziehungen zwischen dem LDOM-Controller und den LDOM-Gast-VMs festzulegen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einer der Seriennummernbefehle *sneep* oder *prtdiag* muss eine korrekte Antwort zurückgeben, um die SN korrekt festzulegen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Die von beiden Mustern erkannten Daten umfassen die folgenden Tabellen und Felder.

Tabelle und Feld	Beschreibung
Solaris-Server [cmdb_ci_solaris_server]	
ldom_version	Auf dem LDOM-Controller installierte LDOM-Version
ldom_role	LDOM-Rolle; „Controller“ oder „Gast“
ldom_state	Status der LDOM-Implementierung auf dem LDOM-Controller
serial_number	Seriennummer des Computers
virtual	Gibt an, ob für den LDOM-Controller ein virtueller Computer (für Gast-VMs) verwendet wird oder nicht
ram	Auf dem LDOM-Controller verfügbarer Arbeitsspeicher
cpu_core_count	Anzahl der CPU-Kerne auf dem LDOM-Controller

CI-Beziehungen

CI	Beziehung	CI
LDOM-Controller	Gehostet auf::Hostet	LDOM-Gast-VM

Palo Alto Networks-Firewall-Erkennung

Die Anwendung ServiceNow Discovery verwendet das Muster Next-Generation Palo Alto Firewall, um die Firewalls Palo Alto Networks von zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Das Erkennungsmuster verwendet eine Reihe von SNMP-Aufrufen, um die Palo Alto Networks-Firewalls zu finden. Discovery verwendet das Muster zum Ausführen der horizontalen Erkennung.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

- Stellen Sie sicher, dass Ihr Netzwerkfirewallgerät über SNMP-Zugriff verfügt.
- Konfigurieren Sie die SNMP-Anmeldeinformationen in der ServiceNow-Instanz. Weitere Informationen finden Sie unter SNMP-Anmeldeinformationen .
- Fügen Sie der ServiceNow-Instanz den OID-Datensatz des SNMP-Systems für das Palo Alto Networks-Gerät hinzu. Aktualisieren Sie Folgendes:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Klassifizierung: Palo-Alto-Firewall
- Klasse: Palo-Alto-Firewall-Gerät

- Stellen Sie das Muster wie folgt bereit:
  1. Laden Sie Firewall-Erweiterungsklassen aus ServiceNow Storeherunter, und installieren Sie sie. Die App fügt die neuen CMDB-Klassen hinzu, die für die Erkennung der Netzwerkfirewall erforderlich sind.
  2. Laden Sie das Erkennungsmuster aus dem ServiceNow Store herunter, und installieren Sie es.
  3. Synchronisieren Sie das Muster mit dem entsprechenden MID-Server.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das Palo Alto Firewall-Muster der nächsten Generation ausgeführt wird.

Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Palo Alto-Geräts.
Seriennummer [serial_number]	Seriennummer des Palo Alto-Geräts.
Vollständig qualifizierter Domänenname [fqdn]	Vollständig qualifizierter Domänenname (FQDN) des Palo Alto-Geräts.
Hersteller [manufacturer]	Palo Alto-Gerätehersteller.
Modell-ID [model_id]	Modell-ID des Palo Alto-Geräts.
Betriebsstatus [operational_status]	Gibt an, ob sich das Palo Alto-Gerät im Status „Aktiv“ befindet.
Hardware-Betriebssystem [hardware_os]	Auf der Hardware ausgeführtes Betriebssystem
Hardware-Betriebssystem-Version [hardware_os_version]	Version des auf der Hardware ausgeführten Betriebssystems
Beschreibung [short_description]	Kurzbeschreibung des Palo Alto-Geräts.
Firmware-Version [Firmware-Version]	Firmware-Version des Palo Alto-Geräts.

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
Alias [alias]	Der vom Anwender zugewiesene Name für den Netzwerkadapter.
Netzmaske [netmask]	Netzmaske des Netzwerkadapters
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters
Name [name]	Name des Netzwerkadapters

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkadapter [cmdb_ci_network_adapter] (Fortsetzung)

Feld	Beschreibung
Konfigurationselement [cmdb_ci]	Referenziert die Palo Alto-Firewall-Gerätetabelle [cmdb_ci_firewall_device_palo_alto].

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
IP-Adresse [ip_address]	IP-Adresse der Palo Alto-Firewall.
Netzmaske [netmask]	Netzmaske der Palo Alto-Firewall.
NIC [nic]	Referenziert die Netzwerkadaptertabelle [cmdb_ci_network_adapter].

Seriennummer [cmdb_serial_number]

Feld	Beschreibung
Konfigurationselement [configuration_item]	Referenziert die Palo Alto-Firewall-Gerätetabelle [cmdb_ci_firewall_device_palo_alto].

DNS-Name [cmdb_ci_dns_name]

Feld	Beschreibung
Name [name]	DNS-Name (Domain Name System) des Palo Alto-Firewall-Geräts.
IP-Adresse [ip_address]	Host-IP-Adresse.

CI-Beziehungen

Diese Beziehungen sollen die Palo Alto Networks-Firewall-Erkennung unterstützen:

CI	Beziehung	CI
IP-Adresse [cmdb_ci_ip_address]	Referenzen	Netzwerkadapter [cmdb_ci_network_adapter]
Netzwerkadapter [cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Netzwerkadapter [cmdb_ci_network_adapter]	Referenzen	Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]
Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]	Erweitert::Erweitert um	Firewall-Gerät [cmdb_ci_firewall_device]
Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]	Eigentümer von::Eigentum von	Netzwerkadapter [cmdb_ci_network_adapter]
Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]	Verwendet::Verwendet von	Routerschnittstelle [dscy_router_interface]
Routerschnittstelle [dscy_router_interface]	Referenzen	Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]
Seriennummer [cmdb_serial_number]	Referenzen	Palo-Alto-Firewall-Gerät [cmdb_ci_firewall_device_palo_alto]

Erkennung von Pivotal Cloud Foundry

Die Anwendung ServiceNow Discovery sucht Komponenten Pivotal Cloud Foundry von (PCF) Version 3 mithilfe des Musters Pivotal Cloud Foundry. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Sie können dieses Muster in der Now Platform -Startversion von Kingstonverwenden.

Die Discovery von PCF V3-Komponenten wird unterstützt, wenn das Plugin Muster für Discovery und Service-Mapping, Version 1.0.99, März 2023, installiert ist. Das Muster unterstützt weiterhin die Discovery von PCF V2-Komponenten.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Pivotal Cloud Foundry-Anmeldeinformationen

Erstellen Sie die Anmeldeinformationen Pivotal Cloud Foundry.

1. Navigieren zu **Discovery** > **Anmeldeinformationen**.
2. Wählen Sie **Neu**.
3. Wählen Sie **CloudFoundry-Anmeldeinformationen**aus.
4. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Name der Anmeldeinformationen Beispiel: `pcf_user-Anmeldeinformationen`
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Betrifft	Anmeldeinformationen, die Sie auf **Alle MID Server** in Ihrem Netzwerk oder auf einen oder mehrere **Spezielle MID Server** anwenden oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	nicht anwenden möchten. Wählen Sie **Spezielle MID Server** aus.
Auftrag	Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten verwendet. Eine niedrigere Zahl zeigt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Legen Sie die Reihenfolge der Anmeldeinformationen fest, wenn eine große Anzahl von Anmeldeinformationen verwendet wird oder wenn Anwender nach drei fehlgeschlagenen Anmeldeversuchen durch die Sicherheitseinstellungen gesperrt werden. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist 100.
Benutzername	Name des Benutzers dieser Anmeldeinformationen. Vermeiden Sie führende oder nachgestellte Leerzeichen in Benutzernamen. Eine Warnung wird angezeigt, wenn die Plattform führende oder nachfolgende Leerzeichen im Anwendernamen erkennt. Ein Beispiel ist `pcf_user`. Verwenden Sie die `client_id`, die zum Generieren des JWT-Tokens verwendet wird.
Passwort	Passwort des Benutzers dieser Anmeldeinformationen. Verwenden Sie das `client_secret`, das zum Generieren des JWT-Tokens verwendet wird.
Anmeldeinformationsalias	Alternativer Name für diese Anmeldeinformationen. Ein Beispiel ist `cf` Wenn dieses Feld geschlossen ist, wählen Sie das Entsperren-Symbol, um das Feld zu entsperren.

5. Wählen Sie **Aktualisieren**.

JSON-Web-Token-Anmeldeinformationen

Führen Sie die folgenden Schritte zur Tokenvalidierung aus, um das JSON-Web-Token (JWT) zu überprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Format des JWT-Tokens ist: https://docs.cloudfoundry.org/api/uaa/version/4.27.0/index.html#jwt-bearer-token-grant .

1. Führen Sie das folgende cURL-Skript für die Server-API des Benutzerkontos und der Authentifizierung (UAA) aus, und überprüfen Sie die Ergebnisse:

```
curl -s -k https://ip_address:port/oauth/token
-X; POST -H "Content-Type: application/x-www-
form-urlencoded" -H "Accept: application/json" -d
"client_id=<INSERT_USER_HERE>&client_secret=<INSERT_PASS_HERE>&grant_type=client_
```

   Wenn dieser Befehl kein Token generiert, vergewissern Sie sich, dass die Anmeldeinformationen im Repository ServiceNow korrekt sind, andernfalls fahren Sie mit Schritt 2 fort.

2. Führen Sie das folgende cURL-Skript für die Pivotal Cloud Foundry-API aus:

```
Rollen: https://ip_address:port/v3/spaces -k -v -H
„Akzeptieren: application/json" -H „Autorisierung:
Bearer<INSERT TOKEN HERE> "
```

   Wenn dieser Befehl die PCF-Bereichsinformationen nicht abruft, überprüfen Sie die Anmeldeinformationen im Anmeldeinformations-Repository ServiceNow.

Anmeldeinformationen für V3-API-Elemente

Gewähren Sie einem leseberechtigten Benutzer die Berechtigung zur Verwendung der folgenden API-Elemente.

- –/v3/organizations
- –/v3/spaces
- –/v3/Domänen
- –/v3/routes
- –/v3/organization_quotas
- –/v3/space_quotas
- –/v3/apps
- -/v3/service_offerings
- -/v3/service_plans
- -/v3/service_instances
- -/v3/droplets

Hinweis: Das Pivotal Cloud Foundry -Muster unterstützt auch die PCF V2 APIs.

Discovery-Zeitplan ohne Server erstellen

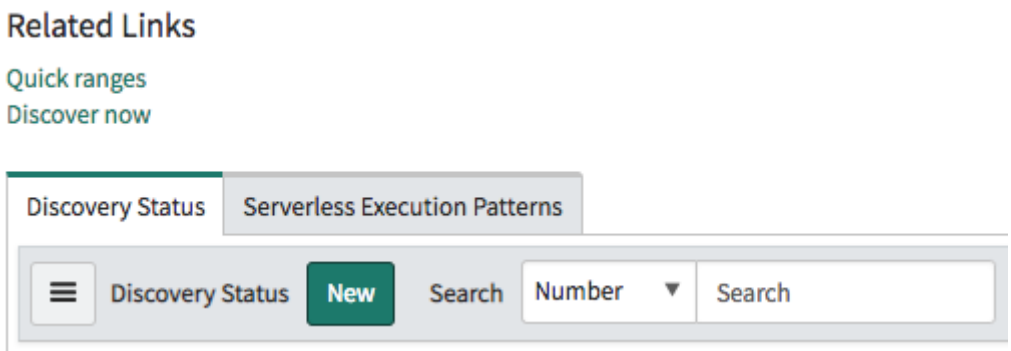
1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Discovery-Zeitplan“

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diesen Discovery-Zeitplan ein, z. B. `pcf`.
Erkennen	Wählen Sie als Erkennungstyp **ohne Server** aus.
MID-Server	MID Servers, für die die Anmeldeinformationen gelten. Geben Sie den erforderlichen MID-Server an, z. B. `Discovery_Server`.
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Anmeldeinformationsalias	Alternativer Name für diese Anmeldeinformationen. Verwenden Sie den Alias für die Pivotal Cloud Foundry -Anmeldeinformationen, die Sie zuvor erstellt haben.

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.



5. Wählen Sie die Registerkarte Ausführungsmuster ohne Server.
6. Wählen Sie **Neu**.
7. Füllen Sie die Felder im Formular aus.

Formular „Ausführungsmuster ohne Server“

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für dieses Ausführungsmuster ohne Server ein, z. B. `PCF1`
Muster	Wählen Sie **CloudFoundry** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Proxyhost	Vollqualifizierter Domänenname des Computers, auf dem Sie den Proxy-Server installieren. Geben Sie **Global** an.
Aktiv	Kontrollkästchen, um diesen Zeitplan für die Erkennung zu aktivieren. Aktivieren Sie das Kontrollkästchen.

8. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Serverlose Ausführungsmuster“, und wählen Sie **Speichern**aus.
9. Wählen Sie die Registerkarte Ausführungsmuster ohne Server
10. Erstellen und definieren Sie das Ausführungsmuster ohne Server wie in der Produktdokumentation beschrieben.

    Konfigurieren Sie die für das Muster Pivotal Cloud Foundry erforderlichen Parameter wie folgt:

Startprogrammparameter für Discovery-Muster

Parameter	Beschreibung
Organisation	Name der Organisation, die erkannt werden muss, oder aller Organisationen, bei denen die Eingabe „*“ ist.
CredentialAlias	Alternativer Name für diese Anmeldeinformationen. Verwenden Sie den Alias für die Pivotal Cloud Foundry -Anmeldeinformationen, die Sie zuvor erstellt haben.
URL_CF	API-URL des Cloud-Controllers, der zum Abrufen der Informationen von Pivotal Cloud Foundryverwendet wird.
URL_CF_AUTH	UAA-Server-API, die zum Generieren des Tokens verwendet wird. Geben Sie den Wert im folgenden Format ein: https://uaa.sys.dev.phx.pcf.example.com/oauth/token.

11. **Führen Sie eine Aktualisierung durch**.
12. Um eine Discovery zu starten, navigieren Sie zur Definition „Serverlos Discovery “ , und wählen Sie **Jetzt erkennen aus**.

EVAL-Abschlussfunktionen

Verwenden Sie die folgenden EVAL-Abschlussfunktionen, um alle Organisationen mit „,“ als Trennzeichen zu verketten.

```
var rtrn = '';
var organizations = ${organizations[*].name};
var beforeReturn = '';
var separator = '';
for (var i = 0; i < organizations.size(); i++)
 {
 beforeReturn += separator + organizations.get(i);
 separator = ',';
 }
rtrn = beforeReturn;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden Sie die folgenden EVAL Abschlussfunktionen, um 1 zurückzugeben, wenn der Betriebsstatus aktiv ist, und 2, wenn er nicht aktiv ist.

```
var rtrn = '';
var currentOrgStatus = ${organizations[].operational_status};
var status = currentOrgStatus.toLowerCase();
if(status == "active"){
   rtrn = "1";
}
else {
   rtrn = "2";
}
```

Verwenden Sie die folgende Abschlussfunktion EVAL, um 1 zurückzugeben, wenn der Betriebsstatus gestartet wird, und 2, wenn er nicht gestartet wird.

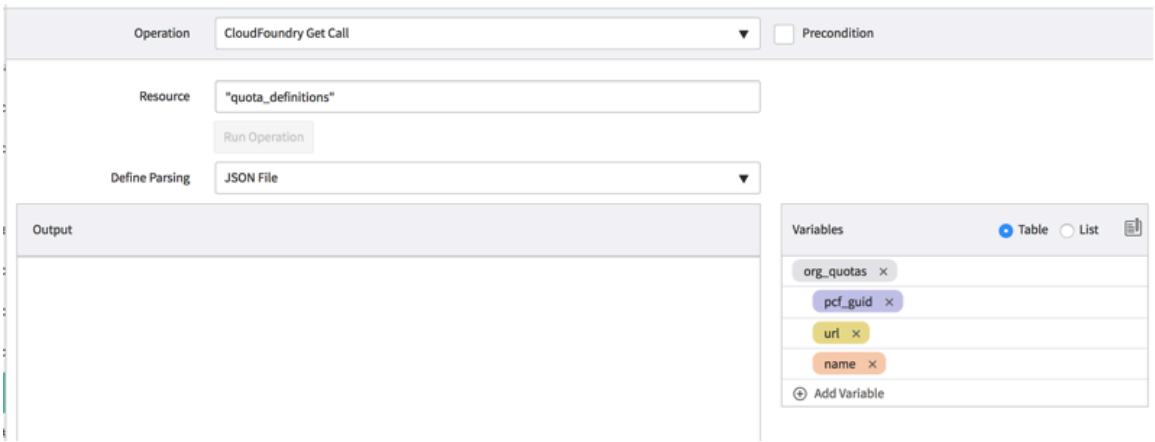
```
var rtrn = '';
var currentAppStatus = ${apps[].state};
var status = currentAppStatus.toLowerCase();
if(status == "started"){
   rtrn = "1";
}
else {
   rtrn = "2";
}
```

CloudFoundry Get Call

Der benutzerdefinierte Vorgang „CloudFoundry Get Call“ behandelt die Generierung von Token. Er verwendet die Anmeldeinformationen und die Kontextvariable URL_CF_AUTH, um ein Token zu generieren, das zum Erstellen von API-Aufrufen verwendet wird.

Wenn ein Token generiert wird, wird URL_CF verwendet, um die im Feld **Ressource** definierten API-Aufrufe zu erstellen. Der benutzerdefinierte Vorgang behandelt auch die Paginierung, wenn die Antwort mehr als eine Seite umfasst.

CloudFoundry Get Call analysiert die Eingabe JSON, um die Tabellen und Variablen auszufüllen.



Pivotal Cloud Foundry BOSH Erweiterungsabschnitt

Pivotal Cloud Foundry BOSH ist ein Erweiterungsabschnitt des Pivotal Cloud Foundry -Musters.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Erweiterung ist unter ServiceNow® Store für das Release von Muster für Discovery und Service-Mapping 1.6.0 vom Juni 2023 verfügbar.

Anforderungen für Pivotal Cloud Foundry BOSH

Hinweis: Die folgenden Anforderungen gelten nur für den BOSH-Erweiterungsabschnitt.

Die Opsman-Authentifizierungs-URL muss als Musterparameter mit dem Namen *URL_OPSMAN_AUTH*angegeben werden. Beispiel: `https://`<opsman entry point> /uaa/oauth/token

Die hinzugefügten Anmeldeinformationen müssen berechtigt sein, die folgenden APIs auszuführen:

- */uaa/oauth/token*
- */api/v0/deployed/products*

Hinweis: Anwenderdefinierte APIs werden als Schritt *„Tanzu Opsman-API abrufen"* zum Muster hinzugefügt.

Von Discovery während der horizontalen Erkennung erfasste Daten

Erfasste Informationen

Feld	Beschreibung
Haupt-CI: PCF Foundation [cmdb_ci_pcf_foundation]	
Name	Pivotal Cloud Foundry Name des Clustereintrags <name>-<hostCf:<portCf>
ip_address	Pivotal Cloud Foundry Host-IP.
port	Pivotal Cloud Foundry Serviceport
short_description	Pivotal Cloud Foundry Service-Build-Nummer
Organisation	Organisationsliste, verwaltet vom PCF-Cluster. Die Einträge werden durch Kommata „,“ getrennt.
PCF-Organisation [cmdb_ci_pcf_organization]	
Name	Organisationsname
URL	Eindeutige Organisations-URL
pcf_guid	Organisations-UID in CF
operational_status	Organisationsstatus
PCF-Bereich [cmdb_ci_pcf_space]	
Name	Platzname
URL	Eindeutige Speicherplatz-URL
pcf_guid	Platz-UID in CF
PCF-Anwendung [cmdb_ci_pcf_appl]	
Name	Anwendungsname

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfasste Informationen (Fortsetzung)

Feld	Beschreibung
URL	Eindeutige Anwendungs-URL
pcf_guid	Eindeutige Anwendungs-UID in CF
PCF-Route [cmdb_ci_pcf_route]	
Name	Routenname
URL	Eindeutige Routen-URL
pcf_guid	Routen-UID in CF
port	Routenport
Typ	Routentyp
PCF-Kontingent [cmdb_ci_pcf_quota]	
Name	Kontingentname
URL	Eindeutige Kontingent-URL
pcf_guid	Kontingent-UID in CF
PCF-Domäne [cmdb_ci_pcf_domain]	
name	Domänenname
URL	Eindeutige Domänen-URL
pcf_guid	Domänen-UID in CF
PCF-Bereichsinstanz [cmdb_ci_pcf_space_instance]	
name	Name der Platzserviceinstanz
URL	Eindeutige Platzserviceinstanz-URL
pcf_guid	UID-Platzserviceinstanz in CF
PCF-Serviceplan [cmdb_ci_pcf_service_plan]	
name	Name der Serviceplaninstanz
URL	Eindeutige Serviceplan-URL
pcf_guid	UID-Platzserviceinstanz in CF
PCF-Service [cmdb_ci_pcf_service]	
name	Servicename
URL	Eindeutige Service-URL
pcf_guid	Service-UID in CF
PCF-Droplet [cmdb_ci_pcf_droplet]	
name	Ressourcen-URL
pcf_guid	Droplet-ID
URL	Droplet-URL
install_status	Installationsstatus: 1, „installiert“
operational_status	Betriebsstatus: 1, „funktional“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfasste Informationen (Fortsetzung)

Feld	Beschreibung
Schlüsselwert [cmdb_key_value]	
Schlüssel	Tag-Schlüssel der Ressource **Hinweis:** Diese Daten werden nur für V3-API-Aufrufe gesammelt.
Wert	Ressourcen-Tag-Wert **Hinweis:** Diese Daten werden nur für V3-API-Aufrufe gesammelt.

Daten, die vom BOSH-Erweiterungsabschnitt Pivotal Cloud Foundry erkannt wurden

Feld	Beschreibung
BOSH-Bereitstellung (cmdb_ci_bosh_deployment)	
Name	Der Installationsname der Ressource.
object_id	Die ID des bereitgestellten Produkts.
install_status	Hartcodiert auf den Wert: *1= Installiert*.
operational_status	Hartcodiert auf den Wert: *1=funktionsfähig*.
deployment_version	Die Version des bereitgestellten Produkts.
deployment_type	Der Typ des bereitgestellten Produkts.

CI-Beziehungen

Diese Beziehungen sollen die Pivotal Cloud Foundry-Erkennung unterstützen.

CI	Beziehung	CI
PCF-Bereich [cmdb_ci_pcf_space]		
cmdb_ci_pcf_space	Enthält::Enthalten in	cmdb_ci_pcf_organization
PCF-Anwendung [cmdb_ci_pcf_appl]		
cmdb_ci_pcf_appl	Enthält::Enthalten in	cmdb_ci_pcf_space
PCF-Route [cmdb_ci_pcf_route]		
cmdb_ci_pcf_route	Enthält::Enthalten in	cmdb_ci_pcf_foundation
PCF-Kontingent [cmdb_ci_pcf_quota]		
cmdb_ci_pcf_quota	Verwendet::Verwendet von	cmdb_ci_pcf_space cmdb_ci_pcf_organization
PCF-Domäne [cmdb_ci_pcf_domain]		
cmdb_ci_pcf_domain	Verwendet::Verwendet von	cmdb_ci_pcf_route

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
	Eigentümer von::Eigentum von	cmdb_ci_pcf_organization
	Enthält::Enthalten in	cmdb_ci_pcf_foundation
PCF-Bereichsinstanz [cmdb_ci_pcf_space_instance]		
cmdb_ci_pcf_space_instance	Enthält::Enthalten in	cmdb_ci_pcf_space
PCF-Serviceplan [cmdb_ci_pcf_service_plan]		
cmdb_ci_pcf_service_plan	Verwendet::Verwendet von	cmdb_ci_pcf_space_instance
PCF-Service [cmdb_ci_pcf_service]		
cmdb_ci_pcf_service	Verwendet::Verwendet von	cmdb_ci_pcf_service_plan
PCF-Droplet [cmdb_ci_pcf_droplet]		
cmdb_ci_pcf_appl	Enthält::Enthalten in	cmdb_ci_pcf_droplet
Schlüsselwert [cmdb_key_value]		
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_droplet
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_organization
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_space
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_domain
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_route
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_appl
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_service
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_service_plan
cmdb_key_value	Nur Referenz. Beispiel: Configuration_item	cmdb_ci_pcf_space_instance

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Pivotal Cloud Foundry BOSH-Beziehungen

Diese Beziehungen werden erstellt, um die Discovery von BOSH-Erweiterungsabschnitten Pivotal Cloud Foundry zu unterstützen.

CI	Beziehung	CI
Cloud-Foundry-Cluster [cmdb_ci_pcf_foundation]	Enthält::Enthalten in	BOSH-Bereitstellung [cmdb_ci_bosh_deployment]

Discovery für reinen Speicher FlashArray .

Die Anwendung Muster für Discovery und Service-Mapping verwendet das Muster „Pure Storage Flash Array“, um den Speicherort „Pure Storage FlashArray “ in Ihrer Infrastruktur zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Hinweis: Ab März 2024 ist die Musterausführung standardmäßig deaktiviert. Um ein CI für den reinen Speicher FlashArrayzu erstellen, synchronisieren Sie das Muster mit MID-Server.

Im ServiceNow® Store neue oder erweiterte Muster anfordern

Besuchen Sie die ServiceNow Store um alle verfügbaren Updates anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie unter ServiceNow Store Versionshinweise zum Versionsverlauf .

Voraussetzungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- Visibility Content

Überprüfen Sie die Konfiguration der Anmeldeinformationen

Konfigurieren Sie die Anmeldeinformationen für die Standardauthentifizierung, um FlashArrayzu klassifizieren. Weitere Informationen finden Sie unter Standardauthentifizierung .

Überprüfen Sie die Berechtigungen zum Ausführen von REST-API-Aufrufen

Das Muster „Pure Storage Flash Array“ unterstützt die API 2.17-Version.

- `/api/1.17/auth/apitoken`
- `/api/2.17/auth/session`
- `/api/2.17/arrays`
- `/api/2.17/volumes`
- `/api/2.17/volume-groups`
- `/api/2.17/host-groups`
- `/api/2.17/hardware`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- */api/2.17/dns*
- */api/2.17/ports*

Hinweis: Die Musterversion „Pure Storage“ vom Februar 2024 unterstützt nur die iSCSI-Protokoll-Discovery.

Wird ausgeführt Discovery

Um eine Discovery mit Mustern auszuführen, erstellen Sie einen Discovery-Zeitplan, der auf die Verwaltungs-IP-Adresse des Speichers FlashArray abzielt. Weitere Informationen finden Sie unter Erkennungen im Netzwerk ausführen.

Von Discovery während der horizontalen Erkennung erfasste Daten

Discovery füllt die Daten in CMDB aus, wenn das Pattern „Pure Storage Flash Array“ ausgeführt wird.

Speicherserver [cmdb_ci_storage_server]

Feld	Beschreibung
Name [name]	Der vom Anwender zugewiesene Bezeichner oder die Bezeichnung für den FlashArray -Speicher.
Seriennummer [serial_number]	Seriennummer, die jeden einzelnen FlashArray -Speicher eindeutig identifiziert.
Betriebssystem [os]	Betriebssystem, das auf dem Speicher FlashArray ausgeführt wird.
BS-Version [os_version]	Softwareversion, die im Speicher FlashArray installiert ist.
Physische Kapazität (GB) [physical_capacity]	Gesamtmenge des im System FlashArray verfügbaren Speicherplatzes, gemessen in Gigabyte (GB). Diese Kapazität umfasst sowohl zugeteilte als auch nicht zugeteilte Speicherressourcen.
Freie Kapazität (GB) [total_free_capacity]	Gesamtmenge an Speicherplatz, der derzeit auf dem Speichersystem FlashArray verfügbar ist, gemessen in GB.
IP-Adresse [ip_address]	IP-Adresse des Speichers FlashArray.
Hersteller [manufacturer]	Herstellername: True Storage.
Objekt-ID [object_id]	Anmeldeinformationsaffinität, die während der Discovery dem Speicher FlashArray zugewiesen wurde. Weitere Informationen zur Anmeldeinformationsaffinität finden Sie unter Anmeldeinformationsaffinität für Discovery und Orchestration .
Modell-ID [model_id]	Modell-ID des Speichers FlashArray.
Verschlüsselung im Ruhezustand [encryption_at_rest]	Verschlüsselte Daten, die auf einem physischen Gerät oder in einer Datenbank gespeichert sind. Mögliche Werte: • aktiv • Deaktivieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speicherserver [cmdb_ci_storage_server] (Fortsetzung)

Feld	Beschreibung
Verschlüsselungsalgorithmus [encryption_algorithm]	Typ des Algorithmus, den der Speicherserver verwendet. Mögliche Werte: • AES-256: Advanced Encryption Standard (AES) 256-Verschlüsselung • mehrere Methoden: Cloud Storage unterstützt derzeit nicht mehrere Methoden • Unbekannt: Wenn während einer vorherigen Discovery ein Algorithmustyp erkannt wurde, bei der nächsten Erkennung jedoch nicht erkannt wird, ist der Wert unbekannt

Speicherclusterknoten [cmdb_ci_storage_cluster_node]

Feld	Beschreibung
Name [name]	Name des Clusterknotens.
Cluster [cluster]	Hostgruppe, die diesem Clusterknoten in der Umgebung FlashArray zugeordnet ist.
Gruppe ändern [assignment_group]	iSCSI- oder Fibre Channel-Initiator-Verbindungen zwischen Speicher und Host.
Hersteller [manufacturer]	Herstellername: True Storage.
Kommentare [comments]	Alle mit dem Clusterknoten verbundenen logischen Einheitsnummern (Logical Unit Numbers, LUN).

Speichercluster [cmdb_ci_storage_cluster]

Feld	Beschreibung
Name [name]	Name des Speicher-Clusters.
Korrelations-ID [correlation_id]	Kombiniert den Clusternamen und die Seriennummer des Speichers, um einen eindeutigen Bezeichner (UID) zu erstellen.
Hersteller [manufacturer]	Herstellername: True Storage.

Speichervolume [cmdb_ci_storage_volume]

Feld	Beschreibung
Name [name]	Volumename
Seriennummer [serial_number]	Seriennummer des Volumes.
Volume-ID [volume_id]	Volume-ID.
Installiert [install_date]	Datum, an dem das Volume installiert wurde.
Größe in Byte [size_bytes]	Datenträgergröße in Byte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichervolume [cmdb_ci_storage_volume] (Fortsetzung)

Feld	Beschreibung
Pool-ID [pool_id]	ID des Pools, der die Volumes enthält.
Attribute [attributes]	Namen der mit den Volumes verbundenen Hosts.
Hersteller [manufacturer]	Herstellername: True Storage.

Speicherpool [cmdb_ci_storage_pool]

Feld	Beschreibung
Name [name]	Name des Speicher-Pools.
Objekt-ID [object_id]	ID des Speicher-Pools.
Hersteller [manufacturer]	Herstellername: True Storage.

Speichercontroller [cmdb_ci_storage_controller]

Feld	Beschreibung
Name [name]	Kombination aus Asset und Asset-Tag.
Modell-ID [model_id]	Modell-ID des Controllers.
Zugewiesen [assigned]	Verfügbarkeitsstatus.
Geräte-ID [device_id]	Eine eindeutige Bezeichnung für den Controller.
Hersteller [manufacturer]	Herstellername: True Storage.

Datenträger [cmdb_ci_disk]

Feld	Beschreibung
Name [name]	Achsen-ID
Größe in Byte [size_bytes]	Datenträgergröße in Byte.
Laufwerkstyp [drive_type]	Typ des auf dem Datenträger installierten Laufwerks.
Geräte-ID [device_id]	Kombination der Seriennummer des Speichersystems mit dem Datenträgernamen, die jeden Datenträger in der Umgebung FlashArray eindeutig identifiziert.
Hersteller [manufacturer]	Datenträgerhersteller.

Netzwerkadapter [cmdb_ci_network_adapter]

Feld	Beschreibung
Name [name]	Name des Netzwerkadapters
IP-Adresse [ip_address]	IP-Adresse des Netzwerkadapters
MAC-Adresse [mac_address]	MAC-Adresse des Netzwerkadapters

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkadapter [cmdb_ci_network_adapter] (Fortsetzung)

Feld	Beschreibung
IP-Standard-Gateway [ip_default_gateway]	IP-Adresse des Standard-Gateways.
Alias [alias]	Der vom Anwender zugewiesene Name für den Netzwerkadapter.
Netzmaske [netmask]	Netzmaske des Netzwerkadapters

Fibre Channel-Export [cmdb_ci_fc_export]

Feld	Beschreibung
Initiator-WWPN [initiator_wwpn]	UID, die die Direktor-ID, die Portnummer und die Initiator-ID kombiniert.

iSCSI-Export [cmdb_ci_iscsi_export]

Feld	Beschreibung
Name [name]	Initiator-ID in FlashArray -Systemen, die als UID für den Initiator im Kontext von iSCSI-Exporten dient.
Export-ID [export_id]	UID für einen iSCSI-Export in FlashArray -Systemen, erleichtert die Verwaltung und Nachverfolgung von iSCSI-Verbindungen.
Initiator-IQN [initiator_Iqn]	Qualifizierter iSCSI-Name (IQN), der einem Initiator im iSCSI-Netzwerk zugewiesen ist.

CI-Beziehungen

CI	Beziehungstyp	CI
[cmdb_ci_disk]	Enthält::Enthalten in	[cmdb_ci_storage_server]
[cmdb_ci_iscsi_export]	Gehostet auf::Hostet	[cmdb_ci_storage_server]
[cmdb_ci_iscsi_export]	Referenz	[cmdb_ci_storage_cluster_node]
[cmdb_ci_network_adapter]	Eigentümer von::Eigentum von	[cmdb_ci_storage_server]
[cmdb_ci_storage_cluster_node]	Cluster von::Cluster	[cmdb_ci_storage_cluster]
[cmdb_ci_storage_controller]	Controller für::Gesteuert von	[cmdb_ci_storage_server]
[cmdb_ci_storage_server]	Zugeordnet zu::Zugeordnet von	[cmdb_ci_storage_cluster_node]
[cmdb_ci_storage_server]	Enthält::Enthalten in	[cmdb_ci_storage_pool]
[cmdb_ci_storage_server]	Wird ausgeführt auf::Wird ausgeführt	[cmdb_ci_storage_cluster]
[cmdb_ci_storage_volume]	Enthält::Enthalten in	[cmdb_ci_cluster_node]
[cmdb_ci_storage_volume]	Enthält::Enthalten in	[cmdb_ci_storage_server]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehungstyp	CI
[cmdb_ci_storage_volume]	Referenz	[cmdb_ci_storage_pool]

Pure Storage FlashBlade-Erkennung

Die ServiceNow Discovery-Anwendung verwendet das FlashBlade Pure Storage-Muster, um FlashBlade-Komponenten zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery kann Pure Storage FlashBlade Version 4 erkennen.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Konfigurieren Sie Anwenderberechtigungen für das Betriebssystem UNIX

Konfigurieren Sie einen Benutzer für den Zugriff auf das Betriebssystem UNIX.

- Definieren Sie den BS-Anwender mit Berechtigungen zum Ausführen der folgenden Befehle.

Befehl	Parameter	Obligatorisch/ Optional	Beschreibung
Pureman	-	Obligatorisch	Greift auf die Liste der Pure Storage-Befehle zu und verwendet sie für die Klassifizierung
Echo	$$username$$	Obligatorisch	Füllt den Benutzernamen für die temporäre Variable aus
"pureadmin list "	+ $usr + " --api-token --expose --csv"	Obligatorisch	Ruft das Benutzer-API-Token ab, um die x-auth für die REST-Aufrufbefehle zu generieren.

- Definieren Sie den BS-Anwender mit den erforderlichen Berechtigungen zum Ausführen der folgenden REST API-Aufrufe.
  - `/api/login` – Ruft den x-auth-Tokenleser aus der Antwort in Groovy ab.
  - `/api/1.2/file -systems` – Ruft Informationen zu den Dateisystemen ab.
  - `/api/1.2/blatts` – Ruft Informationen zu Blatt.
  - `/api/1.2/dns` – Ruft Informationen über DNS ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- `/api/1.2/hardware` – Ruft Informationen zur Speicherhardware ab.
- `/api/1.4/network-interfaces` – Ruft Informationen zu Netzwerkschnittstellen ab.

Konfigurieren Sie die SSH-Anmeldeinformationen

Konfigurieren Sie unter Now Platformdie SSH-Anmeldeinformationen für den -Betriebssystembenutzer. Weitere Informationen finden Sie unter SSH-Anmeldeinformationen .

Konfigurieren Sie die Applicative-Anmeldeinformationen

Konfigurieren Sie unter Now Platformdie Applicative-Anmeldeinformationen für den Betriebssystembenutzer. Das Feld „Passwort“ ist nicht relevant. Sie können einen beliebigen Wert für das Passwort eingeben oder das Feld leer lassen. Weitere Informationen finden Sie unter Applicative-Anmeldeinformationen .

Zugriff auf den für REST-Aufrufe verwendeten Port

Geben Sie für relevante MID Servers einem Benutzer Zugriff auf den für REST-Aufrufe verwendeten Port.

Von Discovery für reines Speicher-FlashBlade gesammelte Daten

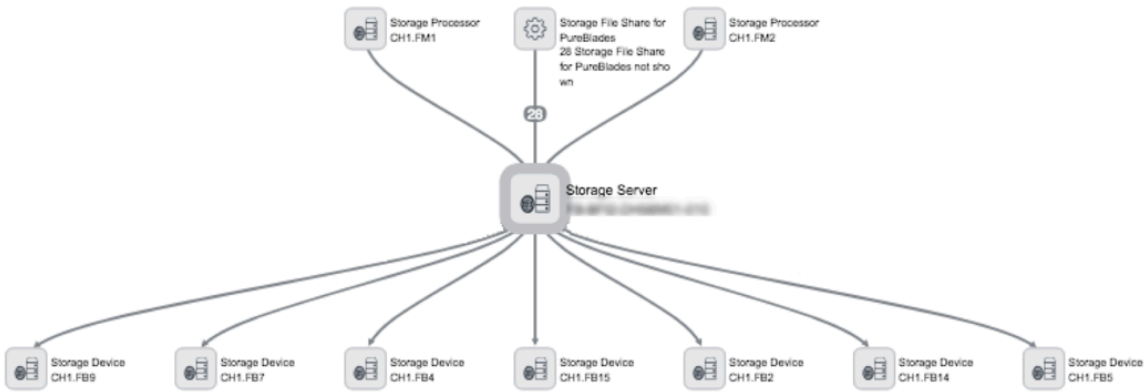
Discovery füllt die Daten in CMDB aus, wenn das FlashBlade Natural Storage-Muster ausgeführt wird.

Tabelle und Feld	Beschreibung
Speicherserver [cmdb_ci_storage_server]	Die von FileShare for PureBlade bereitgestellten Attribute des Speicherservers
IP-Adresse [ip_address]	
Seriennummer [serial_number]	
Name [name]	
Pure Storage-Prozessor [cmdb_ci_storage_processor_pure]	Die Attribute des PureBlade-Speicherprozessors
Name [name]	
Seriennummer [serial_number]	
Geräte-ID [device_id]	
Modellnummer [model_number]	
Seriell [serial]	
Steckplatz [slot]	
Typ [type]	
Status [status]	
Pure Storage-Dateifreigabe [cmdb_ci_storage_fileshare_pure]	Die Attribute des FileShare-Speichers
Name [name]	
Pfad [path]	
Protokolle [protocols]	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle und Feld	Beschreibung
Bereitgestellter Speicherplatz [provisioned_space]	
Eindeutiger Speicherplatz [unique_space]	
Snapshots-Speicherplatz [snapshots_space]	
Gesamter physischer Speicherplatz [total_physical_space]	
Freigegebener Speicherplatz [shared_space]	
Datenreduktion [data_reduction]	
Systemspeicherplatz [system_space]	
Speichergerät [cmdb_ci_storage_device]	Die Attribute des im Speicherserver enthaltenen Speichergeräts.
Geräte-ID [device_id]	
Name [name]	
Seriennummer [serial_number]	
Modellnummer [model_number]	
Speichertyp [storage_type]	

Die Grafik stellt CIs dar, die Teil der FlashBlade-Erkennung sind.



CI-Beziehungen

Discovery erstellt diese Beziehungen zur Unterstützung der Discovery von FlashBlade mit reinem Speicher.

CI	Beziehung	CI
Pure Storage-Dateifreigabe [cmdb_ci_storage_fileshare_pure]	Bereitgestellt von::Stellt bereit	Speicherserver [cmdb_ci_storage_server]
Speichergerät [cmdb_ci_storage_device]	Enthält::Enthalten in	Speicherserver [cmdb_ci_storage_server]
Speicherserver [cmdb_ci_storage_server]	Enthält::Enthalten in	Pure Storage-Prozessor [cmdb_ci_storage_processor_pure]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Red Hat JBoss Fuse-Erkennung

Die Anwendungen ServiceNow Discovery und Service-Mapping können den Fuse-Anwendungsserver mithilfe des JBoss-Fuse-Musters finden und zuordnen. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Berechtigungen

Konfigurieren Sie SSH-Anmeldeinformationen im Modul für Anmeldeinformationen der ServiceNow-Plattform für den Zugriff auf den Server, auf dem der Fuse-Server gehostet wird.

Anwender

Gewähren Sie einem Benutzer die Leserechte für den Zugriff auf die folgenden Verzeichnisse:

- `$install_directory + "/readme.txt"`

  Der Zugriff auf dieses Verzeichnis ermöglicht das Abrufen von Versionsinformationen.

- /etc/services

  Der Zugriff auf dieses Verzeichnis ermöglicht das Lesen der Hostservice-Definition.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Jboss Fuse [cmdb_ci_appl_jboss_fuse]	
config_directory	Das Konfigurationsverzeichnis des Fuse-Servers
config_file	Die Konfigurationsdatei des Fuse-Servers
install_folder	Der Installationsordner des Fuse-Servers
Version	Die Version des Fuse-Servers
name	Der während der Installation für den Fuse-Server konfigurierte Name

Von Service-Mapping während der Erkennung von oben nach unten erfasste Daten

Service-Mapping erkennt die Verbindung zwischen dem JBoss Fuse-Server und dem IBM Informix Dynamic-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Red Hat Virtualisierung-Erkennung

Die Anwendung ServiceNow Discovery verwendet das Erkennungsmuster Red Hat Virtualization (RHV), um RHV-Komponenten zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Discovery verwendet dieses Muster zum Ausführen einer horizontalen Erkennung.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

MID-Server-Anforderungen

Stellen Sie den dedizierten MID-Server für den Zugriff auf die Red Hat Virtualization Manager-Instanz (RHV-M) bereit, und verbinden Sie ihn.

Anmeldeinformationen

Konfigurieren Sie die folgenden Anmeldeinformationen:

1. Navigieren zu **Discovery** > **Anmeldeinformationen**.
2. Wählen Sie **Neu**.
3. Wählen Sie **RHV-Anmeldeinformationen**aus, füllen Sie das Formular aus, und wählen Sie **Absenden**aus.

Feld	Beschreibung
Name	Name der Anmeldeinformationen
Benutzername	Name des Benutzers, der die RHV-Erkennung ausführt
Passwort	Passwort für diesen Benutzer
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Bearertoken	Option zur Aktivierung der Verwendung eines Bearer-Tokens. Aktivieren Sie dieses Kontrollkästchen, wenn ein Bearer-Token verwendet werden soll.

Anmeldeinformationen für API-Elemente

Während der Erkennung verwendet das Muster folgende API-Elemente. Der Benutzer, der zu den Anmeldeinformationen hinzugefügt wurde, muss berechtigt sein, diese Anfragen zu senden.

- /ovirt-engine/api/
- /ovirt-engine/api/datacenters
- /ovirt-engine/api/clusters
- /ovirt-engine/api/hosts
- /ovirt-engine/api/vms

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie CI-Klassenmodelle CMDB hinzu

Fügen Sie Klassenmodelle hinzu, die die Klassenhierarchie CMDB erweitern, indem Sie die Anwendung CMDB CI-Klassenmodelle verwenden. Die App ist im ServiceNow Storeverfügbar. Discovery -Muster verwenden diese Klassenerweiterungen, um CIs auszufüllen. Weitere Informationen finden Sie unter Erweiterungsklassen für Red Hat Virtualization (RHV) .

Cloud-Servicekonten erstellen

Erstellen Sie ein RHV-Cloud-Servicekonto in der Instanz ServiceNow.

1. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**.
2. Wählen Sie **Neu** aus, und füllen Sie das Formular aus.

Feld	Beschreibung
Name	Name für das Konto. Beispiel: RHV-Phase
Konto-ID	Konto-ID, zu der diese Anmeldeinformationen gehören. Geben Sie die API-URL der RHV-M-Instanz an, einschließlich des Ports. Beispiel: https://my-manager-instance.com:443
Discovery-Anmeldeinformationen	Die Erkennung-Anmeldeinformationen, die zuvor erstellt wurden
Datencenter-Typ	Die Tabelle aus der CMDB, die den Typ des Rechenzentrums darstellt. Wählen Sie RHV LDC [cmdb_ci_rhv_ldc] aus.

Erkennungszeitpläne erstellen

Erstellen Sie einen Erkennungszeitplan, um eine vollständige Erkennung von RHV-Komponenten durchzuführen.

1. Öffnen Sie das zuvor erstellte RHV-Cloud-Servicekonto.
2. Wählen Sie unter **Zugehörige Linksdie Option Discovery-Zeitplan erstellen aus**.

   Unter dem Menüelement **Discovery-Zeitplan** wird ein neuer Zeitplan erstellt.

Von Discovery während der horizontalen Erkennung erfasste Daten

Das Muster erkennt Daten, die Ihnen helfen, die RHV-Topologie Ihrer Organisation und die Beziehungen zwischen ihren Komponenten zu verstehen. Die erkannten Daten umfassen die folgenden Tabellen und Felder.

RHV-LDC [cmdb_ci_rhv_ldc]

Feld	Beschreibung
Name [name]	Name des RHV-Rechenzentrums.
Objekt-ID [object_id]	Eindeutiger Objektbezeichner.
Beschreibung [short_description]	Beschreibung des von Ihnen angegebenen RHV-Rechenzentrums zur einfachen Identifizierung.
Quotenmodus [quota_mode]	Kontingentmodusrichtlinie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

RHV-LDC [cmdb_ci_rhv_ldc] (Fortsetzung)

Feld	Beschreibung
URL [url]	API-URL für den Zugriff auf das Rechenzentrum.
href-ID [href_id]	Href-ID

RHV-Cluster [cmdb_ci_rhv_cluster]

Feld	Beschreibung
Name [name]	Name des RHV-Clusters
Objekt-ID [object_id]	Eindeutiger Objektbezeichner.
Beschreibung [short_description]	Beschreibung des RHV-Clusters, die Sie zur einfachen Identifizierung angeben
CPU-Typ [cpu_type]	CPU-Typ Beispiel: x86_64
CPU-Architektur [cpu_architecture]	CPU-Architektur. Beispiel: Intel Broadwell IBRS SSBD MDS Family
KSM [KSM]	Aktivierungsstatus der Kernel-Richtlinie für das Zusammenführen derselben Seite (Kernel Same-Page Merging, KSM).
Fencing-Richtlinie [fencing_policy]	Fencing-Richtlinie
Overcommit für Arbeitsspeicher [memory_overcommit]	Menge des im Cluster zulässigen Speichers mit Mehrfachvergabe
Große transparente Seiten [thp]	Richtlinie für transparente Seiten mit großem Arbeitsspeicher
Ballonfahren [Ballonieren]	Arbeitsspeicher-Ballooning für Gäste
Kompatibilitätsversion [compatibility_version]	Kompatibilitätsversion
URL [url]	API-URL für den Zugriff auf das Cluster
href-ID [href_id]	Href-ID

RHV-Server [cmdb_ci_rhv_server]

Feld	Beschreibung
Name [name]	Name des RHV-Servers
Seriennummer [serial_number]	Seriennummer
Objekt-ID [object_id]	Eindeutiger Objektbezeichner.
Anzahl der CPU-Kerne [cpu_core_count]	Gesamtzahl der Kerne
CPU-Anzahl [cpu_count]	Gesamtzahl der CPUs.
CPU-Typ [cpu_type]	CPU-Typ

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

RHV-Server [cmdb_ci_rhv_server] (Fortsetzung)

Feld	Beschreibung
CPU-Geschwindigkeit (MHz) [cpu_speed]	CPU-Geschwindigkeit (MHz)
Hostname [host_name]	Hostname
IP-Adresse [ip_address]	IP-Adresse des RHV-Servers
Modell-ID [model_id]	Modell-ID
Betriebssystem [os]	Betriebssystemfamilie
BS-Version [os_version]	Version des Betriebssystems.
RAM (MB) [ram]	Menge des Arbeitsspeichers (MB)
URL [url]	Verwendete API-URL, die für den Zugriff auf den Server verwendet wird

RHV-VM-Instanz [cmdb_ci_rhv_vm_instance]

Feld	Beschreibung
Name [name]	Name der RHV-Instanz
Status [state]	Status der RHV-Instanz
Objekt-ID [object_id]	Eindeutiger Objektbezeichner.
IP-Adresse [ip_address]	IP-Adresse der RHV-Instanz
Datenträger [disks]	Anzahl der Datenträger
MAC-Adresse [mac_address]	MAC-Adresse der RHV-Instanz
Verwaltungs-URL [mgmt_url]	Verwaltungs-API-URL
Beschreibung [short_description]	Beschreibung der RHV-Instanz, die Sie zur einfachen Identifizierung angeben
Vollständig qualifizierter Domänenname [fqdn]	Vollqualifizierter Domänenname (FQDN) der RHV-Instanz
CPU-Architektur [cpu_architecture]	CPU-Architektur. Beispiel: Intel Broadwell IBRS SSBD MDS-Familie.
Geschützte löschen [delete_protected]	Geschützte löschen, mögliche Werte: true oder false.
CPUs [cpus]	Anzahl an CPUs
HA-Priorität [ha_priority]	Priorität für hohe Verfügbarkeit (HA).
Hochverfügbarkeit [high_availability]	Hochverfügbarkeit, mögliche Werte: true oder false.
Arbeitsspeicher MAX [memory_policy_max]	Maximaler Arbeitsspeicher in der dynamischen Zuteilungsrichtlinie für Arbeitsspeicher für die virtuelle Maschine (VM).
Arbeitsspeichergarantie (MB) [memory_policy_guaranteed]	Garantierter Arbeitsspeicher für die VM (MB)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

RHV-VM-Instanz [cmdb_ci_rhv_vm_instance] (Fortsetzung)

Feld	Beschreibung
Mehrere Warteschlangen [multi_queues]	Mehrere Warteschlangen
Platzierungsrichtlinie [placement_policy]	Platzierungsrichtlinie
Zustandslos [stateless]	Zustandslos, mögliche Werte: wahr oder falsch.
Bei Speicherfehler [storage_error_resume_behaviour]	Verhalten einer VM, die aufgrund eines Speicher-E/A-Fehlers angehalten wurde. Beispiel: AUTO_RESUME, LEAVE_PAUSED und KILL.
Startzeit [start_time]	Startzeit der VM.
Endzeit [stop_time]	Endzeit der VM.
Themen [threads]	Anzahl der Threads
Zeitzone [time_zone]	Zeitzone der VM.
USB [usb]	USB-aktivierter Status
Einmal ausführen [run_once]	Einmal ausführen
RHV-Typ [rhv_type]	RHV-Typ

Cloud-Servicekonto [cmdb_ci_cloud_service_account]

Feld	Beschreibung
Account-ID [account_id]	Konto-ID für dieses Cloud-Servicekonto
Objekt-ID [object_id]	Konto-ID für dieses Cloud-Servicekonto
Rechenzentrumstyp [datacenter_type]	Typ des Rechenzentrums: RHV LDC [cmdb_ci_rhv_ldc].
Discovery-Anmeldeinformationen [discovery_credentials]	Anmeldeinformationen für dieses Cloud-Servicekonto

IP-Adresse [cmdb_ci_ip_address]

Feld	Beschreibung
Name [name]	Die IP-Adresse der Netzwerkschnittstellenkarte (NIC), die der VM zugewiesen ist.
IP-Adresse [ip_address]	Die IP-Adresse der NIC, die der VM zugewiesen ist.
IP-Version [ip_version]	IP-Version: IPv4 oder IPv6.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

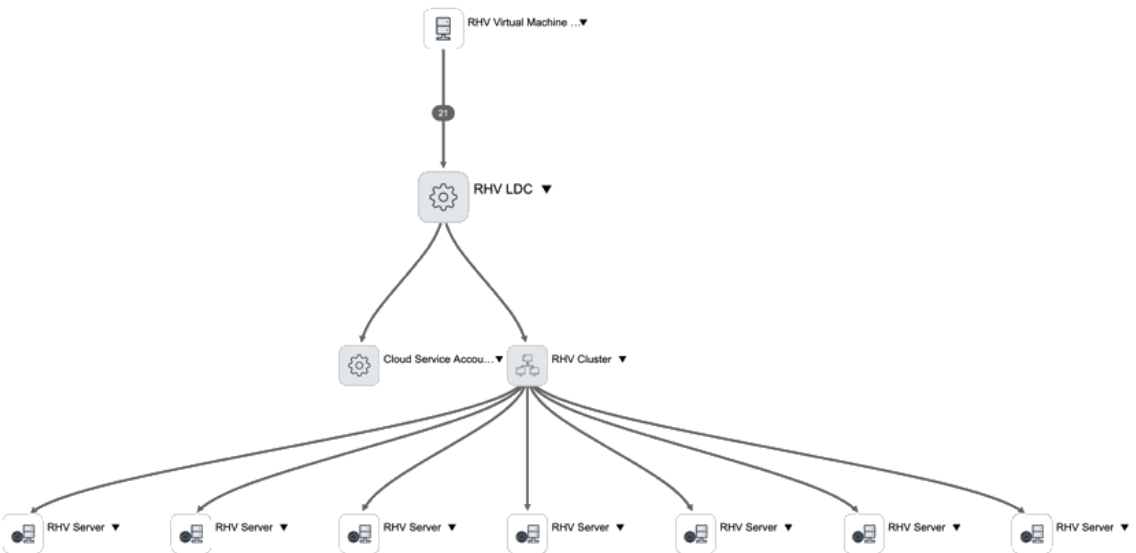
VNIC-Endpunkt [cmdb_ci_endpoint_vnic]

Feld	Beschreibung
Objekt-ID [object_id]	Eindeutiger Bezeichner, der von RHV für diese Ressource zugewiesen wird.
Name [name]	Name für den Endpunkt der virtuellen Netzwerkschnittstellenkarte (vNIC).
IP-Adresse [ip_address]	An die Netzwerkschnittstelle gebundene IP-Adresse.

Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]

Feld	Beschreibung
Objekt-ID [object_id]	ID der Netzwerkschnittstelle.
Name [name]	Name der Netzwerkschnittstelle.
IP-Adresse [ip_address]	An die Netzwerkschnittstelle gebundene IP-Adresse.
Öffentliche IP [public_ip]	Öffentliche IP-Adresse, die an die Netzwerkschnittstelle gebunden ist.
Private IP [private_ip]	An die Netzwerkschnittstelle gebundene private IP-Adresse.

Die Abhängigkeitsansichten-Karte zeigt die erkannten RHV-Komponenten in Ihrer Organisation und die Beziehungen zwischen ihnen an.



CI-Beziehungen

Die folgenden -Beziehungen werden erstellt, um die RHV-Discovery zu unterstützen.

CI	Beziehung	CI
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	Gehostet auf::Hostet	RHV-LDC [cmdb_ci_rhv_ldc]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	Erweitert::Erweitert um	Netzwerkadapter [cmdb_ci_network_adapter]
Cloud-Servicekonto [cmdb_ci_cloud_service_account]	Erweitert::Erweitert um	VM-Objekt [cmdb_ci_vm_object]
IP-Adresse [cmdb_ci_ip_address]	Erweitert::Erweitert um	Konfigurationselement [cmdb_ci]
RHV-Cluster [cmdb_ci_rhv_cluster]	Mitglieder::Mitglied von	RHV-Server [cmdb_ci_rhv_server]
RHV-Cluster [cmdb_ci_rhv_cluster]	Erweitert::Erweitert um	RHV-Objekt [cmdb_ci_rhv_object]
RHV-LDC [cmdb_ci_rhv_ldc]	Enthält::Enthalten in	RHV-Cluster [cmdb_ci_rhv_cluster]
RHV-LDC [cmdb_ci_rhv_ldc]	Gehostet auf::Hostet	Cloud-Servicekonto [cmdb_ci_cloud_service_account]
RHV-LDC [cmdb_ci_rhv_ldc]	Erweitert::Erweitert um	Logisches Rechenzentrum [cmdb_ci_logical_datacenter]
RHV-Server [cmdb_ci_rhv_server]	Wird ausgeführt auf::Wird ausgeführt	Linux-Server [cmdb_ci_linux_server]
RHV-Server [cmdb_ci_rhv_server]	Erweitert::Erweitert um	Virtualisierungsserver [cmdb_ci_virtualization_server]
RHV-VM-Instanz [cmdb_ci_rhv_vm_instance]	Gehostet auf::Hostet	RHV-Cluster [cmdb_ci_rhv_cluster]
RHV-VM-Instanz [cmdb_ci_rhv_vm_instance]	Gehostet auf::Hostet	RHV-LDC [cmdb_ci_rhv_ldc]
RHV-VM-Instanz [cmdb_ci_rhv_vm_instance]	Eigentümer von::Eigentum von	IP-Adresse [cmdb_ci_ip_address]
RHV-VM-Instanz [cmdb_ci_rhv_vm_instance]	Registriert am::Registriert	RHV-Server [cmdb_ci_rhv_server]
RHV-VM-Instanz [cmdb_ci_rhv_vm_instance]	Endpunkt verwenden an::Endpunkt verwenden von	VNIC-Endpunkt [cmdb_ci_endpoint_vnic]
RHV-VM-Instanz [cmdb_ci_rhv_vm_instance]	Erweitert::Erweitert um	VM-Instanz [cmdb_ci_vm_instance]
VNIC-Endpunkt [cmdb_ci_endpoint_vnic]	Endpunkt implementieren in::Endpunkt implementieren von	Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]
VNIC-Endpunkt [cmdb_ci_endpoint_vnic]	Erweitert::Erweitert um	Endpunkt [cmdb_ci_endpoint]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erkennung von Rubrik-Clustern

Discovery verwendet mehrere Muster, um sämtliche Daten über Rubrik-Cluster zu finden. Um diese Ressourcen zu erkennen, müssen Sie die Anwendungen Discovery and Service Mapping Patterns und CMDB CI Class Models aus dem ServiceNow Store installieren, da die beiden Anwendungen voneinander abhängig sind.

Sie können die Muster zur Erkennung von Rubrik-Komponenten auf der Now Platform mit Release Paris oder höher verwenden.

Hinweis: Das in Version 1.0.78 von Discovery and Service Mapping Patterns angewendete Update behebt ein Problem mit doppelten CI-Typen in der CMDB. Wenn Sie Rubrik-Erkennungsmuster verwenden und bereits die Versionen 1.21.0, 1.23.0, 1.24.0 oder 1.25.0 der Store-App CMDB CI Class Models (sn_cmdb_ci_class) oder die Versionen 1.0.73, 1.0.74, 1.0.75 oder 1.0.76 der Anwendung Discovery and Service Mapping Patterns (sn_itom_pattern) installiert haben, sollten Sie den Anweisungen in KB0957523 folgen.

Alle Informationen für das Haupt-CI (Rubrik-Cluster) und die entsprechenden CI-Typen werden durch Aufrufe von REST APIs zurückgegeben. Alle Informationen für das Haupt-CI (Rubrik-Cluster) und die entsprechenden CI-Typen werden durch Aufrufe von REST APIs zurückgegeben.

Beachten Sie die folgenden Einschränkungen:

- Aufgrund der Einschränkungen des Mechanismus für große Nutzlasten werden in den Releases Paris und Quebec keine Referenzfelder unterstützt.
- Alle von der Rubrik REST API für Hosts (Server) zurückgegebenen Entitäten mit IP-Adressen, die nicht in Hostnamen aufgelöst werden, werden aus der Rubrik-Erkennung herausgefiltert (ausgeschlossen). Dies geschieht, um die Erstellung von Duplikaten in der CMDB zu verhindern.

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Store-App Discovery and Service Mapping Patterns

Stellen Sie Release 1.0.73 oder höher aus dem ServiceNow Store bereit.

Store-App „CMDB CI Class Models“

Stellen Sie Release 1.21.0 oder höher aus dem ServiceNow Store bereit.

Berechtigungen für Basisauthentifizierung

Stellen Sie sicher, dass zur Authentifizierung der REST API-Aufrufe die Anmeldeinformationen für die Basisauthentifizierung konfiguriert sind.

Anmeldeinformationsaliase, die den Rubrik-Anmeldeinformationen vom Typ Standardauthentifizierung zugeordnet sind, müssen ebenfalls erstellt werden. Diese Aliase dienen zusammen mit der IP-Adresse als Eingabeparameter.

Diese werden für die Erkennung aller CI-Typen verwendet, die dem Rubrik-Cluster zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sicherheitsschematyp: HTTP
- HTTP-Autorisierungsschema: Standard

MID-Server

Stellen Sie sicher, dass der MID Server auf die Ziel-Appliance zugreifen kann.

Zeitplan für Erkennung ohne Server erstellen

Erstellen Sie einen Erkennungszeitplan ohne Server, um eine gezielte Erkennung von Rubrik-Clusterressourcen durchzuführen.

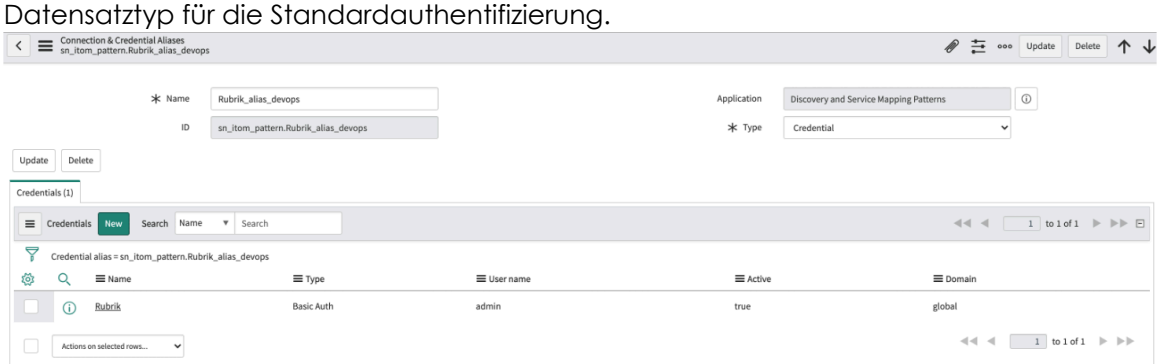
Hinweis: Der Discovery-Zeitplan, der alle mit Rubrik verknüpften Muster auslöst, unterstützt nur den Typ der serverlosen Erkennung. Außerdem muss für jedes Rubrik-Cluster (Brik) ein neuer Zeitplan für die serverlose Erkennung erstellt werden. Der Zeitplan muss die IP-Adresse aller Rubrik-Knoten enthalten, die dem Rubrik-Cluster zugeordnet sind, und den Anmeldeinformationsalias, der dem Anmeldeinformationsdatensatz der Rubrik-Standardauthentifizierung zugeordnet ist.

1. Navigieren zu **Discovery** > **Discovery-Zeitpläne**.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

Formular „Discovery-Zeitplan“

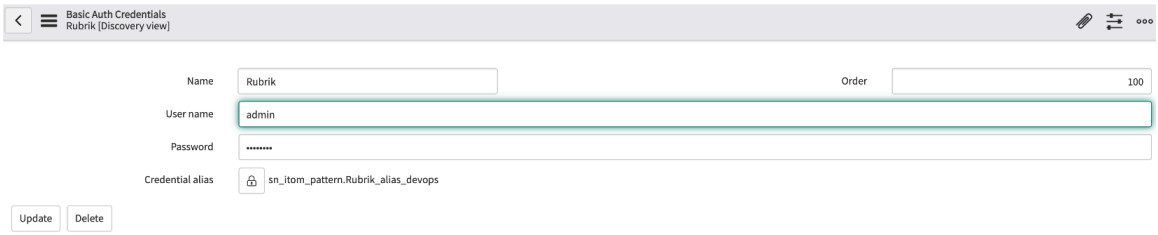
Feld	Beschreibung
Name	Name des Discovery-Zeitplans. Zum Beispiel `Erkennung Rubrik`.
Erkennen	Erkennungstyp. Wählen Sie **Ohne Server** aus.
MID-Server	Name des MID-Servers
Aktiv	Option zum Aktivieren dieses Erkennungszeitplans. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

3. Klicken Sie mit der rechten Maustaste auf den Header des Formulars „Discovery-Zeitplan“, und wählen Sie **Speichern** aus.
4. Navigieren Sie zu **Aliasse für Verbindungen und Anmeldeinformationen**, und erstellen Sie einen neuen Datensatztyp für Anmeldeinformationen. Erstellen Sie im Formular der zugehörigen Liste „Anmeldeinformationen“ einen neuen Datensatztyp für die Standardauthentifizierung.

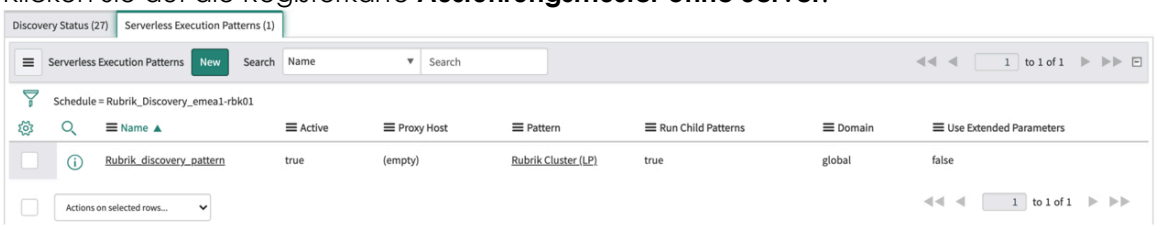


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Der Anmeldeinformationsalias kann vorhandenen Anmeldeinformationen zugeordnet werden. Beim Erstellen eines Anmeldeinformationsdatensatzes können Sie ihm auch den Anmeldeinformationsalias zuordnen. Klicken Sie auf das Schloss-Symbol **Anmeldeinformationsalias** im Datensatztyp „Aliasse für Verbindungen und Anmeldeinformationen“, den Sie oben angelegt haben, und ordnen Sie ihn nach Bedarf zu.

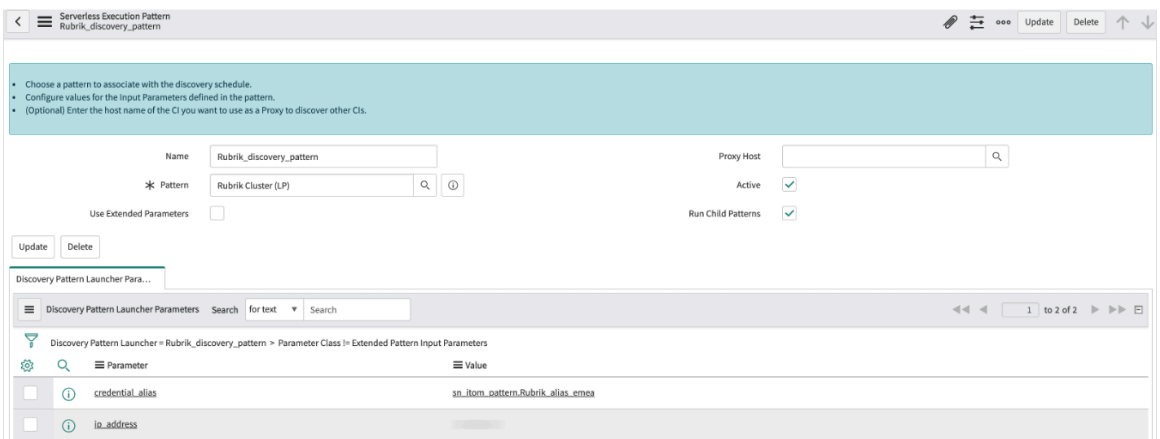


5. Klicken Sie auf die Registerkarte **Ausführungsmuster ohne Server**.



6. Stellen Sie sicher, dass die Spalte „Untergeordnete Muster ausführen“ für das Rubrik-Erkennungsmuster auf **true** gesetzt ist. Dadurch werden alle untergeordneten Muster ausgelöst, die dem Rubrik-Erkennungsmuster zugeordnet sind. Dies ist aufgrund des Mechanismus für große Nutzlasten erforderlich, der für die Erkennung des Rubrik-Clusters und aller entsprechenden CI-Typen verwendet wird.
7. Legen Sie unter **Startprogrammparameter für Discovery-Muster** die Parameter **credential_alias** und **ip_adresse** fest, die als Eingabeparameter für die Auslösung des Discovery-Zeitplans und das zugehörige Rubrik-Erkennungsmuster dienen.

   Setzen Sie den Parameter **ip_address** auf eine der IP-Adressen eines der Rubrik-Knoten, die dem Rubrik-Cluster zugeordnet sind. Setzen Sie **credential_alias** auf die ID des Anmeldeinformations-Datensatztyps, der in **Aliasse für Verbindungen und Anmeldeinformationen** erstellt wurde und mit dem Datensatztyp der Standardauthentifizierung für Rubrik-Anmeldedaten verwandt ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Ressourcen, die mithilfe des Musters „Rubrik AIX Host (LP)“ erkannt wurden

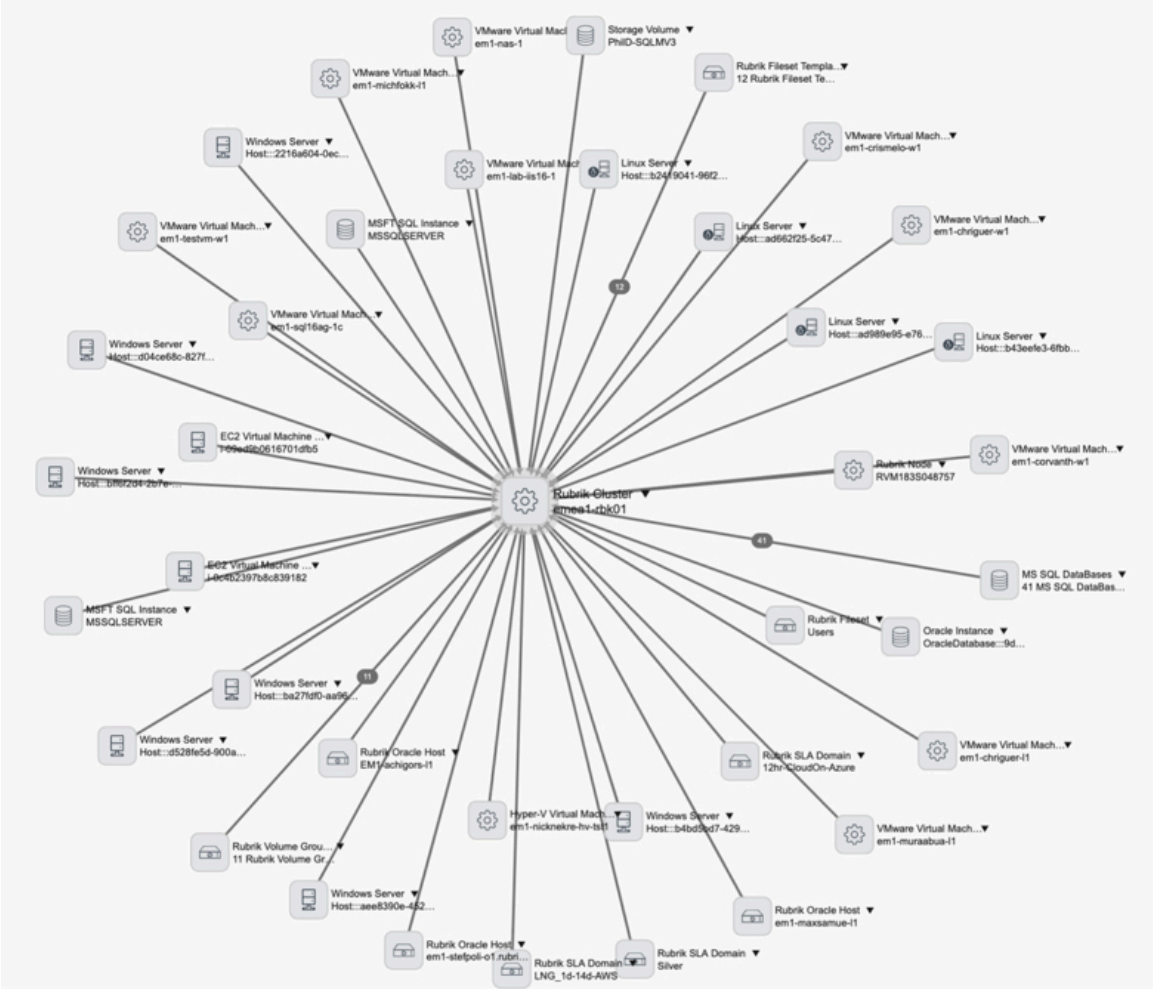
Feld	Beschreibung
Rubrik AIX-Host [cmdb_ci_aix_server]	
name	Name des Hosts.
host_name	Hostname des Hosts.
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
os	Typ des auf dem Host konfigurierten Betriebssystems.
os_version	Version, Edition oder Distribution des auf dem Host konfigurierten Betriebssystems.
operational_status	Aktueller Betriebsstatus des Hosts.

Ressourcen, die mithilfe des Musters „Rubrik Cluster (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Cluster [cmdb_ci_rubrik_cluster]	
cluster_id	Eindeutige ID des Rubrik-Clusters
name	Name des Rubrik-Clusters
cluster_version	Aktuelle Version des Rubrik-Clusters
api_version	API Version des Rubrik-Clusters
timezone	Vom Rubrik-Cluster verwendete Zeitzone

Die Dependency Views-Zuordnung zeigt die erkannten Clusterressourcen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



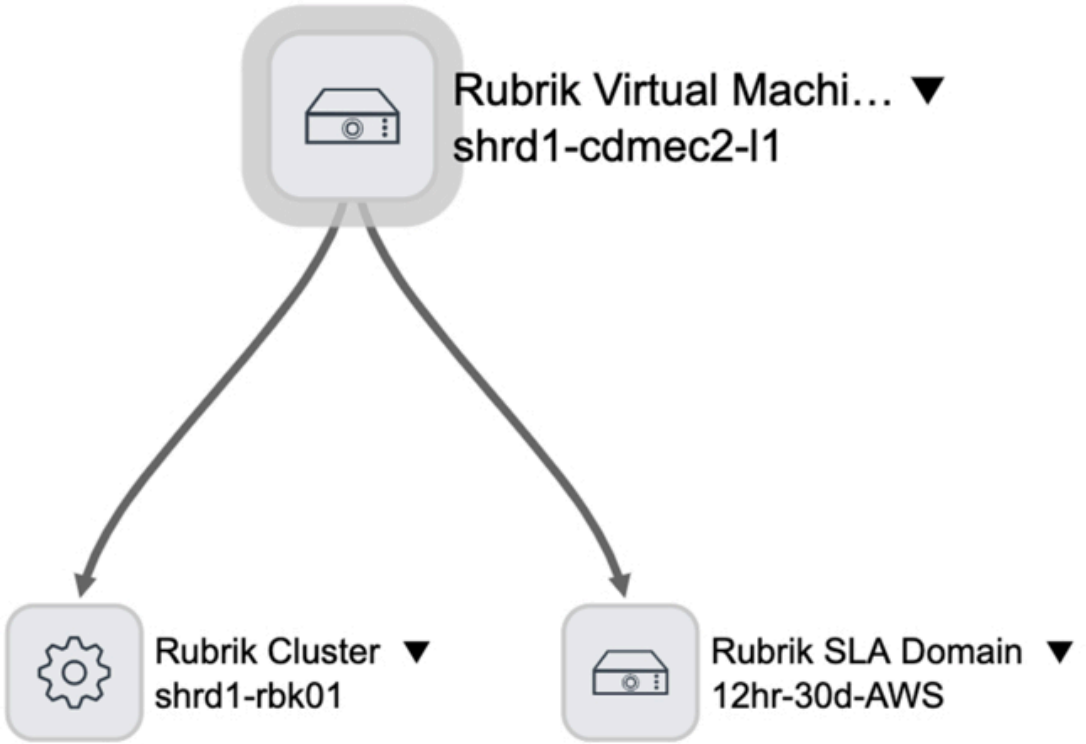
Ressourcen, die mithilfe des Musters „Rubrik EC2 Instance (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-EC2-Instanz [cmdb_ci_rubrik_vm_instance]	
object_id	ID der EC2-Instanz im Rubrik-Kontext
name	Name der EC2-Instanz im AWS-Kontext
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
account_id	ID des der EC2-Instanz zugeordneten AWS-Kontos
account_name	Name des der EC2-Instanz zugeordneten AWS-Kontos
instance_id	ID der EC2-Instanz im AWS-Kontext
instance_name	Name der EC2-Instanz im Rubrik-Kontext
instance_type	Vorlagentyp der EC2-Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
region	Geografische Region, in der sich die EC2-Instanz im AWS-Kontext befindet

Die Dependency Views-Zuordnung zeigt die erkannten EC2-Instanzen und deren Beziehungen untereinander.

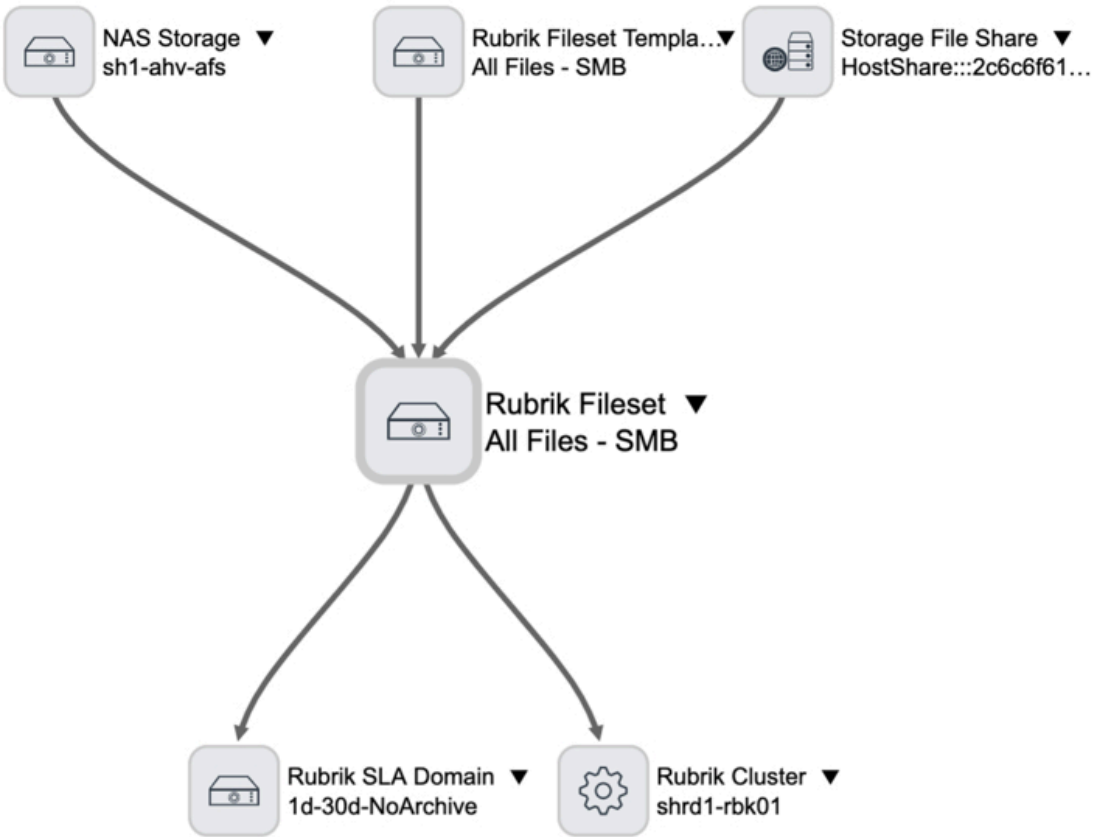


Ressourcen, die mithilfe des Musters „Rubrik Fileset (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Dateisatz [cmdb_ci_rubrik_fileset]	
object_id	ID des Rubrik-Dateisatzes
name	Name des Rubrik-Dateisatzes
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
host_id	ID des Hosts, dem der Rubrik-Dateisatz zugeordnet ist
template_id	ID der Rubrik-Dateisatzvorlage, aus der der Rubrik-Dateisatz die Ressourcen definiert
share_id	ID der Rubrik-Freigabe, die Besitzer des Rubrik-Dateisatzes ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Dependency Views-Zuordnung zeigt die erkannten Dateisätze und deren Beziehungen untereinander.

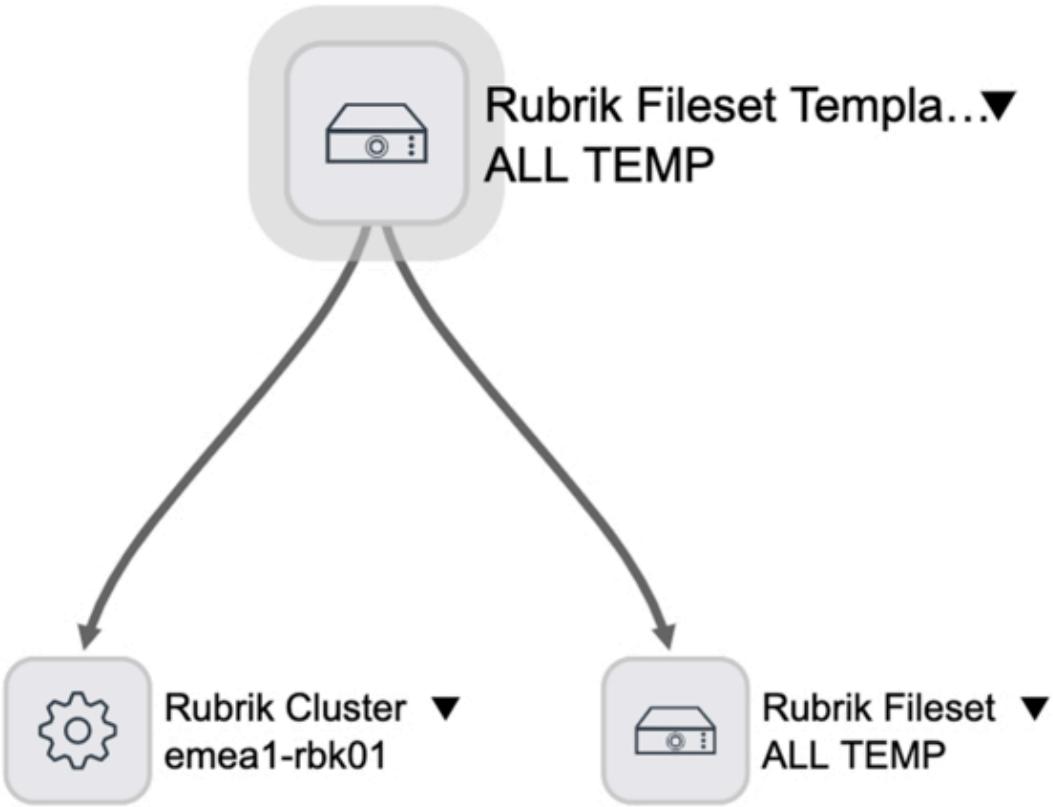


Ressourcen, die mithilfe des Musters „Rubrik Fileset Template (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Dateisatzvorlage [cmdb_ci_rubrik_fileset]	
object_id	ID der Rubrik-Dateisatzvorlage
name	Name der Rubrik-Dateisatzvorlage
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
share_count	Anzahl der Freigaben, die der Rubrik-Dateisatzvorlage zugeordnet sind
share_type	Typ der Freigaben, die der Rubrik-Dateisatzvorlage zugeordnet sind
host_count	Hostzähler, der der Rubrik-Dateisatzvorlage zugeordnet ist
os_type	Typ des Betriebssystems, das der Rubrik-Dateisatzvorlage zugeordnet ist

Die Dependency Views-Zuordnung zeigt die erkannten Dateisatzvorlagen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



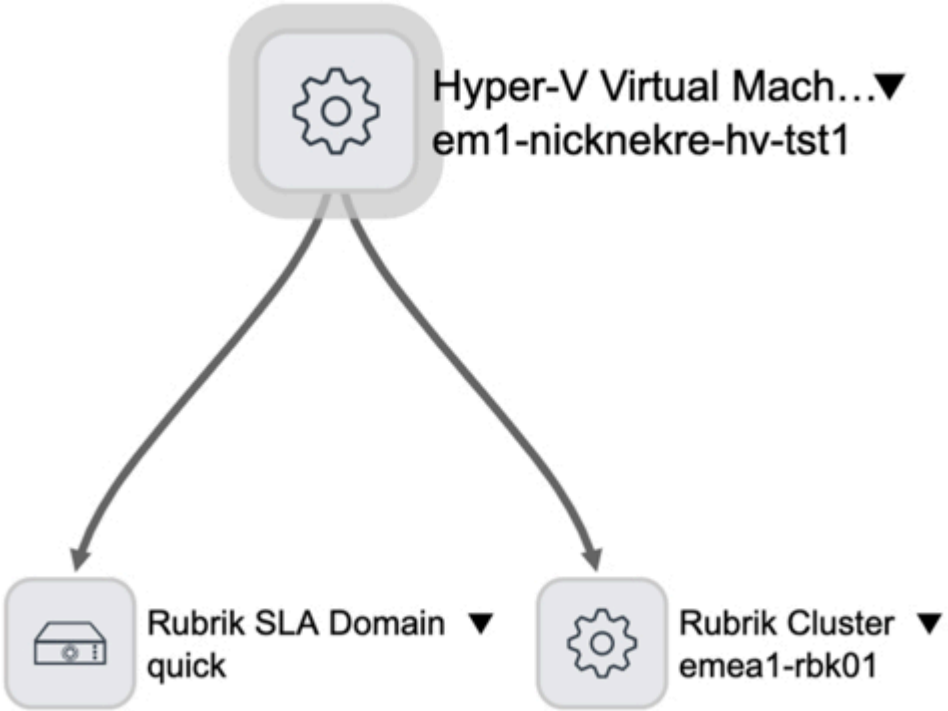
Ressourcen, die mithilfe des Musters „Rubrik Hyper-V Instance (LP)“ erkannt wurden

Hinweis: Bei der Erkennung von Hyper-V-Instanzen werden nur vorhandene CIs aktualisiert. Das liegt an einer Einschränkung in der Rubrik-REST API, die die GUID (object_id) der Hyper-V-Instanz nicht zurückgibt. Wenn keine Übereinstimmung zwischen den Daten aus der REST API und der CMDB besteht, werden keine CIs aktualisiert. Darüber hinaus wird das Muster „Rubrik Hyper-V Instance (LP)“ mit dem Status „Fehler“ abgeschlossen, wenn es keine Übereinstimmung gibt. Das ist das erwartete Verhalten.

Feld	Beschreibung
Rubrik Hyper-V-Instanz [cmdb_ci_hyper_v_instance]	
name	Name der Hyper-V-Instanz
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
host_id	ID des Hosts, dem die Hyper-V-Instanz zugeordnet ist

Die Dependency Views-Zuordnung zeigt die erkannten Hyper-V-Instanzen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

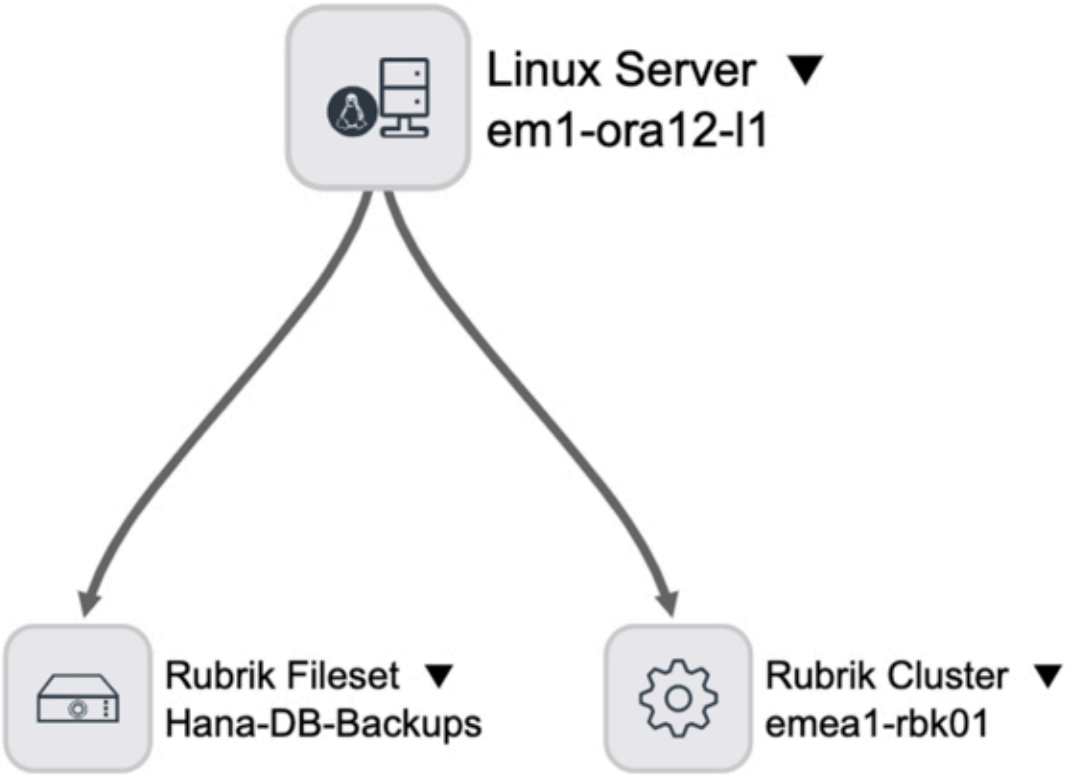


Ressourcen, die mithilfe des Musters „Rubrik Linux Host (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Linux-Host [cmdb_ci_linux_server]	
name	Name des Hosts.
host_name	Hostname des Hosts.
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
os	Typ des auf dem Host konfigurierten Betriebssystems.
os_version	Version, Edition oder Distribution des auf dem Host konfigurierten Betriebssystems.
operational_status	Aktueller Betriebsstatus des Hosts.

Die Dependency Views-Zuordnung zeigt die erkannten Hosts und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

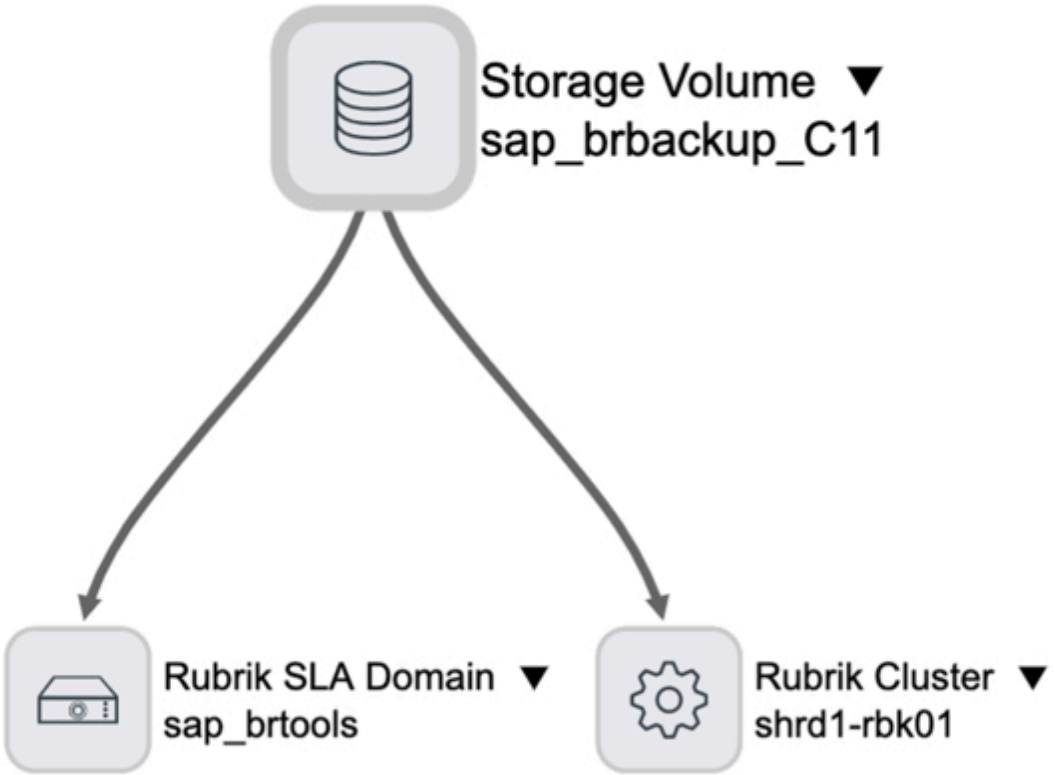


Ressourcen, die mithilfe des Musters „Rubrik Managed Volume (LP)“ erkannt wurden

Feld	Beschreibung
Verwaltetes Rubrik-Volume [cmdb_ci_storage_volume]	
object_id	ID des verwalteten Speichervolume
volume_id	Volume-ID des verwalteten Speichervolume
name	Name des verwalteten Speichervolume
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
size_bytes	Gesamtkapazität des Speichervolume in Byte
used_size_bytes	Größe der insgesamt genutzten Kapazität in Byte
snapshot_count	Snapshot-Zähler des verwalteten Speichervolume
share_type	Freigegebener Typ des verwalteten Speichervolume
state	Status des verwalteten Speichervolume

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Dependency Views-Zuordnung zeigt die erkannten verwalteten Speicherinstanzen und deren Beziehungen untereinander.



Ressourcen, die mithilfe des Musters „Rubrik MS SQL DB (LP)“ erkannt wurden

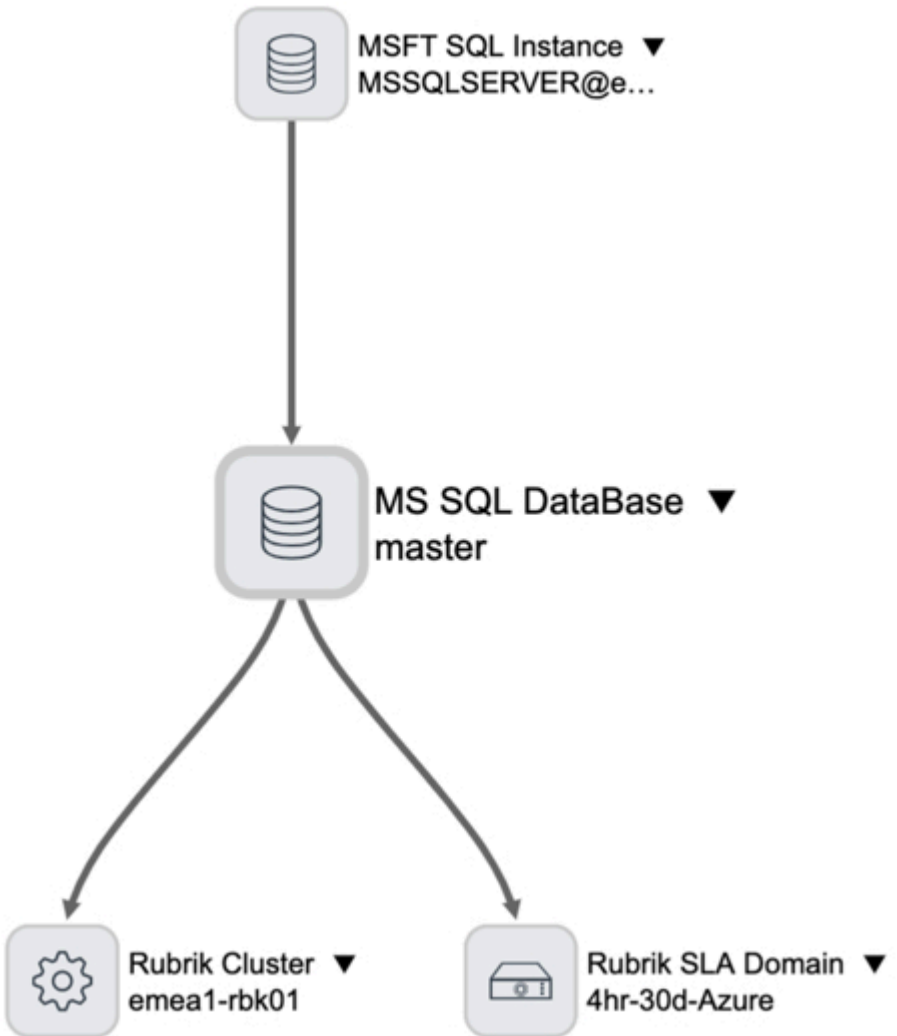
Hinweis: Beziehungen zwischen MS SQL-Instanzen, die in Windows-Clustern gehostet werden, und den zugeordneten MS SQL-Datenbanken werden ab Release 1.0.79 der Anwendung Discovery and Service Mapping Patterns nicht unterstützt. Das liegt an unzureichenden Informationen, die von der Rubrik-REST API für Windows-Cluster zurückgegeben werden. Die mit Windows-Clustern verknüpften MS SQL-Instanzen und MS SQL-Datenbanken werden aus den zugeordneten Mustern der Rubrik-Erkennung herausgefiltert.

Feld	Beschreibung
Rubrik MS SQL-DB [cmdb_ci_db_mssql_database]	
Datenbank	ID der MS SQL-Datenbank
name	Name der MS SQL-Datenbank
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
host_id	ID des Hosts, auf dem die MS SQL-Datenbank ausgeführt wird
instance_id	ID der Datenbankinstanz, der die MS SQL-Datenbank zugeordnet ist
state	Status der MS SQL-Datenbank
recovery_model	Typ des Wiederherstellungsmodells der MS SQL-Datenbank
last_snapshot	Letzter Snapshot der MS SQL-Datenbank im Format JJ-MM-TT HH-MM-SS
missed_snapshot_count	Anzahl der verpassten Snapshots der MS SQL-Datenbank

Die Dependency Views-Zuordnung zeigt die erkannten MS SQL-Datenbanken und deren Beziehungen untereinander.



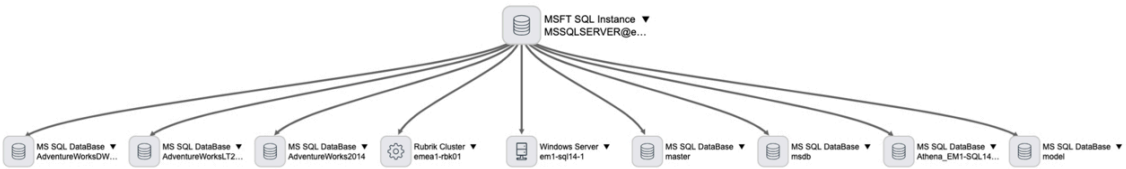
Ressourcen, die mithilfe des Musters „Rubrik MS SQL Instance (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Beziehungen zwischen MS SQL-Instanzen, die in Windows-Clustern gehostet werden, und den zugeordneten MS SQL-Datenbanken werden ab Release 1.0.79 der Anwendung Discovery and Service Mapping Patterns nicht unterstützt. Das liegt an unzureichenden Informationen, die von der Rubrik-REST API für Windows-Cluster zurückgegeben werden. Die mit Windows-Clustern verknüpften MS SQL-Instanzen und MS SQL-Datenbanken werden aus den zugeordneten Mustern der Rubrik-Erkennung herausgefiltert.

Feld	Beschreibung
Rubrik MS SQL-Instanz [cmdb_ci_db_mssql_instance]	
instance_name	ID der MS SQL-Instanz
name	Name der MS SQL-Instanz
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
host_id	ID des Hosts, dem die MS SQL-Instanz zugeordnet ist
Version	Version der MS SQL-Instanz

Die Dependency Views-Zuordnung zeigt die erkannten MS SQL-Instanzen und deren Beziehungen untereinander.

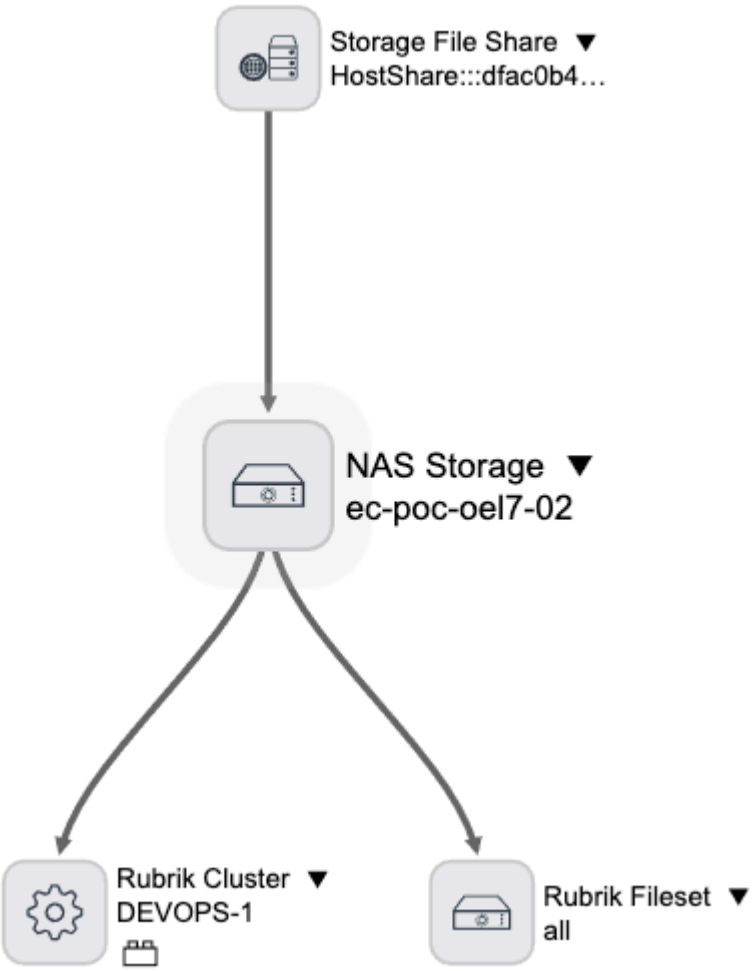


Ressourcen, die mithilfe des Musters „Rubrik NAS Host (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik NAS-Host [cmdb_ci_nas_storage]	
name	Name des Hosts.
host_name	Hostname des Hosts.
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
short_description	Lieferantentyp des NAS-Speichers.
operational_status	Aktueller Betriebsstatus des Hosts.

Die Dependency Views-Zuordnung zeigt die erkannten Hosts und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



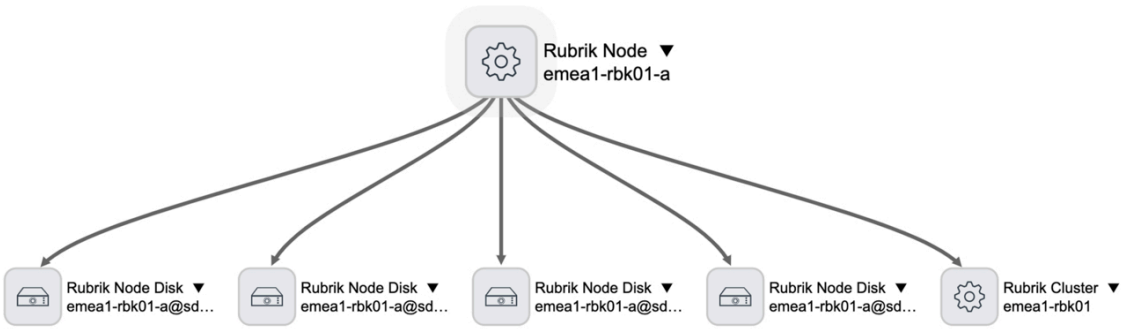
Ressourcen, die mithilfe des Musters „Rubrik Node (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Knoten [cmdb_ci_rubrik_node]	
brik_id	Gehäuse-ID des Rubrik-Knotens
name	Eindeutiger Name des Rubrik-Knotens, der als ID des Rubrik-Knotens dient
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
unavailable_disks	True/False. Gibt an, dass im Rubrik-Knoten nichtverfügbare Datenträger vorhanden sind
ip_address	IP-Adresse des Rubrik-Knotens, der dem Rubrik-Cluster zugeordnet ist
tunnel_enabled	True/False. Gibt an, ob für den Rubrik-Knoten Tunneling aktiviert ist
cpu_core_count	Anzahl der CPU-Kerne des Rubrik-Knotens

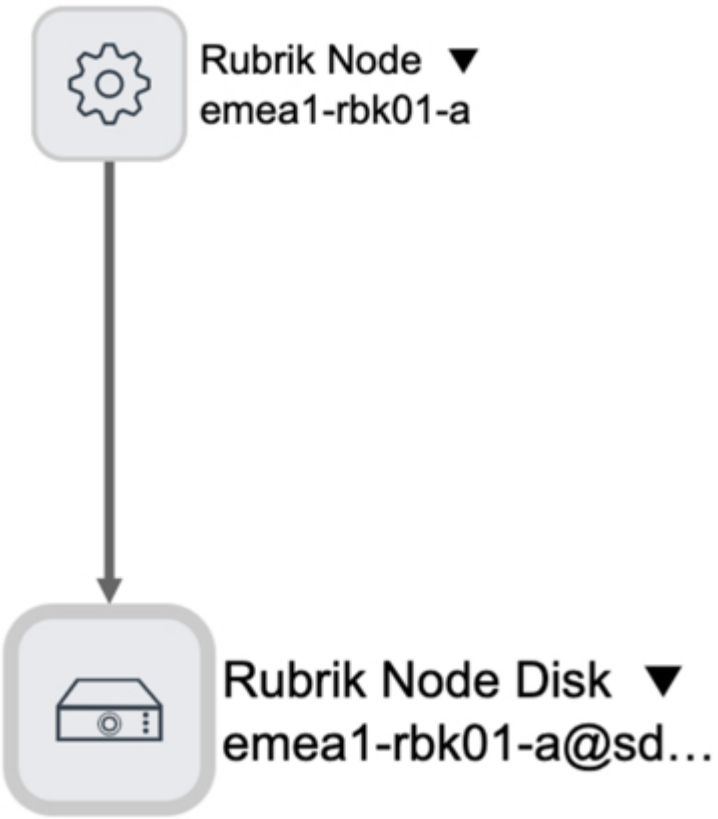
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
ram	Menge an RAM-Speicher (in MB), der für den Rubrik-Knoten reserviert ist
[cmdb_ci_rubrik_node_disk]	
node_name	Name des Rubrik-Knotens, dem der Datenträger zugeordnet ist
device_id	Datenträger-ID und Name des Rubrik-Knotens, miteinander verkettet im Format `ID@NODE_NAME`.
name	Name des Datenträgers, der dem Rubrik-Knoten zugeordnet ist Der Name enthält die Verkettung des Rubrik-Knotennamens, die ID des Datenträgers und den Typ des Datenträgers im Format `NODE_NAME@DISK_ID@DISK_TYPE`.
size_bytes	Größe der Gesamtkapazität in Byte
unallocated_size_bytes	Größe der gesamten nicht zugeteilten Kapazität in Byte
usable_size_bytes	Größe der verfügbaren Gesamtkapazität in Byte
storage_type	Typ des Speicherdatenträgers: SSD oder HDD
storage_path	Verzeichnispfad des Speicherdatenträgers
operational_status	Betriebsstatus des Speicherdatenträgers

Die Dependency Views-Zuordnung zeigt die erkannten Knoten und Knotendatenträger und deren Beziehungen untereinander.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

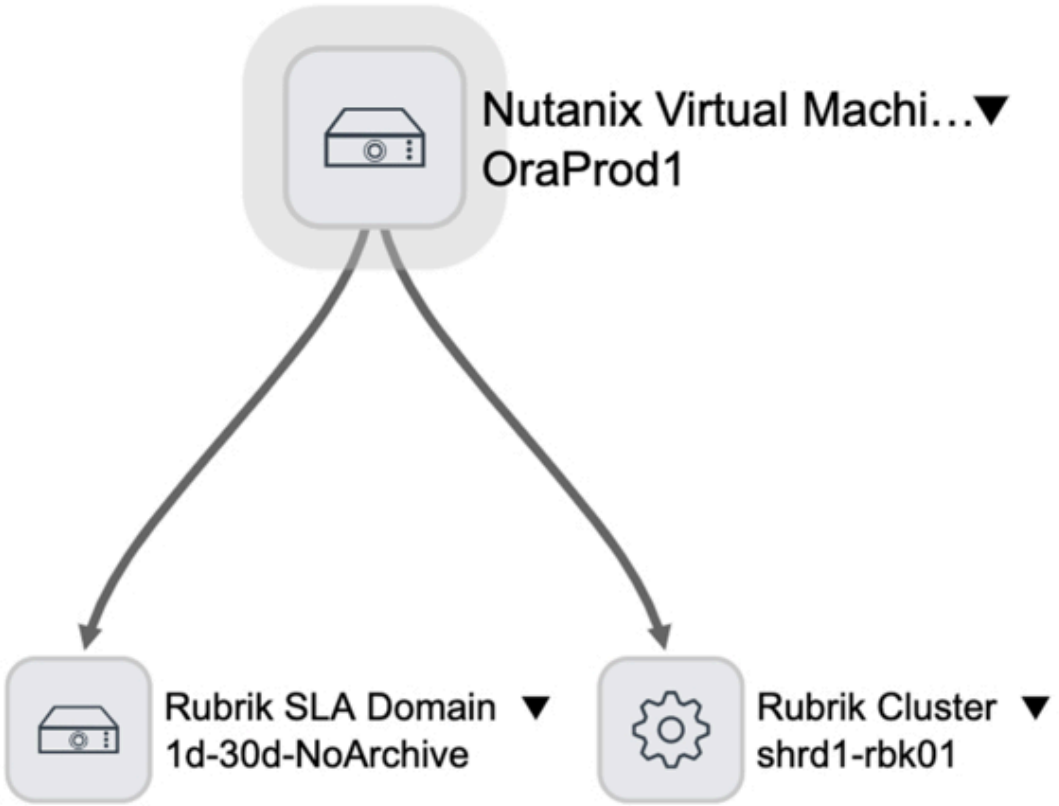


Ressourcen, die mithilfe des Musters „Rubrik Nutanix Instance (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Nutanix-Instanz [cmdb_ci_nutanix_vm_instance]	
object_id	ID der Nutanix VM-Instanz
vm_inst_id	ID der Nutanix VM-Instanz
name	Name der Nutanix VM-Instanz
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
vm_cluster_id	ID des Clusters, zu dem die Nutanix VM-Instanz gehört
vm_cluster_name	Name des Clusters, zu dem die Nutanix VM-Instanz gehört
os_type	Der auf der Nutanix VM-Instanz konfigurierte Betriebssystemtyp

Die Dependency Views-Zuordnung zeigt die erkannten Nutanix-Instanzen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



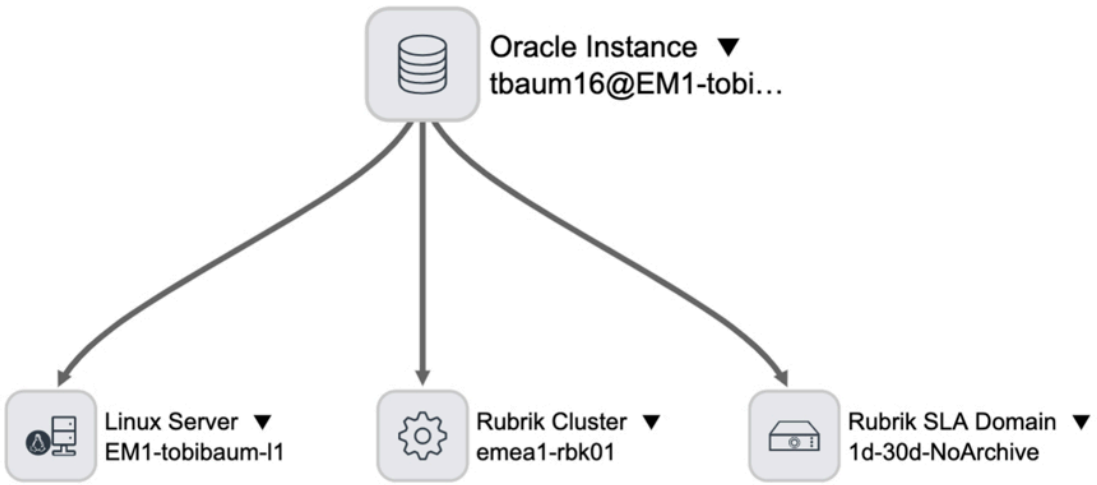
Ressourcen, die mithilfe des Musters „Rubrik Oracle DB (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Oracle-DB [cmdb_ci_db_ora_instance]	
sid	Oracle-System-ID der Datenbank
name	ID der Oracle-Datenbank im Rubrik-Kontext
database_name	Name der Oracle-Datenbank
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
rac_id	ID des Oracle RAC (Real Application Cluster), zu dem die Datenbank gehört
host_id	ID des Hosts, auf dem die Oracle-Datenbank ausgeführt wird
instance	ID der Oracle-Instanz, die die der Datenbank zugeordneten Daten verwaltet
Instance_count	Anzahl der Oracle-Instanzen, die die der Datenbank zugeordneten Daten verwalten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
last_snapshot	Letzter Snapshot der Oracle-Datenbank im Format JJ-MM-TT HH-MM-SS
missed_snapshot_count	Anzahl der verpassten Snapshots der Oracle-Datenbank
tablespaces_count	Anzahl der logischen Speichereinheiten, die der Oracle-Datenbank zugeordnet sind

Die Dependency Views-Zuordnung zeigt die erkannten Oracle-Datenbanken und deren Beziehungen untereinander.

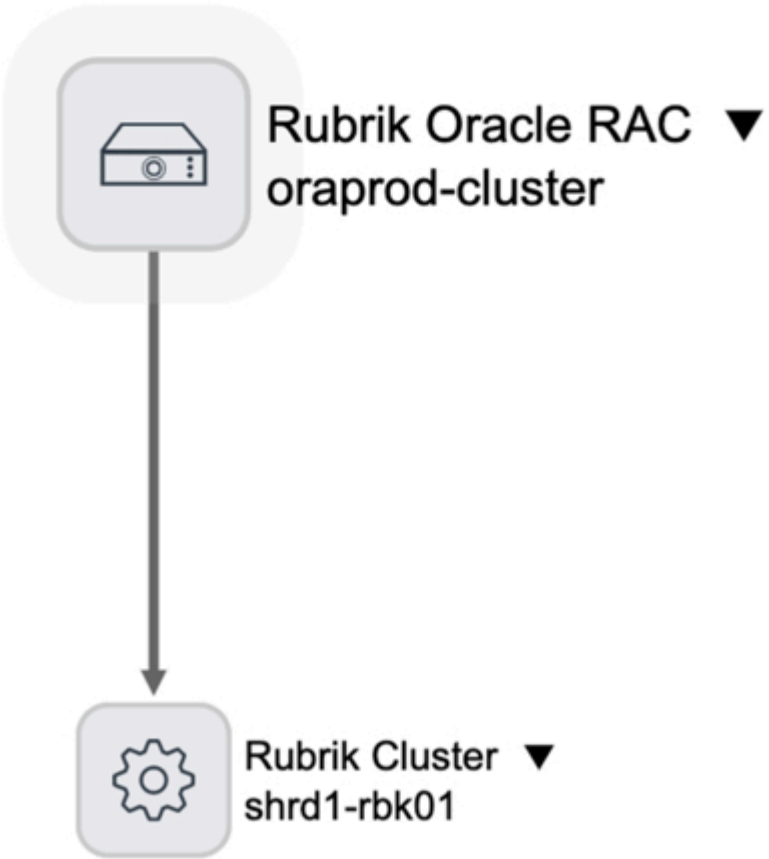


Ressourcen, die mithilfe des Musters „Rubrik Oracle RAC (Real Application Cluster) (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Oracle-RAC [cmdb_ci_rubrik_db_ora_rac]	
object_id	ID des Rubrik Oracle-RAC
name	Name des Rubrik Oracle-RAC
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
db_count	Anzahl der Datenbanken, die dem Rubrik Oracle-RAC zugeordnet sind
node_count	Anzahl der Knoten, die Teil des Rubrik Oracle-RAC sind
state	Status des Rubrik Oracle-RAC

Die Dependency Views-Zuordnung zeigt die erkannten Oracle-RACs und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

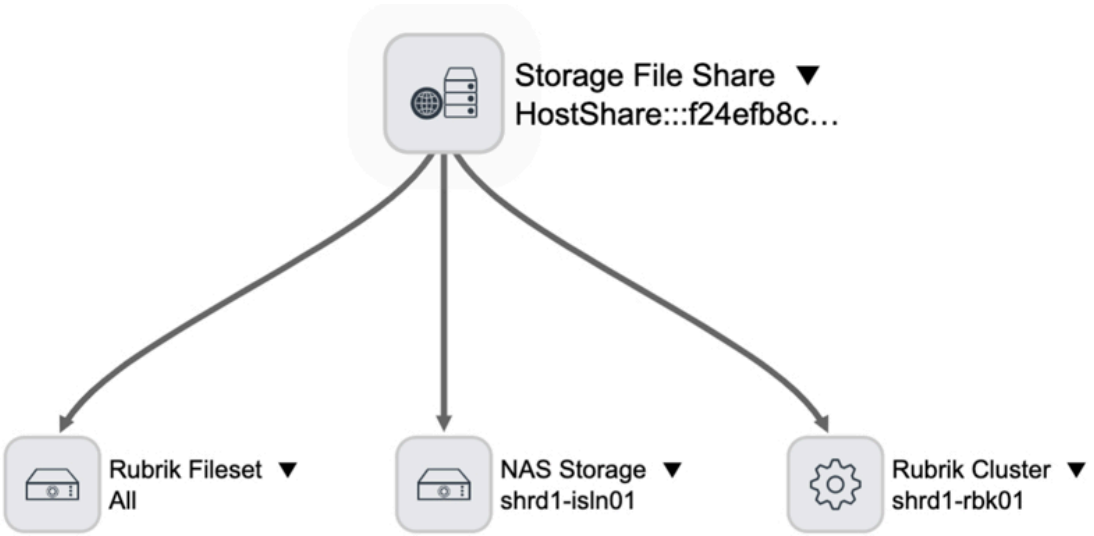


Ressourcen, die mithilfe des Musters „Rubrik Share (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Freigabe [cmdb_ci_storage_fileshare]	
name	ID der Hostfreigabe
Pfad	Exportpunkt der Hostfreigabe
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
host_id	ID des Hosts, dem die Hostfreigabe zugeordnet ist
share_type	Freigabetyp der Hostfreigabe
vendor_type	Typ des Anbieters der Hostfreigabe
Status	Aktueller Status der Hostfreigabe

Die Dependency Views-Zuordnung zeigt die erkannten Hostfreigaben und deren Beziehungen untereinander.

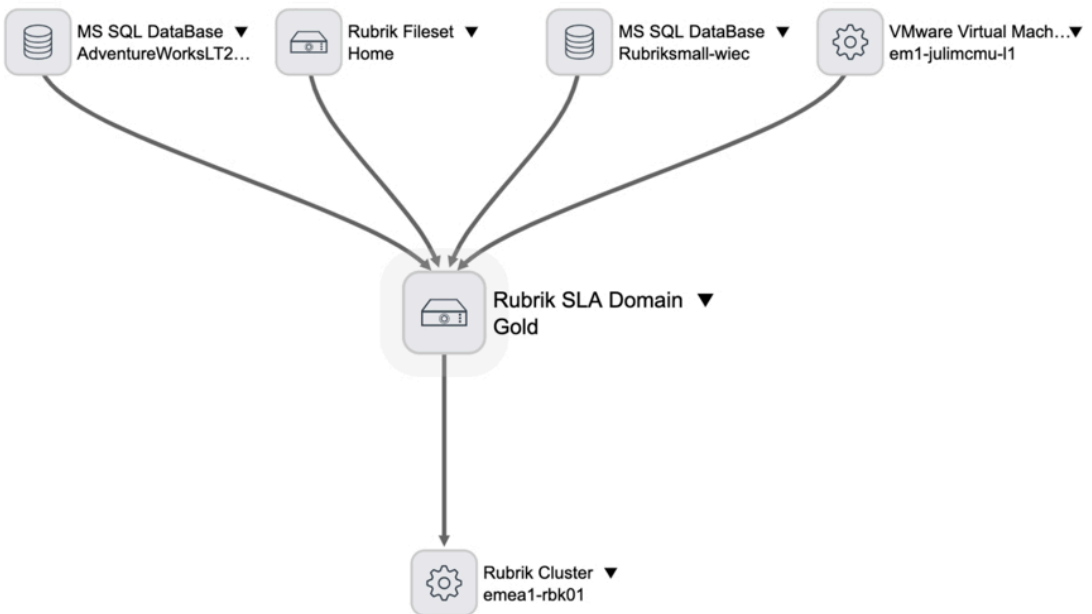
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ressourcen, die mithilfe des Musters „Rubrik SLA Domain (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-SLA-Domäne [cmdb_ci_rubrik_sla_domain]	
object_id	ID der Rubrik-SLA-Domänenrichtlinie
name	Name der Rubrik-SLA-Domänenrichtlinie
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
max_local_retention_limit	Maximale lokale Aufbewahrungsgrenze der SLA-Domänenrichtlinie

Die Dependency Views-Zuordnung zeigt die erkannten SLA-Domänen und deren Beziehungen untereinander.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen, die mithilfe des Musters „Rubrik Solaris Host (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Solaris-Host [cmdb_ci_solaris_server]	
name	Name des Hosts.
host_name	Hostname des Hosts.
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
os	Typ des auf dem Host konfigurierten Betriebssystems.
os_version	Version, Edition oder Distribution des auf dem Host konfigurierten Betriebssystems.
operational_status	Aktueller Betriebsstatus des Hosts.

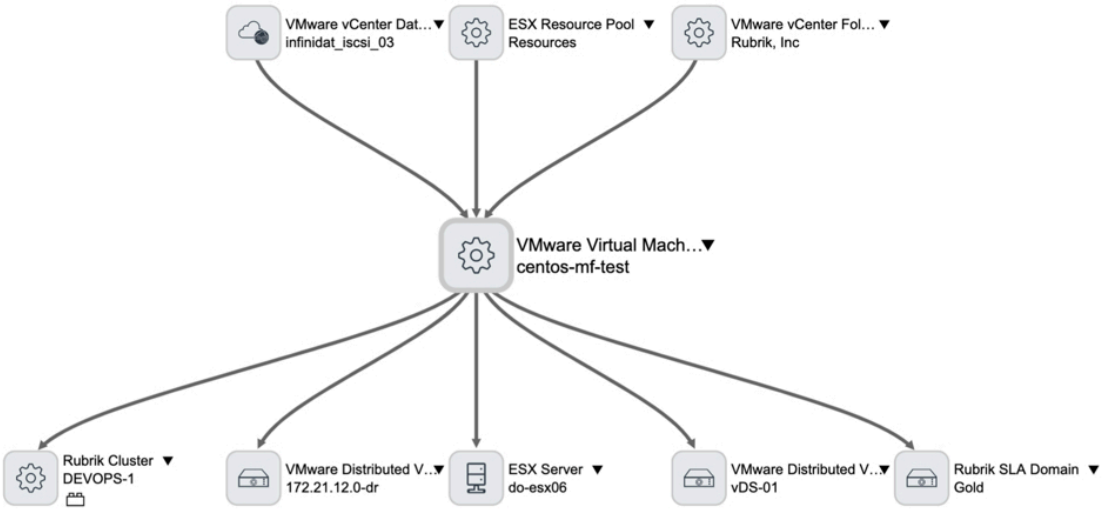
Ressourcen, die mithilfe des Musters „Rubrik VMware Instance (LP)“ erkannt wurden

Hinweis: Bei der Erkennung von VMware-Instanzen werden nur vorhandene CIs aktualisiert. Das liegt daran, dass bei der regulären vCenter-Erkennung die IRE (Identification and Reconciliation Engine) nicht verwendet wird und das Muster „Rubrik VMware“ Duplikate erzeugt. Wenn keine Übereinstimmung zwischen den Daten aus der REST API und der CMDB besteht, werden keine CIs aktualisiert. Darüber hinaus wird das Muster „Rubrik VMware Instance (LP)“ mit dem Status „Fehler“ abgeschlossen, wenn es keine Übereinstimmung gibt. Das ist das erwartete Verhalten.

Feld	Beschreibung
Rubrik VMware-Instanz [cmdb_ci_vmware_instance]	
object_id	ID der VMware-Instanz
name	Name der VMware-Instanz
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
host_id	ID des Rubrik VMware-Hosts
host_name	Name des Rubrik VMware-Hosts
vm_cluster_name	Name des Clusters, zu dem die VM-Instanz gehört
ip_address	IP-Adresse der VMware-Instanz, falls zugewiesen
guest_os_fullname	Typ des Gastbetriebssystems
state	Status der VMware-Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Dependency Views-Zuordnung zeigt die erkannten VMware-Instanzen und deren Beziehungen untereinander.

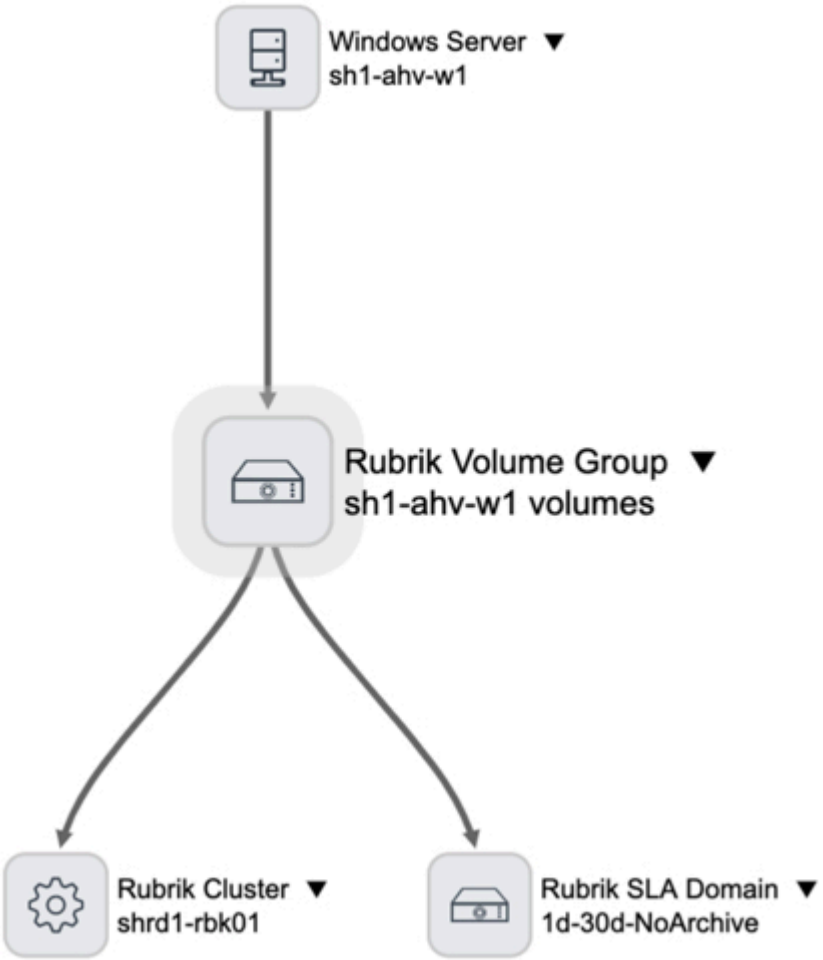


Ressourcen, die mithilfe des Musters „Rubrik Volume Group (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik-Volumegruppe [cmdb_ci_rubrik_volume_group]	
object_id	ID der Volumegruppe
volume_id	Volume-ID der Volumegruppe
name	Name der Volumegruppe
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
effective_sla_domain	ID der Rubrik-SLA-Domäne
effective_sla_domain_name	Name der Rubrik-SLA-Domäne Siehe auch: [cmdb_ci_rubrik_sla_domain]
host_id	ID des Hosts, dem die Volumegruppe zugeordnet ist

Die Dependency Views-Zuordnung zeigt die erkannten Volumegruppen und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

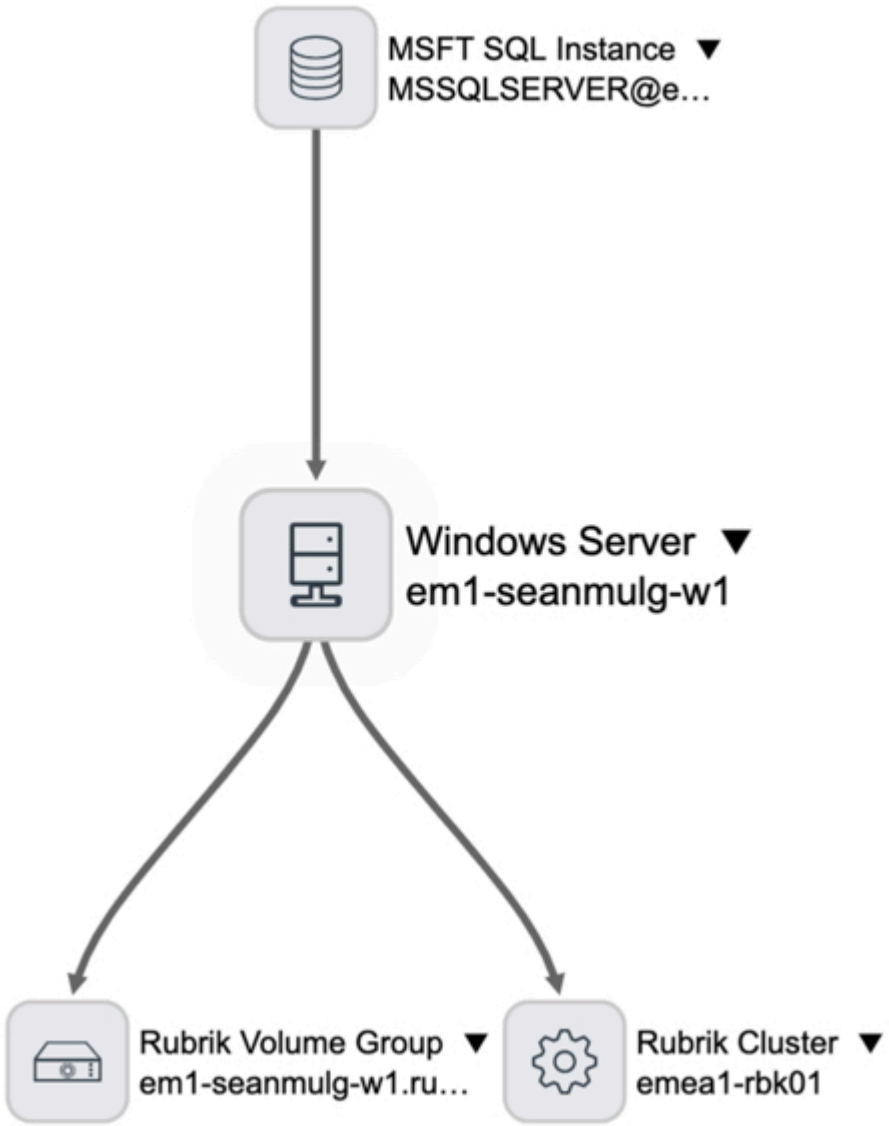


Ressourcen, die mithilfe des Musters „Rubrik Windows Host (LP)“ erkannt wurden

Feld	Beschreibung
Rubrik Windows-Host [cmdb_ci_win_server]	
name	Name des Hosts.
host_name	Hostname des Hosts.
cluster_id	ID des Rubrik-Clusters
cluster_name	Name des Rubrik-Clusters Siehe auch: [cmdb_ci_rubrik_cluster]
os	Typ des auf dem Host konfigurierten Betriebssystems.
os_version	Version, Edition oder Distribution des auf dem Host konfigurierten Betriebssystems.
operational_status	Aktueller Betriebsstatus des Hosts.

Die Dependency Views-Zuordnung zeigt die erkannten Hosts und deren Beziehungen untereinander.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CI-Beziehungen

Ressourcen, die mithilfe des Musters „Rubrik AIX Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_aix_server	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik EC2 Instance (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_vm_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_rubrik_vm_instance	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain

Ressourcen, die mithilfe des Musters „Rubrik Fileset (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_server	Eigentümer von::Eigentum von	cmdb_ci_rubrik_fileset
cmdb_ci_storage_fileshare	Eigentümer von::Eigentum von	cmdb_ci_rubrik_fileset
cmdb_ci_rubrik_fileset_template	Definiert Ressourcen für::Erhält Ressourcen von	cmdb_ci_rubrik_fileset
cmdb_ci_rubrik_fileset	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_rubrik_fileset	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain
cmdb_ci_nas_storage	Eigentümer von::Eigentum von	cmdb_ci_rubrik_fileset

Ressourcen, die mithilfe des Musters „Rubrik Fileset Template (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_fileset_template	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik Hyper-V Instance (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_hyper_v_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_hyper_v_instance	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain

Ressourcen, die mithilfe des Musters „Rubrik Linux Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_linux_server	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik Managed Volume (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_storage_volume	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_storage_volume	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain

Ressourcen, die mithilfe des Musters „Rubrik MS SQL DB (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_db_mssql_database	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_db_mssql_database	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain
cmdb_ci_db_mssql_instance	Enthält::Enthalten in	cmdb_ci_db_mssql_database

Ressourcen, die mithilfe des Musters „Rubrik MS SQL Instance (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_db_mssql_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_db_mssql_instance	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_server

Ressourcen, die mithilfe des Musters „Rubrik NAS Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_nas_storage	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik Node (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_node	Cluster von::Cluster	cmdb_ci_rubrik_cluster
cmdb_ci_rubrik_node	Verwendet::Verwendet von	cmdb_ci_rubrik_node_disk

Ressourcen, die mithilfe des Musters „Rubrik Nutanix Instance (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_nutanix_vm_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_nutanix_vm_instance	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain

Ressourcen, die mithilfe des Musters „Rubrik Oracle DB (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_db_ora_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_db_ora_instance	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain
cmdb_ci_db_ora_instance	Wird ausgeführt auf::Wird ausgeführt	cmdb_ci_server
cmdb_ci_db_ora_instance	Cluster von::Cluster	cmdb_ci_rubrik_db_ora_rac

Ressourcen, die mithilfe des Musters „Rubrik Oracle RAC (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_db_ora_rac	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik Share (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_storage_fileshare	Verwaltet von::Verwaltet	cmdb_ci_nas_storage
cmdb_ci_storage_fileshare	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik SLA Domain (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_rubrik_sla_domain	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik Solaris Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_solaris_server	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Ressourcen, die mithilfe des Musters „Rubrik VMware Instance (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_vmware_instance	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_vmware_instance	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain

Ressourcen, die mithilfe des Musters „Rubrik Volume Group (LP)“ erkannt wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
cmdb_ci_rubrik_volume_group	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster
cmdb_ci_rubrik_volume_group	Geschützt durch::Schützt	cmdb_ci_rubrik_sla_domain
cmdb_ci_server	Eigentümer von::Eigentum von	cmdb_ci_rubrik_volume_group

Ressourcen, die mithilfe des Musters „Rubrik Windows Host (LP)“ erkannt wurden

CI	Beziehung	CI
cmdb_ci_win_server	Verwaltet von::Verwaltet	cmdb_ci_rubrik_cluster

Erkennung von Veritas Cluster Server

Die Anwendung ServiceNow Discovery verwendet das Muster „Unix-Cluster – VERITAS Cluster“, um Veritas Cluster Server-Komponenten zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Sie können dieses Muster auf der Now Platform mithilfe von Kingston Patch 8, London oder Madrid verwenden.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

SSH-Anmeldeinformationen

Konfigurieren Sie auf Now Platform® die SSH-Anmeldeinformationen für einen Benutzer mit erhöhten Rechten für die Ausführung des Befehls *`cat`*. Weitere Informationen zu Befehlen finden Sie im Abschnitt zu Service-Mapping-Befehlen, die einen privilegierten Benutzer erfordern, in der Service-Mapping-Dokumentation.

Berechtigungen zum Lesen der Veritas Cluster Server-Konfigurationsdatei

Erteilen Sie dem Unix-Betriebssystembenutzer die Berechtigungen zum Lesen der folgenden Konfigurationsdatei: `/etc/VRTSvcs/conf/config/main.cf`.

Berechtigungen zum Ausführen von Veritas Cluster-Befehlen

Geben Sie dem Unix-Betriebssystembenutzer Berechtigungen, die folgenden Befehle gegen den Veritas Cluster-Server auszuführen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Parameter	Obligatorisch/ Optional	Beschreibung
“privilege user” + cat /etc/VRTSvcs/ conf/config/ main.cf	-	Obligatorisch	Liest die Veritas Cluster Server-Konfigurationsdatei
“privilege user” + /opt/VRTSvcs/ bin/haclus -value ClusterUUID 2>/dev/null	-	Obligatorisch	Ruft die Veritas Cluster Server-Cluster-UUID ab
“privilege user” + /opt/VRTSvcs/ bin/haclus -value ClusterName 2>/dev/null	-	Obligatorisch	Ruft den Veritas Cluster Server-Clusternamen ab
“privilege user” + /opt/VRTSvcs/ bin/haclus -value EngineVersion	-	Obligatorisch	Ruft die Veritas Cluster Server-Clusterversion ab
“privilege user” + /opt/VRTSvcs/ bin/haclus -value ClusterAddress	-	Obligatorisch	Ruft die Veritas Cluster Server-Clusteradresse ab
“privilege user” + /opt/VRTSvcs/ bin/haclus -value ClusState	-	Obligatorisch	Ruft den Veritas Cluster Server-Clusterstatus ab
“privilege user” + / opt/VRTSvcs/bin/ hasys -state	-	Obligatorisch	Ruft die Veritas Cluster Server-Clusterknoten ab
“privilege user” + / opt/VRTSvcs/bin/ hares -state	-	Obligatorisch	Ruft die Cluster-Ressourcen des Veritas Cluster Servers ab
“privilege user” + /opt/VRTSvcs/ bin/hares -display |grep -w 'Type' |grep 'global' 2>/dev/null	-	Obligatorisch	Ruft den Cluster-Ressourcentyp des Veritas Cluster Servers ab.
“privilege user” + /opt/VRTSvcs/ bin/hares -display | grep Group 2>/dev/null	-	Obligatorisch	Ruft die Cluster-Ressourcengruppe des Veritas Cluster Servers ab
“privilege user” + /opt/VRTSvcs/	-	Obligatorisch	Ruft den Ressourcengruppennamen und Status des

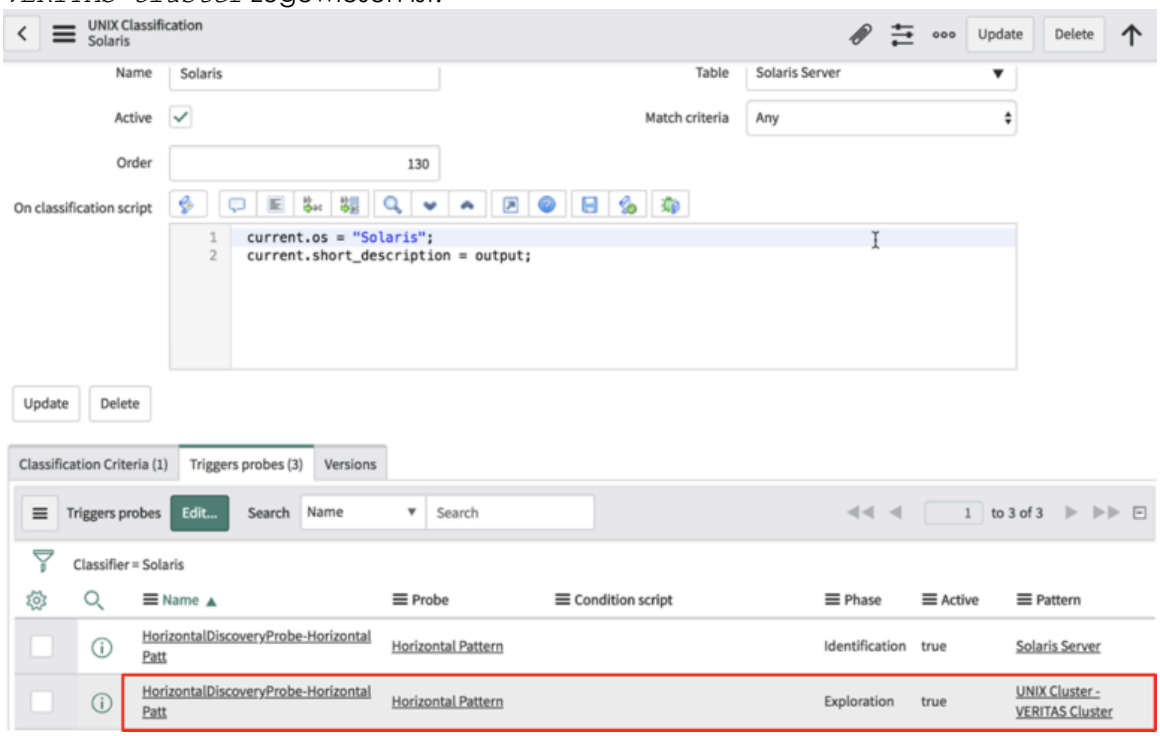
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehl	Parameter	Obligatorisch/ Optional	Beschreibung
bin/hagrp -state 2>/dev/null			Veritas Cluster Servers ab

Klassifizierungs-Probe zum Auslösen des Musters „UNIX-Cluster – VERITAS Cluster“

So überprüfen Sie, ob die Klassifizierungs-Probe zum Auslösen des Musters „UNIX-Cluster – VERITAS Cluster“ festgelegt ist:

1. Navigieren zu **Discovery-Definition** > **CI-Klassifizierung** > **CI-Klassifizierung** > **UNIX**.
2. Klicken Sie in der Liste **UNIX-Klassifizierung** auf **Solaris** oder **Linux**.
3. Überprüfen Sie auf der Registerkarte **Auslösertests**, ob die Probe *HorizontalDiscoveryProbe-HorizontalPatt* dem Muster *UNIX Cluster – VERITAS Cluster* zugewiesen ist.



Hinweis: Im Discovery-Protokoll wird der Fehler für den Schritt der Betriebssystemerkennung selbst dann angezeigt, wenn die Erkennung erfolgreich verläuft.

Systemeigenschaft für die neue Hostklasse

Fügen Sie eine Systemeigenschaft [sys_property] *sa.host_classes* hinzu, und legen Sie den Wert auf cmdb_ci_unix_cluster fest. Das Erstellen einer neuen Hostklasse für Veritas Cluster-Server hilft bei der korrekten Identifizierung dieses Hosttyps.

Einschränkungen

Sie können das Muster „Unix-Cluster – VERITAS Cluster“ im Debug-Modus im Musterdesigner nicht anpassen.

Automatische Übersetzung

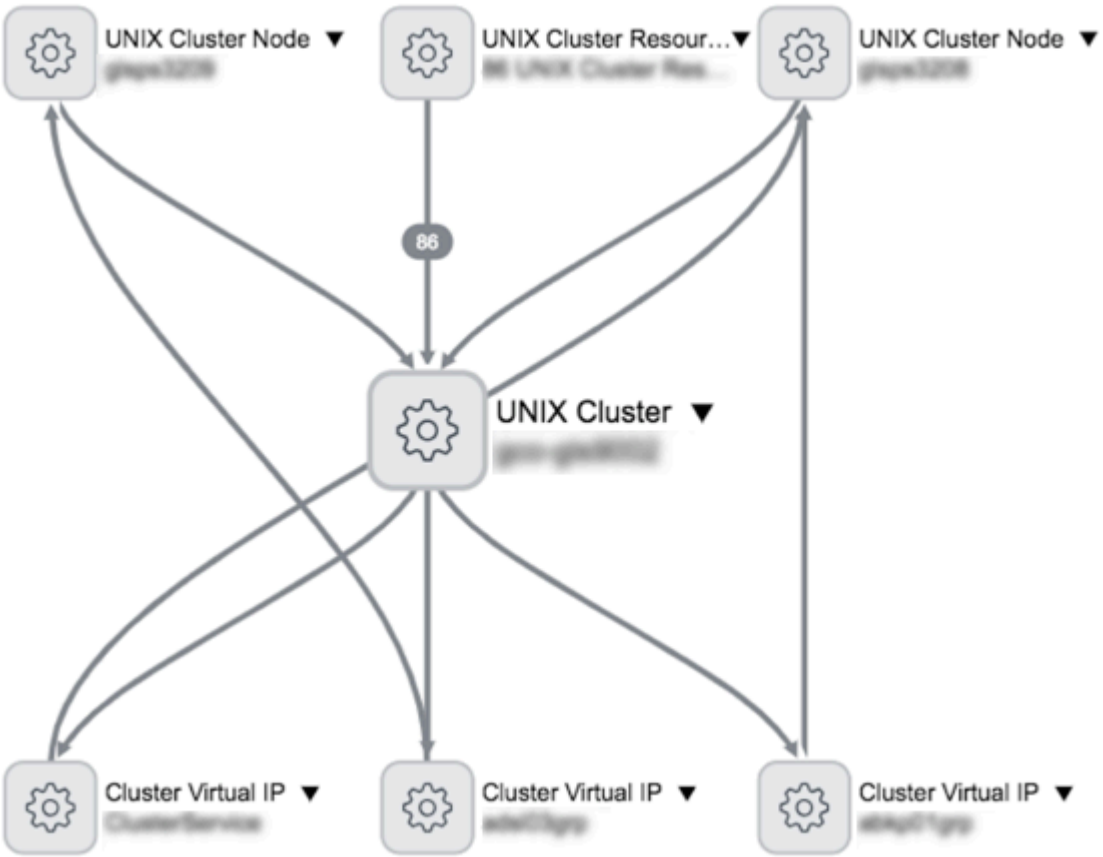
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Discovery während der horizontalen Erkennung erfasste Daten

Tabelle und Feld	Beschreibung
Unix-Cluster [cmdb_ci_unix_cluster]	Die Attribute des Unix-Clusters
IP-Adresse [ip_address]	
Clustertyp [cluster_type]	
Name [name]	
Clusterversion [cluster_version]	
Clusterstatus [cluster_status]	
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Die Attribute des Unix-Clusterknotens
Name [name]	
Cluster [cluster]	
Server [Server]	
Knotenstatus [node_status]	
IP-Adresse [ip_address]	
UNIX Cluster-Ressourcengruppe [cmdb_ci_unix_cluster_resource_group]	Die Attribute der UNIX-Cluster-Ressourcengruppe
Name [name]	
Knoten [node]	
Server [Server]	
Cluster [cluster]	
Ressourcengruppenstatus [resource_group_status]	
UNIX-Clusterressource [cmdb_ci_unix_cluster_resource]	Die Attribute der UNIX-Cluster-Ressource
Ressourcentyp [resource_type]	
Name [name]	
Ressourcenstatus [resource_status]	
Virtuelle Cluster-IPs [cmdb_ci_cluster_vip]	Die Attribute der Cluster virtuellen IP-Adressen
IP-Adresse [ip_address]	
Name [name]	
Cluster [cluster]	
Clusterstatus [cluster_status]	
Knoten [node]	

Die Grafik stellt CIs dar, die Teil der Veritas Cluster Server-Erkennung sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



CI-Beziehungen

Das Muster „Unix Cluster – VERITAS Cluster“ erstellt die folgenden CI-Beziehungen:

CI	Beziehung	CI
Unix-Cluster [cmdb_ci_unix_cluster]	Hostet: Gehostet auf	Linux-Server [cmdb_ci_linux_server]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Hostet: Gehostet auf	Linux-Server [cmdb_ci_linux_server]
Virtuelle Cluster-IPs [cmdb_ci_cluster_vip]	Virtualisiert von: Virtualisiert	Unix-Cluster [cmdb_ci_unix_cluster]
Virtuelle Cluster-IPs [cmdb_ci_cluster_vip]	Verwendet: Verwendet von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Unix-Clusterknoten [cmdb_ci_unix_cluster_node]	Cluster von: Cluster	Unix-Cluster [cmdb_ci_unix_cluster]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für: Erhält Ressourcen von	Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Unix-Clusterressource [cmdb_ci_unix_cluster_resource]	Definiert Ressourcen für: Erhält Ressourcen von	Das Clusterfeld auf [cmdb_ci_unix_cluster]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Unix Cluster-Ressourcengruppe [cmdb_ci_unix_cluster_cresource_group]	Enthält:Enthalten von	Das Clusterfeld auf UNIX-Cluster [cmdb_ci_unix_cluster]
Unix Cluster-Ressourcengruppe [cmdb_ci_unix_cluster_cresource_group]	Enthält:Enthalten von	Das Knotenfeld auf Unix-Clusterknoten [cmdb_ci_unix_cluster_node]
Unix Cluster-Ressourcengruppe [cmdb_ci_unix_cluster_cresource_group]	Enthält:Enthalten von	Unix-Clusterressource [cmdb_ci_unix_cluster_resource]

VMware NSX Erweiterte Erkennung des Lastenausgleichsmoduls

Die Anwendung ServiceNow Discovery verwendet das Discovery-Muster für das Lastenausgleichsmodul „VMware NSX Advanced“, um das Lastenausgleichsmodul VMware NSX zu finden. Um einige dieser Ressourcen zu erkennen, müssen Sie die Anwendung Muster für Discovery und Service-Mapping aus dem ServiceNow Storeaktualisieren.

Das -Muster verwendet eine Reihe von REST APIs, um die Lastenausgleichsmodule zu finden. Sie wird von der HTTP-Klassifizierung NSX ausgelöst, die auf die Probe **„HTTP – Klassifizieren“** antwortet. Weitere Informationen finden Sie unter Erkennung von HTTP-Geräten.

Hinweis: Es sind zwei Muster verfügbar. Das veraltete Muster „VMware NSX Load Balancer“ gilt für die S-Serie. Das neue Muster „VMware NSX-T Load Balancer“ ist für die T-Serie. Die Funktionalität und die erfassten Informationen bleiben unverändert.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Voraussetzungen

Aktivieren Sie die Standardauthentifizierung für NSX .

Aktivieren Sie in VMware NSXdie Standardauthentifizierung für NSX.

Vergewissern Sie sich, dass die Anwendungen aktuell sind

- CMDB CI-Klassenmodelle
- Visibility Content
- Muster für Discovery und Service-Mapping

Konfigurieren Sie die Anmeldeinformationen für die Standardauthentifizierung

Konfigurieren Sie unter Now Platformdie Anmeldeinformationen für die Standardauthentifizierung. Die Anmeldeinformationen müssen die folgenden API-Berechtigungen aufweisen:

- NSX:
  - /api/4.0/edges
  - /api/4.0/edges/<edge_id>loadbalancer/config
- NSX-T: /api/v1/edge-cluster

Weitere Informationen zu den Anmeldeinformationen für die Standardauthentifizierung finden Sie unter Virtual Server Interface .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass die HTTP-Discovery für die Hauptcontroller-IP NSX ausgelöst wird

Die HTTP-Discovery wird nur ausgelöst, wenn die SSH- oder SNMP-Discovery nicht erfolgreich ist.

Erkennungszeitpläne erstellen

Erstellen Sie den Discovery-Zeitplan für die Discovery des Lastenausgleichsmoduls VMware NSX, oder führen Sie eine Schnell-Discovery für die IP-Adresse des Hauptcontrollers NSX aus. Weitere Informationen zum Ausführen einer Schnell-Discovery finden Sie unter Schnell-Discovery ausführen.

Von Discovery für VMware NSX Advanced Load Balancer gesammelte Daten

Discovery füllt die Daten in CMDB bei der Ausführung der Muster für erweiterte Lastenausgleichsmodule von VMware NSX.

NSX-Lastenausgleichsmodul [cmdb_ci_nsx_lb]

Feld	Beschreibung
Name [name]	Edge-Name
Objekt-ID [object_id]	Edge-ID
IP-Adresse [ip_address]	IP-Adresse des NSX -Hauptcontrollers.
Betriebsstatus [operational_status]	Lastenausgleichsmodulstatus: aktiv oder inaktiv

Load Balancer-Service [cmdb_ci_lb_service]

Feld	Beschreibung
Name [name]	Name des virtuellen Servers
IP-Adresse [ip_address]	IP-Adresse des virtuellen Servers
Objekt-ID [object_id]	Objekt-ID des virtuellen Servers
Port [port]	Virtueller Serverport, mit dem kommuniziert werden soll
Listenerprotokoll [listener_protocol]	Listenerprotokoll. Beispiel: HTTP, HTTPS

Load Balancer-Pool [cmdb_ci_lb_pool]

Feld	Beschreibung
Name [name]	Poolname.
Objekt-ID [object_id]	Poolobjekt-ID

Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]

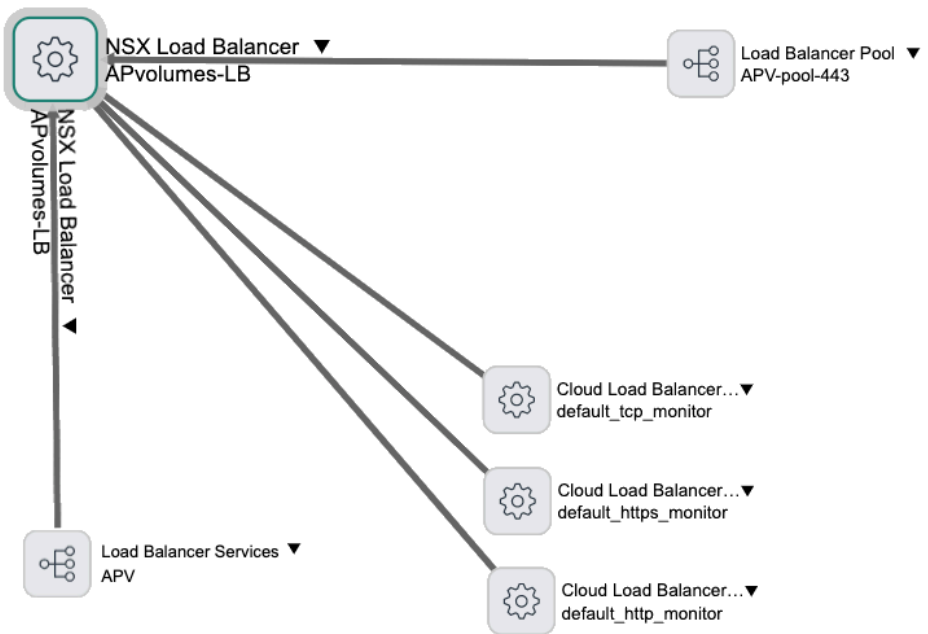
Feld	Beschreibung
Name [name]	Poolmitgliedsname
IP-Adresse [ip_address]	Poolmitglieds-IP-Adresse
Objekt-ID [object_id]	Poolmitgliedsobjekt-ID
Serviceport [service_port]	Poolserverport, mit dem kommuniziert werden soll

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integritätsservice für Cloud-Lastenausgleichsmodul [cmdb_ci_lb_health_service]

Feld	Beschreibung
Name [name]	Name des Monitors
Objekt-ID [object_id]	Objekt-ID des Monitors
Zeitüberschreitung in Sekunden [timeout_sec]	Zeit in Sekunden, die auf eine Antwort gewartet wird
Intervall in Sekunden [check_interval_sec]	Intervall in Sekunden, nach dem der Monitor die Anforderung erneut sendet
Überwachungstypprotokoll [monitor_type]	Monitortyp. Beispiel: HTTP, HTTPS, TCP
Anforderungspfad [request_path]	Pfad, an den der Monitor die Anforderung sendet
Max. Wiederholungen [max_retries]	Die maximale Häufigkeit, mit der die Ressource getestet wird, bevor sie als „inaktiv“ deklariert wird.

Die Dependency Views-Zuordnung zeigt alle erkannten Lastenausgleichsmodul-CIs und ihre Beziehungen untereinander.



CI-Beziehungen

Discovery erstellt diese Beziehungen, um die Erkennung des Lastenausgleichsmoduls VMware NSX zu unterstützen.

CI	Beziehung	CI
Load Balancer-Service [cmdb_ci_lb_service]	Wird ausgeführt auf::Wird ausgeführt	NSX-Lastenausgleichsmodul [cmdb_ci_nsx_lb]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI	Beziehung	CI
Load Balancer-Service [cmdb_ci_lb_service]	Verwendet::Verwendet von	Load Balancer-Pool [cmdb_ci_lb_pool]
Load Balancer-Pool [cmdb_ci_lb_pool]	Gehostet auf::Hostet	NSX-Lastenausgleichsmodul [cmdb_ci_nsx_lb]
Load Balancer-Pool [cmdb_ci_lb_pool]	Eigentümer von::Eigentum von	Load Balancer Pool-Mitglied [cmdb_ci_lb_pool_member]
Integritätsservice für Cloud-Lastenausgleichsmodul [cmdb_ci_lb_health_service]	Gehostet auf::Hostet	NSX-Lastenausgleichsmodul [cmdb_ci_nsx_lb]
Integritätsservice für Cloud-Lastenausgleichsmodul [cmdb_ci_lb_health_service]	Verwendet von::Verwendet	Load Balancer-Pool [cmdb_ci_lb_pool]

Problembehandlung

Wenn der Zuordnungsprozess nicht so verläuft, wie Sie es erwartet haben, sollten Sie den folgenden Vorschlägen folgen.

Symptom	Ursache	Lösung
Discovery fehlgeschlagen. Die Discovery-Nachricht enthält die Informationen zu einem Fehler, der durch die REST-Zeitüberschreitung verursacht wurde.	Es gibt viele CIs, deren REST-Aufrufantwort in der Bereitstellung gesendet wird. Der MID-Server kann die REST-Aufrufantwort nicht verarbeiten, ohne dass die vom Parameter *mid.sa.cloud.request_timeout* gesteuerte Zeitbegrenzung überschritten wird.	Standardmäßig ist der Parameter *mid.sa.cloud.request_timeout* auf 30.000 Millisekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem entsprechenden MID-Server, und führen Sie die Discovery erneut aus. **Hinweis:** Wenn dieser Parameter in der zugehörigen Liste der **Konfigurationsparameter** für den betreffenden MID-Server nicht angezeigt wird, müssen Sie ihn möglicherweise hinzufügen.
Bei Musterdesigner tritt während einer Debug-Sitzung ein Fehler auf. Die Musterdesigner-Meldung enthält die Informationen zu einem Fehler, der durch eine Zeitüberschreitung verursacht wurde.	Beim Musterdesigner tritt ein Fehler aufgrund einer Zeitüberschreitung beim Muster-Debugging auf (und nicht während der Discovery).	Standardmäßig ist der Parameter *sa.debugger.max_timeout* auf 240 Sekunden festgelegt. Erhöhen Sie den Wert dieses Parameters auf dem betreffenden MID-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Musterdesigner und zugehörige Anwendungen konfigurieren

Installieren Sie die neuesten verfügbaren Versionen der ServiceNow-Anwendungen, um die neuesten Discovery-Muster zu verwenden.

Von der Anwendung Musterdesigner (com.snc.pattern.designer) wird die Benutzeroberfläche zum Erstellen oder Anpassen von Discovery-Mustern bereitgestellt. Musterdesigner wird automatisch mit Discovery oder Service-Mapping installiert. Die Muster selbst werden mit dedizierten Musteranwendungen veröffentlicht.

Ab Tokyo gibt ServiceNow alle Discovery-Muster mit den folgenden Anwendungen frei:

Muster für Discovery und Service-Mapping (sn_itom_pattern)

Diese Anwendung stellt die neuesten Versionen von Discovery-Mustern bereit, deren ursprüngliche Version ServiceNow im ServiceNow Store veröffentlichte.

Visibility Content (sn_pattern_design)

Diese Anwendung stellt die aktualisierte Version der Muster bereit, die bis Tokyo Teil der Familien-Releases waren.

Sie können die neuesten verfügbaren Versionen der Musteranwendungen aus dem ServiceNow Store installieren. Alternativ können Sie diese Anwendungen als Plugins auf Ihrer Instanz von ServiceNow installieren.

Plugins auf darin enthaltene erforderliche Muster überprüfen

Da ServiceNow Discovery-Muster mithilfe von zwei verschiedenen Plugins veröffentlicht, müssen Sie möglicherweise überprüfen, welches Plugin installiert oder aktualisiert werden soll.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

Ab Tokyo gibt ServiceNow alle Discovery-Muster mit den folgenden Anwendungen frei:

Muster für Discovery und Service-Mapping (sn_itom_pattern)

Diese Anwendung stellt die neuesten Versionen von Discovery-Mustern bereit, deren ursprüngliche Version ServiceNow im ServiceNow Store veröffentlichte.

Visibility Content (sn_pattern_design)

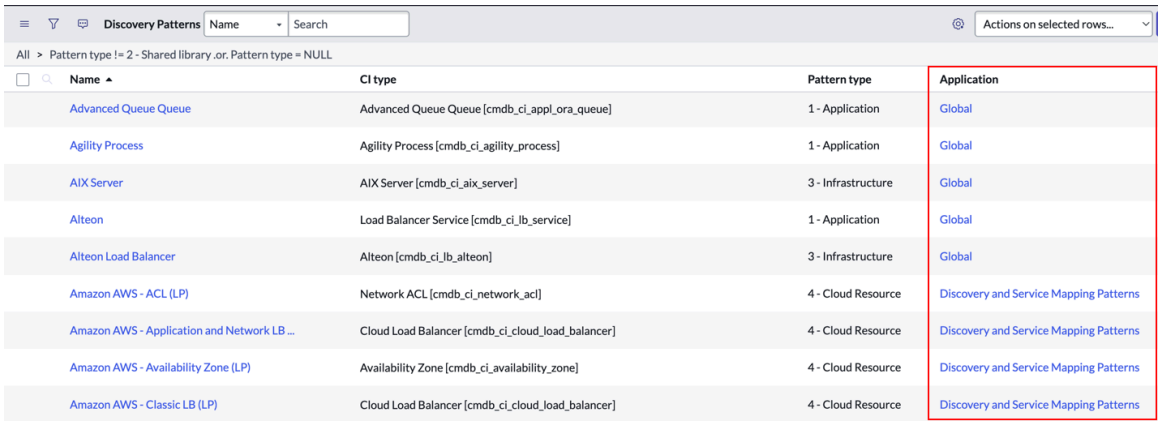
Diese Anwendung stellt die aktualisierte Version der Muster bereit, die bis Tokyo Teil der Familien-Releases waren.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**.
2. Zeigen Sie die Spalte **Anwendung** an.
   a. Klicken Sie auf **Liste personalisieren**.
   b. Wählen Sie im Dialogfeld „Listenspalten personalisieren“ unter **Verfügbar** die Option **Anwendung** aus, und klicken Sie auf den Rechtspfeil.
3. Wahlweise: Sie können gemeinsam genutzte Bibliotheken herausfiltern, um nur Muster in der Liste anzuzeigen.
4. Suchen Sie in der Liste nach dem entsprechenden Muster.
5. Überprüfen Sie, zu welcher Anwendung das Muster gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Global steht für Visibility Content.



Name	CI type	Pattern type	Application
Advanced Queue Queue	Advanced Queue Queue [cmdb_ci_appl_ora_queue]	1 - Application	Global
Agility Process	Agility Process [cmdb_ci_agility_process]	1 - Application	Global
AIX Server	AIX Server [cmdb_ci_aix_server]	3 - Infrastructure	Global
Alteon	Load Balancer Service [cmdb_ci_lb_service]	1 - Application	Global
Alteon Load Balancer	Alteon [cmdb_ci_lb_alteon]	3 - Infrastructure	Global
Amazon AWS - ACL (LP)	Network ACL [cmdb_ci_network_acl]	4 - Cloud Resource	Discovery and Service Mapping Patterns
Amazon AWS - Application and Network LB ...	Cloud Load Balancer [cmdb_ci_cloud_load_balancer]	4 - Cloud Resource	Discovery and Service Mapping Patterns
Amazon AWS - Availability Zone (LP)	Availability Zone [cmdb_ci_availability_zone]	4 - Cloud Resource	Discovery and Service Mapping Patterns
Amazon AWS - Classic LB (LP)	Cloud Load Balancer [cmdb_ci_cloud_load_balancer]	4 - Cloud Resource	Discovery and Service Mapping Patterns

Muster für Discovery und Service-Mapping installieren

Sie können die Anwendung Muster für Discovery und Service-Mapping (sn_itom_pattern) installieren, wenn Sie über die Administratorrolle verfügen.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfen Sie den Eintrag der Anwendung Discovery and Service Mapping Patterns im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

Erforderliche Rolle: admin

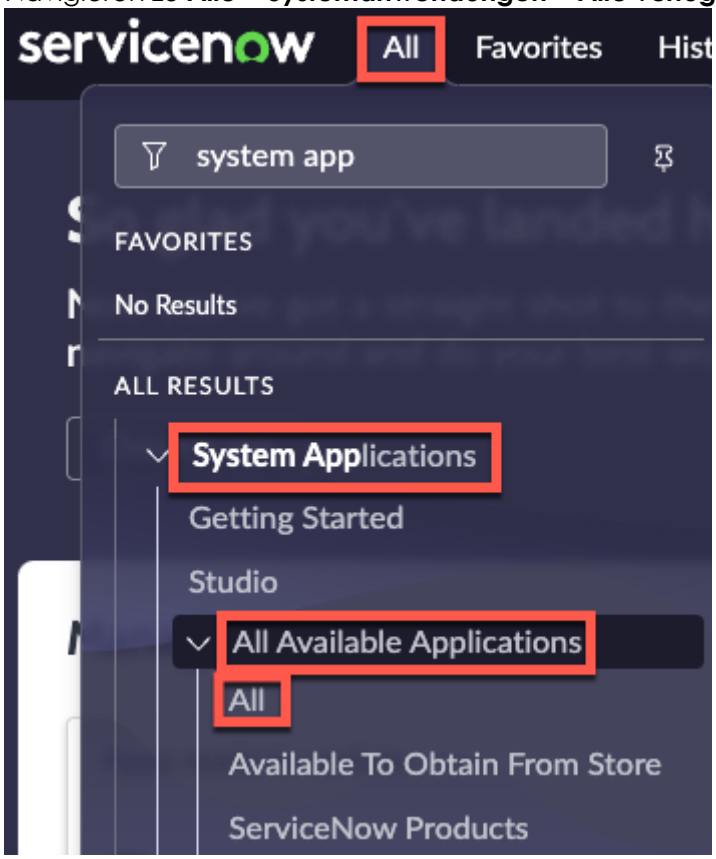
Warum und wann dieser Vorgang ausgeführt wird

Mit Muster für Discovery und Service-Mapping werden mehrere Tabellen installiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie über die Filterkriterien und die Suchleiste nach der Anwendung Muster für Discovery und Service-Mapping (sn_itom_pattern).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Visibility Content installieren

Sie können die Anwendung Visibility Content (sn_pattern_design) installieren, wenn Sie über die Administratorrolle verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfen Sie den Eintrag der Anwendung Visibility Content im ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Release-Kompatibilität.

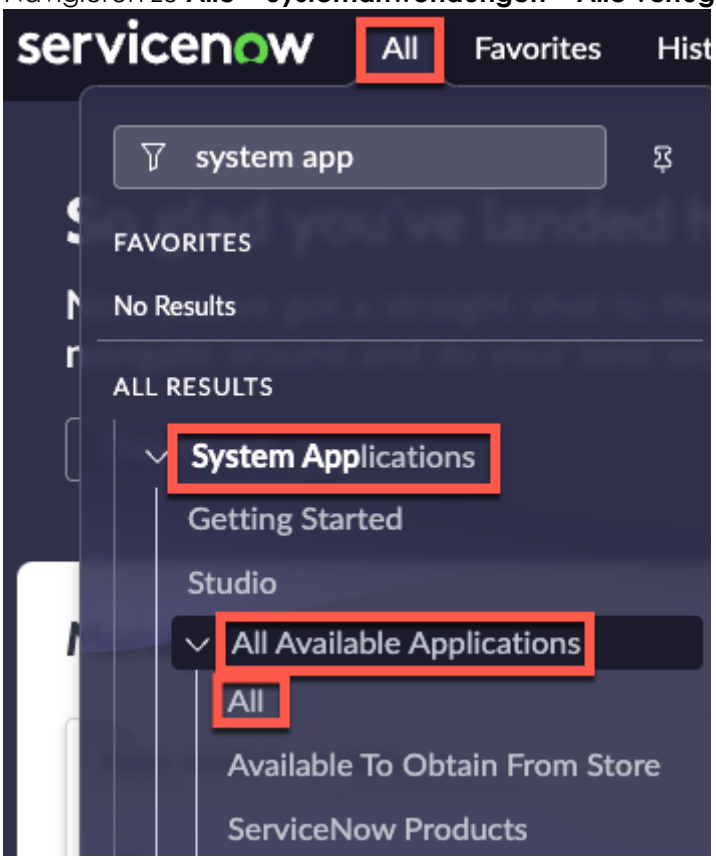
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Mit Visibility Content werden mehrere Tabellen installiert.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie über die Filterkriterien und die Suchleiste nach der Anwendung Visibility Content (sn_pattern_design).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Password2-Verschlüsselung für Muster

Der Feldtyp Passwort (zweifach-Wege verschlüsselt) wird zum Verschlüsseln und Entschlüsseln von Daten verwendet. Der Feldtyp funktioniert gemäß den NIST 800-57-Richtlinien und bietet FIPS 140-2-L3-Schutz.

Passwort2 ist ein Textfeld, in dem vertrauliche Daten mit Zwei-Wege-Verschlüsselunggespeichert werden. Die Zwei-Wege-Verschlüsselungspeichert die Daten als sicheren verschlüsselten Wert, der innerhalb der Instanz Now Platform entschlüsselt werden kann.

Ab Quebec können Sie mit Key Management Framework Schlüssel verwalten, die für Password2-Felder verwendet werden. Auf einer Now Platform mit Release Rome oder höher ist die Implementierung von Password2 jedoch verbindlich vorgeschrieben.

Hinweis: Nur neu erstellte Datensätze, die Password2-Felder enthalten, werden zweifachverschlüsselt. Vorhandene Daten werden nicht automatisch zur Verwendung der Password2-Verschlüsselung konvertiert.

Password2-Implementierung überprüfen

Store-App Discovery and Service Mapping Patterns

Stellen Sie sicher, dass die Store-App Discovery and Service Mapping Patterns (Version 1.0.76) installiert ist.

Sicherstellen, dass Password2 in XML-Datensätzen enthalten ist

Zeigen Sie die XML-Datensätze in der Now Platform-Instanz an, und überprüfen Sie, ob die Verschlüsselung diesem Beispiel ähnelt:

CI-Typen für Service-Mapping und Discovery erstellen

Erstellen Sie CI-Typen (oder CI-Klassen) für Anwendungen und Geräte, die Service-Mapping und Discovery standardmäßig nicht unterstützen.

Vorbereitungen

Erforderliche Rolle: service_mapping_admin, personalize_dictionary oder admin
Stellen Sie sicher, dass kein CI-Typ für diese Anwendung oder dieses Gerät vorhanden ist.

Warum und wann dieser Vorgang ausgeführt wird

Alle Anwendungen und Hosts in Ihrer Organisation müssen über einen entsprechenden Typ von Konfigurationselement bzw. Configuration Item (CI) verfügen, der dafür erforderlich ist, dass diese Anwendungen und Hosts richtig erkannt und verarbeitet werden.

Hinweis: Die Discovery- und CMDB-Benutzeroberfläche beziehen sich auf CI-Typen als CI-Klassen.

Ihnen steht eine große Auswahl vorkonfigurierter CI-Typen zur Verfügung, die die am häufigsten verwendeten Anwendungen abdecken. Wenn Ihre Organisation eine weniger bekannte oder eine proprietäre Anwendung verwendet, die über keinen entsprechenden CI-Typ verfügt, müssen Sie ihn erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein CI-Typ ist ein generischer Begriff, der von mehreren ServiceNow-Anwendungen verwendet wird, es gibt jedoch einige spezifische Attribute für Service-Mapping und Discovery.

Ein CI-Typ (oder eine Klasse) enthält mehrere wichtige Definitionen, die für alle zugehörigen CIs gelten. Beispiel:

- CI-Attribute werden den CMDB-Tabellen als Felder hinzugefügt.
- Bezeichner helfen Service-Mapping und Discovery bei der Unterscheidung zwischen neuen und vorhandenen CIs. Wenn beispielsweise in der CMDB ein Apache-Webserver-CI-Typ definiert ist und sowohl Service-Mapping als auch Discovery ein Apache-Webserver-CI erkennen, verarbeitet sie es mit Bezeichnern. Sie erkennt es dann als aktualisierte Version des Apache-Webserver-CI, das bereits im System vorhanden ist, und nicht als neues Apache-Webserver-CI.
- Es gibt Abgleichsregeln , die der ServiceNow-Plattform helfen, CI-Attribute korrekt zu konsolidieren, die aus verschiedenen Anwendungen eingegangen sind. Diese Regeln sind für Organisationen erforderlich, in denen mehr als eine Anwendung Gegenstand des Discovery-Prozesses ist. Abgleichsregeln definieren, wie Attribute desselben CI, die von verschiedenen Erkennungsquellen erkannt wurden, zusammengeführt werden. Zum Beispiel entdeckt Service-Mapping Versions- und Startverzeichnisattribute eines Apache-Webserver-CI, während Discovery die Versions- und Patch-Ebenen-Attribute für das gleiche Apache-Webserver-CI entdeckt. Mit Now Platform wird die Abgleichsregel angewendet, und Service-Mapping überschreibt daher nicht die von Discovery gefundenen Attribute.
- Zugehörige Elemente, sowohl CIs als auch Nicht-CIs, dienen als Referenz und liefern zusätzliche Informationen zum CI. Beispielsweise können Sie eine Seriennummer, einen Port und eine Netzwerk-APR-Tabelle als zugehörige Elemente für einen Hardwareserver definieren. Diese Elemente werden vom System nicht zur Identifizierung verwendet. Nachdem Sie zugehörige Elemente für den CI-Typ konfiguriert haben, können Sie die Horizontal-Discovery für CIs dieses Typs zusammen mit den zugehörigen Elementen verwenden.Diesbezügliche Informationen finden Sie unter Zugehörige Elemente zusammen mit dem Haupt-CI erkennen.

  Hinweis: Nicht-CIs sind Elemente, die die Konfigurationselement-Tabelle [cmdb_ci] nicht erweitern. Beispiele für Nicht-CIs sind Ports, Seriennummern oder Netzwerk-ARP-Tabellen.

- CMDB speichert die CI-Klasse in Form einer Hierarchie, in der einige CI-Klassen übergeordnete Elemente anderer CI-Klassen sind. Diese untergeordneten CI-Klassen leiten (zusätzlich zu den Attributen, die Sie speziell für sie konfigurieren) automatisch die Attribute der ihnen übergeordneten Klassen ab. Die CI-Klassenhierarchie wird häufig zum Konfigurieren des CI-Verhaltens, der Beziehungen und der Anzeige verwendet. In diesem Beispiel ist das Apache-Webserver-CI dem Webserver-CI untergeordnet und leitet viele Attribute vom übergeordneten Element ab, z. B. Name, Version, Modell-ID. Standardmäßig übernehmen untergeordnete CI-Klassen Bezeichner von ihren übergeordneten CI-Klassen.

Zusätzlich zu diesen CI-Typ-Definitionen verwendet der horizontale Erkennungsprozess eine CI-Klassifizierung, um zu definieren, zu welchem CI-Typ ein CI gehört. Erstellen Sie eine Geräte-CI-Klassifizierung, wenn Sie einen CI-Typ für Geräte mit SNMP und eine Prozess-CI-Klassifizierung für einen Anwendungs-CI-Typ erstellen.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **CI-Klassen Manager**.
2. Wenn Sie einen vorhandenen CI-Typ als übergeordnetes Element für den neuen CI-Typ verwenden möchten, klicken Sie auf **Hierarchie**, um die Liste der CI-Klassen anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf das Kontextmenü für den erforderlichen CI-Typ und wählen Sie **Untergeordnete Klasse hinzufügen** aus.
4. Tabelle erstellen zum Speichern der CI-Typattribute:

Formular „Neue Tabelle“

Feld	Beschreibung
Bezeichnung	Name des CI-Typs. Beispiel: Apache-Webserver
Name	Der Tabellenname. Beispiel: cmdb_ci_apache_web_server. Verwenden Sie einen Namen, der den anderen CMDB-Klassen ähnlich ist (z. B. `u_cmdb_ci_laptop`).
Erweitert Tabelle	Der Tabellenname des übergeordneten CI-Typs. Alle CI-Typen sind Erweiterungen der Konfigurationselement-Tabelle [cmdb_ci] oder ihrer untergeordneten Tabellen. Beispiel: Wenn die neue Klasse Laptops ist, was eine Unterklasse von Computern ist, wählen Sie die Tabelle cmdb_ci_computer aus. Wenn die neue Klasse eine Klasse der obersten Ebene ist, wählen Sie die Tabelle cmdb_ci aus. Die am häufigsten verwendeten übergeordneten CI-Typen sind: ◦ cmdb_ci - Standard ◦ cmdb_ci_database - für Datenbanken ◦ cmdb_ci_app_server - für Anwendungsserver ◦ cmdb_ci_infra_service - für Infrastrukturservices ◦ cmdb_ci_endpoint_inclusion - für Einstiegspunkte des Integrationstyps ◦ cmdb_ci_appl - für Anwendungen ◦ cmdb_ci_web_server - für Webserver ◦ cmdb_ci_lb - für Lastenausgleichsmodule ◦ cmdb_ci_endpoint - für Einstiegspunkte

5. Konfigurieren Sie, wie die Instanz bestimmt, ob ein erkanntes CI ein aktualisiertes CI in der Instanz oder ein brandneues CI ist.
Die Einzelheiten des Verfahrens finden Sie unter CI-Identifizierungsregel erstellen oder bearbeiten .

> ⚠ **Warnung:** Wenn keine CI-Identifizierungsregel für einen CI-Typ vorhanden ist, erkennt Service-Mapping CIs, die zu diesem Typ gehören, kann die Ergebnisse des Erkennungsprozesses jedoch nicht interpretieren. In diesem Fall lehnt Now Platform die Erkennungsergebnisse für diese CIs ab, und ihre Informationen werden nicht aktualisiert.

a. Konfigurieren Sie auf der Seite **Bezeichner** die Parameter wie folgt:

Bezeichner-Formular

Feld	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Betrifft	Geben Sie den CI-Typ ein.
Aktiv	Aktivieren Sie das Kontrollkästchen .
Unabhängig	Deaktivieren Sie das Kontrollkästchen .

b. Konfigurieren Sie die Bezeichner-Eintragsparameter wie folgt:

Bezeichnereintrags-Formular

Feld	Beschreibung
Kriteriumsattribute	Wählen Sie das Attribut aus, das Sie zum Identifizieren des CI verwenden möchten. Beispielsweise **Klasse**, **Installationsverzeichnis** oder **Seriennummer**.
Null-Attribut unterstützen	Aktivieren Sie das Kontrollkästchen .
Priorität	Wenn mehr als ein Bezeichnet-Eintrag vorhanden ist, fügen Sie die Priorität hinzu, um die Reihenfolge zu bestimmen, in der Service-Mapping diese Einträge anwendet. Wenn keines der Identifizierungskriterien mit dem erkannten CI übereinstimmt, ist dieses CI neu.

6. Wahlweise: Konfigurieren Sie Verweise auf andere CIs oder Nicht-CIs als zugehörige Elemente für den CI-Typ.

Formular „Zugehörige Einträge“

Feld	Beschreibung
Aktiv	Kontrollkästchen, das angibt, dass der zugehörige Eintrag aktiv ist.
Zugehörige Tabelle	Eine zugehörige Tabelle, die auf das CI verweist, das abgeglichen wird.
Referenziertes Feld	Ein referenziertes Feld in der **Zugehörigen Tabelle**, das das referenzierte CI speichern soll. Dieses Feld verweist immer auf die Tabelle „cmdb_ci“ oder auf eine untergeordnete Tabelle der Tabelle „cmdb_ci“.
Priorität	Priorität des zugehörigen Eintrags für die angegebene **Zugehörige Tabelle**. Regeln mit niedrigeren Prioritätszahlen werden bei der Abgleichung eines zugehörigen Elements mit einer bestimmten zugehörigen Tabelle mit höherer Priorität behandelt. Zugehörige Einträge für die angegebene zugehörige Tabelle von identischer Priorität werden nach dem Zufallsprinzip angewendet. Sie können zwischen den Prioritätszahlen Lücken lassen, um die Zuweisung ungenutzter Zahlen für neue Einträge zu ermöglichen, ohne die bestehende Prioritätsreihenfolge verändern zu müssen.
Kriteriumsattribute	Der Satz von Attributen, um das zugehörige Element eindeutig zu identifizieren. Attribute gehören entweder zu der aktuellen Klasse oder einer übergeordneten Klasse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Das Hinzufügen von Referenzfeldern als Kriteriumsattribute ist möglich. Solche Felder sind jedoch möglicherweise nicht immer wirksam: ◦ In Referenzfeldern werden *sys_ids* gespeichert, die auf einen Datensatz in einer anderen Tabelle verweisen. Somit gelten Referenzfelder (bezüglich der Eindeutigkeit) als schwache Kriteriumsattribute für die aktuelle Tabelle. ◦ Vom System werden ungültige Werte in einem Referenzfeld erkannt und dann durch „Unbekannt“ ersetzt. Beispielsweise wird ein ungültiger Wert für *Model ID* durch den Wert „Unbekannt“ ersetzt. Wenn für mehrere CIs dasselbe Referenzfeld auf „Unbekannt“ festgelegt ist, werden diese CIs auch zu doppelten CIs. Wählen Sie das Sperrsymbol, um Attribute zur Identifizierungsregel anzuzeigen, hinzuzufügen oder zu entfernen.
Null-Attribut unterstützen	Wenn mindestens ein Kriteriumsattribut in der zugehörigen Tabelle nicht null ist, lassen Sie den Versuch zu, eine Übereinstimmung mit einem Bezeichner-Eintrag zu erzielen, selbst wenn Kriteriumsattribute vorliegen, die null sind.
Filterbedingungen	Fügen Sie Bedingungen hinzu, um einen Filter zum Eingrenzen der Datensätze zu erstellen, die nach einem übereinstimmenden zugehörigen Element durchsucht werden.

7. Wahlweise: Konfigurieren Sie die Instanz so, dass CI-Attribute aus verschiedenen Datenquellen korrekt konsolidiert werden.
Siehe CI-Abgleichregeln erstellen oder bearbeiten .

   Konfigurieren Sie die folgenden Service-Mapping zugehörigen Parameter korrekt:

   Abgleichsdefinitions-Formular

Feld	Beschreibung
Datenquelle	Wählen Sie `ServiceWatch`.
Betrifft	Wählen Sie den entsprechenden CI-Typ aus.
Optionale Bedingung	Legen Sie ggf. eine Bedingung fest.

   Hinweis: Wenn Sie keine CI-Abgleichsregel erstellen, werden von Mustern erkannte Daten zum Aktualisieren von CI-Attributen verwendet.

8. Konfigurieren Sie die CI-Klassifizierung für Ihren CI-Typ:
   - Führen Sie für CI-Typen, die Anwendungen darstellen, die Konfiguration wie in Discovery-Prozessklassifizierung erstellen beschrieben aus.
   - Führen Sie für CI-Typen, die SNMP-Geräte darstellen, die Konfiguration gemäß der Beschreibung in Discovery-CI-Klassifizierung erstellen durch.

   Hinweis: CI-Klassifizierungen für Hosts müssen nicht erstellt werden, da diese Klassifizierungen im Basissystem enthalten sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Definieren Sie für CI-Typen, die Einschlüsse darstellen, die Hierarchie für den neuen CI-Typ.

   Deaktivieren Sie während dieser Konfiguration das Kontrollkästchen **Beziehungsrichtung umkehren**.

   Siehe Abhängige Beziehungen erstellen .

10. Passen Sie bei Bedarf die Symbole an, die CIs in Zuordnungen darstellen.
    Siehe Zuordnungssymbole erstellen oder ändern .

Einstiegspunkttypen für Service-Mapping erstellen

Ein Einstiegspunkt ist ein Punkt, auf den Clients auf eine Serviceinstanz zugreifen. Service-Mapping startet den Zuordnungsprozess für jeden Anwendungsservice ab dem Einstiegspunkt, den Sie dafür definieren. Service-Mapping beinhaltet eine Vielzahl vorkonfigurierter Einstiegspunkttypen, die die am häufigsten verwendeten Anwendungen abdecken. Wenn Ihre Organisation eine weniger bekannte oder eine proprietäre Anwendung verwendet, die über keinen entsprechenden Einstiegspunkt in Service-Mapping verfügt, müssen Sie ihn erstellen.

Vorbereitungen

Wenn in Ihrer ServiceNow-Instanz Domänentrennung eingesetzt wird und Sie Zugriff auf die globale Domäne haben, melden Sie sich bei der entsprechenden Domäne an. Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.

Erforderliche Rolle: service_mapping_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Darüber hinaus verwenden Service-Mapping-Muster Einstiegspunkte, um ausgehende CI-Verbindungen zu erkennen und so den Zuordnungsprozess für Einstiegspunkte zu starten.

Einstiegspunkte werden in ServiceNow CMDB als CIs des Endpunkttyps modelliert. Einstiegspunkte werden als Datensätze in den Endpunkttabellen [cmdb_ci_endpoint] gespeichert.

Wie auch andere CI-Typen enthält ein Einstiegspunkt mehrere wichtige Definitionen, die für alle zugehörigen CIs gelten:

- CI-Attribute werden den CMDB-Tabellen als Felder hinzugefügt.
- Bezeichner helfen Service-Mapping und Discovery bei der Unterscheidung zwischen neuen und vorhandenen CIs. Beispiel: Wenn in der Multisource-CMDB ein Endpunkt-CI-Typ für die Active Directory-Gesamtstruktur definiert ist und Service-Mapping ein Active Directory-Gesamtstruktur-CI erkennt, verarbeitet Service-Mapping dieses CI mit Bezeichnern und erkennt es als aktualisierte Version des vorhandenen Active Directory-Gesamtstruktur-CI im System und nicht als neues Active Directory-Gesamtstruktur-CI.
- CI-Typhierarchie CMDB speichert die CI-Klasse in Form einer Hierarchie, in der einige CI-Klassen übergeordnete Elemente anderer CI-Klassen sind. Diese untergeordneten CI-Klassen leiten (zusätzlich zu den Attributen, die Sie speziell für sie konfigurieren) automatisch die Attribute der ihnen übergeordneten Klassen ab. Die CI-Klassenhierarchie wird häufig zum Konfigurieren des CI-Verhaltens, der Beziehungen und der Anzeige verwendet. Erstellen Sie Standardeinstiegspunkte als untergeordnete CIs für den Endpunkt-CI-Typ, wodurch eine Erweiterung für die Tabelle cmdb_ci_endpoint erstellt wird. Erstellen Sie für Einstiegspunkte des Integrationstyps untergeordnete CIs für den CI-Typ des Integrationsendpunkts, der die Tabelle cmdb_ci_endpoint_inclusion erweitert. Bei einer Inklusion hostet ein Server Anwendungen, die als unabhängige Objekte behandelt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **CI-Klassen Manager**.
2. Wählen Sie **Offene Hierarchie**.
3. Klicken Sie zum Erstellen eines Standardeinstiegpunkts mit der rechten Maustaste im Fenster **Klassenhierarchie** auf **Endpunkt** und wählen Sie **Untergeordnete Klasse hinzufügen** aus.
4. Klicken Sie zum Erstellen eines Einstiegspunkts des Integrationstyps mit der rechten Maustaste im Fenster **Klassenhierarchie** auf **Inclusion Endpoint** und wählen Sie **Nachfolgeklasse hinzufügen** aus.
5. Definieren Sie die Parameter für den neuen Einstiegspunkttyp wie in CI-Klasse erstellen beschrieben.

Zugehörige Informationen

Ordnen Sie einen einzelnen Anwendungsservice mit zu klassisch Service-Mapping

CI-Typen für Service-Mapping und Discovery erstellen

Muster erstellen oder anpassen

Erstellen oder ändern Sie ein Erkennungsmuster, und definieren Sie seine Standardattribute.

Vorbereitungen

Stellen Sie sicher, dass die Anwendung, für die Sie ein Muster erstellen möchten, über einen entsprechenden CI-Typ (Configuration Item) und eine CI-Klassifizierung verfügt. Wenn sich der erforderliche CI-Typ nicht in der Liste befindet, erstellen Sie ihn wie unter CI-Typen für Service-Mapping und Discovery erstellen beschrieben.

Wenn in Ihrer ServiceNow-Instanz Domänentrennung eingesetzt wird und Sie Zugriff auf die globale Domäne haben, melden Sie sich bei der entsprechenden Domäne an. Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.

Erforderliche Rolle: pd_admin

Grundkenntnisse in der Programmierung sind wünschenswert.

Warum und wann dieser Vorgang ausgeführt wird

Muster können den Infrastruktur- oder Anwendungstyp aufweisen. Infrastrukturmuster werden nur von Discovery zum Erstellen von Gerätelisten verwendet. Anwendungsmuster dienen Service-Mapping und Discovery, die für ihre Zwecke dieselben Anwendungsmuster verwenden.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**.
2. Klicken Sie auf **Neu**, oder wählen Sie das entsprechende Muster aus der Liste aus.
3. Definieren Sie die Standardmusterattribute auf der Registerkarte **Standard**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Mustertyp	◦ Wählen Sie **Anwendung** für ein Anwendungsmuster aus. Es kann sowohl für die Erkennung von oben nach unten von Service-Mapping als auch für die horizontale Erkennung von Discovery verwendet werden. ◦ Wählen Sie **Infrastruktur** aus, um ein Infrastrukturmuster für die horizontale Host-Erkennung von Discovery zu verwenden.
Name	Geben Sie den Musternamen ein. Dieser Name muss für dieses Muster eindeutig sein. Verwenden Sie selbsterklärende Namen wie `Apache auf Unix-Muster`.
CI-Typ	Wählen Sie den CI-Typ aus, den dieses Muster erkennen soll. **Hinweis:** Die Erkennung kann mehrere CIs finden, die zum gleichen CI-Typ gehören.
Betriebssystem [nur für Anwendungsmuster]	Wählen Sie das Betriebssystem aus, das das ausgewählte CI ausführt: ◦ Klicken Sie auf **Alle**, wenn das CI auf mehr als einem Betriebssystem ausgeführt wird. Oder ◦ Wählen Sie das relevante Betriebssystem aus der Liste aus.
Ausführungsreihenfolge [nur für Anwendungsmuster]	Definieren Sie für ein Anwendungsmuster, das von Service-Mapping verwendet wird, wann das Muster ausgeführt wird. **a.** Wählen Sie die Reihenfolge aus, in der dieses Muster immer ausgeführt wird: ▪ **Vor** ▪ **Nach** **b.** Wählen Sie dann das andere zutreffende Muster aus. Dieses Feld ist nur relevant, wenn ein bestimmtes Muster mit einem anderen Muster verwechselt werden kann. Beispielsweise verfügen IIS- und MS Exchange-Anwendungen über einen HTTP-Einstiegspunkt. MS Exchange verwendet jedoch einige der Komponenten von IIS. Daher kann die Erkennung MS Exchange fälschlicherweise als IIS identifizieren, wenn das IIS-Muster zuerst ausgeführt wurde. Klicken Sie im Feld **Ausführungsreihenfolge** in der MS Exchange-Musterdefinition auf **Vor** und **IIS**, um diesen Fehler zu vermeiden.
Beschreibung	Geben Sie eine Beschreibung für dieses Muster an.

4. Wahlweise: Wenn Sie ein Anwendungsmuster erstellen, darf dieses Muster vom MID-Server nur ausgeführt werden, wenn der auf einem CI erkannte Prozess mit den Klassifizierungskriterien für dieses Muster übereinstimmt. Wählen Sie dazu **Prozessklassifizierung erzwingen** aus.
   Bei allen vereinfachten Mustern, die aus generischen Anwendungen erstellt werden, ist dieses Attribut aktiviert. Weitere Informationen zum Erstellen der Prozessklassifizierung finden Sie unter Discovery-Klassifizierer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Definieren Sie einen Satz von Identifizierungsschritten für jede eingehende Verbindung eines Configuration Item (CI), wie in KB1698521: Muster erstellen oder anpassen beschrieben.
6. Erstellen Sie bei Bedarf weitere Identifizierungsabschnitte.
7. Speichern Sie das Muster.
8. Wahlweise: Um das Muster zu testen, wählen Sie **den Debug-Modus**, und geben Sie die IP-Adresse des Hosts ein.
9. Laden Sie die aktualisierte Gruppe von Mustern auf den MID-Server hoch:
   a. Navigieren zu **Discovery** > **MID-Server**.
   b. Alternativ navigieren Sie zu **Service-Mapping** > **MID-Server**.
   c. Klicken Sie auf **Mustersynchronisierung mit MID**.

Nächste Maßnahme

Fahren Sie für Anwendungstypmuster mit dem Erstellen eines Verbindungsabschnitts fort, wie im KB-Artikel KB1698521: Muster erstellen oder anpassen beschrieben.

Zugehörige Informationen

Cloud-Discovery erkunden

KB0747679: Pre/Post Processing Scripts for patterns (Vor-/Nachverarbeitungsskripts für Muster)

KB0854603: Zeitüberschreitung bei Muster-Debugger-Sitzung

Zugehörige Elemente zusammen mit dem Haupt-CI erkennen

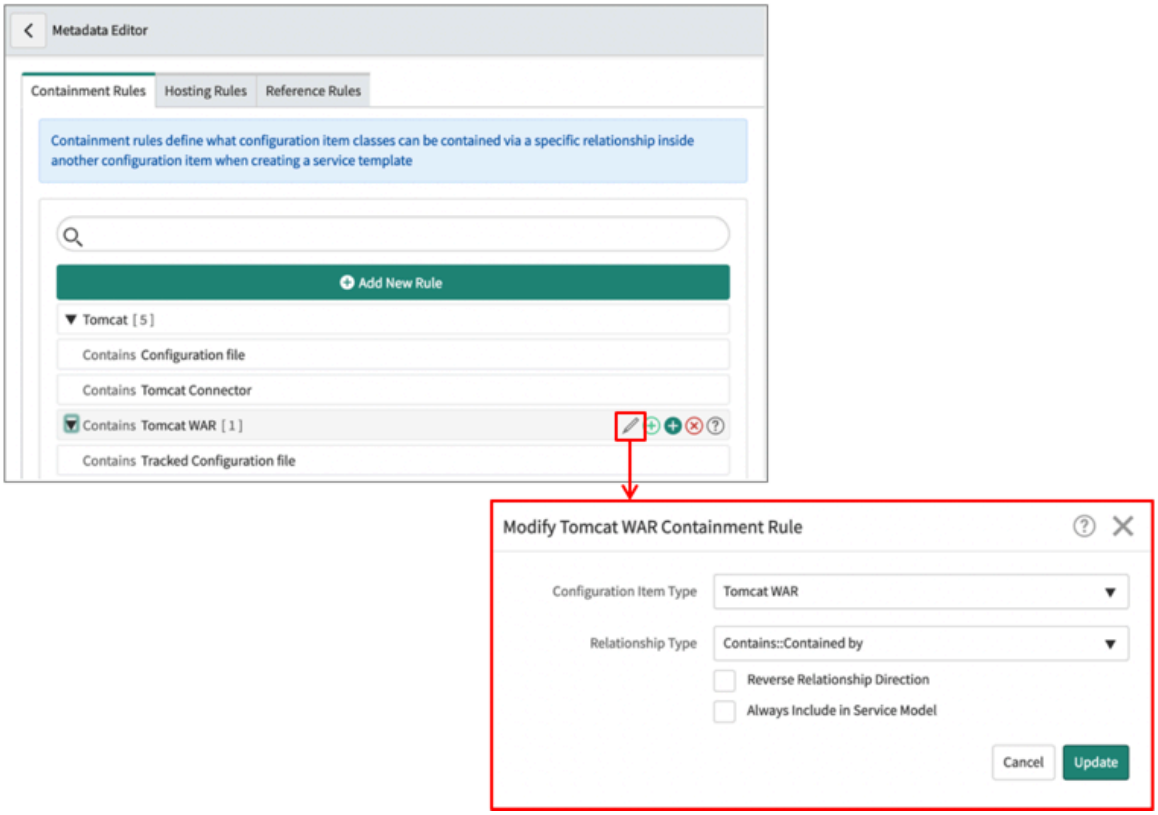
Fügen Sie den Mustern zugehörige Elemente hinzu, um eine horizontale Erkennung von Konfigurationselementen mit allen zugehörigen Elementen durchzuführen: CIs oder Nicht-CIs wie Ports oder Seriennummern.

Vorbereitungen

1. (Optional) Überprüfen Sie, ob das CI abhängig ist: Das System verwendet die Identifizierungsregeln, um das CI unabhängig von anderen CIs zu identifizieren. Weitere Informationen finden Sie unter Eine CI-Identifizierungsregel erstellen oder bearbeiten .
2. (Optional) Um das Modell besser zu verstehen, überprüfen Sie abhängige Beziehungsregeln, die die Abhängigkeitsstruktur der CI-Typen und die Beziehungstypen in diesen Servicedefinitionen definieren. Beispielsweise können Sie einen Tomcat-Server erkennen, zu dem Tomcat-WARs gehören. Weitere Informationen finden Sie unter Abhängige Beziehungsregeln .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für die Containment-Regel für Tomcat-WAR



3. Um dem Muster ein Nicht-CI hinzuzufügen, fügen Sie es als zugehöriges Element für den CI-Typ hinzu, zu dem das Haupt-CI gehört. Weitere Informationen zum Hinzufügen zugehöriger Elemente für den CI-Typ finden Sie unter Referenzen auf andere CIs oder Nicht-CIs als zugehörige Elemente für den CI-Typ konfigurieren.

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird

Zugehörige Elemente, sowohl CIs als auch Nicht-CIs, dienen als Referenz und liefern zusätzliche Informationen zum CI. Beispielsweise können Sie eine Seriennummer, einen Port und eine Netzwerk-APR-Tabelle als zugehörige Elemente für einen Hardwareserver definieren. Diese Elemente werden vom System nicht zur Identifizierung verwendet. Nachdem Sie zugehörige Elemente für den CI-Typ konfiguriert haben, können Sie die Horizontal-Discovery für CIs dieses Typs zusammen mit den zugehörigen Elementen verwenden.

Hinweis: Nicht-CIs sind Elemente, die die Konfigurationselement-Tabelle [cmdb_ci] nicht erweitern. Beispiele für Nicht-CIs sind Ports, Seriennummern oder Netzwerk-ARP-Tabellen.

Der Musterdesigner zeigt Attribute zugehöriger CI-Typen an, die Sie dem Muster im CI-Attributbereich hinzugefügt haben. Sie können diese Attribute anzeigen und verwenden, während Sie das Haupt-CI-Muster erstellen oder ändern.

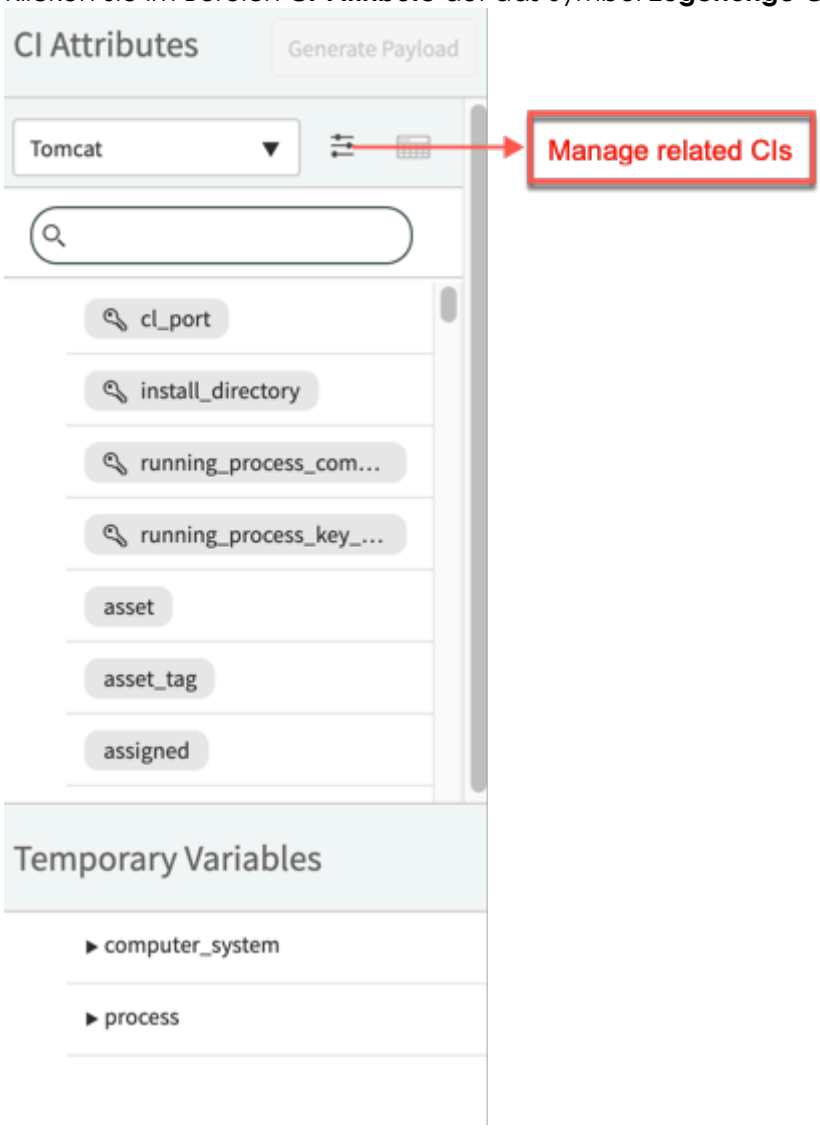
Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**.
2. Wählen Sie das entsprechende Muster aus.
3. Wählen Sie im Musterformular den entsprechenden Identifikationsteil aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

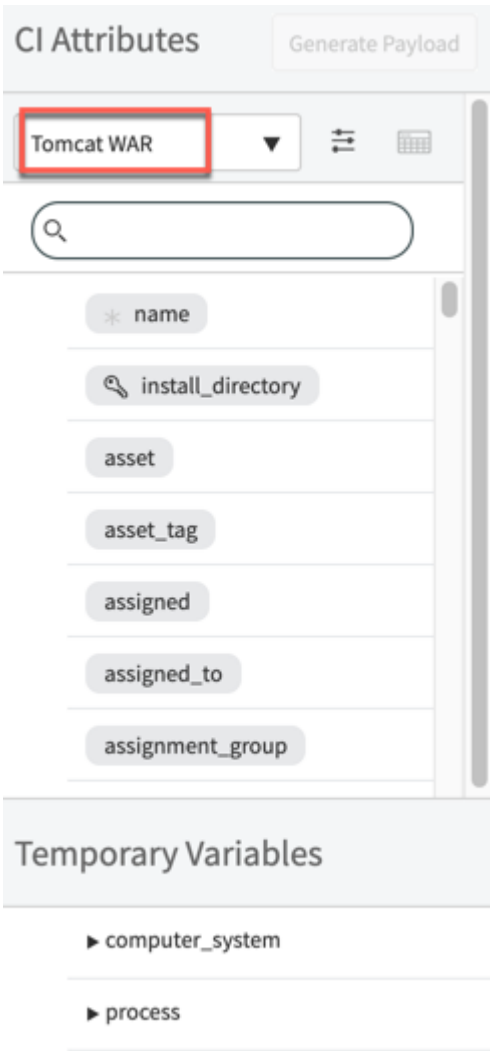
4. Stellen Sie sicher, dass Sie sich nicht im Debug-Modus befinden.
5. Klicken Sie im Bereich **CI-Attribute** auf das Symbol **Zugehörige CIs verwalten**.



6. Wählen Sie den entsprechenden CI-Typ aus.
   Sie können das Suchfeld verwenden, um nach einem bestimmten CI-Typ zu suchen.
7. Klicken Sie auf das Plussymbol.
   Das neue zugehörige Element „CI-Typ“ wird zur Liste hinzugefügt.
8. Wahlweise: Fügen Sie andere zugehörige CI-Typen hinzu.
9. Klicken Sie auf **OK**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Neue Registerkarten für zugehörige CI-Typen, die Sie hinzugefügt haben, werden unter der Registerkarte für das Haupt-CI angezeigt:



Nächste Maßnahme
Bearbeiten Sie das Muster weiter, indem Sie nach Bedarf weitere Schritte hinzufügen. Zum Anzeigen oder Verwenden von Attributen eines zugehörigen CI-Typs klicken Sie im Bereich **CI-Attribute** auf die entsprechende Registerkarte.

Muster verbessern, ohne ihre Identifizierungsabschnitte zu ändern

Ermöglichen Sie Mustern die Suche nach zusätzlichen Attributen und ändern Sie die in Identifizierungsabschnitten definierte Mustererkennungslogik mithilfe von Erweiterungsabschnitten. Jeder Erweiterungsabschnitt enthält einen vorkonfigurierten Satz von Erkennungsschritten, die als gemeinsam genutzte Bibliothek bezeichnet werden.

Vorbereitungen
Wenn in Ihrer ServiceNow-Instanz Domänentrennung eingesetzt wird und Sie Zugriff auf die globale Domäne haben, melden Sie sich bei der entsprechenden Domäne an. Die ausgewählte Domäne muss eine Domäne ohne untergeordnete Domänen sein.

Grundkenntnisse in der Programmierung sind wünschenswert.

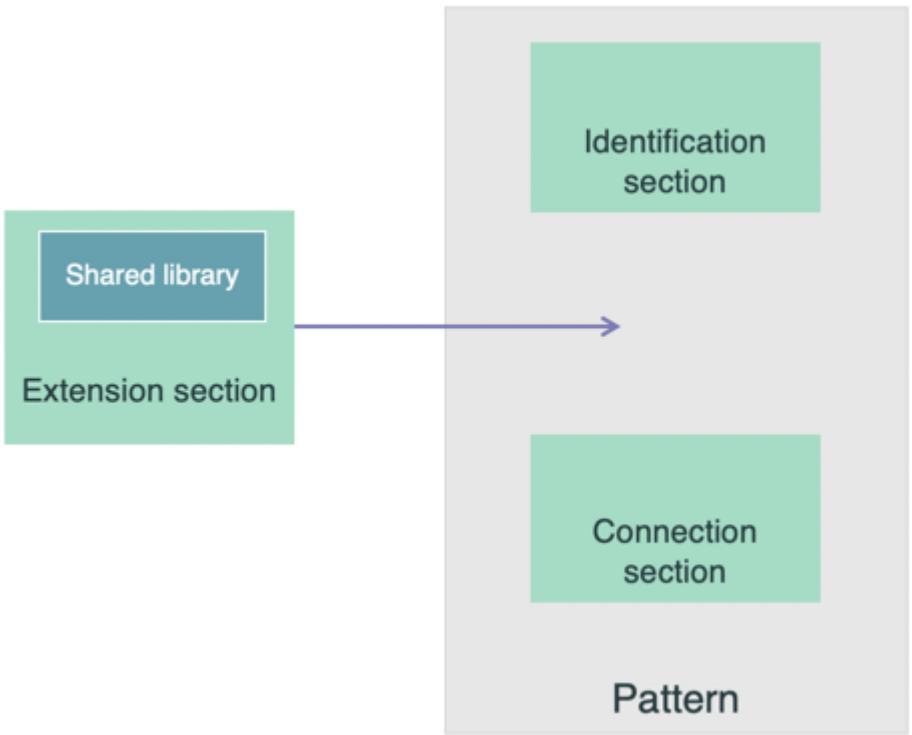
Erforderliche Rolle: pd_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird
Muster können den Infrastruktur- oder Anwendungstyp aufweisen. Infrastrukturmuster werden nur von Discovery zum Erstellen von Gerätelisten verwendet. Anwendungsmuster dienen Service-Mapping und Discovery, die für ihre Zwecke dieselben Anwendungsmuster verwenden. Jedes Muster, einschließlich seiner Identifizierungs- und Verbindungsabschnitte, ist eine einzelne Datei. Es gibt auch wiederverwendbare Sequenzen von Erkennungsschritten, die als gemeinsam genutzte Bibliotheken bezeichnet werden. Jede gemeinsam genutzte Bibliothek ist eine einzelne Datei, sie ist jedoch immer Teil der Infrastruktur oder des Anwendungsmusters und wird nicht als eigenständiges Muster verwendet. Datensätze für Muster und gemeinsam genutzte Bibliotheken befinden sich in der Tabelle „Erkennungsmuster“ [sa_pattern].

Um die Erkennungslogik in Identifizierungsabschnitten zu ändern, ohne die Identifizierungsabschnitte selbst zu ändern, können Sie dem Muster Erweiterungsabschnitte hinzufügen. Jeder Erweiterungsabschnitt besteht aus einer gemeinsamen Bibliothek, entweder neu oder vorhanden.

Erweiterungsabschnitt zu einem Muster hinzufügen



Wenn Sie im Erweiterungsabschnitt eine gemeinsam genutzte Bibliothek erstellen oder ändern, speichern Sie Änderungen nur in der gemeinsam genutzten Bibliothek, nicht am Muster, das diesen Erweiterungsabschnitt enthält.

⚠ **Warnung:** Die Änderungen an der freigegebenen Bibliothek wirken sich auf alle Muster aus, die diese gemeinsam genutzte Bibliothek verwenden.

Der MID-Server führt Erweiterungsabschnitte nach Identifizierungsabschnitten aus und nur, wenn mindestens ein Identifizierungsabschnitt erfolgreich abgeschlossen wurde.

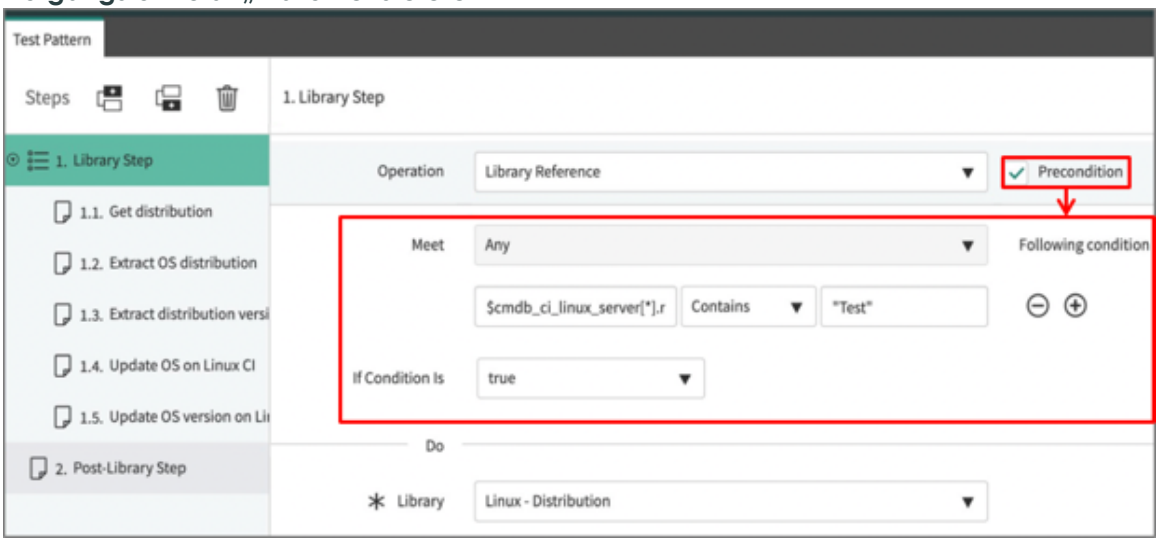
Wenn diesem Muster mehrere Erweiterungsabschnitte zugeordnet sind, definieren Sie die Reihenfolge, in der MID-Server diese Erweiterungsabschnitte ausführt.

Sie können gemeinsam genutzte Bibliotheken deaktivieren, sodass die verwendeten Muster Schritte in deaktivierten gemeinsam genutzten Bibliotheken überspringen. Weitere Informationen finden Sie unter Discovery Konfigurationskonsole. Wenn eine für einen Schritt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der gemeinsamen Bibliothek definierte Vorbedingung nicht erfüllt ist, werden alle Schritte, die zu dieser gemeinsamen Bibliothek gehören, vom Muster übersprungen. Beispiel: Wenn die Datei, auf die von der Variable verwiesen wird, nicht „test“ enthält, werden die Schritte 1-1 bis 1-5 der freigegebenen Bibliothek nicht ausgeführt. Die Voraussetzung ist nur für das Muster vorhanden, in dem Sie sie erstellt haben. Die Vorbedingung hat keine Auswirkungen auf andere Muster, von denen diese gemeinsam genutzte Bibliothek genutzt wird.

Vorgangsformular „Bibliotheksreferenz“



Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster** und öffnen Sie das gewünschte Muster aus der Musterliste.

   Das Muster kann vom Infrastruktur- oder Anwendungstyp sein.

2. So erstellen Sie einen Erweiterungsabschnitt und definieren Erkennungsschritte für die gemeinsam genutzte Bibliothek.

   a. Klicken Sie im **Erweiterungsabschnitt** auf **Neu**.

   b. Geben Sie den Namen dieses Erweiterungsabschnitts ein.

   c. Klicken Sie auf **Erledigt**.
   Das Musterformular zeigt den neuen Abschnitt unter **Erweiterungsabschnitt** an.

   d. Klicken Sie auf den Namen des neuen Erweiterungsabschnitts.

   Der Musterdesigner wird geöffnet und zeigt die Schritte-Struktur auf der linken Seite an.

   Wenn für dieses Muster keine Erkennungsschritte identifiziert wurden, wird der **Schritt ohne Titel** in der Schritte-Struktur im linken Fensterbereich angezeigt.

   e. Definieren Sie Discovery-Schritte.

   f. Klicken Sie auf **Speichern**, um den Erweiterungsabschnitt zu speichern und damit Service-Mapping und Discovery diesen verwenden.
   Sie veröffentlichen keine Erweiterungsabschnitte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. So verwenden Sie eine vorhandene gemeinsam genutzte Bibliothek für den neuen Erweiterungsabschnitt:
   a. Klicken Sie im **Erweiterungsabschnitt** auf **Hinzufügen**.
   b. Wählen Sie die erforderliche gemeinsam genutzte Bibliothek aus der Namensliste aus.
4. Wenn mehrere Erweiterungsabschnitte vorhanden sind, definieren Sie die Reihenfolge, in der MID-Server diese Erweiterungsabschnitte ausführt.
   a. Aktivieren Sie das Kontrollkästchen neben dem Erweiterungsabschnitt.
   b. Klicken Sie im **Erweiterungsabschnitt** auf **Bearbeiten**.
   c. Geben Sie eine neue Ordnungszahl in das Feld **Reihenfolge** ein.
      Wenn nur ein Erweiterungsabschnitt vorhanden ist, ist die Reihenfolge standardmäßig **1**.

      Die Aktion mit der niedrigsten Nummer wird zuerst ausgeführt.
   d. Klicken Sie auf **Erledigt**.

Nächste Maßnahme
Klicken Sie auf **Debuggen**, um den neu erstellten Erweiterungsabschnitt auszuführen. Der Musterdesigner führt Erweiterungsabschnitte aus, nachdem Identifizierungsabschnitte ausgeführt wurden.

Muster mithilfe der datenverkehrsbasierten Erkennung optimieren

Als Alternative zum Anpassen des Musters auf der Seite des Musterdesigners verbessern Sie die vorhandenen Muster, damit Service-Mapping sie verwenden kann, um Konfigurationselement-Verbindungen (CIs) zu finden, die zuvor mithilfe der datenverkehrsbasierten Erkennung gefunden wurden.

Vorbereitungen
Erforderliche Rolle: pd_admin

Grundkenntnisse in der Programmierung sind wünschenswert.

Warum und wann dieser Vorgang ausgeführt wird
Service-Mapping kann Konfigurationselemente (CIs) anhand ihrer datenverkehrsbasierten Verbindungen erkennen und zuordnen. Diese Methode wird als datenverkehrsbasierte Zuordnung bezeichnet und ergänzt die musterbasierte Zuordnung.

Mithilfe der datenverkehrsbasierten Erkennung erkennt Service-Mapping möglicherweise eine wichtige CI-Verbindung. In diesem Fall können Sie sicherstellen, dass diese Verbindung immer für alle CIs gefunden wird, die zum gleichen CI-Typ gehören. Dazu ändern Sie das Muster, das zum Erkennen von CIs dieses CI-Typs verwendet wird. Ein Muster ist eine Folge von Befehlen, deren Zweck darin besteht, Attribute eines CI und seiner ausgehenden Verbindungen zu ermitteln.

Sie können CI-Konfigurationsdateien durchsuchen, um Daten zu finden, die mithilfe der datenverkehrsbasierten Erkennung ermittelt wurden, z. B. IP-Adresse und Port. Wenn Konfigurationsdateien diese Daten enthalten, erstellen Sie einen Musterschritt, um diese Datei zu analysieren. Wenn Service-Mapping das CI das nächste Mal mit dem geänderten Muster erkennt, extrahiert es die Informationen zu dieser Verbindung direkt aus der Konfigurationsdatei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Service-Mapping** > **Services** > **Anwendungsservices**.
2. Klicken Sie neben der betreffenden Serviceinstanz **auf Karte anzeigen**.
3. Klicken Sie mit der rechten Maustaste auf das entsprechende CI.
4. Wählen Sie **Traffic-basierte Verbindungen anzeigen**.
   Die Liste der datenverkehrsbasierten Verbindungen wird mit folgenden Informationen angezeigt:

Liste der datenverkehrsbasierten Verbindungen (wenn Discovery basierend auf Predictive Intelligence deaktiviert ist)

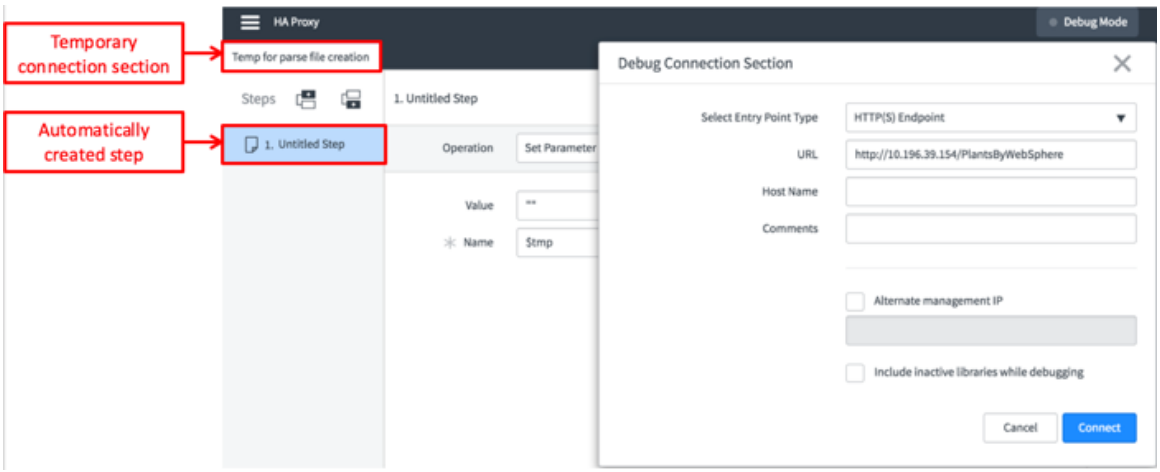
Feld	Beschreibung
IP	Die IP-Adresse der Anwendung, die mit dem ausgewählten CI verbunden ist.
Port	Der Port des ausgewählten CI, der zur Kommunikation mit der anderen Anwendung verwendet wird.
Prozess	Die ID des Prozesses im ausgewählten CI.
Bereits in der Darstellung	◦ **Ja** – wenn diese Verbindung in der Zuordnung angezeigt wird. ◦ **Nein** – wenn diese Verbindung nicht Teil der Serviceinstanz und nicht in der Zuordnung ist.
Systementscheidung	Die Einstellung legt fest, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Der Wert stammt von dem Algorithmus, den Service-Mapping Verwendet.
Benutzerentscheidung	(Optional) Die Einstellung überschreibt die Einstellung Systementscheidung, in der festgelegt wird, ob Service-Mapping die erkannte Traffic-basierte Verbindung behält oder entfernt. Wenn die Systementscheidungseinstellung für eine Verbindung beispielsweise Behalten lautet und Sie diese Verbindung entfernen möchten, wählen Sie `Entfernen`.

Hinweis: Es kann vorkommen, dass in der Zuordnung datenverkehrsbasierte Verbindungen angezeigt werden, nicht jedoch in der Liste der datenverkehrsbasierten Verbindungen. Dies geschieht für die Verbindungen, die vor weniger als drei Tagen aus der Tabelle TCP Connection [cmdb_tcp] entfernt wurden.

5. Doppelklicken Sie auf die Verbindung, die Sie zum Erstellen eines Musterschritts verwenden möchten.
6. Wenn zur Erkennung dieses CI mehrere Muster verwendet werden, wählen Sie das Muster aus, für das Sie den Schritt erstellen möchten, und klicken Sie auf **OK**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Musterdesigner erstellt einen vorübergehenden Verbindungsabschnitt für dieses Muster mit einem neuen Schritt.



Das Fenster „Verbindungsabschnitt debuggen“ wird mit teilweise automatisch ausgefüllten Feldern angezeigt.

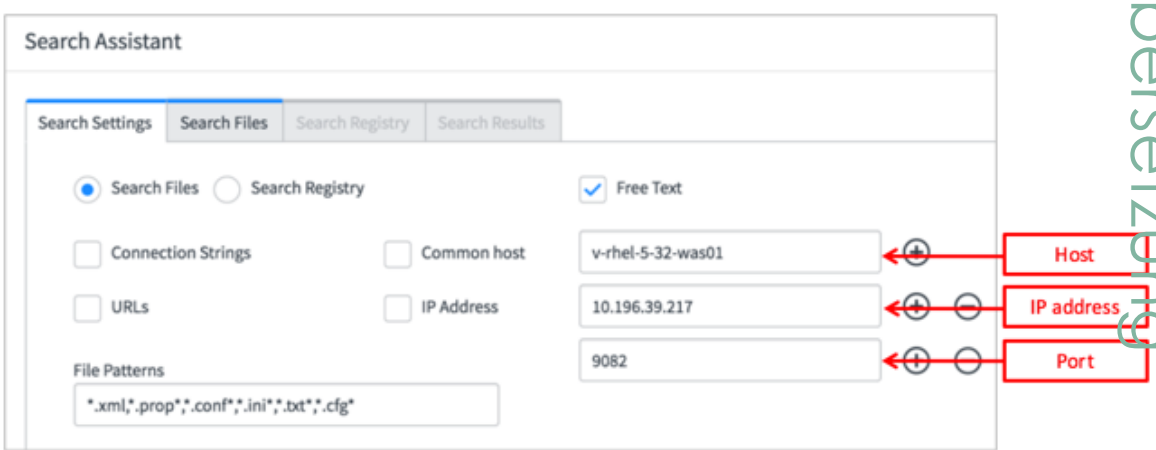
7. Klicken Sie auf **Verbinden**.

   Der Debug-Modus ist aktiviert.

   Das Fenster „Suchassistent“ wird geöffnet.

8. Durchsuchen Sie CI-Konfigurationsdateien nach Daten, die mithilfe der datenverkehrsbasierten Erkennung empfangen wurden:

   a. Überprüfen Sie unter **Freitext** Daten, die automatisch mit der Liste der datenverkehrsbasierten Verbindungen ausgefüllt werden.



   Das Feld „Dateimuster“ zeigt Dateitypen an, in denen der Musterdesigner die Suche durchführt.

   b. Klicken Sie auf die Registerkarte **Dateien durchsuchen**, und überprüfen Sie die Dateien. Bei Bedarf können Sie irrelevante Dateien aus der Suche entfernen, indem Sie auf das Minuszeichen klicken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

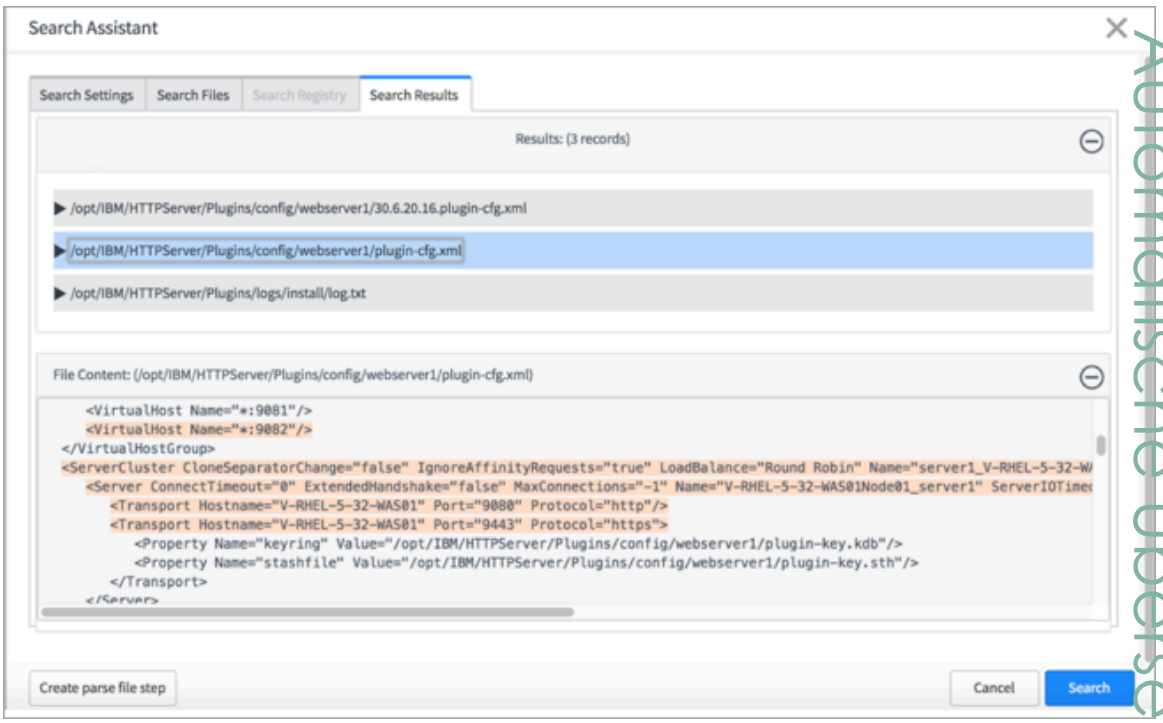
c. Klicken Sie auf **Suche**.

Nach Abschluss der Suche wird die Registerkarte **Suchergebnis** mit der Liste der Dateien geöffnet, in denen eines der Suchkriterien gefunden wurde.

9. Erstellen Sie einen Musterschritt für die Analyse der Konfigurationsdatei, die Informationen zur Verbindung enthält:

a. Klicken Sie auf der Registerkarte Suchergebnis auf eine der Dateien, und überprüfen Sie die Verbindungsdaten in dieser Datei.

b. Warten Sie, bis der Dateiinhalt geladen ist, und wählen Sie den entsprechenden Eintrag unter dem Dateinamen aus:



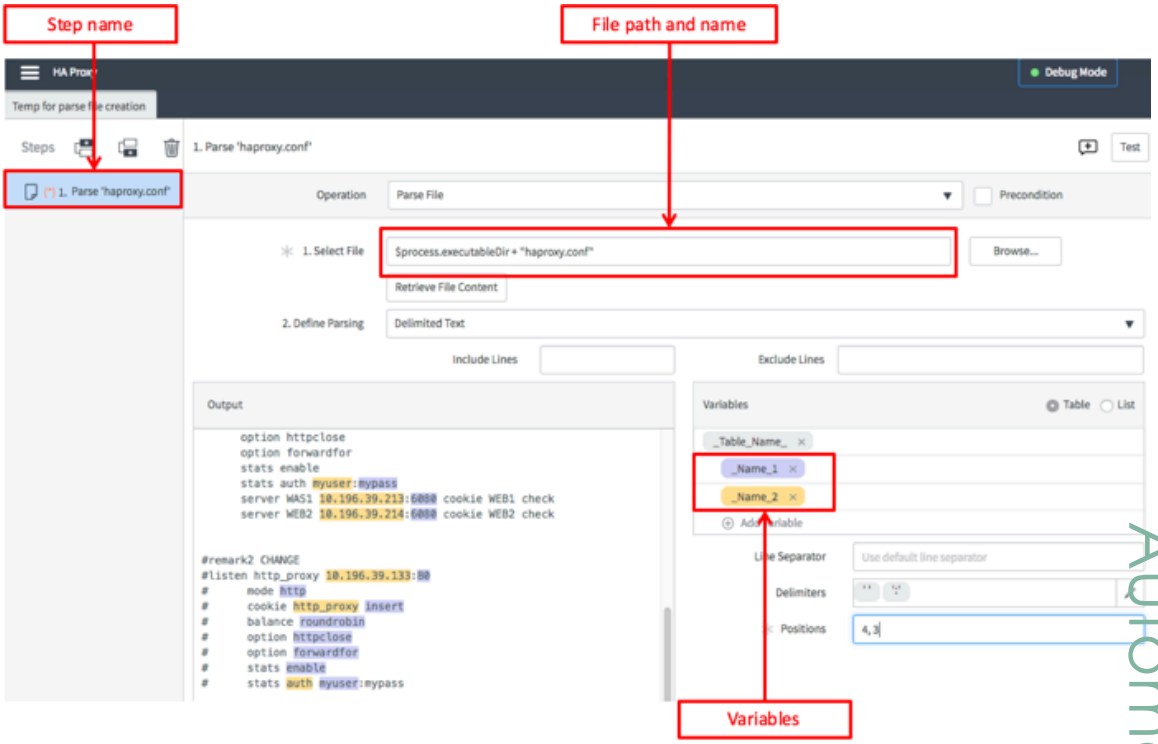
c. Klicken Sie auf **Analysedateischritt erstellen**, um diese Daten zum Erstellen des Musterschritts zu verwenden.

Der Musterdesigner zeigt den neuen Schritt mit dem Vorgang „Datei analysieren“ an. Er weist diesem Schritt automatisch den Namen im folgenden Format zu: Analyse <Dateiname>.

Der Musterdesigner legt automatisch den Dateinamen, den Dateipfad und die Analysestrategie für den Schritt fest. Außerdem werden Variablen erstellt, die Daten enthalten, nach denen Sie gesucht haben. Wenn eine Variable vorhanden ist, die den Dateipfad enthält, gibt der Musterdesigner diese Variable für den Pfad ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Wahlweise: Bei Bedarf können Sie die Analysestrategie ändern.

e. Benennen Sie den Abschnitt um, um einen aussagekräftigen Namen anzugeben, z. B. „HA-Proxy-Clientverbindung erkennen“.
Oder

Kopieren Sie den Schritt und fügen Sie ihn in den entsprechenden Verbindungsabschnitt ein.

10. Schließen Sie die Bearbeitung des Musters wie in Muster abschließen beschrieben ab.

Zugehörige Informationen

Datenverkehrsbasierte Erkennung in Service-Mapping

Datenverkehrsbasierte Erkennung für CI-Typen oder bestimmte CIs aktivieren

Von ITOM-Transparenz verwendete Erkennungsmuster

Muster abschließen

Nachdem Sie Ihr Muster definiert haben, machen Sie es für die Verwendung von Service-Mapping und Discovery bereit.

Vorbereitungen

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird

Es gibt mehrere Möglichkeiten, ein Muster nach der Erstellung oder Änderung abzuschließen:

- Speichern – Speichern Sie alle Informationen, die Sie für das Muster definiert haben, das einen Entwurf erstellt. Sie können den Musterentwurf jederzeit weiter bearbeiten. Service-Mapping und Discovery verwenden den Musterentwurf nicht für Erkennung und Zuordnung.

Automatische Übersetzung

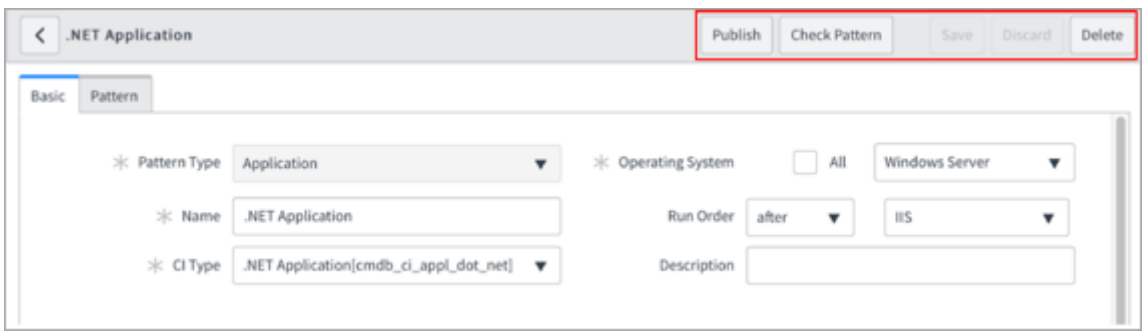
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Änderung verwerfen – Wenn Sie festgestellt haben, dass die Änderungen, die Sie an einem Muster vorgenommen haben, falsch sind, können Sie sie verwerfen.
- Überprüfen – Führen Sie das Muster für das relevante Konfigurationselement (CI) aus, um zu überprüfen, ob die dafür definierten Vorgänge korrekt sind. Überprüfen Sie Ihr Muster, bevor Sie es aktivieren. Diese Option ist nur für Anwendungsmuster verfügbar, die von Service-Mapping verwendet werden.
- Veröffentlichen – Service-Mapping und Discovery verwenden dieses Muster für Erkennung und Zuordnung. Eine neue Version dieses Musters wird erstellt. Der Status der zuvor verwendeten Musterversion ändert sich in Verlauf.

Prozedur

1. Vervollständigen Sie im Musterdefinitionsformular Ihre Musterdefinition, indem Sie eine oder mehrere der folgenden Aktionen ausführen.

Durchzuführende Aufgabe	Aktion
Muster speichern	Klicken Sie auf **Speichern**.
Unerwünschte Änderungen verwerfen	Klicken Sie auf **Verwerfen**.
Muster prüfen (nur für Anwendungsmuster verfügbar, die von Service-Mapping verwendet werden)	**a.** Klicken Sie auf **Muster prüfen**. **b.** Geben Sie Parameter für die Verbindung mit diesem CI ein. **c.** Klicken Sie auf **Verbinden**. **d.** Warten Sie, bis der Musterdesigner das Muster ausgeführt hat, und überprüfen Sie, ob keine Fehler vorhanden sind. **e.** Beheben Sie Fehler. Wenn keine Fehler auftreten, können Sie Ihr Muster veröffentlichen oder speichern.
Muster veröffentlichen	Klicken Sie auf **Veröffentlichen**.



2. Schließen Sie die Registerkarte „Musterdesigner“.

Muster aus einer Instanz in eine andere kopieren

Wenn Sie Muster von einer Instanz in eine andere kopieren möchten, erstellen Sie ein Update Set mit neuen oder geänderten Mustern mit zugehörigen Elementen in Ihrer Entwicklungsinstanz. Importieren Sie dann das Update Set in Ihre Produktionsinstanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird
Normalerweise pflegen Sie zwei ServiceNow-Instanzen in Ihrer Organisation: für die Produktion und für die Entwicklung. Erstellen oder ändern Sie Muster, testen Sie sie und überprüfen Sie die Ergebnisse in der Entwicklungsinstanz. Wenn Sie mit den Discovery-Ergebnissen zufrieden sind, exportieren Sie relevante Muster aus der Entwicklungsinstanz, um einen Update-Satz zu erstellen.

Update Sets ist eine Funktion von ServiceNow zum Übertragen von Anpassungen von einer Instanz zur anderen. Jedes Update Set wird in der Update Set-Tabelle [sys_update_set] gespeichert. Spezifische dem Update Set zugeordnete Anpassungen sind die Einträge in der Tabelle „Kundenupdate“ [sys_update_xml]. Diese erscheinen als zugehörige Liste im Datensatz des Update Sets. Die Methode zum Erstellen von Update Sets für Muster unterscheidet sich von der Erstellung von Update Sets für andere Anpassungstypen.

Warnung: Befolgen Sie immer dieses Verfahren, um Update Sets für Muster zu erstellen. Verwenden Sie nicht das standardmäßige Plattformverfahren zum Erstellen von Update Sets.

Je nach Umfang der Änderungen können Sie die folgenden Musterexportmethoden verwenden:

Muster exportieren

Diese Option erstellt ein Update Set mit den geänderten Mustern und den zugehörigen Elementen, die für das Funktionieren der Muster erforderlich sind. Die zugehörigen Elemente umfassen

- Erweiterungsabschnitte
- Nachverfolgte Dateien
- Zugehörige CI-Typen
- Klassifizierungsdatensätze
- Zugeordnete Skripts

Hinweis: Update Sets enthalten keine Änderungen an Skripteinbindungen in Mustern.

Muster mit CMDB-Elementen exportieren

Diese Option erstellt ein Update Set, das geänderte Muster mit den zugehörigen Elementen aus der vorherigen Option und den geänderten Mustern zugeordneten CMDB-Elementen enthält. Die CMDB-Elemente umfassen:

- Haupt-CI-Typ
- Einstiegspunkttypen
- Nachschlagetabellen
- Kennungen
- Regeln für das Hosting und den Abgleich

Das Update Set ist eine XML-Datei mit der folgenden Namenskonvention: sys_remote_update_set <alphanumerische Zufallszeichenfolge>.xml.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Führen Sie in der Entwicklungsinstanz die folgenden Schritte aus, um Muster zu exportieren:

   a. Navigieren zu **Musterdesigner** > **Discovery-Muster**.

   b. Wählen Sie Anwendungs- oder Infrastrukturmuster aus, die Sie exportieren möchten.

      Hinweis: Gemeinsame Bibliotheken können nicht exportiert werden.

   c. Klicken Sie am unteren Bildschirmrand auf **Aktionen für ausgewählten Zeilen**.

      Hinweis: Sie können nicht mehr als 20 Muster gleichzeitig für die Methode **Muster mit CMDB-Elementen exportieren** verwenden.

   d. Klicken Sie auf **Muster exportieren** oder **Muster mit CMDB-Elementen exportieren**.

   e. Wenn das System den Musterexport abgeschlossen hat, wird das Update Set erstellt.

   f. Klicken Sie zum Anzeigen der Liste der im Update Set enthaltenen Elemente in der Erfolgsmeldung auf **Protokolle anzeigen**.

   g. Klicken Sie auf **Schließen**.
   Die Update Set-Datei im XML-Format wird automatisch auf den Computer heruntergeladen.

   h. Speichern Sie die Update Set-Datei lokal zur zukünftigen Verwendung.

2. Führen Sie in der Produktionsinstanz die folgenden Schritte aus, um die angepassten Muster zu importieren:

   a. Erhöhen Sie die Berechtigungen auf die Rolle security_admin.

   b. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.

   c. Wählen Sie den Link **Update Set aus XML importieren aus**.

   d. Wählen Sie **Datei wählen aus,** und wählen Sie eine XML-Datei aus.

   e. Wählen Sie **Hochladen** aus.
   Die Anpassung ist jetzt als abgerufener Aktualisierungssatz mit Status *Geladen* verfügbar.

3. Zeigen Sie eine Vorschau des importierten Update Set an .
   Das System scannt und validiert das Update Set und zeigt seinen Inhalt auf der Registerkarte **Kunden-Updates** an.
4. Committen Sie den Update-Satz .
5. Klicken Sie in der Erfolgsmeldung auf **Schließen**.
   Die Produktionsinstanz enthält alle neuen oder geänderten Muster mit zugehörigen Elementen aus dem Update Set.
6. Laden Sie die aktualisierte Gruppe von Mustern und zugehörigen Elementen auf den MID-Server hoch:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Discovery** > **MID-Server**.

b. Alternativ navigieren Sie zu **Service-Mapping** > **MID-Server**.

c. Klicken Sie auf **Mustersynchronisierung mit MID**.

7. Wenn die Erkennung fehlschlägt oder das Ergebnis nicht den Erwartungen entspricht, starten Sie MID-Server erneut , um sicherzustellen, dass MID-Server den neuesten Mustersatz ausführt.

Zugehörige Informationen

System-Update Sets

Musterversion auswählen

Jedes Mal, wenn Sie ein Muster ändern und speichern, erstellen Sie eine Version dieses Musters. Wählen Sie aus, welche Musterversion Service-Mapping und Discovery für die Erkennung verwenden.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

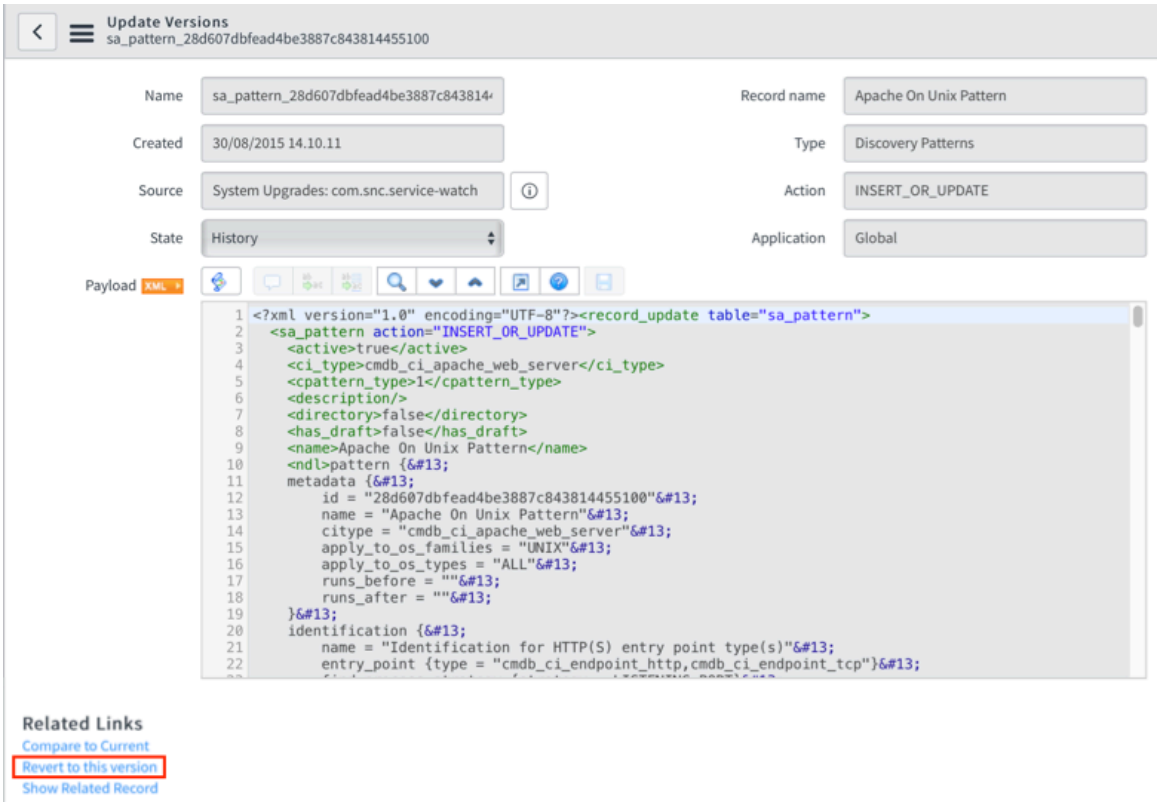
Standardmäßig wird die neueste Version für die Erkennung verwendet, Sie können jedoch eine beliebige andere Version auswählen.

Bei Bedarf können Sie Musterversionen vergleichen.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**.
2. Klicken Sie auf das erforderliche Muster.
   Das Formular für dieses Muster wird geöffnet.
3. Klicken Sie auf die Registerkarte **Muster**.
4. Scrollen Sie nach unten zum Abschnitt **Versionen**.
   Der Status der aktiven Musterversion, die Service-Mapping und Discovery verwenden, ist **Aktuell**.
5. Klicken Sie auf die Version, die Sie verwenden möchten.
6. Klicken Sie unter **Zugehörige Links** auf **Diese Version wiederherstellen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Diese Musterversion wird zur aktiven Version, die Service-Mapping und Discovery verwenden. Ihr Status wird zu „Aktuell“ geändert.

Musterversionen vergleichen

Wenn Sie mehrere Versionen desselben Musters haben, können Sie sie vergleichen, um zu entscheiden, welche Musterversion für die Erkennung verwendet werden soll.

Vorbereitungen

Erforderliche Rolle: pd_admin

Warum und wann dieser Vorgang ausgeführt wird

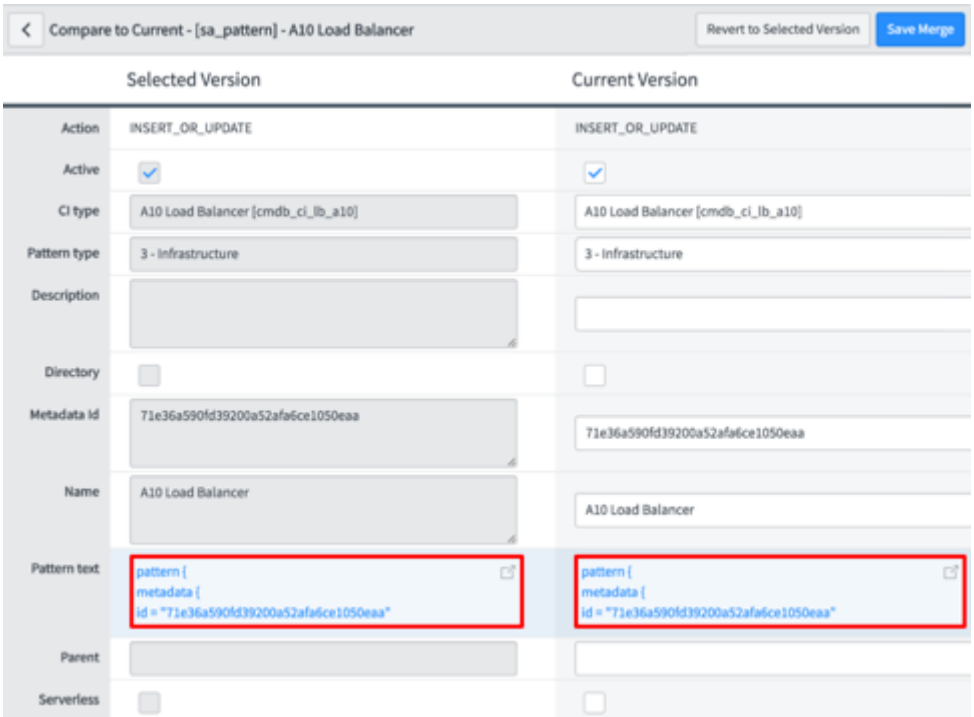
Service-Mapping und Discovery verwenden Muster in ihrem Erkennungsprozess. Jedes Mal, wenn Sie ein Muster ändern und speichern, erstellen Sie eine Version dieses Musters.

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**.
2. Klicken Sie auf das erforderliche Muster.
   Das Formular für dieses Muster wird geöffnet.
3. Klicken Sie auf die Registerkarte **Muster**.
4. Scrollen Sie nach unten zum Abschnitt **Versionen**.
   Der Status der aktiven Musterversion, die Service-Mapping und Discovery verwenden, ist **Aktuell**.
5. Klicken Sie auf die vorherige Musterversion, die Sie mit der aktuellen Version vergleichen möchten.
6. Klicken Sie unter **Zugehörige Links** auf **Mit Aktuellem vergleichen**.
7. Klicken Sie im Fenster „Mit Aktuellem vergleichen“ auf den Bereich **Mustertext** unter **Ausgewählte Version** oder **Aktuelle Version**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

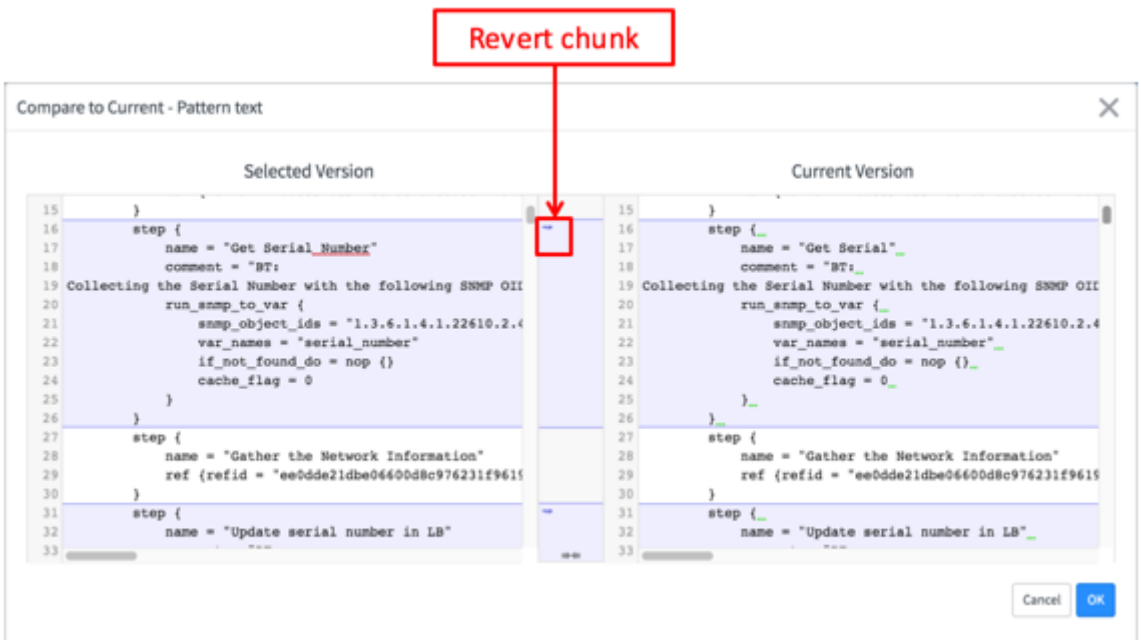


Die Textvergleichsansicht wird geöffnet und zeigt nebeneinander den Text der ausgewählten Musterversion und der aktuellen Musterversion an. Der Schritt, der den Unterschied enthält, wird hervorgehoben.

Hervorhebungsfarben geben die Art der Änderung an:

- Aktualisierter Schritt – violett
- Neue Zeile oder Zeichen – grün
- Zeile oder Zeichen gelöscht – rot

8. Überprüfen Sie die Unterschiede in den Musterversionen.
9. Klicken Sie ggf. auf **Block zurücksetzen**, um den Schritt in der aktuellen Version durch den Schritt aus der vorherigen Version zu ersetzen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Klicken Sie auf **OK**, wenn Sie fertig sind.
11. Wenn Sie Schritte aus der vorherigen Version kopiert haben und die Änderung speichern möchten, klicken Sie auf **Zusammenführung speichern**.

Aktivieren Sie ein deaktiviertes Muster

Wenn Sie ein standardmäßig deaktiviertes Muster für die Discovery verwenden möchten, aktivieren Sie es manuell.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Musterdesigner** > **Discovery-Muster**.
2. Suchen Sie im Feld **Name** nach dem entsprechenden Muster.
3. Wählen Sie das Muster aus.
4. Aktivieren Sie die Checkbox **Aktiv**.
5. Wählen Sie **Aktualisieren**.

ITOM Content Service

ServiceNow® ITOM Content Service bietet eine umfassende Transparenz der Produkte in Ihrer Infrastruktur. Die Klassifizierung von mit Predictive Intelligence identifizierten Prozessen ermöglicht eine umfassendere Erkennung und wöchentliche Aktualisierungen neuer Configuration Items in CMDB. Verwenden Sie Discovery-Administratorarbeitsbereich , um Vorschläge ITOM Content Service von zu überprüfen und zu verwalten.

ITOM Content Service Modell

Über ITOM Content Service

ITOM-Transparenz bietet mehrere Methoden zum Erkennen von Produkten in Ihrer Infrastruktur. Wenn Sie Discovery beispielsweise mit Muster für Discovery und Service-Mapping ausführen, sucht jedes Muster nach einer Version eines Produkts und kann eine detaillierte Transparenz der Produktinformationen bieten.

Ihre Infrastruktur nimmt mit großer Geschwindigkeit zu, und neue IT-Produkte werden schnell auf den Markt gebracht. Gleichzeitig benötigen Sie eine breitere und schnell aktualisierte Transparenz. Jede Woche identifiziert ITOM Content Service Produkte, die Sie derzeit verwenden, und stellt neue Configuration Items (CI) für Sie bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM Content Service bietet die folgenden Vorteile:

- Prüft jede Woche die Produkte, die Sie derzeit verwenden, und liefert neue Configuration Items (CIs).
- Basierend auf KI hilft es Ihnen, Fingerabdrücke laufender Prozesse und SNMP-System-OIDs zu identifizieren und die CIs zu erstellen, die Sie für die Überwachung Ihrer Infrastruktur benötigen.
- Identifiziert irrelevante Prozesse, die keine geeigneten Kandidaten für CIs sind.
- Erkennt eine höhere Anzahl von Produkten mithilfe von KI-Fähigkeiten, die laufende Anwendungsprozesse gruppieren und klassifizieren.

Vorteile der Integration von Software Asset Management mit ITOM Content Service

ITAM-Benutzer Software Asset Management (SAM) profitieren in mehrfacher Weise von der Integration mit ITOM Content Service.

- Verschaffen Sie sich einen Überblick über die Prozesse, die derzeit für die installierte Software ausgeführt werden. Auf diese Weise können Sie auch herausfinden, welche installierte Software keine laufenden Prozesse hat und möglicherweise redundant ist.
- ITOM Content Service ergänzt Software Asset Management in Fällen von Services, die keine Installation erfordern, z. B. eine Oracle -Datenbank, die als Service ausgeführt wird und nicht installiert ist. In Fällen wie diesem erstellt ITOM Content Service den Datensatz für installierte Software basierend auf der Kombination der Fingerabdruckdaten des Prozesses mit den von SAM erkannten Daten. Ohne ITOM Content Servicekönnen Sie diese Art der Transparenz nicht erreichen.
- Mithilfe dateibasierter Discovery-Funktionen kann ITOM Content Service eine laufende Systemdatei erkennen, die mit einer App identifiziert wird. Beispielsweise kann ITOM Content Service einen Datensatz für eine installierte Software mit einem Apache Kafka abgleichen, der eine `exe`– Datei ausführt. Weitere Informationen finden Sie unter File-based Discovery.

Weitere Informationen zu Software Asset Management finden Sie unter Software Asset Management Content Service .

Vorteile der Verwendung von Service-Mapping mit ITOM Content Service

Mit der neuesten Version von ITOM Content Servicekönnen Service-Mapping -Benutzer die Vorschläge Service-Fingerabdrücke von nutzen, um Anwendungsservices basierend auf klassifizierten Komponenten auszuwählen. Durch das Anzeigen von Komponentendetails wie Produkt, Produktkategorie, Herausgeber und Beschreibung können Sie fundierte Entscheidungen darüber treffen, welche Kandidaten in Anwendungsservices umgewandelt werden sollen. Sie können auch sehen, welche zusätzlichen Prozesse in den Service integriert werden können, da bestimmte Prozesse zusammen einen umfassenden Service bilden.

Sowohl ITOM Content Service -Vorschläge als auch Service-Fingerabdrücke bieten automatisierte, wöchentliche Vorschläge für Kandidaten, unterscheiden sich jedoch in einigen Punkten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich zwischen Vorschlägen von ITOM Content Service und Service-Fingerabdrücke

Name	Typ	Identifiziert	Fokus	Details zum Herausgeber	Standort
ITOM Content Service Vorschläge	Fingerabdrücke verarbeiten	Einzelne Prozesse, die Komponenten eines Service oder eigenständig sein können.	Bestimmte Aktionen eines Prozesses mit höherer Granularität	Herausgeber des Prozesses. Wenn ein Prozess Teil eines Service ist, aber einen anderen Herausgeber hat, stellt der Prozess nur Details zum eigenen Herausgeber bereit.	Registerkarte **„Inhalts** in Discovery-Administratorarbeits Inhalt 360
Service-Fingerabdrücke	Service-Fingerabdrücke	Services basierend auf klassifizierten Komponenten.	Der Service als Ganzes, der eine breitere Perspektive bietet	Herausgeber des Services. Wenn ein Prozess Teil eines Service ist, aber einen anderen Herausgeber hat, enthält der Servicefingerabdruck nur Details zum Herausgeber des Service.	Registerkarte **„Servic Fingerabdrücke“** im Arbeitsbereich Servi Mapping

Weitere Informationen zur Verwendung von Service-Fingerabdrücke in Service-Mappingfinden Sie unter Anwendungsservices zuordnen basierend auf Empfehlungen für automatisierte Services.

Für weitere Informationen über Kandidaten für Service-Fingerabdrücke, finden Sie unter KB1706310 .

ITOM Content Service mit Discovery-Administratorarbeitsbereich verwalten

Überprüfen Sie empfohlene Aktionen und Anwendungsvorschläge, und konfigurieren Sie die Discovery über Discovery-Administratorarbeitsbereich .

Beachten Sie, dass Discovery-Administratorarbeitsbereich ab dem Release Vancouver unterstützt wird.

Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich Inhalt 360.

Freigeben von Daten auf dem CDS

Das Continuance Delivery System (CDS) ist eine Technologie ServiceNow®, die Daten zwischen der Datenserviceinstanz , die Daten speichert und verteilt, und den Kundeninstanzen synchronisiert.

Wenn Sie die Freigabe von Anwendungsfingerabdruck-Prozessdaten für ITOM Content Service über das CDS aktivieren, können sie von KI-Bibliothekaren markiert und klassifiziert werden. ITOM Content Service liefert dann jede Woche neue CIs. Ihre Daten werden für

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Instanz ServiceNow® in einer sicheren Umgebung freigegeben. Sie können den Zugriff auf Ihre Daten steuern, indem Sie Berechtigungen im Discovery-Administratorarbeitsbereich festlegen.

Die beiden Optionen zum Freigeben Ihrer Daten sind:

- Freigeben der Fingerabdruckdaten laufender Prozesse, wodurch der Zugriff auf die Tabelle „Prozessgruppen“ [cmdb_process_groups] ermöglicht wird.
- Freigabe der SNMP-System-OIDs-Daten, wodurch der Zugriff auf die SNMP-OID-Tabelle [discovery_snmp_oid] ermöglicht wird.

Weitere Informationen zum Festlegen von Berechtigungen finden Sie unter Daten freigeben für ITOM Content Service

ITOM Content Service – Anwendungsfall

Dieser Anwendungsfall ITOM Content Service demonstriert, wie Unternehmen die Transparenz ihrer Umgebung verbessern können.

Übersicht über Anwendungsfälle

Die Klasse für Anwendungskonfigurationselemente (CIs) ist eine Schlüsselkomponente der Datenplattform einer Organisation innerhalb von Gemeinsames Servicedatenmodell (CSDM). Anwendungs-CIs helfen bei der Protokollierung von Softwareaktivitäten und unterstützen kritische IT-Vorgänge.

Viele Produkte und Anwendungen sind für wichtige Aufgaben auf Anwendungs-CIs angewiesen. Einige wichtige Beispiele:

- Service-Mapping: Verwendet Anwendungs-CIs zum Erstellen von Servicezuordnungen
- ITOM-Integrität: Überwacht die Integrität der Anwendung und löst Incidents mithilfe von Anwendungs-CIs
- IT Asset Management (ITAM): Verfolgt und verwaltet Softwareanwendungen und die zugehörigen Lizenzen mit Anwendungs-CIs
- IT Service Management (ITSM): Analysiert die Serviceauswirkung und berechnet den Blast-Radius mit Anwendungs-CIs
- Enterprise-Architektur (EA): Nutzt Anwendungs-CIs, um Geschäftsergebnisse zu generieren

Herausforderung

Eine große Organisation mit zahlreichen Anwendungen erfordert eine genaue Discovery. Die Verwaltung von Anwendungs-CIs ist von grundlegender Bedeutung, doch für das IT-Team ist es eine Herausforderung, die Transparenz über die steigende Infrastruktur zu wahren.

ITOM-Transparenz bietet verschiedene Methoden zum Erkennen von Produkten innerhalb der Infrastruktur einer Organisation, z. B. Muster für Discovery und Service-Mapping. Diese Methode bietet detaillierte Einblicke in die Informationen zu einem Produkt. Wenn eine breite Palette von Anwendungen verwendet wird, können nicht alle ein dediziertes Muster aufweisen. Wenn eine Anwendung kein dediziertes Muster hat, füllt Discovery nur die Tabelle „Laufender Prozess“ [cmdb_running_process], ohne das Produkt zu identifizieren oder ein CI dafür zu erstellen.

Ohne ein Anwendungs-CI fehlt dem Unternehmen der genaue Einblick in seine Infrastruktur, und es könnte Schwierigkeiten haben, die folgenden wichtigen Aktionen zu optimieren:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Binden Sie CIs mit Überwachungswarnungen und offenen Incidents bezüglich der CIs
- Planen Sie automatisierte Software-Upgrades
- Automatisieren Sie Skripts, um das Produkt zu optimieren oder Probleme zu beheben
- Führen Sie Folgenbewertungen und Change-Auswirkungsanalysen durch
- Erstellen Sie Sicherheits-Workflows

Lösung

ITOM Content Service verbessert den Erkennungsprozess durch Markieren und Klassifizieren von Prozessfingerabdrücken. Dieser Service bietet Details zum Herausgeber, zum Produkt und zur wichtigsten Komponente des CI. Im Gegensatz zur musterbasierten Discovery identifiziert ITOM Content Service Anwendungen direkt in der Umgebung des Unternehmens, ohne dass veröffentlichte Musterklassifizierer erforderlich sind. Dieser Ansatz ermöglicht die kontinuierliche Bereitstellung von Inhalten, ohne durch einen geplanten Releasezyklus eingeschränkt zu werden.

Beispiel: Discovery identifiziert den Prozess der Elipse Software E3 Database Engine (E3DBEngine.exe) und listet ihn in der Tabelle „Laufender Prozess“ [cmdb_running_process] auf. Wenn die Prozessklassifizierungsbedingung E3DBEngine.exe nicht zum Auslösen eines Musters festgelegt ist, wird kein Muster gestartet, und es wird kein CI erstellt. Bei ITOM Content Servicewird der Prozess E3DBEngine.exe jedoch mit Tags und Klassifizierungen versehen, sodass Discovery den Prozess beim nächsten Scan in ein CI umwandeln kann.

Ergebnis

Discovery erstellt mit ITOM Content Service einen CI-Datensatz durch Tagging und Klassifizierung des Herausgebers, des Produkts und der wichtigsten Komponente für alle -Anwendungen in der Umgebung des Unternehmens. Diese Methode bietet einen verbesserten und kontinuierlichen Einblick in die Anwendungslandschaft und ermöglicht eine effektive Überwachung, proaktive Maßnahmen und laufende Optimierung.

Installieren Sie ITOM Content Service mit Discovery dem -Administrator-Arbeitsbereich

Installieren Sie ITOM Content Service über den Discovery -Administratorarbeitsbereich, um die Erstellung von Konfigurationselementen basierend auf Anwendungsfingerabdrücken zu verwalten und zu überwachen.

Vorbereitungen

Stellen Sie sicher, dass die folgenden Anwendungen aktuell sind:

- Discovery
- Muster für Discovery und Service-Mapping

Erforderliche Rolle: discovery_admin oder admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich**.
2. Wählen Sie im Abschnitt **„Inhaltsservice-Setup“ App herunterladen aus**.
3. Aktualisieren Sie die Webseite.
   Die Option **Aktivieren** wird im Administrator-Arbeitsbereich Discovery angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Daten freigeben für ITOM Content Service

Zugehörige Informationen

ITOM Content Service

Discovery-Administratorarbeitsbereich

Daten freigeben für ITOM Content Service

Steuern Sie die Datenfreigabe, indem Sie die Freigabeoptionen für ITOM Content Service im Administrator-Arbeitsbereich von Discovery aktivieren oder deaktivieren.

Vorbereitungen
Installieren Sie ITOM Content Service mit Discovery dem -Administrator-Arbeitsbereich

Erforderliche Rolle: discovery_admin oder admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich**.
2. Geben Sie an, ob und welche Daten Sie für KI-Bibliothekare freigeben möchten.

Option	Aktionen
Aktivieren Sie die Freigabe Ihrer Daten	**a.** Wählen Sie auf der Kachel **Inhaltsservice-Setupdie Option Aktivieren aus**. **b.** Lesen Sie die Vereinbarung, und wählen Sie **Ja, ich habe die Teilnahmevereinbarung gelesen und stimme zu**. **c.** Wählen Sie **Weiter**. **d.** Wählen Sie Ihr Setup aus. ▪ Erweitert: Aktiviert einen umfassenden Satz von Klassifizierern für erweiterte Transparenz ▪ Standard: Aktiviert die gängigsten Klassifizierer. ▪ Anwenderdefiniert: Sie wählen aus, welche Klassifizierer aktiviert werden sollen. **e.** Aktivieren Sie die Datenfreigabeoptionen, die Sie verwenden möchten. ▪ Fingerabdruckdaten des laufenden Prozesses: Gibt Metadaten und einige Beispiele für Prozesse aus der Tabelle „Prozessgruppen“ frei. ▪ SNMP-System-OIDs: Gibt Metadaten und einige Beispiele für Prozesse aus der SNMP-OID-Tabelle frei. **f.** Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktionen
	g. Wenn die Aktivierung abgeschlossen ist, wählen Sie **Startseite**, um zum Arbeitsbereich zurückzukehren. Die Kachel **„Inhaltsservicevorschläge“** ersetzt die Kachel **„Inhaltsservice-Setup“**. Im neuen Abschnitt **„Inhaltsservice-Setup“** wird ein grünes Häkchen angezeigt, das angibt, dass Sie ITOM Content Serviceaktiviert haben.
Deaktivieren Sie die Berechtigungen für die Datenfreigabe	**a.** Wählen Sie im Abschnitt **„Inhaltsservice-Setup“Setup konfigurieren aus**. **b.** Deaktivieren Sie eine Option oder beide Optionen. **c.** Wählen Sie **Speichern**. **d.** Wenn die Einstellung abgeschlossen ist, wählen Sie **Startseite**, um zum Arbeitsbereich zurückzukehren.
Deaktivieren Sie die Freigabe Ihrer Daten .	**a.** Wählen Sie im Abschnitt **„Inhaltsservice-Setup“die Option Deaktivieren aus**. **b.** Wählen Sie **Deaktivieren aus**. **c.** Lesen Sie die Systemmeldung **zum Deaktivieren von,** *ITOM Content Service* und wählen Sie **Deaktivieren aus**. **d.** Wenn der Abwählvorgang abgeschlossen ist, wählen Sie **Startseite**, um zum Arbeitsbereich zurückzukehren. ITOM Content Service verwendet Ihre Daten nicht mehr, und in Ihrem Arbeitsbereich werden nur von Ihnen definierte CIs angezeigt. Weitere Informationen finden Sie unter Discovery-Administratorarbeitsbereich.

Zugehörige Informationen

ITOM Content Service

Aktivieren Sie die Discovery mit ITOM Content Service

Überprüfen Sie die Vorschläge ITOM Content Service für die Anwendungs-Discovery, und aktivieren Sie die Discovery-Klassifizierungen, um die Erstellung von Konfigurationselementen zu ermöglichen.

Vorbereitungen

ITOM Content Service muss installiert sein. Weitere Informationen finden Sie unter Installieren Sie ITOM Content Service mit Discovery dem -Administrator-Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM Content Service muss aktiv sein. Weitere Informationen finden Sie unter Daten freigeben für ITOM Content Service.

Erforderliche Rolle: discovery_admin oder admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Content 360**.
2. Wählen Sie die Kachel **Inhaltsservicevorschläge**.
3. Überprüfen Sie die Inhaltsservice-Vorschläge für die Discovery nach Produkt.
   - Um die Liste zu filtern, wählen Sie die Produkte auf der Registerkarte **Inhaltsservicevorschläge** aus.
   - Um die Beschreibung und Details eines Produkts zu überprüfen, wählen Sie den Link in der Spalte **Name** aus.
4. Wählen Sie das Produkt aus, für das Sie Discovery aktivieren möchten.
5. Aktivieren Sie Discovery-Klassifizierungen nach Produktkategorien.

   Hinweis: Die Anzahl der zu aktivierenden Klassifizierer wird auf der Schaltfläche **Aktivieren** angegeben.

   - Um die Discovery nach Produktkategorien zu aktivieren, aktivieren Sie die Kontrollkästchen Produktkategorien, aktivieren Sie das Kontrollkästchen neben der Spalte **Name**, und wählen Sie **Aktivieren**aus.
   - Um die Discovery nach einzelnen Produkten zu aktivieren, wählen Sie das Produkt in der Spalte **Name** aus, und wählen Sie **Aktivieren**aus.

Ergebnisse

Die neuen Configuration Items werden zu CMDB hinzugefügt, wenn Discovery das nächste Mal einen Zeitplan ausführt. Der Administrator-Arbeitsbereich Discovery listet dann die hinzugefügten CIs auf und entfernt sie aus der Liste der vorgeschlagenen Anwendungen.

Zugehörige Informationen

ITOM Content Service

Discovery-Administratorarbeitsbereich

Erkennen Sie Daten der installierten Software mit ITOM Content Service

Verwenden Sie ITOM Content Service und ITSM Software Asset Management, um installierte Software zu erkennen, die nicht automatisch mit Software Asset Management Core oder Software Asset Management Professional oder dateibasiert Discoveryerkannt wird.

Vorbereitungen

ITOM Content Service muss installiert sein. Weitere Informationen finden Sie unter Installieren Sie ITOM Content Service mit Discovery dem -Administrator-Arbeitsbereich

ITOM Content Service muss aktiv sein. Weitere Informationen finden Sie unter Daten freigeben für ITOM Content Service.

Software Asset Management Core oder Software Asset Management Professional Plugins müssen installiert sein.

Das dateibasierte Plugin Discovery muss installiert sein.

Erforderliche Rolle: discovery_admin oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Intelligenter Inhalt** > **Intelligente Inhaltskategorien**.
2. Aktivieren Sie die installierte Softwarekategorie.
   a. Doppelklicken Sie auf das Feld **Installierte Software erstellen**.
   b. Wählen Sie in der Liste **Wahr**aus.
   c. Überprüfen Sie den Wert, indem Sie das grüne Häkchenwählen.

Ergebnisse

Der neue Datensatz für installierte Software wird erstellt und der Liste der CI-Softwareinstallationen hinzugefügt.

Zugehörige Informationen

ITOM Content Service

ITOM Content Service – Referenz

Mit ITOM Content Service können Sie festlegen, dass CMDB jede Woche mit neuen Daten gefüllt wird. Erfahren Sie in den Knowledge Base-Artikeln mehr über die veröffentlichten Kandidaten für Konfigurationselemente.

Weitere Informationen zu den CI-Kandidaten der Anwendung finden Sie unter KB1584650 .

Weitere Informationen zu den SNMP-OID-CI-Kandidaten finden Sie unter KB1702434 .

Um mehr über die Kandidaten Service-Fingerabdrücke für zu erfahren, finden Sie unter KB1706310 .

Tag-Governance

Eine effektive Tag-Verwaltung verbessert die Berichterstellung und die allgemeine Effizienz des Betriebsmanagements. Verwenden Sie die App ServiceNow® Tag-Governance, um lokale oder cloudbasierte Ressourcen zu identifizieren und zu korrigieren, die inkonsistent sind und nicht den Tag-Richtlinien Ihres Unternehmens entsprechen.

Apps im Store anfordern

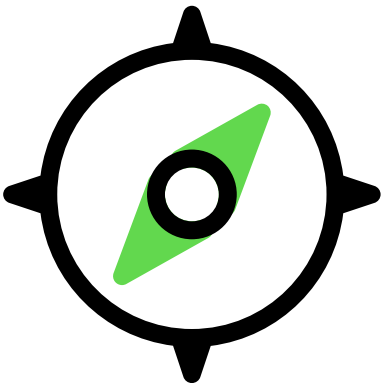
Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Erste Schritte

Ein Tag ist ein Schlüssel-Wert-Paar, das einem CI oder einer Cloud-Ressource zugewiesen ist. Ihre Organisation kann Tags zur Kategorisierung von Assets verwenden, um die Transparenz von Cloud-Nutzung und Kosten zu verbessern.

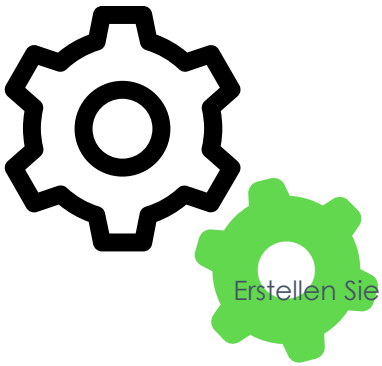
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untersuchen



Erfahren Sie mehr über Tag-Governance

Konfigurieren

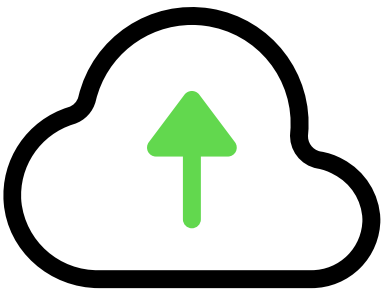


Erstellen Sie Tag-Richtlinien

Installieren Sie die App.

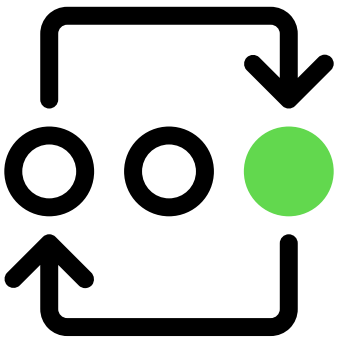
Definieren Sie Tag-Standards, die geprüft werden.

Cloud-Tags werden aktualisiert



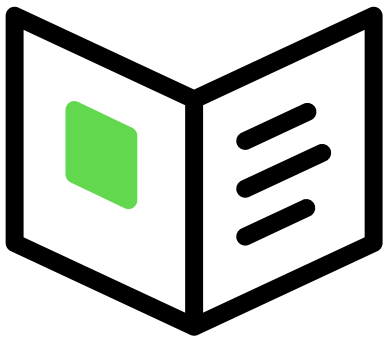
Echtzeitaktualisierung von Tags für Cloud-Ressourcen.

Beheben



Beheben Sie Tag-Probleme

Referenz



Zusätzliche Informationen zu Formularen und Einstellungen.

Automatische Übersetzung

Problembehandlung und Hilfe

- Stellen Sie Fragen, und erkunden Sie andere Ressourcen für Tag-Governance in ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Tag-Governance erkunden

Erfahren Sie mehr über Tag-Governance -Berichte und Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tag-Governance – Übersicht

Eine effektive Tag-Verwaltung verbessert die Berichterstellung und die allgemeine Effizienz des Betriebsmanagements. Verwenden Sie die App ServiceNow® Tag-Governance, um lokale oder cloudbasierte Ressourcen zu identifizieren und zu korrigieren, die inkonsistent sind und nicht den Tag-Richtlinien Ihres Unternehmens entsprechen.

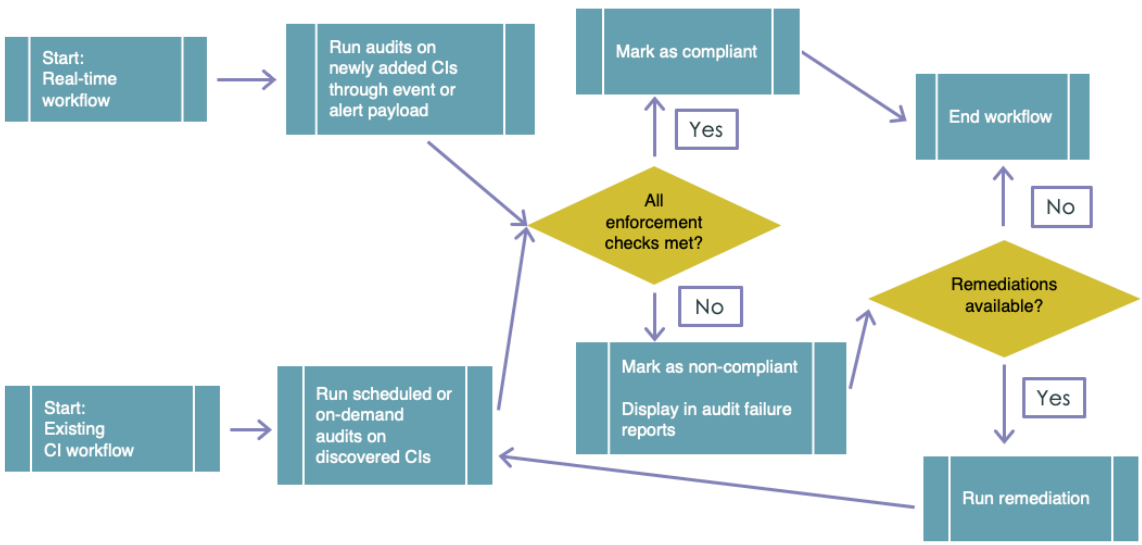
Tag-Governance Anwender

Anwender

Anwender	Beschreibung
Tag-Governance-Administrator	Verantwortlich für die Pflege einheitlicher Richtlinien für die Tag-Verwaltung und die Sicherstellung, dass Ressourcen für Transparenz, Compliance und Kostenmanagement ordnungsgemäß gekennzeichnet werden.
Berichtsanzeige	Nur Ansichtsberechtigungen: • Überwachen Sie Berichte von Audit-Ausführungen • Analysieren Sie die Daten, um Einblicke zur Steuerung von Aktionen abzuleiten

Tag-Governance – Workflow

Tag-Governance – Workflow



Tag-Governance – Vorteile

Tag-Governance – Vorteile

Vorteil	Funktion	Anwender
Implementieren Sie die Verarbeitung von Cloud-Ereignissen, und konfigurieren Sie eine Tag-Richtlinie, um Cloud-Ressourcen-Tags automatisch in Echtzeit zu aktualisieren.	Es werden Echtzeit-Updates an Tags für Cloud-Ressourcen durchgeführt	Cloud-Administratoren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tag-Governance – Vorteile (Fortsetzung)

Vorteil	Funktion	Anwender
Tag-Governance unterstützt die Domänentrennung, sodass Sie Daten, Prozesse und Verwaltungsaufgaben logisch gruppieren und in verschiedene Domänen trennen können. Dies ermöglicht eine genaue Kontrolle von Aspekten wie Benutzerzugriff und Datentransparenz.	Domain Separation und Tag-Governance	Cloud-Administratoren
Überprüfen Sie nicht konforme CIs, die von Tag-Audits gekennzeichnet wurden, und beheben Sie sie, indem Sie die erforderlichen Tags hinzufügen.	Tag-Auditfehler in der Vorschau anzeigen und korrigieren	Tag-Administratoren

erkunden

Beitrag von Discovery zu Tag-Governance

Die Funktionen Discovery und Cloud-Discovery erkennen alle Ressourcen in CMDB sowie Cloud-Ressourcen von Cloud-Anbietern wie Amazon AWS Cloud, Microsoft Azure Cloudund Google Cloud Platform (GCP).

Tag-Governance Dashboard – Registerkarte „Übersicht“.

Auf der Registerkarte **Übersicht** werden die Integrität und Compliance von CIs basierend auf Tag-Audits nachverfolgt. Interaktive Widgets enthalten Informationen, mit denen Sie den Compliance-Status von Tags und die am häufigsten verwendeten und die am wenigsten verwendeten Tags anzeigen und analysieren können.

Tag-Governance Dashboard – Registerkarte „Richtlinienansicht“.

Verwenden Sie die Registerkarte Richtlinienansicht, um die Tag-Compliance gefiltert nach Cloud-Servicekonto, Tag-Richtlinie und Rechenzentrum anzuzeigen und zu analysieren. Mithilfe von Filtern können Sie sich auf die Verbesserung der Tag-Compliance konzentrieren.

Tag-Governance Dashboard: Registerkarte „Wirkungsgrad“.

Auf der Registerkarte Effizienz werden die Ergebnisse von Tag-Audits als Tag-Integritätsbewertungen und Compliance-Abdeckung von CIs angezeigt. Interaktive Widgets zeigen den Status der Tag-Abdeckung und Tagging-Trends im Zeitverlauf an.

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Tag-Governance finden Sie unter:

- Tag-Governance konfigurieren
- Tag-Governance verwenden
- Tag-Governance – Referenz

Beitrag von Discovery zu Tag-Governance

Die Funktionen Discovery und Cloud-Discovery erkennen alle Ressourcen in CMDB sowie Cloud-Ressourcen von Cloud-Anbietern wie Amazon AWS Cloud, Microsoft Azure Cloudund Google Cloud Platform (GCP).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Rolle der Discovery

Mit Discovery und Cloud Provisioning and Governance können die von allen wichtigen Cloud Providern und Container-Ökosystemen verwendeten Tags anhand von Service-Mapping-Mustern erkannt werden. Sobald die Tags erkannt wurden, kann Service-Mapping Anwendungsservices erstellen, die auf den Tags basieren. In der Regel verwenden Unternehmen Tags in virtualisierten, hyperkonvergenten oder Multi-Cloud-Infrastrukturen. Beispiele für die dafür verwendeten Infrastrukturtypen und Tags finden Sie unter Tag-basierte Discovery in Service-Mapping.

Discovery erfasst auch Cloud-Tags, die für jede virtuelle Maschine (VM) spezifisch sind, und speichert sie in der Tabelle „Schlüsselwert“ [cmdb_key_value].

Der Discovery-Prozess erkennt auch Tags, die CIs zugeordnet sind. Wenn Ihre Organisation jedoch keine einheitlichen Tagging-Standards oder -Begriffe (Schlüssel-Wert-Paare) verwendet, wird die Verwaltung von CIs mit Tags jedoch schwierig.

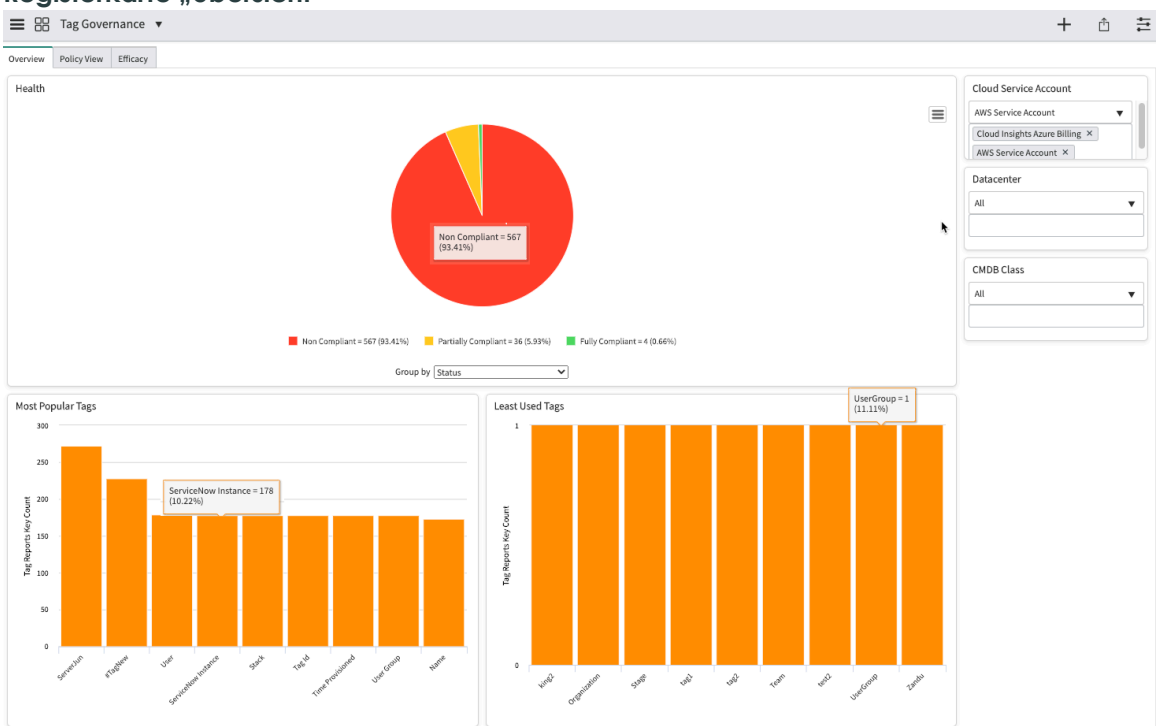
Tag-Governance Dashboard – Registerkarte „Übersicht“.

Auf der Registerkarte **Übersicht** werden die Integrität und Compliance von CIs basierend auf Tag-Audits nachverfolgt. Interaktive Widgets enthalten Informationen, mit denen Sie den Compliance-Status von Tags und die am häufigsten verwendeten und die am wenigsten verwendeten Tags anzeigen und analysieren können.

Zugriff auf das -Dashboard

Melden Sie sich als Tag-Governance -Administrator (sn_itom_tag.tag_governance_admin) an, um Berichte zu konfigurieren und der Tag-Governance-Betrachter (sn_itom_tag.tag_reports_viewer) die Berichte anzuzeigen. Um auf das Dashboard zuzugreifen, navigieren Sie zu**Tag-Governance** > **Dashboard**.

Registerkarte „Übersicht“



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filter werden angewendet

Auf der Registerkarte Health (Integrität) wird der kumulative Status der Tag-Integrität aller CIs angezeigt, für die die Tag-Audits ausgeführt wurden. Für jede Kategorie werden der prozentuale Anteil und die Anzahl der CIs mit Status „Übereinstimmung“ angezeigt.

Standardmäßig werden Daten nach Status gruppiert. Sie können die Ergebnisse auch mit den Filtern in der Liste **Group By** (Gruppieren nach) gruppieren.

Verwenden Sie die folgenden interaktiven Filter, um Berichte zu verfeinern:

- **Cloud Service Account (Cloud-Servicekonto)**
- **Logisches Rechenzentrum**
- **CMDB Class** (CMDB-Klasse)

> **Hinweis:** Der Filter **CMDB Class** (CMDB-Klasse) gilt nur für den Bericht zur **Tag Health** (Tag-Integrität). Die Verwendung dieses Filters wirkt sich nicht auf die Ergebnisse der Berichte **Most Popular Tags** (Beliebteste Tags) und **Least Used Tags** (Am wenigsten verwendete Tags) aus.

Sie können beispielsweise eine Kombination der Filter **Cloud Service Account** (Cloud-Servicekonto), **CMDB Class** (CMDB-Klasse) und **Logical Datacenter** (Logisches Rechenzentrum) verwenden. Dann können Sie die Tag-Auditergebnisse für die VM-Instanzen anzeigen, die einem bestimmten Cloud-Servicekonto zugeordnet sind und sich in einem bestimmten logischen Rechenzentrum befinden.

Berichte

Tag-Audits werden für alle erkannten Ressourcen in der Tabelle CMDB CI [*cmdb_ci*] ausgeführt. Auf der Registerkarte werden Integritäts- und Compliance-Ergebnisse für erkannte CIs angezeigt.

Widget	Beschreibung	Beschreibung
Gesundheitswesen	Kreisdiagramm	Prozentsatz und Anzahl aller CIs in den folgenden Kategorien: • Nicht konform: CIs, die keine der Tag-Richtlinienanforderungen erfüllen. • Teilweise konform: CIs, die einige Tag-Richtlinienanforderungen erfüllen. • Vollständig konform: CIs, die alle Tag-Richtlinienanforderungen erfüllen Wählen Sie ein zugehöriges Segment oder eine zugehörige Kategorie aus, um einen detaillierteren Bericht anzuzeigen.
Most Popular Tags (Beliebteste Tags)	Balkendiagramm	Die zehn am häufigsten verwendeten Tags für alle erkannten CIs, die von Tag-Audits ausgewertet werden.

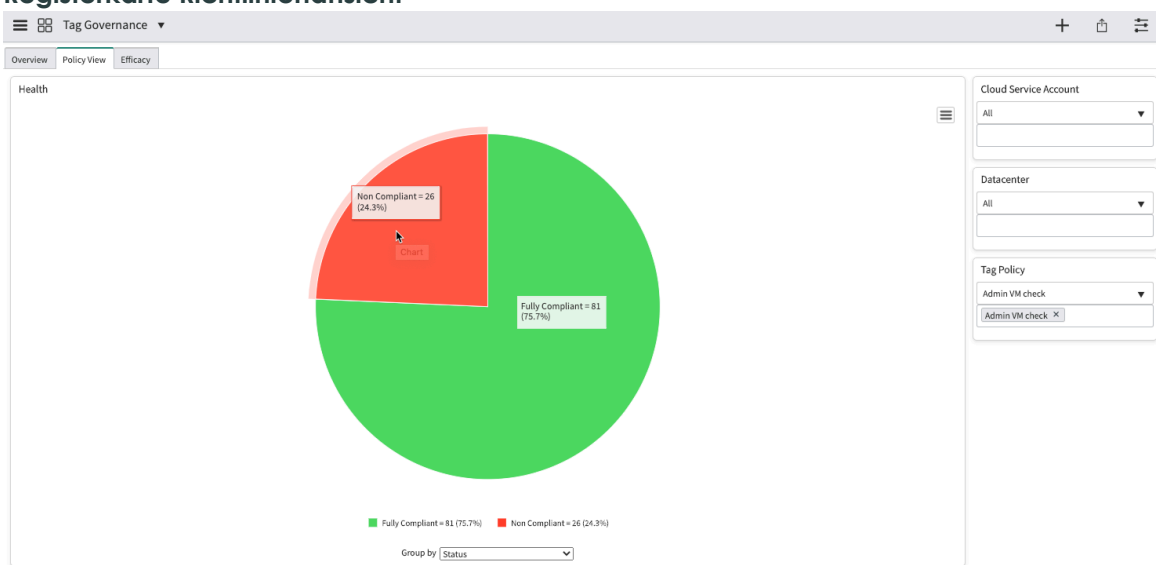
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Widget	Beschreibung	Beschreibung
		• Zeigen Sie auf einen Balken, um den entsprechenden Prozentsatz der Gesamtzahl und die Anzahl der Vorkommen des Tags anzuzeigen. • Wählen Sie einen Balken aus, um die Liste der CIs mit diesem Tag anzuzeigen.
Least Used Tags (Am wenigsten verwendete Tags)	Balkendiagramm	Die zehn am wenigsten verwendeten Tags für alle erkannten CIs, die von Tag-Audits ausgewertet werden. • Zeigen Sie auf einen Balken, um den entsprechenden Prozentsatz der Gesamtzahl und die Anzahl der Vorkommen des Tags anzuzeigen. • Wählen Sie einen Balken aus, um die Liste der CIs mit diesem Tag anzuzeigen.

Tag-Governance Dashboard – Registerkarte „Richtlinienansicht“.

Verwenden Sie die Registerkarte Richtlinienansicht, um die Tag-Compliance gefiltert nach Cloud-Servicekonto, Tag-Richtlinie und Rechenzentrum anzuzeigen und zu analysieren. Mithilfe von Filtern können Sie sich auf die Verbesserung der Tag-Compliance konzentrieren.

Registerkarte Richtlinienansicht



Auf der Registerkarte Richtlinienansicht wird die kumulative Tag-Integrität aller geprüften CIs angezeigt. Das Richtlinien-Dashboard stellt die Tag-Richtlinien-Compliance für erkannte CIs in einem interaktiven Kreisdiagramm dar. Die Ergebnisse werden in den folgenden Kategorien aufgelistet.

- Vollständig konform: CIs, die alle Tag-Richtlinienanforderungen erfüllen
- Nicht konform: CIs, die die Tag-Richtlinienanforderungen nicht erfüllen.

Verwenden Sie die folgenden interaktiven Filter, um Berichte zu verfeinern:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

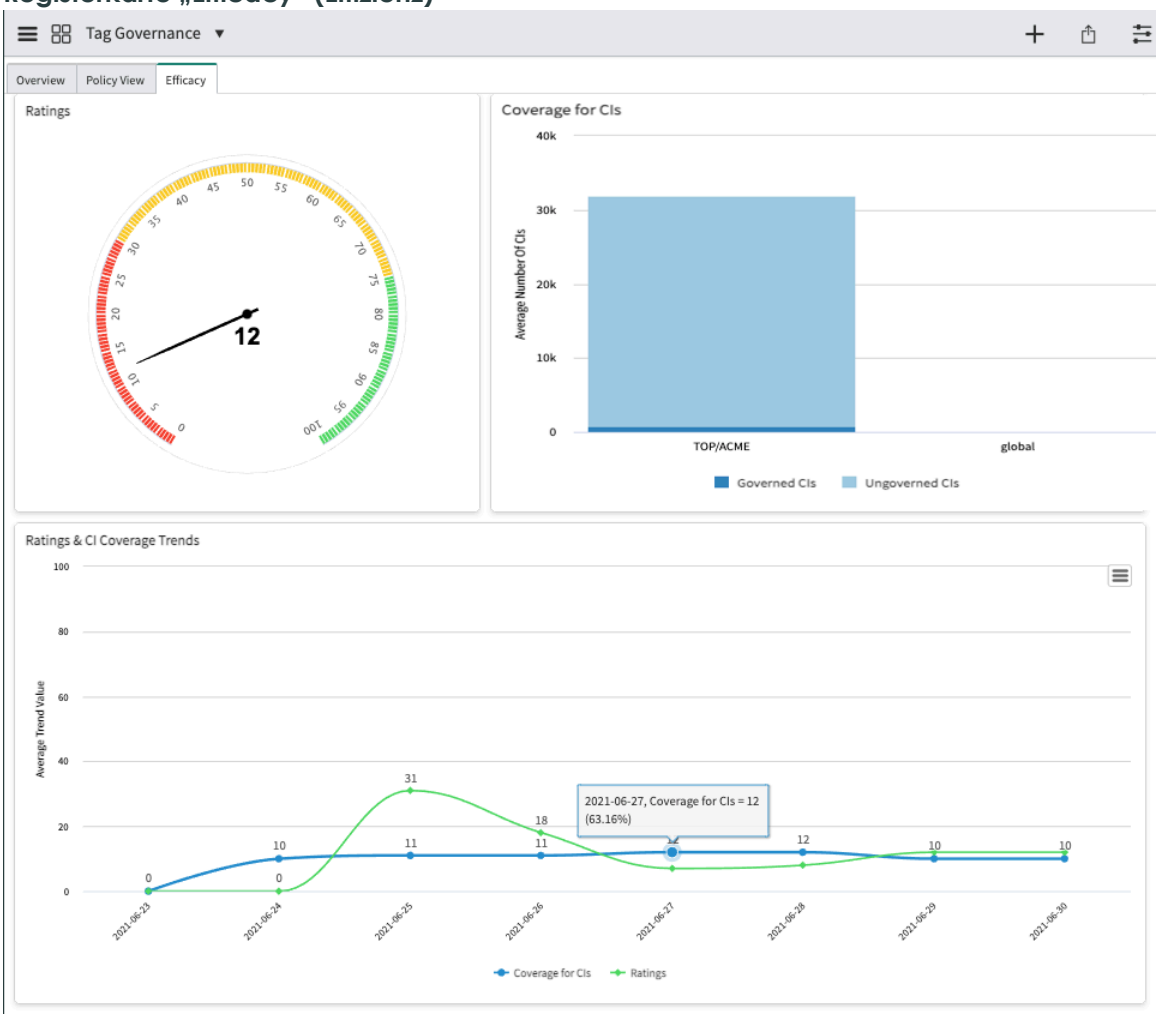
- **Cloud Service Account (Cloud-Servicekonto)**
- **Rechenzentrum**
- **Tag-Richtlinie**

Beispielsweise können Sie eine Kombination aus den Filtern für **Cloud-Servicekonten**, **Tag-Richtlinien**und **Rechenzentrum** verwenden, um Tag-Audit-Ergebnisse für CIs anzuzeigen, die den von Ihnen konfigurierten Filtern entsprechen.

Tag-Governance Dashboard: Registerkarte „Wirkungsgrad“.

Auf der Registerkarte Effizienz werden die Ergebnisse von Tag-Audits als Tag-Integritätsbewertungen und Compliance-Abdeckung von CIs angezeigt. Interaktive Widgets zeigen den Status der Tag-Abdeckung und Tagging-Trends im Zeitverlauf an.

Registerkarte „Efficacy“ (Effizienz)



Bewertungen

Sehen Sie sich den Bericht „Bewertungen“ an, um die Qualität der CI-Tag-Integrität zu überprüfen. Die Punktzahl basiert auf einem Algorithmus, der die folgenden Informationen und Daten berücksichtigt, die bei der Ausführung von Tag-Audits gesammelt wurden:

- Compliance der Tag-Richtlinie
- Allgemeine Compliance der CI-Tags

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abdeckung für CIs

Der Bericht „Abdeckung für CIs“ zeigt die Anzahl der CIs in CMDB an, die von Tag-Richtlinien gesteuert werden, und den Prozentsatz aller CIs, die gesteuert werden. Sie können diese Informationen verwenden, um die Abdeckung von Tag-Richtlinien zu verbessern.

Ratings and CI Coverage Trends (Bewertungen und Trends der CI-Abdeckung)

Der Bericht **„Trends“** zeigt den durchschnittlichen Trendwert der Tag-Governance-Bewertung und der Abdeckung von CIs im Zeitverlauf an. Der Bericht bietet Einblicke in die Entwicklung der Tag-Qualität und der Tag-Abdeckung im Laufe der Zeit.

Berichte

Titel	Typ	Beschreibung
Ratings (Bewertungen)	Messbericht	Punktzahl, die die allgemeine Tagging-Qualitätsbewertung aller CIs angibt. Dieser Wert basiert auf einem Algorithmus, der die Anzahl der CIs verwendet, die von der Tag-Richtlinie abgedeckt werden, und die Gesamtzahl der CIs, die von der Tag-Richtlinie zertifiziert werden.
Abdeckung für CIs	Gestapelter Balkenbericht	Prozentsatz und Anzahl aller CIs, die von Tag-Richtlinien gesteuert werden, im Vergleich zu allen CIs in CMDB. Der Wert basiert auf der Gesamtzahl der CIs, die von Tag-Richtlinien gesteuert werden, geteilt durch die Gesamtzahl der CIs in CMDB. Ein einzelner Balken stellt die CI-Abdeckungsdaten jeder Domäne dar.
Trends	Linientrendbericht	Leistungstrends von Tag-Qualität und Tag-Abdeckung im Zeitverlauf.

Automatische Übersetzung

Tag-Governance konfigurieren

Installieren Sie die App Tag-Governance, um Tag-Audits auszuführen, das Dashboard „Tag Data Governance“ anzuzeigen und eine Tag-Korrektur durchzuführen.

Konfiguration – Übersicht

- Domain Separation und Tag-Governance

  Die Domänentrennung wird in Tag-Governance unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Tag-Governance installieren

  Installieren Sie die App Tag-Governance, um Tag-Audits auszuführen, das Dashboard „Tag Data Governance“ anzuzeigen und eine Tag-Korrektur durchzuführen.

Tag-Governance installieren

Installieren Sie die App Tag-Governance, um Tag-Audits auszuführen, das Dashboard „Tag Data Governance“ anzuzeigen und eine Tag-Korrektur durchzuführen.

Vorbereitungen

- Stellen Sie sicher, dass Sie Muster für Discovery und Service-Mapping für tagbasierte Erkennung verwenden.
- Installieren Sie die App ServiceNow Cloud Access Interface für die Cloud-Korrektur.

Erforderliche Rolle: sn_itom_tag.tag_governance_admin, admin

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **ServiceNow Store**.
2. Verwenden Sie das Suchfeld, um die Anwendung Tag-Governance zu finden, und wählen Sie **Installieren**aus.

Nächste Maßnahme

Konfigurieren Sie die Richtlinien Tag-Governance, die für erkannte Ressourcen ausgeführt werden sollen. Weitere Informationen finden Sie unter Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance.

Tag-Governance verwenden

Verwenden Sie die App ServiceNow® Tag-Governance, um lokale oder cloudbasierte Ressourcen zu identifizieren und zu korrigieren, die inkonsistent sind und nicht den Tag-Richtlinien Ihres Unternehmens entsprechen.

Tag-Governance-Aufgaben

- Tag-Governance -Richtlinien werden erstellt

  Konfigurieren Sie Tag-Richtlinien, die die Kriterien für Tag-Audits für erkannte Cloud-Ressourcen oder CIs definieren. Zeigen Sie Audit-Ergebnisse zu Tag-Qualität und -Compliance im Dashboard „Tag-Integrität“ an. Sie erstellen Tag-Richtlinien, die den Umfang und die Anforderungen der verschiedenen Gruppen in Ihrer Organisation unterstützen, damit alle Benutzer davon profitieren können.

- Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance

  Konfigurieren Sie Tag-Richtlinien, die die Kriterien für Tag-Audits für erkannte Cloud-Ressourcen oder CIs definieren. Zeigen Sie Audit-Ergebnisse zu Tag-Qualität und -Compliance im Dashboard „Tag-Integrität“ an.

- Konfigurieren Sie Korrekturrichtlinien für Tag-Audit-Ergebnisse

  Konfigurieren Sie Korrekturoptionen, zeigen Sie eine Vorschau an, generieren Sie Schlüssel, und führen Sie Aktionen aus, um Nichteinhaltung oder Fehler zu beheben, die auf Tag-Audit-Berichten basieren.

- Tag-Auditfehler in der Vorschau anzeigen und korrigieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basierend auf den von Ihnen erstellten Tag-Richtlinien können Sie eine Vorschau der Korrektur-Flows anzeigen und fehlende Tags für nicht konforme CIs automatisch generieren.

- Es werden Echtzeit-Updates an Tags für Cloud-Ressourcen durchgeführt

  Sie können die Verarbeitung von Cloud-Ereignissen einrichten und eine Tag-Richtlinie zuordnen, um Tags für Cloud-Ressourcen in Echtzeit zu aktualisieren.

Tag-Governance -Richtlinien werden erstellt

Konfigurieren Sie Tag-Richtlinien, die die Kriterien für Tag-Audits für erkannte Cloud-Ressourcen oder CIs definieren. Zeigen Sie Audit-Ergebnisse zu Tag-Qualität und -Compliance im Dashboard „Tag-Integrität“ an. Sie erstellen Tag-Richtlinien, die den Umfang und die Anforderungen der verschiedenen Gruppen in Ihrer Organisation unterstützen, damit alle Benutzer davon profitieren können.

Überlegungen

Achten Sie bei der Definition von Tagging-Standards auf einen systematischen Ansatz, um die Anzahl der Tags niedrig zu halten. Standardisierte Tag-Richtlinien verbessern die Leistungsfähigkeit der App Tag-Governance bei der Überwachung und Verwaltung von Tags für alle CIs in Ihrer Organisation.

Möglicherweise benötigen Sie ausführliche Diskussionen und Recherchen, um die Anforderungen der unterschiedlichen Teams in Ihrer Organisation zu verstehen. Beispielsweise möchten Finanzteams möglicherweise, dass CIs basierend auf Kostenstellenzuteilungen, Anwendungszuweisungen und Geschäftszweck getaggt werden. Im Gegensatz dazu möchten IT-Sicherheitsteams in ihrem Schwachstellenmanagementplan möglicherweise CIs nach Betriebssystem und Sicherheitspatch-Ebene kategorisieren.

Bevor Sie Ihren Tagging-Ansatz abschließen, vergewissern Sie sich, dass Sie die folgenden Probleme berücksichtigt haben:

- Tag-Filter, die von verschiedenen Teams verwendet werden
- Die Zugriffsebene, die verschiedene Benutzer benötigen
- Ob Echtzeitprüfungen erforderlich sind.
- Ob Sie Tags mit Cloud-Ressourcen synchronisieren müssen.

Zugehörige Informationen

Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance

Konfigurieren Sie Korrekturrichtlinien für Tag-Audit-Ergebnisse

Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance

Konfigurieren Sie Tag-Richtlinien, die die Kriterien für Tag-Audits für erkannte Cloud-Ressourcen oder CIs definieren. Zeigen Sie Audit-Ergebnisse zu Tag-Qualität und -Compliance im Dashboard „Tag-Integrität“ an.

Vorbereitungen

Erforderliche Rolle: sn_itom_tag.tag_governance_admin, admin.

Warum und wann dieser Vorgang ausgeführt wird

Sie können Filter angeben, die den Umfang eines Audits einschränken, z. B. um nur Servicekonten und Rechenzentren zu prüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Tag-Governance** > **Richtlinien**.
2. Wählen Sie **Neu** aus, und füllen Sie das Formular Tag-Richtlinien aus.
   Die Formularfelder werden unter Formular „Tag-Richtlinien“.beschrieben.
3. Wählen Sie **Absenden**.
   - In der zugehörigen Liste „Tag-Richtlinienausführungen“ wird die Liste der Tag-Audit-Ausführungen mit den entsprechenden Zeitstempeln für Status, Erstellung und Aktualisierung angezeigt.
   - In der zugehörigen Liste Neueste Richtlinienausführungsergebnisse werden die Ergebnisse des Tag-Audits angezeigt.

Nächste Maßnahme

- Wählen Sie den zugehörigen Link **Audit-Ergebnisse anzeigen** aus, um alle Audit-Ergebnisse anzuzeigen.
- Wählen Sie den zugehörigen Link **Punktscan ausführen** aus, um alle zutreffenden Prüfungen für den Datensatz auszuführen.
- Weitere Informationen hierzu finden Sie unter Flows und Subflows .

Konfigurieren Sie Korrekturrichtlinien für Tag-Audit-Ergebnisse

Konfigurieren Sie Korrekturoptionen, zeigen Sie eine Vorschau an, generieren Sie Schlüssel, und führen Sie Aktionen aus, um Nichteinhaltung oder Fehler zu beheben, die auf Tag-Audit-Berichten basieren.

Vorbereitungen

Stellen Sie sicher, dass Tag-Richtlinien konfiguriert sind und sich im Status „Aktiv“ befinden.

Erforderliche Rolle: sn_itom_tag.tag_governance_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Remediation automatisch ausführen, wenn Sie einer Tag-Richtlinie eine Remediationsrichtlinie zuordnen. Sie können die Tags nicht konformer CIs auch in Echtzeit auf der Seite des Cloud-Anbieters aktualisieren.

Konfigurieren Sie Korrekturrichtlinien und -logik, und aktivieren Sie auch die Aktualisierung von Tags für Cloud-Ressourcen, die den folgenden CMDB -Klassen zugeordnet sind:

- Virtuelle Maschinen
- Compute-Sicherheitsgruppen
- Speicher-Laufwerke
- Cloud-Netzwerke
- Cloud-Subnetz
- Netzwerkschnittstellen
- Lastenausgleichsmodule
- Verfügbarkeitszonen
- Öffentliche IP-Adressen
- Speicherkonten
- Ressourcengruppen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Liste der CMDB -Klassen, für die Sie Tags für CIs in CMDB sowie Cloud-Ressourcen aktualisieren können, wird auch im Formular „Tag-Korrektur“ angezeigt. Wenn Sie im Formular „Remediation“ das Kontrollkästchen **Tags in Cloud aktualisieren** aktivieren, zeigt die Remediation nur eine Vorschau der CI-Fehler an, die zu den aufgeführten Klassen CMDB gehören.

Prozedur

1. Navigieren zu **Alle** > **Tag-Governance** > **Korrektur**.
2. Wählen Sie **Neu** aus, um einen neuen Datensatz zu erstellen.
3. Geben Sie im Feld **Name** einen eindeutigen beschreibenden Namen ein.
4. Wählen Sie im Feld **Richtlinie** das .

   Hinweis: Das Feld **Richtlinientyp** wird automatisch ausgefüllt, nachdem Sie eine Richtlinie aus der Suchliste ausgewählt haben.

5. Konfigurieren Sie in der Liste „Tag-Richtlinien“ eine Korrekturrichtlinie auf eine der folgenden Arten:
   - Wählen Sie aus der Nachschlageliste eine vorhandene Tag-Richtlinie aus.
   - Wählen Sie **Neu**. Füllen Sie die Felder im Formular „Tag-Richtlinien“ aus (die Felder werden in Formular „Tag-Richtlinien“.beschrieben).

     Hinweis: Wenn Sie eine neue Tag-Richtlinie erstellen, müssen Sie ein Audit ausführen, bevor Sie Korrektur-Flows ausführen können.

   Sie haben eine Richtlinie für den Fehlerkorrektur-Datensatz erstellt oder ausgewählt.
6. Wahlweise: Aktivieren Sie das Kontrollkästchen **Automatische Korrektur**, um automatisch eine Korrektur für nicht konforme CIs auszuführen.
   Wenn ein Audit abgeschlossen ist, wird die Remediation für alle CIs mit Richtlinienfehlern ausgeführt.
7. Wahlweise: Aktivieren Sie das Kontrollkästchen **Tags in Cloud aktualisieren,** um die Korrektur anzuwenden und die Tags in der entsprechenden Cloud-Provider-Umgebung für unterstützte CMDB CI-Klassen zu aktualisieren.

   Wichtig: Die Funktion **„Tags in der Cloud aktualisieren“** funktioniert nur für AWS - und Microsoft Azure Cloud -Ressourcen für CMDB -Klassen, die im Formular „Tag-Korrektur“ aufgeführt sind. Weitere Informationen finden Sie unter Es werden Echtzeit-Updates an Tags für Cloud-Ressourcen durchgeführt.

8. Wählen Sie im Formular „Tag-Korrektur“ **Absenden aus**.
   Die Korrekturrichtlinie ist konfiguriert. Die Liste der Tag-Korrekturen wird geöffnet.

Tag-Auditfehler in der Vorschau anzeigen und korrigieren

Zeigen Sie eine Vorschau von Audit-Berichten für Ressourcen an, die Tag-Richtlinien als nicht konform identifizieren. Beheben Sie -Fehler durch Hinzufügen oder Aktualisieren von Tags.

Vorbereitungen

Konfigurieren Sie Tag-Richtlinien und Korrekturrichtlinien. Siehe Konfigurieren Sie eine Tag-Richtlinie für Tag-Governance und Konfigurieren Sie Korrekturrichtlinien für Tag-Audit-Ergebnisse.

Hinweis: Das Update in die Cloud funktioniert nur für AWS - und Microsoft Azure Cloud -Ressourcen für CMDB -Klassen, die im Formular „Tag-Korrektur“ aufgeführt sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: sn_itom_tag.tag_admin, admin

Warum und wann dieser Vorgang ausgeführt wird

Basierend auf den von Ihnen erstellten Tag-Richtlinien können Sie eine Vorschau der Korrektur-Flows anzeigen und fehlende Tags für nicht konforme CIs automatisch generieren. Diese Informationen werden in der zugehörigen Liste „Tag Remediation Preview“ (Vorschau der Tag-Fehlerkorrektur) angezeigt. Siehe Flows und Subflows .

Hinweis:

- Wenn Sie bei der Konfiguration der Fehlerkorrektur das Kontrollkästchen **Update Tags in Cloud** (Tags in Cloud aktualisieren) aktivieren, werden in der Vorschau Auditfehler herausgefiltert, die zu den aufgeführten CI-Klassen gehören.
- Wenn Sie bei der Konfiguration der Remediation sowohl die **Option Automatische Korrektur** als auch **Tags in Cloud aktualisieren** ausgewählt haben, werden Tags sowohl in CMDB als auch in Cloud-Ressourcen aktualisiert (nur für unterstützte CMDB CI-Klassen).
- Wenn Sie nur **Automatische Korrektur**auswählen, werden die Tags nur in CMDB ausgeführt und aktualisiert.

Prozedur

1. Navigieren zu **Alle** > **Tag-Governance** > **Korrektur**.
2. Wählen Sie in der Liste der Tag-Fehlerkorrekturen den Datensatz aus, den Sie anzeigen möchten.
3. Wählen Sie den zugehörigen Link **Vorschau der Korrektur anzeigen** aus.
   In der zugehörigen Liste „Tag Remediation Previews“ (Vorschau der Tag-Fehlerkorrektur) werden die nicht konformen CIs angezeigt.
4. Wählen Sie die zugehörige Liste Vorschau auf Tag-Korrektur aus, um die fehlenden Tags und ihre Werte zu identifizieren.
5. Wählen Sie in der zugehörigen Liste „Tag-Korrekturschlüssel“ **Neu**, um einen Tag-Korrekturschlüssel zu erstellen.
   Die Felder im Formular „Schlüssel für Tag-Korrektur“ sind unter Formular „Tag Remediation Key“ (Schlüssel der Tag-Fehlerkorrektur)beschrieben.
6. Wählen Sie **Absenden**.
   Sie haben die Tag-Korrekturschlüssel erstellt, die der Richtlinie zugeordnet sind.
7. Wahlweise: Wählen Sie den zugehörigen Link **Schlüssel generieren** aus, wenn Sie die **Tag-Schlüsselrichtlinie**ausgeführt haben.
   Der zugehörige Link **Generate Keys** (Schlüssel generieren) wird nur für den Richtlinientyp *Tag Key Policy* angezeigt. Da die Richtlinie die erwarteten Tags angibt, können Sie den zugehörigen Link **Schlüssel generieren** auswählen, um die Schlüssel zu generieren, die Sie für die Remediation benötigen, anstatt sie manuell in der zugehörigen Liste Tag-Korrekturschlüssel hinzuzufügen.
8. Wahlweise: Wählen Sie den zugehörigen Link **Schlüsselwerte generieren** aus, wenn Sie die **Tag-Schlüssel- und -Wertrichtlinie**ausgeführt haben.
   Der zugehörige Link **Generate Key Values** (Schlüsselwerte generieren) wird nur für den Richtlinientyp *Tag Key and Value Policy* angezeigt. Da Sie die gesuchten Werte bereits in der Tag-Richtlinie angegeben haben, können Sie den zugehörigen Link **Schlüsselwerte generieren** auswählen, um die erwarteten Schlüsselwerte hinzuzufügen.
9. Wählen Sie den zugehörigen Link **Tags korrigieren** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Fehlerkorrektur-Flow zum Hinzufügen fehlender Tags wird initiiert. Eine entsprechende Informationsmeldung wird im Formular angezeigt, wenn die Fehlerkorrektur aktiv ist. Wählen Sie in der Nachricht den Link **Weitere Informationen** aus, um zum Standard-Flow-Kontext zu navigieren.

Ergebnisse

Basierend auf den Tag-Auditergebnissen und den von Ihnen erstellten Schlüsseln der Tag-Fehlerkorrektur fügt der Fehlerkorrektur-Flow den nicht konformen CIs fehlende Tags hinzu, um die Richtlinienkonformität herzustellen.

Es werden Echtzeit-Updates an Tags für Cloud-Ressourcen durchgeführt

Sie können die Verarbeitung von Cloud-Ereignissen einrichten und eine Tag-Richtlinie zuordnen, um Tags für Cloud-Ressourcen in Echtzeit zu aktualisieren.

Voraussetzungen

- Die Tabelle „Cloud-Ereignisse“ [sn_cmp_cloud_events] enthält keine Datensätze im Status *processed*.
- CIs, die von Tag-Change-Events betroffen sind, werden entweder durch CAPI oder Discovery and Service Mapping Patterns identifiziert.
- Mindestens eine Tag-Richtlinie konfiguriert.
- Aktivieren Sie das Kontrollkästchen **Bei Cloud-Ereignissen ausführen** in der von Ihnen erstellten Tag-Richtlinie.

Die Anweisungen hängen vom Cloud-Anbieter ab

Beachten Sie die folgenden Setupanweisungen für die Verarbeitung von Cloud-Ereignissen:

- Konfigurieren Sie den Amazon AWS Config-Service für die automatische Aktualisierung der CMDB
- Konfigurieren Sie den Microsoft Azure Alert-Service, um die CMDB automatisch zu aktualisieren
- Konfigurieren Sie den Protokollierungsservice der Operations Suite von Google Cloud, um die CMDB automatisch zu aktualisieren

Verarbeiten Sie Cloud-Ereignisse im Zusammenhang mit Änderungen in Tags, und führen Sie Tag-Audits für die Ereignisse in Echtzeit aus.

Im Gegensatz zu regulären Tag-Audits, bei denen das Audit für alle CIs in CMDB durchgeführt wird, für die die Tag-Richtlinie gilt, werden Tag-Ereignisse pro CI verarbeitet. Basierend auf den Voraussetzungen erfolgt die Tag-Event-Verarbeitung für Events, die mit einem Tag-Change identifiziert werden. Das betroffene CI wird identifiziert. Wenn die zugeordnete Richtlinie für das CI gilt, wird die Tag-Richtlinie für das identifizierte CI ausgeführt.

Wenn das Kontrollkästchen **Für Cloud-Ereignisse** ausführen während der Richtlinienerstellung aktiviert ist, wird die Richtlinie ausgewählt, um ein Audit für Tag-Change-Ereignisse auszuführen. Wenn das Kontrollkästchen deaktiviert ist, wird das Audit für das CI nicht ausgeführt, auch wenn Cloud-Ereignisse für Tag-Änderungen vorhanden sind.

Zeigen Sie in der Tabelle „Tag-Change-Protokoll“ [sn_itom_tag_change_log] den Change-Typ an, der für das Tag gilt (den Change, der das Audit ausgelöst hat). Die Datensätze in der Tabelle werden standardmäßig 90 Tage lang gespeichert. Die Change-Protokolldatensätze werden unabhängig davon angezeigt, ob eine Korrekturausführung oder ein Ereignis den Change am CI ausgelöst hat. Sie können auch Tags anzeigen, die im Rahmen des Change hinzugefügt oder aktualisiert wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Leistung optimieren

Ein hoher Ereignis-Zufluss oder eine große Anzahl von Tag-Richtlinien können die Leistung beeinträchtigen. Sie können die folgenden Systemeigenschaften ändern, um eine akzeptable Leistung sicherzustellen:

- [sn_itom_tag.azure_window_size] − Diese Systemeigenschaft ist konfigurierbar (in Minuten).
- [sn_itom_tag.max_audit_lag_r]: Geben Sie die Verzögerung zwischen bereits laufenden Tag-Audits an, bevor das Audit für die für das Audit bereiten Datensätze ausgelöst wird.
- [sn_itom_tag.policy_batch_size]: Batchgröße, für die das Tag-Audit ausgeführt wird.
- [sn_itom_tag.event_batch_size]: Zu verarbeitende Ereignis-Batch-Größe.

Tag-Governance – Referenz

Referenzthemen enthalten zusätzliche Informationen zu Formularen Tag-Governance und anderen Ressourcen.

Domain Separation und Tag-Governance

Die Domänentrennung wird in Tag-Governance unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Domänentrennung

Sie können CIs oder Cloud-Ressourcen identifizieren, die inkonsistent sind und nicht den Richtlinien entsprechen, die Sie für die Steuerung von Tag-Daten konfigurieren. In Tag-Governancezielt Domain Separation auf Anwendungsfälle der anfordernden Person der Mandantendomäne in einer Anwendung ab. Die Anwendung wurde entwickelt, um Aktivitäten der anfordernden Person in Mandantendomänen zu unterstützen. Es wurde Logik zum Weiterleiten von Daten an Mandantendomänen abhängig von den jeweiligen Anwendungsfällen implementiert. Der Besitzer der Instanz muss in der Lage sein, die Anwendung so einzurichten, dass sie mandantenübergreifend normal funktioniert. Die Anwendung verarbeitet die Datenweiterleitung an Domänen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Tabellen in Tag-Governance unterstützen nur Datentrennung, delegierte Domänentrennung wird dagegen nicht unterstützt.

Um sicherzustellen, dass domänensensible Informationen nicht in einer globalen Domäne verfügbar sind, stellen Sie sicher, dass Sie Richtlinien auf Domänenebene und nicht auf globaler Ebene erstellen. Erstellen Sie bei der Verwaltung von Service Providern Richtlinien auf Service Provider-Ebene. Wenn Sie Richtlinien stattdessen auf globaler Ebene erstellen, werden die Ergebnisse beim Ausführen des Audits in der globalen Domäne anstelle der entsprechenden Domänen erstellt.

Zugehörige Informationen

Domänentrennung für Service Provider

Tag-Richtlinien und Remediation für AWS

Tag-Audits wenden Richtlinien auf erkannte CIs an, um die Tag-Compliance zu bestimmen. Vorhandensein von Tags, angemessene Anzahl von Tags und Vorhandensein angegebener Schlüssel-Wert-Paare.

Tag-Richtlinien

Führen Sie ein Tag-Audit aus, um erkannte CIs für die folgenden Tag-Richtlinientypen zu prüfen:

- Tag-Anzahl: Überprüft CIs auf die von Ihnen angegebene Tag-Schlüssel-Anzahl
- Tag-Präsenz: Überprüft CIs auf das Vorhandensein der von Ihnen angegebenen Tag-Schlüsselwerte
- Tag-Schlüssel und -Wert: Überprüft CIs auf das Vorhandensein von von Ihnen angegebenen Schlüssel-Wert-Paaren.

Geben Sie den Zeichenfolgewert oder die Tag-Schlüssel, nach denen Sie suchen, in einem kommagetrennten Format im Richtlinientyp „Tag Presence“ (Tag-Vorhandensein) an. Sie können auch eine Zahl im Richtlinientyp „Tag Count“ (Tag-Anzahl) angeben, um CIs mit einem oder mehreren Tags zu identifizieren. Nachdem Sie die Tag-Audits ausgeführt haben, können Sie die Audit-Ergebnisse anzeigen und Korrekturmaßnahmen konfigurieren, die auf der Qualität des Compliance-Index basieren. Optional können Sie auch Benutzergruppen und Benutzern Folgeaufgaben für Korrekturaufgaben für nicht konforme CIs zuweisen.

Die automatische Korrektur funktioniert mit der Rolle Assume Role (Rolle übernehmen) für AWS, um das Tagging von Cloud-Ressourcen zu automatisieren, indem die Schritte in Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurierenausgeführt werden.

Die „Rolle übernehmen“ muss über die folgenden Berechtigungen (Richtlinie) verfügen, damit die Remediation funktioniert:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "tag:TagResources",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "Resource": [
                "arn:aws:ec2:*:*:instance/*",
                "arn:aws:ec2:*:*:security-group/*",
                "arn:aws:ec2:*:*:volume/*",
                "arn:aws:ec2:*:*:vpc/*",
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:network-interface/*",
                "arn:aws:elasticloadbalancing:*:*:loadbalancer/*",
                "arn:aws:ec2:*:*:availability-zone/*",
                "arn:aws:ec2:*:*:public-ip/*",
                "arn:aws:storagegateway:*:*:gateway/*",
                "arn:aws:resource-groups:*:*:group/*"
            ]
        }
    ]
}
```

Hinweis:

Wenn bei der Tag-Korrektur festgestellt wird, dass Discovery ohne Anmeldeinformationen ist, wird MID-Server mit Tag-Verwaltungsfunktionalität ausgewählt. Fügen Sie daher die Tag-Verwaltungsfunktionalität dem richtigen MID-Server hinzu, indem Sie die IAM-Rolle für den Serviceaccount anhängen. Diese Aktion ist wichtig, da es mehrere Konten geben kann, aus denen die IAM-Rolle MID Servers auswählen muss.

Hinweis: Sie müssen über die Berechtigungen ITOM-Transparenz verfügen, um eine Remediation für CIs in CMDBauszuführen. Weitere Informationen Kontakt Kundenservice und Support.

Formular „Tag-Richtlinien“.

Sie verwenden das Formular „Tag-Richtlinie“ zum Konfigurieren von Tag-Compliance- und -Integritätsrichtlinien, die in Tag-Audits für erkannte Cloud-Ressourcen oder CIs verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-Richtlinien“.

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für die Richtlinie.
Kurzbeschreibung	Eine kurze Zusammenfassung, die die Richtlinie beschreibt.
Richtlinientyp	Auswahl des Richtlinientyps für das Audit der Tag-Compliance und -Integrität. • Tag-Anzahl-Richtlinie: Prüft auf eine bestimmte Anzahl von Tags für CIs. • Tag-Schlüsselrichtlinie: Suchen Sie nach Tags mit bestimmten Werten (Zeichenfolgenausdrücke). • Tag-Schlüssel- und -Wertrichtlinie: Überprüft, ob Schlüssel-Wert-Paare und Wertzeichenfolgen vorhanden sind. Basierend auf Ihrer Auswahl geben Sie zusätzliche Werte an.
Erwartete Tag-Anzahl	Dieses Feld wird nur angezeigt, wenn der Richtlinientyp **Tag-Anzahl** Richtlinie ausgewählt ist. CIs mit weniger Tags als der angegebenen Anzahl gelten als fehlgeschlagen oder nicht konform. CIs, die den Wert erfüllen, gelten als gemäß dieser Richtlinie zertifiziert. Wenn Sie beispielsweise `4`angeben, prüft die Richtlinie, ob für die CIs mindestens vier Tags angegeben sind.
Erwartete Tag-Schlüssel	Dieses Feld wird nur angezeigt, wenn der Richtlinientyp **Tag-Schlüsselrichtlinie** ausgewählt ist. Richtlinie, die erkannte CIs auf die im Feld **Erwartete Tag-Schlüssel** angegebenen Tags überprüft. Geben Sie mehrere Tags oder Zeichenfolgenausdrücke in einer durch Kommas getrennten Liste an. Wenn Sie beispielsweise `prod,finance,coststelle` angeben, prüft die Richtlinie, ob die CIs alle angegebenen Tags aufweisen. CIs, die alle angegebenen Tags aufweisen, gelten als zertifiziert oder vollständig konform. Wenn bei CIs eines

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-Richtlinien“. (Fortsetzung)

Feld	Beschreibung
	der aufgeführten Tags fehlt, gelten sie als fehlerhaft oder nicht konform.

Prüfungen von Tag-Schlüsseln und -Werten	Führen Sie diese Richtlinie aus, um erkannte CIs auf den Tag-Schlüssel und die Werte zu überprüfen, die im Feld **Prüfungen von Tag-Schlüsseln und -Werten** angegeben sind.
	
	Sie können mehrere Tag-Schlüssel-Wert-Paare oder ein Skript angeben, um nach einer Sammlung von Werten zu suchen.
	
	Sie können beispielsweise `„user“` im Feld **„Schlüssel“** und `„admin“` im Feld **„Wert“** angeben.
	
	Hinweis:
	
	Das Feld **Skript** wird nur angezeigt, wenn **Richtlinie für Tag-Schlüssel und -Wert** im Feld **Richtlinientyp** ausgewählt ist. Verwenden Sie das Feld **Skript**, um mehrere Werte anzugeben und einen Zeichenfolgensatz zurückzugeben.
	
	Beispielcode
	
	`// The script should return a string set to tagValues variable.`
	`// the code sets the tagValues array with name of the CI`
	`// by this the check will be done for the tag to match the CI’s name`
	`tagValues = [ci.name.toString()];`

Aktiv	Option zum Aktivieren oder Deaktivieren der Ausführungszeitpläne.
Für Cloud-Ereignisse ausführen	Option zum Aktivieren von Echtzeit-Audit-Ausführungen, wenn Cloud-Ereignisse auftreten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-Richtlinien“. (Fortsetzung)

Feld	Beschreibung
	Hinweis: Stellen Sie sicher, dass die automatische Aktualisierung von CMDB mit Cloud-Ereignissen für den entsprechenden Cloud-Anbieter konfiguriert ist.
Speichern Sie das Audit-Ergebnis für die Zertifizierung	Option zum Speichern der Zertifizierungsauditergebnisse und zur Integration von Tag-Auditergebnissen in die Integritätsberechnungen eines CI. **Hinweis:** Diese Option kann aktiviert werden, wenn ein Geschäftsbedürfnis besteht, Tag-Audit-Ergebnisse in CI-Integritätsberechnungen zu integrieren.
Ausführen	Häufigkeit, mit der das Tag-Audit ausgeführt wird. • **Täglich** • **Monatlich** • **Wöchentlich** • **In regelmäßigen Abständen** • **Einmal** • **Bei Bedarf** **Hinweis:** Um ein Audit unmittelbar nach dem Konfigurieren der Richtlinie auszuführen, wählen Sie die Option **Bei Bedarf**. • **Business Calendar: Entry Start (Geschäftskalender: Eintragsbeginn)** • **Business Calendar: Entry End (Geschäftskalender: Eintragsende)**
Nächstes geplantes Ausführungsdatum	Datum und Uhrzeit der nächsten geplanten Ausführung des Tag-Audits. Dieses Feld wird nur für geplante Ausführungen und nicht für Ausführungen bei Bedarf angezeigt.
Filter	Bedingungsanweisungen mit einer Reihe von kontextabhängig generierten Feldern. Verwenden Sie Nachschlagelisten, um

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-Richtlinien“. (Fortsetzung)

Feld	Beschreibung
	Bedingungen zu erstellen und die für das Audit geeigneten CIs zu filtern. Dynamische Bedingungen und Filter, die Sie angeben, um die gewünschten Tags basierend auf Servicekonten und zugehörigen Rechenzentren abzurufen.
Tabelle	Zeigt die Tabelle *Configuration Item [cmdb_ci]* an, auf die Filter angewendet werden.
Richtlinienkriterien	Andere Richtlinienkriterien, die Sie mit dynamisch gefüllten Referenznachschlaglisten konfigurieren können. Die Tabelle „Configuration Item“ [cmdb_ci] füllt die Daten für diese Suchliste. Weitere Informationen finden Sie unter Referenzsuche .
Tag-Filter	Filtern Sie CIs weiter basierend auf Ihren Angaben für **Schlüssel**, **Stichwörter** und **Wert**. Verwenden Sie den Bedingungsgenerator, um einen Filter anzupassen.
Aufgabenzuweisung	Option zum Zuweisen von Folgeaufgaben zu Benutzern oder Benutzergruppen.
Aufgaben erstellen	Option zum Erstellen von Folgeaufgaben. **Hinweis:** Wenn eine vorhandene Aufgabe einer CI- und Tag-Richtlinie zugeordnet ist, bestimmt die Systemeigenschaft *sn_itom_tag.allow_new_cert_follow_on_task*, ob bei einem Compliance-Fehler eine neue Aufgabe erstellt oder eine vorhandene Aufgabe aktualisiert werden soll: • Um die vorhandene Aufgabe mit den Compliance-Fehlerdetails zu aktualisieren, aber keine neue Aufgabe zu erstellen, legen Sie die Eigenschaft auf „falsch“ fest (Standard). • Um eine neue Aufgabe zu erstellen, legen Sie die Eigenschaft auf „true“ fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-Richtlinien“. (Fortsetzung)

Feld	Beschreibung
Gruppe	Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Aufgaben erstellen** aktivieren. Zuweisungsgruppe, der die Aufgabe zugewiesen werden soll. Verwenden Sie Suchlisten, um eine Gruppe auszuwählen.
Anwender	Ein bestimmter Benutzer der Zuweisungsgruppe, dem Sie die Aufgabe zuweisen möchten. Verwenden Sie Nachschlagelisten, um einen Benutzer auszuwählen. Dieses Feld wird nur angezeigt, wenn Sie das Kontrollkästchen **Aufgaben erstellen** aktivieren.

Formular „Tag Remediation Key“ (Schlüssel der Tag-Fehlerkorrektur)

Um einen Tag-Korrekturschlüssel zu erstellen, verwenden Sie das Formular „Tag-Korrekturschlüssel“.

Formular „Tag Remediation Key“ (Schlüssel der Tag-Fehlerkorrektur)

Feld	Beschreibung
Schlüssel	Tag-Schlüsselwert, der zur Fehlerkorrektur nicht konformer CIs verwendet wird. Wenn in der Fehlerkorrekturvorschau als Wert beispielsweise `Kostenstelle` angezeigt wird, können Sie die `Kostenstelle` als neuen Fehlerkorrekturschlüssel angeben, sofern dieser noch nicht vorhanden ist.
Auftrag	Reihenfolge der Ausführung, die das System berücksichtigt, wenn Sie die Remediation initiieren. Sie können beispielsweise eine Tag-Anzahl-Richtlinie für vier Tags ausführen und CIs identifizieren, denen zwei Tag-Schlüssel fehlen. Wenn Sie mehrere Fehlerkorrekturschlüssel konfiguriert haben, berücksichtigt das System die beiden Schlüssel mit den niedrigsten Werten im Reihenfolgefeld.
Fehlerkorrektur	Name der Fehlerkorrektur und Datensatzvorschau.
Werttyp	Typ des Werts, den Sie im Feld **„Wert“** angeben – **statisch** oder **Zeichenfolge**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag Remediation Key“ (Schlüssel der Tag-Fehlerkorrektur) (Fortsetzung)

Feld	Beschreibung
	Je nach Auswahl müssen Sie ein Skript oder einen Wert für den Tag-Schlüssel angeben.
Wert	Zeichenfolgenwert für den Schlüssel, den Sie erstellen. Dieses Feld wird nur angezeigt, wenn im Feld **„Werttyp“eine Zeichenfolge** ausgewählt ist.
Skript	Skriptcode zum Generieren von Werten für den Schlüssel. Dieses Feld wird nur angezeigt, wenn im Feld **„Werttyp“ein Skript** ausgewählt ist.

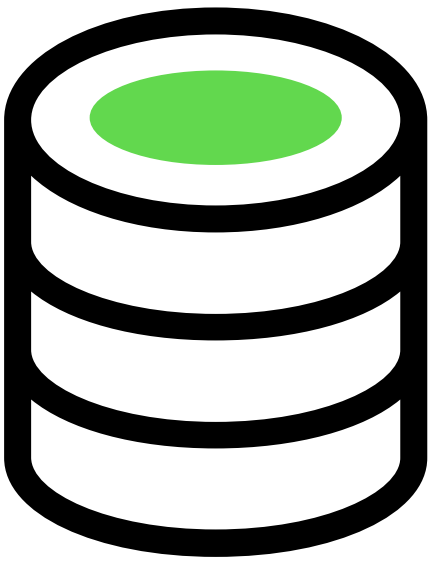
Arbeitsbereich für Cloud-Vorgänge

Arbeitsbereich für Cloud-Vorgänge bietet eine umfassende Lösung zum Verwalten der Cloud-Vorgänge Ihres Unternehmens.

Erste Schritte

Klicken Sie auf eine dieser Kacheln, um zu beginnen.

Installieren



Arbeitsbereich für Cloud-Vorgänge installieren

Verwenden

Arbeitsbereich für Cloud-Vorgänge verwenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

- Fragen stellen oder beantworten im Arbeitsbereich für Cloud-Vorgänge-Forum der ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Arbeitsbereich für Cloud-Vorgänge installieren

Sie können die Anwendung Arbeitsbereich für Cloud-Vorgänge (com.cloud_operations_workspace) installieren, wenn Sie über die Administratorrolle verfügen.

Vorbereitungen

Hinweis: Wenn Arbeitsbereich für Cloud-Vorgänge installiert wird, werden mehrere Plugins und Anwendungen installiert. Weitere Informationen finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Transparenz.

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Arbeitsbereich für Cloud-Vorgänge erfordert das folgenden Plugin. Stellen Sie sicher, dass das folgende Plugin aktiviert ist, bevor Sie Arbeitsbereich für Cloud-Vorgänge installieren.

  Benötigte ServiceNow-Plugins

  Discovery (com.snc.discovery)

  ServiceNow Cloud-Discovery erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die Multisource-CMDB mit den gefundenen Informationen. Weitere Informationen zur Aktivierung von Discovery finden Sie unter Discovery anfordern.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die Anwendung Arbeitsbereich für Cloud-Vorgänge installieren, wird automatisch die folgende Rolle installiert:

Arbeitsbereich für Cloud-Vorgänge-Rolle

Rollenname	Beschreibung und Aufgaben	Verschachtelte Rollen
sn_cloud_ops_ws.cloud_ops_admin	Der Arbeitsbereich für Cloud-Vorgänge-Administrator kann die folgenden Aktionen ausführen: • Arbeitsbereich für Cloud-Vorgänge-Dashboards anzeigen • Cloud-Discovery-Zeitpläne erstellen	• sn_itom_ui_comp.itom_component_user • discovery_admin • cloud_admin

Automatische Übersetzung

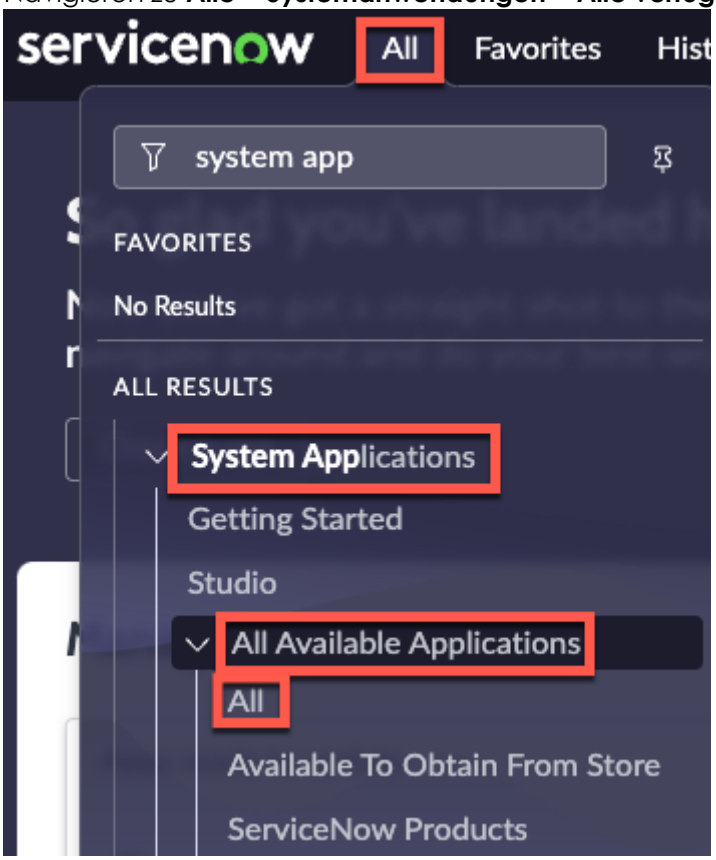
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeitsbereich für Cloud-Vorgänge-Rolle (Fortsetzung)

Rollenname	Beschreibung und Aufgaben	Verschachtelte Rollen
	• Cloud-Discovery-Vorgänge überwachen • Cloud-Discovery-Berichte anzeigen	

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Arbeitsbereich für Cloud-Vorgänge (com.cloud_operations_workspace).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

3. Überprüfen Sie im Dialogfeld „Anwendungsinstallation" die Anwendungsabhängigkeiten.

   Abhängige Plugins und Anwendungen werden aufgelistet, wenn sie installiert werden sollen, derzeit installiert sind oder installiert werden müssen. Wenn die Installation von Plugins

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

oder Anwendungen erforderlich ist, müssen Sie sie installieren, bevor Sie Arbeitsbereich für Cloud-Vorgänge installieren können.

4. Wahlweise: Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.
   Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für die gängigen Anwendungsfälle veranschaulichen. Laden Sie die Demodaten, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

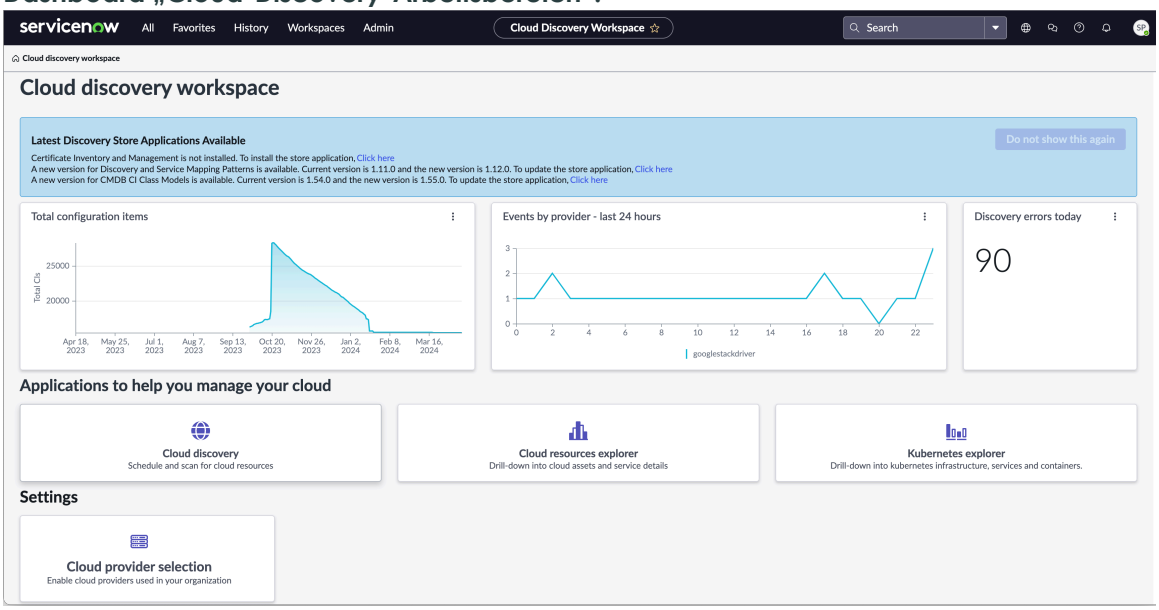
   Wichtig: Wenn Sie die Demodaten nicht während der Installation laden, stehen sie nicht zum späteren Laden zur Verfügung.

5. Wählen Sie **Installieren** aus.

Arbeitsbereich für Cloud-Vorgänge-Dashboard

Das ServiceNow® Arbeitsbereich für Cloud-Vorgänge-Dashboard bietet eine Zusammenfassung der Cloud-Vorgänge Ihrer Organisation und zeigt die ServiceNow-Anwendungen, mit denen Sie sie verwalten können.

Dashboard „Cloud-Discovery-Arbeitsbereich“.



Hinweis: Um auf die produktinterne Hilfe zuzugreifen, aktivieren Sie Next Experience . Sie können die visuelle Experience verbessern, indem Sie das dunkle Design verwenden. Weitere Informationen finden Sie unter Designs in Next Experience erkunden .

Erforderliche Now Platform-Rollen

sn_cloud_ops_ws.cloud_ops_admin.

Zugriff auf das Dashboard von Arbeitsbereich für Cloud-Vorgänge

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Cloud-Discovery-Arbeitsbereich**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsfälle

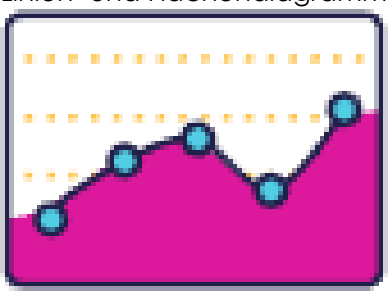
Anwender	Dashboard-Verwendung
sn_cloud_ops_ws.cloud_ops_admin	• Gewinnen Sie Einblick in den Trend der CI-Erkennung, den Trend von Cloud-Discovery-Ereignissen und Cloud-Discovery-Fehlern. • Wählen Sie den Cloud-Provider Ihrer Organisation aus. • Greifen Sie auf die Anwendungen zu, mit denen Sie die Cloud-Vorgänge Ihrer Organisation verwalten können.

Indikatoren

Heutige Discovery-Fehler: Anzahl aller Cloud-Discovery-Fehler, die während der geplanten Erkennungen in den letzten 24 Stunden aufgetreten sind.

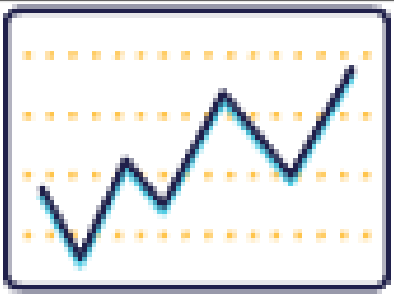
Berichte

Folgende Berichte sind im Dashboard Arbeitsbereich für Cloud-Vorgänge verfügbar:

Titel	Typ	Quelltabelle	Beschreibung
Total configuration items (Gesamte Konfigurationselemente)	Linien- und Flächendiagramm 	cmdb_ci	In diesem Bericht wird die Anzahl der im Laufe der Zeit erkannten CIs angezeigt. Wählen Sie den Bericht aus, um die Liste aller bisher erkannten Konfigurationselemente anzuzeigen. Sie können einen beliebigen CI-Datensatz auswählen, um weitere Informationen zum CI und den zugehörigen Daten aus mehreren Quellen anzuzeigen, falls verfügbar.
Ereignisse nach Anbieter – letzte 24 Stunden	Liniendiagramm	sn_cmp_cloud_event_list	In diesem Bericht wird der Trend der in den letzten 24 Stunden empfangenen Cloud-Ereignisse angezeigt. Der Bericht enthält eine separate Trendlinie für jeden Cloud-Anbieter.

Automatisch übersetzt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			
Heutige Discovery-Fehler	Ringdiagramm	discovery_errors_list	In diesem Bericht wird die Anzahl aller Cloud-Discovery Fehler angezeigt, die während der geplanten Erkennungen in den letzten 24 Stunden aufgetreten sind.

Zusätzlich werden auf den Dashboard-Karten die Anwendungen angezeigt, mit denen Sie die Cloud-Vorgänge Ihrer Organisation verwalten können. Verwenden Sie die Auswahlseite für Cloud-Anbieter, um den Cloud-Anbieter für Ihre Organisation auszuwählen. Die Auswahl hilft, die Menüs der Arbeitsbereich für Cloud-Vorgänge-Anwendungen anzupassen und nur die Cloud-Anbieter anzuzeigen, die für Ihre Organisation relevant sind.

Zugehörige Informationen

Liste der Arbeitsbereiche

Öffnen Sie Ihre konfigurierbare Arbeitsbereich-Experience in UI Builder für Arbeitsbereich für Cloud-Vorgänge

Greifen Sie zur Bearbeitung auf die Oberfläche Ihres konfigurierbaren Arbeitsbereichs in UI Builder zu.

Vorbereitungen

Erforderliche Rolle: admin, ui_builder_admin

Prozedur

1. Navigieren Sie im Navigationsfilter zu **Alle** > **Now-Experience-Framework** > **UI Builder**.
2. Wählen Sie **Experiences**.
3. Wählen Sie Ihre Experience aus.

Ergebnisse

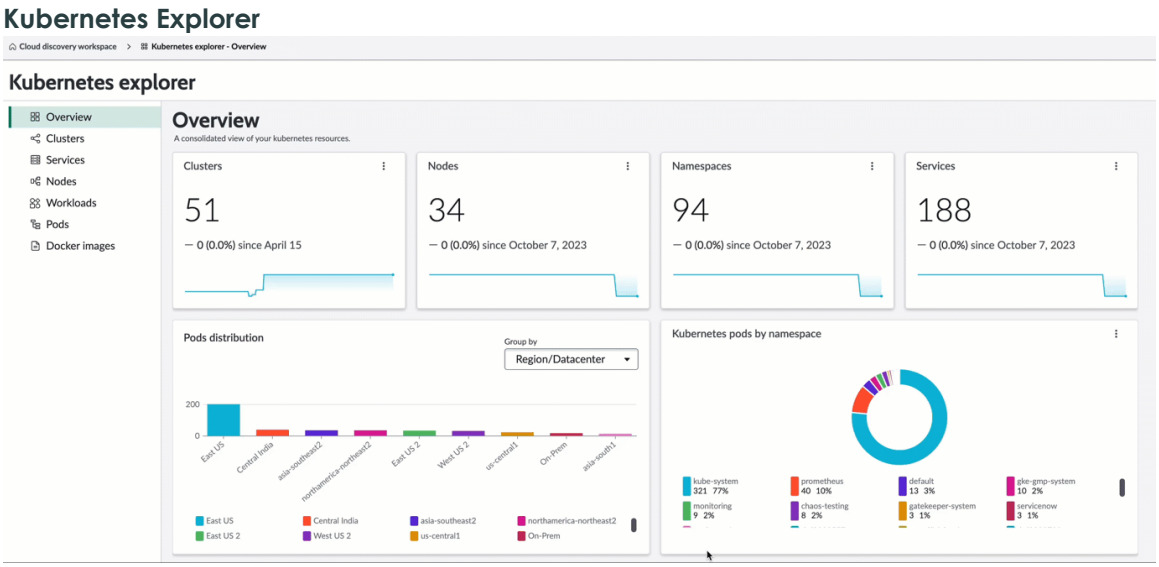
Ihre konfigurierbare Experience wird in UI Builder geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kubernetes Explorer

Verwenden Sie den ServiceNow® Kubernetes Explorer, um die Kubernetes-Umgebungen und -Ressourcen Ihres Unternehmens anzuzeigen.



Der Kubernetes Explorer bietet Unterstützung für folgende Cloud-Anbieter:

- Amazon Web Services (AWS): Amazon Elastic Kubernetes Service (EKS)
- Microsoft Azure Cloud: Azure Kubernetes-Service
- Google Cloud Platform (GCP): Google Kubernetes Engine (GKE)
- OpenShift

Wichtig: Im Kubernetes Explorer gilt jede unter OpenShift gehostete Kubernetes-Ressource als lokal. Dagegen gilt jede unter Amazon Web Services (AWS), Microsoft Azureund Google Cloud Platform (GCP) gehostete Kubernetes-Ressource als in der Cloud gehostet.

Erforderliche Now Platform-Rollen

Zum Anzeigen des Kubernetes-Explorer ist die Rolle sn_cloud_ops_ws.cloud_ops_admin erforderlich.

Auf Kubernetes Explorer zugreifen

Um das Dashboard zu öffnen, wechseln Sie zu: **Alle** > **Cloud-Discovery-Arbeitsbereich** > **Kubernetes-Explorer**.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Benutzer	Dashboard-Verwendung
Anwendungsbesitzer	Überprüfen Sie die Statistiken der in den Kubernetes-Clustern ausgeführten Anwendungen und Arbeitsauslastungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzer	Dashboard-Verwendung
IT-Administrator, Cloud-Administrator	• Überprüfen Sie die Statistiken der Kubernetes-Infrastruktur: Cluster, Knoten, Namespaces, Services, Pods und Arbeitsauslastungen. • Überprüfen Sie die Verteilung der Pods über Dimensionen wie Region/ Rechenzentrum, geografischer Standort oder Land. • Überprüfen Sie die Verteilung der Pods über Namespaces. • Überprüfen Sie die Liste der in Ihrer Organisation verwendeten Kubernetes-Docker-Images.

Indikatoren

Cluster

Ein Kubernetes-Cluster ist ein Satz von Knoten, auf denen containerisierte Anwendungen ausgeführt werden. Der Indikator „Cluster“ zeigt die tägliche Gesamtanzahl und den Erkennungstrend der Kubernetes-Cluster an, die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden.

Der Kubernetes Explorer liest die Tabelle „Analytics für Kubernetes-Cluster“ [sn_cow_k8s_cluster_analytics], um den Indikator „Cluster“ zu berechnen.

Knoten

Ein Knoten ist ein Worker-Computer in Kubernetes und kann je nach Cluster entweder ein virtueller oder ein physischer Computer sein. Der Indikator „Knoten“ zeigt die tägliche Gesamtanzahl und den Erkennungstrend der Kubernetes-Knoten an, die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden.

Der Kubernetes Explorer liest die Tabelle „Analytics für Kubernetes-Knoten“ [sn_cow_k8s_node_analytics], um den Indikator „Knoten“ zu berechnen.

Namespaces

Kubernetes-Namespaces bieten einen Mechanismus zum Isolieren von Ressourcengruppen innerhalb des Clusters. Der Indikator „Namespaces“ zeigt die tägliche Gesamtanzahl und den Erkennungstrend der Kubernetes-Namespaces an, die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden.

Der Kubernetes Explorer liest die Tabelle „Analytics für Kubernetes-Namespace“ [sn_cow_k8s_namespace_analytics], um den Indikator „Namespaces“ zu berechnen.

Services

Ein Kubernetes-Service ist eine Abstraktion, die einen logischen Satz von Pods und eine Richtlinie für den Zugriff auf diese definiert (manchmal wird dieses Muster auch als Mikroservice bezeichnet). Der Indikator „Services“ zeigt die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

tägliche Gesamtanzahl und den Erkennungstrend der Kubernetes-Services an, die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden.

Der Kubernetes Explorer liest die Tabelle „Analytics für Kubernetes-Service“ [sn_cow_k8s_service_analytics], um den Indikator „Services“ zu berechnen.

Der Indikator „Services“ ist auch auf der Registerkarte „Services“ von Kubernetes Explorer verfügbar.

Aufgliederungen

- Pod-Verteilung: Diese Aufgliederung zeigt die Verteilung der Kubernetes-Pods an, die in der lokalen Infrastruktur und der Cloud-Infrastruktur gehostet werden.

  Sie können die Aufgliederung nach folgenden Dimensionen filtern:

  - Region/Rechenzentrum
  - Geo-Standort
  - Land

  Die Pod-Verteilungsaufgliederung ist auf der Registerkarte „Übersicht“ von Kubernetes Explorer verfügbar.

- Kubernetes-Services nach Plattform oder Kubernetes-Services nach Typ: Diese Aufgliederung zeigt die Verteilung von Kubernetes-Services über Dimensionen wie Plattform und Typ an.
- Knoten nach Region: Diese Aufgliederung zeigt die Verteilung der Kubernetes-Knoten über Hosting-Regionen an.

Filter

Sie können die Liste filtern, indem Sie mit Datenvisualisierungen wie Ring und Einzel-Bewertungskarte interagieren.

Datenvisualisierungen

Titel	Typ	Quelltabelle	Beschreibung
Kubernetes-Pods nach Namespace	Ring	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht wird die Verteilung der Kubernetes-Pods über die erkannten Namespaces angezeigt. Dieser Bericht ist auf der Registerkarte „Übersicht“ verfügbar.
Cluster insgesamt	Liste	Analytics für Kubernetes-Cluster [sn_cow_k8s_cluster_analytics]	In diesem Bericht werden die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannten Kubernetes-Cluster aufgelistet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Dieser Bericht ist auf der Registerkarte „Cluster“ verfügbar. Wenn Sie auf den Clusternamen klicken, wird Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt.
Services insgesamt	Einzelne Punktzahl	Analytics für Kubernetes-Arbeitsauslastung [sn_cow_k8s_service_analytics]	Dieser Bericht zeigt die Gesamtzahl der Kubernetes-Services an. Dieser Bericht ist auf der Registerkarte „Services“ verfügbar.
Kubernetes-Services nach Plattform/Typ	Ring	Analytics für Kubernetes-Knoten [sn_cow_k8s_service_analytics]	Dieser Bericht zeigt die Verteilung der Kubernetes-Services über die Anbieter an. Dieser Bericht ist auf der Registerkarte „Services“ verfügbar.
Kubernetes-Services	Liste	Analytics für Kubernetes-Namespace [sn_cow_k8s_service_analytics]	Dieser Bericht listet die erkannten Kubernetes-Services auf. Dieser Bericht ist auf der Registerkarte „Services“ verfügbar. Wenn Sie auf den Servicenamen klicken, wird die Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt.
Knoten nach Cluster	Ring	Analytics für Kubernetes-Knoten [sn_cow_k8s_node_analytics]	Dieser Bericht zeigt die Verteilung der Kubernetes-Knoten über die erkannten Cluster an. Dieser Bericht ist auf der Registerkarte „Knoten“ verfügbar.
Knoten nach Region	Ring	Analytics für Kubernetes-Knoten [sn_cow_k8s_node_analytics]	Dieser Bericht zeigt die Verteilung der Kubernetes-Knoten über die erkannten Cluster an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Dieser Bericht ist auf der Registerkarte „Knoten“ verfügbar.
Knoten insgesamt	Liste	Analytics für Kubernetes-Knoten [sn_cow_k8s_node_analytics]	In diesem Bericht werden die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannten Kubernetes-Knoten aufgelistet. Dieser Bericht ist auf der Registerkarte „Knoten“ verfügbar. Wenn Sie auf den Knotennamen klicken, wird die Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt.
Gesamtanzahl der Arbeitsauslastungen	Einzelne Punktzahl	Analytics für Kubernetes-Arbeitsauslastung [sn_cow_k8s_workload_analytics]	Dieser Bericht zeigt die Gesamtanzahl der Kubernetes-Arbeitsauslastungen an, die für die Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden. Dieser Bericht ist auf der Registerkarte „Arbeitsauslastungen“ verfügbar.
Gewünschte/ Verfügbare Replikate stimmen nicht überein	Einzelne Punktzahl	Analytics für Kubernetes-Arbeitsauslastung [sn_cow_k8s_workload_analytics]	In diesem Bericht wird die Anzahl der Nichtübereinstimmungen zwischen den gewünschten und verfügbaren Replikaten angezeigt. Wenn eine Nichtübereinstimmung vorliegt, ergreifen Sie geeignete Maßnahmen, um das Problem zu beheben.
Arbeitsauslastungen nach Klasse	Ring	Analytics für Kubernetes-Arbeitsauslastung [sn_cow_k8s_workload_analytics]	Dieser Bericht zeigt die Arbeitsauslastungen nach Arbeitsauslastungsklasse an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Dieser Bericht ist auf der Registerkarte „Arbeitsauslastungen“ verfügbar.
Gesamtanzahl der Arbeitsauslastungen	Liste	Analytics für Kubernetes-Arbeitsauslastung [sn_cow_k8s_workload_analytics]	In diesem Bericht werden die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannten Kubernetes-Arbeitsauslastungen aufgelistet. Dieser Bericht ist auf der Registerkarte „Arbeitsauslastungen“ verfügbar. Wenn Sie auf den Namen der Arbeitsauslastung klicken, wird die Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt.
Pods insgesamt	Einzelne Punktzahl	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	Dieser Bericht zeigt die Gesamtanzahl der Kubernetes-Pods an, die für die Kubernetes-Bereitstellungen Ihrer Organisation erkannt wurden. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar.
Ausgeführte Pods	Einzelne Punktzahl	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht wird die Gesamtanzahl der Kubernetes-Pods angezeigt, die sich im Status „Ausgeführt“ befinden. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar.
Ausstehende Pods	Einzelne Punktzahl	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht wird die Gesamtanzahl der Kubernetes-Pods angezeigt, die sich im Status „Ausstehend“ befinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar.
Erstellende Pods	Einzelne Punktzahl	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht wird die Gesamtanzahl der Kubernetes-Pods angezeigt, die sich im Status „Erstellung“ befinden. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar.
Crashloop-Backoff-Pods	Einzelne Punktzahl	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht wird die Gesamtanzahl der Kubernetes-Pods angezeigt, die sich im Status „Crashloop-Backoff“ befinden. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar.
Pods insgesamt	Liste	Analytics für Kubernetes-Pod [sn_cow_k8s_pod_analytics]	In diesem Bericht werden die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannten Kubernetes-Pods aufgelistet. Dieser Bericht ist auf der Registerkarte „Pods“ verfügbar. Wenn Sie auf den Pod-Namen klicken, wird die Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt.
Docker-Images	Liste	Analytics für Kubernetes-Image [sn_cow_k8s_img_analytics]	In diesem Bericht werden die in den Kubernetes-Bereitstellungen Ihrer Organisation erkannten Docker-Images aufgelistet. Dieser Bericht ist auf der Registerkarte für Docker-Images verfügbar. Wenn Sie auf den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Quelltabelle	Beschreibung
			Namen des Docker-Image klicken, wird die Abhängigkeitsansichten-Karte für das Konfigurationselement „Cluster“ angezeigt. Sie können die SBOM herunterladen. Weitere Informationen zum Generieren der SBOM finden Sie unter Software-Stückliste herunterladen (SBOM).

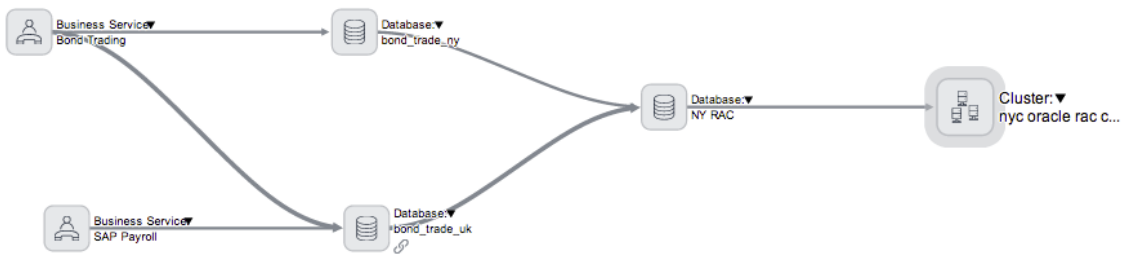
Abhängigkeitsansichten-Karte

ServiceNow® Die Zuordnung der Abhängigkeitsansichten zeigt eine -Gesamtperspektive für Kubernetes von oben nach unten, beginnend mit einem Cluster der obersten Ebene bis zum Container und innerhalb des Containers.

Eine Abhängigkeitsansichten-Zuordnung hat einen Ausgangspunkt, der als Stamm-CI oder Stammknoten der Zuordnung bezeichnet wird. Das Root-CI ist von einem dunkleren Frame umgeben, der sich mit einem pulsierenden Effekt neu zeichnet, um die Aufmerksamkeit auf das Root-CI zu lenken. Die Zuordnungen können sowohl vor- als auch nachgelagerte Abhängigkeiten für das Stamm-CI anzeigen. Standardmäßig zeigt die Abhängigkeitsansichten-Karte drei Ebenen an, sowohl Upstream- als auch Downstream-Beziehungen. Administratoren können die Anzahl der angezeigten Ebenen konfigurieren. Die Karte reduziert und vergrößert Cluster, um sie besser anzeigen zu können. Standardmäßig werden Cluster reduziert.

Das Modul „Abhängigkeitsansichten“ ist in allen Instanzen aktiv und enthält Demodaten.

Dependency Views-Beispielzuordnung



In einer Abhängigkeitsansichten-Karte zeigen Kartenindikatoren an, ob für ein CI aktive, ausstehende Probleme vorliegen. Sie können die mit einem CI verbundenen Aufgaben untersuchen, um weitere Details zu erhalten. Wenn Sie aus einem anderen Formular zur Karte zurückkehren, stellt das System die zuletzt angezeigte Karte wieder her, wobei die Standardfilter- und Layouteinstellungen verwendet werden.

Viele der Beziehungen in der Zuordnung werden durch den Discovery-Prozess erstellt. Sie können auch CI-Beziehungen in der Karte erstellen, definieren und löschen. Sie können die Karte aus verschiedenen Perspektiven anzeigen und bestimmte Datensätze öffnen, die sich auf Configuration Items beziehen. Das System aktualisiert die Zuordnung automatisch, um Änderungen an der CMDB widerzuspiegeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: CIs, die nicht aus der Tabelle „Configuration Item“ [cmdb_ci] erweitert wurden, werden nicht in Abhängigkeitsansichten-Zuordnungen und in CI-Beziehungsformatierern angezeigt.

Rollen

Benutzer mit den Rollen itil und ecmdb_admin können Karten anzeigen und alle Aktionen in der Karte ausführen. Zu den Aktionen gehört der Zugriff auf die Kartenansichten und gespeicherten Filter, sowohl von den Listen in der Karte als auch von dem Modul **Gespeicherte Filter** aus.

ITOM-Transparenz-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Zuordnen und Optimieren von Anwendungsservices mithilfe von ITOM-Transparenz-Listen und -Formularen.

Ausführungsoptionen für Discovery-Zeitpläne

Sowohl die Horizontal-Discovery als auch die Top Down-Discovery verwenden diese Ausführungsoptionen.

Discovery Planausführungsoptionen

Option ausführen	Beschreibung
Bei Bedarf	Wird nicht nach einem Zeitplan ausgeführt. Wählen Sie **Jetzt erkennen**, um Discov Standardoption.
Täglich	Läuft jeden Tag. Verwenden Sie das Feld**Zeit**, um die Uhrzeit anzugeben.
Wöchentlich	Läuft an einem bestimmten Wochentag. Verwenden Sie das Feld **Zeit**, um die Uhr
Monatlich	Läuft an einem bestimmten Tag jedes Monats. Verwenden Sie das Feld **Tag**, um a auszuwählen. Verwenden Sie das Feld **Zeit**, um die Uhrzeit anzugeben. Wenn der Monat vorkommt, wird der Zeitplan in diesem Monat nicht ausgeführt. Wenn Sie b wird der Zeitplan im Februar nicht ausgeführt.
Regelmäßig	Wird zu jeder angegebenen Zeit ausgeführt. Verwenden Sie das Feld **Wiederholu** in Tagen, Stunden, Minuten und Sekunden zu definieren. Das erste Mal, wenn Disc **Start** festgelegten Zeitpunkt ausgeführt wird. Die nachfolgenden Erkennungen we **Wiederholungsintervall**-Zeitraums ausgeführt.
Einmal	Einmal ausführen, wie durch das Datum und die Uhrzeit festgelegt, die im festgele
An Wochentagen	Läuft jeden Montag, Dienstag, Mittwoch, Donnerstag und Freitag. Verwenden Sie Tageszeit.
An Wochenenden	Läuft jeden Samstag und Sonntag. Verwenden Sie das Feld **Zeit** zur Auswahl der T
Letzter Tag des Monats	Führen Sie den letzten Tag jedes Monats aus. Verwenden Sie das Feld **Zeit** zur Aus
Ende des Kalenderquartals	Läuft am 31. März, 30. Juni, 30. September und 31. Dezember. Verwenden Sie das Tageszeit. Ändern Sie das Skript `DiscoveryScheduleRunType`, um das Datum zu a
Nach Discovery	Ermöglicht die sequenzielle Staffelung des Zeitplans. Verwenden Sie diese Option dem im Feld **Ausführen nach** bezeichneten Discovery auszuführen. Aktivieren Sie **bei Abbruch**, um anzugeben, dass diese Erkennung auch dann ausgeführt werde Discovery vor Abschluss abgebrochen wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery Planausführungsoptionen (Fortsetzung)

Option ausführen	Beschreibung
	• Diese Option ist nicht gültig, wenn Discovery über DiscoverNow gestartet wird o erkennen“ verwendet wird. • Sie können keinen inaktiven Discovery -Zeitplan festlegen. • Sie können keine Schleife erstellen, indem Sie festlegen, dass die Ausführung na Discoveryidentisch ist. • Discovery wird nicht ausgeführt, wenn **Ausführen nach** Discovery nicht abgesc Ausnahme, dass das Kontrollkästchen **Auch bei Abbruch** aktiviert ist und Discov

Zugehörige Informationen

Erkennung von oben nach unten mithilfe von Service-Mapping planen

Horizontale Erkennung planen

Mit installierte Plugins oder Anwendungen ITOM-Transparenz

Tabellen, die die Plugins oder Anwendungen auflisten, die mit den -Anwendungen ITOM-Transparenz installiert werden. Wenn Sie Ihre Anwendung aktualisieren, werden alle neu erforderlichen Anwendungsabhängigkeiten installiert.

Discovery

Mit Discovery (com.snc.discovery) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Cloud Provisioning and Governance Core (com.snc.cloud.core)	Enthält Ressourcenblöcke und Cloud API-Zuordnungen (Cloud Application Programming Interface) im Zusammenhang mit der Cloud API-basierten Erkennung und Ereignissen, die entweder durch Antwortzuordnungs- oder Aufrufmuster verarbeitet werden.
Service Watch Suite commons (com.snc.service-watch.commons)	Enthält allgemeine UI-Komponenten für Discovery und Service-Mapping.
Discovery IP-basiert (com.snc.discovery.ip_based)	Enthält gemeinsam genutzte Komponenten der Horizontal-Discovery, die von Discovery und Service-Mappingverwendet werden.

Discovery-Administratorarbeitsbereich

Mit Discovery-Administratorarbeitsbereich aktiviertes Plugin (sn_disco_workspace)

Plugin- oder Anwendungsname	Beschreibung
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service-Mapping

Mit Service-Mapping (com.snc.service-mapping) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Service-Mapping – Zuordnung (com.itom-map-app)	Ein abhängiges internes Plugin, das zur Unterstützung der Kernkomponenten der Anwendungen Service-Mapping, Ereignismanagementund Service Operations-Arbeitsbereich ITOM erforderlich ist.
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.
Ereignismanagement und Service-Mapping Core (com.snc.service-watch)	Besteht aus den gemeinsamen Komponenten von Ereignismanagement und Service-Mapping.
Cloud Provisioning and Governance Core (com.snc.cloud.core)	Enthält Ressourcenblöcke und Cloud API-Zuordnungen (Cloud Application Programming Interface) im Zusammenhang mit der Cloud API-basierten Erkennung und Ereignissen, die entweder durch Antwortzuordnungs- oder Aufrufmuster verarbeitet werden.
Musterdesigner (NG-Version) (com.snc.ng.pattern.designer)	Die NG-Version (nächste Generation) von Musterdesigner, mit der Sie Muster erstellen, bearbeiten und debuggen können, die von der horizontalen Erkennung und der Erkennung von oben nach unten verwendet werden.
Service-Mapping Plus (sn_sm_scoped_app)	bietet erweiterte Funktionen für Service-Mapping. Wenn die zugehörigen ServiceNow® Store -Anwendungen und -Plugins noch nicht installiert sind, werden sie installiert.

Tag-Governance

Mit Tag-Governance (sn_itom_tag) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Cloud Access Interface (sn_cai)	Bietet einfachen Zugriff auf die Cloud durch Skripting. Sie können diese Anwendung ServiceNow Store verwenden, um Aktionen auf virtuellen Computern auszuführen, die auf Amazon Web Services (AWS) und Microsoft Azurebereitgestellt werden.
Zertifizierungskern (com.snc.certification_core)	Enthält Kernzertifizierungsstrukturen wie Filter und Vorlagen und bietet Compliance-Funktionen.
ITOM-Transparenz Lizenz (com.snc.itom.vis.license)	Ermöglicht die Aktivierung jeder ServiceNow Store -Anwendung, die ITOM-Transparenz eine -Lizenzierung erfordert.
ITOM/OT SU-Lizenzierung sn_itom_licensing	Berechnet, wie viele Abonnements für ITOM-Anwendungen Ihr Unternehmen erworben und genutzt hat, und zeigt das Ergebnis an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Tag-Governance (sn_itom_tag) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.
Flow Designer-Aktionsschritt – Skript auf MID (com.glide.hub.action_step.script_mid)	Stellt einen Aktionsschritt zum Ausführen von anwenderdefiniertem JavaScript innerhalb einer wiederverwendbaren Aktion für einen MID-Server bereit.

Arbeitsbereich für Cloud-Vorgänge

Mit Arbeitsbereich für Cloud-Vorgänge (sn_cloud_ops_ws) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Muster für Discovery und Service-Mapping (sn_itom_pattern)	Stellt die neuesten im ServiceNow Store veröffentlichten Versionen von Muster für Discovery und Service-Mapping bereit. ServiceNow veröffentlicht im ServiceNow® Store jeden Monat neue Muster, damit Ihr Unternehmen die neuesten Geräte und Anwendungen nach Branchenstandard erkennen kann.
Cloud Provisioning and Governance Core (com.snc.cloud.core)	Enthält Ressourcenblöcke und Cloud API-Zuordnungen (Cloud Application Programming Interface) im Zusammenhang mit der Cloud API-basierten Erkennung und Ereignissen, die entweder durch Antwortzuordnungs- oder Aufrufmuster verarbeitet werden.
Performance Analytics Inhaltspaket für Cloud-Ressourcen (sn_disco_cd)	Zeigt die zusammengefasste Ansicht aller Ihrer Cloud-Ressourcen an. Sie bietet auch Analytics-Tabellen und -Ansichten, die Tags mit Ressourcen verknüpfen, sodass Sie Ihre eigenen anwenderdefinierten Dashboards und Berichte erstellen können.
Musterdesigner (NG-Version) (com.snc.ng.pattern.designer)	Die NG-Version (nächste Generation) von Musterdesigner, mit der Sie Muster erstellen, bearbeiten und debuggen können, die von der horizontalen Erkennung und der Erkennung von oben nach unten verwendet werden.

Agent Client Collector Visibility – Inhalt

Mit Agent Client Collector Visibility – Inhalt (sn_acc_visibility) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Agent Client Collector Visibility – Inhalt Inhalt (sn_acc_vis_content)	Bietet agentbasierte Infrastruktur-Discovery und sammelt Software Asset Management (SAM)-Metriken zur Unterstützung der Anwendungen Discovery und Digitale Endanwender-Experience (DEX).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Agent Client Collector Visibility – Inhalt (sn_acc_visibility) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.
Agent Client Collector Framework (sn_agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
CMDB CI-Klassenmodelle (sn_cmdb_ci_class)	Fügt Klassenmodelle hinzu, die die CMDB-Klassenhierarchie erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen, falls zutreffend. Anwendungen wie Discovery und Service-Mapping können diese Klassenerweiterungen verwenden, um Konfigurationselemente (CIs) auszufüllen und verschiedene Technologien und Software zu erkennen.

Agent Client Collector Visibility – Inhalt Inhalt

Mit Agent Client Collector Visibility – Inhalt Content (sn_acc_vis_content) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Erweitertes Modell und Asset-Klassen (sn_ent)	Stellt neue, erweiterte Modellklassen, Asset-Klassen und Modellkategorien bereit, die im Basissystem enthalten sind und durch ServiceNow definiert werden. Installieren Sie das Plugin „Asset-Management“ (com.snc.asset_management) als Voraussetzung zur Nutzung dieser Anwendung.
Discovery – IP-basiert (com.snc.discovery.ip_based)	Enthält gemeinsam genutzte Komponenten der Horizontal-Discovery, die von Discovery und Service-Mappingverwendet werden.
Agent Client Collector Framework (sn_agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
CMDB CI-Klassenmodelle (sn_cmdb_ci_class)	Fügt Klassenmodelle hinzu, die die CMDB-Klassenhierarchie erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen, falls zutreffend. Anwendungen wie Discovery und Service-Mapping können diese Klassenerweiterungen verwenden, um Konfigurationselemente (CIs) auszufüllen und verschiedene Technologien und Software zu erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

- Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate
- Mit installierte Plugins oder Anwendungen ITOM-Integrität
- Mit aktivierte Plugins ITOM-Optimierung
- Mit Now Assist für ITOM installierte Anwendungen

ITOM-Integrität

Das Produkt ServiceNow® ITOM-Integrität umfasst die Anwendungen ServiceNow® Ereignismanagement und ServiceNow® Metrikdaten, die Ihnen helfen, die Integrität von Services in Ihrer Organisation nachzuverfolgen und aufrechtzuerhalten.

Funktionen von ITOM-Integrität

Ereignismanagement

Ereignismanagement sammelt Warnungen von Infrastruktur-Events, die von Überwachungstools von Drittanbietern erfasst werden. Ereignismanagement verwendet IT-bezogene Informationen, die von Discovery gesammelt wurden, um Konfigurationselemente Warnungen zuzuordnen. Basierend auf den erfassten Informationen stellt Ereignismanagement Dashboards bereit, die eine konsolidierte Ansicht aller Serviceeinfluss-Events anzeigen.

Agent Client Collector

Mit der Anwendung ServiceNow® Agent Client Collector können Sie die Serviceverfügbarkeit überwachen, Integrität und Leistung Ihrer Umgebung untersuchen und sicherstellen, dass Ihre Infrastruktur und die darin enthaltenen Anwendungen ordnungsgemäß ausgeführt werden. Sie können Metrikdaten auch verwenden, um Ihre IT-Infrastruktur proaktiv zu analysieren und so Probleme zu erkennen und Serviceausfälle zu verhindern. Mithilfe von erweitertem maschinellem Lernen zur Analyse von Informationen über Ihre IT-Infrastruktur ermittelt die Anwendung Metrikdaten automatisch dynamische Schwellenwerte und identifiziert Anomalien, die auf potenzielle Serviceausfälle hindeuten.

Health Log Analytics

Die Anwendung ServiceNow® Health Log Analytics prognostiziert IT-Probleme, bevor Benutzer durch diese beeinträchtigt werden. Die Anwendung hilft Ihnen, Probleme schneller zu lösen, indem maschinell generierte Protokolldaten in Echtzeit erfasst, interpretiert und korreliert werden. Sie erkennt jede Abweichung vom normalen Verhalten, sobald sie auftritt, und warnt Sie vor möglichen geschäftlichen Auswirkungen. Health Log Analytics empfängt und verarbeitet Protokolle über den MID-Server und sendet Events an die Anwendung ServiceNow® Ereignismanagement.

Service Operations-Arbeitsbereich für ITOM

Service Operations-Arbeitsbereich for ITOM ist ein konfigurierbarer Arbeitsbereich, der eine einheitliche Experience für mehrere IT Operations Management-Workflows bietet. Mit Service Operations-Arbeitsbereich for ITOM können Sie den Lebenszyklus von Warnungen verwalten, einschließlich der Ausführung von Aktionen zum Auflösen von Warnungen und Identifizieren des zugrunde liegenden Problems einer Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ITOM-Integrität Lizenzierung

Bei der für Now Platform® verwendeten Lizenzierungsmethode zahlt Ihre Organisation für die Nutzung von ITOM-Integrität Anwendungen. ITOM-Integrität und Health Log Analytics sind als separate Lizenzen verfügbar. Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung und -Abonnements.

Guided Setup zum Implementieren von IT Operations Management-Anwendungen

Das IT Operations Management-Guided Setup mit Anleitung bietet eine Reihe an Aufgaben, die Sie beim Konfigurieren von IT Operations Management-Anwendungen auf Ihrer ServiceNow-Instanz unterstützen. Um das geführte Setup für IT Operations Management zu öffnen, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**. Weitere Informationen zur Nutzung der Guided Setup-Benutzeroberfläche finden Sie unter Guided Setup verwenden .

MID-Webservererweiterung konfigurieren

Dank der Erweiterung „MID Web Server“ können externe Clients Metrikdaten per Push an den MID Server übertragen. Konfigurieren Sie die MID-Webservererweiterung, um die ITOM Health-Funktionen (Ereignismanagement, Agent Client Collector und Health Log Analytics) zu aktivieren.

ITOM-Integrität – Anwendungsfall

Moderne Unternehmen setzen innerhalb des IT-Betriebs (AIOps) auf Technologien der künstlichen Intelligenz (KI), um das eskalierende Volumen und die eskalierende Vielfalt von Daten zu bewältigen. AIOps-Plattformen bieten Lösungen für die Analyse von Daten, die Automatisierung von Prozessen und die präventive Vorhersage von Problemen, um der zunehmenden Komplexität von IT-Umgebungen Rechnung zu tragen.

Zu den wichtigsten Funktionen des Anwendungsfalls ITOM-Integrität gehören:

- Erfassung von Ereignissen und Metriken über Basissystem -Integrationen mit ausgewählten Überwachungssystemen.
- Verarbeiten von Ereignissen und Metriken, um Warnungen zu erstellen.
- Sie korrelieren Warnungen und führen eine Ursachenanalyse durch.
- Anomalien im System erkennen
- Berechnung der Auswirkung auf Anwendungsservices.
- Verwendung des Service Operations-Arbeitsbereichs für das Betriebsmanagement.
- Automatisieren von Korrekturaktionen basierend auf Warnungen.

Anwendungsservicezuordnungen sind für Betreiber von Network Operations Center (NOC) an zentralen Hubs von entscheidender Bedeutung, da sie die genaue Vorhersage von Ursachenwarnungen und die Korrelation dieser Warnungen mit erkannten Topologiedaten erleichtern. Diese Korrelation ermöglicht eine genaue Vorhersage der Auswirkungen auf Services. So können Sie anhand einer effektiven Auswirkungsanalyse die Auswirkungen auf Anwendungsservices ermitteln und in der Anwendungsservice-Zuordnung visualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Produkte, die ITOM-Integrität Mehrwert hinzufügen

Im Kontext von ITOM-Integrität, dessen Schwerpunkt auf der Aufrechterhaltung der Integrität und Leistung von IT-Systemen und -Infrastrukturen liegt, gibt es mehrere Produkte ServiceNow von , die einen erheblichen Mehrwert bieten können:

Discovery

Discovery identifizieren und erfassen automatisch Informationen über IT-Assets, -Konfigurationen und -Beziehungen. Dadurch erhalten Unternehmen einen umfassenden Bestand, mit dem sie ihre IT-Infrastruktur effektiv verwalten und überwachen können.

Service-Mapping

Service-Mapping bietet detaillierte Informationen zu Anwendungsinstanzservices in der Tabelle [cmdb_ci_service_discovered]. Diese Daten helfen beim Herstellen von Verbindungen zwischen Infrastruktur- und Anwendungskonfigurationselementen (CIs), die in der Tabelle [cmdb_ci_appl] gespeichert sind, verbessern die Transparenz in IT-Umgebungen und ermöglichen effiziente Verwaltungs- und Überwachungsprozesse.

Service-Portfoliomanagement

Service-Portfoliomanagement (SPM) bietet das zugehörige Produktmodell, während Software Asset Management (SAM) und Hardware Asset Management (HAM) Lebenszyklusdaten für Technologie-Portfoliomanagement (TPM) bereitstellen. Zusammen ermöglichen sie eine umfassende Verwaltung von IT-Assets und stellen eine effektive Nutzung, Compliance und Optimierung während ihrer Lebenszyklen sicher.

Produkte, die von ITOM-Integrität profitieren

Incident-Management

Die ToolsIncident-Management nutzen nachgelagerte Informationen von Ereignismanagement, um schnell Incidents zu erstellen und so eine rechtzeitige Lösung von Problemen sicherzustellen.

Kundenservice-Management (CSM)

Kundenservice-Management (CSM) -Systeme profitieren von ITOM-Integrität, indem sie Auswirkungsdaten von Anwendungsservices verwenden, um betroffene Benutzer umgehend zu identifizieren und so die Effizienz und Zufriedenheit des Kundensupports zu verbessern.

Ereignismanagement

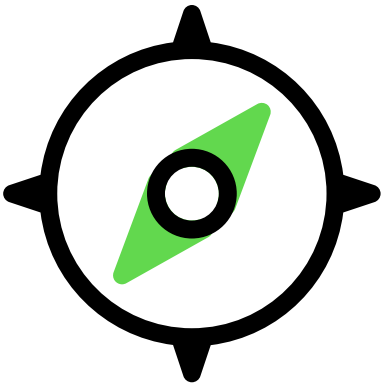
ServiceNow® Ereignismanagement ist eine robuste Anwendung, die hilft, Ihre IT-Systeme in einwandfreiem Zustand zu halten, indem Probleme schnell erkannt und behoben werden. Es sammelt Ereignisse aus verschiedenen Quellen, ermittelt die Ursachen der Probleme und wandelt sie in Warnungen um. Diese Warnungen werden dann analysiert, gruppiert und bearbeitet, um Probleme zu beheben und die Systemintegrität aufrechtzuerhalten.

Ereignismanagement lässt sich über Connectors und Listener nahtlos in verschiedene Überwachungstools integrieren, was eine umfassende Datenerfassung und -korrelation ermöglicht. Ereignismanagement ist als separates Abonnement von der Hauptplattform ServiceNow verfügbar und ermöglicht Unternehmen, ihre Nutzung an bestimmte Bedürfnisse anzupassen, und stellt so ein effektives und effizientes Incident-Management ohne unnötigen Aufwand sicher.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

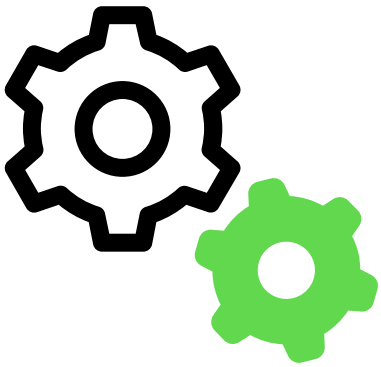
Erste Schritte

Untersuchen



Machen Sie sich mit den verschiedenen Arten der Warnungsgruppierung und den Regeln für die Korrelation vertraut

Konfigurieren

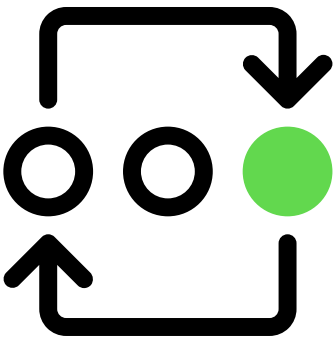


Einrichtung Ereignismanagement

Verwenden

Zeigen Sie Warnungsinformationen an, und überwachen Sie die Serviceintegrität

Integrationen



Erfahren Sie, wie Sie Ereignismanagement in andere Überwachungssysteme integrieren können

Ereignisverarbeitung

Nachvollziehen, wie Ereignisse analysiert und verwaltet werden

Referenz

Rufen Sie Details zu Domain Separation in ab Ereignismanagement

Automatische Übersetzung

Problembehandlung und Hilfe

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Fragen in der Event Management Community stellen oder beantworten
- Technischen Support von ServiceNow kontaktieren
- Video: Erste Schritte mit Ereignismanagement
- Videos: Erste Schritte mit ITOM

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Entwicklerschulungen
- Entwicklerdokumentation

Ereignismanagement erkunden

Erkunden Sie Ereignismanagement, um sich mit der Übersicht, dem Prozessablauf, den Anwenderrollen und den Vorteilen für eine umfassende Überwachung und Lösung von IT-Problemen vertraut zu machen.

Ereignismanagement bietet eine umfassende Überwachung, Analyse und Behebung von IT-Problemen durch die effektive Verwaltung verschiedener Komponenten in einer IT-Umgebung. Zu diesen Komponenten gehören erkannte Services, Anwendungsservices, dynamische CI-Gruppen und Warnmeldungsgruppen.

- Erkannte Services: Ein erkannter Service, der durch verbundene Configuration Items (CIs) aus der CMDB definiert wird, wird durch Service Mapping identifiziert. Sie enthält eine Servicezuordnung mit Zuordnungsbeziehungen, eine Auswirkungsstruktur, die den Schweregrad der Ausfälle, aktive und zugehörige Warnungen und CI-Eigenschaften anzeigt. Diese Serviceinformationen werden in Dashboards, in der Warnungsliste und in der Ereignisliste angezeigt.
- Anwendungsservices: Anwendungsservices werden durch die Auswahl bestimmter CIs erstellt und ermöglichen eine gezielte Überwachung und Verwaltung. Weitere Informationen finden Sie in der Dokumentation zu Anwendungsservices.
- Dynamische CI-Gruppen: Dies sind Sammlungen von CIs, die nach gemeinsamen Kriterien gruppiert sind, z. B. nach dem Standort. Dynamische CI-Gruppen helfen beim Füllen von Anwendungsservices und vereinfachen so die Verwaltung.
- Warnmeldungsgruppen: Warnmeldungsgruppen organisieren Warnungssätze, um die Wartung und Verwaltung zu optimieren und dadurch eine effiziente Reaktion auf IT-Probleme zu erleichtern.

Prozessablauf

Ereignismanagement empfängt externe Ereignisse und generiert Warnungen basierend auf vordefinierten Regeln. MID-Server fragt externe Ereignisnachverfolgungstools ab und sendet Daten an Ereignismanagement zur Speicherung und Verarbeitung. Ereignisse werden in der Tabelle „Ereignis“ [em_event] gespeichert, und Warnungen werden durch den Abgleich von Ereignisregeln erstellt. Warnungen werden dann umgewandelt und mit zusätzlichen Inhalten angereichert, gesammelt, wenn die Schwellenwerte erreicht werden, und bestimmten Feldern zugeordnet. Das System sucht nach übereinstimmenden Nachrichtenschlüsseln, um vorhandene Warnungen zu aktualisieren oder neue zu erstellen und zugehörige Ereignisse unter einer einzigen Warnung zuzuordnen. Für die Ursachenanalyse werden Warnungen an bestimmte Configuration Items (CIs) gebunden. Weitere Informationen finden Sie unter Prozess-Flow in Ereignismanagement.

Anwender

Rollentitel [Name]	Beschreibung
Administrator [evt_mgmt_admin]	Hat Lese- und Schreibzugriff auf alle Ereignismanagement-Funktionen zum Konfigurieren von Ereignismanagement.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung
	Hinweis: Seien Sie vorsichtig mit der Rolle evt_mgmt_admin, die zur Administratorrolle hochgestuft werden kann. Ein Benutzer mit der Rolle „evt_mgmt_admin“ kann Skripts hinzufügen und ändern, die in einem globalen Bereich ausgeführt werden. Stellen Sie eine ordnungsgemäße Zugriffssteuerung sicher. Mit dieser Rolle kann der Benutzer die folgenden Skripts erstellen und/oder aktualisieren: • Regeln zur Warnungskorrelation • Warnungsverwaltungsregeln • Wartungsregeln • Erweiterte Skripts • Ereignisfeldzuordnung • Vor- und Nachbindungsskripts
Betreiber [evt_mgmt_operator]	Verwaltet Warnungen, einschließlich Schließen und Bestätigen von Warnungen. Überwacht den gesamten Prozess Ereignismanagement und stellt sicher, dass Ereignisse ordnungsgemäß kategorisiert, priorisiert und zur Lösung weitergeleitet werden.
Teamoperator [evt_team_operator]	Verwaltet Vorgänge Ereignismanagement innerhalb eines bestimmten Teams, wie im Feld **Zuweisungsgruppe** definiert. Mit dieser Rolle kann der Bediener Warnungen ausschließlich für das ihm zugewiesene Team lesen und schreiben. Darüber hinaus kann der Operator Konfigurationsänderungen speziell für sein Team vornehmen, einschließlich Updates für die Warnungsautomatisierung und das Integrations-Launchpad. **Hinweis:** Die Rolle evt_team_operator muss einer Zuweisungsgruppe zugewiesen werden, um Warnungen für diese Gruppe anzuzeigen und zu verwalten. Wenn die Rolle erstellt, aber keinen Gruppen zugeordnet ist, denen Warnungen zugewiesen sind, kann der Bediener keine Warnungen sehen.
Anwender [evt_mgmt_user]	Verwaltet den Lebenszyklus von Warnungen, einschließlich der Durchführung grundlegender Vorgänge wie Anzeigen und Bestätigen von Warnungen.

Vorteile

- Schnelle Problemerkennung: Identifiziert und hebt schnell potenzielle IT-Probleme hervor.
- Effiziente Warnungsverarbeitung: fasst Warnungen zusammen und korreliert Warnungen, um die Verwaltung zu optimieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Automatisierte Aktionen: Initiiert automatische Korrekturprozesse, um die Problemlösung zu beschleunigen.
- Umfassende Überwachung: Integration mit mehreren -Tools für einen vollständigen Systemüberblick.
- Ursachenanalyse: Bietet Tools zur Identifizierung der zugrunde liegenden Ursachen von Problemen.
- Anpassbare Regeln: Passt Event- und Warnungsverwaltungsregeln an bestimmte Anforderungen an.
- Reduzierte Ausfallzeit: Minimiert die Ausfallzeit des Systems durch schnelle Problemlösung.
- Verbesserte Transparenz: Echtzeit-Dashboards bieten Einblicke in die Systemintegrität.
- Kosteneffizienz: Senkt die Betriebskosten, indem längere Probleme verhindert werden.

Prozess-Flow in Ereignismanagement

Ereignismanagement sammelt, analysiert und konvertiert Ereignisse in Warnungen und ermöglicht so eine effiziente Nachverfolgung und Behebung.

Ereignismanagement empfängt externe Events und generiert Warnungen basierend auf den Event- und Warnungsverwaltungsregeln. Ereignisse werden über E-Mail-Server, Skript, SNMP-Trap oder Webservice-API direkt an Ihre Instanz gesendet. Die entsprechenden Warnungen werden zu Nachverfolgungs- und Nachbesserungszwecken in Dashboards angezeigt.

Während der Computer, die Software oder der Service Events generiert, ruft der MID-Server das externe Event-Nachverfolgungstool ab. Der MID-Server, der eine Verbindung zu Ereignismanagementaufrechterhält, sendet die Informationen zur Speicherung, Verarbeitung und Korrektur an Ihre -Instanz.

Die Instanz speichert Ereignisse in der Tabelle „Ereignis“ [em_event] und versucht, Warnungen basierend auf vordefinierten Regeln und Ereigniszuordnungen zu generieren. Unabhängig davon, ob eine Warnung generiert wird, steht das ursprüngliche Ereignis zur Überprüfung und Korrektur zur Verfügung. Warnungen werden gemäß dem folgenden Prozessablauf generiert.

1. Ereignisregel abgleichen: Suchen Sie die am besten übereinstimmende Ereignisregel für ein Ereignis.

   Eine Regel wird abgeglichen, wenn die Quelle des Ereignisses mit der in einer vorhandenen Regel angegebenen Quelle übereinstimmt. Darüber hinaus wird eine Regel abgeglichen, wenn das Ereignis mit dem optionalen Regelfilter übereinstimmt und der Wert „additional_info“ des Ereignisses mit dem Filter „Zusätzliche Informationen“ der Regel übereinstimmt. Eine Regel ohne Filter wird ignoriert, z. B. wenn der Quellfilter oder der Filter „Zusätzliche Informationen“ fehlen. Wenn mehrere Regeln für den gleichen Ereignistyp definiert sind, verwenden Sie die Regelreihenfolge, um die Reihenfolge der Regelanwendung zu bestimmen.

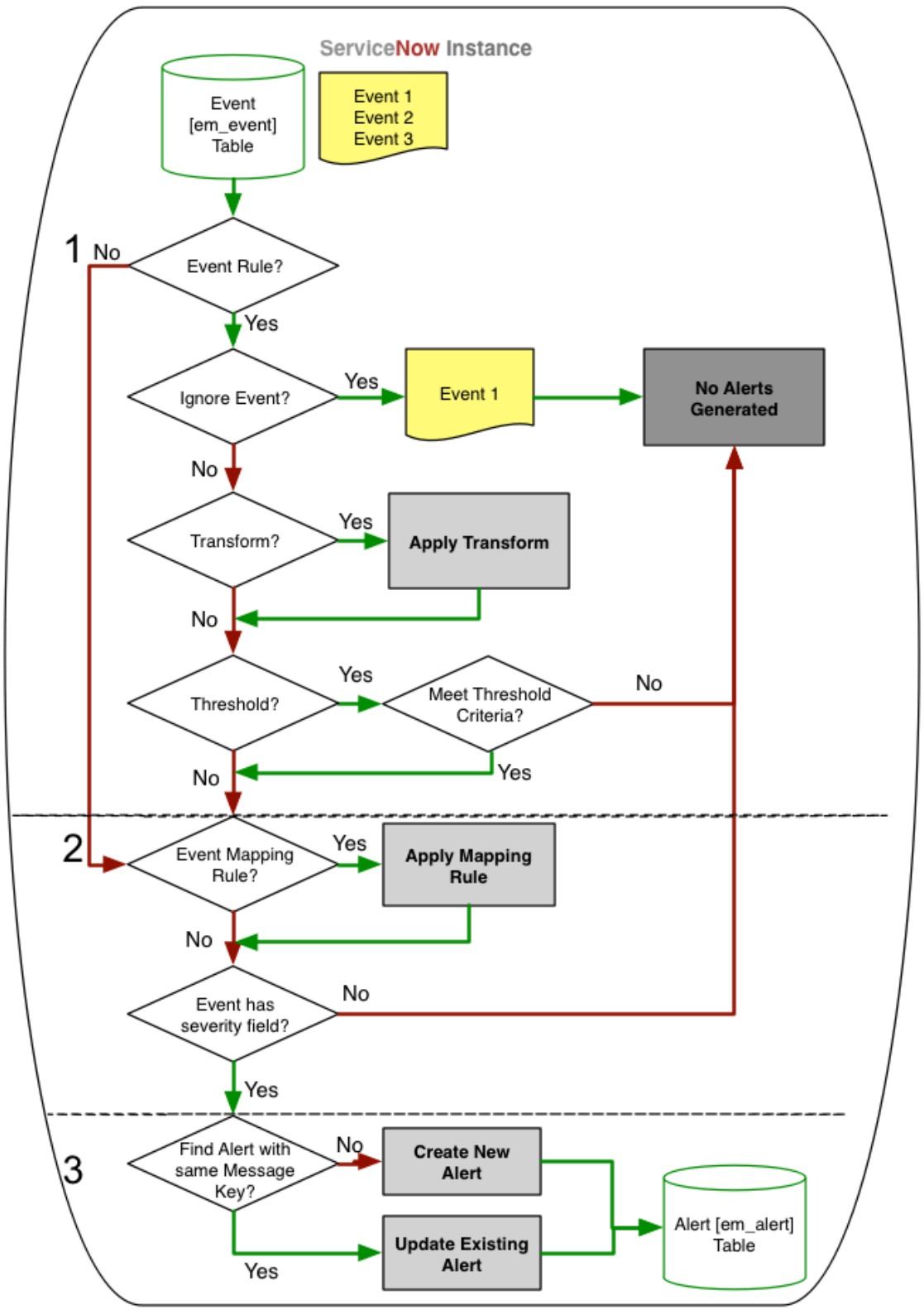
2. Regel ignorieren: Wenn das Kontrollkästchen Regel **ignorieren** aktiviert ist, wird keine Warnung generiert. Das Event steht jedoch weiterhin zur Überprüfung und Nachbesserung zur Verfügung.
3. Transformationen anwenden:
   - Wenn Umwandlungen definiert wurden, wenden Sie sie an.
   - Wenn Erstellungsparameter festgelegt sind, wenden Sie den zusätzlichen Inhalt an, der dem Benutzer in der Warnung angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Schwellenwertakkumulation: Wenn im Abschnitt „Schwellenwert“ Aktiv ausgewählt ist, werden alle Ereignisse gesammelt, bis der Schwellenwert erreicht ist, und dann wird eine einzelne Warnung für die Ereignisse generiert.
5. Ereignisfeldzuordnung
   - Suchen Sie nach einer Event-Feldzuordnung, auch wenn keine Event-Regel vorhanden war.
   - Wenn eine Event-Feldzuordnung gefunden wird, wenden Sie die Zuordnungsinformationen an.
   - Wenn das Event nach den Event-Umwandlungen keinen Schweregrad aufweist, behalten Sie das Event zu Referenzzwecken bei und generieren Sie keine Warnung.
6. Warnungsgenerierung
   - Durchsuchen Sie die Warnungstabelle [em_alert] nach einem passenden Nachrichtenschlüssel.
   - Wenn ein passender Nachrichtenschlüssel vorhanden ist, aktualisieren Sie die Warnung entsprechend den Event-Informationen.
   - Wenn kein passender Nachrichtenschlüssel vorhanden ist, erstellen Sie eine Warnung.
   - Wenn ein anderes Event denselben übereinstimmenden Schlüssel aufweist, ordnen Sie die Events einer einzelnen Warnung zu.
   - Binden Sie für die Ursachenanalyse die Warnung an ein bestimmtes Configuration Item (CI) an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Workflow



Automatische Übersetzung

Ereignismanagement-Architektur

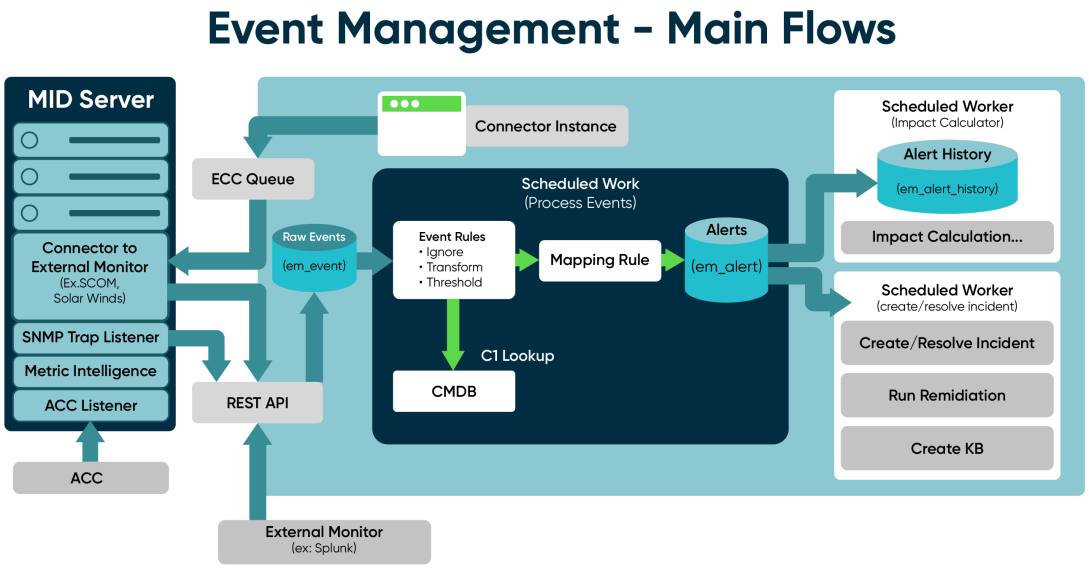
Ereignismanagement -Architektur integriert die Datenerfassung, -verarbeitung und -warnung in ein einheitliches System, um die Erkennung und Lösung von IT-Problemen zu optimieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Architektur

Wenn Ereignisse auf verschiedenen Systemen auftreten, werden sie von der Connector-Instanz MID-Server an die Hauptinstanz gesendet. Ereignismanagement generiert Warnungen, wendet Warnungsverwaltungsregeln an und priorisiert Warnungen für die Behebung und Ursachenanalyse. Diese Informationen können in Dashboards, in der Warnungsliste in Alert Intelligence oder in einer Servicezuordnung angezeigt werden.

Ereignismanagement-Architektur



Ereignismanagement konfigurieren

Ereignismanagement-Administratoren verwalten Events, verwalten und überwachen Warnungen, fassen Warnungen zusammen und prüfen und überwachen den Status von Services mit dem Service Monitor des Betreiber-Arbeitsbereichs.

Ereignismanagement-Operatoren suchen nach Warnungen, analysieren sie und ergreifen Maßnahmen zur Lösung des zugrunde liegenden Problems.

Event Management für Anforderungen

Das Plugin Ereignismanagement (com.glideapp.itom.snac) erfordert ein separates Abonnement und muss von Mitarbeitern von ServiceNow aktiviert werden. Dieses Plugin enthält Demodaten und aktiviert zugehörige Plugins, wenn sie nicht bereits aktiv sind.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktionsinstanz bzw. untergeordneten Produktionsinstanz Ihrer Organisation.

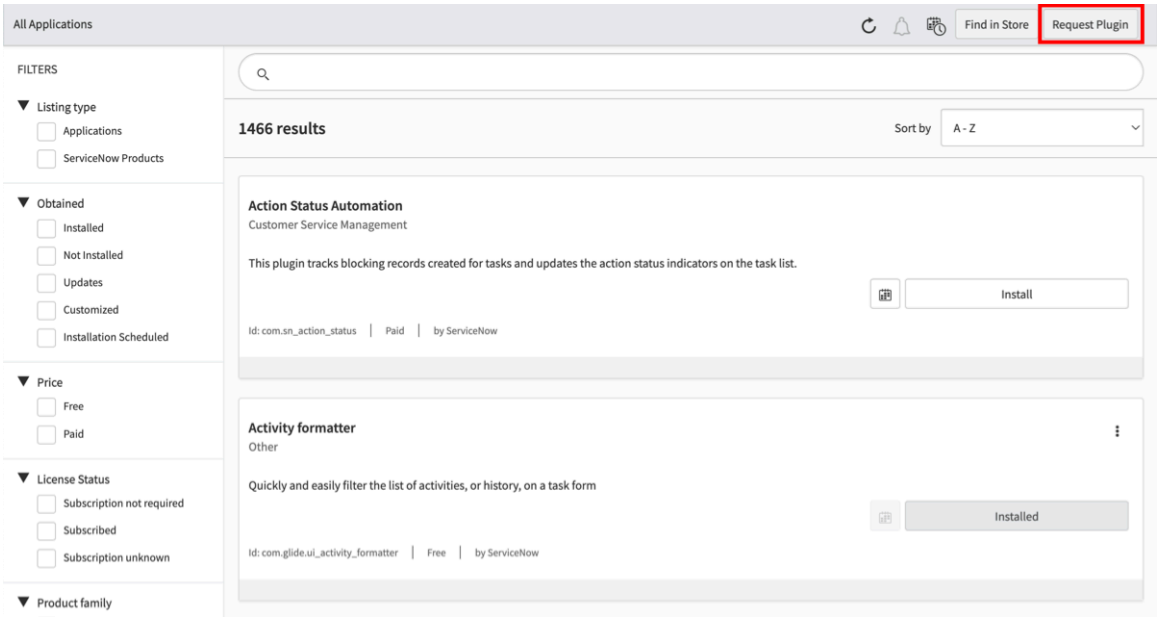
Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Automatische Übersetzung

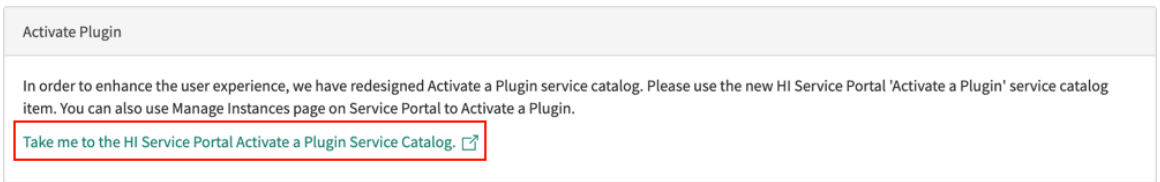
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins

Automatische Übersetzung

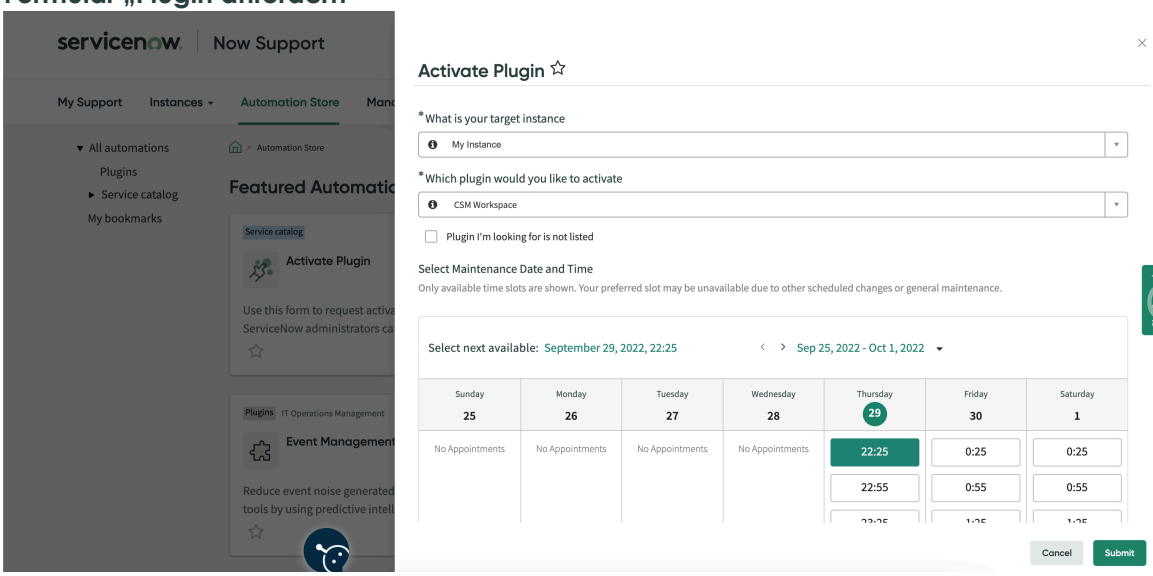
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-Artikel [KB0751715] in Now Support Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignismanagement installieren

Laden Sie aus dem ServiceNow® Store die aktuellen Apps für die Anwendung Ereignismanagement (com.glideapp.itom.snac) herunter. Überprüfen Sie den ServiceNow® Store regelmäßig auf neue App-Versionen.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

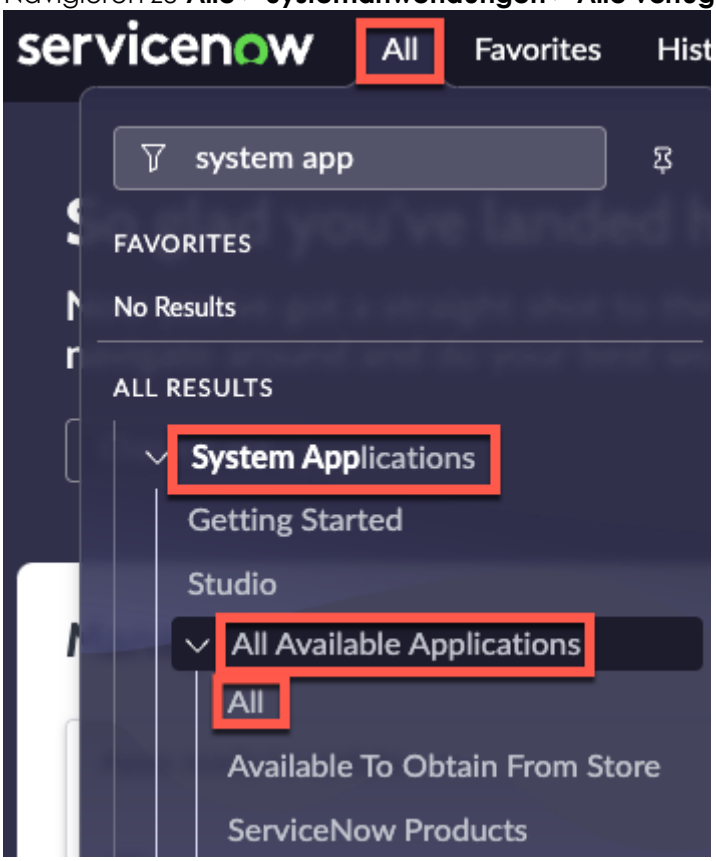
Die folgenden Elemente werden mit Ereignismanagement installiert:

- Rollen
- Regelmäßige Aufgaben
- Tabellen

Weitere Informationen finden Sie unter Mit Ereignismanagement installierte Komponenten.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie die Anwendung ITOM-Integrität über die Filterkriterien und die Suchleiste.

   Wenn Sie die Anwendung nicht finden können, fordern Sie sie über den ServiceNow Store an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Überprüfen Sie im Dialogfeld „Anwendungsinstallation" die Anwendungsabhängigkeiten.

   Abhängige Plugins und Anwendungen werden aufgelistet, wenn sie installiert werden sollen, derzeit installiert sind oder installiert werden müssen. Wenn die Installation von Plugins oder Anwendungen erforderlich ist, müssen Sie sie installieren, bevor Sie Ereignismanagement installieren können.

4. Wahlweise: Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.

   (Optional) Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für häufige Anwendungsfälle veranschaulichen. Das Laden von Demodaten wird empfohlen, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

   Wichtig: Wenn Sie die Demodaten nicht während der Installation laden, stehen sie nicht zum späteren Laden zur Verfügung.

5. Wählen Sie **Installieren** aus.

Ereignismanagement-Leistung verbessern

Das Beschleuniger-Plugin Ereignismanagement stellt sicher, dass Ereignismanagement die Leistung auf hohem Niveau hält. Dieses Plugin ist optional.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die Tabellen *em_alert_history* und *em_impact_status* können sehr groß werden, was sich negativ auf die Leistung von Ereignismanagement auswirkt. Durch Installieren des Beschleuniger-Plugins Ereignismanagement stellen Sie sicher, dass Ereignismanagement die Leistung auf hohem Niveau hält.

Beim Upgrade von einer früheren Version mit mehr als 5 Millionen Datensätzen in den Tabellen *em_alert_history* oder *em_impact_status* müssen Sie dieses Plugin manuell aktivieren. Wenn weniger als 5 Millionen Datensätze vorhanden sind, wird sie automatisch ausgeführt. Sie können diese Zahl anpassen, indem Sie die Eigenschaft *evt_mgmt.plugin_activation.table_max_size* ändern.

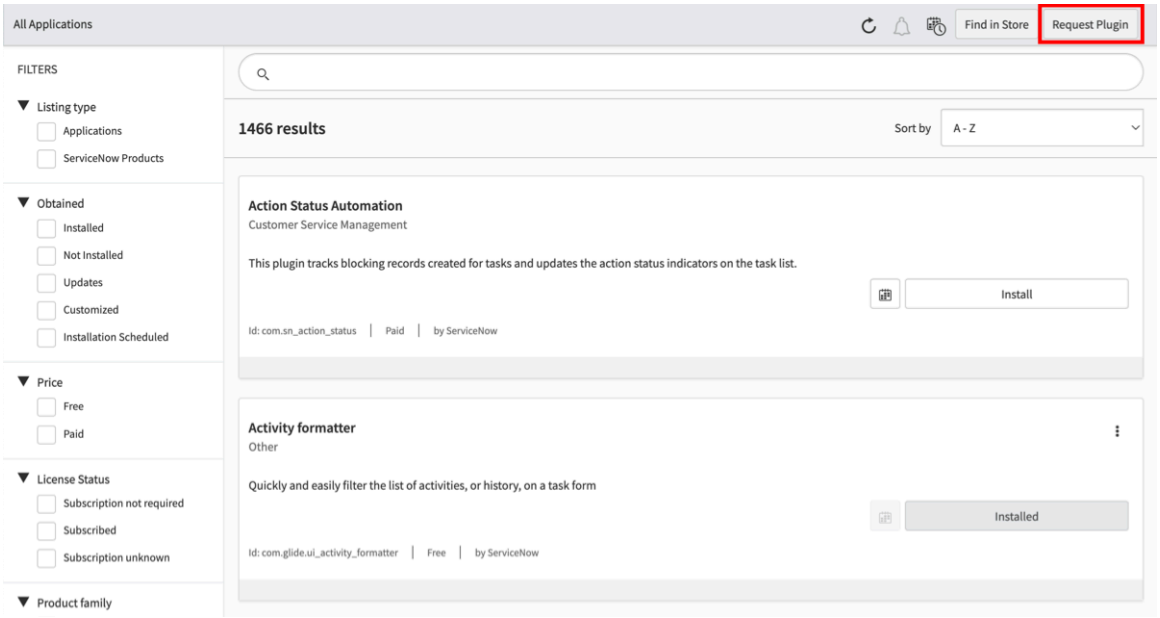
Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktionsinstanz bzw. untergeordneten Produktionsinstanz Ihrer Organisation.

Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

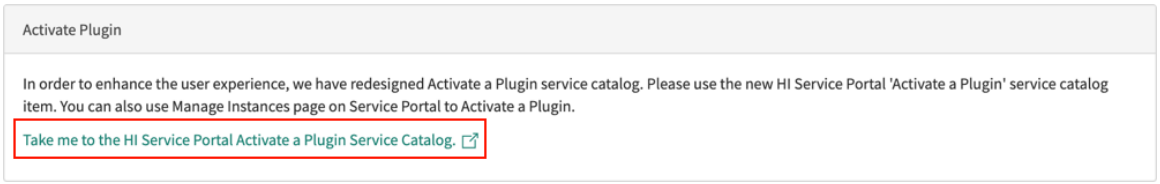
Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen" auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.
5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.

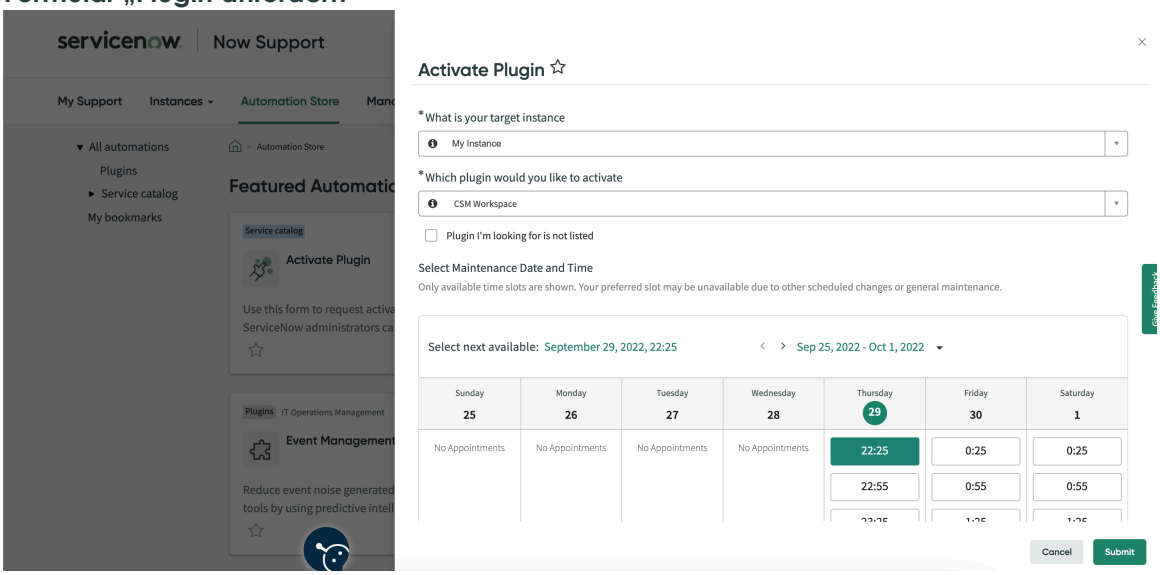
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-Artikel [KB0751715] in Now Support Knowledge Base.

Setup von Ereignismanagement

Nach der Aktivierung von Ereignismanagement richten Sie es so ein, dass es Events empfängt und verarbeitet sowie Warnungen generiert und analysiert.

Einrichtung von Ereignismanagement ohne Guided Setup

Richten Sie Ereignismanagement ein, indem Sie diese Aufgaben in der folgenden Reihenfolge ausführen:

1. Konfigurieren Sie einen MID-Server, um Ereignisse über MID-Serverzu empfangen und zu verarbeiten.
2. MID-Webservererweiterung konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Konfigurieren Sie Konfigurieren Sie Ereignismanagement die -Connectors.
4. Konfigurieren Sie Ereignisfeldzuordnungen und Warnungen an CIs binden, um die Generierung von Warnungen zu verwalten.
5. Warnungsverwaltungsregeln zum Auflösen von Warnungen, Durchführen und CI-Korrektur für die Warnungsverwaltung.
6. Fordern Sie Service Mapping an, und rufen Sie eine Top Down -Discovery ab, um CI-Beziehungen für Software und Hardware zu erhalten.
7. Konfigurieren Sie die Auswirkungsberechnung für Services, um die Priorität für die Warnungsauflösung festzulegen.
8. Konfigurieren Sie Warnungsgruppen, um zugehörige Warnungen zu konsolidieren.
9. Konfigurieren Sie das Plugin Predictive Intelligence (com.glide.platform_ml), um maschinelles Lernen und die Suche nach ähnlichen Warnungen zu ermöglichen.
10. Konfigurieren Sie gegebenenfalls alle anderen allgemeinen Aufgaben, die in diesem Abschnitt angezeigt werden.

Hinweis: Ereignismanagement unterstützt nicht das Erstellen von Incidents auf Remote-Instanzen.

Einrichtung von Ereignismanagement mit Guided Setup

Das Guided Setup für Ereignismanagement stellt eine Reihe von Aufgaben bereit, die Sie beim Konfigurieren von Ereignismanagement in Ihrer ServiceNow-Instanz unterstützen. Um das geführte Setup für Ereignismanagement zu öffnen, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Ereignismanagement während eines Plattform-Upgrades

Während eines Plattform-Upgrades werden weiterhin Ereignismanagement-Jobs ausgeführt, deren Flag für **sicheres Upgrade** als `„true“` markiert ist.

Während eines Upgrades der Plattform funktionieren die Ereignismanagement-Connectors und rufen weiterhin Events ab. Die Events werden verarbeitet und mithilfe von Event-Regeln in eine Warnung umgewandelt. Wenn eine geeignete Warnungsverwaltungsregel vorhanden ist, wird eine Aufgabe erstellt. Die Auswirkungsberechnung wird jedoch während des Plattform-Upgrades nicht unterstützt. Wenn Konfigurationsänderungen oder Upgrades angewendet werden, werden alle betroffenen MID-Server neu gestartet.

Hinweis: Ereignismanagement-Jobs, die vor Beginn des Plattform-Upgrades gestartet wurden, werden während des Upgrades weiterhin ausgeführt.

Die folgenden Ereignismanagement -Aufträge werden weiter ausgeführt, da das Flag **„Upgrade sicher“** als `„wahr“` markiert ist:

- Ereignismanagement – Connector-Ausführung
- Ereignismanagement –Update abgebrochen
- Ereignismanagement – Warteschlange für Warnungspriorität
- Ereignismanagement – Fluktuierende Warnungen schließen
- Ereignismanagement – Schwellenwertwarnung schließen
- Ereignismanagement - Bereichsbezogenes Regel-Management für Warnungen auswerten0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ereignismanagement – Wartungsrechner
- Ereignismanagement – Events verarbeiten

Während des Plattform-Upgrades warten alle anderen Ereignismanagement-Jobs, bis das Plattform-Upgrade abgeschlossen ist.

Hinweis: Während eines Ereignismanagement-Plugin-Upgrades funktionieren nicht alle Ereignismanagement-Jobs.

MID-Webserver

Der MID-Webserver ist Teil der allgemeinen Infrastruktur des MID-Servers.

Die MID-Webservererweiterung bietet Optionen für Authentifizierung und Datensicherheit und wird ausgeführt, solange sie aktiviert ist. Von der Erweiterung wird ein Webserver auf dem MID-Server gestartet, von dem Webanforderungen von externen Systemen verarbeitet werden. Die Rohdaten werden von einem Client oder mithilfe eines benutzerdefinierten Skripts an die Erweiterung übertragen. Die Daten werden vom MID-Server erfasst und dann zur ServiceNow-Instanz übertragen.

Die MID-Webservererweiterung unterstützt MID-Server-Cluster, die für Failover konfiguriert sind. Wenn Sie die Option für MID Server-Cluster auswählen, wird mit einem Algorithmus ermittelt, auf welchem MID-Server im Cluster die Erweiterung ausgeführt wird. Die Erweiterung kann nur auf einem MID-Server ausgeführt werden. Bei einem Ausfall des MID-Servers im Cluster, auf dem die MID-Webservererweiterung ausgeführt wird, wird die Erweiterung automatisch auf dem sekundären MID-Server ausgeführt, der bei einem Ausfall des primären MID-Servers aktiviert wird.

Zugehörige Informationen

MID-Webservererweiterung konfigurieren

Sichere MID-Webservererweiterung konfigurieren

MID-Webservererweiterung konfigurieren

Der MID-Webserver ist eine MID-Servererweiterung, die die Entwicklung von REST APIs zum Senden von Events und Metriken an den MID-Server ermöglicht. Die Erweiterung wird von anderen MID-Server-Erweiterungen genutzt, z. B. Metrikdaten, MID-WebService-Event-Listener und der Agent Client Collector-Websocket-Endpunkterweiterung.

Vorbereitungen

- Stellen Sie einen MID-Server bereit, und starten Sie ihn.
- Aktivieren Sie das MID-Webserver-Plugin [com.snc.sa.mid.webserver].

Erforderliche Rolle: agent_admin.

Warum und wann dieser Vorgang ausgeführt wird

Agent Client Collector unterstützt die folgenden Authentifizierungsstrategien:

- **Schlüsselbasiert**: Nur für Abwärtskompatibilität (vor Yokohama-Release). Weitere Informationen finden Sie unter Schlüsselbasierte MID-Webserverauthentifizierung konfigurieren.
- **API-Schlüssel**: Siehe API-Schlüsselauthentifizierung für MID-Webserver konfigurieren.
- **mTLS**: Siehe MID-Webserver und Agent-mTLS-Authentifizierung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Erweiterungen** > **MID-Webserver**.
2. Klicken Sie in der Liste MID-Webserver Kontexte auf **Neu**.
3. Geben Sie die Werte im Formular „Ereignismanagement MID-Webservererweiterung“ ein.
4. Klicken Sie auf **Speichern**, um die Daten zu speichern.
5. Starten Sie die MID-Webservererweiterung neu, um Ihre Änderungen anzuwenden.
6. Navigieren zu **Alle** > **MID-Server** > **Erweiterungen** > **MID-Webserver** und wählen Sie das soeben erstellte MID-Server aus.
7. Klicken Sie im Abschnitt **Zugehörige Links** auf **Start**, um die Erweiterung zu starten.

Sichere MID-Webservererweiterung konfigurieren

Konfigurieren Sie einen TLS-Listener für zusätzliche Sicherheit und Verschlüsselung von Daten, die an die und von der MID-Webservererweiterung übertragen werden. Greifen Sie über einen Java-Schlüsselspeicher auf einen privaten Schlüssel und ein Zertifikat (oder eine Zertifikatkette) zu, um sie während des TLS-Handshake zu verwenden, bei dem sich der MID-Webserver und der Client gegenseitig bestätigen.

Vorbereitungen

Erforderliche Rolle: agent_admin

Prozedur

1. Navigieren zu **MID-Server** > **Erweiterungen** > **MID-Webserver**.
2. Wählen Sie **Neu**.
3. Wählen Sie im Feld **Authentifizierungstyp** einen zu verwendenden Authentifizierungstyp aus.
   - Schlüsselbasiert – Siehe Schlüsselbasierte MID-Webserverauthentifizierung konfigurieren
   - Standard – Standardmäßige Authentifizierung mit Benutzername/Passwort
   - API-Schlüssel – Siehe API-Schlüsselauthentifizierung für MID-Webserver konfigurieren
   - mTLS – Siehe MID-Webserver und Agent-mTLS-Authentifizierung
4. Wählen Sie entweder den einheitlichen MID-Schlüsselspeicher oder den Webserver-Schlüsselspeicher aus.
   Der einheitliche MID-Webserver-Schlüsselspeicher ist die effizienteste Option. Wenn Sie die Abwärtskompatibilität und die Möglichkeit zum Speichern von Schlüsselpaaren in einem zusätzlichen Schlüsselspeicher aktivieren möchten, verwenden Sie den Webserver-Schlüsselspeicher (mit dem Sie auch den einheitlichen MID-Schlüsselspeicher verwenden können).

Option	Beschreibung
Einheitlicher MID-Schlüsselspeicher	**a.** Aktivieren Sie das Kontrollkästchen **Einheitlichen MID-Schlüsselspeicher verwenden**. **b.** Geben Sie einen Aliasnamen in das Feld **Schlüsselspeicher-Zertifikatalias** ein oder lassen Sie das Feld leer, um den Standardalias des Schlüsselspeichers zu verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Weitere Informationen finden Sie im Abschnitt **Anwenderdefinierte Zertifikate im einheitlichen Schlüsselspeicher des MID-Servers installieren** in Einheitlicher Schlüsselspeicher des MID-Servers . **Wichtig:** Wenn Sie das Feld **Schlüsselspeicher-Zertifikatalias** leer lassen, wird bei Clients, bei denen eine Verbindung hergestellt wird, die Zertifikatverifizierung übersprungen. Stattdessen wird vom MID-Server sein eigenes selbstsigniertes Zertifikat verwendet.
Webserver-Schlüsselspeicher	**a.** Deaktivieren Sie das Kontrollkästchen **Einheitlichen MID-Schlüsselspeicher verwenden**. **b.** Geben Sie einen Aliasnamen in das Feld **Schlüsselspeicher-Zertifikatalias** ein oder lassen Sie das Feld leer, wenn Sie einen einzigen Alias in diesem Schlüsselspeicher haben. **c.** Wenn sich das Passwort für den privaten Schlüssel des erforderlichen Alias vom Schlüsselspeicher-Passwort unterscheidet, geben Sie den Alias im Feld **Schlüsselpasswort des Schlüsselspeichers** an. **d.** Geben Sie in dem Feld **Schlüsselspeicher-Passwort** das Passwort des Schlüsselspeichers ein.

Schlüsselbasierte MID-Webserverauthentifizierung konfigurieren

Bieten Sie Ihrer MID-Webservererweiterung zusätzliche Sicherheit, indem Sie schlüsselbasierte Authentifizierung verwenden. Generieren Sie ein Authentifizierungstoken, das im Autorisierungsheader eingehender Client-Anforderungen gesendet werden soll.

Vorbereitungen

Hinweis: Dieses Verfahren dient nur der Kompatibilität mit Releases vor Yokohama. Weitere Informationen zum Verfahren im Release Yokohama für die Konfiguration des MID-Webservers finden Sie unter MID-Webservererweiterung konfigurieren.

- Stellen Sie einen MID-Server bereit, und starten Sie ihn.
- Konfigurieren Sie eine MID-Webserver-Erweiterung und wählen Sie „Schlüsselbasiert“ als Authentifizierungstyp aus. Einzelheiten hierzu finden Sie unter MID-Webservererweiterung konfigurieren.

Erforderliche Rolle: agent_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie mit einem Skriptprogramm ein Token, indem Sie mithilfe definierter Elemente der HTTP/HTTPS-Anforderung (HTTP-Verb, Inhaltstypheader und Anforderungspfad, die vom Client empfangen werden, der auf die Endpunkte der MID-Webservererweiterung zugreift) eine Zeichenfolge erstellen.
2. Erstellen Sie einen HMAC (Hash Message Authentication Code) der Zeichenfolge, indem Sie die generierte Zeichenfolge mit dem automatisch generierten geheimen Schlüssel signieren, der unter **Geheimer Key** angezeigt wird.
   Dieser Schlüssel ist pro Kontext eindeutig.
3. Geben Sie Informationen an, um dieses Authentifizierungstoken im Autorisierungsheader der Anforderung zu übermitteln.

Element	Wert
Pfad zu einer Webservice-API zum Senden von Rohdaten	URL-Format: `https://<MID Server-IP-Adresse>:<Portnummer>/api/mid/sa/metrics` Verwenden Sie eine Portnummer, die einer der in der Webservererweiterung eingerichteten Portnummern entspricht. Beispiel: `http://10.10.10.10:8097/api/mid/sa/metrics`
Anforderungstyp	POST
Datumsformat	`yyyy-MM-dd'T'HH:mm:ss.SSS'Z'` Beispiel: 2016-06-08T20:54:58.917Z
Content-Type	Anwendung/JSON

Verwenden Sie die folgenden Anforderungselemente, um die erforderliche Zeichenfolge zu generieren: HTTP-Verb, Inhaltstyp, Datum und Anforderungspfad. Geben Sie diese Elemente an, und platzieren Sie sie in dieser Reihenfolge:

- HTTP-Verb + „\n“ +
- Inhaltstyp + „\n“ +
- Datum + „\n“ +
- Anforderungspfad

In diesem Beispiel lautet die Anforderungszeichenfolge:

```
POST\napplication/json\n2016-06-08T20:54:58.917Z\n/api/mid/sa/metrics
```

Für die Zeitstempelanforderung ist zur Authentifizierung der Anforderung ist ein gültiger Zeitstempel erforderlich, der den HTTP-Datumsheader verwendet. Stellen Sie sicher, dass der Zeitstempel nicht mehr als 15 Minuten von der Zeit des MID Servers abweicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example: Generieren Sie den HMAC der Zeichenfolge, die definierte Elemente der HTTP/HTTPS-Anforderung verwendet, mit Java

```
package sample;
import com.glide.util;
import java.security.SignatureException;

import javax.crypto.Mac;
import javax.crypto.spec.SecretKeySpec;

public class AuthUtil {

private static final String HMAC_SHA1_ALGORITHM = "HmacSHA1";

/***
 * Generates base64-encode the HMAC(Hash Message Authentication Code) of
 input data
 *
 * @param data
 * @param key
 * @return
 * @throws java.security.SignatureException
 */
public static String signData(String data, String key) throws
 java.security.SignatureException {
 String result;
 try {
  // get an hmac_sha1 key from the raw key bytes
  SecretKeySpec signingKey = new SecretKeySpec(key.getBytes(),
 HMAC_SHA1_ALGORITHM);

  // create hmac_sha1 Mac instance and initialize with the signing key
  Mac = Mac.getInstance(HMAC_SHA1_ALGORITHM);
  mac.init(signingKey);

  // compute the hmac on input data bytes
  byte[] rawHmac = mac.doFinal(data.getBytes("UTF-8"));

  // base64-encode the hmac
  result = Base64.encode(rawHmac);

 } catch (Exception e) {
  throw new SignatureException("Failed to generate HMAC : " +
 e.getMessage());
 }
 return result;
}
}
```


API-Schlüsselauthentifizierung für MID-Webserver konfigurieren

Authentifizieren Sie von Clients eingehende Anforderungen an die MID-Webservererweiterung mithilfe der API-Schlüsselauthentifizierung. Die API-Authentifizierung ist eine sichere und einfache Möglichkeit, Ihre Anforderung zu authentifizieren. Sie können einen MID-Webserver-API-Schlüssel erstellen oder ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erstellen Sie eine MID-Webservererweiterung, um die API-Schlüsselauthentifizierung zu verwenden, wie in MID-Webservererweiterung konfigurieren beschrieben. Stellen Sie sicher, dass Sie im Feld **Authentifizierungstyp** der Erweiterung **API-Schlüssel** auswählen.

Erforderliche Rolle: event_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig können Sie in einer Instanz maximal 10 API-Schlüssel erstellen. Um diese Zahl zu ändern, ändern Sie auf der Seite „Systemeigenschaften“ den Wert der Eigenschaft *mid.webserver.max.api.keys*.

Wenn Sie in der globalen Domäne arbeiten, während die Domänentrennung aktiviert ist, sind API-Schlüssel für alle Erweiterungen verfügbar, unabhängig von ihrer Domäne. Wenn Sie in einer bestimmten Domäne arbeiten, stehen API-Schlüssel für Erweiterungen in dieser Domäne, den übergeordneten Domänen und der globalen Domäne zur Verfügung.

Sie können API-Schlüssel so konfigurieren, dass sie an einem bestimmten Datum ablaufen.

Wenn Sie eine neue Erweiterung mit API-Schlüsselauthentifizierung erstellen (oder eine vorhandene aktualisieren, um die API-Schlüsselauthentifizierung zu verwenden), wird vom System nach einem verfügbaren API-Schlüssel für die Erweiterung gesucht. Wenn kein API-Schlüssel verfügbar ist, wird vom System einer erstellt.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Profile und Bereitstellungen** > **MID-Webserver API-Schlüssel**.
2. Erstellen Sie entweder einen neuen API-Schlüssel oder ändern Sie einen vorhandenen API-Schlüssel.
   - So erstellen Sie einen neuen API-Schlüssel:
     a. Wählen Sie **Neu**.
     b. Füllen Sie im Formular „MID-Webserver API-Schlüssel“ die Felder aus.

Formular „MID-Webserver API-Schlüssel“

Feld	Beschreibung
Name	Name für den API-Schlüssel
Aktiv	Option zur Aktivierung des API-Schlüssels
Authentifizierungsschlüssel	Schreibgeschützter codierter Wert des Authentifizierungsschlüssels. Erst nach der Konfiguration des Schlüssels wird ein Wert angezeigt.
Läuft ab	Option zum Festlegen eines Ablaufdatums für den API-Schlüssel. Abgelaufene, deaktivierte oder gelöschte API-Schlüssel werden von der Webservererweiterung nicht akzeptiert.

     c. Wählen Sie **Absenden** aus, um den API-Schlüssel zu speichern.

     Der API-Schlüssel wird auf der Seite „MID-Webserver API-Schlüssel“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

◦ So ändern Sie einen vorhandenen API-Schlüssel:

a. Navigieren zu **MID-Server** > **Profile und Bereitstellungen** > **MID-Webserver API-Schlüssel**.

b. Wählen Sie auf der Seite einen API-Schlüssel aus.

c. Wählen Sie im Abschnitt **Zugehörige Links** die Option **API-Schlüssel anzeigen** aus.

d. Kopieren Sie den API-Schlüssel, der im Dialogfeld „MID-Webserver“ angezeigt wird.

Wenn Sie eine Verbindung mit einer MID-Webservererweiterung herstellen, die mit der API-Schlüsselauthentifizierung konfiguriert ist, fügen Sie einen API-Schlüssel, auf den die Erweiterung zugreifen kann, im Autorisierungsheader der Anforderung im folgenden Format ein:

```
Key <API_KEY>
```

Dabei ist `<API_KEY>` der Wert des API-Schlüssels, der nach Auswahl von **API-Schlüssel anzeigen** angezeigt wird.

e. Wählen Sie **Absenden** aus.

MID-Webserver und Agent-mTLS-Authentifizierung

Die gegenseitige Authentifizierung mit dem Transport Layer Security-Protokoll (mTLS) ist ein sicheres, zertifikatbasiertes Authentifizierungsschema. Bei mTLS authentifizieren sich der Server (die Erweiterung MID-Webserver) und der Client (der Agent) gegenseitig.

Die TLS-Authentifizierung tritt auf, wenn ein Client (z. B. ein Webbrowser) den Server, auf den er zugreift, authentifiziert, indem er das vom Server vorgelegte Zertifikat validiert. Vom Client wird überprüft, ob das Zertifikat (oder die Zertifikatkette) von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) signiert ist. Der Client muss Zugriff auf ein Paket von CA-Zertifikaten haben, mit dem das Serverzertifikat validiert wird.

Wenn mTLS konfiguriert ist, wird vom Client ein Zertifikat oder eine Zertifikatkette dem Server vorgelegt und vom Server wird der Client auf die gleiche Weise authentifiziert wie der Server vom Client (gegenseitige Authentifizierung).

Bei einigen TLS-Implementierungen wird nicht nur die Zertifikatsignatur überprüft, sondern auch der Sperrstatus des Zertifikats. In diesen Fällen wird das Online Certificate Status Protocol (OCSP) verwendet. In diesem Protokoll sendet die verifizierende Partei eine Anforderung an den OCSP Responder, der von der CA eingerichtet wurde, die das vorgelegte Zertifikat ausgestellt hat. (Die Adresse des Beantworters ist normalerweise in den von der Zertifizierungsstelle ausgestellten Zertifikaten eingebettet). Die Antwort gibt an, ob das vorgelegte Zertifikat widerrufen wurde.

Bevor Sie mTLS aktivieren, müssen Sie zuerst Schlüssel und Zertifikate erstellen, die PEM-Datei auf dem MID-Serverinstallieren und den -Agent mit dem MID-Serververbinden.

Zugehörige Informationen

MID-Webservererweiterung konfigurieren

mTLS-Authentifizierung für einen MID-Webserver konfigurieren

Erstellen Sie Schlüssel und Zertifikate

Erstellen Sie Schlüssel und Zertifikate in Ihrem Stammverzeichnis, um das TLS-Setup (Transport Layer Security) zu aktivieren. Das TLS-Setup ist erforderlich, bevor Sie mTLS auf MID-Webserver und dem Agent konfigurieren können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass im einheitlichen MID-Schlüsselspeicher keine Schlüssel installiert sind, indem Sie den folgenden Befehl ausführen:

  ```
  bin/scripts/manage-certificates.(sh/bat) -l
  ```

  Wenn keine Schlüssel installiert sind, lautet die Ausgabe: `defaultsecuritypairhandle`

- MID-Serverfür ungültig erklären.

  Wenn in der Ausgabe zusätzliche Schlüssel vorhanden sind, installieren Sie diese Schlüssel neu, nachdem Sie MID-Serverfür ungültig erklärt haben.

- Stellen Sie sicher, dass MID-Server mit der -Instanz verbunden ist.
- Wählen Sie ein Verzeichnis, in dem Sie Zertifikate erstellen möchten, das als *root* -Verzeichnis bezeichnet wird.

Hinweis: Die im folgenden Verfahren angegebenen Befehle sind nur für einen Centos7-Host relevant. Wenn Sie mit einem anderen Betriebssystem arbeiten, verwenden Sie die für Ihren Host relevanten Befehle.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Erstellen Sie im Stammverzeichnis Unterverzeichnisse für Ihre Zertifikate.

   ```
   mkdir -p labca labmid labacc;
   ```

2. In Ihrem Stammverzeichnis:

   a. Generieren Sie ein anwenderdefiniertes Zertifizierungsstellen-Schlüsselpaar.

   ```
   openssl ecparam -list_curves;
   openssl ecparam -out labca/ec-labcakey.pem -name prime256v1 -genkey;
   ls labca/;
   ```

   Die generierte Ausgabe ist die Datei `ec-labcooky.pem`.

   b. Führen Sie die folgenden Befehle aus:

   ```
   openssl ecparam -in labca/ec-labcakey.pem -text -noout;
   openssl req -x509 -new -nodes -key labca/ec-labcakey.pem
    -sha512 -days 365 -out labca/labcacert.pem -subj
    "/C=<country>/ST=<state>/L=<location>/O=<organization>
    Lab/OU=<organization unit>/CN=<cn abbreviation>";
   openssl verify labca/labcacert.pem;
   ```

   Die generierte Ausgabe ist:

   - `Labca/labcacert.pem: C =<country> , ST =<state> , L =<location> , O =<organization> , OU =<organization unit> , CN =<cn abbreviation>`
   - `Fehler 18 bei Suchtiefe 0: selbstsigniertes Zertifikat`
   - `OK`

   Hinweis: Die `Fehlermeldung` kann ignoriert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Bereiten Sie den Schlüssel MID-Webserver und das Zertifikat vor.

   a. Führen Sie die folgenden Befehle im Stammverzeichnis aus:

   ```
   sudo cp -a labca/labcacert.pem /etc/pki/ca-trust/source/anchors/;
   sudo update-ca-trust extract;
   openssl verify labca/labcacert.pem
   ```

   Die generierte Ausgabe lautet: `Labca/Labcacert.pem: OK`

   b. Führen Sie den Befehl „`hostname --all-fqdns`" aus, um alle gültigen Hostnamen für die spezifische VM zu erhalten.

   c. Führen Sie die folgenden Befehle aus:

   ```
   openssl req -new -newkey rsa:4096 -keyout
    labmid/rsa-labmidkey.pem -sha512 -nodes -out labmid/mid.csr -subj
    "/C=<country>/ST=<state>/L=<location>/O=<organization>/OU=<organizat
   ion unit>/CN=<hostname>";
   openssl x509 -req -days 365 -in labmid/mid.csr -CA labca/labcacert.pem
    -CAkey labca/ec-labcakey.pem -CAcreateserial -extensions
    SAN -extfile <(cat /etc/pki/tls/openssl.cnf <(printf
    "\n[SAN]\nsubjectAltName=DNS:<hostname>")) -out labmid/mid.crt;
   ```

   Geben Sie als FQDN Folgendes ein<hostname> Wert im vorherigen Befehl. Wenn der Befehl mehr als einen fqdn-Wert zurückgibt, verwenden Sie den Wert im folgenden Format: `hostname.domain.domain.com`.

   Die generierte Ausgabe lautet: `Signature OK subject=/C=`<country> /ST=<state> / L=<location> /O=<organization> /OU=<organization unit> /CN=<mid server host fqdn> : Privater CA-Schlüssel wird abgerufen

4. Kombinieren Sie in Ihrem Stammverzeichnis die Schlüssel- und Zertifikatdateien in einer Datei mit dem Namen `mid.pem`.

   ```
   cat labmid/rsa-labmidkey.pem labmid/mid.crt > labmid/mid.pem;
   ```

Nächste Maßnahme

Installieren Sie die PEM-Datei im einheitlichen MID-Schlüsselspeicher, und richten Sie die ein MID-Webserver.

Installieren Sie die PEM-Datei im einheitlichen MID-Schlüsselspeicher, und richten Sie die ein MID-Webserver

Installieren Sie die PEM-Datei im einheitlichen MID-Schlüsselspeicher, und richten Sie MID-Webserver ein, um die Konfiguration von mTLS auf Ihrem MID-Webserver und Agent zu ermöglichen.

Vorbereitungen

Kopieren Sie die Datei „`labmid/mid.pem`" (erstellt im Verfahren Erstellen Sie Schlüssel und Zertifikate) in Ihr Hostverzeichnis MID-Webserver.

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Greifen Sie auf das Unterverzeichnis `des Agent` im Hostverzeichnis von MID-Serverzu.
2. Führen Sie die folgenden Befehle aus:

```
bin/scripts/manage-certificates.sh -a midwss /<path>/mid.pem;
bin/scripts/manage-certificates.sh -l;
```

   Der relevante Teil der Ausgabe lautet: `„defaultsecuritypairhandle,midwss".`

3. Validieren Sie MID-Server in der Instanz.
4. Wählen Sie MID-Server in der Instanz aus, und wählen Sie **ACC-Listener einrichten**aus. Ein neues MID-Webserver wird erstellt.
5. Navigieren Sie zu dem neu erstellten MID-Webserver -Datensatz (*ecc_agent_ext_context_webserver*) in der Instanz.
6. Wählen Sie in der Instanz MID-Webserver aus, und legen Sie den Wert des **Schlüsselspeicher-Zertifikatalias** auf **midwss**fest.
7. Wählen Sie **Speichern**.
8. Starten Sie MID-Webserverneu.

Nächste Maßnahme

Verbinden Sie den -Agent per TLS mit MID-Webserver.

Verbinden Sie den -Agent per TLS mit MID-Webserver

Verbinden Sie den -Agent mit dem MID-Webserver, um die Konfiguration von mTLS auf Ihrem MID-Webserver und dem Agent zu aktivieren.

Vorbereitungen

Stellen Sie sicher, dass Sie die PEM-Datei installiert und MID-Webservereingerichtet haben. Details finden Sie unter Installieren Sie die PEM-Datei im einheitlichen MID-Schlüsselspeicher, und richten Sie die ein MID-Webserver.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Fügen Sie die Datei `„labcacert.pem"` dem Truststore Ihres Agent-Hosts hinzu.

```
sudo cp
 -a /<path>/<to>/labcacert.pem /etc/pki/ca-trust/source/anchors/;
sudo update-ca-trust extract
openssl verify /<path>/<to>/labcacert.pem
```

   Die generierte Ausgabe ist /<path> /labcacert.pem: OK

2. Konfigurieren Sie die Datei `acc.yml` für die Verwendung von TLS.

   a. Legen Sie die Eigenschaft *insecure-skip-tls-verify* auf **den Wert false**fest.

   b. Legen Sie die Eigenschaft *backend-url* so fest, dass der FQDN von MID-Serververwendet wird.

```
Backend-URL = „wss://"<mid server fqdn> :<mid web server port> /
ws/events"
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Starten Sie den Agent neu.

```
systemctl restart acc;
```

4. Überprüfen Sie in den Protokollen, ob der -Agent mit MID-Serververbunden ist.

Nächste Maßnahme

mTLS-Authentifizierung für einen MID-Webserver konfigurieren.

mTLS-Authentifizierung für einen MID-Webserver konfigurieren

Verbessern Sie die Sicherheit in der MID-Webservererweiterung, indem Sie die mTLS-Authentifizierung aktivieren.

Vorbereitungen

Vergewissern Sie sich, dass Transport Layer Security (TLS) auf dem Agent aktiviert ist. Details finden Sie unter Verbinden Sie den -Agent über mTLS mit MID-Server ..

Stellen Sie sicher, dass der Parameter *insecure-skip-tls-verify* in der `acc.yml`-Konfigurationsdatei auf **false**festgelegt ist. Einzelheiten zur Datei `acc.yml` finden Sie unter Konfigurationsdateioptionen.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Erweiterung MID-Webserver durchsucht die folgenden Speicherorte (in der angegebenen Reihenfolge), um auf den Truststore-Speicherort und das Passwort zuzugreifen:

- Truststore-Speicherort: Die JVM-Systemeigenschaft *mid.webserver.truststore.path*.

  Wenn diese Eigenschaft leer ist, wird von der Erweiterung der Speicherort aus der JVM-Systemeigenschaft *javax.net.ssl.trustStore* abgerufen.

  Wenn kein Speicherort angegeben ist, wird standardmäßig der absolute Pfad der `cacerts`-Datei der JRE verwendet, auf der der MID-Server ausgeführt wird.

- Truststore-Passwort: Das Feld **Truststore-Passwort** im Erweiterungsformular in der Instanz.

  Wenn dieses Feld leer ist, wird vom System das Passwort aus der JVM-Systemeigenschaft *javax.net.ssl.trustStorePassword* abgerufen.

  Wenn kein Speicherort angegeben ist, lautet das Passwort standardmäßig *changeit*.

Prozedur

1. Navigieren Sie zum Stammordner Ihres MID-Server.
2. Führen Sie den folgenden Befehl aus, um Ihr Zertifikat dem MID-Truststore hinzuzufügen:

```
./jre/bin/keytool -importcert
 -file /etc/pki/ca-trust/source/anchors/labcacert.pem
 -destkeystore ./jre/lib/security/cacerts -alias mtlsca
```

3. Geben Sie **changeit** ein, wenn Sie zur Eingabe eines Passworts aufgefordert werden.
4. Wählen Sie im Bestätigungsmeldungsfenster **„Ja“,** um zu bestätigen, dass Sie dem Zertifikat vertrauen.
5. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob Ihr Zertifikat erfolgreich dem MID-Trust Store hinzugefügt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
./jre/bin/keytool -list -keystore ./jre/lib/security/cacerts -alias
 mtlsca
```

6. Geben Sie **changeit** ein, wenn Sie zur Eingabe eines Passworts aufgefordert werden.
7. Konfigurieren Sie in der Konfigurationsdatei für die Wrapper-Überschreibung MID-Server (`Wrapper-override.conf`, im Verzeichnis „`home/conf`" von MID-Server) das Widerrufen von Client-Zertifikaten in der Eigenschaft *`mid.webserver.cert.revocation.check.enabled`*.
   - Wenn Sie ein anwenderdefiniertes internes Zertifikat haben, setzen Sie den Wert auf **„false"**, indem Sie der Datei `conf/wrapper-override.conf` auf dem MID Server die folgende Zeile hinzufügen:

     ```
     wrapper.java.additional.4=-Dmid.webserver.cert.revocation.check.enable
     d=false
     ```

   - Wenn Sie diese Eigenschaft (**true**) aktivieren, konfigurieren Sie die Eigenschaft *`mid.webserver.ocsp.responder.url`* mit der OCSP-Responder-URL. Dieser Wert überschreibt alle im Zertifikat eingebetteten URLs.
8. Wenn Sie Eigenschaften in der Konfigurationsdatei für die Wrapper-Überschreibung geändert haben, starten Sie den MID-Server neu.
9. Greifen Sie in der Instanz ServiceNow® auf den Datensatz MID-Server zu, und ändern Sie den Wert des Felds **Authentifizierungstyp** in **mTLS**.
10. Starten Sie MID-Webserverneu.
11. Vergewissern Sie sich, dass MID-Webserver und der Websocket-Endpunkt aktiv sind und ausgeführt werden.

Nächste Maßnahme

Verbinden Sie den -Agent über mTLS mit MID-Server ..

Verbinden Sie den -Agent über mTLS mit MID-Server .

Bevor Sie die mTLS-Authentifizierung für den -Agent konfigurieren, müssen Sie eine Reihe von Befehlen ausführen, die die Konfiguration der Transport Layer Security-Authentifizierung (TLS) aktivieren.

Vorbereitungen

Stellen Sie sicher, dass Sie die folgenden Aufgaben ausgeführt haben:

1. Erstellen Sie Schlüssel und Zertifikate
2. Installieren Sie die PEM-Datei im einheitlichen MID-Schlüsselspeicher, und richten Sie die ein MID-Webserver
3. Verbinden Sie den -Agent per TLS mit MID-Webserver
4. mTLS-Authentifizierung für einen MID-Webserver konfigurieren
5. Verbinden Sie den -Agent über mTLS mit MID-Server .

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Generieren Sie einen Schlüssel für Ihren Service Desk-Mitarbeiter.

   ```
   openssl ecparam -out labacc/acc.key -name prime256v1 -genkey
   ```

2. Generieren Sie eine Zertifikatanforderung für Ihren Agent gemäß dem folgenden Format:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
openssl req -new -key labacc/acc.key -out labacc/acc.csr -subj
 "/C=<country>/ST=<state>/L=<location>/O=<organization>/OU=<organizat
ion unit>/CN=<cn abbreviation>/emailAddress=<email address>"
```

Zum Beispiel:

```
openssl req -new -key labacc/acc.key -out labacc/acc.csr
 -subj "/C=US/ST=NC/L=Raleigh/O=ServiceNow/OU=ITOM
 Lab/CN=acclinux/emailAddress=john.smith@servicenow.com"
```

3. Generieren Sie ein signiertes Zertifikat für Ihren Agent.

```
openssl x509 -req -days 365 -in labacc/acc.csr -CA labca/labcacert.pem
 -CAkey labca/ec-labcakey.pem -CAcreateserial -extensions client -out
 labacc/acc.crt
```

4. Kopieren Sie im Ordner „`labacc`“ Ihre Schlüssel- und Zertifikatdateien in den virtuellen Computer des Agent-Hosts.

```
cp ./acc.key <agent host config folder>
cp ./acc.crt <agent host config folder>
```

Die Pfade zum Konfigurationsordner hängen von Ihrem Betriebssystem ab.

- Linux: `/etc/servicenow/agent-client-collector/`
- Windows: `C:\ProgramData\servicenow\agent-client-collector\config\`
- macOS: `/Library/Application\ Support/servicenow/agent-client-collector/`

5. Navigieren Sie zu dem Speicherort, von dem Sie die Dateien `.key` und `.crt` aus kopiert haben.
6. Führen Sie die folgenden Befehle aus, um die Leseberechtigungen der Dateien zu aktualisieren und dem Agent das Lesen von Dateien zu ermöglichen.
   - Linux:
     a. `ausgewählten servicenow:servicenow acc.key`
     b. `chmod 0400 acc.key`
   - Windows:
     a. Wählen und halten Sie die Datei `.key` (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie in den Dateieigenschaften die Registerkarte **Sicherheit** aus.
     b. Fügen Sie den Anwender *`servicenow`* der Liste der Anwender mit Lesezugriff auf die Datei hinzu.
   - macOS:
     a. `chown _servicenow:_servicenow acc.key`
     b. `chmod 0400 acc.key`

   Hinweis: Der Agent muss mit dem ServiceNow-Standardanwender ausgeführt werden.

7. Fügen Sie in der Konfigurationsdatei acc.yml die folgenden Parameter hinzu, um den Pfad zu Ihren Schlüssel- und Zertifikatdateien anzugeben.

```
key-file: "<path to acc.key file>/acc.key"
cert-file: "<path to acc.cert file>/acc.crt"
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Starten Sie den Agent neu.
   - Linux: `systemctl-Neustart gemäß`
   - Windows:
     a. Öffnen Sie die Anwendung Services.
     b. Wählen Sie den Eintrag Agent Client Collector aus, und halten Sie ihn, (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Neu starten**aus.
   - macOS:
     a. `launchctl unload -w /Library/LaunchDaemons/com.sn.acc.plist`
     b. `launchctl load -w /Library/LaunchDaemons/com.sn.acc.plist`
9. Überprüfen Sie die Protokolle, um sicherzustellen, dass der Agent mithilfe von TLS eine Verbindung zur Instanz herstellen konnte.

   Agent Client Collector Protokolle sind zugänglich von:

   - Linux: `/var/log/servicenow/agent-client-collector/acc.log`
   - Windows: Der durch die `Protokolldatei-` Konfigurationskennzeichnung angegebene Speicherort. Der Standardspeicherort lautet: `C:/ProgramData/ServiceNow/agent-client-collector/log/acc.log`.

     Wenn das Verzeichnis `C:/ProgramData` ausgeblendet ist (z. B. bei älteren Windows-Versionen), ändern Sie den Explorer-Filter, um ausgeblendete Elemente anzuzeigen.
   - macOS: Der Standardspeicherort lautet: `/Library/Application\ Support/servicenow/agent-client-collector/log/acc.log`

Zugehörige Informationen

MID-Webserver und Agent-mTLS-Authentifizierung

Ereignismanagement-Konfigurationspräferenzen

Bevorzugte Einstellungen für Eigenschaften und allgemeine Konfiguration.

Verwenden Sie das Known Error-Portal und die Community zur Suche nach weiteren Informationen.

Allgemeine Präferenzen

Selbstintegrität

Standardmäßig ist die Selbstintegritätsüberwachung nicht aktiviert. Um dies zu aktivieren, navigieren Sie zu **Ereignismanagement** > **Einstellungen** > **Eigenschaften** und wählen Sie **Ja** für die Eigenschaft *Enable Event Management self-health monitoring* (evt_mgmt.self_health_active). Verwenden Sie dieses Feature zum Überwachen und Nachverfolgen vieler Ereignismanagement-Funktionen

Hinweis: Im Selbstintegritätsservice verwendete CIs werden in der CMDB erstellt.

Verwenden Sie die folgenden Einstellungen, um einer Verschlechterung der Leistung vorzubeugen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Thema	Details
Business Rules	• Schreiben Sie keine Business Rules für Event-Tabellen [em_event], da sie nicht in der aktuellen Standard-REST-URL ausgeführt werden, die für die Event-Injektion verwendet wird. • Business Rules, die für Warnungstabellen [em_alert] geschrieben werden, müssen sehr effizient sein, da sie sonst zu einer Verschlechterung der Leistung führen können. Überlegen Sie, anstatt eine Geschäftsregel zu schreiben, ob besser ein Job geschrieben werden sollte. Eine ineffiziente Geschäftsregel kann dazu führen, dass die Incident-Erstellung fehlschlägt und die Berechnung der Warnungsauswirkung fehlschlägt. • Schreiben Sie keine asynchronen Business Rules für Warnungstabellen. • Business Rules dürfen das Feld **Kategorie** in Event-Tabellen [em_event] nicht ändern.
Hochskalierung	Überprüfen Sie die durchschnittliche Event-Verarbeitungszeit, bevor Sie den Event-Durchsatz beim ersten Start mit Ereignismanagement hochskalieren. Führen Sie diese Überprüfung nach einem ersten Flow von Events durch, wenn alle Regeln vorhanden sind. Wenn die Verarbeitungszeit pro Event einige Millisekunden dauert, ermitteln Sie die Ursache für die Verlangsamung der Verarbeitung, bevor Sie mit der Skalierung fortfahren. Die Leistungsdauer kann in der Tabelle Leistungsstatistiken [sa_performance_statistics] überprüft werden.
Für große Umgebungen konfigurieren	• Legen Sie die Eigenschaft **Event-Verarbeitung für mehrere Knoten aktivieren** (*evt_mgmt.event_processor_enable_multi_node*) auf **Ja** fest. Aktivieren Sie Mehrknotenpunkte in Produktionsumgebungen, und legen Sie Werte basierend auf der Größe der Bereitstellung und der erwarteten Event-Rate fest. • Legen Sie die **Anzahl der Scheduled Jobs zur Event-Verarbeitung** (*evt_mgmt.event_processor_job_count*) auf `4` fest. • Wenn Sie Events aus einer benutzerdefinierten Quelle senden, stellen Sie sicher, dass Events über **Nachrichtenschlüssel** oder die Daten **Quelle**, **Knoten**, **Typ** und **Ressource** verfügen.
Latenzprobleme beim Empfang von Events	Überprüfen Sie die folgenden Einstellungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Thema	Details
	• Stellen Sie sicher, dass das **Bucketfeld** in der Event-Tabelle [em_event] auf einen Wert festgelegt ist, der größer als Null (*0*) ist. • Navigieren zu **Systemzeitplaner** > **Geplante Aufgaben** und suchen Sie nach *– process events**. Überprüfen Sie, ob alle *– process events**-Jobs gemäß der Eigenschaftskonfiguration der **Anzahl der geplanten Events** (*event_processor_job_count*) zur Verarbeitung von Events vorhanden sind. Stellen Sie sicher, dass der **Status** *Running* oder *Ready* ist. Wenn der Status *Queued* oder *Error* ist, setzen Sie den Jobstatus auf *Ready*.
Events archivieren	• Vermeiden Sie, die standardmäßige Aufbewahrungszeit für Events zu ändern. • Um Events länger zu protokollieren, erstellen Sie eine Archivtabelle und einen Job, der neue Events kopiert. Führen Sie dazu einen Auftrag durch, um Events [em_event] regelmäßig in einer benutzerdefinierten Tabelle zu sichern. • Erweitern Sie die Tabellenrotation nicht um weitere Tage.

Event-Integration

SNMP-Traps

- Verwenden Sie zum Senden von SNMP-Traps ein Überwachungstool, anstatt sie direkt von Geräten zu senden.
- Um zu vermeiden, dass Event-Regeln neu geschrieben werden müssen, laden Sie MIBs hoch, bevor Sie die Event-Regeln definieren.

Webservice-API

- Die Verwendung einer Webservice-API für die Integration kann die Anzahl der erforderlichen Event-Regeln reduzieren. Diese Aktion verhindert, dass Events umgewandelt werden müssen (vorbereitete Daten werden in einem Event an die Instanz gesendet).
- Verwenden Sie dedizierte Anmeldeinformationen für die Integration. Geben Sie optional Anmeldeinformationen an, die für jede Event-Quelle spezifisch sind.

CloudWatch

Verwenden Sie dedizierte Anmeldeinformationen für die Integration von CloudWatch mit ServiceNow.

E-Mail

Verwenden Sie E-Mail nur, wenn die Quelle ein geringes Volumen hat und andere Optionen nicht verfügbar sind, z. B. Ausführen eines Skripts oder Weiterleiten eines SNMP-Traps.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Regeln

Regeln für Konfigurationseinstellungen bei der Erstellung von Event-Regeln:

- Schreiben Sie Event-Regeln, um sie auf möglichst viele Events anzuwenden. Spezifischere Regeln können dann je nach Bedarf erstellt werden und sollten einen Wert niedrigerer Ordnung verwenden.
- Wenn eine allgemeinere Regel zum gleichen Ergebnis führen kann, vermeiden Sie das Schreiben von Event-Regeln, die nur für eine bestimmte Teilmenge von Events gelten.
- Wenn Event-Regeln auf Events angewendet werden, werden keine Änderungen am ursprünglichen Event vorgenommen. Die gesamte Verarbeitung erfolgt im Arbeitsspeicher. Verwenden Sie daher das Feld **Verarbeitungshinweise** und/oder verwenden Sie den Link **Prozess der Event-UI-Aktion überprüfen**, um Fehler zu beheben.
- Wenn Sie eine Regel/Umwandlung ändern, die über Zuordnungsregeln verfügt, sollten Sie tatsächliche und/oder simulierte Events überprüfen und erneut testen.
- Stellen Sie sicher, dass der Wert im Feld **Von** genau mit einer Zeichenfolge im JSON-Text im Feld *additional_info* eines Events übereinstimmt. Diese Zuordnung erfolgt, wenn eine Regel basierend auf Informationen in einer MIB-Datei konfiguriert wurde. Wenn die MIB-Datei nicht hochgeladen wird, zeigt die JSON für die SNMP-Trap varbinds (Variablenbindung) mit gepunkteten Namen anstelle des übersetzten Namens in der MIB an. Die Zuordnungsregel für das Event-Feld kann dann nicht angewendet werden.
- Erstellen Sie eine konsistente Namenskonvention. Eine gängige Konvention ist: *<customer acronym>.<Event Source>.<Description>*. Beispiel: *ACME.OEM.Normalize*
- Wenn für zwei Event-Regeln ähnliche Bedingungen festgelegt sind, verwenden Sie das Feld **Reihenfolge**, um zu steuern, welche Event-Regel ausgeführt wird.
- Verwenden Sie Event-Regeln, um eine Warnung einem CI zuzuordnen.

Zusätzliche Einstellungen zum Erstellen von Event-Regeln:

Gewünschtes Ergebnis	Erforderliche Aktivität
Effektive Deduplizierung und Aktivierung einer effizienten parallelen Event-Verarbeitung	Füllen Sie die Felder **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** aus.
CI-Bindung	• An Host binden – durch Ausfüllen des **Knotenfelds** und optional von **CI-Bezeichnern**. • Bindung an Anwendung und/oder Gerät – durch Ausfüllen der Felder **CI-Bezeichner** und **Zusätzliche Informationen**.
Warnungskorrelation mithilfe von Warnungszusammenfassur	Füllen Sie die Felder **Ressource** und **Metrikname** aus. **Hinweis:** Wenn das CI auch gebunden ist, wird die Warnungskorrelation verbessert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Benutzerdefinierte Event-Felder

Fügen Sie zusätzliche Felder nur in das Feld **Zusätzliche Informationen** des Events ein.

Fügen Sie einem Event keine zusätzlichen Felder hinzu, indem Sie der Event-Tabelle [em_event] ein benutzerdefiniertes Feld hinzufügen.

Fügen Sie der Event-Tabelle [em_event] keine Spalten hinzu.

Informationen zum Einbinden zusätzlicher Felder in Events finden Sie unter Benutzerdefinierte Warnungsfelder.

Deduplizierung

Konfigurationseinstellungen für Deduplizierung.

- Das Feld **message_key** wird für die Deduplizierung verwendet. Wenn beim Quell-Event keine zuverlässigen Nachrichtenschlüsselwerte bereitgestellt werden, ist ein gut definierter Plan für die Erstellung dieser Bezeichner wichtig.
- Wenn der Nachrichtenschlüssel nicht definiert ist, lautet der Standard-Nachrichtenschlüssel *<Source + Node + Type + Resource + Metric Name>*.
- Die Leitlinie besteht darin, dass die Event-Quelle die *<Source + Node + Type + Resource + Metric Name>*-Felder vorab ausfüllt und den Nachrichtenschlüssel ausfüllt. Diese Aktion ermöglicht eine bessere Verteilung der Event-Verarbeitung zwischen Instanzarbeitern und Knoten.
- Wenn das Quell-Event keine Werte für diese Felder enthält, müssen Sie sie mithilfe von Umwandlungsregeln ausfüllen. Diese Aktion wirkt sich nicht auf die Event-Verarbeitung aus, wird jedoch zur Deduplizierung verwendet. Füllen Sie so viele dieser Felder wie möglich aus, bevor sie an die Instanz gesendet werden. Diese Aktion bietet eine bessere Verteilung von Events auf die Prozessorarbeiter und somit einen besseren Durchsatz und eine bessere Skalierung.

CI-Bindung

- Versuchen Sie nach Möglichkeit immer, eine Warnung an ein CI zu binden.

  Hinweis: Obwohl Event-Regeln für Events definiert sind, sind CIs an Warnungen gebunden, die aus diesen Events resultieren, und nicht an das Event selbst.

- Um einen Host, Computer oder ein beliebiges Gerät mit einer IP zu binden, füllen Sie das **Event-Knotenfeld** mit einem eindeutigen Hostnamen, FQDN, einer IP-Adresse oder einer MAC-Adresse aus. Wenn zur Identifizierung eines Hosts andere Bezeichner erforderlich sind, füllen Sie das Feld „ci_identifiers“ mit einem JSON-Format aus. Das JSON-Format muss den **CMDB**-Feldnamen und -Wert enthalten, um die Übereinstimmung durchzuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Das **Event-Knotenfeld** muss aus einer Event-Regel oder mit einem eindeutigen Hostnamen aus der Quelle ausgefüllt werden, bevor das Event eingefügt wird.

- Die primäre Bindungsstrategie besteht in der Verwendung des Felds **Knoten**. Wenn das **Knotenfeld** im Event nicht bereits ausgefüllt ist, kann es mithilfe von Event-Regeln ausgefüllt werden.

Warnungseinstellungen

Warnungslebenszyklus

Allgemeine Warnungsfunktionalität:

- Eine Warnung wird immer dann geöffnet, wenn ein Event nicht ignoriert wird oder dessen Schwellenwert von einer Event-Regel überschritten wird und die Deduplizierung das Event nicht als zu einer vorhandenen Warnung gehörig identifiziert.
- Eine Warnung wird geschlossen, wenn ein Abschluss-Event auf demselben Nachrichtenschlüssel gesendet wird, oder wenn die Warnung manuell geschlossen wird.
- Eine Warnung wird erneut geöffnet, wenn eine Eröffnungswarnung mit demselben Nachrichtenschlüssel innerhalb des in den Eigenschaften definierten Zeitrahmens gesendet wird (Standard ist eine Stunde).
- Wenn eine Warnung in schneller Abfolge (gemäß der Definition in den Eigenschaften) geöffnet und geschlossen wird, wechselt sie in den Status „Fluktuierend“. Wenn diese Öffnungs- und Schließungsrate aufhört, verliert die Warnung ihren Status „Fluktuierend“.
- Wenn ein Incident aus einer Warnung geöffnet wird, bleibt diese Warnung offen, solange der Incident offen bleibt. Standardmäßig wird beim Schließen des Incidents oder der Warnung auch der jeweils andere geschlossen. Dieses Verhalten kann mithilfe von Eigenschaften konfiguriert werden.
- Schließen Sie keine Warnung, wenn Sie einen entsprechenden Incident erstellen.
- Löschen Sie keine offenen Warnungen. Schließen Sie zuerst eine Warnung, und löschen Sie sie dann.
- Verwenden Sie `Bestätigen`, um anzugeben , dass die Warnung bekannt ist und vorübergehend ignoriert werden kann.
- Verwenden Sie `Bestätigen` nicht, um eine Warnung mit einem Handlungsbedarf zu versehen.
- Erstellen Sie keine Warnungen in einem der folgenden Status:
  - `Geschlossen`
  - `OK`
  - `Offen`
- Die Eigenschaft `evt_mgmt.alert_auto_close_interval` schließt Warnungen nach dem angegebenen Zeitraum automatisch. Geben Sie nicht 0 an, da dieser Wert die Funktion deaktiviert und zu einer Verschlechterung der Leistung führen kann.
- Erstellen Sie keine Warnungen im Status `OK`. In einigen Überwachungssystemen bedeutet `OK`, dass ein Problem gelöst wurde, während in anderen Überwachungssystemen `OK` verwendet wird, um Events zu kennzeichnen, die keine operative Bedeutung haben. Im ersten Fall verwenden Sie `Löschen` anstatt `OK` mithilfe einer Zuordnungsregel. Im letzteren Fall müssen Sie eine Ignorieren-Regel verwenden, es sei denn, die Events haben einen bestimmten Wert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsaktionsregeln

- Bei einem Scheduled Job werden alle 11 Sekunden Warnungsaktionsregeln auf neue Warnungen angewendet. Wenn eine Warnungsregel nicht sofort gestartet wird, warten Sie 10–15 Sekunden, bevor Sie mit der Problembehandlung beginnen.
- Wenn für zwei Warnungsregeln ähnliche Bedingungen festgelegt sind, verwenden Sie das Feld **Reihenfolge**, um zu steuern, welche Warnungsregel ausgeführt wird.
- Verwenden Sie Warnungsaktionsregeln mit Aufgabenvorlagen, um statische Werte in einem Incident auszufüllen. Verwenden Sie das Ausfüllerskript, um dynamische Werte im Incident zuzuweisen. Das Ausfüllerskript kann den Wert `false` zurückgeben, um die Incident-Erstellung abzubrechen.
- Erstellen Sie einen Benutzer namens Ereignismanagement (oder einen ähnlichen Namen). Anschließend kann das Feld **Erstellt von** in einer Aufgabenvorlage (z. B. **Incident**) festgelegt werden, um anzugeben, dass der Benutzer die Quelle der Aufgabe war.
- Verwenden Sie die Skripteinbindung **EvtMgmtCustomIncidentPopulator**, um dynamische Wertzuweisungen durchzuführen oder dynamische OOB-Wertzuweisungen zu überschreiben.

Fehlerkorrektur

- Legen Sie für die Fehlerkorrekturaufgaben-Tabelle [em_remediation_task] immer Eigenschaften für den Orchestrierungs-Workflow fest.
- Verwenden Sie die ECC-Warteschlange und **Workflow** > **Live-Workflow** > **Alle Kontexte** um detailliertere Informationen zu Korrekturaktivitäten zu erhalten.

Business-Regeln

- Business Rules, die für Warnungstabellen erstellt werden, sollten nicht länger als einige Millisekunden dauern. Anstatt eine Geschäftsregel zu verwenden, sollten Sie in Betracht ziehen, ob die gleiche Funktionalität mit einem Job erreicht werden kann.
- Verwenden Sie keine Business Rules, um eine Warnung einem CI zuzuordnen. Verwenden Sie Event-Regeln für Bindungen anstelle von Business Rules.

Planung

- Organisieren Sie die Konfiguration der Event-Quelle von Filtern, Modulen usw. in mehreren parallelen Vorgängen anstatt in seriellen.
- Validieren Sie verarbeitete Event-Formate, um sicherzustellen, dass die analysierten Daten mit den gewünschten Ergebnissen übereinstimmen.
- Testen Sie Produktions-Events in einer Umgebung außerhalb der Produktion. Integrieren Sie sie mit Elementmanagern und ServiceNow-Instanzen außerhalb der Produktion. Wenn Elementmanager außerhalb der Produktion nicht verfügbar sind, senden Sie Events von Elementmanagern sowohl an Produktionsumgebungen als auch an Nichtproduktionsumgebungen.

Services und Dashboard

- Verwenden Sie Servicegruppen, um Services in logischen Gruppen zu gruppieren, um die Anzahl der Services zu reduzieren, die im Dashboard „Serviceintegrität“ angezeigt werden.
- Importieren Sie manuell erstellte Servicezuordnungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikdaten-Sammlerprotokolle und -dateien

Metrikdaten-Sammlerprotokolle und -dateien befinden sich unter dem Pfad `$(MID_SERVER_DIR)/agent`. Verwenden Sie diese Protokolle und Dateien für die Fehlerbehebung und Überwachung.

Speicherort der Metrikdaten Sammlungsprotokolle und -dateien

Protokoll oder Datei	Pfad
Protokolldatei für PowerShell-Metriksammler	Protokolle/retrieve_metrics{connector instance ID}.log
PowerShell-Ausgabedatei	work/metrics/metrics_output_{connector instance ID}.txt
PowerShell-Ausgabedatei	work/metrics/parameters_{connector instance ID}.txt

Die Metrikdaten-Leistung kann in der MID-Server-Protokolldatei überprüft werden, wenn sich der Parameter *mid.log.level* MID-Server im Debug-Modus befindet.

Metrikdaten-Leistungszahlen sind in der Tabelle „Leistungsstatistiken“ [sa_performance_statistics] verfügbar. Um die Leistungsnummern anzuzeigen, filtern Sie die Liste der Leistungsstatistiken für **Metriksammler**.

Zugehörige Informationen

Event-Tabellen rotieren und Warnungstabellen bereinigen

Domain Separation und Ereignismanagement

Die Domänentrennung wird in Ereignismanagement unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

So funktioniert Domain Separation in Ereignismanagement

Wenn Domänen in Ereignismanagement getrennt sind, können Benutzer nur Warnungen und Events in ihrer eigenen (Mandanten-)Domäne sehen und verwalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für Ereignismanagement-Tabellen, die im Basissystem bereitgestellt werden, ist eine Domänenspalte vorhanden. In der Spalte wird der Name der Domäne angezeigt, zu der das Event oder die Warnung gehört.

Hinweis:

Wenn die Domänenspalte nicht in der Liste angezeigt wird, klicken Sie auf , und fügen Sie die gewünschte Spalte hinzu. Darüber hinaus können Sie eine Spalte hinzufügen, die den Domänenpfad anzeigt.

Informationen zu Einschränkungen der Domänentrennung in Ereignismanagement finden Sie unter Ereignismanagement-Domain Separation konfigurieren.

Zugehörige Informationen

Domänentrennung für Service Provider

Ereignismanagement-Domain Separation konfigurieren

Sie können Ereignismanagement für die **Domain Separation** konfigurieren, um logisch definierte Domänen zu erstellen, die den nicht autorisierten Zugriff auf Daten beschränken. Wenn Domänen in Ereignismanagement getrennt sind, können Benutzer nur Warnungen und Events in ihrer eigenen (Mandanten-)Domäne sehen und verwalten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin und evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Aktivieren Sie das Plugin **Domain Support – Domain Extension Installer** und konfigurieren Sie den MID Server für Ereignismanagement.

Die folgenden Funktionen von Ereignismanagement unterstützen die Domain Separation nur eingeschränkt.

Funktionen mit eingeschränkter Domain Separation

Funktion	Support
Event – Warnungs-Flow	Unterstützt. Die Trennung basiert auf dem Domänenbenutzer, der Events gesendet hat. Benutzerzugriff ist für die Anmeldeinformationen der sendenden API-Events oder in der Konfiguration der MID Server-Reporting-Events erforderlich. In einer Umgebung mit mehreren Domänen kann jeder MID Server je nach verwendetem Integrationsbenutzer nur eine Domäne bedienen. Stellen Sie in der Konfiguration der Connector-Instanz sicher, dass der MID Server die gleiche Domäne wie Ereignismanagement verwendet . Informationen zur Konfiguration von Pull-Connectors zur Unterstützung von anwenderdefinierter Domain Separation finden Sie unter Personalisieren Sie Domänen für Pull-Connector-Ereignisse, die bei der Ereigniserstellung verwendet werden sollen.
Auswirkungsberechnung	Unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionen mit eingeschränkter Domain Separation (Fortsetzung)

Funktion	Support
	Segregation basiert auf der Art und Weise, wie CIs getrennt werden.
Anwendungsservices	Teilweise unterstützt. Segregation basiert auf der Art und Weise, wie CIs getrennt werden.
Dynamische CI-Gruppen	Teilweise unterstützt. Segregation basiert auf der Art und Weise, wie CIs getrennt werden. **Hinweis:** Der Discovery-Prozess trennt CIs nicht nach Domäne.
Fehlerkorrektur	Unterstützt. Beim Bearbeiten von Warnungsverwaltungsregeln können Benutzer nur relevante Workflows anwenden. Informationen zum Aufrufen der Domain Separation durch Subflows finden Sie unter Domänentrennung über Subflows aufrufen. Weitere Informationen zur Domain Separation im Flow Designer finden Sie unter Domänentrennung und Flow Designer.
Warnungszusammenfassung	Unterstützt. In domänengetrennten Umgebungen werden Warnmeldungsgruppen nur für Warnungen in derselben Domäne erstellt.

Prozedur

1. Aktivieren Sie das Plugin „Domain Support – Domain Extension Installer“, wenn es noch inaktiv ist.
2. Konfigurieren Sie die Connector-Instanz so, dass sie sich in derselben Domäne wie der MID Server befindet.

Ereignismanagement-Integrationen

Ein Event ist eine Benachrichtigung von einem oder mehreren Überwachungstools, die anzeigt, dass etwas von Interesse aufgetreten ist, z. B. eine Protokollnachricht, eine Warnung oder ein Fehler.

Events werden verarbeitet und Warnungen werden basierend auf den folgenden Faktoren generiert:

- Konfiguration des Eventsammlers über einen MID-Server, ein Skript, einen SNMP-Trapsammler oder eine E-Mail-Nachricht.
- Eine Event-Regel, Warnungsbindung oder Event-Feldzuordnungskonfiguration für die Verarbeitung von Events aus verschiedenen Quellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein Event-Paket verarbeitet wird, das Events mit einem benutzerdefinierten (nicht unterstützten) Status enthält, werden die Events mit dem benutzerdefinierten Status nicht verarbeitet.

Integration mit externen Events

Ereignismanagement empfängt externe Events über eine Integration oder Skripts. Wenn Sie ein Skript zum Erfassen von Events verwenden, ist keine Konfiguration erforderlich. Alle anderen Integrationen müssen konfiguriert werden.

Nach der Konfiguration einer Integration kann Ereignismanagement Events erfassen, die direkt an die Now Platform-Instanz oder über den MID Server, den SNMP-Trap oder per E-Mail gesendet werden.

Die Integration mit externen Systemen kann von einer Now Platform-Instanz mithilfe eines Pull-Connector oder von einem externen System mithilfe eines Push-Mechanismus initiiert werden.

Integration über eine Now Platform-Instanz

Die Now Platform-Instanz enthält Push-Connectors, mit denen sich externe Überwachungssysteme direkt mit Ereignismanagement integrieren lassen.

Sie können die Authentifizierung in der Now Platform-Instanz konfigurieren und die externen Überwachungssysteme so aktualisieren, dass Endpunkte zum Senden der Events für die verfügbaren Push-Connectors verwendet werden. Weitere Informationen finden Sie unter Push-Connectors.

Integration über MID Server

Der MID Server ermöglicht die Kommunikation und den Transport von Daten zwischen externen Anwendungen, Datenquellen, Services und der Now Platform-Instanz.

Connector-Vorgang	Beschreibung
Pull	Sie können Connector-Instanzen zur Verwendung von Connector-Definitionen (Skriptanweisungen) konfigurieren. Dadurch kann sich der MID Server mit externen Servern verbinden, um Event-Informationen über einen Pull-Vorgang abzurufen.
Veröffentlichen	Sie können externe Systeme so konfigurieren, dass Event-Informationen an die Now Platform-Instanz über den MID Server übertragen werden. Konfigurieren Sie beispielsweise den MID WebService-Event-Sammler zum Übertragen von Event-Nachrichten an den MID Server. Weitere Informationen finden Sie unter Ereignisse werden mithilfe der Webservice-API an MID-Server übertragen.

Standard-Event-Formular

Ein Standard-Event-Formular muss von allen Events verwendet werden, unabhängig davon, wie sie bei der Now Platform-Instanz eintreffen. Weitere Informationen finden Sie unter Event-Feldformat für die Event-Erfassung.

Ereignismanagement Domänenpersonalisierung von Connectors

Erstellen Sie Ereignisse in verschiedenen Domänen für alle Ereignismanagement Connectors mit nur einer einzigen Connector-Instanz, indem Sie die Domänentrennung von Ereignismanagement Connectors personalisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wie die Domäne identifiziert wird

In einer ServiceNow -Instanz werden Ereignisse innerhalb der angemeldeten oder MID-Server -Benutzerdomänen erstellt. Sie können jedoch Ereignisse in einer anderen Domäne erstellen, indem Sie Metadatenwerte in der Ereignis-HTTP-Anforderung angeben, einschließlich URL, Header, Anforderungstext (Payload) und Connector-Parameter.

Der angemeldete -Benutzer oder der -Benutzer MID-Server muss Zugriff auf die angegebene Domäne haben. Der Connector löst die Domäne basierend auf dem angegebenen Bezeichner auf und erstellt Ereignisse in dieser Domäne.

Systemeigenschaften stellen die Standardmetadaten bereit, die die domänengetrennte Tabelle zum Identifizieren der Domäne festlegen. Weitere Informationen finden Sie unter Mit installierte Domäneneigenschaften Ereignismanagement.

Connector-Ausnahmen

Sie können Domain Separation für die folgenden Pull-Connectors nicht personalisieren:

- SCOM
- IBM Netcool (unterstützt nur IBM Netcool_v2)
- HPOM
- Hyperic

Sie können Domain Separation für die folgenden Push-Connectors nicht personalisieren:

- SAP SolMan-Transformationsskript
- bmcTrueSight-Transformationsskript
- Transformieren Sie die MID für generische Ereignisse
- Transformationsereignisse_xmlBeispiel

Zugehörige Informationen

Domain Separation und Ereignismanagement

Personalisieren Sie Domänen für Pull-Connector-Ereignisse, die bei der Ereigniserstellung verwendet werden sollen

Konfigurieren Sie Pull-Connectors, um die Domänentrennung von Ereignissen zu personalisieren, damit Sie sie zum Erstellen von Ereignissen in anderen Domänen als der aktuell angemeldeten oder der Domäne MID-Server des Benutzers verwenden können.

Vorbereitungen

Stellen Sie sicher, dass Sie über das folgende Setup verfügen:

- Sie haben red Zugriff auf die Domäneninformationstabelle für die Rolle evt_mgmt_integration (Standardtabelle: core_company). Weitere Informationen finden Sie unter Konfigurieren einer ACL-Regel .
- Sie haben die Systemeigenschaft [für `evt_mgmt.connector_enable_custom_domain_separation` aktiviert.
- Sie haben die folgenden Plugins in Ihrer ServiceNow -Instanzinstalliert:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ereignismanagement *com.glideapp.itom.snac* Plugin
- Ereignismanagement Connectors *sn_em_connector* Plugin
- Plugin „Domänen-Support – Domänenerweiterungs-Installationsprogramm *com.glide.domain.msp_extensions.installer*“ .

Sie können die Plugins aus dem ServiceNow Store herunterladen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen** > .
2. In der Liste **Connector-Instanzen** daktivieren Sie die Connector-Instanz des Connectors, für den Sie Domain Separation konfigurieren möchten, indem Sie sie auswählen und das Kontrollkästchen **Aktiv** deaktivieren.
3. Wählen Sie **Aktualisieren**.
4. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussdefinitionen**.
5. Wählen Sie in der Liste **Connector-Definitionen** Ihre Connector-Definition aus.
6. Legen Sie fest, ob alle Ereignisse in einer angegebenen Domäne erstellt oder von einer Domäne bestimmt werden sollen, die in der Nutzlast jedes Ereignisses angegeben ist.

   a. Doppelklicken Sie in der Tabelle **Connector-Parameterauf Neue Zeile einfügen**

   b. Wählen Sie den Definitionsspeicherort der Domäne für die Ereigniserstellung.
      - Damit alle Ereignisse in der angegebenen Domäne erstellt werden, geben Sie in der Spalte **Name**`den Wert payloadDomainInfoFieldValue` ein.
      - Damit Ereignisse in der in der Nutzlast des Ereignisses angegebenen Domäne erstellt werden, geben Sie in der Spalte **Name**`den Wert payloadDomainInfoFieldName` ein.

      Hinweis: Wenn *payloadDomainInfoFieldValue* und *payloadDomainInfoFieldName* angegeben werden, hat die in der Nutzlast des Ereignisses angegebene Domäne Vorrang.

   c. Wählen Sie **Aktualisieren**.

7. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
8. Wählen Sie auf der Seite **Connector-Instanzen** Ihre Connector-Instanz aus der Liste aus.
9. Geben Sie in der Liste Connector-Instanzwerte einen Wert im Feld **Wert** der Parameter an.

Parameter	Wert
payloadDomainInfoFieldValue	Der Wert, der zum Abgleichen des Domänendatensatzes verwendet wird. Beispiel: ServiceNow.
payloadDomainInfoFieldName	Der Schlüssel in der Nutzlast, der den Domänenbezeichner enthält. Wenn beispielsweise das **Nutzlastschlüsselunternehmen** den Domänenbezeichner enthält, liefert der Wert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert

	in der Spalte **„Wert“** die Unternehmensinformationen. Zum Beispiel:
	Unternehmen
	{
	„source“: „Solarwinds“,
	„Host“: „127.0.0.1“,
	„Unternehmen“: „ServiceNow“
	}
	Hinweis: Dot-Walking wird nicht unterstützt.

10. Wählen Sie **Speichern**.
11. Wählen Sie **Connector testen** aus, um die Verbindung zwischen MID-Server und dem Connector zu überprüfen.
    - Wenn der Test erfolgreich ist, wird eine Bestätigungsmeldung angezeigt.
    - Wenn der Test fehlschlägt, erhalten Sie in einer Meldung Anweisungen zur Behebung des Problems.

    Bei einem erfolgreichen Test wird eine Bildschirmmeldung angezeigt. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Bildschirmnachricht, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

    Hinweis: Verwenden Sie ein Netzwerktool wie *Ping*, um zu überprüfen, ob die Anmeldeinformationen korrekt sind, und überprüfen Sie die Netzwerkverbindung zwischen MID-Server und dem Connector-Server.

12. Nachdem der Connector verifiziert wurde, wählen Sie den Link **Zurück zur Connector-Instanz**.
13. Aktivieren Sie die Connector-Instanz, indem Sie **Aktiv** und **Aktualisieren**wählen.
14. Wahlweise: Konfigurieren Sie die Domäne für Ereignisse, indem Sie Domänenmetadaten über die Connector-Parameterbereitstellen.

    Um beispielsweise die Tabelle „Benutzer“ [sys_user] für eine einzelne Connector-Instanz im Formular **„Connector-Definitionen“** zu verwenden, erstellen Sie Parameter mit den folgenden Namen, und fügen Sie ihre Werte im Formular **„Connector-Instanz“** hinzu.
    - *connectorDomainInfoTableName* - sys_user

      Hinweis: Die Tabelle muss domänengetrennt sein.

    - *connectorDomainInfoColumnName* Anwendername
    - *connectorDomainIdColumnName* sys_domain
    - *connectorDomainPathColumnName* sys_domain_path

    Weitere Informationen finden Sie unter Metadaten der Connector-Domäne.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Der Connector Ereignismanagement ist für Domain Separation eingerichtet.

Personalisieren Sie Domänen für Push-Connector-Ereignisse zur Verwendung bei der Ereigniserstellung

Konfigurieren Sie Push-Connectors, um die Domänentrennung von Ereignissen zu personalisieren, damit Sie sie zum Erstellen von Ereignissen in anderen Domänen als der aktuell angemeldeten Person oder der Domäne MID-Server verwenden können.

Vorbereitungen
Stellen Sie sicher, dass Sie über das folgende Setup verfügen:

- Sie haben Lesezugriff auf die Domäneninformationstabelle für die Rolle „evt_mgmt_integration“ (Standardtabelle: core_company). Weitere Informationen finden Sie unter Konfigurieren einer ACL-Regel .
- Sie haben taktiviert, er *evt_mgmt.connector_enable_custom_domain_separation*. Systemeigenschaft
- Sie haben die folgenden Plugins in der Now Platform® -Instanzinstalliert:
  - Ereignismanagement (*com.glideapp.itom.snac*)
  - Ereignismanagement Connectors (*sn_em_connector*)
  - Domänen-Support – Installationsprogramm für Domänenerweiterungen (*com.glide.domain.msp_extensions.installer*)

    Sie können die Plugins aus dem ServiceNow Store herunterladen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur
1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Push-Connectors**.
2. Öffnen Sie einen Push-Connector.
3. Scrollen Sie im Bildschirm **Push-Connector** nach unten zur Liste **Push-Connector-Konfigurationen**, und wählen Sie **Neu**aus.

   Hinweis: Wenn diese Liste nicht angezeigt wird, müssen Sie einen Push-Connector-Konfigurationsparameter erstellen. Weitere Informationen finden Sie unter Erstellen Sie einen Push-Connector-Konfigurationsparameter.

4. Im Bildschirm **Push-Connector-Konfigurationen** bestimmt , ob Ereignisse in der angegebenen Domäne oder in der Domäne erstellt werden sollen, die in der Nutzlast jedes Ereignisses angegeben ist.

Ort der Domänenerstellung	Parameter und Werte
Die angegebene Domäne	◦ **Feldname**: payloadDomainInfoFieldValue ◦ **Wert**: Domänenbezeichner
Die in der Nutzlast jedes Ereignisses bereitgestellte Domäne	◦ **Feldname**: payloadDomainInfoFieldName ◦ **Wert**: „field-name-in-payload“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ort der Domänenerstellung	Parameter und Werte

	Beispiel: Wenn der Nutzlastschlüssel „company“ den Domänenbezeichner enthält, ist „company“ der Wert.
	„Unternehmen“
	{
	„source“: „Solarwinds“,
	„Host“: „127.0.0.1“,
	„Unternehmen“: „ServiceNow“
	}

Hinweis: Wenn sowohl der Parameter *payloadDomainInfoFieldValue* als auch der Parameter *payloadDomainInfoFieldName* angegeben werden, hat der Parameter *payloadDomainInfoFieldName* Vorrang.

5. Wählen Sie **Absenden**.

Ergebnisse
Ereignisse werden in der Domäne erstellt, auf die der Domänen-Identifier verweist.

Hinweis: Die Tabelle, in der Domäneninformationsdatensätze (z. B. core_company) gespeichert werden, muss domänengetrennt sein. Weitere Informationen finden Sie unter Trennen Sie eine benutzerdefinierte Tabelle von der Domäne .

Zugehörige Informationen

Integrieren Sie mit Push-Connectors

Metadaten der Connector-Domäne

Konfigurieren Sie Ereignismanagement die -Connectors

Ereignismanagement stellt viele Connectors zum Abrufen oder Veröffentlichen von Events von externen Geräten bereit. Connectors sind auch im ServiceNow-Store und von Drittanbietern verfügbar. Zudem können Sie benutzerdefinierte Connectors erstellen.

Bereitgestellte Connectors (Pull)
Diese Tabelle enthält die mit Ereignismanagement bereitgestellten Connectors.

Hinweis:

- Die Connectors für Azure-Metriken und AWS CloudWatch-Metriken werden im Basissystem nur angezeigt, wenn das Operational Intelligence-Plugin (com.snc.sa.metric) aktiviert ist.
- Alle Connectors unterstützen externe Anmeldeinformationsspeicherlösungen. Weitere Informationen zur Konfiguration des externen Anmeldeinformationsspeichers finden Sie unter Konfiguration des externen Anmeldeinformationsspeichers .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Unterstützte Version	Beschreibung
Azure Monitor		Sendet Warnungsstatusänderungen an das Azure-Portal
HPOM	08.60.005	Empfangen von Events vom HP Operations Manager (HPOM)
Hyperic	5.8.4.0	Empfangen von Events vom VMware vRealize Hyperic-Server
Logicmonitor	156	Empfangen von Events vom Logicmonitor-Server.
IBM Netcool	8.1.0	Empfangen von Events von IBM Netcool/OMNIbus-Objektservern und Auswirkungsservern.
Icinga2	2.4.1	Empfangen von Events vom Icinga2-Server
Apache Kafka Consumer Connector	• 3.0.0 • 3.2.0	Empfangen Sie Ereignisse vom Apache-Kafka-Server.
ServiceNow Cloud Observability	2.1.1 oder höher	Empfangen Sie Ereignisse von der Plattform ServiceNow Cloud Observability.
NagiosXI	5.5.2	Empfangen von Events vom Nagios XI-Server
NNMi	10.30.653	Empfangen von Events vom NNMi-Server
OBM, auch als OMi v2 bezeichnet	10.01, 10.10, 10.11, 10.12, 10.60, 10.61 und 11.01	Empfangen von Warnungen vom OBM-Server.
OMi	10.01, 10.10, 10.11, 10.12, 10.60 und 10.61	Empfängt Warnungen vom OMi-Server
Op5	7.3.15	Empfangen von Warnungen von einem OP5-Monitor
Opsview	5.4.0	Empfangen von Warnungen von einem Opsview-Monitor
PRTG	21.3.71	Empfangen von Warnungen von einer Paessler PRTG Network Monitor-Quelle
SAP Solution Manager	7.2 740 SP16	Empfangen von Warnungen von einer SAP Solution Manager Monitor-Quelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Unterstützte Version	Beschreibung
SCOM	• 2007 – Version 6.1.7221.0 • 2012 – Version 7.1.10226.0 • 2016 – Version 7.2.117190	Warnungs- und Metriksammlung vom Microsoft System Center Operations Manager (SCOM)
SolarWinds	• NPM 12.0 • SAM 6.2.4	Empfangen von Events vom SolarWinds-Monitor
vCenter	6.5	Empfangen von Events aus Ihrer VMware vSphere-Umgebung
vRealize	VMware vRealize Operations Manager Unterstützte Version: 8.10.0	Empfangen von Events vom vRealize-Betriebsprotokoll und den Ereignismanagement-Servern
Zabbix	5.0.9	Empfangen von Events vom Zabbix-Server

Bereitgestellte Connectors (Push)

Diese Tabelle enthält die mit Ereignismanagement bereitgestellten Connectors. Generische Push-Connectors werden ebenfalls bereitgestellt, einer für die Event-Erfassung über den MID-Server und der andere über die Instanz.

Bevor Sie beginnen, stellen Sie sicher, dass das Plugin „Ereignismanagement Connectors“ in der Now Platform-Instanz installiert ist. Sie können das Plugin herunterladen von ServiceNow Store Website von.

Connectors	Beschreibung	Unterstützte Authentifizierung
AWS	Verwenden Sie den Connector, um AWS-Warnungen (Amazon Web Services) als Events zu verarbeiten. Die Event-Erfassung erfolgt über die Instanz.	N/V
Azure	Verwenden Sie die OAuth-Authentifizierung, um Event-Nachrichten der Azure-Plattform zu verarbeiten. Die Event-Erfassung erfolgt über die Instanz.	• Azure Monitor mit OAuth-Authentifizierung integrieren • Azure Monitor mit Standardauthentifizierung integrieren
Bidirektionalen Azure Monitor-Connector konfigurieren	Verwenden Sie den Azure Monitor-Pull-Connector, um Informationen von ServiceNow	Standardauthentifizierung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Beschreibung	Unterstützte Authentifizierung
	Ereignismanagement an das Azure-Portal zu senden.	
Microsoft Azure MID Push Connector	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Microsoft Azure gesendet wurden. Die Erfassung erfolgt über den MID-Server.	Standardauthentifizierung
BMC TrueSight	Erfassen von JSON-formatierten Event-Nachrichten, die von BMC TrueSight Operations Management (TrueSight) gesendet wurden. Die Event-Erfassung erfolgt über den MID-Server.	Standardauthentifizierung
New Relic	Erfassen Sie JSON-formatierte Event-Nachrichten, die von New Relic gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung
Dynatrace	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Dynatrace gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	• Integrieren Sie Dynatrace mit der OAuth-Authentifizierung • Integrieren Sie Dynatrace mit der Standardauthentifizierung
Datadog	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Datadog gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	• Integrieren Sie Datadog mit der OAuth-Authentifizierung • Integrieren Sie Datadog mit der Standardauthentifizierung
Catchpoint	Konfigurieren Sie den Catchpoint-Connector für den Empfang von Catchpoint-Ereignissen. Von Ereignismanagement können die Catchpoint-Ereignisse als ServiceNow-Ereignisse verarbeitet werden.	Standardauthentifizierung
Google Cloud Platform (GCP)	Erfassen Sie Event-Nachrichten im JSON-Format, die von GCP gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Beschreibung	Unterstützte Authentifizierung
Google Cloud Platform (GCP) MID Push Connector	Erfassen Sie Event-Nachrichten im JSON-Format, die von GCP gesendet wurden. Die Event-Erfassung erfolgt über den MID-Server.	Standardauthentifizierung
Logicmonitor	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Logicmonitor gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung
Logicmonitor MID Push-Connector	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Logicmonitor gesendet wurden. Die Event-Erfassung erfolgt über den MID-Server.	Standardauthentifizierung
Oracle Cloud Push-Connector	Verwenden Sie die Standardauthentifizierung, um Oracle Cloud-Warnungen zu verarbeiten. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung
Prometheus	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Prometheus gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung
Sentry	Konfigurieren Sie den Sentry-Connector, um Sentry-Ereignisse zu empfangen. Von Ereignismanagement können die Sentry-Ereignisse als ServiceNow-Ereignisse verarbeitet werden.	Standardauthentifizierung
SNMP-Traps	SNMP-Traps als Events verarbeiten.	Standardauthentifizierung
ThousandEyes	Erfassen Sie JSON-formatierte Event-Nachrichten, die von ThousandEyes gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	• Integrieren Sie ThousandEyes mit OAuth-Authentifizierung • Integrieren Sie ThousandEyes mit der Standardauthentifizierung
E-Mail	Konfigurieren Sie eine Aktion für eingehende E-Mails, um E-Mail-Benachrichtigungen zu senden, wenn Events und Warnungen ausgelöst werden.	Standardauthentifizierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Beschreibung	Unterstützte Authentifizierung
Oracle Enterprise Manager-Trap-Erfassung	Konfigurieren Sie den SNMP-Trap-Connector für den Empfang von Oracle Enterprise Manager Cloud Control-SNMP-Traps. Ereignismanagement kann diese Traps als Events verarbeiten.	Standardauthentifizierung
Grafana	Erfassen Sie JSON-formatierte Event-Nachrichten, die von Grafana gesendet wurden. Die Event-Erfassung erfolgt über die Instanz.	Standardauthentifizierung
EIF-Listener	Konfigurieren Sie den EIF-Listener-Kontext für den Empfang von EIF-Events. Ereignismanagement kann diese EIF-Events als ServiceNow-Events verarbeiten.	Standardauthentifizierung
Honeycomb-Ereignisse integrieren	Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Ereignissen von Honeycomb, indem Sie Honeycomb als Datenquelle authentifizieren. Legen Sie auf der Honeycomb-Plattform die Now Platform mit einem Webhook als REST-Endpunkt fest.	Standardauthentifizierung
Instana-Events integrieren	Konfigurieren Sie Instana mit Ereignismanagement, indem Sie in der Instana-Konsole einen Standard-Webhook hinzufügen.	Standardauthentifizierung
Scout APM-Ereignisse integrieren	Aktivieren Sie die Sammlung von Ereignissen aus Scout APM, indem Sie Scout APM als Datenquelle authentifizieren, um es in zu integrieren Ereignismanagement	Standardauthentifizierung
Panopta als Datenquelle integrieren	Konfigurieren Sie die cloudbasierte Überwachungslösung Panopta mit Ereignismanagement.	Standardauthentifizierung
URL-Format für generisches JSON	Konfigurieren Sie die folgende generische JSON-	N/V

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors	Beschreibung	Unterstützte Authentifizierung
Diese URL kann unverändert verwendet werden und erfordert die Konfiguration einer Event-Regel.	Ziel-URL und eine Event-Regel zum Erfassen von Events: `https://<<INSTANCE>>/api/sn_em_connector/em/inbound_event?source=genericJson`.	

ServiceNow-Store – Connectors

Connectors sind im ServiceNow-Store verfügbar. Laden Sie die erforderlichen Inhalte aus dem ServiceNow-Store herunter.

Connectors von Drittanbietern

Connectors sind auch von Drittanbietern verfügbar. Weitere Informationen über verfügbare Connectors und Listeners erhalten Sie von Ihrem Vertriebsmitarbeiter.

Connectors von Drittanbietern	Link
AppDynamics-Servicemodellintegration Verwenden Sie diese Integration, um zu ermöglichen, dass Ihre Instanz AppDynamics Application Performance Monitoring-Daten in Ereignismanagement einspeist.	AppDynamics-Servicemodellintegration
NetScout – nGeniusONE Alert integration Mit dem NETSCout-Integrationsmodul kann nGeniusONE erweiterte Warnungen für ServiceNow ITOM mit einer kontextbezogenen Startfunktion für die Serviceselektierung generieren. ServiceNow ITOM-Benutzer können Abfragen in nGeniusONE aus jeder anderen Warnung mit diesem Kontext starten. nGeniusONE-Dashboards und -Berichte unterstützen die Visualisierung dieser Warnungsbedingungen an und von ServiceNow ITOM	NetScout – nGeniusONE Alert integration
Panopta-Integration Integration dieser Anwendung für die Übertragung von Events in eine Richtung von Panopta an Ereignismanagement.	Panopta-Integration
Splunk-Integration Integrieren Sie das Splunk-Add-on in ServiceNow, damit Splunk-Benutzer Incidents und Ereignisse in Ereignismanagementerstellen können. Weitere Informationen zur Konfiguration dieser Integration finden Sie unter Splunk-Add-on für ServiceNow .	Splunk-Integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connectors von Drittanbietern	Link
ScienceLogic Integration mit dieser Anwendung für unidirektionale Übertragung von Ereignissen von ScienceLogic an Event Management	ScienceLogic-Integration
SevOne Integration mit dieser Anwendung für unidirektionale Übertragung von Ereignissen von SevOne an Event Management	SevOne-Integration
Site24X7 Integration mit dieser Anwendung für unidirektionale Übertragung von Ereignissen von Site24x7 an Event Management	Site24x7-Integration

Erstellen Sie einen benutzerdefinierten Pull-Connector

Sie können einen benutzerdefinierten Pull-Connector erstellen, der ein Skript, eine Connector-Definition und eine Connector-Instanz erfordert, um Events im Namen einer Event-Quelle abzurufen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein benutzerdefiniertes Connector-Skript kann Remote-API-Aufrufe für eine neue Event-Quelle ausführen, um Events an die ServiceNow-Instanz zu senden. Sie können ein Skript erstellen und es dann als Teil einer neuen Ereignismanagement-Connector-Definition und Connector-Instanz hinzufügen. Dieses Verfahren erstellt automatisch eine JavaScript-Codedatei unter Verwendung des Namens, den Sie im Feld **Name** als Dateinamen eingeben. Der anwenderdefinierte JavaScript-Code, mit dem diese Aktionen durchgeführt werden, muss:

- Verbindung mit einem Event-Überwachungstool herstellen
- Events aus einem Event-Überwachungstool abrufen
- Events mithilfe einer Webservice-API an die Tabelle Event [em_event] senden Siehe REST API .

Jede Connector-Definition ist spezifisch für einen Event-Quellenanbieter. Die Connector-Definition gibt die MID Server-Skripteinbindung an, die Events aus der externen Event-Quelle abruft. Darüber hinaus gibt die Connector-Definition an, welche Connector-Instanzwertparameter erforderlich sind, um eine Verbindung mit dem externen Event-Quellhost herzustellen.

Prozedur

1. Erstellen Sie eine benutzerdefinierte MID Server-Skripteinbindung.
   In diesem Beispiel wird Groovy (veraltet) verwendet. Anstelle einer Skripteinbindung in Groovy wird die Verwendung von JavaScript empfohlen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Implementieren Sie diese Methoden:

- `@Override OperationStatus testConnection()`
- `@Override OperationStatus execute()`

b. Entwerfen Sie die Klasse, um den `ThirdPartyConnector` zu erweitern.

Example

```
public class HypericConnector extends ThirdPartyConnector
```

c. Importieren Sie Plattformklassen für Event-Erstellung, -versand, -protokollierung und Connector-Basisklassen von Drittanbietern.

Example

```
package com.service_now.mid.probe.tpcon.test

import com.glide.util.Log
import com.service_now.mid.MIDServer
import com.service_now.mid.probe.event.IEventSender
import com.service_now.mid.probe.event.SNEventSender
import com.service_now.mid.probe.tpcon.OperationStatus
import com.service_now.mid.probe.tpcon.OperationStatusType
import com.service_now.mid.probe.tpcon.ThirdPartyConnector
import com.snc.commons.eventmgmt.Event
```

d. Stellen Sie über die vom Sammler bereitgestellte API eine Verbindung zum Datensammler her, z. B. SCOM oder VMware vRealize Hyperic (Hyperic).

e. Verwenden Sie die `context`-Parameter, um die Ereignisfeldwerte festzulegen, die von einer Connector-Instanz stammen.

Example

```
def authString = (context.username +
 ':'+ context.password).getBytes().encodeBase64().toString()
def urlStr = 'http://'+context.host + ':' + context.parameters.port +
 '/' + apiFunction
```

f. Implementieren Sie die `Ausführungsfunktion` im Skript.
Es liest Events vom Connector mithilfe seiner API, um Event-Objekte zu erstellen und an die ServiceNow-Instanz zu senden. Zum Beispiel:

Example

```
GPathResult alertsResponse1 = readAlerts('hqu/hqapi1/alert/find.hqu?begin='
 + lastSignatureStr +
'&end='+ tillStr +'&count=1000000&severity=1&inEscalation=false&notFixed=false');
Event event = new Event()
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
event.emsSystem = context.name
event.source = "Hyperic"
event.description = it.@reason
event.type = it.@name
...
IEventSender eventSender = MIDServer.getSingleton(SNEventSender.class)
    for (Event event  : list) {
        eventSender.sendEvent(event)
     }
```

2. Navigieren zu **MID-Server** > **MID-Serverskriptdateien** und erstellen Sie ein Skript.
3. Geben Sie das Feld **Übergeordnet** als *Groovy* an, füllen Sie das Formular entsprechend aus, und klicken Sie dann auf **Senden**.
4. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussdefinitionen** und erstellen Sie eine Connector-Definition.
5. Wählen Sie im Feld **Auszuführendes Groovy-Skript** die MID Server-Skriptdatei aus und füllen Sie das Formular entsprechend aus.
   Zusätzlich zum **Benutzernamen** oder **Host** können Sie weitere Parameter, z. B. **Port**, hinzufügen und dann auf **Senden** klicken.
6. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen** und erstellen Sie eine Connector-Instanz.
7. Wählen Sie im Feld **Connector-Definition** die Connector-Definition aus, füllen Sie das Formular entsprechend aus, und klicken Sie dann auf **Senden**.
8. Zum Bestätigen oder Debuggen des Skripts verwenden Sie Debug-Ausdrucke von Groovy im MID Serverprotokoll.
9. Um eingehende Ereignisse mit der anwenderdefinierten Connector-Instanz zu überwachen, navigieren Sie zu **ECC** > **Warteschlange** und filtern Sie nach **ConnectorProbe**.
10. Erstellen Sie eine anwenderdefinierte Connector-Definition.
    a. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussdefinitionen**.
    b. Klicken Sie auf **Neu**.
    c. Geben Sie im Feld **Name** einen beschreibenden Namen für die Connector-Definition ein.
    d. Wählen Sie im Feld **Skripttyp** die Option **Javascript** aus.
    e. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
    Das Feld **Javascript ausführen** wird automatisch mit dem Namen der JavaScript-Vorlagendatei ausgefüllt.
11. Um die Standard-JavaScript-Datei zu bearbeiten, klicken Sie auf das Informationssymbol (ⓘ) rechts neben dem Namen der JavaScript-Datei, und gehen Sie wie folgt vor:

    a. Geben Sie die erforderlichen Informationen für die Funktion **testConnection** an.
    Diese Funktion testet die Connector-Definition, um sicherzustellen, dass die Verbindung mit dem Ziel gültig ist.

    b. Geben Sie die erforderlichen Informationen für die Funktion **execute** an.
    Diese Funktion ruft die Informationen aus der externen Quelle ab.

    c. Geben Sie die erforderlichen Informationen für die Funktion **retrieveKpi** an.
    Diese Funktion ruft die Metrikdaten aus der externen Quelle ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Wahlweise: Sie können das Standard-JavaScript durch Ihren JavaScript-Code ersetzen.
13. Füllen Sie die Felder entsprechend aus.

Formular Connector-Definition

Feld	Beschreibung
Standardzeitplan	Die Anzahl der Sekunden zwischen Versuchen, Events zu empfangen.
Bidirektional	Geben Sie an, dass das externe Überwachungssystem aktualisiert werden soll, wenn die Warnung geändert wird. Für SCOM ist eine Standardimplementierung vorhanden.
Bezeichner für Warnungsfeld	Geben Sie an, dass das externe Überwachungssystem aktualisiert werden soll, wenn das Warnungsfeld manuell geändert wird. **Hinweis:** Dieses Feld ist nur sichtbar, wenn **Bidirektional** ausgewählt ist.
Metriken erfassen	Wählen Sie diese Option aus, um die Erfassung von Metriken zu aktivieren. **Hinweis:** Metriken werden nur für externe SCOM-Event-Quellen erfasst.
Standardzeitplan für Metrikerfassung (Sekunden)	Geben Sie die Anzahl der Sekunden an Informationen an, die erfasst werden müssen. Der Standardwert beträgt 10 Sekunden. **Hinweis:** Dieses Feld wird nur angezeigt, wenn **Metriken erfassen** ausgewählt ist.
Connector-Parameter	Geben Sie die Parameter an, um die Kommunikation mit einem Event-Server zu ermöglichen.
Connector-Definition zu MID-Server-Fähigkeiten	Der MID-Server-Name zur Verarbeitung von Events vom Event-Server. Wenn nicht angegeben, wird ein verfügbarer MID-Server verwendet.

14. Klicken Sie auf **Absenden**.

Konfigurieren Sie einen Pull-Connector

Konfigurieren Sie einen Pull-Connector, um die Häufigkeit der Ereignissammlung zu planen.

Vorbereitungen

Bevor Sie dieses Verfahren beginnen:

- Suchen oder definieren Sie eine Connector-Definition.
- Erstellen Sie die Anmeldeinformationen, um eine Verbindung zur Event-Quelle herzustellen.
- Wenn die Connector-Instanz für die Sammlung von Metrikdaten Metrikdaten verwendet werden soll, muss das Plugin Metrikdaten aktiviert werden.

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Connector-Instanz verwenden, um den Ort und die Art und Weise zu steuern, in der Events aus externen Quellen ankommen. Sie können optional auswählen, Informationen Metrikdaten aus den externen Quellen zu sammeln, mit denen Sie eine Verbindung herstellen. Die Funktion Metrikdaten dient der Analyse von Trends, Schwellenwertdefinitionen und der Erkennung von Anomalien. Sie können einen Test ausführen, um zu bestätigen, dass Connector-Instanzparameter zulassen, dass der MID-Server Events von einer unterstützten externen Event-Quelle an die Event-Tabelle [em_event] empfängt. Der Test bestätigt auch:

- Der MID-Server wird ausgeführt.
- Der Host wird mit der IP-Adresse ausgeführt, die sich im Feld **Host-IP** befindet.
- Sowohl der MID-Server als auch der Host werden in derselben Domäne ausgeführt.
- Die Wertfelder der Connector-Instanz sind gültig.
- Zum Abrufen von Events kann über die API eine Verbindung zur Event-Quelle hergestellt werden.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

Formular Connector-Instanz

Feld	Beschreibung
Name	Ein eindeutiger Name für den Connector-Instanzdatensatz, z. B. der Name des Event-Quellhosts.
Beschreibung	Alle optionalen Informationen, die der Administrator zur Identifizierung dieses Datensatzes verwenden möchte.
Connector-Definition **Hinweis:** Metrikdaten -Connectors (z. B. AWS CloudWatch und AzureConnector) werden im Basissystem nur angezeigt, wenn das Plugin Metrikdaten (com.snc.sa.metric) aktiviert ist.	Lieferant und Protokoll, die zum Sammeln von Ereignissen aus der externen Quelle verwendet werden. Wählen Sie die Connector-Definition aus, die der Quelle externer Events entspricht. Die im Basissystem verfügbaren Optionen sind z. B.: ◦ AWS CloudWatch ◦ AzureConnector ◦ HPOM ◦ IBM Netcool ◦ NagiosXI ◦ NNMi ◦ OMi ◦ SCOM ◦ SolarWinds ◦ Op5

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ PRTG ◦ vCenter ◦ Zabbix Eine Liste der im Basissystem verfügbaren Connector-Definitionen finden Sie unter Konfigurieren Sie Ereignismanagement die -Connectors.
Host-IP	Die IP-Adresse des Event-Quellhosts. Das System verwendet diese IP-Adresse, um den entsprechenden MID-Server für die Kommunikation mit dem Event-Quellhost auszuwählen.
Anmeldeinformationen	Der Datensatz aus der Tabelle „Anmeldeinformationen“ [discovery_credentials], der gültige Anmeldeinformationen für den Event-Quellhost enthält.
Zeit der letzten Ausführung der Event-Erfassung	Datum und Uhrzeit des letzten Event-Imports. Das Feld wird automatisch mit einem Wert ausgefüllt.
Letzter Event-Erfassungsstatus	Der Status des letzten Imports. Das Feld wird automatisch mit einem Wert ausgefüllt. ◦ **Keine**– Es wurde noch keine gültige Verbindung hergestellt. ◦ **Erfolgreich** – Es wurde eine erfolgreiche Verbindung hergestellt. ◦ **Fehler** – Es wurde eine Verbindung hergestellt. Die externe Event-Quelle wurde jedoch nicht aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Events aus der externen Event-Quelle sucht. Dieser Wert darf nicht unter dem Mindestwert für die Zeitplan-Eigenschaft liegen, die standardmäßig 120 Sekunden beträgt.
Letzte Fehlermeldung	Letzte Fehlermeldung, die vom Connector empfangen wurde Wenn der Test-Connector fehlschlägt, wird in diesem Feld eine Fehlermeldung angezeigt.
Aktiv	Diese Option wird erst angezeigt, nachdem das Formular gespeichert wurde. Aktivieren Sie dieses Kontrollkästchen erst, nachdem Sie die Verbindung zwischen MID-Server und dem Connector getestet haben. Aktivieren Sie dieses Kontrollkästchen, um das Abrufen von Events aus dieser externen Event-Quelle zu aktivieren.
Bidirektional	Wählen Sie diese Option, um die bidirektionale Option aufzurufen. Diese Option ist nur verfügbar, wenn die angegebene Connector-Definition mit bidirektionalen Werten konfiguriert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn diese Option ausgewählt ist, ermöglicht sie den bidirektionalen Austausch von Werten mit der externen Ereignis-Quelle. Die Option **Letzter bidirektionaler Status** wird nur angezeigt, wenn diese Option ausgewählt ist. Diese Option wird nur angezeigt, wenn SCOM als Connector-Definition ausgewählt ist.
Letzter bidirektionaler Status	Das Feld wird automatisch mit einem Wert ausgefüllt. Die Statuswerte sind: ◦ **Keine**– Es wurde noch keine gültige Verbindung hergestellt. ◦ **Erfolgreich** – Es wurde eine erfolgreiche Verbindung hergestellt. ◦ **Fehler** – Es wurde eine Verbindung hergestellt. Die externe Event-Quelle wurde jedoch nicht aktualisiert. Diese Option wird nur angezeigt, wenn SCOM als Connector-Definition ausgewählt ist.
Metrikensammlung	Bezeichnet eine Sammlung von Metrikdaten Metrikdaten. **Hinweis:** Der Metrik-Connector unterstützt das Arbeiten mit der SCOM-Datenbank (MSSQL), die für die Verwendung mit SSL konfiguriert ist. Diese Option wird nur angezeigt, wenn die Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Zeit der letzten Ausführung der Metrikerfassung	Das Datum und die Uhrzeit der letzten Metrikdatenerfassung. Das Feld wird automatisch mit einem Wert ausgefüllt.
Letzter Metrikerfassungsstatus	Status der Aktivität zur Erfassung von Metrikdaten. Das Feld wird automatisch mit einem Wert ausgefüllt. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die **Metrikerfassung** (z. B. SCOM) unterstützt und die Option „ Metrikerfassung“ ausgewählt ist.
Zeitplan für Metrikerfassung (Sekunden)	Die Zeit in Sekunden zur Wiederholung des geplanten Auftrags zur Metrikdatenerfassung. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die **Metrikerfassung** (z. B. SCOM) unterstützt und die Option „ Metrikerfassung“ ausgewählt ist.
Metrikdatenbank-Host	Geben Sie entweder die IP-Adresse oder den Hostnamen des Metrikdatenbank-Hosts ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Verbindung mithilfe einer benannten Instanz	Bei Auswahl dieser Option geben Sie die benannte MSSQL-Instanz an, mit der eine Verbindung hergestellt werden soll. Diese Option wird nur angezeigt, wenn SCOM als Connector-Definition ausgewählt ist.
Metrikendatenbank – benannte Instanz	Der Name der Metrikdatenbank-Instanz. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Metrikdatenbank-Port	Der von der Metrikdatenbank verwendete Port. Die Verbindung wird über JDBC hergestellt. Der Basissystemwert ist 1.433. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Datenbankanmeldung mit Windows-Authentifizierung	Bei Auswahl dieser Option erfolgt die Datenbankanmeldung mit dem Anmeldebenutzernamen, der im MID Server-Service definiert ist. Diese Option wird nur angezeigt, wenn SCOM als Connector-Definition ausgewählt ist.
Metrikensammlung wird ausgeführt	Diese Option zeigt an, dass die Sammlung Metrikdaten ausgeführt wird. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Metrikdatenbank-Anmeldeinformationen	Anmeldeinformationen für die Metrikdatenbank. Diese Option wird nur angezeigt, wenn die ausgewählte Connector-Definition die Metrikerfassung unterstützt, z. B. SCOM.
Connector-Instanzwerte	Die zugehörige Liste mit Verbindungsparametern für den Event-Quellenhost. Die Liste der Parameter hängt von der ausgewählten Connector-Definition ab.
MID Server für Connectors	Der Name des MID-Server zur Verarbeitung von Events vom Event-Server.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Connector testen**, um sicherzustellen, dass der MID-Server mit dem externen Serverhost kommunizieren kann.
6. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen auf der Seite, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus. Die Beschreibung der Fehlerursache wird im MID-Server-Protokoll entsprechend dem Fehlertyp angezeigt, z. B. Events, Metriken oder bidirektional.
7. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.
8. Bestätigen Sie, dass Ereignismanagement Events mit dieser Connector-Instanz verarbeitet, indem Sie ein Event manuell erstellen.

Zugehörige Informationen

Konfigurieren Sie Ereignismanagement die -Connectors

Standardmäßigen MID Server für Connectors konfigurieren

Sie können einen standardmäßigen MID Server für Connectors festlegen, um sicherzustellen, dass immer ein MID Server für den Empfang von externen Events verfügbar ist.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird
Der standardmäßige MID Server muss Konnektivität zu allen externen Event-Quellen haben.

Prozedur

1. Geben Sie im Navigationsfilter `sys_properties.list` ein, um die Tabelle zu den Systemeigenschaften [sys_properties] zu öffnen.
2. Wählen Sie die Systemeigenschaft `mid.server.connector_default` aus.
3. Füllen Sie die Felder des Formulars aus.

Aufgabenvorlagenformular

Feld	Beschreibung
mid.server.connector_default	Standardmäßiger MID Server für Connectors Bestimmt die zu verwendenden MID Server-Connectors, wenn kein MID Server angegeben ist. Muss mit einem MID Server-Namen übereinstimmen. ◦ **Typ**: Wählen Sie `Zeichenfolge` aus der Liste aus. ◦ **Wert**: Geben Sie den Namen eines vorhandenen MID Servers ein, z. B. SNC MID Server. ◦ **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]

Hinweis: Sie können den standardmäßigen MID Server zurücksetzen, indem Sie die Eigenschaft *`mid.server.connector_default`* löschen oder den Wert dieser Eigenschaft auf einen anderen MID Server aktualisieren. Diese Eigenschaft wird nicht in allen Szenarien automatisch zurückgesetzt.

4. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Connector-Instanz Dynatrace .

Konfigurieren Sie die Connector-Instanz Dynatrace für den Empfang von Rohdaten Metrikdaten vom Server Dynatrace.

Vorbereitungen

Um die Metrikensammlung zu aktivieren, vergewissern Sie sich, dass MID-Server, das Metriken abruft, mit der Erweiterung Metrikdaten konfiguriert ist und dass sich die Erweiterung im Modus „ **Gestartet“** befindet. Weitere Informationen finden Sie unter Konfigurieren Sie die Erweiterung Metrikdaten manuell.

- Erstellen Sie in Dynatrace ein Zugriffstoken mit Bereichsberechtigungen für das Lesen von Metriken (metrics.read), um das Abrufen von Metrikdaten zu ermöglichen. Dieses Token wird im -Connector zum Aufrufen der Dynatrace -REST-API verwendet.
- Konfigurieren Sie den Service Graph Connector für Dynatrace. Wird in der -Instanz konfiguriert und erkennt Dynatrace CIs. Weitere Informationen zur Konfiguration dieses Connectors finden Sie unter Service Graph Connector für Observability – Dynatrace konfigurieren .

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig erkennt der Service Graph Connector Dynatrace CIs und unterstützt die Metriksammlung für die folgenden Entitätstypen:

- HOST
- ANWENDUNG
- SERVICE
- PROCESS_GROUP_INSTANCE

Konfigurieren Sie andere Entitätsmetriken für die Sammlung, wenn Sie Ereignisregeln für die CI-Bindung erstellen.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Wählen Sie **Neu** aus, und erstellen Sie eine Connector-Instanz.
   Weitere Informationen zu den auf der Seite angezeigten Connector-Instanzfeldern finden Sie unter Dynatrace Formular für die Connector-Instanz.
3. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Wahlweise: Im Abschnitt „Connector-Instanzwerte“ können Sie die Werte der obligatorischen Dynatrace -Parameter bearbeiten.
   Einzelheiten zu den Wertparametern der Connector-Instanz finden Sie unter Dynatrace Wertparameter der Connector-Instanz.
5. Fügen Sie im Abschnitt MID Servers für Connectors ein MID-Server für den zu verwendenden Connector Dynatrace hinzu.
6. Wählen Sie im Abschnitt „Zugehörige Links“ **Zu erfassende Metriken konfigurieren aus**.
   Nur Metriken mit dem Wert **Active=true** werden von der Instanz gesammelt.
7. Konfigurieren Sie die Metriken, die die Instanz sammeln soll, mit dem Wert **Active=true**.
   Metriken mit dem Wert **Active=false** werden von der Instanz nicht erfasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wahlweise: Wählen Sie **Neu** aus, um neue Metriken zu erstellen.
   Konfigurieren Sie die Felder auf der Seite Connector-Instanzmetriken – Neuer Datensatz (sn_em_connector_instance_metric).

Seite mit Connector-Instanzmetriken – Neuer Datensatz

Feld	Beschreibung
Metrikname	Anzeigename für die Metrik, die in der Instanz ServiceNow konfiguriert werden soll.
Metrik-Connector-Instanz	Standardmäßig auf **Dynatrace-Connector-Instanz**festgelegt. Alle Metriken werden für die Connector-Instanz Dynatrace gesammelt.
Metriktyp	Der Name des Entitätstyps Dynatrace, zu dem die Metrik gehört.
Metrik-ID	Die Metrik-ID Dynatrace der erfassten Metrik.
Aktiv	Wählen Sie für die zu erfassenden Metriken aus.

   - Stellen Sie sicher, dass die CIs, die sich auf die Metriken beziehen, in der Instanz vorhanden sind.
   - Erstellen Sie eine Ereignisregel, um bei Bedarf die CI-Bindung durchzuführen. Details finden Sie unter Event-Regel erstellen oder bearbeiten.

9. Wählen Sie **Connector testen** aus, um die Verbindung zwischen MID-Server und dem Connector zu überprüfen.
10. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und wählen dann **Aktualisieren** aus.

Event-Erfassung von HP OMi konfigurieren

Konfigurieren Sie die Connector-Instanz von HP Operations Manager (OMi) für den Empfang von Warnungen vom HP OMi-Server.

Vorbereitungen

Unterstützte Versionen: 10.01, 10.10, 10.11, 10.12, 10.60 und 10.61.
Der OMi-Connector wird in Versionen unter Version 10 nicht unterstützt.

Erstellen Sie den Standardauthentifizierungstyp für Anmeldeinformationen, um eine Verbindung mit OMI herzustellen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

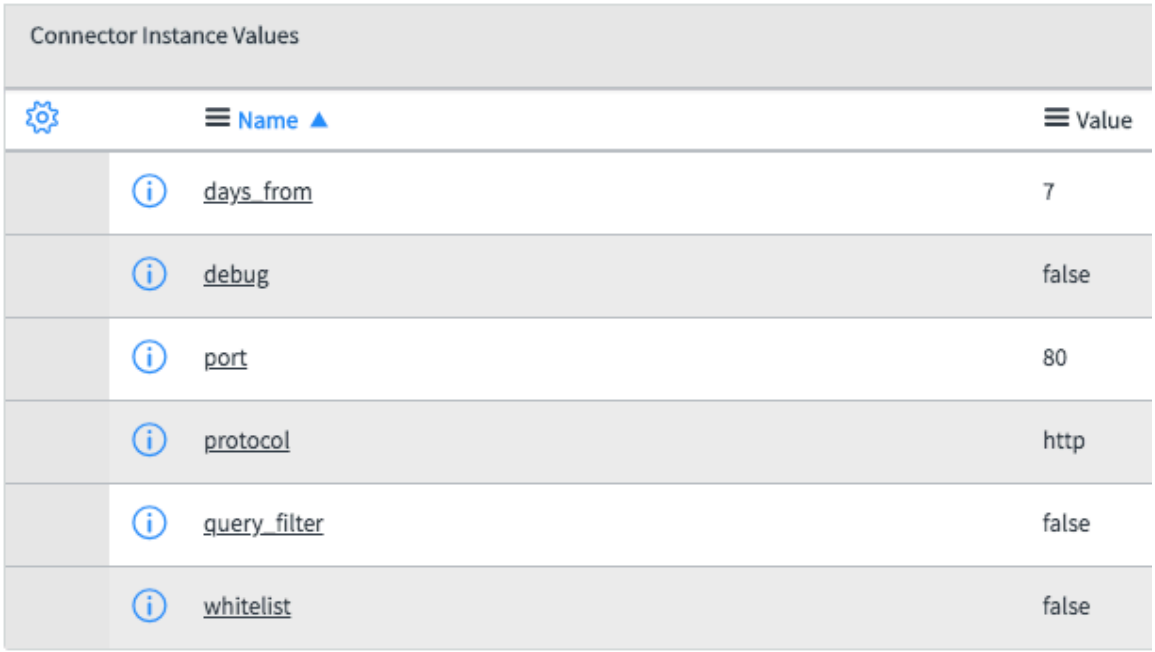
1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Name	Beschreibender Name für den OMi-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der OMi-Event-Erfassung.
Host-IP	Geben Sie die OMi-IP-Adresse an.
Anmeldeinformationen	Klicken Sie in das Feld **Anmeldeinformationen**. Wählen Sie Anmeldeinformationen für die Standardauthentifizierung aus der Liste aus, oder klicken Sie auf das Suchsymbol. Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen mit dem Typ „Standardauthentifizierung“. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „OMiOPS“.
Zeit der letzten Ausführung der Event-Erfassung	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Letzter Ausführungszeitstatus. Automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Events von OMi sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.
Connector-Definition	Wählen Sie **OMi** aus.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Optional. Name eines MID-Server. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet. Geben Sie im Abschnitt „MID-Server für Connectors“ einen aktiven und gültigen MID-Server an. Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Geben Sie im Abschnitt Connector-Instanzwerte die OMi-Werte an.

a. days_from.
Geben Sie die Anzahl der Tage an, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: `7`.

b. debug.
Standardwert: `false`. Zum Aufrufen des Debug-Modus geben Sie `true` an.

c. port.
Standardwert: `80`.

d. protocol.
Standardwert: `http`.

e. query_filter.
Standardwert: false. Wenn Sie diesen zusätzlichen Filter zum Abfragen von Events verwenden möchten, geben Sie die Event-Attribute an. Beispiel: `assigned_user = „admin“ UND title = „My Title“`. Die Abfragefilterkriterien sind:

- Eine Filtereigenschaft, die ein Event-Attribut angibt, z. B. `related_ci`
- Ein unterstützter Operator, z. B. `ODER` oder `UND`
- Ein Wert für die Filtereigenschaft, z. B. `admin` oder `integrator`

Alles aus dem Feld „query_filter“ wird einer URL-Codierung unterzogen und dann als Parameter an den OMi-API-Aufruf übergeben. Ausführliche Informationen zum Erstellen der Filterabfrage finden Sie unter „Filtern nach Event-Attributen: query“ im HP OMi-Erweiterungsleitfaden. Um beispielsweise die Events nach einer Liste von Events abzufragen, die dem Administrator zugewiesen sind, geben Sie Folgendes an:

```
event_list?query=assigned_user%20EQ%20"admin"
```

Zum Verschachteln von query_filter-Event-Attributen geben Sie die Hierarchie in eckigen Klammern „[]“ an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. **Aufnahmeliste**.
Standardwert: `false`. Geben Sie eine kommagetrennte Liste an, damit dieses Feature Attribute hinzufügt, die erfasst und dem Feld Ereignismanagement **Zusätzliche Informationen** hinzugefügt werden sollen.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Connector zu überprüfen.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum HP OMi-Server zu überprüfen.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Event-Erfassung von HPOM konfigurieren

Konfigurieren Sie die Connector-Instanz von HPOM für den Empfang von Events vom HP Operations Manager (HPOM).

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin
Unterstützte Version: 08.60.005.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu** und erstellen Sie eine HPOM-Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Geben Sie einen eindeutigen Namen für die HPOM-Connector-Instanz an.
Host-IP	Geben Sie die HPOM-IP-Adresse an.
Anmeldeinformationen	Klicken Sie in das Feld **Anmeldeinformationen**. Wählen Sie Anmeldeinformationen aus der Liste aus, oder klicken Sie auf das Suchsymbol. Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „HPOMOPS“.
Zeitplan (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von HPOM sucht.
Beschreibung	Geben Sie eine Beschreibung für die Verwendung der Instanz der HPOM-Ereigniserfassung ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Connector-Definition	Lieferant und Protokoll, die zum Sammeln von Events aus der externen Quelle verwendet werden. Wählen Sie die **HPOM**-Connector-Definition aus.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Letzte Ausführungszeit	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ausführungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.
MID Server (Abschnitt MID Server für Connectors)	Optional. Der Name des MID Servers. Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet. Geben Sie im Abschnitt MID Server für Connectors einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile des Formulars, und klicken Sie auf **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt Connector-Parameter die Werte der obligatorischen HPOM-Parameter an.
   - **driver**. Geben Sie den Treiber an, der für den Aufruf verwendet werden soll. Dieser Treiber ist spezifisch für den Typ der Datenbank, die Sie aufrufen.
     - Geben Sie für einen IBM DB2 Universal-Treiber Folgendes ein: com.ibm.db2.jcc.DB2Driver
     - Geben Sie für einen Oracle-Treiber Folgendes ein: oracle.jdbc.OracleDriver
     - Geben Sie für einen Microsoft SQL-Treiber Folgendes ein: com.microsoft.sqlserver.jdbc.SQLServerDriver
     - Geben Sie für einen MySQL-Treiber Folgendes an: com.mysql.jdbc.Driver
     - Geben Sie für einen Sybase-Treiber Folgendes an: com.sybase.jdbc3.jdbc.SybDriver
   - **url**. Geben Sie eine URL an. Das JDBC-Protokoll verwendet eine Verbindungszeichenfolge, um die Authentifizierung herzustellen, und andere Parameter, um eine Verbindung zwischen dem Client und der Datenbank herzustellen. Jede Datenbank verfügt über ein eigenes Format für Verbindungszeichenfolgen. Ersetzen Sie in den folgenden URLs die Variablen, z. B. <username> und <password> mit Ihren Werten.
     - Geben Sie für eine universelle IBM DB2-URL Folgendes an: [jdbc:db2://sysmvs1.stl.ibm.com:<port number>/<database name>:user=<username>;password=<password>]

       Beispiel: jdbc:db2://sysmvs1.stl.ibm.com:5021/regionsdb:user=example;password=wlrs21.
     - Geben Sie für eine Oracle-URL Folgendes an: [jdbc:oracle:thin:@<IP address>:<port number>:<database name>]

       Beispiel: jdbc:oracle:thin:@172.31.255.255:4028:OracleMain.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geben Sie für eine Microsoft SQL-URL Folgendes an: [jdbc:sqlserver://<IP address>;user=<username>;password=<password>]

  Beispiel: jdbc:sqlserver://localhost;user=example;password=w3lrs2.

- Geben Sie für eine MySQL-URL Folgendes an: [jdbc:mysql://<IP address>/database?user=<username>;password=<password>]

  Beispiel: jdbc:mysql://localhost/database?user=example;password=65wlrs.

- Geben Sie für eine Sybase-URL Folgendes an: [jdbc:sybase:Tds:<IP address>:<port number>/<database name>?user=<username>;password=<password>]

  Beispiel: jdbc:sybase:Tds:172.31.255.255:4100/SYBMAIN?user=example;password=wlrs1m.

5. Verwenden Sie ein Netzwerk-Tool wie Ping, um sicherzustellen, dass der HPOM-Server ausgeführt wird und die IP-Adresse mit dem Wert im Feld *Host IP* übereinstimmt.
6. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem HPOM-Connector zu überprüfen.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum HPOM-Server zu überprüfen.

8. Nach einem erfolgreichen Test wählen Sie **Aktiv** aus und klicken dann auf **Aktualisieren**.

Zugehörige Informationen

Konfigurieren Sie einen Pull-Connector

Event-Erfassung von Hyperic konfigurieren

Konfigurieren Sie die Hyperic-Connector-Instanz für den Empfang von Events vom VMware vRealize Hyperic-Server.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin
Unterstützte Version: 5.8.4.0.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu** und erstellen Sie eine Hyperic-Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Geben Sie einen eindeutigen Namen für die Hyperic-Connector-Instanz an.
Host-IP	Geben Sie die Hyperic-IP-Adresse an.
Anmeldeinformationen	Klicken Sie im Formular Anmeldeinformationen auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	Speichern Sie die Anmeldeinformationen unter einem eindeutigen und erkennbaren Namen, z. B. „HypericOPS“.
Zeitplan (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von Hyperic sucht.
Beschreibung	Geben Sie eine Beschreibung für die Verwendung der Instanz der Hyperic-Ereigniserfassung ein.
Connector-Definition	Lieferant und Protokoll, die zum Sammeln von Events aus der externen Quelle verwendet werden. Wählen Sie die **Hyperic**-Connector-Definition aus.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Letzte Ausführungszeit	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ausführungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.
MID Server (Abschnitt MID Server für Connectors)	Optional. Der Name des MID Servers. Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet. Geben Sie im Abschnitt MID Server für Connectors einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt Connector-Parameter die Werte der obligatorischen Hyperic-Parameter an.
   a. **port** Standardwert: 7080.
   b. **protocol** Standardwert: http.
5. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Connector zu überprüfen.
6. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum Hyperic-Server zu überprüfen.

7. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Zugehörige Informationen

Konfigurieren Sie einen Pull-Connector

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Erfassung von IBM Netcool konfigurieren

Konfigurieren Sie den Connector IBM Netcool_V2 für den Empfang von Ereignissen von IBM Netcool/OMNIbus-Objektservern und Impact-Servern. Der Connector IBM Netcool_V2 verwendet REST-API-Aufrufe und ist bidirektional.

Vorbereitungen

Für den Connector IBM Netcool_2:

- Erforderliche Rolle: evt_mgmt_admin
- Führen Sie die Connector-Validierung für IBM NetCool/OMNIbus Version 8.1.0 durch.

Warum und wann dieser Vorgang ausgeführt wird

Zur Verwendung IBM des Netcool_V2-Connectors konfigurieren Sie eine Connector-Instanz für den MID-Server.

Hinweis: Der IBM Netcool-Connector ist veraltet und nur IBM der Netcool_V2-Connector wird unterstützt.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Geben Sie einen eindeutigen Namen für die Netcool-Connector-Instanz an.
Beschreibung	Geben Sie eine Beschreibung für die Verwendung der Instanz der Netcool-Ereigniserfassung ein.
Host-IP	Geben Sie die Netcool-IP-Adresse an.
Anmeldeinformationen	Klicken Sie im Formular „Anmeldeinformationen“ auf **Neu**, und erstellen Sie die erforderlichen Anmeldeinformationen. Speichern Sie die Anmeldeinformationen unter einem eindeutigen und erkennbaren Namen, z. B. „NetcoolOPS“.
Zeit der letzten Ausführung der Event-Erfassung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ereigniserfassungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Events von Netcool sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Connector-Definition	Wählen Sie IBM Netcool_V2 aus, um Ereignisse aus der externen Ereignisquelle zu sammeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
MID Server (Abschnitt MID Server für Connectors)	Geben Sie einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden. Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile des Formulars, und klicken Sie auf **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt „Anschlussparameter“ den Wert der erforderlichen Netcool-Parameter an.

Connector	Erforderliche Parameter
IBM Netcool_V2	**port**: Nummer des Ports, auf dem IBM Net-cool ausgeführt wird. Beispiel: 8080 **initial_sync_in_days**: Anzahl der Tage, über die Daten beim ersten Abruf abgerufen wurden. Der Standardwert lautet 3. Er kann jedoch entsprechend Ihren Anforderungen geändert werden.

5. Stellen Sie sicher, dass die Netcool-Server aktiv sind und ausgeführt werden:
   Verwenden Sie für den Connector IBM Netcool_V2 den folgenden REST API-Aufruf, um zu überprüfen, ob die Netcool-API aktiv ist und ausgeführt wird: `http://hostname:port/objectserver/restapi/alerts/status`
6. Klicken Sie mit der rechten Maustaste in den Header Kopfzeile des Formulars, und wählen Sie **Speichern** aus.
7. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Netcool-Connector zu überprüfen.
8. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.
9. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Zugehörige Informationen

Konfigurieren Sie einen Pull-Connector

Event-Erfassung über einen Icinga2-Connector konfigurieren

Konfigurieren Sie die Icinga-2-Connector-Instanz (Icinga), um bei der Überwachung Ihrer Netzwerkressourcen Events zu empfangen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Unterstützte Version: 2.4.1.

Prozedur

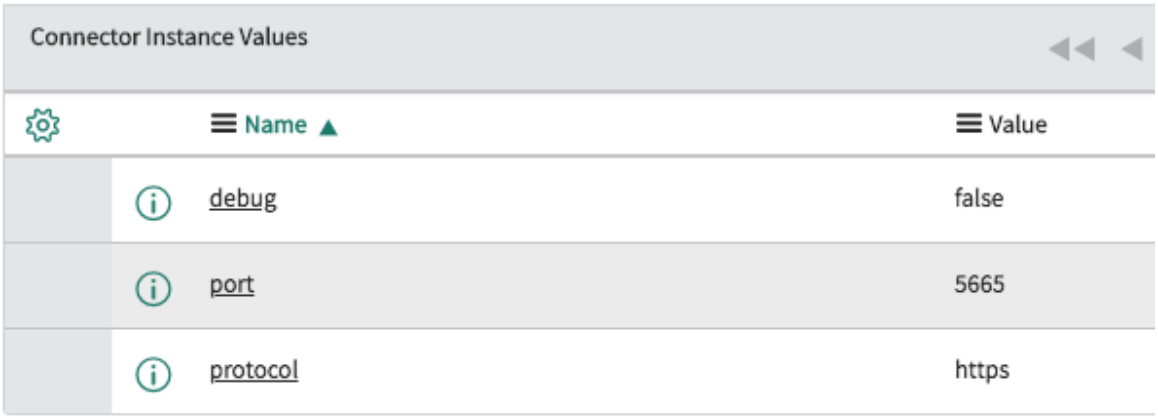
1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular Connector-Instanz

Feld	Beschreibung
Name	Beschreibender und einzigartiger Name für den Icinga-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der Icinga-Ereigniserfassung.
Connector-Definition	Name der erforderlichen Connector-Definition. Wählen Sie **Icinga2** aus.
Host-IP	IP-Adresse, unter der Icinga installiert ist.
Anmeldeinformationen	Berechtigung zum Herstellen einer Verbindung mit Icinga. Klicken Sie auf das Suchsymbol im Feld **Anmeldeinformationen**. Verwenden Sie die Anmeldeinformationen für die Standardauthentifizierung. Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen im entsprechenden Formular. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „ICINGA2CHCK“.
Zeit der letzten Ausführung der Event-Erfassung	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Letzter Ausführungsstatus. Automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Events von Icinga sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



a. debug: Zeigt Debug-Nachrichten an. Standardwert: false. Geben Sie true an, um Debug-Nachrichten anzuzeigen.

b. logPayloadForDebug: Nutzlastbezogene Debug-Nachrichten anzeigen. Standardwert: false. Geben Sie „wahr“ an, um nutzlastbezogene Debug-Nachrichten anzuzeigen.

5. Überprüfen Sie im Abschnitt Connector-Instanzwerte die Standardwerte der Connector-Instanz, und ändern Sie sie bei Bedarf.

Feld	Beschreibung
debug	Debug-Nachrichten anzeigen. Standardwert: `false`. Geben Sie `true` an, um Debug-Nachrichten anzuzeigen.
port	Nummer des Connector-Ports. Standardwert: `5665`.
protocol	Protokolltyp. Standardprotokolltyp: `https`.
alert_type	Geben Sie die Details zum Icinga-Warnungstyp an. Es gibt 2 Arten von Warnungen in Icinga2: WEICHE und HARTE WEICHEN: Die Connector-Instanz ruft eine Soft-Warnung ab. HARD: Die Connector-Instanz ruft eine harte Warnung ab.

6. Wahlweise: Geben Sie im Abschnitt „MID-Server für Connectors“ einen aktiven und gültigen MID-Server an.
Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

8. Testen Sie die Verbindung zwischen dem MID-Server und dem Connector Icinga.

a. Klicken Sie auf **Connector testen**.
Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Korrektheit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID-Server zum externen Überwachungs-Tool zu überprüfen.

b. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv**.

9. Klicken Sie auf **Aktualisieren**.

Event-Erfassung von Logicmonitor konfigurieren

Der Logicmonitor Pull-Connector sendet Informationen von Ereignismanagement an Logicmonitor. Der Pull-Connector sendet Antworten, die von einem Push-Connector in einer bidirektionalen Umgebung empfangen wurden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Regeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die**Option Zusätzliche Abgleichsregeln anwenden**Checkbox auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für den Connector ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Prozedur

1. Navigieren zu**Alle** > **Ereignismanagement** > **Ereignis-Connectors (Pull)** > **Anschlussinstanzen**.

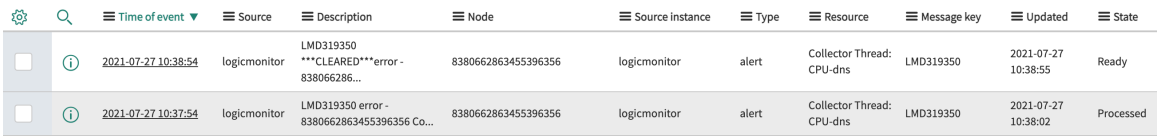
2. Klicken Sie auf **Neu**.
Die Seite**Connector-Instanz – Neuer Datensatz**wird angezeigt.

3. Geben Sie Werte in die erforderlichen Felder ein, die durch ein rotes Sternchen gekennzeichnet sind.

Feld	Beschreibung
Name	Beschreibender Name für den Connector
Connector-Definition	Suchen Sie nach**Logic Monitor**, und wählen Sie den Eintrag aus.
Referenz	Wählen Sie**Standardauthentifizierung**für die Standardauthentifizierung aus. Geben Sie access_id und access_key aus der Token-basierten API-Authentifizierung von Logicmonitor in den Anmeldeinformationen als Benutzername und Passwort für die Standardauthentifizierung an.
Host-IP	Die Logicmonitor IP-Adresse.

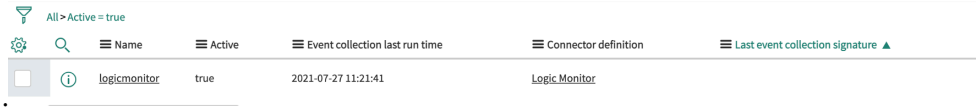
Beim Hinzufügen der bidirektionalen Funktionalität für einen Push-Connector muss der Name der Connector-Instanz mit dem Feld „Quellinstanz“ des von dieser Quelle generierten Events übereinstimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Time of event	Source	Description	Node	Source instance	Type	Resource	Message key	Updated	State
2021-07-27 10:38:54	logicmonitor	LMD319350 ***CLEARED***error - 838066286...	8380662863455396356	logicmonitor	alert	Collector Thread: CPU-dns	LMD319350	2021-07-27 10:38:55	Ready
2021-07-27 10:37:54	logicmonitor	LMD319350 error - 8380662863455396356 Co...	8380662863455396356	logicmonitor	alert	Collector Thread: CPU-dns	LMD319350	2021-07-27 10:38:02	Processed

Die Quelle der Ereignisse ist**LogicMonitor.**Daher müssen Sie eine Instanz mit dem NamenLogicMonitorerstellen.



All > Active = true

Name	Active	Event collection last run time	Connector definition	Last event collection signature ▲
logicmonitor	true	2021-07-27 11:21:41	Logic Monitor	

Hinweis: Die Geschäftsregel „Update-Warteschlange“ der Warnungstabelle identifiziert jede manuelle Aktualisierung der Warnung und aktualisiert die Connector-Warteschlange dementsprechend. Standardmäßig werden Änderungen an allen Warnungsfeldern nachverfolgt.

4. Aktivieren Sie das Kontrollkästchen**Aktiv**, und klicken Sie auf**Speichern**.

Event-Erfassung von NNMi konfigurieren

Konfigurieren Sie die HP Network Node Manager i (NNMi)-Connector-Instanz, um bei der Überwachung Ihrer Netzwerkressourcen Events zu empfangen.

Vorbereitungen

Unterstützte Version: 10.30.653.
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

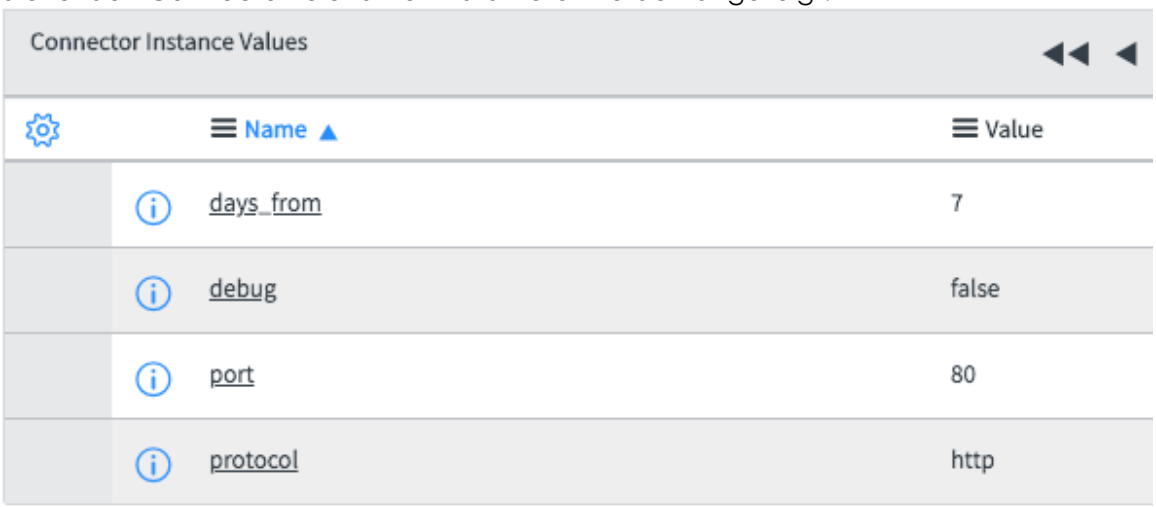
Formular Connector-Instanz

Feld	Beschreibung
Name	Beschreibender und einzigartiger Name für den NNMi-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der NNMi-Ereigniserfassung.
Connector-Definition	Name der erforderlichen Connector-Definition. Wählen Sie **NNMi** aus.
Host-IP	IP-Adresse, unter der NNMi installiert ist.
Anmeldeinformationen	Berechtigung zum Herstellen einer Verbindung mit NNMi. Klicken Sie auf das Suchsymbol im Feld **Anmeldeinformationen**. Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen im entsprechenden Formular. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „NNMiCHCK“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Für die ausgewählten Anmeldeinformationen wird die Standardauthentifizierung verwendet.
Zeit der letzten Ausführung der Event-Erfassung	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Letzter Ausführungsstatus. Automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Events von NNMi sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**. Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.



5. Überprüfen Sie im Abschnitt Connector-Instanzwerte die Standardwerte der Connector-Instanz, und ändern Sie sie bei Bedarf.

Feld	Beschreibung
days_from	Anzahl der Tage, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: `7` Tage. **Hinweis:** Die maximale Anzahl vergangener Events, die erfasst werden können, beträgt 3.000. Bei der ersten Ausführung des Connectors werden alle Events (bis zur Grenze von 3.000) erfasst, die zwischen dem Datum von `days_from` und dem aktuellen Datum erstellt wurden.
debug	Debug-Nachrichten anzeigen. Standardwert: `false`. Geben Sie `true` an, um Debug-Nachrichten anzuzeigen.
port	Nummer des Connector-Ports. Standardwert: `80`.
protocol	Protokolltyp. Standardprotokolltyp: `http`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wahlweise: Geben Sie im Abschnitt „MID Servers für Anschlüsse“ einen aktiven und gültigen MID Server an.
   Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

   Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn MID-Server nicht verfügbar ist, wird das nächste ausgewählt usw. MID-Server werden in der Reihenfolge sortiert, in der ihre Daten im Abschnitt MID-Server für Connectors eingegeben wurden.

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
8. Testen Sie die Verbindung zwischen dem MID-Server und dem Connector NNMi.

   a. Klicken Sie auf **Connector testen**.
      Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

      Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum externen Überwachungstool zu überprüfen.

   b. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv**.

9. Klicken Sie auf **Aktualisieren**.

Event-Erfassung von NagiosXI konfigurieren

Konfigurieren Sie die NagiosXI-Connector-Instanz für den Empfang von Events vom Nagios Core-Monitor.

Vorbereitungen

Unterstützte Version: 5.5.2.
Die NagiosXI-Connector-Instanz erfordert Anmeldeinformationen, mit denen die Instanz auf NagiosXI-Serverkonten zugreifen kann. Sie können vorhandene Anmeldeinformationen verwenden oder neue erstellen. Weitere Informationen finden Sie unter Erstellen Sie Nagios XI-Server-Anmeldeinformationen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Beschreibender Name für den Nagios-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der NagiosXI-Ereigniserfassung.
Host-IP	Geben Sie die Nagios XI-IP-Adresse an.
Anmeldeinformationen	Wählen Sie die Anmeldeinformationen mit Standardauthentifizierung aus, die Sie für diesen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Connector erstellt haben. Weitere Informationen finden Sie unter Erstellen Sie Nagios XI-Server-Anmeldeinformationen. Stellen Sie sicher, dass das Benutzerpasswort den NagiosXI-Benutzer-API-Schlüssel enthält, z. B. 04lquEPqf4JimWCm8RWbJokOpW8LYBUfEvJp9OSHSRYe4QDrHPFndYbW
Zeit der letzten Ausführung der Ereigniserfassung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ereigniserfassungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Events von Nagios sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Connector-Definition	Wählen Sie **NagiosXI** aus.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Optional. Name eines MID-Server. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet. Geben Sie im Abschnitt „MID-Server für Connectors“ einen aktiven und gültigen MID-Server an. Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
5. Geben Sie im Abschnitt Connector-Instanzwerte die Nagios-Werte an.
   - **initial_sync_in_days**. Geben Sie die Anzahl der Tage an, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: `7` Tage.
   - **port**. Standardwert: `80`.
   - **protocol**. Standardprotokolltyp: `http`.
   - **time_zone**. Die Standardzeitzone ist `GMT`. Aktualisieren Sie diesen Wert auf die Nagios-Zeitzone. Wenn Nagios beispielsweise die Ereignisse gemäß der EDT-Zeitzone sendet, aktualisieren Sie diesen Wert auf `GMT-04:00` (Abkürzungen wie **EDT** werden nicht unterstützt).
   - **severity_by_state_type**. Der Standardwert ist `„false“`. Bei Festlegung auf `wahr`wird der Statustyp zusammen mit dem Status verwendet, um den Schweregrad zu bestimmen. Dabei werden weniger kritische Ereignisse erstellt, wie in der folgenden Zuordnungstabelle gezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuordnungstabelle

_state_type(Connect Definitionsparameter	Status (Nagios-JSON-Nutzlastattribut)	State_type (Nagios-JSON-Nutzlastattribut)	ServiceNow **Schweregrad**
falsch	2	0/1	1 (Kritisch)
falsch	1	1	1(Kritisch)
falsch	1	0	2(Schwerwiegend)
falsch	0	0/1	5 (OK)
wahr	0	0/1	5 (OK)
wahr	1	0	4 (Warnung-weich -> Warnung)
wahr	2	0	2(Kritisch-weich -> Schwerwiegend)
wahr	3	0	4(Unbekannt-weich -> Warnung)
wahr	1	1	3(Warnung-hart -> Gering)
wahr	2	1	1(Kritisch-hart -> Kritisch)
wahr	3	1	3(Unbekannt-hart -> Gering)

6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
7. Klicken Sie auf **Connector testen**, um die Verbindung zwischen MID-Server und Connector zu überprüfen.
8. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.
   Wenn diese Meldung angezeigt wird: `Verbindungstest fehlgeschlagen: Fehler beim Herstellen einer Verbindung zu Nagios im Test-Connector. Ungültiger API-Schlüssel`, geben Sie dann den API-Schlüssel für den jeweiligen Benutzer ein, damit die Nagios-Events gelesen werden können.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Korrektheit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID-Server zum Überwachungs-Tool Nagios Core zu überprüfen.

9. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Erstellen Sie Nagios XI-Server-Anmeldeinformationen

Erstellen Sie Anmeldeinformationen, um auf den Nagios XI-Server zuzugreifen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung** aus.
4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie `Nagios-Authentifizierung` nennen.
Benutzername	Name zum Identifizieren des Benutzers. Stellen Sie sicher, dass das Benutzerpasswort den NagiosXI-Benutzer-API-Schlüssel enthält, z. B. `04lquEPqf4JimWCm8RWbJokOpW8LYBUfEvJp9OSHSRYe4QDr`
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher wird der Berechtigungsnachweis in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: `100`

5. Klicken Sie auf **Absenden**.

Ergebnisse

Die Anmeldeinformationen für die Verwendung mit dem Nagios XI-Server-Connector werden erstellt.

Zugehörige Informationen

Anmelde- und Verbindungsinformationen

Event-Erfassung von OBM konfigurieren

Konfigurieren Sie die Connector-Instanz von Operation Bridge Manager (OBM), auch als OMi v2 bezeichnet, für den Empfang von Warnungen vom OBM-Server. Das OBM-Connector-Skript OBM v2 ist nach der Installation der App Ereignismanagement Connectors verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Unterstützte Versionen: 10.01, 10.10, 10.11, 10.12, 10.60, 10.61 und 11.01.

Warum und wann dieser Vorgang ausgeführt wird
Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Ereignisregeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Zuordnung** anwenden Checkbox für Regeln auf „wahr“ gesetzt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie mehr Ereignisregeln oder Automatisierung mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Prozedur
1. Navigieren zu **Alle** > **Ereignismanagement** > **Ereignis-Connectors (Pull)** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Beschreibender Name für den OBM-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der OBM-Ereigniserfassung.
Host-IP	Geben Sie die OBM-IP-Adresse an.
Anmeldeinformationen	Wählen Sie die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu**, und erstellen Sie die erforderlichen Anmeldeinformationen. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und leicht wiedererkennbaren Namen, z. B. „OBMOPS“.
Zeit der letzten Ausführung der Event-Erfassung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ereigniserfassungsstatus	Die letzte Ausführungszeit wird automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Events von OBM sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Connector-Definition	Wählen Sie **OBM V2** aus. **Hinweis:** Dieses Skript ist nach der Installation der bereichsbezogenen App Ereignismanagement Connectors verfügbar.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Geben Sie den MID-Server zur Ausführung der OBM-Connector-Instanz an. Sie können mehrere MID Servers konfigurieren. Wenn der erste Server nicht verfügbar ist, wird der nächste MID-Server verwendet, wenn dieser MID-Server nicht verfügbar ist, wird der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	übernächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die für den OBM-Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt „Anschlussinstanzwerte“ die OBM-Werte an.

   a. **days_from**.
   Geben Sie die Anzahl der Tage an, für die Events im ersten Erfassungszyklus erfasst werden müssen. Der Standardwert beträgt `7` Tage, und Daten können maximal 7 Tage aus dem OBM-System abgerufen werden.

   b. **debug**.
   Der Standardwert ist `„false“`. Um in den Debug-Modus zu wechseln, ändern Sie den Wert in `true`.

   c. **port**.
   Der Standardwert beträgt `80`.

   d. **protocol**.
   Der Standardwert ist `http`.

   e. **query_filter**.
   Der Standardwert ist „false“. Wenn Sie diesen zusätzlichen Filter zum Abfragen von Events verwenden möchten, geben Sie die Event-Attribute an. Beispiel: `assigned_user = „admin“ UND title = „My Title“`. Die Abfragefilterkriterien sind:

   - Eine Filtereigenschaft, die ein Event-Attribut angibt, z. B. `related_ci`
   - Ein unterstützter Operator, z. B. `ODER` oder `UND`
   - Ein Wert für die Filtereigenschaft, z. B. `admin` oder `integrator`

   Alles aus dem Feld „query_filter“ wird einer URL-Codierung unterzogen und dann als Parameter an den OBM-API-Aufruf übergeben. Ausführliche Informationen zum Erstellen der Filterabfrage finden Sie unter „Filtern nach Event-Attributen: query“ im OBM-Erweiterungsleitfaden. Um beispielsweise die Events nach einer Liste von Events abzufragen, die dem Administrator zugewiesen sind, geben Sie Folgendes an:

   ```
   event_list?query=assigned_user%20EQ%20"admin"
   ```

   Zum Verschachteln von query_filter-Event-Attributen geben Sie die Hierarchie in eckigen Klammern „[]“ an.

   f. **Aufnahmeliste**.
   Der Standardwert ist `„false“`. Geben Sie eine kommagetrennte Liste an, damit dieses Feature Attribute hinzufügt, die erfasst und dem Feld Ereignismanagement **Zusätzliche Informationen** hinzugefügt werden sollen.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Connector zu überprüfen.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um sicherzustellen, dass der OBM-Server ausgeführt wird und die IP-Adresse mit dem Wert im Feld **Host-IP** übereinstimmt.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

OP5- oder OP5_v2-Connector konfigurieren

Konfigurieren Sie die OP5- oder OP5_v2-Monitor-Connector-Instanz, um Warnungen von einer OP5-Monitor-Quelle zu erhalten.

Vorbereitungen

Der OP5_v2-Connector wird in Ereignismanagement-Connectors, Version 2.3.0, August 2022, unterstützt – verfügbar im ServiceNow Store .

Unterstützte Version:

- OP5: 7.3.15
- OP5_v2: 8.3.8

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Ereignisregeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Zuordnung** anwenden Checkbox für Regeln auf „wahr“ gesetzt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie mehr Ereignisregeln oder Automatisierung mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Beschreibender Name für den OP5- oder OP5_v2-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der OP5- oder OP5_v2-Ereigniserfassung.
Host-IP	Geben Sie die OP5- oder OP5_v2-IP-Adresse an.
Anmeldeinformationen	Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen. Wenn Sie die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. OP5OPS.
Zeit der letzten Ausführung der Event-Erfassung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ereigniserfassungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.
Zeitplan für Ereigniserfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von OP5 oder OP5_v2 sucht.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Anschlussdefinition	Wählen Sie **OP5** oder **OP5_v2** aus.
Abschnitt Connector-Instanzwerte	Die für **OP5** oder **OP5_v2** spezifischen Parameter werden hier angezeigt, wenn das Formular gespeichert wird.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Optional. Name eines MID-Server. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet. Geben Sie im Abschnitt „MID Servers für Anschlüsse“ einen aktiven und gültigen MID-Server an. Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt „Anschlussinstanzwerte“ die OP5- oder OP5_v2-Werte an.

   a. **days_from**.
   Geben Sie die Anzahl der Tage an, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: `7` Tage.

   b. **debug**.
   Zeigt Debug-Nachrichten an. Standardwert: false. Geben Sie „wahr“ an, um Debug-Nachrichten anzuzeigen

   c. **logPayloadForDebug**.
   Zeigt nutzlastbezogene Debug-Nachrichten an. Standardwert: false. Geben Sie „wahr“ an, um nutzlastbezogene Debug-Nachrichten anzuzeigen.

   d. **port**.
   Standardwert: `443`.

   e. **state_types**.
   Geben Sie Filter für die Event-Erfassung basierend auf dem Attribut **state_types** an. Sie können Events basierend auf dem Statustyp filtern. Geben Sie den Typ an, z. B. `weich` oder `hart`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Connector zu überprüfen.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.
8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Konfigurieren Sie den Opsview_v2-Connector

Konfigurieren Sie die Opsview_V2-Connector-Instanz, um Warnungen von einer Opsview-Monitor-Quelle zu erhalten.

Vorbereitungen

Stellen Sie sicher, dass Sie die unterstützte Version des Connectors Opsview_V2 verwenden: 6.7.0.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Beschreibender Name für den Opsview-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der Opsview-Ereigniserfassung.
Host-IP	Geben Sie die Opsview-IP-Adresse an.
Anmeldeinformationen	Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. „OpsviewOPS“. **Hinweis:** Der Anwender muss über die Rolle „CONFIGUREVIEW“ mit Zugriff auf „ALLE ANZEIGEN, KEINE ÄNDERN“ verfügen.
Zeit der letzten Ausführung der Ereignissammlung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ereigniserfassungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.
Zeitplan für Ereigniserfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von Opsview sucht.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Connector-Definition	Wählen Sie **Opsview_v2**aus.
Abschnitt Connector-Instanzwerte	Die für Opsview_V2 spezifischen Parameter werden hier angezeigt, wenn das Formular gespeichert wird.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Optional. Name eines MID-Server. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet. Geben Sie im Abschnitt „MID Servers für Anschlüsse“ einen aktiven und gültigen MID-Server an. Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt Connector-Instanzwerte die Opsview_v2-Werte an.

   a. **days_from**.

      Geben Sie die Anzahl der Tage an, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: 7 Tage.

   b. **debug**.
      Debug-Nachrichten anzeigen. Standardwert: false. Geben Sie true an, um Debug-Nachrichten anzuzeigen.

   c. **logPayloadForDebug**.
      Zeigen Sie nutzlastbezogene Debug-Meldungen an. Standardwert: false. Geben Sie „wahr“ an, um nutzlastbezogene Debug-Nachrichten anzuzeigen.

   d. **eventtype_filter**.
      Geben Sie Filter für die Event-Erfassung basierend auf dem Attribut eventtype an. Geben Sie einen dieser Werte 0,1,2,3 an.

   e. **port**.

      Der Standardwert ist 80.

      .

   f. **protocol**.
      Standardprotokolltyp: HTTPS.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. Um die Verbindung zwischen dem MID-Server und dem Connector zu überprüfen, wählen Sie **Connector testen**aus.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn diese Meldung angezeigt wird: `Verbindungstest fehlgeschlagen: Fehler beim Herstellen einer Verbindung zu Opsview im Test-Connector. Ungültiger API-Schlüssel`, geben Sie dann den API-Schlüssel für den jeweiligen Benutzer ein, damit die Opsview-Events gelesen werden können.

Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zur Opsview-Monitor-Quelle zu überprüfen.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und wählen dann **Aktualisieren** aus.

PRTG-Connector konfigurieren

Konfigurieren Sie die PRTG-Connector-Instanz, um Warnungen von einer Paessler PRTG-Monitor-Quelle zu erhalten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin
Unterstützte Version: 21.3.71.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Beschreibender Name für den PRTG-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der PRTG-Ereigniserfassung.
Host-IP	Geben Sie die PRTG-IP-Adresse an.
Anmeldeinformationen	Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. `PRTGOPS`.
Zeit der letzten Ausführung der Event-Erfassung	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ereigniserfassungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.
Zeitplan für Ereigniserfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von PRTG sucht.
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Connector-Definition	Wählen Sie **PRTG** aus.
Abschnitt Connector-Instanzwerte	Die für **PRTG** spezifischen Parameter werden hier angezeigt, wenn das Formular gespeichert wird.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Optional. Name eines MID-Server. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	Server mit übereinstimmendem IP-Bereich verwendet. Geben Sie im Abschnitt „MID Servers für Anschlüsse“ einen aktiven und gültigen MID-Server an. Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt Connector-Instanzwerte die PRTG-Werte an.

   a. **add_columns**.
   Geben Sie an, welche Spalten vom Connector zurückgegeben werden sollen. Trennen Sie die Namen durch ein Komma, ohne Leerzeichen zwischen den Namen. Die Ausgabe wird im Feld **Zusätzliche Informationen** des Events gespeichert. Standardwert: `false`. Wenn `false` angegeben ist, wird nur die Standardliste der Spalten abgerufen: parent, name, type, objid, tags, message, status, priority, datetime, actions, baselink, basetype, modifiedby.

   > **Hinweis:** Es können nur Spaltennamen, die für den **Nachrichteninhaltstyp** gelten, angegeben werden.

   b. **date_format**.
   Das Datums- und Uhrzeitformat. Standardformat M/t/jjjj/ h:mm:ss a. Wenn Sie ein Event erhalten, dessen Datum in einem anderen Format vorliegt, ändern Sie diesen Wert so, dass es dem Format des eingehenden Events entspricht. Andernfalls wird das Event nicht ordnungsgemäß verarbeitet.

   Beispiel: Wenn ein Event am 27. Juni 2019 um 11:25 Uhr mit dem aufgelisteten Datum *`2019/06/27/ 11:25:00 a`* ankommt, ändern Sie den Wert **date_format** in *`yyyy/M/d/ h:mm:ss a`*, damit es dem Format des empfangenen Events entspricht.

   In **date_format** steht `a` für morgens und `p` für nachmittags.

   c. Geben Sie im Feld **days_from** die Anzahl der Tage an, für die beim ersten Erfassungszyklus Ereignisse gesammelt werden sollen.
   Standardwert: `7` Tage.

   d. **debug**.
   Standardwert: `false`.

   e. **port**.
   Standardwert: `80`.

   f. **protocol**.
   Standardprotokolltyp: `http`.

   g. **prtg_api_fetched_events_num**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Maximale Anzahl von Events pro Abfrage, die vom PRTG-Client auf den MID-Server abgerufen werden können. Standardanzahl: `50.000`.

h. time_zone.
Die Standardzeitzone ist `GMT`. Aktualisieren Sie diesen Wert auf die PRTG-Zeitzone. Wenn PRTG beispielsweise Ereignisse gemäß der `EDT-` Zeitzone sendet, aktualisieren Sie diesen Wert auf `GMT-4` (Abkürzungen wie EDT werden nicht unterstützt).

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
6. Klicken Sie auf **Connector testen**, um die Verbindung zwischen MID-Server und Connector zu überprüfen.
7. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.
Wenn diese Meldung angezeigt wird: `Verbindungstest fehlgeschlagen: Fehler beim Herstellen einer Verbindung zu PRTG im Test-Connector. Ungültiger API-Schlüssel`, geben Sie dann den API-Schlüssel für den jeweiligen Benutzer ein, damit die PRTG-Events gelesen werden können.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Korrektheit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID-Server zu PRTG zu überprüfen.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Apache Kafka Consumer Connector

Mit der Verbraucher-Connector-Instanz Apache Kafka können Sie Ereignisse aus Nachrichten erstellen, die aus dem Thema Apache Kafka als JSON-Payload gesammelt wurden, die wichtige Informationen in einem Datenblock enthält.

Apache Kafka ist ein verteiltes Publish/Subscribe-Messagingsystem, das Daten aus unterschiedlichen Quellsystemen empfängt und die Daten in Echtzeit für Zielsysteme verfügbar macht.

Sie können diesen Connector verwenden, um ServiceNow Ereignisse aus Kafka-Nachrichten zu erstellen. Nachrichten im Kafka-Thema müssen im JSON-Format vorliegen.

Wie andere Nachrichten-Broker-Systeme erleichtert Kafka den asynchronen Datenaustausch zwischen Prozessen, Anwendungen und Servern.

Kafka-Software wird auf einem oder mehreren Servern ausgeführt. Jeder Knoten, der als Broker bezeichnet wird, in einem Kafka-Cluster hilft Erstelleranwendungen, Daten in Themen zu schreiben, in denen Datensätze gespeichert und veröffentlicht werden. Verbraucheranwendungen lesen aus Themen. Themen sind in Partitionen unterteilt, um sie leichter verwaltbar zu machen, und Kafka garantiert eine strenge Reihenfolge für jede Partition.

Konfigurieren Sie den Verbraucher-Connector Apache Kafka .

Konfigurieren Sie die Instanz des Verbraucher-Connectors Apache Kafka, um Ereignisse aus Streaming-Nachrichten zu erstellen, die vom Connector Apache Kafka gesammelt werden.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular Connector-Instanz

Feld	Wert
Name	Beschreibender und eindeutiger Name für den Kafka-Verbraucher-Connector.
Beschreibung	Beschreibung, die von der Instanz der Kafka-Verbraucher-Ereignissammlung verwendet werden soll.
Connector-Definition	Name der erforderlichen Connector-Definition, in diesem Fall Kafka-Verbraucher.
Host-IP	Die Host-IP. **Hinweis:** Dieses Feld muss einen Wert enthalten, um den Erstellungsprozess abzuschließen. Daher muss der Platzhalter 1.1.1.1 als temporärer Wert eingegeben werden.
Zeit der letzten Ausführung der Ereignissammlung	Dieses Feld wird automatisch auf den letzten Laufzeitwert festgelegt.
Status der letzten Ereignissammlung	Dieses Feld wird automatisch auf den letzten Laufzeitstatus gesetzt.
Zeitplan für Ereignissammlung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen vom Kafka Consumer sucht. Der Standardwert beträgt 60 Sekunden.
Letzte Fehlermeldung	Dieses Feld wird automatisch auf die letzte Fehlermeldung festgelegt.

4. Erstellen Sie für PLAINTEXT oder SASL_PLAINTEXT im Feld **Anmeldeinformationen** die Anmeldeinformationen für die Standardauthentifizierung.
   Verwenden Sie den **SSL-Anmeldeinformationstyp Kafka** für eine neue Kafka-Pull-Connector-Instanz mit **SASL_PLAINTEXT-** Authentifizierung. Fahren Sie mit Schritt 5 fort.

   Verwenden Sie den **SSL-Anmeldeinformationstyp Kafka**, wenn der Wert des Parameters **„sasl.enabled.mechanismen“** oder **„sasl.mechanismus“** des Kafka-Servers nicht gleich **PLAIN**ist. Fahren Sie mit Schritt 5 fort.

   a. Wählen Sie das Suchsymbol neben dem Feld **Anmeldeinformationen**.

   b. Wählen Sie im Bildschirm Anmeldeinformationen **Neu**.

   c. Wählen Sie in der Liste der verfügbaren Anmeldeinformationen **Anmeldeinformationen für Standardauthentifizierung**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Geben Sie im Bildschirm „Standardauthentifizierung“ Informationen für die PLAINTEXT-Authentifizierung an, für die keine Anmeldeinformationen erforderlich sind, oder für die SASL_PLAINTEXT-Authentifizierung, für die Anmeldeinformationen erforderlich sind.

- Geben Sie für die PLAINTEXT-Authentifizierung im Feld **Name** einen beliebigen Wert ein, und lassen Sie die Felder **Anwendername** und **Passwort** leer.
- Geben Sie für die SASL_PLAINTEXT-Authentifizierung im Feld **Name** einen Namen für die Anmeldeinformationen ein, vorzugsweise mit dem Präfix `SASL`. Geben Sie den Anwendernamen und das Passwort in den Feldern **Anwendername** und **Passwort an**.

e. Wählen Sie **Absenden**.

5. Erstellen Sie für SASL_PLAINTEXT-, SSL- oder SASL_SSL-Authentifizierungsanmeldeinformationen im Feld **Anmeldeinformationen** Kafka SSL-Anmeldeinformationen.

a. Wählen Sie das Suchsymbol neben dem Feld **Anmeldeinformationen**.

b. Wählen Sie im Bildschirm Anmeldeinformationen **Neu**.

c. Wählen Sie in der Liste der verfügbaren Anmeldeinformationen **Kafka SSL-Anmeldeinformationen**aus.

d. Füllen Sie im Bildschirm „Kafka SSL-Authentifizierung“ die Felder für Kafka SSL-Anmeldeinformationen aus.
Beschreibungen der Felder für SSL-Anmeldeinformationen für Kafka finden Sie unter .

Hinweis: Wenn Sie das Feld **Verifizierung des Hostnamens deaktivieren** löschen, geben Sie im Feld **Zusätzliche Kafka-Verbrauchereigenschaften** den Wert des Parameters *`ssl.endpoint.identification.algorithm`* ein, der dem Wert des Kafka-Serverparameters entspricht. Zum Beispiel:

```
ssl.enabled.protocols=TLSv1.2,TLSv1.1,TLSv1;
sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLogin
Module required username=<username> password=<password>;
sasl.enabled.mechanisms=PLAIN;ssl.endpoint.identification.algorith
m=;
```

e. Wählen Sie **Absenden**.

6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

7. Überprüfen Sie in der Tabelle mit den Connector-Instanzwerten die ausgefüllten Connector-Instanzwerte basierend auf Ihrem Kafka-Setup und der Nachricht (JSON-Nutzlast), die Sie vom Kafka-Thema erhalten haben.

Ändern Sie bei Bedarf die Werte der Connector-Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wertetabelle für die Connector-Instanz

Feld	Beschreibung
authentication_type	Der Kafka-Verbraucher-Authentifizierungstyp. Die derzeit unterstützten Werte sind: ◦ PLAINTEXT (keine Authentifizierung) (Standard) ◦ SASL_PLAINTEXT (Standardauthentifizierung – Anwendername und Passwort)
bootstrap_servers	Die Server, die die Verbindung zum Kafka-Cluster herstellen. Die Werte in diesem Feld müssen das Format „host1:port1“, „host2:port2“ usw. haben (kommagetrennt). Dies ist ein Pflichtfeld.
consumer_group_name	Verbrauchergruppenname. Wenn dasselbe Kafka-Thema von zwei verschiedenen Instanzen verwendet wird, verwenden Sie unterschiedliche Verbrauchergruppennamen, damit alle Ereignisse für beide Instanzen erfasst werden. Dies ist ein Pflichtfeld.
time_of_event_field	Der Name des Felds in der JSON-Nutzlast/ Nachricht, das die Zeit des Ereignisses enthält. Wenn ein Feld in der JSON-Nutzlast/ Nachricht die Zeit des Ereignisses enthält, sollte dieser Wert der Wert für diesen Parameter sein. Wenn kein Zeitfeldwert angegeben ist, wird die Empfangszeit des Ereignisses in der Instanz ServiceNow als „time_of_event“ festgelegt. Das Feld „time_of_event“ muss ein Feld der ersten Ebene in der JSON-Nutzlast/ Nachricht sein. Verschachtelte Feldnamen sind nicht zulässig.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zeitzone	Die Zeitzone des Felds „time_of_event“ in der JSON-Nutzlast/Nachricht. Der Zeitzonenwert wird nicht verwendet, wenn das Feld „time_of_event“ leer ist. Wenn sich beispielsweise „time_of_event“ in der Nutzlast/Nachricht in der IST-Zeitzone befindet, lautet der Wert „GMT+0530“. Standardwert: GMT.
date_format	Das Format „date_time“ des Felds „time_of_event“ in der JSON-Nutzlast/ Nachricht Wenn kein Zeitfeldwert angegeben wird, wird die Zeit verwendet, zu der das Ereignis in der Instanz in GMT-Zeit empfangen wurde. Der Wert von „date_time“ wird nicht verwendet, wenn das Feld „time_of_event“ leer ist. Standardwert: jjjj-MM-tt HH:mm:ss.
debuggen	Zeigt Debug-Nachrichten an. Standardwert: false. Geben Sie true an, um Debug-Nachrichten anzuzeigen.
logPayloadForDebug	Zeigt nutzlastbezogene Debug-Nachrichten an. Standardwert: false. Geben Sie „wahr“ an, um nutzlastbezogene Debug-Nachrichten anzuzeigen.
Thema	Das Kafka-Thema, aus dem die Nachrichten abgerufen werden. Dies ist ein Pflichtfeld.

8. Geben Sie im Abschnitt **„MID-Server für Connectors“** einen aktiven und gültigen MID-Server an.

   Hinweis: Sie können mehrere MID Servers konfigurieren. Wenn der erste Server ausgefallen ist, wird der nächste MID-Server verwendet. Wenn MID-Server nicht verfügbar ist, wird das nächste ausgewählt usw. MID Servers sind in der Reihenfolge sortiert, in der ihre Daten im Abschnitt **„MID-Server für Connectors“** eingegeben wurden.

   Wenn Sie kein MID-Serverangeben, wird ein verfügbares MID-Server mit einem übereinstimmenden IP-Bereich verwendet.

9. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
10. Testen Sie die Verbindung zwischen MID-Server und dem Kafka Consumer-Connector.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie **Connector testen**.

b. Wenn die Testverbindung fehlschlägt, überprüfen Sie, ob die Anmeldeinformationen gültig sind und ob das Netzwerk von MID-Server mit dem Kafka-Broker verbunden ist.

Hinweis: Die Validierung des Kafka-Themennamens erfolgt nur bei der **Test-Connector** -Validierung.

11. Aktivieren Sie nach einem erfolgreichen Test die Connector-Instanz, indem Sie das Kontrollkästchen **Aktiv** aktivieren.
12. Wählen Sie die Schaltfläche **Aktualisieren** aus.

Nächste Maßnahme
Nachdem der Connector erstellt wurde, müssen Sie die Felder zuordnen. Weitere Informationen finden Sie unter Nutzlastattribute der Kafka-Nachricht an Warnungsfelder zuordnen.

Nutzlastattribute der Kafka-Nachricht an Warnungsfelder zuordnen

Ordnen Sie Kafka-Nachrichtenattribute Warnungsfeldern zu, um Warnungen basierend auf den Nachrichten aussagekräftiger zu machen. Verwenden Sie die Ereignisfeldzuordnung, um Kafka-Schweregradwerte den entsprechenden ServiceNow -Werten zuzuordnen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie je nach Nutzlast Ereignisfeldzuordnungen, um umfassendere Informationen in einer Ereigniswarnmeldung bereitzustellen, indem Sie Werte aus der Ereignisfeld-Zuordnungsregel durch das Ereignis ersetzen. Transformieren Sie abhängig von Ihrer Nutzlast Informationen in Ereignisse, um die angegebenen Warnungsfeldwerte auszufüllen, und erstellen Sie Warnungsfelder aus verschiedenen Werten, um Warnungen für die Nachverfolgung und Behebung zu generieren. Verwenden Sie bei Bedarf sowohl Ereignisfeldzuordnungen als auch Warnungsregeln.

In der folgenden Tabelle werden eine von einem -Thema empfangene Nachricht und eine reduzierte Nutzlast im Feld **„Zusätzliche Informationen“** zum Ereignis verglichen. Die von einem Thema empfangene Nachricht wird als einzelnes Feld reduziert und im Feld **Zusätzliche Informationen** zum Ereignis angezeigt. Verwenden Sie diese reduzierten Nachrichten, um Ereignisregeln und Zuordnungen zu erstellen.

Tatsächliche vs. reduzierte Nutzlast

Tatsächliche Nutzlast, die in ein Thema eingefügt wurde	Vereinfachte Nutzlast im Feld „Zusätzliche Informationen“.

<pre>{
"version": "v0.1.0",
"name": "fibsrc",
"id": "mnop6789",</pre>
	<pre>{
	"flattened.alert_type": "on_true",
	"flattened.description": "Current value (12.296815 k) greater than threshold value (5 k)",</pre>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tatsächliche vs. reduzierte Nutzlast (Fortsetzung)

Tatsächliche Nutzlast, die in ein Thema eingefügt wurde	Vereinfachte Nutzlast im Feld „Zusätzliche Informationen“.

"trigger_description": "Triggers on duration_ms goes above 5K",
"status": "TRIGGERED",
"alert_type": "on_true",
"summary": "Triggered: fibsrc",
"description": "Current value (12.296815 k) greater than threshold value (5 k)",
"operator": "greater than",
"threshold": 5000,
"groups": [
{
"Group": "GroupA",
"Result": 12296.815478000368
}
],
"trigger": {
"Result": 12296.815478000368
}
}
	"flattened.id": " mnop6789",
	"flattened.kafkaKey": "null",
	"flattened.kafkaOffset": "28",
	"flattened.kafkaPartition": "0",
	"flattened.kafkaTopicName": "topic123",
	"flattened.name": "fibsrc",
	"flattened.operator": "greater than",
	"flattened.status": "TRIGGERED",
	"flattened.summary": "Triggered: fibsrc",
	"flattened.trigger_description": "Triggers on duration_ms goesa above 5K",
	"flattened.version": "v0.1.0",
	"flattened.version": 5000,
	"flattened.groups.0.Group": "GroupA",
	"flattened.groups.0.Result": 12296.815478000368,
	"flattened.trigger.Result": 12296.815478000368
	}

Prozedur

1. Dient zum Zuordnen der Kafka-Nachrichtenattribute zu vordefinierten Warnungsfeldern, um durch die Erstellung von Ereignisfeldzuordnungen Warnungen zu generieren.
   a. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisfeldzuordnung**.
   b. Wählen Sie im Fenster „Ereignisfeldzuordnung“ **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Geben Sie im Feld Name einen Namen für die Feldzuordnung ein.

d. Geben Sie im Feld Quelle **den Wert Kafka Consumer**ein.

e. Wählen Sie im Feld Zuordnungstyp den entsprechenden Zuordnungstyp aus

f. Eine Liste der verfügbaren Zuordnungstypen finden Sie unter Ereignisfeldzuordnungen.

2. Um die Attribute der Kafka-Nachricht den vordefinierten Warnungsfeldern zuzuordnen, um durch das Erstellen von Ereignisregeln Warnungen zu generieren.

a. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.

b. Wählen Sie **Neu** aus.

c. Geben Sie im Feld Name einen Namen für die Ereignisregel ein.

d. Geben Sie im Feld Quelle **den Wert Kafka Consumer**ein.

e. Wählen Sie **Ereignisfilter**aus.

f. Geben Sie den entsprechenden Filter für Ihre Anforderung ein.

g. Wählen Sie **Umwandeln und Warnungsausgabe verfassen aus**.

Beim Erstellen von Ereignisregeln werden die Ereignisfelder auf der Registerkarte Ereignisregeln transformieren und Warnungsausgabe erstellen angezeigt. Da die Kafka-Nachricht von Anwender zu Anwender unterschiedlich ist, müssen Sie die Ereignisfelder in Warnungsfelder umwandeln, um die Details in der Warnung anzuzeigen.

Hinweis: Da der Schweregradwert zum Erstellen einer Warnung erforderlich ist, müssen Sie das Feld **Schweregrad** mithilfe von Ereignisregeln oder Ereignisfeldzuordnungen zuordnen. Wenn das Feld Schweregrad leer ist, wird das Ereignis nicht verarbeitet und geht in einen Fehlerstatus über.

h. Ordnen Sie die Felder des Ereignisses und des Feldes **Zusätzliche Informationen** den Feldern der Warnung zu.

i. Wählen Sie **Bindung**aus.

j. Geben Sie die entsprechende Bindung für Ihre Anforderung ein.

k. Wählen Sie **Absenden**.
Weitere Informationen finden Sie unter Event-Regel erstellen oder bearbeiten.

3. Überprüfen Sie im Bildschirm „Alle Ereignisse“, ob sich eines der Ereignisse von Kafka aufgrund einer fehlenden Ereignisregel in einem Fehlerstatus befindet, und geben Sie fehlende Regeln an.

a. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**.

b. Öffnen Sie in der Tabelle „Alle Ereignisse“ ein beliebiges Kafka-Verbrauchereereignis, für das als Status „Fehler“ in der Spalte **Schweregrad** angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die vom Kafka-Verbraucher empfangene Nachricht kann variieren. Da der Connector die empfangenen Attribute nicht kennen kann, müssen Sie das Feld **Schweregrad** oder andere Ereignisfelder den Feldern in der Nachricht zuordnen, um sicherzustellen, dass die Warnungsfelder ordnungsgemäß ausgefüllt werden.

c. Erstellen Sie im Bildschirm „Alle Ereignisse“ eine neue Ereignisregel, indem Sie **Ereignisregel erstellen**auswählen.
Weitere Informationen zum Erstellen von Ereignisregeln finden Sie unter Ereignisregeln.

Wenn für den neuen Ereignistyp keine Ereignisfeldzuordnungen vorhanden sind, erstellen Sie Ereignisfeldzuordnungen. Weitere Informationen finden Sie unter Event-Feldzuordnungen erstellen.

Ergebnisse
Ihr Apache Kafka-Verbraucher-Connector ist konfiguriert. Wenn neue Nachrichten im Kafka-Thema eingehen, werden sie in der Instanz ServiceNow als Ereignisse, empfangen; aus diesen Ereignissen werden dann Warnungen erstellt.

SAP Solution Manager-Connector konfigurieren

Konfigurieren Sie die Connector-Instanz von SAP Solution Manager (Solman), um die Kommunikation zwischen SAP Solution Manager und Ereignismanagement zu ermöglichen.

Vorbereitungen
Erforderliche Rolle: admin
Unterstützte Versionen: Getestet in SAP Solution Manager 7.2. Funktioniert möglicherweise auch mit anderen Versionen.

Warum und wann dieser Vorgang ausgeführt wird
Mit dieser Konfiguration können Sie den SAP Solution Manager mit den Status aktualisieren, die von ServiceNow aktualisiert wurden. Allgemeine Informationen zum SAP Solution Manager finden Sie unter SAP-Konfigurationen zur Aktivierung des SAP Solution Manager-Connectors.

Prozedur
1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu** und erstellen Sie eine Connector-Instanz.
3. Füllen Sie die Felder im Formular aus.

Formular Connector-Instanz

Feld	Beschreibung
Name	Beschreibender Name für den SAP Solman-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der SAP Solman-Ereigniserfassung.
Aktiv	Option, die die Connector-Instanz aktiviert. Wählen Sie diese Option nur nach erfolgreichem Test aus.
Connector-Definition	Lieferant und Protokoll, die zum Sammeln von Events aus der externen Quelle verwendet werden. Wählen Sie **SAP Solman** aus.
Host-IP	Die IP-Adresse, unter der SAP Solman installiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anmeldeinformationen	Erforderliche Anmeldeinformationen wurden entweder durch Auswahl aus den Ergebnissen einer Suche über das Suchsymbol oder durch Klicken auf **Neu** eingegeben. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter einem eindeutigen und erkennbaren Namen, z. B. `SAPSOLMANOPS`.
Zeit der letzten Ausführung der Event-Erfassung	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Letzter Ausführungszeitstatus. Automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von SAP Solman sucht.
Bidirektional	Wählen Sie diese Option aus, um den bidirektionalen Austausch von Werten mit der externen Ereignis-Quelle auszulösen. Die Option **Letzter bidirektionaler Status** wird nur angezeigt, wenn diese Option ausgewählt wird.
Letzter bidirektionaler Status	Dieses Feld ist nur sichtbar, wenn **Bidirektional** ausgewählt ist. Dieses Feld wird automatisch mit dem neuesten bidirektionalen Status ausgefüllt.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.
Abschnitt Connector-Instanzwerte	Die für SAP Solman spezifischen Parameter, die beim Speichern des Formulars automatisch angezeigt werden.
MID Servers (Abschnitt „MID-Server für Anschlüsse“)	Aktiver und gültiger MID-Server. Sie können mehrere MID Servers so konfigurieren, dass bei Ausfall des ersten Servers der nächste MID-Server verwendet wird. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.

5. Geben Sie im Abschnitt Connector-Instanzwerte die Standardwerte der Connector-Instanz an.
   - **Client**: Standardwert = `001`
   - **Port**: Standardwert = `8000`
6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
7. Klicken Sie auf **Connector testen**, um die Verbindung zwischen MID-Server und Connector zu überprüfen.
   Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung und führen Sie dann einen weiteren Test aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Verwenden Sie ein Netzwerk-Tool wie *Ping*, um die Anmeldeinformationen und die Netzwerkkonnektivität vom MID-Server zum Überwachungs-Tool SAP Solman zu überprüfen.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken auf **Aktualisieren**.

Zugehörige Informationen

Pull-Connector des SAP Solution Manager verwenden

SAP-Konfigurationen zur Aktivierung des SAP Solution Manager-Connectors

Konfigurieren Sie Ihre SAP-Umgebung für die Verwendung mit der ServiceNow Ereignismanagement-Plattform, damit Sie den SAP Solution Manager-Connector verwenden können.

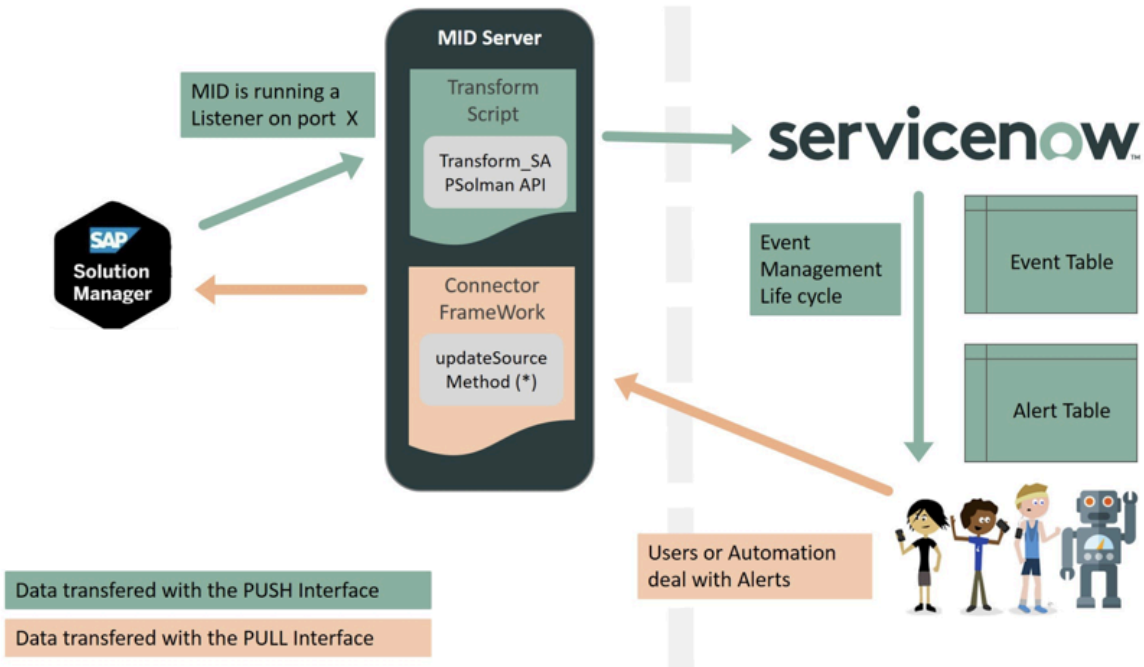
Bei der Integration Ihrer SAP-Umgebung mit Ereignismanagement werden Events von SAP Solution Manager über einen MID-Server an Ereignismanagement gesendet, das aus dem Event eine Warnung generiert.

Nachdem der MID-Server Events verarbeitet hat, können Sie in SAP Solution Manager die folgenden Aktionen ausführen:

- Kommentare hinzufügen
- Warnungen bestätigen
- Den Status auf **Extern verwaltet** festlegen

Das folgende Diagramm veranschaulicht den Datenfluss zwischen SAP und Ereignismanagement.

SAP Solution Manager-Connector



Daten werden mithilfe von Push- und Pull-Schnittstellen zwischen SAP und Ereignismanagement verschoben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Pull-Schnittstelle**:

  Die Tabelle der Connector-Update-Warteschlangen [em_connector_update_queue] listet manuelle Updates von Warnungen auf und sendet sie an den SAP Solution Manager.

  Die Geschäftsregel der Tabelle identifiziert jede manuelle Aktualisierung von Warnungen in Ereignismanagement und aktualisiert die Connector-Warteschlange mit diesen Änderungen. Standardmäßig werden Änderungen an allen Warnungsfeldern nachverfolgt. Informationen zum Anpassen dieser Einstellung finden Sie in der Dokumentation zum SAP Solution Manager.

  Mit der regelmäßigen Aufgabe „Ereignismanagement – Warteschlangen-Connector-Prozessor“ werden Warnungsänderungen aus der Warteschlange entfernt und an den MID-Server gesendet. Standardmäßig führt das System diesen Prozess in Batches von 1.000 Warnungen aus. Sie können die Batch-Größe anpassen, indem Sie die *evt_mgmt.max_update_source_records*-Einstellung ändern.

  Hinweis: Sie müssen die Pull-Schnittstelle definieren, um die bidirektionale Funktionalität im SAP Solution Manager-Connector zu aktivieren. Weitere Informationen finden Sie in der Dokumentation zum SAP Solution Manager.

- **Push-Schnittstelle**: Da SAP Daten nur an eine externe Quelle weitergeben kann, verwendet die Integration die Push-Schnittstelle, um von SAP an Ereignismanagement gesendete Warnungen zu speichern.

  SAP-Warnungen erstellen Events in Ereignismanagement, die sowohl Event-Regeln als auch CI-Identifizierungsregeln verwenden, um Ereignismanagement-Warnungen zu erstellen.

  Nachdem Ereignismanagement Warnungen erstellt hat, wartet eine Geschäftsregel auf eine Änderung der Warnung. Wenn eine Änderung erkannt wird, aktualisiert Ereignismanagement die Warnungen des SAP Solution Manager.

Zugehörige Informationen

Ereignismanagement-Integrationen

Pull-Connector des SAP Solution Manager verwenden

Pull-Connector des SAP Solution Manager verwenden

Der Pull-Connector des SAP Solution Manager sendet Informationen aus Ereignismanagement an den SAP Solution Manager. Der Pull-Connector sendet Antworten, die von einem Push-Connector in einer bidirektionalen Umgebung empfangen wurden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Ereignis-Connectors (Pull)** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu**.
   Die Seite **Connector-Instanz – Neuer Datensatz** wird angezeigt.
3. Geben Sie Werte in die erforderlichen Felder ein, die durch ein rotes Sternchen gekennzeichnet sind.

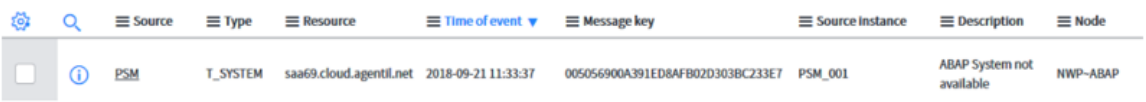
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Beschreibender Name für den Connector
Connector-Definition	Suchen Sie nach **SAP Solution Manager** und wählen Sie ihn aus.
Anmeldeinformationen	Wählen Sie **Standardauthentifizierung** für die Standardauthentifizierung aus.
Host-IP	Die IP-Adresse des SAP Solution Manager.

Die Tabelle der Connector-Update-Warteschlangen [*em_connector_update_queue*] listet manuelle Updates von Warnungen auf und sendet mithilfe der Pull-Schnittstelle ein Event an den SAP Solution Manager.

Hinweis: Beim Hinzufügen der bidirektionalen Funktionalität für einen Push-Connector muss der Name der Connector-Instanz mit dem Feld „Quellinstanz" des von dieser Quelle generierten Events übereinstimmen. Der Feldwert **Connector-Instanz** ist eine Kombination aus `SID + _ + Mandant`.

Das folgende Bild zeigt beispielsweise ein Event, das von der Instanzquelle **PSM_001**generiert wurde. Um das Zurücksenden von Informationen zu ermöglichen, müssen Sie Ihre Connector-Instanz **PSM_001** nennen.



4. Legen Sie die folgenden Werte für die Connector-Instanz fest:
   - **Client**: Stellt den Clientwert in SAP dar, normalerweise 001.
   - **Port**: Der WebService-Port von SAP Solution Manager. Standardwert = 8000.

In der folgenden Tabelle sind die Aktionen aufgeführt, die Sie in Ereignismanagement ausführen können, und die daraus resultierenden Aktualisierungen im SAP Solution Manager.

Ereignismanagement-Aktionen und SAP Solution Manager-Updates

Aktion in Ereignismanagement	**Ergebnis in SAP Solman**
Eine Warnung schließen.	Bestätigt eine Warnung im Warnungs-Posteingang. Die Warnung wird entfernt.
Wählen Sie die Einstellung **Wartung** in einer Warnung aus.	Fügt einen Kommentar hinzu, der angibt, dass sich die Warnung im Wartungsmodus befindet.
Heben Sie die Einstellung **Wartung** in einer Warnung auf.	Entfernt den Wartungsmodus-Kommentar.
Wählen Sie die Einstellung **Bestätigt** in einer Warnung aus.	Fügt einen Kommentar hinzu, der angibt, dass sich die Warnung im bestätigten Modus befindet.
Heben Sie die Einstellung **Bestätigt** in einer Warnung auf.	Entfernt den Kommentar zum bestätigten Modus.

Achten Sie auf die folgenden Verhaltensweisen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Geschäftsregel „Update-Warteschlange“ der Warnungstabelle identifiziert jede manuelle Aktualisierung der Warnung und aktualisiert die Connector-Warteschlange dementsprechend. Standardmäßig werden Änderungen an allen Warnungsfeldern nachverfolgt.
- Der Job Ereignismanagement-Warteschlangen-Connector-Prozessor entfernt Warnungsänderungen aus der Warteschlange und sendet sie an den MID Server. Standardmäßig führt Ereignismanagement diesen Dequeue-Prozess in Batches von 1.000 Warnungen aus. Sie können die Batch-Größe konfigurieren, indem Sie die Eigenschaft `evt_mgmt.max_update_source_records` festlegen.

Pull-Connector des SAP Solution Manager verwenden

Mit dem Eventsammler des MID Server-Webservice können Sie Warnungen erfassen, die vom SAP Solution Manager über Event Stream-Benachrichtigungsfunktionen gesendet wurden. Die Schnittstelle führt sowohl eine Push- als auch eine Pull-Schnittstelle aus, um direkt mit dem SAP Solution Manager zu interagieren.

Vorbereitungen

- Stellen Sie den MID Server bereit und starten Sie ihn.
- Konfigurieren Sie einen MID Web Server.
- Konfigurieren und starten Sie den Eventsammler des MID Server-Webservice.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

SAP Solution Manager sendet Event-Nachrichten im JSON-Format an den MID Server. Der MID Server analysiert die erfassten Warnungsnachrichten und wandelt sie mit dem SAP Solman-Umwandlungsskript [*TransformEvents_SAPSolman*] um.

JSON-formatierte Nachrichten werden mithilfe der Standardauthentifizierung erfasst. Weitere Informationen zu anderen unterstützten Authentifizierungsmethoden finden Sie unter MID-Webservererweiterung konfigurieren.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Push-Connectors**.
2. Wählen Sie das Skript **SAP Solman Transform Script** aus.
3. Verwenden Sie die folgende URL, um Warnungsmeldungen von SAP Solution Manager zum MID Server zu verschieben:
   `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_SAPSolman`, wobei Folgendes zutrifft:
   - **MID_Server_IP** ist die IP-Adresse der MID-Webservererweiterung
   - **MID_Web_Server_Port** ist der Listener-Port der MID-Webservererweiterung

Nächste Maßnahme

Erstellen Sie einen Remote Function Call (RFC) im SAP Solution Manager, und installieren Sie einen Transport, wie in RFC im SAP Solution Manager konfigurieren beschrieben.

Zugehörige Informationen

MID-Server konfigurieren

MID-Webservererweiterung konfigurieren

MID-WebService-Event-Sammlerkontext konfigurieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einrichtungskonfiguration des SAP Solution Manager

Als Teil der Einrichtung von SAP Solution Manager müssen Sie mehrere Konfigurationen durchführen, damit SAP Solution Manager mit Ereignismanagement interagieren kann.

RFC im SAP Solution Manager konfigurieren

Im Rahmen der Aktivierung der Kommunikation mit Ereignismanagement müssen Sie in SAP Solution Manager einen Remote Function Call (RFC) erstellen und eine Übertragung installieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Laden Sie die folgenden PSM-Dateien herunter, und importieren Sie sie in das SAP Solution Manager-System.

- https://downloads.docs.servicenow.com/resource/enus/cad/K900249.PSM
- https://downloads.docs.servicenow.com/resource/enus/cad/R900249.PSM

Prozedur

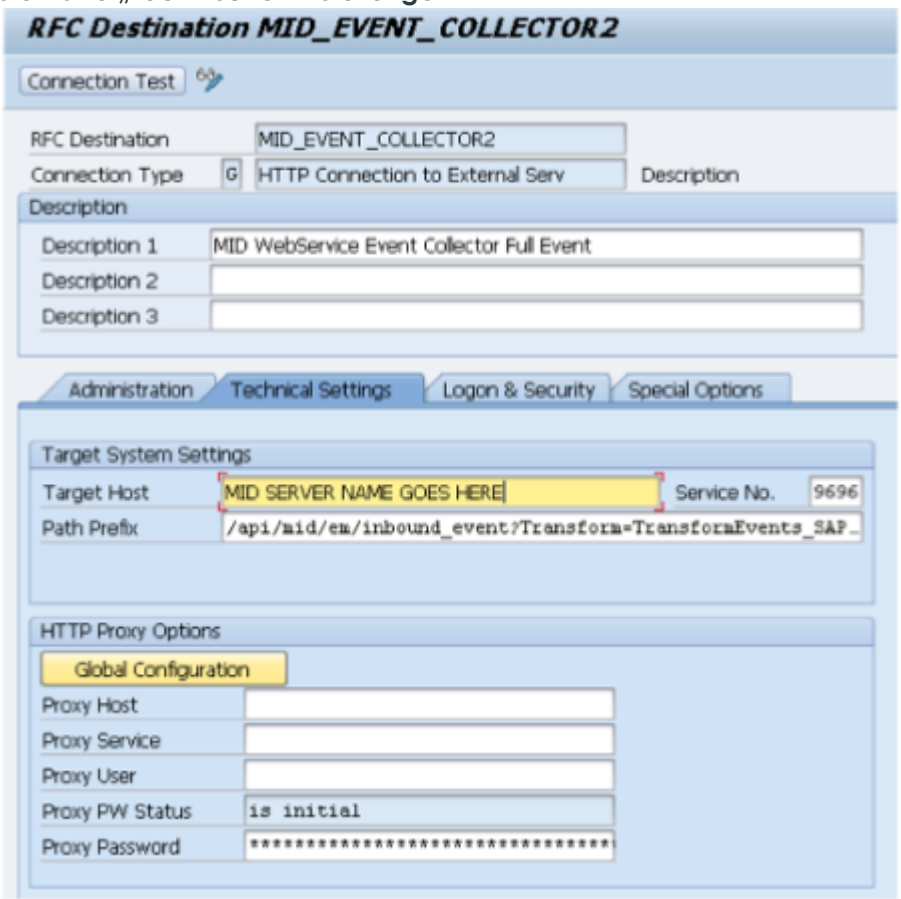
1. Geben Sie auf der SAP-UI den Transaktionscode `SM59` ein, und erstellen Sie auf der Registerkarte **Technische Einstellungen** einen neuen RFC mit den folgenden Parametern:

RFC-Parameter

SAP-Parameter	Wert
Zielhost	Name des MID-Servers
Service-Nr.	Listener-Port auf dem MID-Server
Pfadpräfix	URL des MID-Server-Transformationsskripts: `/api/mid/em/inbound_event?Transform=TransformEvents_SAPSolman`

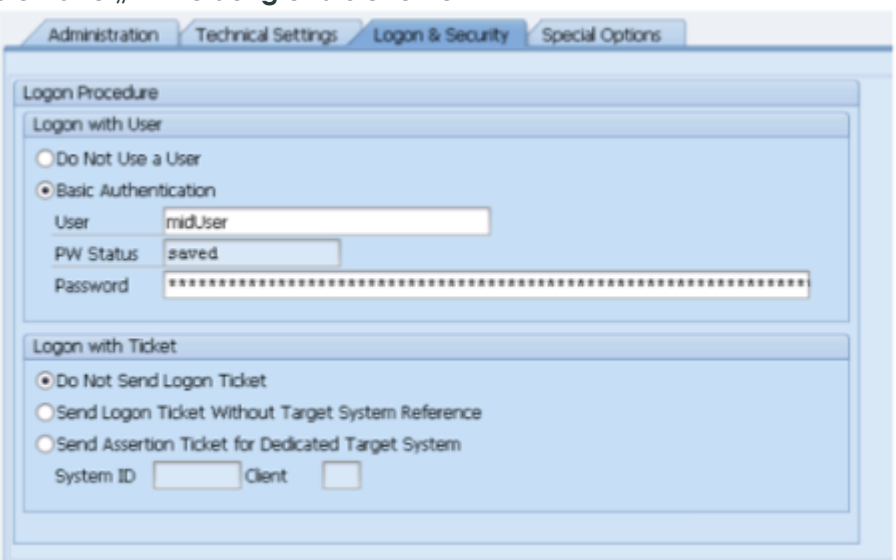
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Technische Einstellungen“



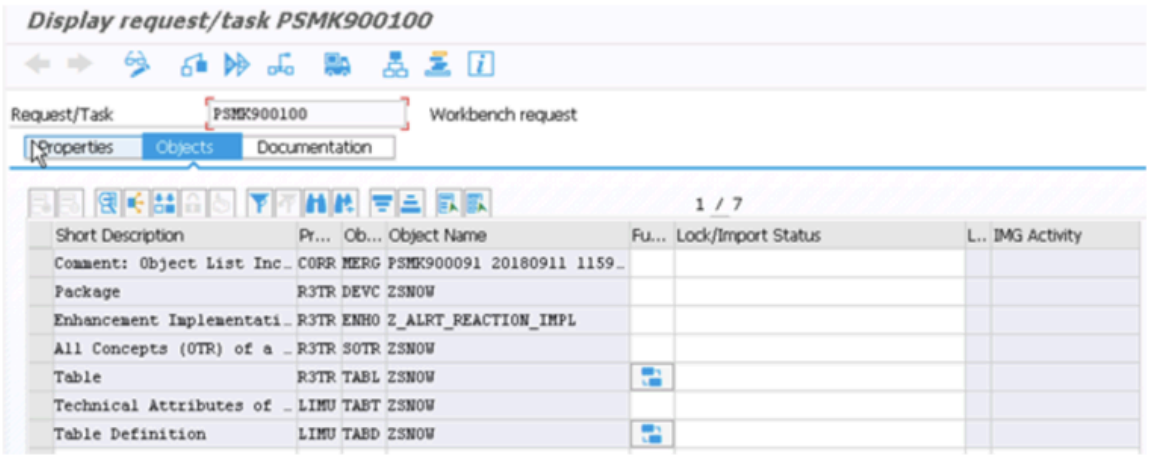
2. Auf der Registerkarte **Anmeldung & Sicherheit** wählen Sie **Standardauthentifizierung** und geben Ihre Ereignismanagement-Anmeldeinformationen in den Feldern **Benutzer** und **Kennwort** ein.

Registerkarte „Anmeldung und Sicherheit“



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein benutzerdefiniertes SAP BADI (Business Add-in) namens Z_ALRT_REACTION_IMPL wird erstellt und als Workbench-Transportauftrag gespeichert. Nach der Installation ruft dieses BADI den RFC auf, um eine Verbindung mit Ereignismanagement herzustellen.



SAP konfigurieren, um Warnungen an Ihr BADI weiterzuleiten

Nach der Einrichtung der Überwachung des SAP Solution Manager müssen Sie SAP so konfigurieren, dass Warnungen an das BADI (Business Add-in) weitergeleitet werden, das Sie als ersten Schritt in der Einrichtung der SAP-Integration erstellen.

Vorbereitungen

Erforderliche Rolle: evt_mgt_admin

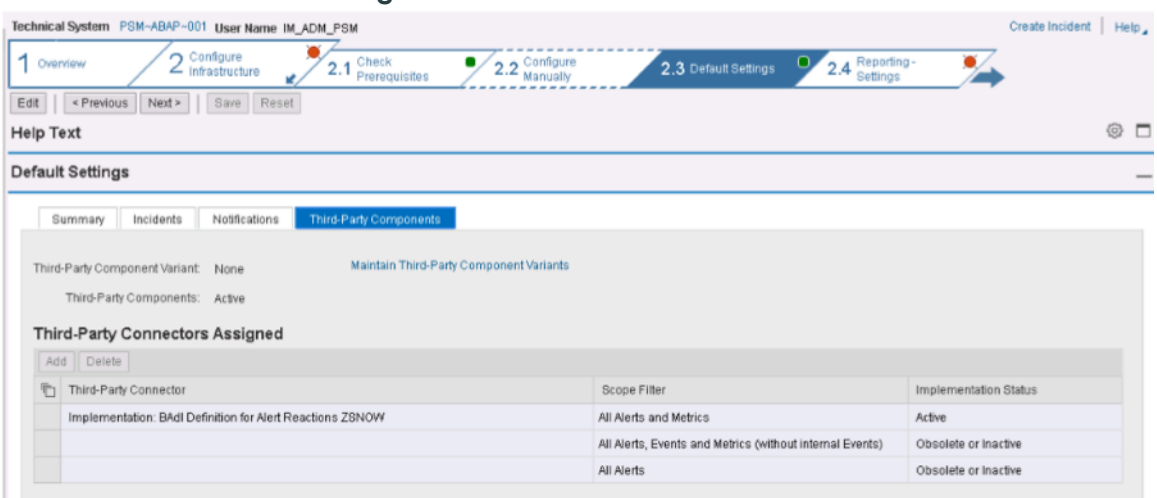
Warum und wann dieser Vorgang ausgeführt wird

Warnungen von Dritten werden global weitergeleitet. Sie können die Warnungsreaktion nur für eine bestimmte Überwachungsvorlage konfigurieren.

Prozedur

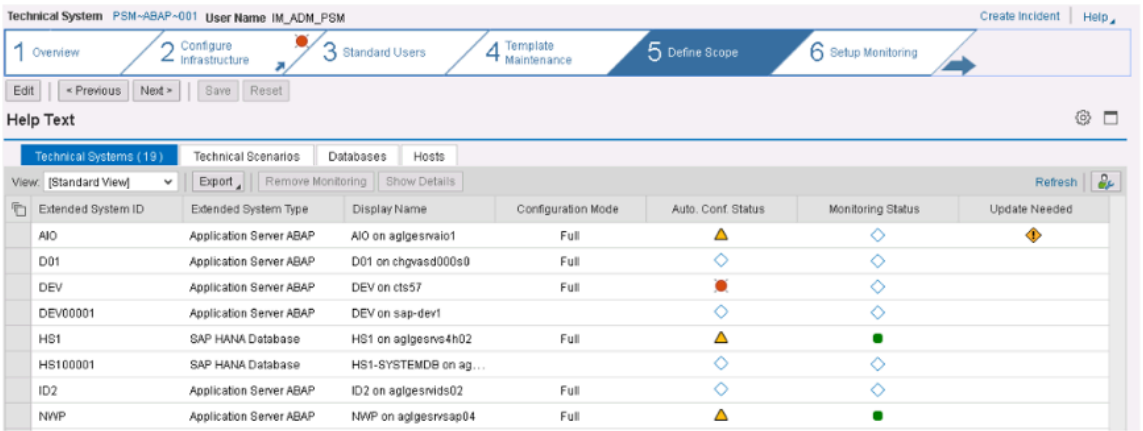
1. Navigieren Sie auf der SAP-UI zu **Anwendungsvorgänge** > **Systemüberwachung**.
2. Wählen Sie im Menüband oben auf der Konfigurationsseite der Systemüberwachung die Option aus **2 Konfigurieren Sie die Infrastruktur** > **2.3 Standardeinstellungen**.
   Die Seite **Standardeinstellungen** wird angezeigt.

Seite Standardeinstellungen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Konfigurieren und aktivieren Sie eine Fremdkomponente.
   a. Wechseln Sie in den Bearbeitungsmodus, indem Sie auf die Schaltfläche **Bearbeiten** klicken.
   b. Wählen Sie die Registerkarte **Fremdkomponenten** aus.
   c. Klicken Sie auf **Hinzufügen** und fügen Sie den folgenden Wert als Fremd-Connector hinzu: `Implementierung: BADI-Definition für Warnungsreaktionen ZSNOW mit Bereich = Alle Warnungen und Metriken`.
   d. Klicken Sie auf **Speichern**, um Fremdkomponenten global zu aktivieren.
4. Definieren Sie die Objekte, denen die Überwachungsvorlage zugewiesen wird.
   a. Wählen Sie im Menüband oben auf der Seite **5 Umfang definieren** aus.
   Die Seite „Umfang definieren“ wird angezeigt.



   b. Wählen Sie das verwaltete Objekt aus, dem Sie die Überwachungsvorlage zuweisen möchten.
   Die Überwachungsvorlage wird den ausgewählten Objekten zugewiesen.

5. Aktivieren Sie die Überwachung von Vorlagen erneut.
   a. Wählen Sie **6 Setup-Überwachung**.
   b. Suchen Sie Einträge mit **Setup-Status = Neukonfigurieren erforderlich** und weisen Sie diesen Einträgen die Überwachungsvorlage zu.
   c. Wählen Sie **Anwenden** und **Aktivieren** aus.
   Stellen Sie nach Abschluss der Aufträge sicher, dass der **Zuweisungsstatus** grün ist.
   Alle Vorlagen und aktiven Warnungen, die den ausgewählten Objekten zugewiesen sind, verwenden die neue Weiterleitungsmethode.

Nächste Maßnahme

Zeigen Sie in SAP Solution Manager generierte Warnungen an, um alle dringenden Probleme anzuzeigen (siehe Warnungen im Posteingang von SAP Solution Manager anzeigen) .

Alert-Eingang in SAP Solution Manager konfigurieren

Konfigurieren Sie SAP Solution Manager, um Warnungen auf dem System abzurufen, indem Sie den Alert-Eingang mit dem SOA-Manager aktivieren.

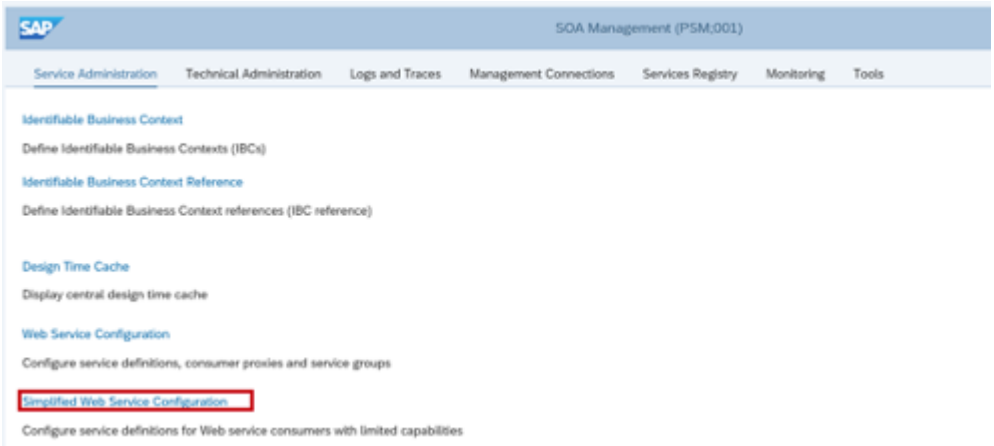
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren Sie in SAP Solution Manager zu `/sap/bc/webdynpro/sap/appl_soap_management?sap-client=XXX&sap-language=EN#`, und wählen Sie **SOA Management** (SOA-Verwaltung) aus.

Seite „SOA Management“ (SOA-Verwaltung)



2. Wählen Sie **Simplified Web Service Configuration** (Vereinfachte Webservicekonfiguration) aus, um das Formular zu validieren, mit dem der Service aktiviert wird.

Nächste Maßnahme
Zeigen Sie in SAP Solution Manager generierte Warnungen an, um alle dringenden Probleme anzuzeigen (siehe Warnungen im Posteingang von SAP Solution Manager anzeigen) .

Warnungen im Posteingang von SAP Solution Manager anzeigen

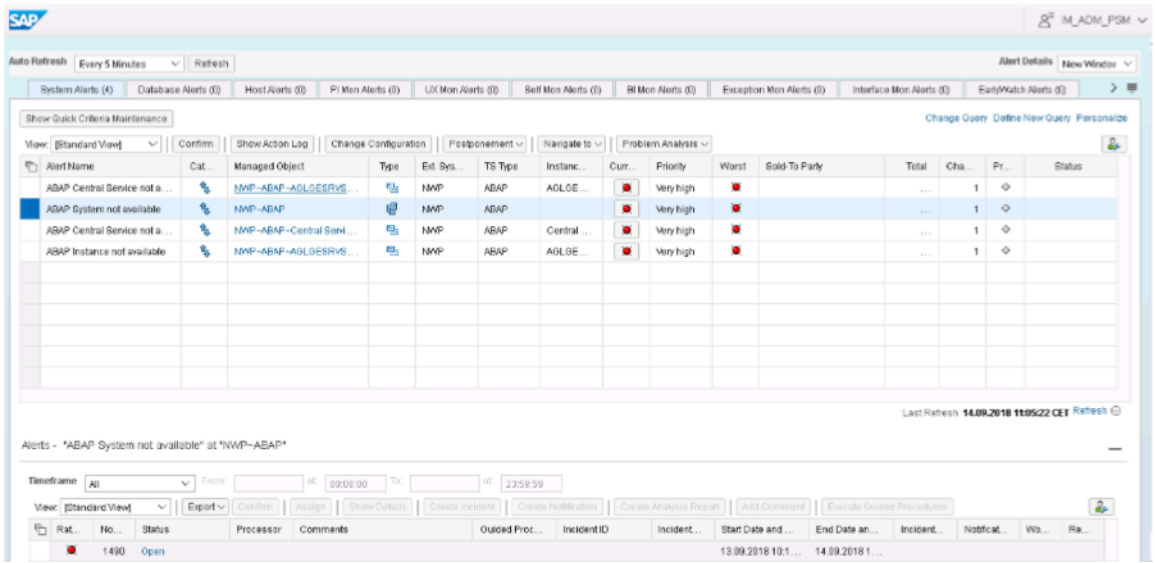
Sie können in SAP Solution Manager generierte Warnungen anzeigen, um alle dringenden Probleme anzusehen. Alle Warnungen werden auch automatisch an Ereignismanagement weitergeleitet.

Vorbereitungen
Erforderliche Rolle: evt_mgt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

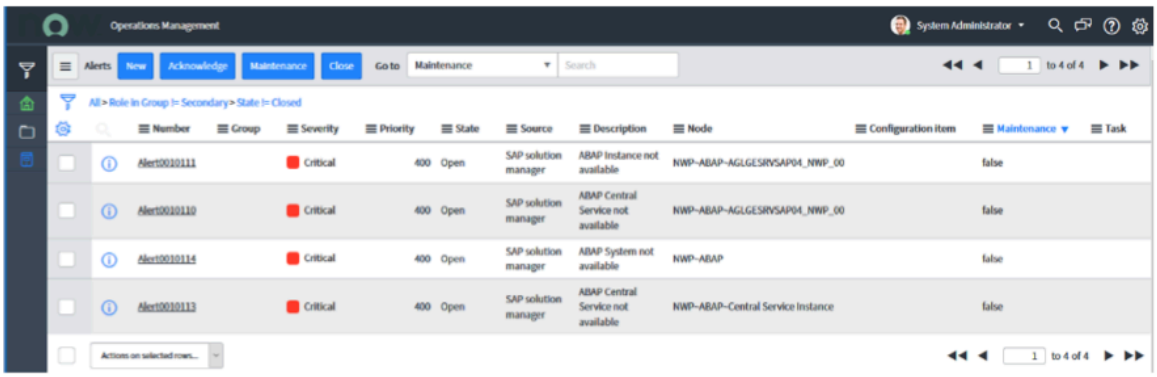
Prozedur

1. Öffnen Sie auf der SAP-UI den Solution Manager und wählen Sie die Registerkarte **Systemwarnungen** aus.



Die Systemwarnungen werden auf der Seite aufgelistet.

2. Navigieren Sie zu (**Ereignismanagement** > **Alle Warnungen** um die Warnungen in Ereignismanagementanzuzeigen.



In der folgenden Tabelle wird die Feldzuordnung zwischen SAP Solution Manager und Ereignismanagement für Warnungen beschrieben.

Feldzuordnung für SAP Solution Manager und Ereignismanagement

SAP-Feld	Event Management-Feld	Beschreibung
severity	severity	SAP verwendet eine Zahl von 1 (weniger kritisch) bis 9 (kritischer)
message_key	message_key	SAP-Nachrichtengruppen-ID, messageGUID
description	description	Event-Beschreibung
source	source	SAP-System-ID

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAP-Feld	Event Management-Feld	Beschreibung
managed_object_type	type	Der Typ des Objekts, z. B. Host oder Instanz
node	node	Objektname
managed_object_name	Ressource	Knotenname Solution Manager
N. z. (von SAP ist kein Wert angegeben. Ereignismanagement generiert das angegebene Feld.)	source instance	Die Ereignisklasse muss mit dem Namen der Connector-Abrufinstanz übereinstimmen und folgende Struktur aufweisen <Source>:<Client> .
Quelle	additional_info.sid	SAP-System-ID
rating	additional_info.rating	Event-Farbe in SAP
resource	additional_info.mandant	SAP-Mandant
metric_name	metric_name	Metrikname für das SAP-Ereignis
time_of_event	time_of_event	Zeit des Events in SAP

Example: Hohe CPU-Auslastung auf SAP-Host

Szenario: In SAP Solution Manager wird eine Warnung generiert, wenn die CPU-Auslastung auf einem kritischen Host für mehr als 10 Minuten 90 % überschreitet.

SAP Solution Manager-Warnung

Feld	Wert
Schweregrad	8 (Kritisch)
Nachrichtenschlüssel	CPU_Überlast_12345
Beschreibung	Hohe CPU-Auslastung auf SAPHost01
Quelle	SAP_Prod
Typ	Host
Knoten	SAP-Knoten_01
Zeit	31.07.2024T14:23:00Z

So wird die Warnung in Ereignismanagementzugeordnet:

Warnung Ereignismanagement wurde zugeordnet

Feld	Wert
Schweregrad	8
Nachrichtenschlüssel	CPU_Überlast_12345
Quelle	SAP_Prod
Typ	Host

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnung Ereignismanagement wurde zugeordnet (Fortsetzung)

Feld	Wert
Knoten/Ressource	SAP-Knoten_01
Quellinstanz	SAP_Prod_100
SID	SAP_Prod
Bewertung	Rot
Mandant	100

SAP Solution Manager-Zertifikat anzeigen und aktualisieren

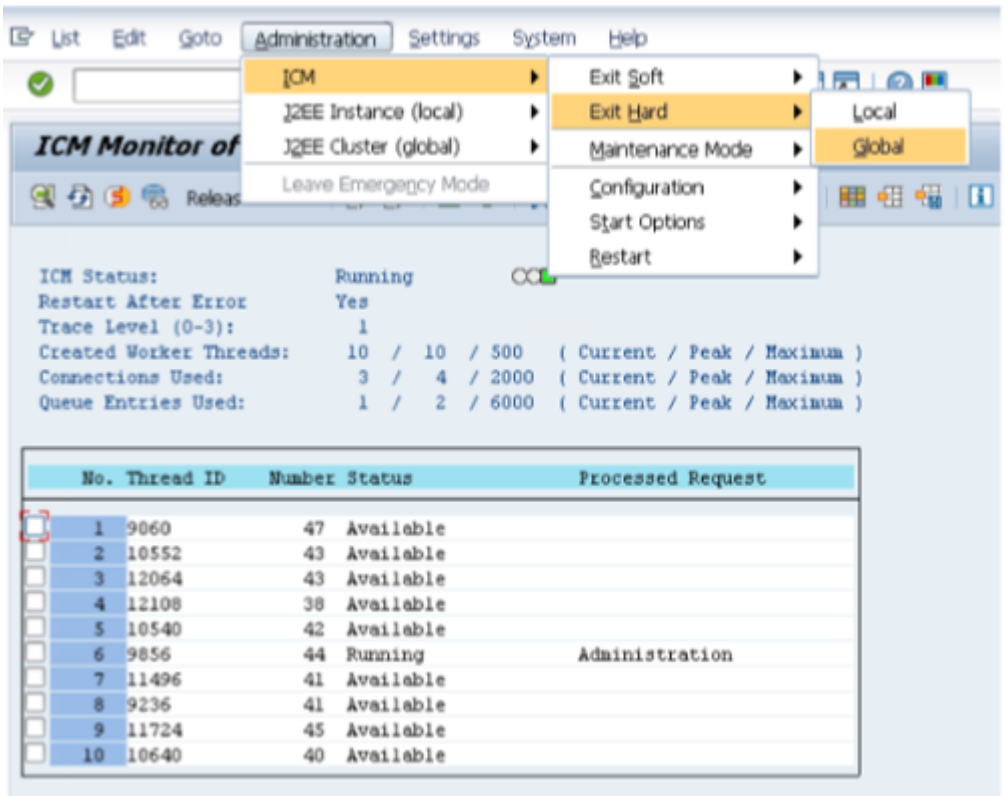
Zeigen Sie Ihr SAP Solution Manager-Zertifikat an und aktualisieren Sie es gegebenenfalls.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Stellen Sie eine Verbindung zu SAP auf Client 00 her.
2. Geben Sie die `strust`-Transaktion ein.
3. Öffnen Sie in der Trust Manager-UI den SSL-Client.
4. Importieren Sie das SSL-Zertifikat, und speichern Sie es.
5. Verwenden Sie die Transaktion `smicm`, um das System mit HTTP- und HTTPS-Clients zu verbinden.
6. Navigieren zu **Administration** > **ICM** > **Hart beenden** > **Global**.



Das ICM-Modul wird neu gestartet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAP-Schnittstellenprotokoll anzeigen

Zeigen Sie das SAP-Schnittstellenprotokoll an, um Probleme zu debuggen.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

Wählen Sie eine Transaktion in der SAP-UI aus.
Die Debugging-Tabelle der ZSNOW-Schnittstelle wird angezeigt.

SAP Solution Manager-Transaktionscodes

Die Transaktionscode-Abkürzungen, die Sie in der SAP-Schnittstelle verwenden können, wenn Sie mit dem SAP Solution Manager-Connector arbeiten.

SAP Solution Manager-Transaktionscodes

Transaktionscode	Beschreibung
ALRTINBOX	Zeigt den Warnungs-Posteingang an.
SOAMANGER	Öffnet und aktiviert den Webservice *Sap_Solman_Alert_Inbox*.
SRT_UTIL	Zeigt die SOA-Manager-Protokolle an.
SOLMAN_WORKCENTER	Öffnet die Oberfläche des SAP Solution Manager in einem Browser.
SM59	Zeigt die gesamte Ausgabeschnittstelle an.
SE38	Führt den ABAP-Code (Advanced Business Application Programming) aus. (Der entsprechende ServiceNow-Code ist *ZTEST_SNOW_CONNECTOR*.)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SAP Solution Manager-Transaktionscodes (Fortsetzung)

Transaktionscode	Beschreibung
MAI_TOOLS	Zeigt das Warnungstool an.
SE16	Zeigt die Schnittstellen-Debugging-Tabelle (ZSNOW) an.

Event-Erfassung von SCOM konfigurieren

Warnungen vom Microsoft System Center Operations Manager (SCOM) werden mit der SCOM-Connector-Instanz erfasst.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die SCOM-Connector-Instanz muss konfiguriert werden, bevor Warnungen und Rohdaten Metrikdaten vom SCOM-Server empfangen werden. Sie können die Erfassung von SCOM-Warnungen auf die Warnungen beschränken, die zu der von Ihnen angegebenen SCOM-Gruppe gehören.

Prozedur

1. Konfigurieren Sie die SCOM-Connector-Instanz.
2. Konfigurieren Sie die Connector-Instanz von Microsoft System Center Operations Manager (SCOM), um Warnungen und Metrikrohdaten vom SCOM-Server zu empfangen.
3. Beschränken Sie gesammelte SCOM-Warnungen auf bestimmte SCOM-Gruppen.

SCOM-Connector-Instanz konfigurieren

Konfigurieren Sie die Connector-Instanz des Microsoft System Center Operations Managers (SCOM), um Warnungen und Metrikdaten-Rohdaten vom SCOM-Server zu empfangen.

Vorbereitungen

Um **die Metriksammlung**zu aktivieren, stellen Sie sicher, dass MID-Server, das Metriken abruft, mit der Erweiterung Metrikdaten konfiguriert ist und dass sich die Erweiterung im Modus „ **Gestartet“** befindet. Weitere Informationen finden Sie unter Konfigurieren Sie die Erweiterung Metrikdaten manuell.

Windows Die Authentifizierung wird vom Connector für den Zugriff auf die SCOM-Datenbank (OperationsManagerDW) verwendet. Wenn daher **Metrikensammlung** ausgewählt ist und die Option **Datenbankanmeldung mit Windows-Authentifizierung** ausgewählt ist, stellen Sie sicher, dass der Service MID-Server mit einem Benutzer ausgeführt wird, der Lesezugriff auf die SCOM-Datenbank hat. Stellen Sie sicher, dass die richtigen Anmeldeinformationen verwendet werden:

1. Klicken Sie in den lokalen Services auf den Service MID-Server, und halten Sie ihn, (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie**Eigenschaften**aus.
2. Stellen Sie auf der Registerkarte**Anmelden**sicher, dass**Dieser Account**ausgewählt ist. Geben Sie die Details des Domänenbenutzers Windows ein, der über Lesezugriff auf die SCOM-Datenbank verfügt.

Bevor Sie mit dem Verfahren zur Konfiguration des Connectors beginnen, stellen Sie Folgendes sicher:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- MID-Server wird mit einem Anwender ausgeführt, der über lokale Administratorberechtigungen verfügt, damit MID-Server PowerShell ausführen kann.
- Der Benutzer MID-Server hat Lesezugriff auf die SCOM-API.
- MID-Server befindet sich in derselben Domäne wie der SCOM-Server.
- Der MID-Server nutzt dieselbe Zeitzone wie der SCOM-Server.
- MID-Server wird unter Windows ausgeführt.
- MID-Server verfügt über .NET Framework Version 3.5.

Wenn **Bidirektional** ausgewählt ist, stellen Sie Folgendes sicher:

- PowerShell Version 3.0 ist unter Windows installiert.
- MID-Server wird mit einem Anwender ausgeführt, der über lokale Administratorberechtigungen verfügt, um die Ausführung von PowerShell zu aktivieren.

So aktualisieren Sie einen vorhandenen SCOM-Connector:

1. Auf der Seite „Connector-Instanz – SCOM-Connector“ (**Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**), deaktivieren Sie das Kontrollkästchen **Metriken sammeln**.
2. Installieren Sie das Plugin *em-connectors* aus dem Store.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Um SCOM-Warnungen zu erhalten, können Sie die verteilbaren SCOM-Dateien von Ihrer SCOM-Anwendung abrufen. Fügen Sie die Dateien dem MID-Server hinzu und konfigurieren Sie dann eine SCOM-Connector-Instanz, um die Warnungen und Metrikdaten-Rohdaten zu erfassen.

Die Erfassung von Metrikdaten wird mithilfe von JavaScript ausgeführt; hier wird JDBC anstelle von PowerShell ausgeführt.

Sie können dieses Setup auch für die von SCOM verwaltete Instanz unter Azureverwenden.

Für diesen Connector ist der Protokollparameter *logPayloadForDebug* aktiviert. Dadurch werden Ereignis- und Metriknutzlasten aus dem Quellsystem protokolliert. Sobald das Debugging abgeschlossen ist, legen Sie diesen Parameter auf **false** fest, um eine Überlastung des Systems zu verhindern.

Unterstützte Versionen:

- 2007 – Version 6.1.7221.0
- 2012 – Version 7.1.10226.0
- 2016 – Version 7.2.117190 und 7.3.13261.0
- 2019 – Version 10.19.10050.0
- 2022 – Version 10.22.10118.0

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Laden Sie auf dem SCOM-Server die folgenden Dateien auf einen lokalen Computer herunter.

Version	SCOM-Pfad- und Bibliotheksnamen
SCOM 2012R2 oder SCOM 2012	`%ProgramFiles%\Microsoft System Center 2012 R2 or 2012\Operations Manager\Server\SDK Binaries` ◦ `Microsoft.EnterpriseManagement.Core.dll` ◦ `Microsoft.EnterpriseManagement.OperationsManager.dll` ◦ `Microsoft.EnterpriseManagement.Runtime.dll`
SCOM 2007	`%ProgramFiles%\System Center Operations Manager 2007\SDK Binaries` ◦ `Microsoft.EnterpriseManagement.OperationsManager.Common.dll` ◦ `Microsoft.EnterpriseManagement.OperationsManager.dll` **Hinweis:** Fügen Sie nicht 2007 an die Datei `Microsoft.EnterpriseManagement.OperationsManager.Common.dll` an.
SCOM 2016	`%ProgramFiles%\Microsoft System Center 2016\Operations Manager\Server\SDK Binaries` ◦ `Microsoft.EnterpriseManagement.Core.dll` ◦ `Microsoft.EnterpriseManagement.OperationsManager.dll` ◦ `Microsoft.EnterpriseManagement.Runtime.dll` **Hinweis:** MID-Server muss mit .NET 4.6 oder höher installiert werden.
SCOM 2019	`%ProgramFiles%\Microsoft System Center 2019\Operations Manager\Server\SDK Binaries` ◦ `Microsoft.EnterpriseManagement.Core.dll` ◦ `Microsoft.EnterpriseManagement.OperationsManager.dll` ◦ `Microsoft.EnterpriseManagement.Runtime.dll`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Version	SCOM-Pfad- und Bibliotheksnamen
	Hinweis: MID-Server muss mit .NET 4.6 oder höher installiert werden.
SCOM 2022	◦ `Microsoft.EnterpriseManagement.Core.dll` ◦ `Microsoft.EnterpriseManagement.OperationsManager.dll` ◦ `Microsoft.EnterpriseManagement.Runtime.dll` **Hinweis:** MID-Server muss mit .NET 4.6 oder höher installiert werden.

Hinweis: Es kann keine Verbindung mit SCOM 2012/SCOM 2016/SCOM 2019/ SCOM 2022 und SCOM 2007 aus demselben MID-Serverhergestellt werden. Um in Ihrer Instanz sowohl mit SCOM 2012/SCOM 2016/SCOM 2019/SCOM 2022 (alle) als auch mit SCOM 2007 zu arbeiten, gehen Sie vor dem Hochladen von Dateien in Ihre Instanz wie folgt vor:

a. Fügen Sie .2012 an das Ende der Datei `Microsoft.EnterpriseManagement.OperationsManager.dll` an, sodass `Microsoft.EnterpriseManagement.OperationsManager.dll.2012`wird. Führen Sie dies für 2012/2016/2019/2022 durch.

b. Hängen Sie .2007 an das Ende der `Microsoft.EnterpriseManagement.OperationsManager.dll`– Datei an, die sich im Pfad 2007 befindet.

Die Verwendung dieser geänderten Dateinamen ermöglicht es MID-Server, die entsprechende DLL-Datei zu laden, wenn beide SCOM-Versionen bereitgestellt werden. Fügen Sie nicht 2007 an die Datei `Microsoft.EnterpriseManagement.OperationsManager.Common.dll` an (für SCOM 2007).

Sie können jederzeit Connectors für SCOM 2007, SCOM 2012/2016 oder SCOM2019 definieren. Da SCOM 2012 und SCOM 2016 dieselben Bibliotheksdateien verwenden, können sie gleichzeitig arbeiten. Da allerdings von SCOM 2019 die verschiedenen SCOM-DLL-Dateien verwendet werden, können Sie SCOM 2012, 2016 und 2019 nicht zusammen konfigurieren. Jeder SCOM-Connector kann die Datenbank eines anderen Connectors für Metrikunterstützung verwenden.

2. Navigieren zu **MID-Server** > **JAR-Dateien**.
3. Wählen Sie **Neu** aus, und fügen Sie für jede der vom SCOM-Server heruntergeladenen DLL-Dateien einen separaten Datensatz für die SCOM-Version hinzu.

a. Geben Sie im Feld **Name** die SCOM-Version und einen Bezeichner an, um den Namen eindeutig zu machen, z. B. `2012 1`.
Wenn Sie SCOM 2016 verwenden, geben Sie 2012 als Version an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Wählen Sie das Büroklammer-Symbol im Formularheader, und hängen Sie dann eine der entsprechenden heruntergeladenen DLL-Dateien an.

c. Wählen Sie **Absenden**.

4. Wiederholen Sie Schritt 3, und erstellen Sie für jede der verbleibenden DLL-Dateien einen separaten Datensatz.
   Stellen Sie sicher, dass Sie nach der SCOM-Version für jede angehängte Datei einen eindeutigen Bezeichner haben, z. B. `2012 2`.
5. Navigieren zu **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
6. Klicken Sie auf **Neu**, und erstellen Sie eine neue Connector-Instanz.
   Weitere Informationen zu den auf der Seite angezeigten Connector-Instanzfeldern finden Sie unter Formular der SCOM-Connector-Instanz.
7. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
8. Im Abschnitt Connector-Instanzwerte können Sie die Werte der obligatorischen SCOM-Parameter bearbeiten.

a. **login_with_windows_authentication** Standardwert: **false**.
   Auf **true** festlegen, um die SCOM-Event-Erfassung und den bidirektionalen Austausch von Event-Werten für die Windows-Authentifizierung zu aktivieren.

   Wenn Sie diesen Wert aufrufen, gehen Sie für MID-Serverwie folgt vor:

   i. Navigieren Sie zur Liste der lokalen Services, wählen Sie den Service MID-Server aus, und halten Sie ihn, (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie**Eigenschaften**aus.

   ii. Stellen Sie auf der Registerkarte **Anmelden** sicher, dass **Dieses Konto** mit den Details des Benutzers in der Windows-Domäne ausgewählt ist, der Lesezugriff auf die SCOM-Datenbank hat.

b. **metric_chunk_size**: Standardwert: 50.000.

c. **scom_date_format**: Standardformat: M/t/jjjj/ h:mm:ss a
   Wenn Sie ein Event erhalten, dessen Datum in einem anderen Format vorliegt, ändern Sie diesen Wert so, dass es dem Format des eingehenden Events entspricht. Andernfalls wird das Event nicht ordnungsgemäß verarbeitet.

   Beispiel: Wenn ein Event am 27. Juni 2019 um 11:25 Uhr mit dem aufgelisteten Datum *`2019/06/27/ 11:25:00 a`* ankommt, ändern Sie den Wert **scom_date_format** in *`yyyy/ M/d/ h:mm:ss a`*, damit es dem Format des empfangenen Events entspricht.

   In **scom_date_format** steht `a` für morgens und `p` für nachmittags.

d. **scom_initial_sync_in_days**: Standardwert: 7.

e. **scom_version**: Die Angabe der SCOM-Version ist obligatorisch.
   Wählen Sie aus 2022, 2019, 2016, 2012 oder 2007 aus.

f. **stop_isMonitorAlert_bidirektional**: Boolesch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setzen Sie den Wert auf **„true“**, um nur bidirektionale SCOM-Überwachungswarnungen zu stoppen. Durch das Beenden von SCOM-Überwachungswarnungen können Sie Fehlalarme in der SCOM-Konsole beim Versuch, die Warnungen zu aktualisieren, vermeiden. Wenn sie auf **false**festgelegt ist, werden SCOM-Überwachungswarnungen für alle Arten von SCOM-Warnungen weiterhin bidirektional ausgeführt.

Standardwert = false.

9. Drücken und halten Sie den Formularheader (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Speichern**.
10. Starten Sie den Service MID-Server neu, um die Dateien zu kopieren.
11. Wählen Sie **Connector testen** aus, um die Verbindung zwischen MID-Server und dem Connector zu überprüfen.
    Wenn der Test fehlschlägt, beheben Sie das Problem, indem Sie die Anweisungen der Fehlermeldung befolgen, und führen Sie dann einen weiteren Test aus.

    Hinweis: Verwenden Sie ein Netzwerktool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität von MID-Server zu SCOM zu überprüfen.

12. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und wählen dann **Aktualisieren** aus.

    Hinweis:

    Die Standardbindungsregeln, die SCOM als externe Quelle enthalten und für IT-Warnungen und Metrikdaten-Rohdaten gelten, sind die folgenden SCOM Management Packs:

    - Alle BS-Management Packs
    - MS SQL-Server
    - IIS

Example:
Wenn bidirektional konfiguriert ist, ist der bidirektionaler Austausch von Werten mit der externen Event-Quelle möglich.
Diese Szenarien beschreiben die bidirektionale Standardfunktionalität für SCOM-Connectors:

- Wenn eine Warnung in SCOM gelöst wird, wird sie in ServiceNow automatisch geschlossen. Sie wird jedoch unabhängig von der bidirektionalen Funktion aktualisiert, da während jedes Erfassungszyklus alle Warnungsänderungen aktualisiert werden.
- Wenn eine Warnung in ServiceNow manuell geschlossen wird, wird sie in SCOM automatisch geschlossen. Wenn der Warnungsstatus in **Erneut öffnen** geändert wird, wird SCOM auch aktualisiert.
- Wenn ein Incident erstellt und einer Warnung in ServiceNow zugeordnet wird, erhält SCOM die Incident-Nummer als Ticket-ID. Der Status des Incidents ist jedoch in SCOM nicht verfügbar. Daher wird bei der Lösung des Incidents in ServiceNow SCOM nicht aktualisiert, da die Incident-Nummer gleich bleibt. Wenn die Warnung einem neuen Incident zugeordnet ist, wird die neue Incident-Nummer in SCOM aktualisiert.

Erfasste SCOM-Warnungen auf bestimmte SCOM-Gruppen beschränken

Sie können die Erfassung von SCOM-Warnungen auf die Warnungen beschränken, die zu der von Ihnen angegebenen SCOM-Gruppe gehören.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur
1. Verwenden Sie den SCOM Authoring-Arbeitsbereich und die Betriebskonsole, um eine SCOM-Gruppe zu definieren und sicherzustellen, dass die Gruppe die erforderlichen Computer oder Instanzen enthält.
   Weitere Informationen zu SCOM-Gruppen finden Sie in der SCOM-Dokumentation.
2. Erstellen Sie eine Rolle mit dem Umfang der SCOM-Gruppe.
3. Fügen Sie dem SCOM-Benutzer die neue Rolle hinzu.
4. Weisen Sie die Rolle dem Benutzer zu, der in den Anmeldeinformationen für die SCOM-Connector-Instanz definiert ist.
5. Entfernen Sie alle anderen Rollen vom Benutzer.

Ergebnisse
Nur Warnungen aus der angegebenen SCOM-Gruppe kommen bei der Instanz an.

SCOM-Metrikereignisregeln

Im Basissystem sind Metrikereignisregeln des Microsoft System Center Operations Manager (SCOM) enthalten. SCOM-Metrikereignisregeln binden Ereignismetriken an Configuration Items (CIs).

Wenn die Metriken eines Ereignisses den Ereignisfilterbedingungen entsprechen, werden die Metriken an das angegebene CI gebunden. Die folgenden Ereignisregeln sind im Lieferumfang des Basissystems enthalten:

Metrikereignis-Regeln des Basissystems

Regelname	CI-Typ
SCOM-Metriken – Windows Server	cmdb_ci_win_server
SCOM-Metriken – IIS-Webserver	cmdb_ci_microsoft_iis_web_server
SCOM-Metriken – SQL Server Reporting Services	cmdb_ci_db_mssql_reporting
SCOM-Metriken – MS SQL-Datenbank	cmdb_ci_db_mssql_database
SCOM-Metriken: MSFT SQL-Instanz	cmdb_ci_db_mssql_instance

Sie können eine anwenderdefinierte Ereignisregel erstellen, um Metriken an andere CI-Typen zu binden. Details finden Sie unter Event-Regel erstellen oder bearbeiten.

Wenn der Ereignisregelfilter nicht übereinstimmt, wird die Standardregel *SCOM Metrics – Default* (CI-Typ = *cmdb_ci_hardware*) aufgerufen. Die Reihenfolgenummer der Standardereignisregel muss höher sein als die Reihenfolgenummer aller SCOM-Ereignisregeln (sowohl der im Basissystem enthaltenen als auch der anwenderdefinierten Regeln), damit alle anderen Regeln vor dem Aufrufen der Standardregel auf Übereinstimmung überprüft werden. Einzelheiten zu Ereignisregeln finden Sie unter Event-Regeln.

Event-Erfassung vom SolarWinds-Monitor konfigurieren

Konfigurieren Sie die SolarWinds-Monitor-Connector-Instanz für den Empfang von Events vom SolarWinds-Monitor.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Unterstützte Versionen:

- SAM 6.2.1
- NPM 2020.2

Hinweis: Die SolarWinds-Monitor-Connector-Instanz kann Events importieren aus:

- Network Performance Monitor (NPM)
- SolarWinds-Service- und Anwendungsüberwachung (SAM)

Die SolarWinds-Connector-Instanz erfordert Anmeldeinformationen, mit denen die Instanz auf SolarWinds-Monitorkonten zugreifen kann. Sie können vorhandene Anmeldeinformationen verwenden oder neue erstellen. Der angegebene Anwender muss Zugriff auf die SolarWinds-API haben, um Ereignisse vom SolarWinds-Connector zu erhalten.

Erforderliche Rolle: evt_mgmt_admin und evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Für diesen Connector sind die Protokollparameter *debug* und *logPayloadForDebug* aktiviert. Mithilfe des Parameters *debug* werden Debug-Meldungen protokolliert, z. B. an das Quellsystem gerichtete Aufrufe zum Abrufen von Ereignissen. Mithilfe des Parameters *logPayloadForDebug* werden Ereignis- und Metriknutzlasten aus dem Quellsystem protokolliert. Sobald das Debugging abgeschlossen ist, legen Sie diesen Parameter auf **false** fest, um eine Überlastung des Systems zu verhindern.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen für den SolarWinds-Monitor-Connector ein.
Beschreibung	Geben Sie eine Beschreibung für die Verwendung der Instanz der SolarWinds-Monitor-Ereigniserfassung ein.
Anschlussdefinition	Wählen Sie **Solarwinds_v2**aus.
Host-IP	Geben Sie die IP-Adresse des SolarWinds-Monitors an.
Anmeldeinformationen	Wählen Sie die Anmeldeinformationen mit Standardauthentifizierung aus, die Sie für diesen Connector erstellt haben. Weitere Informationen finden Sie unter SolarWinds-Monitoranmeldeinformationen erstellen.
Zeit der letzten Ausführung der Event-Erfassung	Der letzte Wert der Ausführungszeit des Scheduled Job. Dieses Feld wird automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Der letzte Event-Erfassungsstatus. Dieses Feld wird automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen vom SolarWinds-Monitor-Server sucht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Letzte Fehlermeldung	Die letzte vom Connector empfangene Fehlermeldung wird automatisch aktualisiert.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
5. Geben Sie im Abschnitt Connector-Instanzwerte diese Felder an:

Feld	Wert
initial_sync_in_days	Geben Sie an, wie viele Tage der erste Abruf zum Abrufen von Events enthalten muss. Der Standardwert lautet 7 Tage.
nodes_custom_properties	Geben Sie die SolarWind-Monitor-Eigenschaftsnamen, die dem entsprechenden Knoten zugeordnet sind, an. Diese Informationen werden dem Feld **Zusätzliche Informationen** des Events im JSON-Format hinzugefügt. Bei den benutzerdefinierten Eigenschaften des SolarWinds-Monitors handelt es sich um benutzerdefinierte Felder, z. B. Land, Gebäude oder Seriennummer, die Sie überwachten Netzwerkobjekten zuordnen können. Trennen Sie mehrere Einträge durch ein Komma.
port	Geben Sie den Wert des Ports an. Der Standardwert lautet 17778.

6. Wahlweise: Der Name des MID Servers.
   Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet. Geben Sie im Abschnitt MID Server für Connectors einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden. Die Berechtigungen, die für das Benutzerkonto erforderlich sind, das für den MID Server zum Erfassen von Events vom SolarWinds-Monitor verwendet wird, sind die von evt_mgmt_integration.
7. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem SolarWinds-Monitor-Connector zu überprüfen.
   Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum SolarWinds-Monitor-Connector zu überprüfen.

8. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv** und klicken dann auf **Aktualisieren**.

Zugehörige Informationen

Konfigurieren Sie einen Pull-Connector

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SolarWinds-Monitoranmeldeinformationen erstellen

Erstellen Sie Anmeldeinformationen, um auf den SolarWinds-Monitor zuzugreifen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung** aus.
4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie `SolarWinds-Authentifizierung` nennen.
Benutzername	Name zum Identifizieren des Benutzers.
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher wird der Berechtigungsnachweis in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: `100`

5. Klicken Sie auf **Absenden**.

Ergebnisse

Die Anmeldeinformationen für die Verwendung mit dem SolarWinds-Monitor-Connector werden erstellt.

Zugehörige Informationen

Anmelde- und Verbindungsinformationen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Erfassung von vCenter konfigurieren

Konfigurieren Sie die VMware vCenter Server-Connector-Instanz (vCenter oder vCenter_V2) für den Empfang von Ereignissen aus Ihrer VMware vSphere-Umgebung.

Vorbereitungen

Von diesem Connector erfasste Events sind Events, die der Event-Regel von vCenter ESX Servers entsprechen.
Unterstützte Version: 7.0.2.00500.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Ereignisregeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Zuordnung** anwenden Checkbox für Regeln auf „wahr“ gesetzt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie mehr Ereignisregeln oder Automatisierung mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Für diesen Connector sind die Protokollparameter *debug* und *logPayloadForDebug* aktiviert. Mithilfe des Parameters *debug* werden Debug-Meldungen protokolliert, z. B. an das Quellsystem gerichtete Aufrufe zum Abrufen von Ereignissen. Mithilfe des Parameters *logPayloadForDebug* werden Ereignis- und Metriknutzlasten aus dem Quellsystem protokolliert. Sobald das Debugging abgeschlossen ist, legen Sie diesen Parameter auf **false** fest, um eine Überlastung des Systems zu verhindern.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

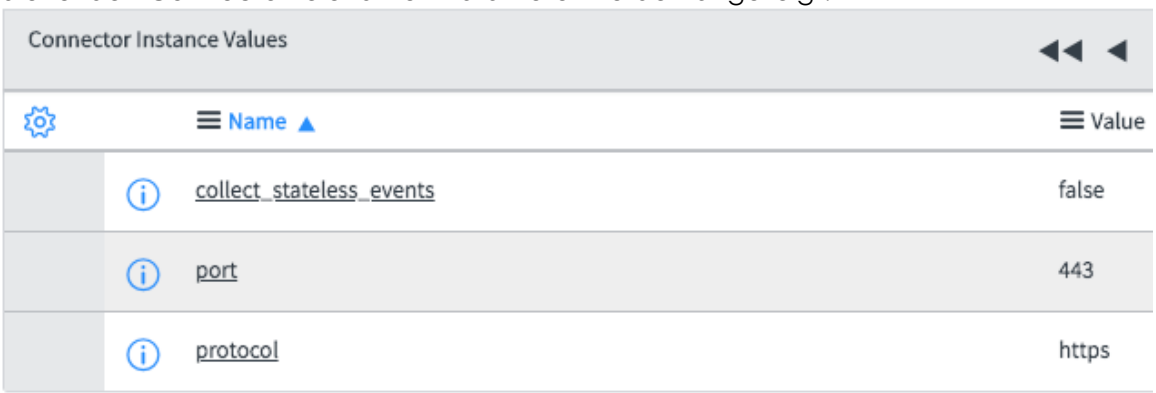
Formular Connector-Instanz

Feld	Beschreibung
Name	Beschreibender und einzigartiger Name für den vCenter-Connector.
Beschreibung	Beschreibung für die Verwendung der Instanz der vCenter-Ereigniserfassung.
Connector-Definition	Name der erforderlichen Connector-Definition. Wählen Sie **vCenter** oder **vCenter_V2** aus (vCenter_V2 befindet sich im Bereich der Ereignismanagement-Connectors).
Host-IP	IP-Adresse, unter der vCenter installiert ist.
Anmeldeinformationen	Berechtigung zum Herstellen einer Verbindung mit vCenter. Klicken Sie auf das Suchsymbol im Feld **Anmeldeinformationen**. Wählen Sie entweder die erforderlichen Anmeldeinformationen aus der Liste aus, oder klicken Sie auf **Neu** und erstellen Sie die erforderlichen Anmeldeinformationen im entsprechenden Formular. Wenn Sie die Anmeldeinformationen erstellen, speichern Sie sie unter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	einem eindeutigen und erkennbaren Namen, z. B. „vCenterCHCK“.
Zeit der letzten Ausführung der Event-Erfassung	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Event-Erfassungsstatus	Letzter Ausführungsstatus. Automatisch aktualisiert.
Zeitplan für Event-Erfassung (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Events von vCenter sucht. Der Standardwert ist 120 Sekunden.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.



5. Geben Sie im Abschnitt Connector-Instanzwerte die vCenter-Werte an.

Feld	Wert
collect_stateless_events	Events, die einen Status (statusbehaftet) haben, werden erfasst, wenn dieses Feld auf `false` (Standard) festgelegt ist. Diese Events sind vom Typ „AlarmStatusChangedEvent“ und „AlarmClearedEvent“. Wenn dieses Feld auf `true` festgelegt ist, werden auch Events anderer Typen erfasst.
port	Geben Sie den Wert des Ports an. Standardwert: `443`.
protocol	Geben Sie das Protokoll an. Standardwert: `https`.

6. Wahlweise: Geben Sie im Abschnitt „MID Servers für Anschlüsse“ einen aktiven und gültigen MID-Server an.
   Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

   Sie können mehrere MID Servers konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID-Server verwendet. Wenn dieser MID-Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Servers werden der Reihenfolge nach sortiert, in der ihre Details im Abschnitt „MID-Server für Anschlüsse“ eingegeben wurden.

7. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
8. Testen Sie die Verbindung zwischen dem MID-Server und dem vCenter-Connector.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf **Connector testen**.
Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

> **Hinweis:** Verwenden Sie ein Netzwerk-Tool wie Ping, um die Korrektheit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID-Server zum externen Überwachungs-Tool zu überprüfen.

b. Nach einem erfolgreichen Test aktivieren Sie das Kontrollkästchen **Aktiv**.

9. Klicken Sie auf **Aktualisieren**.

Event-Erfassung von vRealize konfigurieren

Konfigurieren Sie die Connector-Instanz von VMware vRealize Operations (vRealize oder vRealize_V2), um Ereignisse von den vRealize Operations Log- und Ereignismanagement-Servern zu empfangen. vRealize verwendet Standardauthentifizierung. vRealize_V2 verwendet eine tokenbasierte Authentifizierung.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Unterstützte Version: 8.10.0.

> **Hinweis:** Stellen Sie eine Verbindung zu vRealize her, indem Sie einen lokalen Konto mit mindestens der Berechtigung für schreibgeschützte vRealize Operations verwenden. Sie können vorhandene Anmeldeinformationen verwenden oder neue erstellen.

Warum und wann dieser Vorgang ausgeführt wird

Für diesen Connector sind die Protokollparameter *debug* und *logPayloadForDebug* aktiviert. Mithilfe des Parameters *debug* werden Debug-Meldungen protokolliert, z. B. an das Quellsystem gerichtete Aufrufe zum Abrufen von Ereignissen. Mithilfe des Parameters *logPayloadForDebug* werden Ereignis- und Metriknutzlasten aus dem Quellsystem protokolliert. Sobald das Debugging abgeschlossen ist, legen Sie diesen Parameter auf **false** fest, um eine Überlastung des Systems zu verhindern.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu** und erstellen Sie eine vRealize Operations-Connector-Instanz mit den folgenden Details:

Feld	Wert
Name	Geben Sie einen eindeutigen Namen für die vRealize Operations-Connector-Instanz an.
Host-IP	Geben Sie die IP-Adresse von vRealize Operations an.
Anmeldeinformationen	Wählen Sie die Anmeldeinformationen mit Standardauthentifizierung aus, die Sie für diesen Connector erstellt haben. Von vRealize_V2 wird eine tokenbasierte Authentifizierung verwendet, sofern der Benutzer das Token generieren kann. Weitere Informationen finden Sie unter vRealize-Anmeldeinformationen erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
Zeitplan (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von vRealize Operations sucht.
Beschreibung	Geben Sie eine Beschreibung für die Verwendung des vRealize Operations-Connectors ein.
Connector-Definition	Lieferant und Protokoll, die zum Sammeln von Events aus der externen Quelle verwendet werden. Wählen Sie **vRealize** oder **vRealize_V2** aus (vRealize_V2 befindet sich im Bereich der Ereignismanagement-Connectors).
Letzte Fehlermeldung	Die letzte Fehlermeldung wird automatisch aktualisiert.
Letzte Ausführungszeit	Die letzte Ausführungszeit wird automatisch aktualisiert.
Letzter Ausführungsstatus	Der letzte Ausführungsstatus wird automatisch aktualisiert.
MID Server (Abschnitt MID Server für Connectors)	Optional. Der Name des MID Servers. Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet. Geben Sie im Abschnitt MID Server für Connectors einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden.

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.
4. Geben Sie im Abschnitt Connector-Parameter die Werte der obligatorischen vRealize Operations-Parameter an.

   a. **port**: Standardwert = `443`

   b. **protocol**: Standardwert = `https`

   c. **days_from**:
   Anzahl der Tage, für die Daten bei der ersten Ausführung der Ereignissammlung abgerufen werden sollen. Standardwert = `14`. Die Option **days_from** ist nur verfügbar, wenn vRealize_V2 verwendet wird.

5. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem vRealize Operations-Connector zu überprüfen.
6. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zu vRealize zu überprüfen.

7. Nach einem erfolgreichen Test wählen Sie **Aktiv** aus und klicken dann auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Konfigurieren Sie einen Pull-Connector

vRealize-Anmeldeinformationen erstellen

Erstellen Sie Anmeldeinformationen, um auf vRealize zuzugreifen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie den Standardauthentifizierungstyp für Anmeldeinformationen, um eine Verbindung mit vRealize herzustellen.

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung** aus.
4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Beispiel: `NewvRealize`.
Benutzername	Name zum Identifizieren des Benutzers. ◦ Wenn der Benutzername in vRealize intern ist, verwenden Sie ihn unverändert. ◦ Wenn vRealize in Active Directory (AD) integriert ist, verwenden Sie das Format `DOMAIN\username@sourceauth`. Beispiel: `local\administrator@All vCenter Servers`.
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher wird der Berechtigungsnachweis in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: `100`

5. Klicken Sie auf **Absenden**.

Ergebnisse
Die Anmeldeinformationen für die Verwendung mit dem vRealize-Connector werden erstellt.

Zugehörige Informationen

Anmelde- und Verbindungsinformationen

Event-Erfassung vom Zabbix-Server konfigurieren

Konfigurieren Sie die Zabbix-Server-Connector-Instanz für den Empfang von Warnungen vom Zabbix-Server.

Vorbereitungen
Unterstützte Versionen: von 3.0.0 bis 7.0.0
Die Connector-Instanz des Zabbix-Servers erfordert Anmeldeinformationen, mit denen die Instanz auf Zabbix-Serverkonten zugreifen kann. Sie können vorhandene Anmeldeinformationen verwenden oder neue erstellen.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Für diesen Connector ist der Protokollparameter *`logPayloadForDebug`* aktiviert. Dadurch werden Ereignis- und Metriknutzlasten aus dem Quellsystem protokolliert. Sobald das Debugging abgeschlossen ist, legen Sie diesen Parameter auf **false** fest, um eine Überlastung des Systems zu verhindern.

Prozedur
1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

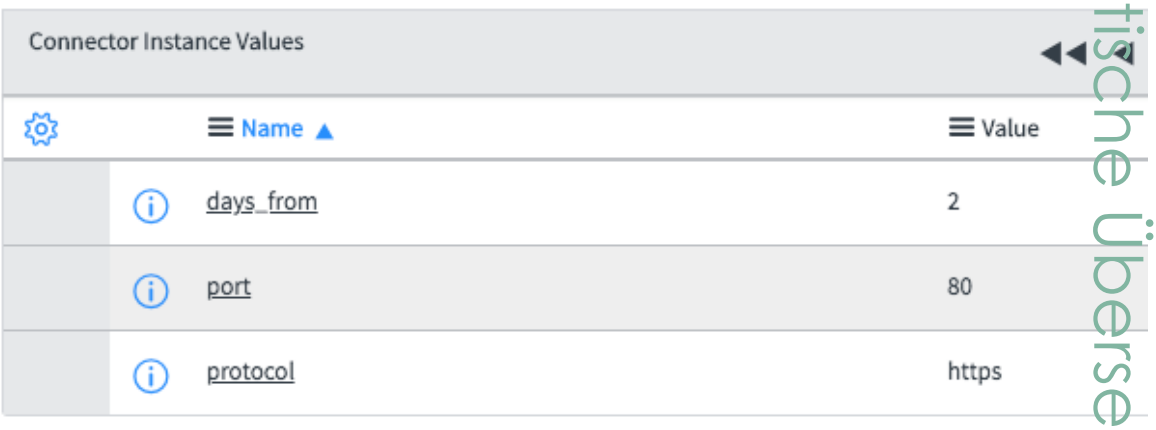
Feld	Beschreibung
Name	Beschreibender Name für den Connector
Host-IP	IP-Adresse für den Zabbix-Server.
Anmeldeinformationen	Wählen Sie die Anmeldeinformationen mit Standardauthentifizierung aus, die Sie für diesen Connector erstellt haben. Weitere Informationen finden Sie unter Erstellen Sie Zabbix-Server-Anmeldeinformationen.
Zeitplan (Sekunden)	Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen vom Zabbix-Server sucht.
Beschreibung	Beschreibung für die Verwendung der Instanz der Ereigniserfassung des Zabbix-Servers.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Connector-Definition	Name der erforderlichen Connector-Definition. Wählen Sie **Zabbix** aus.
Letzte Fehlermeldung	Letzte Fehlermeldung. Automatisch aktualisiert.
Letzte Ausführungszeit	Letzter Ausführungszeitwert. Automatisch aktualisiert.
Letzter Ausführungsstatus	Letzter Ausführungszeitstatus. Automatisch aktualisiert.
MID Server (Abschnitt MID Server für Connectors)	Optional. Der Name des MID Servers. Wenn kein MID Server angegeben ist, wird ein verfügbarer MID Server mit einem übereinstimmenden IP-Bereich verwendet. Geben Sie im Abschnitt MID Server für Connectors einen aktiven und gültigen MID Server an. Sie können mehrere MID Server konfigurieren. Wenn der erste ausgefallen ist, wird der nächste MID Server verwendet. Wenn dieser MID Server nicht verfügbar ist, wird der nächste ausgewählt usw. MID Server werden nach der Reihenfolge sortiert, in der ihre Details im Abschnitt „MID Server für Connectors“ eingegeben wurden.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Die Connector-Instanzwerte werden dem Formular hinzugefügt, und die für den Connector relevanten Parameter werden angezeigt.



5. Überprüfen und ändern Sie die Werte nach Bedarf.
   Im Abschnitt Connector-Instanzwerte erscheinen die Standardwerte der Connector-Instanz.

Felder im der Abschnitt Connector-Instanzwerte

Feld	Beschreibung
days_from	Anzahl der Tage, für die Events im ersten Erfassungszyklus erfasst werden müssen. Standardwert: `2` **Hinweis:** Die maximale Anzahl vergangener Events, die erfasst werden können, beträgt 3.000. Bei der ersten Ausführung dieses Connectors wird die Anzahl der vergangenen Ereignisse in der Vergangenheit ab dem aktuellen Datum gezählt.
port	Port-Nummer. Standardwert: `80`.
protocol	Protokolltyp. Standardwert: `https`.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
7. Klicken Sie auf **Connector testen**, um die Verbindung zwischen dem MID Server und dem Connector zu überprüfen.
8. Wenn der Test fehlschlägt, befolgen Sie die Anweisungen der Fehlermeldung, um das Problem zu beheben, und führen Sie dann einen weiteren Test aus.

   Hinweis: Verwenden Sie ein Netzwerk-Tool wie Ping, um die Richtigkeit der Anmeldeinformationen und die Netzwerkkonnektivität vom MID Server zum Zabbix-Server zu überprüfen.

9. Nach einem erfolgreichen Test wählen Sie **Aktiv** aus und klicken dann auf **Aktualisieren**.

Erstellen Sie Zabbix-Server-Anmeldeinformationen

Erstellen Sie Anmeldeinformationen, um auf den Zabbix-Server zuzugreifen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung** aus.
4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein. Zum Beispiel könnten Sie sie `Zabbix-Authentifizierung` nennen.
Benutzername	Name zum Identifizieren des Benutzers.
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher wird der Berechtigungsnachweis in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: `100`

5. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Die Anmeldeinformationen zur Standardauthentifizierung für die Verwendung mit dem Zabbix-Server-Connector werden erstellt.

Zugehörige Informationen

Anmelde- und Verbindungsinformationen

Konfigurieren Sie einen Push-Connector

Sie können Listener und Connectors so konfigurieren, dass Event-Informationen an die Instanz oder den MID-Server übertragen werden.

Ereignismanagement empfängt externe Events über einen Push-Connector oder ein Skript. Wenn Sie ein Skript zum Erfassen von Events verwenden, ist keine Konfiguration erforderlich. Alle anderen Methoden zum Erfassen von Events müssen konfiguriert werden.

Nach der Konfiguration der Event-Erfassung kann Ereignismanagement Events erfassen, die direkt an die Instanz oder über den MID-Server, den SNMP-Trap oder per E-Mail gesendet werden.

Hinweis: Die Integration mit Push-Connectors ist nur durch die Installation des Plugin „Ereignismanagement Connector“ aus dem ServiceNow Store möglich.

Standard-Event-Formular

Ein Standard-Event-Formular muss von allen Events verwendet werden, unabhängig davon, wie sie bei der Instanz ankommen. Weitere Informationen finden Sie unter Event-Feldformat für die Event-Erfassung.

Event-Erfassung

Ereignismanagement ermöglicht die Kommunikation und den Transport von Daten zwischen externen Anwendungen, Datenquellen, Services und der Now Platform-Instanz.

Event-Erfassungsmodi	Beschreibung
Vom Basissystem bereitgestellt	Mit der Anwendung Ereignismanagement bereitgestellte Listener und Connectors: • AWS CloudWatch, siehe AWS-Plattform als Datenquelle integrieren • Azure-Event-Nachrichten, siehe Azure Monitor als authentifizierte Datenquelle integrieren • BMC TrueSight-Events, siehe Ereignissammlung von BMC TrueSight und BMC TrueSight_v2 • Datadog-Events, siehe Integrieren Sie Plattform-Ereignisse für Datadog . • Dynatrace-Events, siehe Integrieren Sie Plattform-Ereignisse für Dynatrace . • Google Cloud Platform (GCP)-Events, siehe Google Cloud Platform (GCP)-Events integrieren • New Relic-Events, siehe Events der New Relic-Plattform integrieren • Allgemeine Event-Erfassung über den MID-Server • Allgemeine Event-Erfassung über die Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Erfassungsmodi	Beschreibung
	Wenn Event-Nachrichten in XML empfangen werden, können Sie ein Skript verwenden, das auf dem im Basissystem bereitgestellten XML-Transformationsskript basiert.
Über MID WebService	Sie können den MID-WebService-Ereignissammler so konfigurieren, dass Ereignisnachrichten per Push an MID-Servergesendet werden. Weitere Informationen finden Sie unter Ereignisse werden mithilfe der Webservice-API an MID-Server übertragen.
Eigenen Inhalt erstellen	Sie können Ihren eigenen Listener konfigurieren: • Über die MID-Webserver-API. Weitere Informationen finden Sie unter Ereignisse mithilfe einer Webservice-API an die Instanz weiterleiten. • Über benutzerdefinierte Transformation. Weitere Informationen finden Sie unter Event-Erfassung aus benutzerdefinierten Nutzlasten.
Über SNMP.	Mit der Anwendung Ereignismanagement bereitgestellte SNMP-Listener: Generisches SNMPv2. Weitere Informationen finden Sie unter Konfigurieren Sie die Event-Erfassung für SNMP-Traps. Darüber hinaus können Sie Ihren eigenen benutzerdefinierten Listener erstellen. Weitere Informationen finden Sie unter Integrieren Sie mit Push-Connectors.
Per E-Mail	E-Mail-Listener. Weitere Informationen finden Sie unter Event-Erfassung per E-Mail konfigurieren.

Zugehörige Informationen

Formular der Push-Connector-Instanz

Konfigurieren Sie die ServiceNow Cloud Observability Ereignis-Sammlung

Integrieren Sie ServiceNow Cloud Observability mit Ereignismanagement, indem Sie der Plattform ServiceNow Cloud Observability einen Standard-Webhook hinzufügen. Laden Sie das Ereignismanagement Connector-Plugin aus dem ServiceNow Store herunter, damit Sie es in ServiceNow Cloud Observabilityintegrieren können.

Vorbereitungen

- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Authentifizieren Sie ServiceNow Cloud Observability als Datenquelle, damit Ereignismanagement Ereignisse von ServiceNow Cloud Observabilitysammeln kann. Verwenden Sie in Ihrer Plattform ServiceNow Cloud Observability einen Standard-Webhook, um Ihre Instanz Now Platform als REST-Endpunkt festzulegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie ein CI.

   Hinweis: Discovery für Services ServiceNow Cloud Observability wird nicht unterstützt. Erstellen Sie ein CI manuell in einer Instanz ServiceNow (Tabelle „cmdb_ci_service_auto“), um die Bindung zu aktivieren.

   a. Navigieren zu **Alle** > **Konfiguration** > **Anwendungsservice**.

   b. Wählen Sie **Neu**.

   c. Geben Sie im Formular den Namen ein.
   Der Name muss der in der Plattform ServiceNow Cloud Observability angegebene Servicename sein.

   d. Legen Sie in der Liste „Betriebsstatus“ den Betriebsstatus auf **Funktionsfähig**fest.

   e. Wählen Sie **Weiter**.

   f. Wählen Sie **Fertig**.

2. Erstellen Sie in Ihrer Plattform ServiceNow Cloud Observability ein Benachrichtigungsziel.

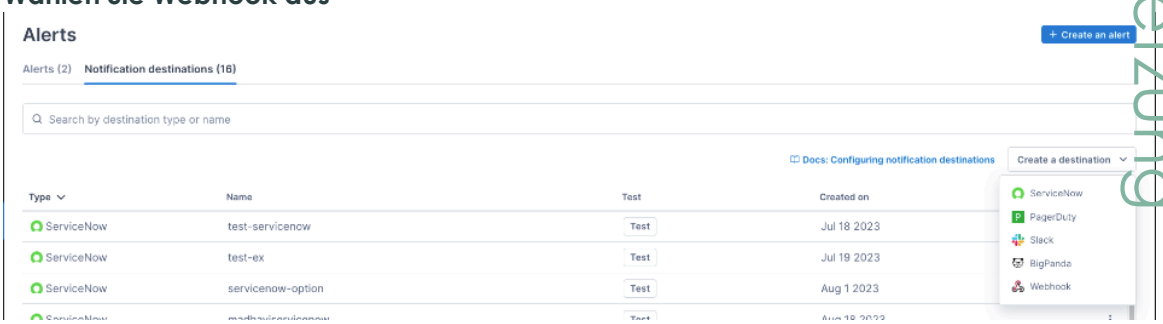
   a. Klicken Sie in der Navigationsleiste auf **Warnungen**.

   b. Wählen Sie die Registerkarte **Benachrichtigungsziele**.

   c. Wählen Sie **Ziel erstellen aus**.

   d. Wählen Sie **Webhook**aus.

   Wählen Sie Webhook aus

   e. Geben Sie im Feld Name einen Namen für den Webhookein.

   f. Geben Sie im Feld „URL“ die Webhook-URL an.
   Dies ist das Standardformat der URL zum Übertragen von Ereignissen von ServiceNow Cloud Observability an die Instanz Now Platform. Dieses Format verwenden:
   `https//`<username> :<password> @<instance-name> .service-now.com/api/sn_em_connector/em/inbound_event?source=lightstep

   g. Wählen Sie **Neuer Header**aus.

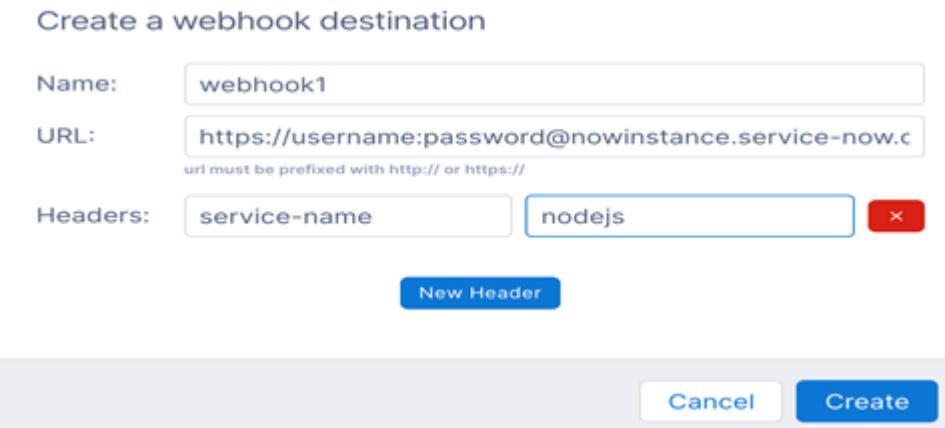
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

h. Geben Sie im Feld Header den **Servicenamen** ein, und definieren Sie den **Wert**.

Hinweis: In einer Instanz ServiceNow erfolgt die CI-Bindung nur, wenn der Headerwert **„service-name“** mit den Namensfeldern des von Ihnen in der**Tabelle cmdb_ci_service_auto**erstellten CI übereinstimmt.

Webhook erstellen



i. Klicken Sie auf **Erstellen**.

3. Konfigurieren Sie auf der Plattform ServiceNow Cloud Observability eine -Warnung.

a. Klicken Sie in der Navigationsleiste auf **Warnungen**.

b. Wählen Sie **Warnung erstellen aus,** und geben Sie einen Warnungsnamen ein.

c. Definieren Sie im Bereich „Warnmeldungskonfiguration“ den Schwellenwert.

d. Wählen Sie im Bereich Benachrichtigungsregeln in den Feldern Benachrichtigungen senden an die Option **Webhook** als Benachrichtigungsziel aus, und suchen Sie nach dem Zielnamen für den Webhook, den Sie in Schritt 2 erstellt haben.

e. Wählen Sie **Speichern**.
Der Standard-Schweregrad für Stream-basierte Warnungen ist **Kritisch**. Sie können den Standard im Bereich Push-Connector-Konfiguration einer Now Platform -Instanz ändern. Die gültigen Schweregradwerte sind:

- 1 - Kritisch
- 2 - Schwer
- 3 – Gering
- 4 – Warnung
- 5 - Info

MID-Server zur Event-Erfassung mithilfe eines Push-Vorgangs (Listener) konfigurieren

Der MID-Server unterstützt die Erfassung von Event-Nachrichten mithilfe des MID-Webservers, der Daten aus externen Quellen erfasst und in das für Event-Felder in der Event-Tabelle [em_event] erforderliche Format umwandelt (analysiert). Die transformierten Events werden dann an die Instanz übertragen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Dank der MID-Webservererweiterung können externe Clients Metrikdaten per Push an den MID-Server übertragen. Weitere Informationen finden Sie unter MID-Webservererweiterung konfigurieren. Verwenden Sie den MID WebService-Event-Sammler, um mit einer URL-Methode Event-Nachrichten an den MID-Server zu übertragen. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Konfigurieren Sie einen MID-Server entweder mit *EventManagement* oder *All* in der Liste der unterstützten Anwendungen.

Um die Unterbrechung von Services zu vermeiden, können Sie ein MID-Server-Failover-Cluster konfigurieren.

Prozedur
1. Navigieren zu **Alle** > **MID-Server** > **Server**.
2. Doppelklicken Sie auf den MID-Server, den Sie konfigurieren möchten, oder klicken Sie auf **Neu**, um einen neuen MID-Server zu erstellen.
3. Klicken Sie im Abschnitt **Unterstützte Anwendungen** auf **Bearbeiten**.
   a. Klicken Sie auf **Bearbeiten**.
   b. Wählen Sie im Slushbucket entweder **Event Management** oder **ALLE** aus, und klicken Sie auf die Schaltfläche **>** Hinzufügen.
   c. Klicken Sie auf **Speichern**.
4. Um sicherzustellen, dass MID-Server validiert ist, wählen Sie unter „Zugehörige Links“ die Option **Validieren**aus.
   Weitere Informationen finden Sie unter MID-Server validieren .
5. Klicken Sie auf **Aktualisieren**.

Nächste Maßnahme
Konfigurieren Sie den MID WebService-Event-Sammler, um mit einer URL-Methode Event-Nachrichten an den MID-Server zu übertragen. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Zugehörige Informationen

Schlüsselbasierte MID-Webserverauthentifizierung konfigurieren

MID-Webservererweiterung konfigurieren

MID-WebService-Event-Sammlerkontext konfigurieren

Ereignisse werden mithilfe der Webservice-API an MID-Server übertragen

Konfigurieren Sie den MID WebService-Eventsammler, damit eine URL-Methode Event-Nachrichten an den MID-Server übertragen kann.

Der MID WebService-Event-Sammler ermöglicht Ihnen standardmäßig das Herstellen einer Verbindung zu einem Event-Generator und das Senden von Event-Nachrichten über den MID-Server mithilfe einer URL im folgenden Format: `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/jsonv2`.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das JSON v2-Format ist mit dem Format identisch, das Clients zum Senden von Event-Nachrichten an die Instanz verwenden. Diese URL bietet eine gute Leistung.

Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Hinweis: Ereignismanagement akzeptiert Events in der Zeitzone des MID-Server, über den der Listener die Event-Nachricht gesendet hat. Wenn Sie eine andere Zeitzone benötigen, können Sie das Skript nach Bedarf konfigurieren, siehe Integrieren Sie mit Push-Connectors.

URL zum Verschieben von benutzerdefinierten Nutzlasten

Der MID-Server kann auch eine benutzerdefinierte Nutzlast im JSON-, XML- oder Nur-Text-Format empfangen. In diesem Fall transformiert der MID-Server die Event-Nachrichten mithilfe der von Ihnen angegebenen Skripteinbindung und sendet die Events dann an die Instanz. Die URL lautet in diesem Fall:

`http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform={Transform_script_name}` Für ein Beispiel für eine Skripteinbindung siehe die Standard-Skripteinbindung `TransformEvents_xmlSample`.

Ein Beispiel für die Umwandlung von JSON-formatierten Event-Nachrichten durch den MID WebService-Eventsammler finden Sie unter Ereignissammlung von BMC TrueSight und BMC TrueSight_v2.

Zum Senden von Events im allgemeinen JSON-Format können Sie die URL in folgendem Format verwenden:

```
http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform=TransformEvents_MidJsonGeneric
```

In diesem Fall transformiert die MID-Einbindung `TransformEvents_MidJsonGeneric`, die in der Basisinstanz bereitgestellt wird, die Event-Nachrichten in die Event-Felder. Alle Felder werden als Felder **Zusätzliche Informationen** dem generierten ServiceNow-Event hinzugefügt.

Hinweis: Die URL im Format `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/{transform_script_name}` wird ebenfalls unterstützt.

Die URL der REST API zum Überprüfen der Konnektivität lautet: `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/ping`.

Skripteinbindung zur Transformation erfasster Events

Verwenden Sie die erforderliche Skripteinbindung MID-Server, um erfasste Event-Nachrichten umzuwandeln (zu analysieren) und in das zugeordnete Event-Feld einzufügen. Der Name der Skripteinbindung MID-Server besteht aus einem Präfix und einem Suffix. Das Präfix ist der obligatorische Text `TransformEvents_` und das Suffix ist der Transformationsname in der URL, z. B. `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/xmlSample` . Der Name des zusammengesetzten Skripts lautet daher `TransformEvents_xmlSample`.

Sie müssen eine Skripteinbindung angeben, die die Event-Nachrichten in einer Textvariablen empfängt. Das Skript muss über eine `transform ()`-Funktion verfügen, die die Transformation durchführt und das Rückgabe-Array von Event-Objekten vorbereitet. Wenn das Ereignismanagement-Plugin aktiviert ist, erhalten Sie das `TransformEvents_xmlSample`-Beispielskript, das Events aus dem XML-Format umwandelt.

Hinweis: Event-Felder, die nicht mit Feldern in der Event-Tabelle identisch sind, werden im Feld **Zusätzliche Informationen** gespeichert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Nachrichtenheader

Geben Sie den entsprechenden Anforderungsheaderwert für das Feld **Inhaltstyp** entsprechend dem Format der Event-Nachricht an.

Header-Werte für den Content-Type anfordern

Nachrichtenformat	Content-Typenwert
JSON	Anwendung/JSON
XML	application/xml
text	text/plain

Authentifizierungs- und Datensicherheitsoptionen

Optionen für Authentifizierung und Datensicherheit:

- **Authentifizierungstyp**: Diese Option kann entweder auf `API-Schlüssel` oder auf `Standard` festgelegt werden.
- Mit **Sichere Verbindung** können Sie auswählen, ob eingehende und ausgehende Daten bei der Übertragung gesichert werden. Wenn Sie die Option für erweiterte Sicherheit auswählen, müssen Sie ein Zertifikat von einer bekannten Zertifizierungsstelle abrufen und dann den **Schlüsselspeicher-Zertifikat-Alias** und das **Schlüsselspeicher-Passwort** angeben.
- **Einheitlichen MID-Schlüsselspeicher verwenden**: Diese Option bietet Verschlüsselungsschutz und ermöglicht es Ihnen, ein benutzerdefiniertes Zertifikat im einheitlichen MID-Server-Schlüsselspeicher zu installieren. Einzelheiten hierzu finden Sie unter Anwenderdefinierte Zertifikate im einheitlichen Schlüsselspeicher des MID-Servers installieren .
- Benutzer müssen eine Skripteinbindung angeben, die JSON-, XML- oder Text-formatierte Event-Nachrichten in einer Textvariablen empfängt. Das Skript muss über eine transform ()-Funktion verfügen, die die Transformation durchführt und das Rückgabe-Array von Event-Objekten vorbereitet. Die Skripteinbindung `TransformEvents_xmlSample`, die Events aus dem XML-Format umwandelt, wird als Beispiel angegeben, wenn das Ereignismanagement-Plugin aktiviert ist.

Weitere Informationen zu Authentifizierung und Datensicherheit finden Sie unter MID-Webservererweiterung konfigurieren.

Zugehörige Informationen

Ereignisse mithilfe einer Webservice-API an die Instanz weiterleiten

Ereignisse mithilfe einer Webservice-API an die Instanz weiterleiten

Sie können eine Webservice-Schnittstelle mit ServiceNow verwenden, die auf dem JSON-Objekt als Dateneingabe- und -ausgabeformat aufbaut.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie diese Webservice-API, um Datensätze mit einem einzelnen Aufruf in die Event-Tabelle [em_event] einzufügen:

`https://<instancename>.service-now.com/api/global/em/jsonv2`

Hinweis: Business Rules in der Event-Tabelle werden nicht aufgerufen, wenn diese URL verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie einem Event keine zusätzlichen Felder hinzu, indem Sie der Event-Tabelle [em_event] ein benutzerdefiniertes Feld hinzufügen. Zusätzliche Felder sollten im Feld **Zusätzliche Informationen** [additional_info] des Events eingeschlossen werden. Weitere Informationen zum Einbinden zusätzlicher Felder in Events finden Sie unter Benutzerdefinierte Warnungsfelder.

Die URL im Format: `http://` <instancename> .service-now.com/em_event.do? JSONv2&sysparm_action=insertMultiple wird auch unterstützt, wenn Sie Business-Regeln aktivieren möchten. Die Leistung der ersten URL ist jedoch überlegen.

Um mit der URL zu arbeiten, die auf `= insertMultiple` endet, fügen Sie dem MID Server die folgenden Eigenschaften mit ihren entsprechenden Werten hinzu:

- „mid.probe.event.queue.compress“ – Wert: false
- „mid.probe.event.bulk_size“ – Wert: 100
- „mid.probe.event.endpoint.url“ – Wert: em_event.do? JSONv2%26sysparm_action=insertMultiple

Prozedur

1. Senden Sie die Anforderung mit diesen Headern:

Parameter	Typ	Beschreibung
Akzeptieren	Zeichenfolge	Der zulässige Typ für diese Nachricht. Der Standardwert ist `application/json`.
Content-Type	Zeichenfolge	Der Inhaltstyp für diese Nachricht. Der Standardwert ist `application/json`.
POST	Zeichenfolge	Der Anforderungstyp ist POST mit mindestens einem nachstehenden Datensatz.

2. Mindestens ein Event im JSON-Format kann als Nutzlast des Webservice-Aufrufs gesendet werden.
   Folgende Event-Felder müssen ausgefüllt werden:

Variable	Beschreibung
Quelle	Der Name des Event-Quelltyps. Beispielsweise SCOM oder SolarWinds.
event_class	Spezifische Instanz der *source*. Beispiel: `SCOM 2012 am 10.20.30.40`
node	Das **Knotenfeld** muss einen Bezeichner für den Host (Server/Switch/ Router usw.) enthalten, für den das Event ausgelöst wurde. Der Wert des **Knotenfelds** kann einer der folgenden Bezeichner des Hosts sein: ◦ Name ◦ FQDN ◦ IP ◦ Mac-Adresse Wenn in der CMDB vorhanden, wird dieser Wert auch verwendet, um das Event an das entsprechende ServiceNow-CI zu binden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Variable	Beschreibung
resource	Wenn sich das Event auf ein Gerät bezieht, z. B. Datenträger, CPU oder Netzwerkadapter, oder auf eine Anwendung oder einen Service, die bzw. der auf einem Host ausgeführt wird, muss der Name des Geräts oder der Anwendung in dieses Feld eingetragen werden. Zum Beispiel: `Disk C:\` oder `Nic 001` oder `Webanwendung Handel`.
metric_name	Name der Metrik, die die Warnung ausgelöst hat. Zum Beispiel: `Verwendeter Arbeitsspeicher` oder `Gesamte CPU-Auslastung`.
type	Der Typ des Events: Dieser Typ ähnelt möglicherweise dem Feld **metric_name**, wird jedoch für die allgemeine Gruppierung von Event-Typen verwendet.
message_key	Dieser Wert wird für die Deduplizierung von Events verwendet. Beispielsweise kann es zwei Events für dasselbe CI geben, wobei ein Event eine CPU von 50 % und das nächste Event eine CPU von 99 % hat. Wenn beide Events derselben ServiceNow-Warnung zugeordnet werden müssen, müssen sie denselben Nachrichtenschlüssel haben. Das Feld kann leer gelassen werden. In diesem Fall lautet der Feldwert standardmäßig `source+node+type+resource+metric_name` . Das Feld **message_key** darf nur ausgefüllt werden, wenn ein besserer Bezeichner als der Standardwert vorhanden ist.
severity	Der Schweregrad des Events. ServiceNow-Werte für den Schweregrad reichen von 1 – Kritisch bis 5 – OK, mit dem Schweregrad 0 – Löschen. Ursprüngliche Schweregradwerte sollten als Teil der zusätzlichen Informationen gesendet werden.
additional_info	Dieses Feld hat das JSON-Schlüssel-/Wert-Format und soll alle Informationen enthalten, die für den Anwender von Nutzen sein könnten. Es wird keinem vordefinierten ServiceNow-Event-Feld zugeordnet. Beispiele: IDs von Objekten in der Event-Quelle, Event-Priorität (wenn nicht gleich Schweregrad), Zuweisungsgruppeninformationen usw. Werte im Feld **Zusätzliche Informationen** eines Events, die nicht im JSON-Schlüssel-/Wert-Format vorliegen, werden auf das JSON-Format normalisiert, wenn das Event verarbeitet wird.
time_of_event	Zeit, zu der das Event am Event-Ursprung aufgetreten ist. Das Format lautet: jjjj-MM-tt HH:mm:ss. Die angegebene Zeit muss GMT entsprechen.
resolution_state	Optional – Um anzugeben, dass ein Event gelöst wurde oder nicht mehr auftritt, verwenden einige Event-Überwachungen den Schweregrad „löschen“, während andere Event-Überwachungen einen Wert für den Schweregrad „schließen“ verwenden. Dieses Feld wird für die Monitore verwendet, die Letzteres anbieten. Gültige Werte sind `Neu` und `Schließen`.

3. Zum Erstellen mehrerer Datensätze mit einem einzigen Aufruf lösen Sie den Event-Webservice mit der folgenden URL aus, wobei die Variable <instance name> durch den Namen der erforderlichen Instanz ersetzt wird:
   `https://<instancename>.service-now.com/api/global/em/jsonv2`

   Example
   Beispiel für die Nutzlast von zwei Events, die in einem Webservice-Aufruf gesendet werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
{
  "records": [
    {
      "source": "SCOM",
      "event_class": "SCOM 2012 on scom.server.com",
      "resource": "D:",
      "node": "name.of.node.com",
      "metric_name": "Percentage Logical Disk Free Space",
      "type": "Disk space",
      "severity": "4",
      "description": "The disk D: on computer V-W2K8-abc.abc.com is
 running out of disk space. The value that exceeded the threshold is
 38% free space.",
      "additional_info": {
        "scom-severity": "Medium",
        "metric-value": "38",
        "os_type": "Windows.Server.2008"
      }
    },
    {
      "source": "SCOM",
      "event_class": "SCOM 2012 on scom.server.com",
      "resource": "MSSQL-database-name",
      "node": "other.node.com",
      "metric_name": "DB Allocated Size (MB)",
      "type": "Database Storage",
      "severity": "3",
      "description": "High number of active connections for
 MSSQL-database-name running on name.of.node.com. Active connections
 exceed 5000.",
      "additional_info": {
        "scom-severity": "Medium",
        "metric-value": "38",
        "os_type": "Windows.Server.2008"
      }
    }
  ]
}
```

4. Zum Erstellen eines Datensatzes mit einem einzigen Aufruf lösen Sie den Event-Webservice mit der folgenden URL aus, wobei die Variable <instancename> durch den Namen der erforderlichen Instanz ersetzt wird:
   `http://<instancename>.service-now.com/api/global/em/jsonv2`

   Example
   Beispiel für die Nutzlast von einem Event, das in einem Webservice-Aufruf gesendet wird:

```
{
  "records": [
    {
      "source": "SCOM",
      "event_class": "SCOM 2007 on scom.server.com",
      "resource": "C:",
      "node": "name.of.node.com",
      "metric_name": "Percentage Logical Disk Free Space",
      "type": "Disk space",
      "severity": "4",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      "description": "The disk C: on computer V-W2K8-dfg.dfg.com is
 running out of disk space. The value that exceeded the threshold is
 41% free space.",
      "additional_info": {
        "scom-severity": "Medium",
        "metric-value": "38",
        "os_type": "Windows.Server.2008"
      }
    }
  ]
}
```

Zugehörige Informationen

Ereignisse werden mithilfe der Webservice-API an MID-Server übertragen

MID-WebService-Event-Sammlerkontext konfigurieren

Konfigurieren Sie den MID-WebService-Event-Sammlerkontext, damit eine URL-Methode Event-Nachrichten von einer externen Quelle an den MID-Server übertragen kann.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Das Standardformat der URL zum Versenden von Eventnachrichten aus einer externen Quelle an den MID-Server ist `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/jsonv2`. Diese URL bietet eine gute Leistung.

Aus einer externen Quelle lautet das URL-Format für Push-Event-Nachrichten, die nicht im jsonv2-Format vorliegen: `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform={Name_of_Transform_Script}`, wobei die Variable *`{Name_of_Transform_Script}`* der vollständige Name des Skripts ist und immer mit dem Text: `TransformEvents_` beginnt.

Nehmen Sie beispielsweise die folgenden Werte an:

- {MID_Server_IP}: 10.118.69.27
- {MID_Web_Server_Port}: 8097
- Name des Transformationsskripts: EventsToProcess

Die zu verwendende URL lautet daher: `http://10.118.69.27:8097/api/mid/em/inbound_event/TransformEvents_EventsToProcess`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die URL im Format `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/{transform_script_name}` wird ebenfalls unterstützt.
- Das Datumsformat für Events ist jjjj-Md h:mm:ss.

  Wenn Sie ein Event erhalten, dessen Datum in einem anderen Format vorliegt, müssen Sie ein `{transform_script_name}` verwenden, das für das Datumsformat des eingehenden Events geeignet ist. Andernfalls wird das Event nicht ordnungsgemäß verarbeitet.

  Beispiel: Wenn ein Event am 27. Juni 2019 um 11:25 Uhr mit dem aufgelisteten Datum *2019/06/27/ 11:25:00 a* ankommt, verwenden Sie ein `{transform_script_name}` mit dem Datumsformat *yyyy/MM/dd/ HH:mm:ss a*, damit es dem Format des empfangenen Events entspricht.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **MID-WebService-Ereignis-Listener**.
2. Klicken Sie in der Liste MID WebService Event-Sammlerkontexte auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular für MID WebService-Event-Sammlerkontext

Feld	Beschreibung
Name	Ein eindeutiger Name für diesen Sammler zur einfachen Identifizierung.
Kurzbeschreibung	Geben Sie eine kurze, aussagekräftige Beschreibung dieses Sammlers ein.
MID-Webservererweiterung	Angeben und dann die MID-Webserver-Erweiterung starten. Die unterstützten Authentifizierungsmethoden werden im Feld **Authentifizierungstyp** der MID-Webserver-Erweiterung aufgeführt. Informationen zum Konfigurieren einer MID-Webserver-Erweiterung finden Sie unter MID-Webserver konfigurieren.
Status	Dieses Feld wird automatisch mit dem Status der MID-Webserver-Erweiterung ausgefüllt. Dieses Feld ist leer, bis die MID-Webserver-Erweiterung gestartet ist. Nach der Ausgabe eines Befehls an die MID-Webserver-Erweiterung wird einer der folgenden Werte angezeigt: ◦ **Gestartet**: Der Sammler läuft. ◦ **Angehalten**: Der Sammler läuft nicht. ◦ **Offline**: Der MID-Server ist nicht erreichbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ **Fehler**: Der Sammler ist mit einem Fehler fehlgeschlagen (die Fehlermeldung wird im Feld **Fehlermeldung**angezeigt). ◦ **Warnung**: Eine Laufzeitausnahme ist aufgetreten.
Ausführen auf	**Spezifischer MID-Server** oder **Spezifischer MID-Server-Cluster**, wie in der angegebenen MID-Webservererweiterung definiert.
MID-Server	Der **spezifische MID Server** oder **spezifische MID Servercluster**, wie in der angegebenen MID-Webserver-Erweiterung definiert.
Ausführung auf	Der Name des MID-Server, auf dem die MID-Webserver-Erweiterung ausgeführt wird.

4. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
5. Klicken Sie unter **Zugehörige Links** auf **Starten**, um den Sammler zu starten.

Befehle im Kontextformular Ereignismanagement

Zugehöriger Link	Beschreibung
Starten	Startet den Sammler, falls er nicht läuft. Diese Aktion überprüft, ob ein Webservice-API-Endpunkt mit der Ereignismanagement-Anwendung auf MID-Server ausgeführt wird.
Stoppen	Hält den laufenden Sammler auf dem konfigurierten MID-Server an. Wenn der Sammler nicht ausgeführt wird, wird keine Aktion ausgeführt.
Neu starten	Stoppt und startet den Sammler auf dem konfigurierten MID-Server.
Parameter aktualisieren	Sendet aktualisierte Parameter an den Sammler. Parameter werden auch aktualisiert, wenn die Kontexterweiterung Ereignismanagement MID-Server aktualisiert wird. Wenn Sie auf dieses Steuerelement klicken, während der Sammler nicht ausgeführt wird, wird keine Aktualisierung vorgenommen.

Example:
Zeigt die Verwendung der URL zum Umwandeln von JSON v2-formatierten Event-Nachrichten an

Angenommen, Event-Nachrichten im JSON v2-Format werden an MID-Server gesendet. Bei Verwendung der `jsonv2`– URL ist keine Skripteinbindung erforderlich.

Daten für das JSON v2-Beispiel

Feld	Wert
MID_Server_IP	10.218.64.27
MID_Web_Server_Extension_Port	8097
Event-Nachrichtenformat	jsonv2

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ersetzen Sie die Variablen im Standardformat der URL `http://<my-instance>.service-now.com/api/global/em/jsonv2` mit Werten aus der vorherigen Tabelle: `http://10.218.64.27:8097/api/global/em/jsonv2`

Beispiel für die URL für Push-Nachrichten, die nicht im jsonv2-Format vorliegen

Das URL-Format für Push-Event-Nachrichten aus einer externen Quelle, die nicht im jsonv2-Format vorliegen, lautet: `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform={Name_of_Transform_Script}`, wobei die Variable {Name_of_Transform_Script} der vollständige Name des Skripts ist und immer mit dem Text: TransformEvents_ beginnt. Der Skriptname muss als Header-Parameter `Transform` angegeben werden und muss immer mit dem Präfix `TransformEvents_` beginnen.

Nehmen Sie in diesem Beispiel an, dass der Skriptname EventsToProcess lautet. Die URL lautet daher:`http://10.138.64.27:8097/api/mid/em/inbound_event/TransformEvents_EventsToProcess`

Beispiel für Event-Nachrichten im JSON v2-Format

Hinweis: Beim Kopieren und Einfügen des folgenden Texts werden möglicherweise auch ausgeblendete Zeichen kopiert, was zu unerwarteten Ergebnissen führen kann.

```
curl -v -H "Accept: application/json" -H "Content-Type: application/json"
 -X POST --data "{
    "records":
    [ {
         \"source\" : \"Simulated\",
        \"node\" : \"nameofnode\",
        \"type\" : \"High Virtual Memory\",
        \"resource\" : \"C:\",
        \"severity\" : \"5\",
        \"description\" : \"Virtual memory usage exceeds 98%\",
        \"ci_type\":\"cmdb_ci_app_server_tomcat\",
        \"additional_info\":\"{\\\"name\\\":\\\"My Airlines\\\"}\"
      },
      {
      \"source\" : \"Simulated\",
      \"node\" : \"01.myairlines.com\",
      \"type\" : \"High CPU Utilization\",
      \"resource\" : \"D:\",
      \"severity\" : \"5\",
      \"description\" : \"CPU on 01.my.com at 60%\"
      }
   ]
}" -u UserName:Password
 http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/jsonv2
```

Example:
Beispiel für Ereignisnachrichten im JSON v2-Format mit MID-Webserver-API-Schlüssel

Hinweis: Beim Kopieren und Einfügen des folgenden Texts werden möglicherweise auch ausgeblendete Zeichen kopiert, was zu unerwarteten Ergebnissen führen kann.

```
curl --location -g --request POST
 'http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/jsonv2' \
--header 'Accept: application/json' \
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
--header 'Content-Type: application/json' \
--header 'Authorization: key <mid_webserver_api_key>' \
--data-raw '{
   "records":
    [ {
         \"source\" : \"Simulated\",
        \"node\" : \"nameofnode\",
        \"type\" : \"High Virtual Memory\",
        \"resource\" : \"C:\",
        \"severity\" : \"5\",
        \"description\" : \"Virtual memory usage exceeds 98%\",
        \"ci_type\":\"cmdb_ci_app_server_tomcat\",
        \"additional_info\":\"{\\\"name\\\":\\\"My Airlines\\\"}\"
      },
      {
      \"source\" : \"Simulated\",
      \"node\" : \"01.myairlines.com\",
      \"type\" : \"High CPU Utilization\",
      \"resource\" : \"D:\",
      \"severity\" : \"5\",
      \"description\" : \"CPU on 01.my.com at 60%\"
      }
   ]
}'
```

Zugehörige Informationen

- MID-Webservererweiterung konfigurieren
- Event-Erfassung von BMC TrueSight
- Event-Erfassung aus Microsoft Azure Monitor
- Event-Erfassung aus Google Cloud Platform

Event-Erfassung aus benutzerdefinierten Nutzlasten

Mit dem MID WebService-Eventsammler können Sie Event-Informationen aus benutzerdefinierten Nutzlasten im JSON-, XML- oder Nur-Text-Format erfassen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Der MID-Server transformiert die erfassten Event-Nachrichten und füllt die Event-Tabellenfelder (em_table) in der Instanz aus. Das folgende Verfahren beschreibt die Erfassung von JSON-formatierten Event-Nachrichten mit Standardauthentifizierung. Weitere Informationen zu unterstützten Authentifizierungsmethoden finden Sie unter MID-Webservererweiterung konfigurieren.

Das Format der erforderlichen MID-Server-URL ist: `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform={Transform_script_name}`. Der Name der MID-Server-Skripteinbindung setzt sich aus dem Anfügen eines Suffixes an das Standardpräfix `TransformEvents_` zusammen. Informationen zur Erfassung von JSON v2-Event-Nachrichten finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die URL im Format `http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/{transform_script_name}` wird ebenfalls unterstützt.

Prozedur

1. Konfigurieren Sie den MID-WebService-Eventsammler, siehe MID-WebService-Event-Sammlerkontext konfigurieren.
2. Starten Sie den MID-WebService-Eventsammler.

Example:

Transformation von XML-formatierten Event-Nachrichten mithilfe der benutzerdefinierten Nutzlast-URL

Angenommen, Event-Nachrichten im XML-Format werden an MID-Server gesendet. Verwenden Sie dieses Beispiel, um ein Array von Event-Objekten aus den erfassten Event-Nachrichten zurückzugeben. Der Name der MID-Server-Skripteinbindung setzt sich aus dem Anfügen eines Suffixes an das Standardpräfix `TransformEvents_` zusammen. Für die Zwecke dieses Beispiels hat der Benutzer die xmlSample-Skripteinbindung angegeben. Anhand dieser Details lautet der Name der MID-Server-Skripteinbindung `TransformEvents_xmlSample`. Der MID-Server wandelt die erfassten Event-Nachrichten um, indem er die Nachrichten mit der Skripteinbindung analysiert und dann an die Instanz übermittelt.

Daten für das XML-Beispiel

Feld	Wert
MID_Server_IP	10.218.64.27
MID_Web_Server_Extension_Port	8097
transform_script_suffix_name	xmlSample

Ersetzen Sie die Variablen in der URL durch die Werte aus der obigen Tabelle:
`http://10.218.64.27:8097/api/mid/em/xmlSample`

Hinweis: Beim Kopieren und Einfügen des folgenden Texts werden möglicherweise auch ausgeblendete Zeichen kopiert, was zu unerwarteten Ergebnissen führen kann.

Beispiel für Event-Nachrichten im XML-Format:

```
<records>
    <event>
    <source>My Source</source>
    <node>host1</node>
    <type>type1</type>
    <severity>3</severity>
    <description>Virtual memory usage exceeds 98%</description>
    </event>
    <event>
    <source>My Source</source>
    <node>host2</node>
    <type>type2</type>
    <severity>2</severity>
    <description>Virtual memory usage exceeds 90%</description>
    </event>
    </records>
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

MID-Webservererweiterung konfigurieren

MID-WebService-Event-Sammlerkontext konfigurieren

Integrieren Sie mit Push-Connectors

Integrieren Sie mit einem Push-Connector, um eine Verbindung zu einer externen Ereignisquelle herzustellen. Push-Connectors verarbeiten die gesammelten Event-Nachrichten und transformieren sie in das erforderliche Event-Format.

Vorbereitungen

Stellen Sie sicher, dass das Plugin „Ereignismanagement Connectors“ (sn_em_connector) installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Hinweis: Beim Upgrade einer Now Platform-Instanz von Paris oder früher können Sie veraltete Listener-Transformationsskripts verwenden. Weitere Informationen finden Sie unter Veraltete Listener-Transformationsskripts verwenden.

Warum und wann dieser Vorgang ausgeführt wird

Die Push-Connectors akzeptieren Event-Nachrichten, die von externen Event-Quellen generiert werden.
Konfigurieren Sie einen Connector für die Überwachung einer externen Event-Quelle.
Verwenden Sie einen benutzerdefinierten Push-Connector, um die Event-Nachrichten entweder über den MID-Server oder die Instanz zu senden.

Hinweis: Sie können die folgende generische JSON-Ziel-URL zum Erfassen von Events verwenden: `https:/<<INSTANCE>>/api/sn_em_connector/em/inbound_event?source=genericJson`. Diese URL kann unverändert verwendet werden und erfordert die Konfiguration einer Event-Regel.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Push-Connectors**.
2. Klicken Sie auf **Neu**, oder klicken Sie auf den Push-Connector, den Sie ändern möchten, z. B. AWS oder Azure.
3. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Eindeutiger Name für diesen Push-Connector zur einfachen Identifizierung
Beschreibung	Geben Sie eine Beschreibung für die Verwendung des Push-Connectors ein.
Header-Name	Geben Sie den Header-Namen an, für den der Wert festgelegt werden soll, z. B. Set-Header.
Header-Wert	Der Header-Wert, für den der Wert festgelegt werden soll, z. B. Set-Header.
Typ	Wählen Sie diese Option aus, um Events entweder an die `Instanz` oder über den `MID`zu senden. Verwenden Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	jeweils die URL des ausgewählten Typs. Weitere Informationen finden Sie in der Beschreibung des Felds **URL-Parameterwert**.
Aktiv	Aktivieren, um das Abrufen von Events aus dieser externen Event-Quelle zu aktivieren.
Reihenfolge	Reihenfolge, in der eine Event-Regel ausgewertet wird, wenn mehrere Regeln für denselben Event-Typ definiert sind. Event-Regeln werden in aufsteigender Reihenfolge ausgewertet.
URL-Parameterwert	◦ Senden Sie Events an die Instanz. Verwenden Sie die URL im folgenden Format für alle Connectors:`https://<<INSTANCE>>/api/sn_em_connector/em/inbound_event?source={URL_parameter_value}`. ◦ Senden Sie Events über den MID-Server. Verwenden Sie die URL in diesem Format:`http://{MID_Server_IP}:{MID_Web_Server_Port}/api/mid/em/inbound_event?Transform={Transform_script}` **Hinweis:** Das Senden von Events an den MID-Server erfordert die vorherige Konfiguration der Erweiterung für MID-WebService-Event-Listener.

4. Im Abschnitt Skript:

- Wenn der für das Feld **Typ** ausgewählte Wert `MID` ist, wird das Feld **Umwandlungsskript** angezeigt. In diesem Feld geben Sie den Namen der MID-Skripteinbindung an, die Event-Nachrichten akzeptiert, die von der erforderlichen externen Event-Quelle generiert werden und die das Skript im erforderlichen Event-Format analysiert, oder suchen Sie nach diesem Namen. Verwenden Sie diese Namenskonvention für das Skript: `TransformEvents_<your source>`
- Wenn der für das Feld **Typ** ausgewählte Wert **Instanz** ist, wird der **Skript**-Editor angezeigt. Im **Skript**-Editor geben Sie das benutzerdefinierte Skript an, das Event-Nachrichten akzeptiert, die von der erforderlichen externen Event-Quelle generiert werden und die das Skript im erforderlichen Event-Format analysiert.

Example
Dieses Beispiel zeigt, wie die transformierten Felder einem Event-Formular hinzugefügt werden.

```
(function process(/*RESTAPIRequest*/ request, body) {
 /*Function that receives a JSON object, adding all its fields to the
 Additional information object. The field name is a concatenation of
 the field key and the parent field key if it exists.*/
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
function updateAdditionalInfo(event, field,jsonObject,additionalInfo)
{
       for (var key in jsonObject) {
           var newKey = key;
           if (field != "") {
               newKey = field + '_' + key;
           }
  // You can do some transformation here and set fields on the event
  //if(key == "MySource")
  //   event.source = jsonObject[key];
           additionalInfo[newKey] = jsonObject[key];
       }
   }

   try
{
       gs.info("TransformEvents_generic received body:" + body);
 var jsonObject = JSON.parse(body);
       var event = new GlideRecord('em_event');
 event.source = "GenericJson"; //TODO: Need to define
       event.event_class = "GenericJsonClass"; //TODO: Need to define
       event.severity = "5";

       var additionalInfo = {};
       updateAdditionalInfo(event, "",jsonObject,additionalInfo);
 /*Iterates over Additional information JSON object and adds all
nested objects' fields as fields of the Additional information
object*/
       var notDone = true;
       while (notDone) {
           notDone = false;
           for (var key in additionalInfo) {
               if (Object.prototype.toString.call(additionalInfo[key])
== '[object Object]') {
                   notDone = true;
                   updateAdditionalInfo(event,
key,additionalInfo[key],additionalInfo);
    additionalInfo[key] = "";
               }
           }
       }
 gs.info("TransformEvents_generic generated additional information:" +
JSON.stringify(additionalInfo));
       event.additional_info = JSON.stringify(additionalInfo);
       event.insert();
}
catch(er){
 gs.error(er);
 status=500;
 return er;
}
return "success";
})(request, body);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Veraltete Listener-Transformationsskripts verwenden

Verwenden Sie veraltete Listener-Transformationsskripts, wenn Sie eine Now Platform-Instanz von Paris oder früher aktualisieren. Diese Skripts können als Teil vorhandener integrierter Systeme oder gemeinsam mit Ereignismanagement-Push-Connectors ausgeführt werden.

Sie können Listener-Transformationsskripts verwenden, um sicherzustellen, dass vorherige Integrationen unterstützt werden. Wenn Sie beispielsweise den Endpunkt `https://<instance-name>.service-now.com/api/global/em/inbound_event` in verschiedenen Integrationen verwenden, können Sie diesen Endpunkt in einer Quebec- oder einer späteren Now Platform-Instanz weiterverwenden.

Wenn Sie die Push-Connectors Ereignismanagement verwenden möchten, laden Sie das Plugin von herunter ServiceNow Store Website von. Sie können dann auf die Push-Connectors in der Now Platform-Instanz zugreifen, und der Endpunkt `https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event` wird ebenfalls erstellt.

Veralteten Endpunkte mit Push-Connectors verwenden

Sie können den Endpunkt `https://<instance-name>.service-now.com/api/global/em/inbound_event` mit den Push-Connectors weiterverwenden, indem Sie die entsprechenden Transformationsskripts deaktivieren. Um ein Skript zu deaktivieren, navigieren Sie zu **Ereignismanagement** > **Integrationen** > **Listener-Transformskripts**. Klicken Sie dann in der angezeigten Liste auf das entsprechende Skript, und deaktivieren Sie das Kontrollkästchen **Aktiv** im Formular.

Veralteten Endpunkt verwenden und alle Listener-Transformationsskripts deaktivieren

Sie können auch den Endpunkt `https://<instance-name>.service-now.com/api/global/em/inbound_event` weiterverwenden, müssen dazu aber Sie die Listener-Transformationsskripts deaktivieren, damit stattdessen die Push-Connectors verwendet werden. Um alle Skripts zu deaktivieren, navigieren Sie zu **Systemeigenschaften** > **Alle Eigenschaften**, suchen Sie die Eigenschaft *sn_em_connector_listener_table_for_InboundEvent*, und legen Sie ihren Wert auf **true**fest.

Anwenderdefinierte Listener-Transformationsskripts zum Push-Connectors-Modul migrieren

Falls Sie benutzerdefinierte Listener-Transformationsskripts erstellt haben, müssen diese zum Push-Connectors-Modul migriert werden, wenn Sie den neuen Endpunkt `https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event` verwenden möchten. Um das anwenderdefinierte Skript zu migrieren, navigieren Sie zu **Ereignismanagement** > **Integrationen** > **Listener-Transformskripts**, klicken Sie auf das entsprechende Listener-Transformskript, und wählen Sie das angezeigte Skript aus. Navigieren Sie dann zu **Integrationen** > **Push-Connectors**, klicken Sie auf **Neu**, und fügen Sie das Skript ein, das Sie aus dem Listener-Transformskript kopiert haben.

AWS-Plattform als Datenquelle integrieren

Integrieren Sie Amazon Web Services (AWS) mit Ereignismanagement. Zum Hinzufügen der Plattform AWS als Datenquelle ist eine Konfiguration in der Plattform AWS erforderlich.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dlädt den Ereignismanagement Connectors Plugin aus dem ServiceNow Store.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine AWS-Plattformwarnung eingeht, führt Ereignismanagement Folgendes aus:

- Extrahiert Informationen aus dem ursprünglichen Plattformalarm AWS , um die erforderlichen Ereignisfelder auszufüllen, und fügt das Ereignis in die -Datenbank ein.
- Erfasst den Inhalt im Feld **additional_info**.

Der Push-Connector der Plattform AWS befindet sich in **Ereignismanagement** > **Integrationen** > **Push-Connectors**. Klicken Sie auf der Seite Push-Connectors auf **AWS-Events-Push-Connector**.

Hinweis: Der AWS -Push-Connector , der im Basissystem bereitgestellt wird, verarbeitet nur AWS CloudWatch-Alarme. Um andere SNS-Warnungen (Simple Notification Service) als AWS CloudWatch zu verarbeiten, erstellen Sie einen neuen -Push-Connector, oder passen Sie den AWS -Push-Connectoran.

Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Ereignisregeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Zuordnung** anwenden Checkbox für Regeln auf „wahr“ gesetzt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie mehr Ereignisregeln oder Automatisierung mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Prozedur

1. Wählen Sie in der Plattformkonsole AWS **Simple Notification Service** aus.
   Wenn kein SNS-Thema vorhanden ist, erstellen Sie eines.
2. Erstellen Sie unter dem SNS-Thema ein neues Abonnement.

   a. Übernehmen Sie **Thema-ARN** aus dem von Ihnen erstellten Thema.
   Der Amazon-Ressourcenname (ARN) ist für die Bindung einer Ereignismanagement-Warnung an ein CI erforderlich.

   b. Legen Sie **Protokoll** als *`https`* fest.

   c. **Endpunkt** festlegen auf: `https://`<username> :<password> @<instance-name> .service-now.com/api/sn_em_connector/em/inbound_event?source=aws

   Wenn die Multifaktor-Authentifizierung (MFA) der Plattform AWS aktiviert ist, werden bei der Anmeldung bei der Website der Plattform AWS Anwendername und Passwort sowie ein Authentifizierungscode vom MFA-Gerät der Plattform AWS des verwendet Benutzer
3. Warten Sie, bis das Abonnement von `Ausstehend` in `Bestätigt` geändert wird und die Abonnement-ARN ausgefüllt ist.
   Dies kann ein paar Minuten dauern.
4. Erstellen Sie Alarme auf der Plattform AWS , um sie an Ereignismanagement zu senden, und verknüpfen Sie die Alarme mit dem von Ihnen erstellten SNS-Thema.
   Diese Event-Regeln werden mit dem Basissystem bereitgestellt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignisregel	Beschreibung
AWS Hostbindung	Binden Sie Plattformwarnungen für AWS , entweder auf dem Host oder auf dem virtuellen Computer (VM), an das Hardware-CI des Hosts.
AWS Allgemein	Binden Sie AWS-Plattformalarme auf dem Lastenausgleichsmodul an das CI des Cloud-Lastenausgleichsmoduls, Amazon Relational Database Service (RDS) an das CI der Cloud-Datenbank sowie den Host oder die virtuelle Maschine (VM) an das CI der VM-Instanz. **Hinweis:** Um Events vom Host oder von der virtuellen Maschine an das Instanz-CI der virtuellen Maschine zu binden, deaktivieren Sie die AWS-Hostbindungsregel.

Dieses Beispiel zeigt eine JSON-Zeichenfolge für AWS die VM-Bindung:

```
{
"Type" : "<type>",
"MessageId" : "<message ID #>",
"TopicArn" : "<topic arn>",
"Subject" : "ALARM: \"<alarm type>\" in <location>",
"Message" : "{\"AlarmName\":\"<alarm
 name>\",\"AlarmDescription\":<alarm
 description>,\"AWSAccountId\":\"<account ID
 #>\",\"NewStateValue\":\"ALARM\",\"NewStateReason\":\"Threshold
 Crossed: <threshold and datapoint which it
 crossed>.\",\"StateChangeTime\":\"<date and
 time>\",\"Region\":\"<location>\",\"OldStateValue\":\"OK\",
\"Trigger\":{\"MetricName\":\"CPUUtilization\",\"Namespace\":
\"<namespace>\",\"Statistic\":\"<statistic
 name>\",\"Unit\":null,\"Dimensions\":[{\"name\":\"InstanceId\",
\"value\":\"<dimension value>\"}],\"Period\":<period
 number>,\"EvaluationPeriods\":<number of evaluation
 periods>,\"ComparisonOperator\":\"GreaterThanOrEqualToThreshold\",
\"Threshold\":<threshold number>}}",
"Timestamp" : "<date and time>",
"SignatureVersion" : "<version number>",
"Signature" : "<signature>",
"SigningCertURL" : "<URL>",
"UnsubscribeURL" : "<URL>"
}
```

Zugehörige Informationen

Event-Feldformat für die Event-Erfassung

Integrieren Sie mit Push-Connectors

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Integrieren Sie AWS mit dem REST-API-Schlüsseltoken

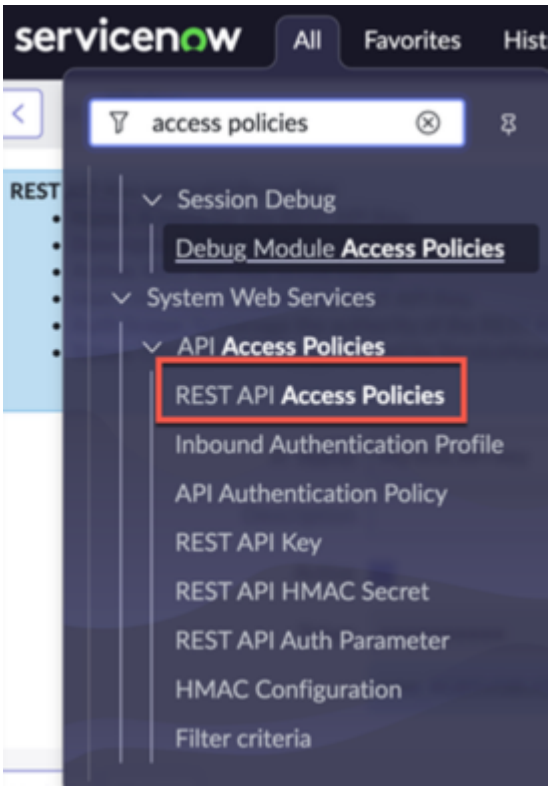
Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und erhöht die betriebliche Effizienz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**.



2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

> **Hinweis:** Der Anwender muss mit der Rolle evt_mgmt_integration erstellt werden. Erstellen Sie in der Tabelle „sys_user“ eine neue, um sie hier zu verwenden, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das

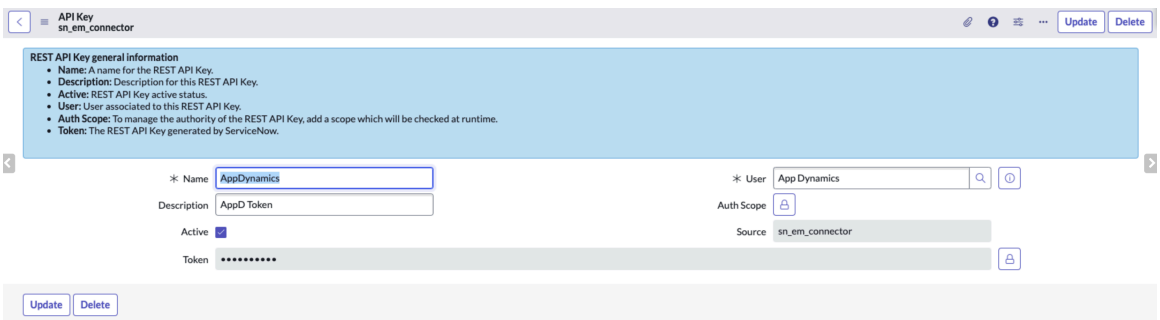
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST-API-Schlüssels zu verwalten.
Token	Der von Now Platformgenerierte REST-API-Schlüssel. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.
Ablauf	Zeitpunkt, nach dem die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie hinzu: UserAccount.
5. Verwenden Sie das Formularmenü, und wählen Sie **Speichern**aus.

   Das System generiert ein Token und speichert es im Feld **Token**. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie den Inhalt, der unter dem Feld angezeigt wird. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Azure Monitor als authentifizierte Datenquelle integrieren

Integrieren Sie Microsoft Azure mit Ereignismanagement, indem Sie Azure Monitor als authentifizierte Datenquelle hinzufügen.

Sie können die Ereignismanagement-Umgebung für die Erfassung von Events aus Azure Monitor konfigurieren, indem Sie Ihre Now Platform-Instanz als REST-Endpunkt festlegen.

Sobald der Endpunkt konfiguriert ist und eine Azure Überwachungswarnmeldung eingeht, Ereignismanagement:

- Authentifiziert die Warnmeldungsmeldung von Azure Monitor beim entsprechenden ServiceNow -Anwender mithilfe der OAuth-Konfiguration oder eines Standard-Webhooks.
- Extrahiert Informationen aus der ursprünglichen Azure -Monitor-Warnungsnachricht, um die erforderlichen Ereignisfelder auszufüllen, und fügt das Ereignis in die Datenbank Now Platform ein.
- Erfasst spezifischen Inhalt im Feld **Zusätzliche Informationen** des Event-Formulars

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Welche Authentifizierung verwendet wird

Die folgenden zwei Authentifizierungsmethoden sind verfügbar:

- OAuth-Authentifizierung: Bietet Authentifizierung auf Unternehmensebene, um die Sicherheit Ihrer Unternehmensumgebung zu gewährleisten. Die Authentifizierung erfolgt mit Azure Monitor V1- oder V2-Zugriffstoken. Weitere Informationen finden Sie unter Azure Monitor mit OAuth-Authentifizierung integrieren.
- Standard-Webhook-Authentifizierung: Bietet einen Basisstandard für die Authentifizierung, ohne dass Azure Active Directory erforderlich ist. Diese Authentifizierung kann besonders für verteilte kleine Teams wie SRE- oder DevOps -Teams nützlich sein. Weitere Informationen finden Sie unter Azure Monitor mit Standardauthentifizierung integrieren.

Was Sie wissen müssen, bevor Sie beginnen

Sie können Ihren integrierten Azure Monitor erst dann als Datenquelle verwenden, nachdem Sie Folgendes überprüft haben:

- Für beide Authentifizierungsmethoden wurde dem relevanten ServiceNow-sys_user die Rolle evt_mgmt_integration zugewiesen.
- In der Now Platform-Instanz wurde das Plugin „Ereignismanagement Connectors“ installiert. Sie können das Plugin herunterladen von ServiceNow Store Website von.
- Azure Cloud-Discovery muss ausgeführt werden, um sicherzustellen, dass die erstellten Warnungen an die Konfigurationselemente in Now Platformgebunden sind. Weitere Informationen finden Sie unter Erkennung von Azure-Clouds.

Event-Regeln und Event-Feldzuordnungen

Die folgenden Ereignisregeln und Ereignis-Feldzuordnungen werden mit dem Basissystem bereitgestellt:

Modul	Beschreibung
Ereignisregeln	**Azure Monitor**: Allgemeine Event-Regel zur Verarbeitung aller Azure Monitor-Events.
Event-Feldzuordnungen	**Azure-Monitor - ci_type**: Zum Zuordnen des ci_type von Events basierend auf dem resourceType-Feld. Ein Basissatz von Zuordnungspaaren wird bereitgestellt.

Die folgenden Zuordnungen werden mit dem Basissystem in **Azure Monitor - ci_type** bereitgestellt:

Wertepaare transformieren

Event Mapping Pairs

Key	Value
microsoft.compute/virtualmachines	cmdb_ci_vm_object
microsoft.documentdb/databaseaccounts	cmdb_ci_cloud_database
microsoft.sql/servers	cmdb_ci_cloud_database
microsoft.web/sites	cmdb_ci_cloud_webserver
microsoft.cache/redis	cmdb_ci_cloud_database
microsoft.documentdb	cmdb_ci_cloud_database
microsoft.sql/servers/databases	cmdb_ci_cloud_database

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können der Event-Feldzuordnung - **Azure Monitor - ci_type** je nach Anforderung neue Zuordnungspaare hinzufügen, um Events dem entsprechenden ci_type basierend auf resourceType zuzuordnen.

Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Regeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Abgleichsregeln anwenden** Checkbox auf „wahr“ festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für den Connector ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Wenn Sie Warnungsstatusänderungen für die ServiceNow-Instanz von den ServiceNow-Warnungen an das Azure-Portal senden möchten, müssen Sie den bidirektionalen Azure Monitor-Connector aktivieren. Weitere Informationen finden Sie unter Bidirektionalen Azure Monitor-Connector konfigurieren.

Azure Monitor mit Standardauthentifizierung integrieren

Integrieren Sie Microsoft Azure mit Ereignismanagement, indem Sie Azure Monitor einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Erforderliche Rollen: evt_mgmt_admin und web_service_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Azure, indem Sie Azure Monitor als Datenquelle authentifizieren. Legen Sie in Ihrem Azure Monitor-Portal Ihre Now Platform-Instanz mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

Im Azure-Portal werden Warnungskorrelationsregeln durch die Einstellung *`Correlate alerts`* unter „Warnungsverarbeitungsregeln“ definiert. Wenn *`Correlate alerts`* im Azure-Portal zugewiesen ist, werden die Azure Monitor-Warnungen, die innerhalb von 60 Minuten in der Instanz ServiceNow® empfangen wurden, mithilfe von tagbasiertem Warnungs-Clustering gruppiert.

Prozedur

1. Erstellen Sie in Now Platform ein Benutzerkonto, oder identifizieren Sie einen vorhandenen ServiceNow-Benutzer für diese Integration.
   Stellen Sie außerdem sicher, dass ServiceNow sys_user die Rolle evt_mgmt_integration zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.
2. Aktualisieren Sie in Ihrem Azure Monitor-Portal die Azure Monitor-Warnungsregeln, um eine Aktionsgruppe mit einen Standard-Webhook zu verwenden:

   a. Erstellen Sie eine Aktionsgruppe mit *`action type=webhook`* und geben Sie die URL an, die die Benutzer-ID und das Passwort des ServiceNow-Benutzers im Endpunkt enthält. Zum Beispiel:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
https://<username> :<password> @<instance-name> .service-now.com/api/
sn_em_connector/em/inbound_event?source=azuremonitor
```

b. Stellen Sie im Abschnitt „Webhook“ sicher, dass für **Enable the common alert schema (Gemeinsames Warnungsschema aktivieren)** die Option **Ja** ausgewählt ist.

Ergebnisse

Die Übertragung von Warnungen von Azure Monitor in das Plugin Event Management beginnt. Das Plugin extrahiert die Informationen aus der ursprünglichen Azure Monitor-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer Now Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen.

Nächste Maßnahme

Wenn Sie Warnungsstatusänderungen für die ServiceNow-Instanz von den ServiceNow-Warnungen an das Azure-Portal senden möchten, müssen Sie den bidirektionalen Azure Monitor-Connector aktivieren. Weitere Informationen finden Sie unter Bidirektionalen Azure Monitor-Connector konfigurieren.

Integrieren Sie Azure mit dem REST-API-Schlüsseltoken

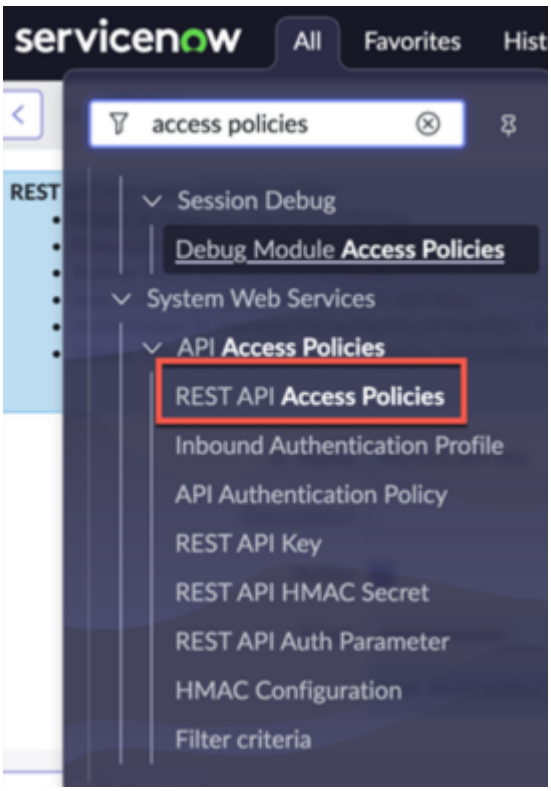
Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und erhöht die betriebliche Effizienz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

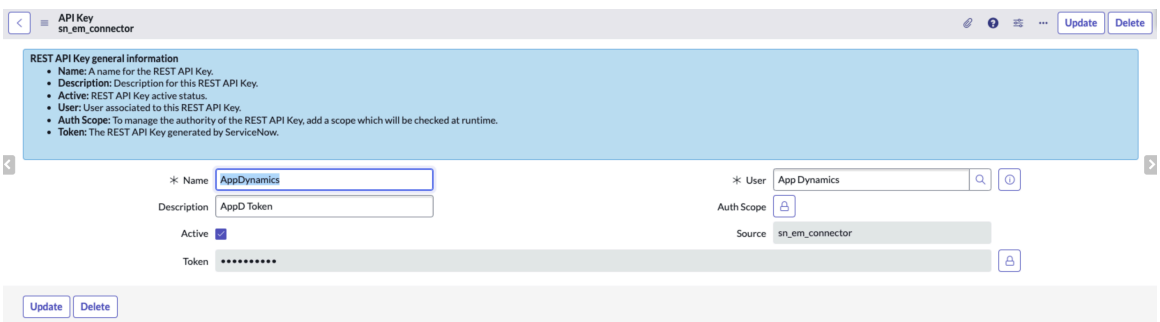
> **Hinweis:** Der Anwender muss mit der Rolle evt_mgmt_integration erstellt werden. Erstellen Sie in der Tabelle „sys_user“ eine neue, um sie hier zu verwenden, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST-API-Schlüssels zu verwalten.
Token	Der von Now Platformgenerierte REST-API-Schlüssel. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.
Ablauf	Zeitpunkt, nach dem die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie hinzu: UserAccount.
5. Verwenden Sie das Formularmenü, und wählen Sie **Speichern**aus.

Das System generiert ein Token und speichert es im Feld **Token**. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie den Inhalt, der unter dem Feld angezeigt wird. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Monitor mit OAuth-Authentifizierung integrieren

Integrieren Sie Microsoft Azure mit Ereignismanagement, indem Sie Azure V1- oder V2-Token im Azure-Monitor authentifizieren.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Im Azure-Portal werden Warnungskorrelationsregeln durch die Einstellung *`Correlate alerts`* unter „Warnungsverarbeitungsregeln“ definiert. Wenn *`Correlate alerts`* im Azure-Portal zugewiesen ist, werden die Azure Monitor-Warnungen, die innerhalb von 60 Minuten in der Instanz ServiceNow® empfangen wurden, mithilfe von tagbasiertem Warnungs-Clustering gruppiert.

Erforderliche Rollen: evt_mgmt_admin, web_service_admin und oauth_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Azure Monitor. Legen Sie in Ihrem Azure Monitor-Portal Ihre Now Platform-Instanz mithilfe von V1- oder V2-Token als REST-Endpunkt fest.

Prozedur

1. Im Azure Monitor-Portal:

   a. Führen Sie die App-Registrierung durch, und stellen Sie eine API bereit.
   Weitere Informationen zum Registrieren einer App und zum Bereitstellen einer API in Azure finden Sie unter https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-configure-app-expose-web-apis .

   b. Erstellen Sie eine Aktionsgruppe mit einem sicheren Webhook, und geben Sie den REST-Endpunkt als `https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=azuremonitor` an.

   Hinweis: Für servicenowservices.com-Instanzen muss der REST-Endpunkt `https://sein.<instance-name>` .servicenowservices.com/api/sn_em_connector/em/inbound_event?source=azuremonitor

   Weitere Informationen zum Hinzufügen eines sicheren Webhooks zu einer Aktionsgruppe finden Sie unter https://docs.microsoft.com/en-us/azure/azure-monitor/platform/action-groups .

   c. Navigieren zu **Warnungen** > **Verwalten Sie Warnungsregeln**.

   d. Stellen Sie im Abschnitt „Secure Webhook“ (Sicherer Webhook) sicher, dass **Ja** für die Option **Enable the common alert schema (Gemeinsames Warnungsschema aktivieren)** ausgewählt ist.

   e. Fügen Sie die Aktionsgruppe mit dem sicheren Webhook einer Warnungsregel hinzu.

2. Überprüfen Sie im Azure Monitor-Portal, welches Azure-Token von Ihrer registrierten Anwendung verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren Sie zu **App Registration** (App-Registrierung), und wählen Sie die registrierte Anwendung aus.

b. Klicken Sie im Abschnitt „Verwalten“ auf **Manifest**.

c. Suchen Sie im Editor-Bildschirm den Parameter *accessTokenAcceptedVersion*. Wenn der Wert von *accessTokenAcceptedVersion* gleich **2** ist, müssen bei der Integration die V2-Token verwendet werden.

   Wenn der Wert von *accessTokenAcceptedVersion* gleich **1** oder**Null** ist, müssen bei der Integration die V1-Token verwendet werden.

3. Stellen Sie in Ihrer Now Platform-Instanz sicher, dass dem ServiceNow-Benutzer die richtige Anwendungs-ID (Client-ID) oder der URI mit der richtigen Anwendungs-ID zugewiesen ist. Stellen Sie außerdem sicher, dass ServiceNow sys_user die Rolle evt_mgmt_integration zugewiesen ist.

   a. Navigieren zu **Systemsicherheit** > **Anwender und Gruppen** > **Anwender**.

      Hinweis: Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

   b. Stellen Sie sicher, dass das Feld **Quelle** für den ServiceNow-sys_user mit der richtigen Anwendungs-ID (Client-ID) oder dem URI mit der richtigen Anwendungs-ID ausgefüllt ist, wie im Azure Monitor-Portal definiert.
   Wenn die Anwendung ein Azure V1-Token verwendet, muss in das Feld **Quelle** der URI der Anwendungs-ID der registrierten Anwendung eingetragen werden. Wenn die Anwendung ein Azure V2-Token verwendet, muss in das Feld **Quelle** die Anwendungs-ID (Client-ID) der registrierten Anwendung eingetragen werden.

   Wenn das Feld **Quelle** nicht angezeigt wird, ändern Sie das Formularlayout so, dass dieses Feld angezeigt wird. Klicken Sie auf das Kontextmenüsymbol ( ), und wählen Sie **Konfigurieren > Formularlayout** aus. Verschieben Sie **Quelle** in die Liste „Ausgewählt“.

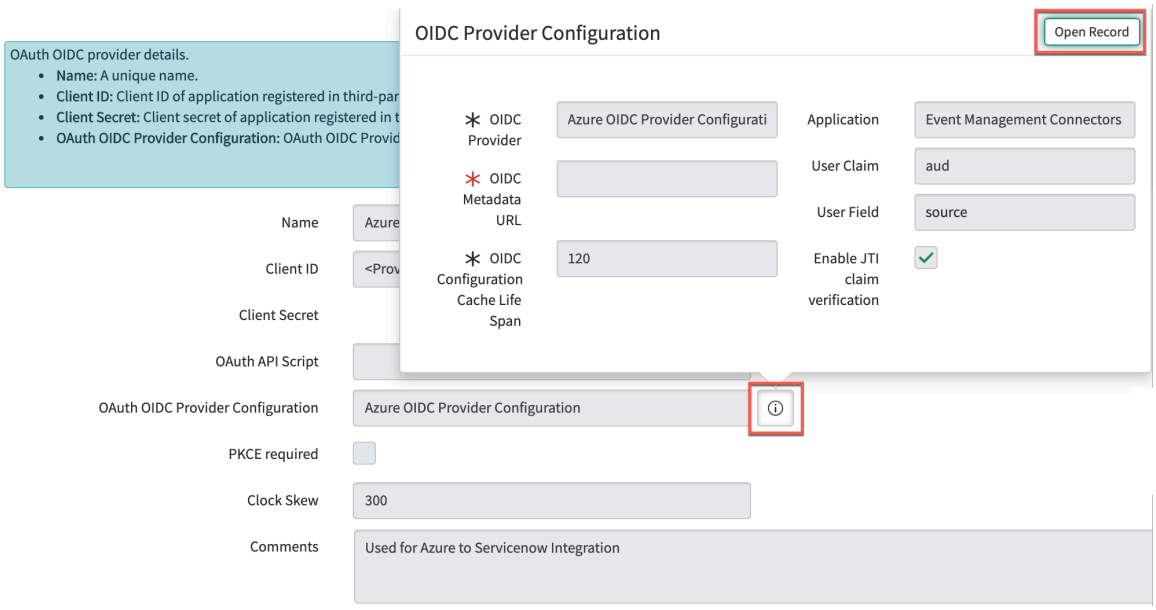
      Hinweis: Wenn Version Ihrer Now Platform-Instanz Paris Patch 2 oder Orlando Patch 9 oder früher ist, muss der Wert im Feld **Quelle** in eckige Klammern eingeschlossen werden. Beispiel: `[api://azuretest]`.

4. Navigieren Sie in Ihrer Instanz von Now Platform zu **Ereignismanagement** > **Integrationen** > **Azure OAuth-Konfiguration**.
5. Klicken Sie auf **Azure OAuth OIDC Entry (Azure OAuth OIDC-Eintrag)**, und geben Sie die `Client-ID` ein.
   Wenn die registrierte Anwendung ein Azure V2-Token verwendet, muss die `Client-ID` mit der `Anwendungs-ID (Client-ID)` der im Azure Monitor-Portal definierten App-Registrierungen identisch sein.

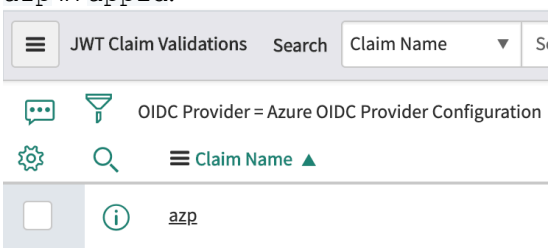
   Wenn die registrierte Anwendung ein Azure V1-Token verwendet, muss die `Client-ID` mit dem `URI der Anwendungs-ID` der im Azure Monitor-Portal definierten App-Registrierungen identisch sein (der bereitgestellten API).

6. Klicken Sie im Feld **OAuth-OIDC-Providerkonfiguration** auf das Info-Symbol ( ).
7. Klicken Sie im Fenster „OIDC-Provider-Konfiguration“ auf **Datensatz öffnen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Geben Sie die `OIDC-Metadaten-URL` gemäß dem Azure-Token ein, das von der registrierten Anwendung verwendet wird, wie in der folgenden Tabelle gezeigt.

Azure-Token	OIDC-Metadaten-URL
V2	Fügen Sie im Formular „OIDC-Provider-Konfiguration“ im Feld **OIDC-Metadaten-URL** die folgende URL hinzu: `https://login.microsoftonline-.com/<tenant-id>/v2.0/.well-known/openid-configuration` Achten Sie darauf, dass `<tenant-id>` durch die richtige Azure-Mandanten-ID ersetzt wird. **Hinweis:** Wenn Sie versuchen, Azure Gov Cloud mit dem ServiceNow Azure Monitor-Connector zu integrieren, denken Sie daran, den Anspruchswert in `f1f34126-d4ef-40e1-ad4b-bf5d47b4860d`zu ändern.
V1	Gehen Sie im Formular „OIDC-Provider-Konfiguration“ wie folgt vor: ◦ Ändern Sie in der Spalte „Anspruchname“ `azp` in `appid`. 

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Token	OIDC-Metadaten-URL
	Hinweis: Wenn Sie versuchen, Azure Gov Cloud mit dem ServiceNow Azure Monitor-Connector zu integrieren, denken Sie daran, den Anspruchswert in `f1f34126-d4e-f-40e1-ad4b-bf5d47b4860d`zu ändern. ◦ Fügen Sie im Feld **OIDC-Metadaten-URL** die folgende URL hinzu: `https://login.microsoftonline.com/<tenant-id>/.well-known/openid-configuration` Achten Sie darauf, dass `<tenant-id>` durch die richtige Azure-Mandanten-ID ersetzt wird.

Ergebnisse

Wenn in Azure Monitor eine Warnung als Teil der Warnungsregel erstellt wird, wird die Benachrichtigung über den sicheren Webhook-Endpunkt an die Now Platform gesendet. Navigieren Sie in Ihrer Now Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen. Wenn Sie Warnungsstatusänderungen für die ServiceNow-Instanz von den ServiceNow-Warnungen an das Azure-Portal senden möchten, müssen Sie den bidirektionalen Azure Monitor-Connector aktivieren. Weitere Informationen finden Sie unter Bidirektionalen Azure Monitor-Connector konfigurieren .

Bidirektionalen Azure Monitor-Connector konfigurieren

Vom Azure Monitor-Pull-Connector werden Informationen aus ServiceNow Ereignismanagement an das Azure-Portal gesendet. Vom Pull-Connector werden die Warnungsstatusänderungen aus der ServiceNow-Umgebung an das Azure-Portal gesendet.

Vorbereitungen

Wenn im Azure-Portal eine Warnung ausgelöst wird, wird ein sicherer Webhook erstellt, um die Warnungsbenachrichtigungen an ServiceNowzu senden. Der Azure Monitor-Connector empfängt die Warnungsbenachrichtigung als Ereignis in der Instanz ServiceNow.

Der bidirektionale Azure Monitor-Connector wird in den folgenden Now Platform-Versionen unterstützt:

- Quebec, Patch 9 oder höher
- Rome, Patch 3 oder höher

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie den bidirektionalen Azure Monitor-Connector konfigurieren, wird der bidirektionale Austausch von Werten mit der externen Event-Quelle aktiviert. Wenn eine Warnung in der ServiceNow-Instanz **Bestätigt**/**Geschlossen**/**Erneut geöffnet** wird, ändert sich der Status in der Azure-Portal-Warnung über den bidirektionalen Connector.

Diese Szenarien beschreiben die bidirektionale Standardfunktionalität für den Azure Monitor-Connector:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn eine Warnung im Azure-Portal geschlossen wird, wird sie in ServiceNow automatisch geschlossen. Sie wird jedoch unabhängig von der bidirektionalen Funktion aktualisiert, da durch das Schließen des über das Azure-Portal empfangenen Events die Warnung geschlossen wird.
- Wenn eine Warnung im ServiceNow-System manuell geschlossen wird, werden alle zugehörigen Azure-Warnungen im Azure-Portal geschlossen.
- Wenn der Warnungsstatus in ServiceNow in **Erneut geöffnet** geändert wird, werden alle zugehörigen Azure-Warnungen im Azure-Portal geöffnet.
- Wenn eine Warnung im ServiceNow-System **Bestätigt** wird, werden alle zugehörigen Azure-Warnungen im Azure-Portal bestätigt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Klicken Sie auf **Azure Monitor**.
3. Aktivieren Sie die Checkbox **Aktiv**.
4. Fügen Sie im Feld **Anmeldeinformationen** die Anmeldeinformationen des Azure-Dienstprinzipals hinzu, die über die Berechtigung zum Ausführen von Aktionen verfügen. Zum Ändern des Warnungsstatus muss der Serviceprinzipal über die Berechtigungen „Microsoft.AlertsManagement“ und die Rolle „ Beitragender bei der Überwachung“ verfügen.
5. Wählen Sie den MID-Server aus, der für diesen Connector verwendet werden soll, oder fügen Sie ihn hinzu.
   Wenn Warnungen im MS Azure-Portal nicht wie erwartet aktualisiert werden, überprüfen Sie die Protokolle MID-Server auf Fehler.

Nächste Maßnahme

Mehrere Warnungen aus dem Azure-Portal können einer einzelnen ServiceNow-Warnung durch Deduplizierung zugeordnet werden. Die Zuordnung zwischen der ServiceNow-Warnung und den Azure-Warnungen wird in der Tabelle sn_em_connector_event_data verwaltet. Die Aufbewahrung von Datensätzen hängt vom Status der Warnung ab:

- Wenn der bidirektionale Azure-Connector nicht aktiv ist, werden die Datensätze nach 2 Tagen gelöscht.
- Wenn der bidirektionale Azure-Connector aktiv ist:
  - Wenn sich die Warnung im Status „Geschlossen“ befindet, werden die Daten 7 Tage lang gespeichert. Diese Dauer kann durch die Systemeigenschaft sn_em_connector.eventdata_closedevent_interval angepasst werden.
    - Wenn die geschlossene Warnung innerhalb von 7 Tagen erneut geöffnet wird, werden die entsprechenden geschlossenen Warnungen aus dem Azure-Portal erneut geöffnet.
    - Wenn die geschlossene Warnung nach 7 Tagen erneut geöffnet wird, werden die entsprechenden geschlossenen Warnungen aus dem Azure-Portal nicht erneut geöffnet.
  - Wenn sich die Warnung im Status „Offen“ befindet, werden die Daten 30 Tage lang gespeichert. . Diese Dauer kann mit „sn_em_connector.eventdata_openevent_interval“ angepasst werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie eine offene ServiceNow-Warnung innerhalb von 30 Tagen schließen oder bestätigen möchten, können Sie alle entsprechenden Azure-Warnungen im Azure-Portal schließen oder bestätigen.
- Wenn Sie eine offene ServiceNow-Warnung nach 30 Tagen schließen oder bestätigen möchten, können Sie alle entsprechenden Azure-Warnungen im Azure-Portal nicht schließen oder bestätigen.

Event-Erfassung von Microsoft Azure Monitor

Mit dem MID WebServer-Event-Sammler können Sie Event-Nachrichten im JSON-Format erfassen, die vom Microsoft Azure-Portal gesendet wurden.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Stellen Sie Folgendes sicher:

- Stellen Sie den MID-Server bereit und starten Sie ihn. Weitere Informationen finden Sie unter MID-Server-Konfiguration .
- Konfigurieren Sie einen MID Web Server. Weitere Informationen finden Sie unter MID-Webservererweiterung konfigurieren.
- Konfigurieren und starten Sie den Eventsammler des MID WebService. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Im Azure-Portal werden Warnungskorrelationsregeln durch die Einstellung *Correlate alerts* unter „Warnungsverarbeitungsregeln“ definiert. Wenn *Correlate alerts* im Azure-Portal zugewiesen ist, werden die Azure Monitor-Warnungen, die innerhalb von 60 Minuten in der Instanz ServiceNow® empfangen wurden, mithilfe von tagbasiertem Warnungs-Clustering gruppiert.

Event-Nachrichten im JSON-Format werden von Microsoft Azure gesendet. MID-Server wandelt die gesammelten Ereignisnachrichten um, indem sie sie mithilfe der Skripteinbindung TransformEvents_MidAzureMonitor analysieren, die sich hier befindet: **Ereignismanagement** > **Integrationen** > **PushConnectors**. Klicken Sie auf der Seite „Push-Connectors“ auf **Azure Monitor Mid Push Connector**.

Das Standardformat der URL zum Übertragen von Push-Event-Nachrichten von Microsoft Azure an den MID-Server lautet: `http://<MID_Web_Server_User>:<MID_Web_Server_Password>@<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidAzureMonitor`.

Variablen in der Standard-URL

Variable	Beschreibung
MID_Server_IP	IP-Adresse der MID-Webserver-Erweiterung.
{MID_Web_Server_Port}	Listener-Port der MID-Webserver-Erweiterung.
MID_Web_Server_User	Anwendername für die MID-Webserver-Erweiterung.
MID_Web_Server_Password	Passwort des Anwenders des MID-Webservers.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das folgende Verfahren beschreibt die Erfassung von JSON-formatierten Ereignisnachrichten mit Standardauthentifizierung.

Prozedur

1. Stellen Sie im Azure Monitor-Portal sicher, dass die MID-Server-IP über das Azure-Portal und der MID-Restpunkt über Microsoft Azure zugänglich ist, oder installieren Sie MID-Server auf einer Azure-VM, geben Sie die öffentliche Azure-VM-Adresse in der URL an, und lassen Sie das zu mid_web_Server_port in **Azure-VM** > **Netzwerkeinstellungen** > **Regeln für eingehende Ports**.
2. Erstellen Sie eine Aktionsgruppe mit Webhook, und geben Sie wie folgt den REST-Endpunkt an: `http://<MID_Web_Server_User>:<MID_Web_Server_Password>@<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidAzureMonitor`.

   Hinweis: Weitere Informationen zum Hinzufügen eines Webhook zu einer Aktionsgruppe finden Sie unter Aktionsgruppen im Azure-Portal erstellen und verwalten auf der MicrosoftMicrosoft Azure Event Hubs-Dokumentationswebsite.

3. Stellen Sie im Abschnitt „Webhook“ sicher, dass für **Enable the common alert schema** (Gemeinsames Warnungsschema aktivieren) die Option **Ja** ausgewählt ist.
4. Navigieren zu **Warnungen** > **Verwalten Sie Warnungsregeln**.
5. Fügen Sie die Aktionsgruppe mit dem Webhook einer Warnungsregel hinzu.

Nächste Maßnahme

Wenn Sie Warnungsstatusänderungen für die ServiceNow-Instanz von den ServiceNow-Warnungen an das Azure-Portal senden möchten, müssen Sie den bidirektionalen Azure Monitor-Connector aktivieren. Weitere Informationen finden Sie unter Bidirektionalen Azure Monitor-Connector konfigurieren.

Ereignissammlung von BMC TrueSight und BMC TrueSight_v2

Der MID WebService-Eventsammler ermöglicht Ihnen das Erfassen von JSON-formatierten Ereignisnachrichten, die von BMC TrueSight Operations Management (TrueSight), früher bekannt als BMC ProactiveNet Performance Management (BPPM), gesendet werden, und nutzt Ereignis-Stream-Benachrichtigungsfunktionen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Stellen Sie Folgendes sicher:

- Stellen Sie den MID-Server bereit und starten Sie ihn. Weitere Informationen finden Sie unter MID-Server-Konfiguration .
- Konfigurieren Sie einen MID Web Server. Weitere Informationen finden Sie unter MID-Webservererweiterung konfigurieren.
- Konfigurieren und starten Sie den Eventsammler des MID WebService. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Event-Nachrichten im JSON-Format werden von BMC TrueSight gesendet. MID-Server wandelt die gesammelten Ereignisnachrichten um, indem sie sie mithilfe der Skripteinbindung TransformEvents_bmcTrueSight analysieren, die sich hier befindet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignismanagement > **Integrationen** > **Listener-Transformskripts**. Klicken Sie auf der Seite „Listener-Umwandlungsskripts“ auf **TransformEvents_bmcTrueSight**.

Das Standardformat der URL zum Übertragen von Event-Nachrichten von BMC TrueSight auf den MID-Server lautet: `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_bmcTrueSight`.

Das Standardformat der URL zum Übertragen von Ereignisnachrichten von BMC TrueSight_v2 an MID-Server lautet `http://`.<MID_Server_IP> :<MID_Web_Server_Port> /api/mid/em/inbound_event?Transform=TransformEvents_bmcTrueSight_v2 .

Variablen in der Standard-URL

Variable	Beschreibung
MID_Server_IP	IP-Adresse der MID-Webserver-Erweiterung.
{MID_Web_Server_Port}	Listener-Port der MID-Webserver-Erweiterung.
MID_Web_Server_User	Anwendername für die MID-Webserver-Erweiterung.
MID_Web_Server_Password	Passwort des Benutzers der MID-Webserver-Erweiterung. Codieren Sie das Passwort jedoch in BASE64. Beispiel: Wenn das Passwort der MID-Webserver-Erweiterung `admin` ist, verwenden Sie in diesem Fall `YWRtaW4=` als Passwort für MID_Web_Server_Password. Um den BASE64-Wert zu bestimmen, können Sie das Dienstprogramm auf dieser Website verwenden: https://www.base64encode.org/

Das folgende Verfahren beschreibt die Erfassung von JSON-formatierten Event-Nachrichten mit Standardauthentifizierung. Weitere Informationen zu unterstützten Authentifizierungsmethoden finden Sie unter MID-Webservererweiterung konfigurieren.

Prozedur

1. Legen Sie in BMC TrueSight den MID WebService-Eventsammler als Ziel für die BMC TrueSight-Benachrichtigung fest, indem Sie diese Parameter verwenden:

Variablen in der generischen BMC-URL

Variable	Beschreibung
serverHost	Name des BMC TrueSight-Servers.
port	Nummer des BMC TrueSight-Ports.

2. Ersetzen Sie im Nachrichtentext und der generischen BMC-URL die Parameter durch die Werte in der vorherigen Tabelle, und stellen Sie eine Verbindung mit BMC TrueSight her. Verwenden Sie den REST-Ansatz von BMC „Veröffentlichen/Abonnieren“, um ein Stream-Event-Abonnement zu erstellen und Event-Nachrichten im JSON-Format zu senden. Das generische Format der BMC-URL zum Erstellen eines Streamereignisabonnements

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

lautet: `http|https://`<serverHost> :<port> /bppmws/api/stream/subscribe? dataType=event . Beispiel: `http://TrueSight1server:40/bppmws/api/stream/subscribe?dataType=event`.

Ergebnisse

Beispiel für die Zuordnung von Event-Nachrichten zu Event-Feldern in der Tabelle Event (em_event)

Ereignisfeld	Ereignisnachricht
node	mc_host
type	mc_object_class
metric_name	mc_parameter
resource	mc_object
severity	severity
time_of_event	date_reception
description	msg

Example:
Beispiel für den Nachrichtentext.

```
{ action: 'create',
  data:
   { mc_abstracted: [],
     itsm_operational_category3: '',
     mc_object_class: 'CPU',
     source: 'MySource',
     adapter_host: '',
     itsm_operational_category2: '',
     itsm_location: '',
     itsm_operational_category1: '',
     mc_abstraction: [],
     mc_tool_id: '',
     mc_original_priority: 'PRIORITY_1',
     event_handle: '3172',
     mc_modhist: [],
     mc_tool_class: '',
     mc_origin: '',
     mc_tool_uri: '',
     mc_service: '',
     mc_smc_type: '',
     mc_object_owner: '',
     mc_object: 'CPU_0',
     mc_notes: [],
     itsm_model_version: '',
     mc_origin_key: '',
     mc_tool_address: '',
     mc_ueid: 'mc.pncell_bmcswetsom96.1829b8ed.0',
     mc_bad_slot_names: [],
     date: '20161114081525.000000-300',
     itsm_item: '',
     mc_timeout: '0',
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    mc_priority: 'PRIORITY_1',
    itsm_type: '',
    itsm_manufacturer: '',
    mc_tool_key: '',
    itsm_product_name: '',
    mc_smc_impact: 'NOT_ELECTED',
    mc_parameter: 'MEMFreeMem',
    mc_bad_slot_values: [],
    itsm_incident_id: '',
    mc_incident_report_time: '0',
    mc_event_model_version: '1.1.00',
    mc_relationships: '0/0',
    CLASS: 'EVENT',
    mc_using_organization: '',
    mc_tool_sev: '',
    mc_parameter_threshold: '',
    mc_smc_effects: [],
    mc_smc_priority: '0',
    itsm_company: '',
    date_reception: '1479129325',
    mc_smc_alias: 'bmcswetsom96_2',
    pn_detail_diag_count: '0',
    mc_effects: [],
    mc_object_uri: '',
    mc_date_modification: '1479129325',
    mc_incident_time: '0',
    status: 'OPEN',
    msg: 'Free Memory Low',
    pn_detail_diag: '0',
    mc_host: 'bmcswetsom97',
    repeat_count: '69',
    mc_host_address: '',
    mc_tool_suggestion: '',
    mc_using_organization_id: '',
    mc_collectors: [ '1.1', '3.1.1', '4.1', '5.1' ],
    mc_account: '',
    mc_long_msg: '',
    mc_owner: '',
    mc_history: [ 'pncell_bmcswetsom96:3172' ],
    itsm_category: '',
    mc_host_class: '',
    mc_tool_rule: '',
    mc_local_reception_time: '1479129325',
    mc_associations: [],
    mc_relation_source: '',
    mc_propagations: [],
    mc_client_address: '172.16.173.131',
    itsm_incident_status: '',
    mc_tool_time: '0',
    mc_origin_class: '',
    mc_tool: '',
    mc_action_count: '0',
    mc_cause: '0',
    mc_origin_sev: '',
    mc_host_id: '0',
    mc_event_relations: [],
    mc_operations: [],
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    mc_event_category: 'CONFIGURATION_MANAGEMENT',
    pn_device_name: '',
    mc_arrival_time: '1479129325',
    severity: 'OK',
    mc_notification_history: [],
    mc_smc_causes: [],
    mc_acl: [],
    mc_original_severity: 'CRITICAL',
    duration: '0',
    mc_location: 'Unknown',
    mc_smc_id: '',
    mc_parameter_value: '20',
    administrator: '',
    mc_event_subcategory: 'OTHER',
    mc_parameter_unit: '' },
  subscriptionId: 'af18f6ba-a2d3-4574-81c8-7f366ca70ebd',
  type: 'EVENT' }
```

Integrieren Sie Plattform-Ereignisse für Dynatrace .

Integrieren Sie Dynatrace mit Ereignismanagement, indem Sie den Dynatrace -Monitor als authentifizierte Datenquelle hinzufügen.

Welche Authentifizierung verwendet wird

Die folgenden zwei Authentifizierungsmethoden sind verfügbar:

- OAuth-Authentifizierung: Bietet Authentifizierung auf Unternehmensebene, um die Sicherheit Ihrer Unternehmensumgebung zu gewährleisten. Die Authentifizierung erfolgt mit Dynatrace Monitor V1- oder V2-Zugriffstoken. Weitere Informationen finden Sie unter Integrieren Sie Dynatrace mit der OAuth-Authentifizierung.
- Standard-Webhook-Authentifizierung: Bietet einen Basisstandard für die Authentifizierung, ohne dass Dynatrace Active Directory erforderlich ist. Diese Authentifizierung kann besonders für verteilte kleine Teams wie SRE- oder DevOps -Teams nützlich sein. Weitere Informationen finden Sie unter Integrieren Sie Dynatrace mit der Standardauthentifizierung.

Ab Release Xanadu ist für die mit dem Connector bereitgestellten Basissystemregeln, die Sie zuvor nicht verwendet haben (d. h. weder aktiviert noch deaktiviert noch geändert) das Kontrollkästchen **Zusätzliche Abgleichsregeln anwenden** auf wahr festgelegt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie weitere Ereignisregeln oder Automatisierungen mit denselben Filterbedingungen für den Connector ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Integrieren Sie Dynatrace mit der Standardauthentifizierung

Integrieren Sie Dynatrace mit Ereignismanagement, indem Sie der Dynatrace-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Stellen Sie sicher, dass Konfigurationselemente für die von Dynatrace verwalteten Hosts in der Instanz Now Platform vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder Cloud-Discovery erkannt werden.

Erforderliche Rollen: evt_mgmt_integration und web_service_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Umgebung Ereignismanagement für die Sammlung von Ereignissen von Dynatrace, indem Sie Dynatrace als Datenquelle authentifizieren. Legen Sie in Ihrer Dynatrace-Konsole die Now Platform-Instanz mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

Prozedur

1. Definieren Sie in Ihrer Konsole Dynatrace Regeln für die Hostbenennung:

a. Navigieren zu **Einstellungen** > **Überwachung** > **Hostbenennung**.

b. Definieren Sie die Hostbenennungsregeln für jeden Cloud-Anbieter (Azure/AWS/GCP), um ein CI aus ServiceNow eindeutig zu identifizieren.
Dadurch wird sichergestellt, dass die ServiceNow CIs anhand der von Dynatraceempfangenen Nutzlast eindeutig identifiziert werden können.

Hinweis: Für VMware -Computer müssen Sie keine Hostbenennungsregel erstellen, da sie von Dynatrace als physische Server verwaltet werden.

2. Definieren Sie Erkennungsregeln für Anomalien:

a. Navigieren zu **Einstellungen** > **Anomalie-Erkennung** > **Infrastruktur**.

b. Definieren Sie auf der Registerkarte **Hosts** Regeln, wann Warnungen auf den verwalteten Hosts erstellt werden sollen.

3. Definieren Sie die Integrationseinstellungen:

a. Navigieren zu **Einstellungen** > **Integration** > **Problembenachrichtigungen** > **Benachrichtigungen einrichten**.

b. Fügen Sie im Formular „Set up custom integration“ (Benutzerdefinierte Integration einrichten) die Webhook-URL hinzu: `https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=dynatrace`.

c. Geben Sie Benutzername und Passwort des entsprechenden Benutzers ein.

Hinweis: Stellen Sie sicher, dass die Rolle „evt_mgmt_integration“ dem ausgewählten Benutzer zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

d. Fügen Sie im Abschnitt „Custom payload“ (Anwenderdefinierte Nutzlast) die folgende Nutzlaststruktur für die zu generierenden Ereignisse hinzu.

```
{
  "ImpactedEntities": {ImpactedEntities},
  "ImpactedEntity": "{ImpactedEntity}",
  "PID": "{PID}",
  "ProblemDetailsHTML": "{ProblemDetailsHTML}",
  "ProblemDetailsJSONv2": "{ProblemDetailsJSONv2}",
  "ProblemDetailsMarkdown": "{ProblemDetailsMarkdown}",
  "ProblemDetailsText": "{ProblemDetailsText}",
  "ProblemID": "{ProblemID}",
  "ProblemImpact": "{ProblemImpact}",
  "ProblemSeverity": "{ProblemSeverity}",
  "ProblemTitle": "{ProblemTitle}",
  "ProblemURL": "{ProblemURL}",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  "State": "{State}",
  "Tags": "{Tags}"
}
```

Ergebnisse

Die Übertragung von Warnungen aus der -Konsole Dynatrace in das Ereignismanagement-Plugin beginnt. Das Plugin extrahiert Informationen aus der ursprünglichen Dynatrace-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer Now Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen.

Hinweis: Standardmäßig ist die Hostbindung für Dynatrace Ereignisse für alle Anbieter (Azure/AWS/Google) aktiviert. Wenn alle Hosts in der Umgebung mit Cloud-Discovery durch die Bereitstellung von Anmeldeinformationen erkannt werden und sich erkannte Ressourcen in der Liste cmdb_ci_vm_object befinden, tritt die VM-Bindung möglicherweise nicht auf. Um dieses Problem zu beheben, müssen Sie die Event-Regel **Dynatrace - Allgemein** aktivieren. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Integrieren Sie Dynatrace mit der OAuth-Authentifizierung

Integrieren Sie Dynatrace mit Ereignismanagement, indem Sie Dynatrace V1- oder V2-Token im Dynatrace -Monitor authentifizieren.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Das Plugin „Ereignismanagement“ muss in der Now Platform-Instanz installiert sein.

Vergewissern Sie sich, dass Konfigurationselemente für die von Dynatrace verwalteten Hosts in ServiceNow vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder cloudbasierter Erkennung erkannt werden.

Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Die IntegrationDynatrace von mit der OAuth-Authentifizierung ist ab dem Plattform-Release Washington DC oder höher verfügbar.

Prozedur

1. Konfiguration in der Instanz ServiceNow

   a. Erstellen Sie die Systemeigenschaft *glide.oauth.inbound.client.credential.grant_type.enabled*, um den Gewährungstyp für Client-Anmeldeinformationen für eingehende OAuth-Integrationen zu verwenden.

      - Typ: true | false
      - Wert: true

   b. Erstellen Sie einen OAuth-Entitätsendpunkt, damit Clients auf die Instanz zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** und wählen Sie **Neu**aus.

ii. Wählen Sie auf der Interceptor-Seite **OAuth-API-Endpunkt für externe Clients erstellen aus**, und füllen Sie das Formular aus.

iii. Um einen OAuth-Client-Datensatz zu erstellen, wählen Sie **Absenden**aus.

c. Fügen Sie dem erstellten OAuth-Client-Datensatz den OAuth-Anwendungsanwender und den Standardgewährungstyp hinzu.

i. Fügen Sie im Formular „OAuth-Entität“ die Felder **OAuth-Anwendungsbenutzer** und **Standardgewährungstyp** hinzu, um den Gewährungstyp „Client-Anmeldeinformationen“ für eingehende OAuth-Integrationen zu verwenden.

ii. Öffnen Sie den erstellten OAuth-Client-Datensatz.

iii. Wählen Sie im Seiten-Header das Symbol „ **Weitere** Optionen“ aus.

iv. Auswahlvorgang **Konfigurieren** > **Formularlayout**

v. Fügen Sie auf der Seite „Formularlayout“ **OAuth-Anwendungsbenutzer und Standardgewährungstyp** aus der Liste der Felder hinzu.

vi. **Speichern** oder **aktualisieren Sie** das Formular.

vii. Wählen Sie im Feld **OAuth-Anwendungsbenutzer** den Benutzer aus.

Der Anwender muss über die Rolle evt_mgmt_integration verfügen, die zum Erstellen der von Dynatracegesendeten Ereignisse verwendet wird.

Hinweis: Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

viii. Legen Sie den Wert im Feld **„Standard-Gewährungstyp“** auf **Client-Anmeldeinformationen**fest.

2. Definieren Sie in der Konsole Dynatrace die Integrationseinstellungen.

a. Navigieren zu **Einstellungen** > **Integration** > **Problembenachrichtigungen** > **Benachrichtigungen einrichten**.

b. Geben Sie im Formular „Anwenderdefinierte Integration einrichten“ die Webhook-URL ein.

```
https://<Instanzname>.service-now.com/api/sn_em_connector/em/inbound_event?source=dynatrace
```

c. Aktivieren Sie **OAuth 2.0 für Authentifizierung verwenden**.

d. Führen Sie im Abschnitt „OAuth 2.0-Anmeldeinformationen“ die folgenden Schritte aus.

i. Geben Sie die Zugriffs-Token-URL als `https:// an.`<instance_name> .service-now.com/oauth_token.do

ii. Geben Sie den Wert für die **Client-ID** mit der Client-ID des in der Instanz ServiceNow erstellten OAuth-Entitätsclients an.

iii. Geben Sie für „Geheimer Clientschlüssel“ den geheimen Clientschlüssel des in der Instanz ServiceNow erstellten OAuth-Entitätsclients an.

iv. Wählen Sie **Speichern**.

e. Fügen Sie im Abschnitt „Custom payload“ (Anwenderdefinierte Nutzlast) die folgende Nutzlaststruktur für die zu generierenden Ereignisse hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
{
  "ImpactedEntities": {ImpactedEntities},
  "ImpactedEntity": "{ImpactedEntity}",
  "PID": "{PID}",
  "ProblemDetailsHTML": "{ProblemDetailsHTML}",
  "ProblemDetailsJSONv2": "{ProblemDetailsJSONv2}",
  "ProblemDetailsMarkdown": "{ProblemDetailsMarkdown}",
  "ProblemDetailsText": "{ProblemDetailsText}",
  "ProblemID": "{ProblemID}",
  "ProblemImpact": "{ProblemImpact}",
  "ProblemSeverity": "{ProblemSeverity}",
  "ProblemTitle": "{ProblemTitle}",
  "ProblemURL": "{ProblemURL}",
  "State": "{State}",
  "Tags": "{Tags}"
}
```

Ergebnisse

Die Übertragung von Warnungen von Dynatrace -Agents in das Plugin Ereignismanagement „ beginnt. Das Plugin extrahiert Informationen aus der ursprünglichen Dynatrace-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer Instanz Now Platform zu Alle Ereignisse, um die Ereignisse anzuzeigen.

Hinweis: Standardmäßig ist die Hostbindung für Dynatrace Ereignisse für die Anbieter (AWS/Azure/GCP) aktiviert. Wenn alle Hosts in der Umgebung mit Cloud-Discovery durch die Bereitstellung von Anmeldeinformationen erkannt werden und sich erkannte Ressourcen in der Liste cmdb_ci_vm_object befinden, tritt die VM-Bindung möglicherweise nicht auf. Um dieses Problem zu beheben, müssen Sie die Ereignisregel Dynatrace – Allgemeines Ereignis aktivieren. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Events der New Relic-Plattform integrieren

Integrieren Sie New Relic in Ereignismanagement, indem Sie in der alten und neuen New Relic-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

Vergewissern Sie sich, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus New Relic, indem Sie New Relic als Datenquelle authentifizieren. Legen Sie Ihre Instanz Now Platform mit einem Standard-Webhook als REST-Endpunkt fest. Führen Sie Verfahrensschritt 1 für die neue Konsole aus. Führen Sie Verfahrensschritt 2 für die alte Konsole aus.

Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Ereignisregeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Zuordnung** anwenden Checkbox für Regeln auf „wahr“ gesetzt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie mehr Ereignisregeln oder Automatisierung mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Für die neue Konsole:

   a. Erstellen Sie ein Ziel.

      i. Navigieren zu**Warnungen und KI** > **Ziele**.

      ii. Wählen Sie im Abschnitt**Ziele hinzufügen**den Kanaltyp**Webhook**aus.

      iii. Geben Sie im Feld**Webhook-Name**den Webhook-Namen ein.

      iv. Geben Sie im Feld**Endpunkt-URL Folgendes**ein:`https://`<InstanceName> .service-now.com/api/sn_em_connector/em/inbound_event?source=newrelic

      v. Geben Sie im Abschnitt**Basisauthentifizierung**Ihren Anwendernamen und Ihr Passwort ein.

      > **Hinweis:** Stellen Sie sicher, dass dem ausgewählten Anwender die Rolle evt_mgmt_integration zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

      vi. Wählen Sie**Ziel speichern**.

   b. Erstellen Sie eine Richtlinie.

      i. Navigieren zu**Warnungen und KI** > **Warnungsbedingungen und -richtlinien**.

      ii. Wählen Sie**die Richtlinie Neue Warnung**aus, und definieren Sie eine Richtlinie.

      iii. Wählen Sie**Benachrichtigungen einrichten**.

      iv. Wählen Sie im Abschnitt**„Kanal hinzufügen“die Option Webhook**aus, und wählen Sie dann das Ziel aus, das Sie im vorherigen Unterschritt erstellt haben.

      v. Fügen Sie im Abschnitt**Nutzlastvorlage**die folgende JSON-Nutzlast ein.

```
{ "account_id": {{nrAccountId}}, "account_name": {{json
 accumulations.tag.account.[0]}}, "closed_violations_count":
 {{closedIncidentsCount}}, "open_violations_count":
 {{openIncidentsCount}}, "condition_description": "{{escape
 accumulations.conditionDescription.[0]}}", "condition_family_id":
 {{accumulations.conditionFamilyId.[0]}}, "condition_name":
 "{{escape accumulations.conditionName.[0]}}", "current_state":
 {{json state}}, "details": {{json issueTitle}}, "duration":
 {{#if issueDurationMs}}{{issueDurationMs}}{{else}}0{{/if}},
 "event_type": "INCIDENT", "incident_acknowledge_url":
 {{json issueAckUrl}}, "incident_id": {{json issueId}},
 "incident_url": {{json issuePageUrl}}, "metadata":
 { {{#if locationStatusesObject}}"location_statuses":
 {{json locationStatusesObject}},{{/if}} {{#if
 accumulations.metadata_entity_type}}"entity.type": {{json
 accumulations.metadata_entity_type.[0]}},{{/if}} {{#if
 accumulations.metadata_entity_name}}"entity.name": {{json
 accumulations.metadata_entity_name.[0]}},{{/if}} "section":
 "metadata" }, "owner": {{json owner}}, "policy_name": {{json
 accumulations.policyName.[0]}}, "policy_url": {{json policyUrl}},
 "runbook_url": {{json accumulations.runbookUrl.[0]}}, "severity":
 {{json priority}}, "targets": [ { "id": "{{labels.targetId.[0]}}",
 "name": "{{#if accumulations.targetName}}{{escape
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 accumulations.targetName.[0]}}{{else if
 entitiesData.entities}}{{escape
 entitiesData.entities.[0].name}}{{else}}N/A{{/if}}",
 "link": "{{issuePageUrl}}", "product":
 "{{accumulations.conditionProduct.[0]}}", "type": "{{#if
 entitiesData.types.[0]}}{{entitiesData.types.[0]}}{{else}}N/A{{/if}
}", "labels": { {{#each accumulations.rawTag}}"{{escape @key}}":
 {{#if this.[0]}}{{json this.[0]}}{{else}}"empty"{{/if}}{{#unless
 @last}},{{/unless}}{{/each}} } } ], "timestamp":
 {{updatedAt}}, "violation_callback_url": {{json issuePageUrl}},
 "violation_chart_url": {{json violationChartUrl}} }
```

vi. Wählen Sie**Testbenachrichtigung senden aus**,um das Testereignis in Ihrer Instanz ServiceNow abzurufen.

vii. Wählen Sie**Nachricht speichern**aus.

viii. Wählen Sie**Workflow aktivieren**aus, um den Workflow zu aktivieren.

c. Erstellen Sie Warnungsbedingungen, die auf die Richtlinie angewendet werden sollen:

i. Navigieren zu**Warnungen und KI** > **Warnungsbedingungen und -richtlinien**.

ii. Wählen Sie**Warnungsbedingung erstellen aus**, definieren Sie die erforderlichen Warnungsdetails, und fügen Sie sie der Richtlinie hinzu, die Sie im vorherigen Schritt erstellt haben.

iii. Wählen Sie**Bedingung speichern**aus.

2. Für die alte Konsole:

a. Erstellen Sie einen Benachrichtigungskanal.

i. Navigieren zu**Warnungen und KI** > **Benachrichtigungskanäle**.

ii. Wählen Sie auf der Registerkarte**Kanaldetails**den Kanaltyp**Webhook**aus.

iii. Geben Sie im Textfeld**Basis-URL**Folgendes ein:`https://`<InstanceName> .service-now.com/api/sn_em_connector/em/inbound_event?source=newrelic

iv. Geben Sie im Abschnitt „Basisauth.“ Benutzername und Passwort des entsprechenden Benutzers ein.

> **Hinweis:** Stellen Sie sicher, dass dem ausgewählten Anwender die Rolle evt_mgmt_integration zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

v. Wählen Sie im Abschnitt**Custom Payload (Anwenderdefinierte Nutzlast**)**Anwenderdefinierte Nutzlast hinzufügen**und anschließend den Nutzlasttyp**JSON**aus.

vi. Fügen Sie die folgende JSON-Payload in**Custom Payload (Anwenderdefinierte Payload)**ein.

```
{ "account_id": "$ACCOUNT_ID", "account_name":
 "$ACCOUNT_NAME", "closed_violations_count_critical":
 "$CLOSED_VIOLATIONS_COUNT_CRITICAL",
 "closed_violations_count_warning":
 "$CLOSED_VIOLATIONS_COUNT_WARNING", "condition_description":
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
"$DESCRIPTION", "condition_family_id": "$CONDITION_FAMILY_ID",
"condition_name": "$CONDITION_NAME", "current_state":
"$EVENT_STATE", "details": "$EVENT_DETAILS",
"duration": "$DURATION", "event_type": "$EVENT_TYPE",
"incident_acknowledge_url": "$INCIDENT_ACKNOWLEDGE_URL",
"incident_id": "$INCIDENT_ID", "incident_url": "$INCIDENT_URL",
"metadata": "$METADATA", "open_violations_count_critical":
"$OPEN_VIOLATIONS_COUNT_CRITICAL", "open_violations_count_warning":
"$OPEN_VIOLATIONS_COUNT_WARNING", "owner": "$EVENT_OWNER",
"policy_name": "$POLICY_NAME", "policy_url": "$POLICY_URL",
"runbook_url": "$RUNBOOK_URL", "severity": "$SEVERITY", "targets":
"$TARGETS", "timestamp": "$TIMESTAMP", "violation_callback_url":
"$VIOLATION_CALLBACK_URL", "violation_chart_url":
"$VIOLATION_CHART_URL" }
```

b. Erstellen Sie eine Richtlinie.

i. Navigieren zu**Warnungen und KI** > **Richtlinien**.

ii. Wählen Sie**die Richtlinie Neue Warnung**aus, und definieren Sie eine Richtlinie.

iii. Wählen Sie im Abschnitt**„Benachrichtigungskanäle“Hinzufügen**, wählen Sie**Webhook**aus, und wählen Sie dann den Kanal aus, den Sie im vorherigen Schritt erstellt haben.

c. Erstellen Sie Warnungsbedingungen, die auf die Richtlinie angewendet werden sollen:

i. Navigieren zu**Infrastruktur** > **Einstellungen** > **Warnungen**.

ii. Wählen Sie**Warnungsbedingung erstellen aus**, definieren Sie die erforderlichen Warnungsdetails, und fügen Sie sie der Richtlinie hinzu, die Sie im vorherigen Schritt erstellt haben.

iii. Wählen Sie**Erstellen**aus.

Ergebnisse

Die Übertragung von Warnungen aus der New Relic-Konsole in das Plugin Event Management beginnt. Das Plugin extrahiert die Informationen aus der ursprünglichen New Relic-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer Instanz Now Platform zu**Alle Ereignisse**, um die Ereignisse anzuzeigen.

Hinweis: Standardmäßig ist die Hostbindung für New Relic-Events für alle Provider (Azure /AWS/GCP) aktiviert. Wenn alle Hosts in der Umgebung mit Cloud-Discovery durch die Bereitstellung von Anmeldeinformationen erkannt werden und sich erkannte Ressourcen in der Liste cmdb_ci_vm_object befinden, tritt die VM-Bindung möglicherweise nicht auf. Um dieses Problem zu beheben, müssen Sie die Ereignisregel**„New Relic – Allgemein“**aktivieren. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Integrieren Sie New Relic in das REST-API-Schlüsseltoken

Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und erhöht die betriebliche Effizienz.

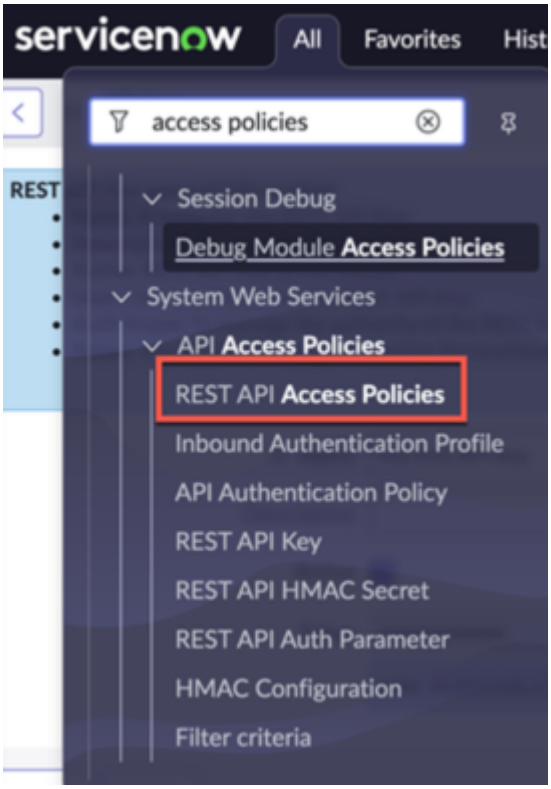
Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**.



2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Hinweis: Der Anwender muss mit der Rolle evt_mgmt_integration erstellt werden. Erstellen Sie in der Tabelle „sys_user“ eine neue, um sie hier zu verwenden, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST-API-Schlüssels zu verwalten.
Token	Der von Now Platformgenerierte REST-API-Schlüssel. Kopieren Sie den Schlüssel,

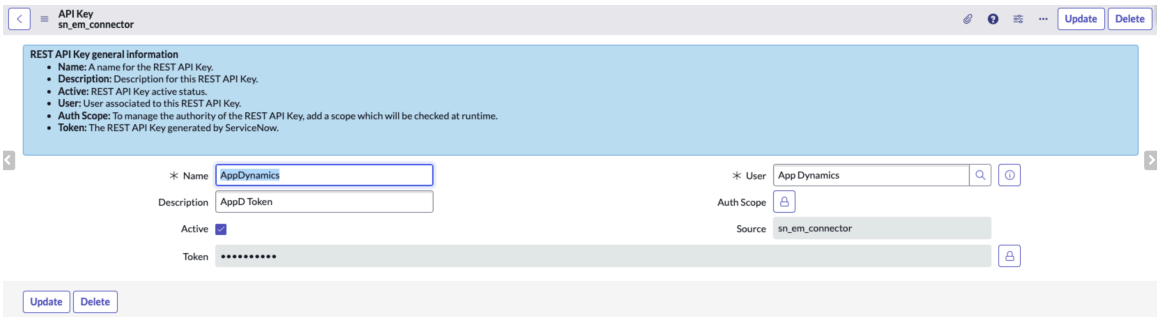
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.
Ablauf	Zeitpunkt, nach dem die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie hinzu: UserAccount.
5. Verwenden Sie das Formularmenü, und wählen Sie **Speichern**aus.

   Das System generiert ein Token und speichert es im Feld **Token**. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie den Inhalt, der unter dem Feld angezeigt wird. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Catchpoint-Ereignisse integrieren

Integrieren Sie Catchpoint mit Ereignismanagement, indem Sie auf der Catchpoint-Plattform einen Warnungs-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Ereignissen aus Catchpoint, indem Sie Catchpoint als Datenquelle authentifizieren. Legen Sie auf der Catchpoint-Plattform die Now Platform mit einem Webhook als REST-Endpunkt fest.

Prozedur

1. Erstellen Sie auf der Catchpoint-Plattform ein Warnungs-Webhook-Ziel.

   a. Melden Sie sich bei der Catchpoint-Plattform an.

   b. Navigieren zu **Catchpoint** > **Einstellung** > **API** > **Warnungsdaten-Webhook** um den Webhook-Endpunkt festzulegen.

   c. Geben Sie im API Alert Webhook (API-Warnungs-Webhook) die folgenden Details an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „API Alert Webhook“ (API-Warnungs-Webhook)

Feld	Wert
Name	Beliebiger Name basierend auf Ihren Anforderungen.
URL	Das Standardformat der URL zum Übertragen von Ereignissen von Catchpoint an die Now Platform-Instanz ist `https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=catchpoint`.
On Failure Alert (Bei Fehlerwarnung)	E-Mail-Adresse für den API-Warnungs-Webhook.
Notification Trigger (Benachrichtigungsauslöser)	Wählen Sie diesen je nach Ihren Anforderungen aus. Der Standardwert ist 3.
Add the following headers (Folgende Header hinzufügen)	▪ Autorisierung: **Basic {Base 64 | username:password}** ▪ Inhaltstyp: **application/json**
Format	Wählen Sie **Vorlage** aus, und fügen Sie die folgende Vorlage hinzu: `{ "Source": "CatchPoint", "severity": "${notificationLevelId}", "alertType": "${AlertType}", "time_of_event": "${alertCreateDateUtc(YYYY-MM-DD HH:MI:SS)}", "monitorType": "${Switch(${MonitorTypeId},'0', 'IE','2', 'Object','3','Emulated','8', 'Ping','9', 'Tracert','10', 'DNS-Traversal','11', 'Ping-TCP','12', 'DNS-Exp', '13','DNS-Direct', '14','Tracert-UDP', '15', 'Port-TCP','16', 'FTP','17', 'Data-Push-API','18', 'Chrome','19', 'Playback', '20', 'Playback-Mobile', '21', 'SMTP', '22', 'Port-UDP', '23', 'Ping-UDP', '24', 'Streaming', '25', 'API', '26', 'Mobile', '27', 'SFTP', '28', 'SSH', '29', 'Tracert-TCP')}", "testName": "${TestName}", "testId": "${TestId}", "testUrl": "${TestUrl}",`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	"testPath": "${testPath}", "testLink": "${testLink}", "productName": "${ProductName}", "clientId": "${ClientId}", "productId": "${productId}", "nodeName":"${nodeDetails("${nodeName}")}", "nodeClientServerAddress":"${nodeDetails(\"${NodeClientAddress},\"),}", "nodeServerAddress": "${nodeDetails(\"${nodeServerAddress},\"),}", "Labels" : "${testLabels}", "addtionalInformation": "Test initial URL: ${testUrl}\n\nAlert type: ${AlertType}\n\nScatter Chart: ${scatterplotChartURL}\n\nWaterfall Chart: ${waterfallChartURL}\n\nTest properties: ${testLink}\n\nTest time of run / Test time of alert (Central Time): ${reportDateLocal(YYYY-MM-DD HH:MI:SS)} / ${alertCreateDateLocal(YYYY-MM-DD HH:MI:SS)}"}

2. Erstellen Sie für die Tests zur HTTP-Endpunktüberwachung in der ServiceNow-Instanz ein CI (Configuration Item).

   Hinweis: Der Catchpoint-Connector bietet Unterstützung für mehrere Arten von Überwachungstests wie Endpunkt, Netzwerk und andere. Die folgenden Schritte gelten nur für die Tests zur HTTP-Endpunktüberwachung.

   a. Navigieren zu **Konfiguration** > **CI-Klassen Manager**.

   b. Klicken Sie auf **Hierarchie** und suchen Sie nach **HTTP(S)-Endpunkt**.

   c. Wählen Sie im Feld „CI-Typ“ **cmdb_ci_endpoint_http** aus.
   Wenn die Services nicht modelliert werden, sollten Sie die CIs manuell unter der Tabelle [cmdb_ci_endpoint_http] hinzufügen. Außerdem sollte der manuelle Endpunkt vor der automatischen Erkennung von Services entfernt werden. Für CI-Bindungen anderer Typen von Tests können Sie Ereignisregeln basierend auf den jeweiligen Anforderungen erstellen.

Ergebnisse
Die Übertragung von Warnungen vom Catchpoint-Connector in das Plugin „Event Management“ beginnt. Aus folgender Tabelle ist ersichtlich, wie die Zuordnung des Catchpoint-Schweregrads in die Zuordnung im ServiceNow-System übertragen wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vergleich der Schweregradstufen zwischen Catchpoint und ServiceNow

Catchpoint-Schweregrad	ServiceNow-Schweregrad
0	Warnung
1	Kritisch
2/3	Leeren

Integrieren Sie Plattform-Ereignisse für Datadog .

Integrieren Sie Datadog mit Ereignismanagement, indem Sie der Datadog-Konsole einen Standard-Webhook hinzufügen.

Welche Authentifizierung verwendet wird

Die folgenden zwei Authentifizierungsmethoden sind verfügbar:

- OAuth-Authentifizierung: Bietet Authentifizierung auf Unternehmensebene, um die Sicherheit Ihrer Unternehmensumgebung zu gewährleisten. Die Authentifizierung erfolgt mit Datadog Monitor V1- oder V2-Zugriffstoken. Weitere Informationen finden Sie unter Integrieren Sie Datadog mit der OAuth-Authentifizierung.
- Standard-Webhook-Authentifizierung: Bietet einen Basisstandard für die Authentifizierung, ohne dass Datadog Active Directory erforderlich ist. Diese Authentifizierung kann besonders für verteilte kleine Teams wie SRE- oder DevOps -Teams nützlich sein. Weitere Informationen finden Sie unter Integrieren Sie Datadog mit der Standardauthentifizierung.

Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Ereignisregeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Zuordnung** anwenden Checkbox für Regeln auf „wahr“ gesetzt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie mehr Ereignisregeln oder Automatisierung mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Integrieren Sie Datadog mit der Standardauthentifizierung

Integrieren Sie Datadog mit Ereignismanagement, indem Sie der Datadog-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

- Erforderliche Rolle: evt_mgmt_integration
- Das Plugin „Ereignismanagement“ muss in der Now Platform-Instanz installiert sein.
- Vergewissern Sie sich, dass Konfigurationselemente für die von Datadog verwalteten Hosts in ServiceNow vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder cloudbasierter Erkennung erkannt werden.

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Datadog. Legen Sie in Ihrer Datadog-Konsole die Now Platform-Instanz mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Fügen Sie in der -Konsole Datadog Cloud-Provider-Tags hinzu:

a. Navigieren zu **Menü** > **Infrastruktur** > **Infrastrukturliste**

b. Klicken Sie für die VM, auf der der Agent Datadog installiert ist, **auf Untersuchen**.

c. Klicken Sie auf **Tags bearbeiten**. und fügen Sie das Tag *cloud_provider* hinzu. Dem Tag sollte ein Suffix mit dem Wert **aws**, **azure** oder **gcp** vorangestellt werden, um die AWS-, Microsoft Azure- oder Google Cloud Platform (GCP)-Anbieteroptionen zu identifizieren. Beispiel: cloud_provider:aws

d. Klicken Sie auf **Tags speichern**, um das neue Tag zu speichern.

Hinweis: Datadog fügt standardmäßig das Tag *„cloud_provider* "hinzu, wenn die Azure- und Google-Integration auf dem Agent Datadog installiert ist. Tags können auch auf Cloud-Provider-Ebene hinzugefügt werden. Datadog sammelt alle auf VM-Ebene definierten Tags in der Cloud.

2. Fügen Sie in der Konsole Datadog einen Webhook hinzu:

a. Navigieren zu **Menü** > **Integration** > **Integrationen**, und suchen Sie nach Webhooks.

b. Erstellen Sie einen Webhook, der die Benutzer-ID und das Passwort des ServiceNow-Benutzers im Endpunkt enthält.
Verwenden Sie beispielsweise `https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=datadog`.

Hinweis: Stellen Sie sicher, dass dem ausgewählten Benutzer die Rolle „evt_mgmt_integration“ zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

c. Fügen Sie ihn in der folgenden Nutzlaststruktur hinzu.

```
{
    "body": "$EVENT_MSG",
    "last_updated": "$LAST_UPDATED",
    "event_type": "$EVENT_TYPE",
    "title": "$EVENT_TITLE",
    "date": "$DATE",
    "org": {
        "id": "$ORG_ID",
        "name": "$ORG_NAME"
    },
    "id": "$ID",
    "alert_id": "$ALERT_ID",
    "alert_metric": "$ALERT_METRIC",
    "metric_namespace": "$METRIC_NAMESPACE",
    "alert_priority": "$ALERT_PRIORITY",
    "alert_transition": "$ALERT_TRANSITION",
    "alert_status": "$ALERT_STATUS",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    "alert_title": "$ALERT_TITLE",
    "alert_type": "$ALERT_TYPE",
    "host_name": "$HOSTNAME",
    "priority": "$PRIORITY",
    "tags": "$TAGS",
    "alert_scope": "$ALERT_SCOPE"
}
```

3. Definieren Sie in der Konsole Datadog Regeln:
   a. Navigieren zu **Menü** > **Monitore** > **Verwalten Sie Überwachungen**, und konfigurieren Sie Regeln, wann ein Problem von Datadog auf den verwalteten Hosts erstellt werden soll.
   b. Wählen Sie im Abschnitt **Notify your team** (Team benachrichtigen) den Webhook aus, für den das Problem gemeldet werden soll.

Ergebnisse

Die Übertragung von Warnungen von Service Desk-Mitarbeitern Datadog in das Ereignismanagement-Plugin beginnt. Das Plugin extrahiert Informationen aus der ursprünglichen Datadog-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer Now Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen.

Hinweis: Standardmäßig ist die Hostbindung für Datadog Ereignisse für die Anbieter (AWS/Azure/GCP) aktiviert. Wenn alle Hosts in der Umgebung mit Cloud-Discovery durch die Bereitstellung von Anmeldeinformationen erkannt werden und sich erkannte Ressourcen in der Liste cmdb_ci_vm_object befinden, tritt die VM-Bindung möglicherweise nicht auf. Um dieses Problem zu beheben, müssen Sie die Event-Regel **Datadog - Allgemein** aktivieren. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Integrieren Sie Datadog mit der OAuth-Authentifizierung

Integrieren Sie Datadog mit Ereignismanagement, indem Sie Datadog V1- oder V2-Token im Datadog -Monitor authentifizieren.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Das Plugin „Ereignismanagement“ muss in der Now Platform-Instanz installiert sein.

Vergewissern Sie sich, dass Konfigurationselemente für die von Datadog verwalteten Hosts in ServiceNow vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder cloudbasierter Erkennung erkannt werden.

Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Die IntegrationDatadog von mit der OAuth-Authentifizierung ist ab dem Plattform-Release Washington DC oder höher verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Konfiguration in der Instanz ServiceNow

   a. Erstellen Sie die Systemeigenschaft *glide.oauth.inbound.client.credential.grant_type.enabled*, um den Gewährungstyp für Client-Anmeldeinformationen für eingehende OAuth-Integrationen zu verwenden.

      - Typ: true | false
      - Wert: true

   b. Erstellen Sie einen OAuth-Entitätsendpunkt, damit Clients auf die Instanz zugreifen können.

      i. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** und wählen Sie **Neu**aus.

      ii. Wählen Sie auf der Interceptor-Seite **OAuth-API-Endpunkt für externe Clients erstellen aus**, und füllen Sie das Formular aus.

      iii. Um einen OAuth-Client-Datensatz zu erstellen, wählen Sie **Absenden**aus.

   c. Fügen Sie dem erstellten OAuth-Client-Datensatz den OAuth-Anwendungsanwender und den Standardgewährungstyp hinzu.

      i. Fügen Sie im Formular „OAuth-Entität“ die Felder **OAuth-Anwendungsbenutzer** und **Standardgewährungstyp** hinzu, um den Gewährungstyp „Client-Anmeldeinformationen“ für eingehende OAuth-Integrationen zu verwenden.

      ii. Öffnen Sie den erstellten OAuth-Client-Datensatz.

      iii. Wählen Sie im Seiten-Header das Symbol „ **Weitere** Optionen“ aus.

      iv. Auswahlvorgang **Konfigurieren** > **Formularlayout**

      v. Fügen Sie auf der Seite „Formularlayout“ **OAuth-Anwendungsbenutzer und Standardgewährungstyp** aus der Liste der Felder hinzu.

      vi. **Speichern** oder **aktualisieren Sie** das Formular.

      vii. Wählen Sie im Feld **OAuth-Anwendungsbenutzer** den Benutzer aus.

      Der Anwender muss über die Rolle evt_mgmt_integration verfügen, die zum Erstellen der von Datadoggesendeten Ereignisse verwendet wird.

      Hinweis: Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

      viii. Legen Sie den Wert im Feld **„Standard-Gewährungstyp“** auf **Client-Anmeldeinformationen**fest.

2. Fügen Sie in der -Konsole Datadog Cloud-Provider-Tags hinzu.

   a. Navigieren zu **Menü** > **Infrastruktur** > **Infrastrukturliste**.

   b. Wählen Sie **Untersuchen** für die VM, auf der der Agent Datadog installiert ist.

   c. Wählen Sie **Tags bearbeiten aus**, und fügen Sie das Tag cloud_provider hinzu.

   Dem Tag muss der Wert „aws“, „azure“ oder „gcp“ vorangestellt werden, um die Anbieteroptionen AWS, Microsoft Azure oder Google Cloud Platform (GCP) zu identifizieren. Beispiel: cloud_provider:aws.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie **Tags speichern**aus.

> **Hinweis:** Datadog fügt standardmäßig das Tag „cloud_provider“ hinzu, wenn die Azure- und Google-Integration auf dem Agent Datadog installiert ist. Tags können auch auf Cloud-Provider-Ebene hinzugefügt werden. Datadog sammelt alle auf VM-Ebene definierten Tags in der Cloud.

3. Fügen Sie in der Datadog-Konsole einen Webhook hinzu:

a. Navigieren zu **Menü** > **Integration** > **Integrationen** und suchen Sie nach Webhooks.

b. Wählen Sie auf der Webhook-Kachel **Konfigurieren**aus.

c. Wählen Sie die Registerkarte **Authentifizierungsmethoden** und dann **Neue Authentifizierungsmethode**aus.

d. Geben Sie den Namen ein, und wählen Sie als Protokoll **OAuth 2.0-Client-Anmeldeinformationen**aus.

e. Geben Sie die Zugriffs-Token-URL als `https:// an.`<instance_name> .service-now.com/ oauth_token.do

f. Geben Sie den Wert für die **Client-ID** mit der Client-ID des in der Instanz ServiceNow erstellten OAuth-Entitätsclients an.

g. Geben Sie für „Geheimer Clientschlüssel“ den geheimen Clientschlüssel des in der Instanz ServiceNow erstellten OAuth-Entitätsclients an.

h. Wählen Sie **Speichern**.

i. Erstellen Sie die Webhook-URL als

```
https://<Instanzname>.service-now.com/api/sn_em_connector/
em/inbound_event?source=datadog
```

j. Wählen Sie die in den vorherigen Schritten erstellte OAuth-Methode in der Dropdown-Liste „AuthMethod“ aus.

k. Fügen Sie ihn in der folgenden Nutzlaststruktur hinzu.

```
{
    "body": "$EVENT_MSG",
    "last_updated": "$LAST_UPDATED",
    "event_type": "$EVENT_TYPE",
    "title": "$EVENT_TITLE",
    "date": "$DATE",
    "org": {
        "id": "$ORG_ID",
        "name": "$ORG_NAME"
    },
    "id": "$ID",
    "alert_id": "$ALERT_ID",
    "alert_metric": "$ALERT_METRIC",
    "metric_namespace": "$METRIC_NAMESPACE",
    "alert_priority": "$ALERT_PRIORITY",
    "alert_transition": "$ALERT_TRANSITION",
    "alert_status": "$ALERT_STATUS",
    "alert_title": "$ALERT_TITLE",
    "alert_type": "$ALERT_TYPE",
    "host_name": "$HOSTNAME",
    "priority": "$PRIORITY",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    "tags": "$TAGS",
    "alert_scope": "$ALERT_SCOPE"
}
```

Ergebnisse

Die Übertragung von Warnungen von Datadog -Agents in das Plugin Ereignismanagement „ beginnt. Das Plugin extrahiert Informationen aus der ursprünglichen Datadog-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer Instanz Now Platform zu Alle Ereignisse, um die Ereignisse anzuzeigen.

Hinweis: Standardmäßig ist die Hostbindung für Datadog Ereignisse für die Anbieter (AWS/Azure/GCP) aktiviert. Wenn alle Hosts in der Umgebung mit Cloud-Discovery durch die Bereitstellung von Anmeldeinformationen erkannt werden und sich erkannte Ressourcen in der Liste cmdb_ci_vm_object befinden, tritt die VM-Bindung möglicherweise nicht auf. Um dieses Problem zu beheben, müssen Sie die Ereignisregel Datadog – Allgemeines Ereignis aktivieren. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Google Cloud Platform (GCP)-Events integrieren

Integrieren Sie Google Cloud Platform (GCP) mit Ereignismanagement, indem Sie der GCP-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

- Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.
- Das Plugin „Ereignismanagement“ muss in der Now Platform-Instanz installiert sein.
- Vergewissern Sie sich, dass Konfigurationselemente für die von GCP verwalteten Hosts in ServiceNow vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder cloudbasierter Erkennung erkannt werden.
- Das Plugin „Ereignismanagement Connector“ unterstützt nur GCP-Warnungsdaten im JSON 1.2-Format.
- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus GCP. Legen Sie in Ihrer GCP-Konsole die Now Platform-Instanz mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Ereignisregeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Zuordnung** anwenden Checkbox für Regeln auf „wahr“ gesetzt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie mehr Ereignisregeln oder Automatisierung mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Fügen Sie in der GCP-Konsole einen Webhook hinzu:

   a. Navigieren zu **Überwachung** > **Warnung**und klicken Sie auf **Benachrichtigungskanäle bearbeiten**.

   b. Klicken Sie im Abschnitt „Webhooks“ auf **Neu hinzufügen**.

   c. Aktivieren Sie das Kontrollkästchen **Use HTTP Basic Auth (HTTP-Standardauthentifizierung verwenden)**, und geben Sie Benutzername und Passwort des entsprechenden ServiceNow-Benutzers ein.

   > **Hinweis:** Stellen Sie sicher, dass dem ausgewählten Benutzer die Rolle „evt_mgmt_integration“ zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

   d. Geben Sie die Endpunkt-URL ein.
   Verwenden Sie beispielsweise`https://`.<instance-name> .service-now.com/api/sn_em_connector/em/inbound_event?source=googlemonitor

2. Erstellen Sie in der GCP-Konsole eine Warnungsrichtlinie.
   a. Navigieren zu **Überwachung** > **Warnung**und wählen Sie **Richtlinie erstellen**.
   b. Konfigurieren Sie Richtlinienbedingungen, die Warnungen auslösen, wenn ein Verstoß gegen die Bedingungen vorliegt.
   c. Wählen Sie den Webhook aus, für den das Problem gemeldet werden soll.

   > **Hinweis:** Wenn Sie einen Incident aus der Warnung direkt in der Konsole GCP öffnen müssen, navigieren Sie zu **Schnelle Antwort (in Warnung)** > **Incident in GCP-Konsole anzeigen**.

Ergebnisse

Die Übertragung von Warnungen von GCP in das Plugin Event Management beginnt. Das Plugin extrahiert Informationen aus der ursprünglichen GCP-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer Instanz Now Platform zu**Alle Ereignisse**, um die Ereignisse anzuzeigen.

Von GCP werden in der Nutzlast keine Werte wie der Schweregrad gesendet. Der Standardschweregrad ist „Gering“, die im Abschnitt*`Push Connector Configuration`* von geändert werden kann **Push-Connectors** > **Google Monitor-Push-Connector**. Die gültigen Werte für den Schweregrad sind**1 – Kritisch**,**2 – Schwerwiegend**,**3 – Gering**,**4 – Warnung**und**5 – Information**.

> **Hinweis:**
>
> Um die Hosts GCP dem Datensatz**cmdb_ci_server**anstatt**cmdb_ci_vm_object**zuzuordnen, deaktivieren Sie die für GCPerstellte**Google Monitor – Allgemeine**Ereignisregel. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Erfassung von Google Cloud Platform (GCP)

Mit dem MID WebService-Event-Sammler können Sie Event-Nachrichten im JSON-Format erfassen, die vom Google Cloud Platform (GCP) gesendet wurden.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Stellen Sie Folgendes sicher:

- Stellen Sie den MID-Server bereit und starten Sie ihn. Weitere Informationen finden Sie unter MID-Server-Konfiguration .
- Konfigurieren Sie einen MID Web Server. Weitere Informationen finden Sie unter MID-Webservererweiterung konfigurieren.
- Konfigurieren und starten Sie den Eventsammler des MID WebService. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Event-Nachrichten im JSON-Format werden von Google Cloud Platform gesendet. MID-Server wandelt die gesammelten Ereignisnachrichten um, indem er sie mithilfe der Skripteinbindung TransformEvents_MidGoogleMonitor analysiert, die sich hier befindet: **Ereignismanagement** > **Integrationen** > **PushConnectors**. Klicken Sie auf der Seite „Push-Connectors“ auf **Google Monitor Mid Push Connector**.

Das Standardformat der URL zum Übertragen von Event-Nachrichten von GCP auf den MID-Server lautet: `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidGoogleMonitor`.

Variablen in der Standard-URL

Variable	Beschreibung
MID_Server_IP	IP-Adresse der MID-Webserver-Erweiterung.
{MID_Web_Server_Port}	Listener-Port der MID-Webserver-Erweiterung.
MID_Web_Server_User	Anwendername für die MID-Webserver-Erweiterung.
MID_Web_Server_Password	Passwort des Anwenders des MID-Webservers.

Das folgende Verfahren beschreibt die Erfassung von JSON-formatierten Event-Nachrichten mit Standardauthentifizierung.

Prozedur

1. Stellen Sie in der Google Cloud Platform (GCP)-Konsole sicher, dass die MID Server-IP von der GCP-Konsole und der MID-REST-Punkt von GCP aus zugänglich ist, oder installieren Sie den MID-Server auf einer GCP-VM, und geben Sie die externe IP-Adresse der GCP-VM in der URL an.
   Erstellen Sie in der GCP-Konsole eine Firewall-Regel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **VPC-Netzwerk** > **Firewall** > **Firewall erstellen**.

b. Legen Sie die Richtung auf **Eingehend** fest, damit mid_web_server_port eine Verbindung herstellen kann.

c. Fügen Sie die GCP-VM, auf der MID-Server installiert ist, der Liste **Applicable to instances** (Anwendbar auf Instanzen) hinzu.

2. Fügen Sie in der GCP-Konsole einen Webhook hinzu:

a. Navigieren zu **Überwachung** > **Warnung** und klicken Sie **auf Benachrichtigungskanäle bearbeiten**.

b. Klicken Sie im Abschnitt „Webhooks“ auf **Neu hinzufügen**.

c. Aktivieren Sie das Kontrollkästchen **Use HTTP Basic Auth** (HTTP-Standardauthentifizierung verwenden), und geben Sie Benutzername und Passwort des entsprechenden MID Webserver-Benutzers ein.

> **Hinweis:** Stellen Sie sicher, dass dem ausgewählten Benutzer die Rolle „evt_mgmt_integration“ zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

d. Geben Sie die Endpunkt-URL ein.
Verwenden Sie zum Beispiel `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidGoogleMonitor`.

3. Erstellen Sie in der GCP-Konsole eine Warnungsrichtlinie.

a. Navigieren zu **Überwachung** > **Warnung** und klicken Sie auf **Richtlinie erstellen**.

b. Konfigurieren Sie Richtlinienbedingungen, die Warnungen auslösen, wenn ein Verstoß gegen die Bedingungen vorliegt.

c. Wählen Sie den Webhook-Benachrichtigungskanal aus, für den das Problem gemeldet werden soll.

d. Aktivieren Sie das Kontrollkästchen **Notify on incident closure** (Beim Schließen des Incident benachrichtigen), um die Abschluss-Events an MID-Server zu senden und die Warnungsrichtlinie zu speichern.

> **Hinweis:** Wenn Sie einen Incident aus der Warnung direkt in der Konsole GCP öffnen müssen, navigieren Sie zu **Schnelle Antwort (in Warnung)** > **Incident in GCP-Konsole anzeigen**. Weitere Informationen zum Erstellen einer Warnungsrichtlinie finden Sie unter Warnungsrichtlinien verwalten auf der Google Cloud-Dokumentationswebsite.

Ergebnisse
GCP sendet keine Werte wie den Schweregrad an die Payload. Der Standardschweregrad ist Gering und kann im Abschnitt *Push Connector Configuration* von geändert werden **Push-Connectors** > **Google Monitor-MID-Push-Connector**. Die gültigen Werte für „Schweregrad“ sind **1- Kritisch**, **2- Schwer**, **3- Gering**, **4- Warnung** und **5- Info**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Grafana-Events integrieren

Integrieren Sie Grafana mit Ereignismanagement, indem Sie der Grafana-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

- Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.
- Das Plugin „Ereignismanagement“ muss in der Now Platform-Instanz installiert sein.
- Die CI-Bindung erfolgt über die IP, Instanzen müssen als Server erkannt werden, um die Bindung zu initiieren. Über die Cloud erkannte CIs oder CIs in **„cmdb_ci_vm_object“** werden nicht gebunden, da Grafana keine Informationen für Objekt-IDs bereitstellt.
- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Grafana. Legen Sie in Ihrer Grafana-Konsole die Now Platform-Instanz mithilfe eines Standard-Webhook als REST-Endpunkt fest.

Hinweis: Führen Sie die Schritte 1 und 2 für Grafana v7.4.3 aus. Für Grafana v9.3.2. fahren Sie mit Schritt 3 fort.

Prozedur

Grafana v7.4.3

1. Erstellen Sie in Ihrer Grafana-Konsole einen Benachrichtigungskanal.

   a. Navigieren zu **Warnung** > **Benachrichtigungskanäle**.

   b. Klicken Sie auf **Neuer Kanal**, und wählen Sie als Typ **Webhook** aus.

   c. Geben Sie eine URL ein.
   Verwenden Sie beispielsweise `https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=grafana`.

   d. Wählen Sie unter **Optionale WebHook-** Einstellungen die HTTP-Methode **POST**aus, und geben Sie Anwendername und Passwort des entsprechenden -Benutzers ServiceNow ein.

      Hinweis: Stellen Sie sicher, dass dem ausgewählten Benutzer die Rolle „evt_mgmt_integration“ zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

   e. Klicken Sie auf **Test**, um die Verbindung zu testen.

2. Erstellen Sie in der Grafana-Konsole Warnungsregeln.

   a. Klicken Sie im erforderlichen Bereich auf **Bearbeiten** und dann auf **Warnung erstellen**.

   b. Fügen Sie auf der Registerkarte **Warnung** die folgenden Tags hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tags	Beschreibung
Schweregrad	(Dieses Tag ist optional und muss in Kleinbuchstaben angegeben werden.) Schweregrad, mit dem die Warnung erstellt werden muss.
Anzahl	(Dieses Tag ist erforderlich, andernfalls werden die Warnungen in ServiceNownicht automatisch geschlossen.) Anzahl der Geräte, Hosts oder Server, die von dieser Warnungsregel überwacht werden.

c. Fügen Sie den Benachrichtigungskanal unter **Benachrichtigungen** in der Warnungsregel hinzu.

d. Klicken Sie auf **Speichern**.

e. Navigieren zu **Warnung** > **Warnungsregeln** um auf die erstellte Regel zuzugreifen.

Grafana v9.3.2.

3. Erstellen Sie in der Grafana-Konsole einen Kontaktpunkt.

a. Navigieren zu **Warnung** > **Kontaktpunkte**.

b. Klicken Sie auf **Neuer Kontaktpunkt**, geben Sie einen Namen ein, und wählen Sie **Webhook**als Typ aus.

c. Geben Sie eine URL ein.
Verwenden Sie beispielsweise `https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=grafana`.

d. Wählen Sie unter **Optionale WebHook-** Einstellungen die HTTP-Methode **POST**aus, und geben Sie Anwendername und Passwort des entsprechenden -Benutzers ServiceNow ein.

> **Hinweis:** Stellen Sie sicher, dass dem ausgewählten Benutzer die Rolle „evt_mgmt_integration“ zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

e. Klicken Sie auf **Speichern** und **testen**, um die Verbindung zu überprüfen.

4. Erstellen Sie in der Grafana-Konsole eine Benachrichtigungsrichtlinie.

a. Navigieren zu **Warnung** > **Benachrichtigungsrichtlinien**.

b. Wählen Sie **Neue Richtlinie**aus, und fügen Sie Matcher hinzu.
Matcher sind Bezeichnungen, die Warnungsregeln an den Kontaktpunkt weiterleiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie Ihren Kontaktpunkt aus.

d. Wählen Sie **Richtlinie speichern**aus.

5. Erstellen Sie in der Grafana-Konsole Warnungsregeln.

a. Navigieren zu **Warnung** > **Warnungsregel**.

b. Wählen Sie **Neue Regel**aus.

c. Legen Sie die Abfrage- und Warnungsbedingung fest.

d. Legen Sie die Datenquelle, Metriken und die erforderlichen Filter fest.

e. Legen Sie das Verhalten der Warnungsauswertung fest.

f. Geben Sie den Regelnamen ein.

g. Fügen Sie im Abschnitt „Zusammenfassung und Anmerkungen“ eine Zusammenfassung oder eine Beschreibung hinzu.

h. Wählen Sie im Bildlauf nach unten **+Neu hinzufügen aus**.

i. Geben Sie die Knoten-, Ressourcen- und Metrikinformationen ein.
Diese Informationen sind für die Felder „node“, „resource“ und „metric_name“ für das Ereignis erforderlich.

Hinweis: Verwenden Sie die Wertzeichenfolge, um diese Werte zu übergeben. Ein Knoten kann beispielsweise {{$values.C0.Labels.instance }} sein.

j. Geben Sie unter anwenderdefinierte Bezeichnungen die erforderlichen Bezeichnungen an, um Ihre Benachrichtigungen an den entsprechenden Kontaktpunkt zu leiten.

Hinweis: Sie können den Schweregrad auch unter anwenderdefinierten Bezeichnungen übergeben. Dasselbe wird für Ereignisse verwendet. Die verfügbaren Schweregradoptionen sind: kritisch, schwerwiegend, geringfügig, Warnung.

k. Klicken Sie auf **Speichern**.

Ergebnisse
Die Übertragung von Warnungen von Grafana in das Plugin Event Management beginnt. Das Plugin extrahiert Informationen aus der ursprünglichen Grafana-Warnmeldung, um die erforderlichen Event-Felder zu füllen, und fügt das Event in die Datenbank ein. Navigieren Sie in Ihrer Now Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Für Grafana v7.4.3 sehen Sie möglicherweise zusätzliche Löschereignisse in ServiceNow, die nicht an eine Warnung gebunden sind. Ignorieren Sie sie, da sie erstellt wurden, um das Problem zu beheben, dass Grafana keine Informationen in der eindeutigen Benachrichtigung sendet.
- Ein Schweregradparameter wird hinzugefügt, der nur für Grafana 8 und höher verwendet wird. Der angegebene Wert wird als Schweregrad für ein Ereignis verwendet, wenn der Schweregrad nicht in anwenderdefinierten Bezeichnungen übergeben wird.

Integrieren Sie Grafana mit dem REST-API-Schlüsseltoken

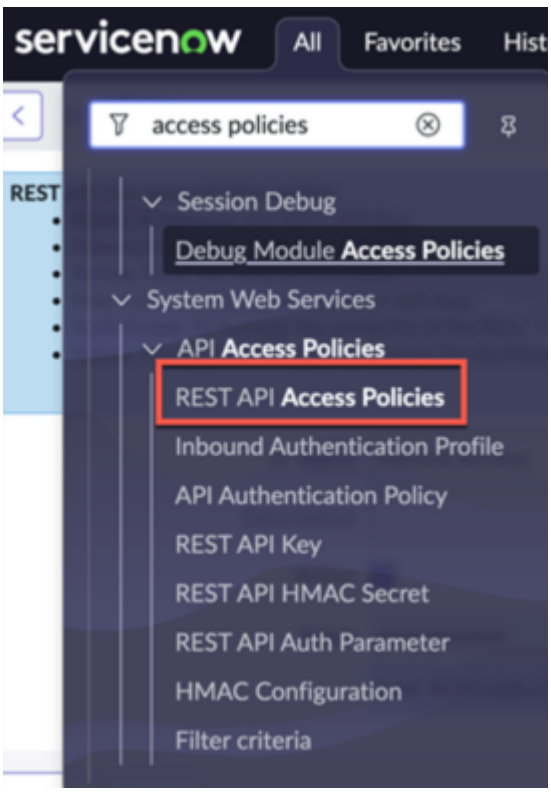
Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und erhöht die betriebliche Effizienz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**.



2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Hinweis: Der Anwender muss mit der Rolle evt_mgmt_integration erstellt werden. Erstellen Sie in der Tabelle „sys_user“ eine neue, um sie hier zu verwenden, um den richtigen Zugriff zu erleichtern.

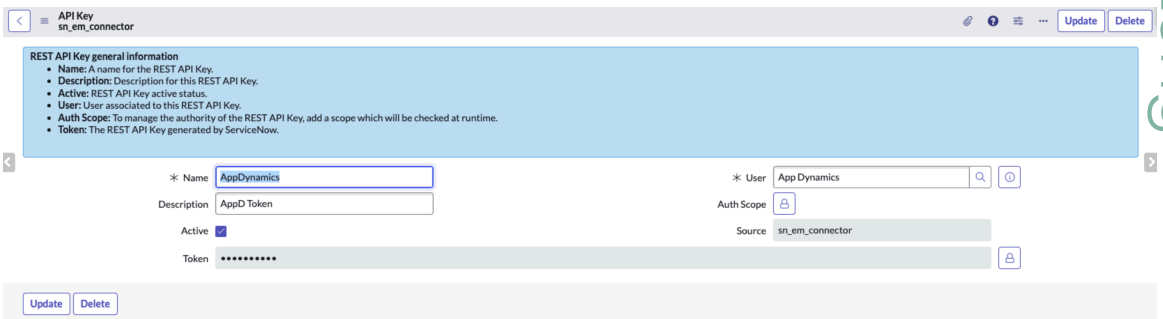
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST-API-Schlüssels zu verwalten.
Token	Der von Now Platformgenerierte REST-API-Schlüssel. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.
Ablauf	Zeitpunkt, nach dem die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie hinzu: UserAccount.
5. Verwenden Sie das Formularmenü, und wählen Sie **Speichern**aus.

   Das System generiert ein Token und speichert es im Feld **Token**. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie den Inhalt, der unter dem Feld angezeigt wird. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Honeycomb-Ereignisse integrieren

Integrieren Sie Honeycomb mit Ereignismanagement, indem Sie einen Webhook erstellen und ihn auf der Honeycomb-Plattform als Auslöser konfigurieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Discovery für Honeycomb-Services und -Datensätze wird nicht unterstützt. Damit die Ereignis-/CI-Bindung funktioniert, erstellen Sie in der ServiceNow-Instanz manuell ein CI (Configuration Item).

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Ereignissen von Honeycomb, indem Sie Honeycomb als Datenquelle authentifizieren. Legen Sie auf der Honeycomb-Plattform die Now Platform mit einem Webhook als REST-Endpunkt fest.

Prozedur

1. Erstellen Sie auf der Honeycomb-Plattform eine Integration von *`type=webhook`*.
   a. Navigieren zu **Monatlich** > **Integrationen**.
   b. Klicken Sie auf die Schaltfläche **Add Integration** (Integration hinzufügen).
   c. Geben Sie Werte in die Felder **Name** und **Webhook URL** ein.
   Verwenden Sie beim Eingeben der Webhook-URL das folgende Format: `https://<USERNAME>:<PASSWORD>@<INSTANCE_NAME>.service-now.com/api/sn_em_connector/em/inbound_event?source=honeycomb`.
   d. Wählen Sie im Feld **Provider** (Anbieter) die Option **Webhook** aus.
   e. Wählen Sie **Add** (Hinzufügen), um die Webhook-Erstellung abzuschließen.
2. Fügen Sie den Webhook einem Auslöser hinzu.
   a. Navigieren zu **Wiederholungen** > **Neuen Auslöser erstellen**.
   b. Fügen Sie in den entsprechenden Feldern einen Namen und eine Beschreibung für den Auslöser hinzu.
   c. Konfigurieren Sie im Abschnitt **Alerts** (Warnungen) den Schwellenwert und die Häufigkeit in den entsprechenden Feldern.
   d. Wählen Sie im Abschnitt **Recipients** (Empfänger) die Option **Add Recipient** (Empfänger hinzufügen) aus, und wählen Sie den in Schritt 1 erstellten Webhook aus.
   e. Wählen Sie **Save Trigger** (Auslöser speichern) aus.

Hinweis: Um den Auslöser auf der Honeycomb-Plattform anzuzeigen, navigieren Sie zu **Quick Response (in Alert)** (Schnelle Antwort (in Warnung)), und wählen Sie **Show Trigger in Honeycomb** (Auslöser in Honeycomb anzeigen) aus.

Ergebnisse

Warnungen werden vom Honeycomb-Connector in das Ereignismanagement-Plugin weitergeleitet. Vom Plugin werden Informationen aus der ursprünglichen Honeycomb-Auslösermeldung zum Füllen der erforderlichen Ereignisfelder extrahiert. Außerdem wird das Ereignis in die Datenbank eingefügt. Sie können die Ereignisse in der Now Platform-Instanz anzeigen, indem Sie zu **Alle Ereignisse** navigieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Auslösermeldung werden von Honeycomb keine Informationen zum Schweregrad gesendet. Der Standardschweregrad für die Honeycomb-Warnung ist *3 - Minor*und kann im Abschnitt „Push-Connector-Konfiguration“ von geändert werden **Push-Connectors** > **Honeycomb-Push-Connector** . Die gültigen Schweregrade lauten: *1- Critical*, *2- Major*, *3- Minor*, *4- Warning* und *5- Info*.

Instana-Events integrieren

Integrieren Sie Instana mit Ereignismanagement, indem Sie der Instana-Konsole einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren Sie in der Instana-Konsole zu **Einstellungen** > **Ereignisse und Warnungen** > **Warnungskanäle**.
2. Öffnen Sie die Dropdown-Liste **Add Alert Channel** (Warnungskanal hinzufügen) und wählen Sie die Option **Generic Webhook** (Generischer Webhook) aus.
3. Erstellen Sie im Feld **Webhook-URLs** einen Warnungskanal, indem Sie die folgende URL eingeben:
   `https://<instance>.service-now.com/api/sn_em_connector/em/inbound_event?source=instana`
4. Um die ServiceNow-URL zu authentifizieren, geben Sie unter **Custom HTTP Request Headers** (Benutzerdefinierte HTTP-Anforderungsheader) Folgendes ein:

Feld	Wert
Schlüssel	Autorisierung
Wert	Standard <base64_encoded username:password>

5. Konfigurieren Sie Instana, um Warnungen für Event-Typen oder Events zu erstellen.

   a. Navigieren zu **Einstellungen** > **Ereignisse und Warnungen** > **Warnungen**.

   b. Wählen Sie **New Alert** (Neue Warnung) aus.

   c. Wählen Sie im Abschnitt **Events** eine der folgenden Optionen aus:
      - Alert on Event Type(s) (Warnung zu Event-Typ(en))
      - Warnung zu Ereignis(sen)

   d. Beim Erstellen von Warnungen für Event-Typen:
      i. Wählen Sie den Typ der Events aus, für die Warnungen erstellt werden sollen, z. B. **Critical Issues** (Kritische Probleme), **Alle Incidents**, **Warning issues** (Warnungsprobleme) usw.
      ii. Wählen Sie im Abschnitt **Warnungen** den Warnungskanal **servicenow** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Beim Erstellen von Warnungen für Events:

i. Wählen Sie die Events aus, für die Warnungen erstellt werden sollen.

ii. Wählen Sie im Abschnitt **Warnungen** den Warnungskanal **servicenow** aus.

Wenn Instana eine Warnung erstellt, wird die Warnung an die ServiceNow-Instanz gesendet. Für die Hostentität erstellte Warnungen werden an die Tabelle „Server“ (cmdb_ci_server) gebunden und für die Website-Entität erstellte Warnungen werden an die Tabelle „HTTP(S)“ (cmdb_ci_endpoint_http) gebunden.

Fügen Sie der Tabelle „Instana – ci_type-Ereignis-Feldzuordnung“ weitere Entitätstypen hinzu, um sicherzustellen, dass die Entität mit dem richtigen CI in der ServiceNow-Instanz verbunden ist.

6. Um das Event im Instanza-Quellsystem anzuzeigen, können Sie über eine ServiceNow-Instanz darauf zugreifen:

a. Navigieren zu **Alle** > **Ereignismanagement** > **Service Operations-Arbeitsbereich**.

b. Wählen Sie **Alle Warnungen** aus.

c. Wählen Sie die entsprechende Warnung aus.

d. Suchen Sie auf der Registerkarte **Details** rechts auf der Seite den Abschnitt **Aktionen** und wählen Sie in der Zelle **Show Event on Instana UI** (Event in Instana-UI anzeigen) die Option **App starten** aus.

Integrieren Sie ServiceNow Cloud Observability Ereignisse

Integrieren Sie ServiceNow Cloud Observability mit Ereignismanagement, indem Sie der Plattform ServiceNow Cloud Observability einen Standard-Webhook hinzufügen. Laden Sie das Ereignismanagement Connector-Plugin aus dem ServiceNow Store herunter, damit Sie es in ServiceNow Cloud Observabilityintegrieren können.

Vorbereitungen

- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Authentifizieren Sie ServiceNow Cloud Observability als Datenquelle, damit Ereignismanagement Ereignisse von ServiceNow Cloud Observabilitysammeln kann. Verwenden Sie in Ihrer Plattform ServiceNow Cloud Observability einen Standard-Webhook, um Ihre Instanz Now Platform als REST-Endpunkt festzulegen.

Hinweis: Stellen Sie sicher, dass die Rolle „evt_mgmt_integration“ dem ausgewählten Benutzer zugewiesen ist. Um eine ordnungsgemäße Authentifizierung sicherzustellen, verwenden Sie den Benutzer mit den geringsten Berechtigungen mit der Rolle evt_mgmt_integration anstelle eines Benutzers mit hohen Berechtigungen.

Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Ereignisregeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Zuordnung** anwenden Checkbox für Regeln auf „wahr“ gesetzt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie mehr Ereignisregeln oder Automatisierung mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie ein CI.

   Hinweis: Discovery für Services ServiceNow Cloud Observability wird nicht unterstützt. Erstellen Sie ein CI manuell in einer Serviceinstanztabelle (cmdb_ci_service_auto), um die Bindung zu aktivieren.

   a. Navigieren zu **Alle** > **Konfiguration** > **Anwendungsservice**.

   b. Wählen Sie **Neu**.

   c. Geben Sie im Formular den Namen ein.
   Der Name muss der in der Plattform ServiceNow Cloud Observability angegebene Servicename sein.

   d. Legen Sie in der Liste „Betriebsstatus“ den Betriebsstatus auf **Funktionsfähig**fest.

   e. Wählen Sie **Weiter**.

   f. Wählen Sie **Fertig**.

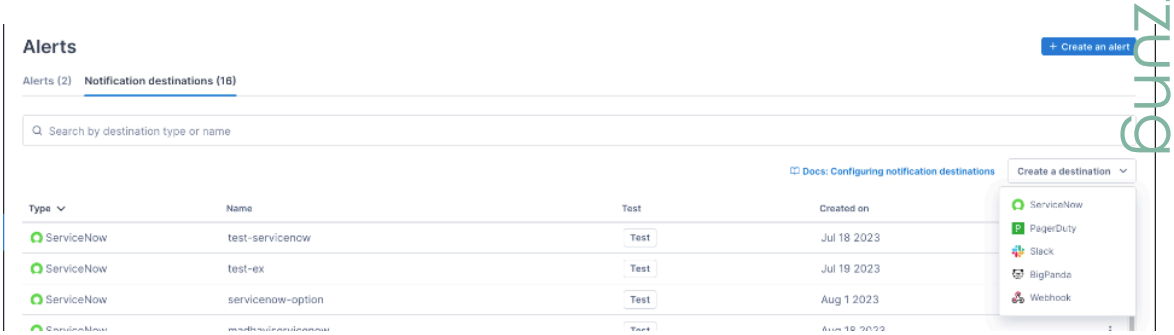
2. Erstellen Sie in Ihrer Plattform ServiceNow Cloud Observability ein Benachrichtigungsziel.

   a. Wählen Sie in der Navigationsleiste **Warnungen**aus.

   b. Wählen Sie die Registerkarte **Benachrichtigungsziele**.

   c. Wählen Sie **Ziel erstellen aus**.

   d. Wählen Sie **ServiceNow** oder **Webhook**aus.
   Verwenden Sie das Ziel ServiceNow nur zum Herstellen einer Verbindung mit der Plattform ServiceNow. Wenn Sie Probleme mit dem Ziel ServiceNow haben, verwenden Sie die **Webhook** -Zieloption.



3. Erstellen Sie auf Ihrer ServiceNow Cloud Observability -Plattform ein ServiceNow -Benachrichtigungsziel.

   a. Geben Sie im Feld **Name** einen Namen für das Ziel ServiceNow ein.

   b. Geben Sie im Feld **„URL“** die Instanz-URL ServiceNow an.
   Dies ist das Standardformat der URL zum Übertragen von Ereignissen von ServiceNow Cloud Observability an die Instanz Now Platform. Dieses Format verwenden:

Automatische Übersetzung

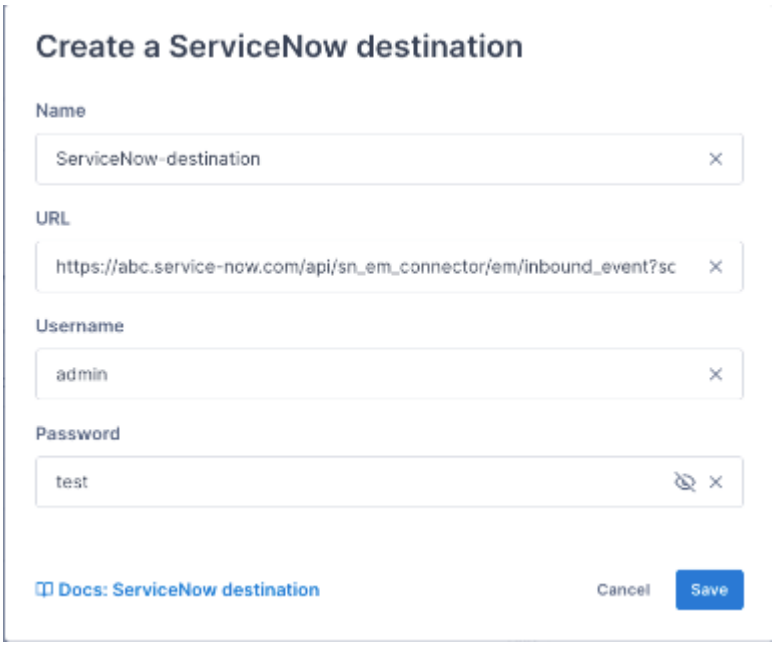
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

`https//`<instance-name> .servicenow.com/api/sn_em_connector/em/inbound_event?source=lightstep

c. Geben Sie im Feld **Anwendername** Ihren ServiceNow -Anwendernamen ein.

d. Geben Sie im Feld **Passwort** Ihr Anwenderpasswort ServiceNow ein.

Erstellen Sie ein ServiceNow-Ziel



Hinweis: In einer Instanz ServiceNow tritt die CI-Bindung nur auf, wenn der Name des Services im Plattformwert ServiceNow Cloud Observability mit den Namensfeldern des von Ihnen in der Tabelle *`cmdb_ci_service_auto`* erstellten CI übereinstimmt.

e. Wählen Sie **Speichern**.

4. **Hinweis:** Wenn Sie im vorherigen Schritt Probleme mit dem Ziel ServiceNow haben, verwenden Sie die **Webhook** -Zieloption.

Erstellen Sie in Ihrer -Plattform ServiceNow Cloud Observability ein **Webhook-**Benachrichtigungsziel.

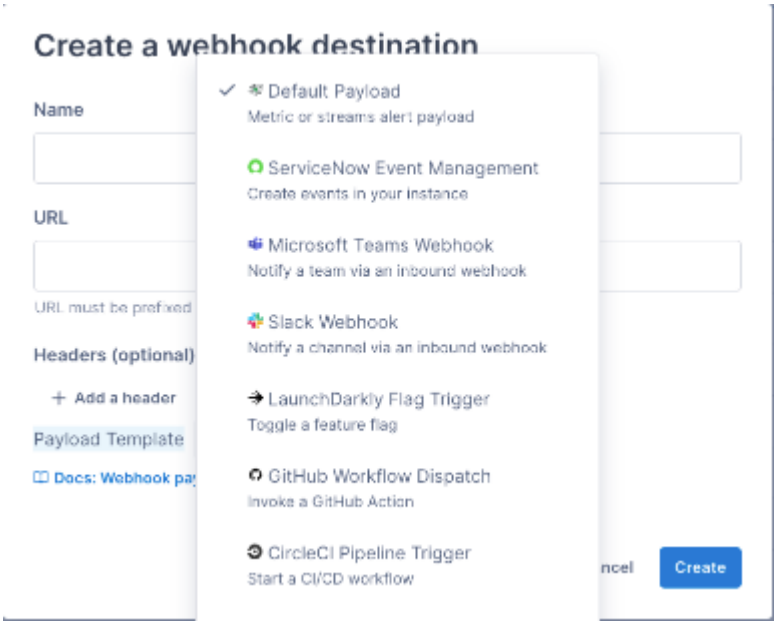
a. Geben Sie im Feld **Name** einen Namen für das Webhook-Ziel [ein.

b. Geben Sie im Feld **URL** die Webhook-URL an.
Dies ist das Standardformat der URL zum Übertragen von Ereignissen von ServiceNow Cloud Observability an die Instanz Now Platform. Dieses Format verwenden:
`https//`<username> :<password> @<instance-name> .service-now.com/api/sn_em_connector/em/inbound_event?source=lightstep

c. Wählen Sie **Nutzlastvorlage**aus.

d. Wählen Sie die Option **ServiceNow Ereignismanagement** aus.

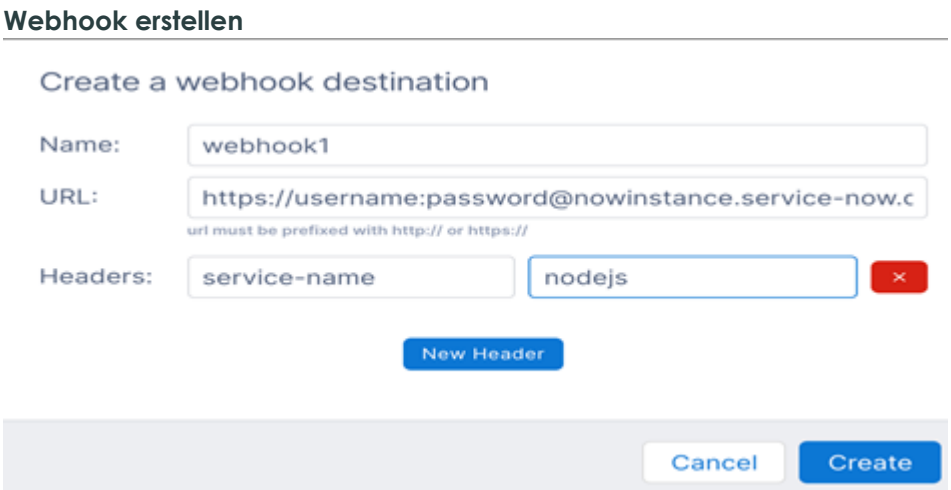
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: In einer Instanz ServiceNow tritt die CI-Bindung nur auf, wenn der Name des Services im Plattformwert ServiceNow Cloud Observability mit den Namensfeldern des von Ihnen in der Tabelle *cmdb_ci_service_auto* erstellten CI übereinstimmt.

e. Wenn Sie im vorherigen Unterschritt die Option **Standardvorlage** ausgewählt haben, wählen Sie **Neuer Header**, geben Sie im Feld **Header** den **Servicenamen** ein, und definieren Sie dessen **Wert**.

Hinweis: In einer Instanz ServiceNow erfolgt die CI-Bindung nur, wenn der Headerwert **„service-name“** mit den Namensfeldern des von Ihnen in der **Tabelle cmdb_ci_service_auto**erstellten CI übereinstimmt.



f. Wählen Sie **Erstellen** aus.

5. Konfigurieren Sie auf der Plattform ServiceNow Cloud Observability eine -Warnung.

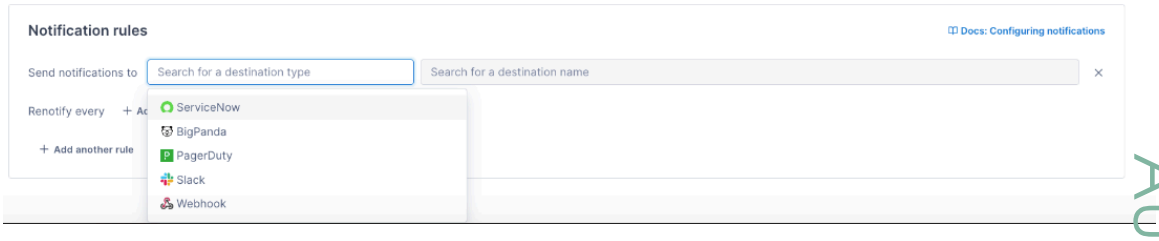
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie in der Navigationsleiste **Warnungen**aus.

b. Wählen Sie **Warnung erstellen aus,** und geben Sie einen Warnungsnamen ein.

c. Definieren Sie im Bereich „Warnmeldungskonfiguration“ den Schwellenwert.

d. Wählen Sie entsprechend dem von Ihnen erstellten Ziel im Bereich **„Benachrichtigungsregeln“** im Feld **Benachrichtigungen senden an** Ihren Benachrichtigungszieltyp aus, und suchen Sie nach dem Zielnamen.



e. Wählen Sie **Speichern**.
Der Standardschweregrad für streambasierte Warnungen ist **Kritisch**. Sie können den Standard im Bereich Push-Connector-Konfiguration einer Now Platform -Instanz ändern. Die gültigen Schweregradwerte sind:

- 1 - Kritisch
- 2 - Schwer
- 3 – Gering
- 4 – Warnung
- 5 - Info

Logicmonitor-Events integrieren

Integrieren Logicmonitor mit Ereignismanagement zum Senden von Ereignissen in ServiceNow, indem Sie einen Webhook mit Standardauthentifizierung hinzufügen. Dieser wird auch mit bidirektionaler Funktionalität zur Verfügung stehen.

Vorbereitungen

- Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.
- Das Plugin „Ereignismanagement“ muss in der Now Platform-Instanz installiert sein.
- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Logicmonitor. Legen Sie in Ihrer Logicmonitor-Konsole die Now Platform-Instanz mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Ereignisregeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Zuordnung** anwenden Checkbox für Regeln auf „wahr“ gesetzt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie mehr Ereignisregeln oder Automatisierung mit denselben Filterbedingungen für die Ereignisse ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

Prozedur

1. Erstellen Sie in der Logicmonitor-Konsole eine benutzerdefinierte HTTP Delivery-Integration.
   a. Navigieren zu **Einstellungen** > **Integrationen** und klicken Sie auf **Hinzufügen** > **Anwenderdefinierte HTTP-Bereitstellungsintegration**.
   b. Füllen Sie im Formular „Manage Custom HTTP Delivery Integration“ die Felder **Name** und **Description** aus und aktivieren Sie das Kontrollkästchen **Use the same URL and data to notify on various alert activity**.
   c. Geben Sie durch die Auswahl der Kontrollkästchen **Acknowledged**, **Cleared** und **Escalated/De-escalated** an, wann eine Benachrichtigung über Alarmaktivitäten versendet werden soll.
   d. Wählen Sie im Menü „HTTP Method“ die Option **HTTP POST** aus.
   e. Füllen Sie das Feld **Benutzername** und **Passwort** aus, und geben Sie eine URL im Format `https://{Instance-name}.service-now.com/api/sn_em_connector/em/inbound_event?source=logicmonitor` ein.
   f. Wählen Sie im Abschnitt „Alert Data“ die Option **Raw** aus, und wählen Sie das Format als **JSON** aus.
   g. Fügen Sie die benutzerdefinierte Nutzlast hinzu, die in der Beschreibung des Connectors angegeben ist.
   h. Klicken Sie auf **Test Alert Delivery**, um die Verbindung zu überprüfen, oder auf **Save**.
2. Wenn Sie mit dem Erstellen der Integration fertig sind, erstellen Sie eine Eskalationskette für die Warnungseinstellungen.
   a. Navigieren zu **Einstellungen** > **Warnungseinstellungen** > **Eskalationsketten** Klicken Sie dann auf **Hinzufügen**.
   b. Füllen Sie im Formular „Manage Testing chain“ die Felder **Name** und **Description** aus, und wählen Sie die Rate aus, mit der über die Warnungen benachrichtigt werden soll.
   c. Wählen Sie im Abschnitt „Stages“ das Hinzufügungssymbol , um eine Phase hinzuzufügen, und klicken Sie dann auf **Save**.
   d. Wenn Sie die neue Phase erstellen, wählen Sie erneut das Symbol zum Hinzufügen aus, um nach dem Benutzer zu suchen und die Integration als Kontaktmethode hinzuzufügen, und klicken Sie dann auf **Save**.
3. Nachdem Sie die Eskalationskette erstellt haben, konfigurieren Sie Warnungsregeln für die von Ihnen erstellte Kette.
   a. Navigieren zu **Einstellungen** > **Warnungseinstellungen** > **Warnungsregeln**und klicken Sie auf **Hinzufügen**.
   b. Konfigurieren Sie im Fenster „Add Alert“ Bedingungen, die Warnungen auslösen, wenn ein Verstoß gegen die Bedingungen vorliegt.
   c. Wählen Sie im Menü „Escalation chain“ die von Ihnen erstellte Eskalationskette aus.
   d. Klicken Sie auf **Speichern**.

Hinweis: Um das CI dem **cmdb_ci_vm_object**-Datensatz anstelle von **cmdb_ci_server** zuzuordnen, aktivieren Sie die für Logicmonitor erstellte Event-Regel. Der Sammlername des Logicmonitors, der als Hostname in der Payload eingeht, muss mit der object_id der virtuellen Maschine übereinstimmen, die im Datensatz **cmdb_ci_vm_object** erkannt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Erfassung von Logicmonitor

Mit dem MID WebService-Eventsammler können Sie Event-Nachrichten im JSON-Format von Logicmonitor erfassen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Stellen Sie Folgendes sicher:

- Stellen Sie den MID-Server bereit und starten Sie ihn. Weitere Informationen finden Sie unter MID-Server-Konfiguration .
- Konfigurieren Sie einen MID Web Server. Weitere Informationen finden Sie unter MID-Webservererweiterung konfigurieren.
- Konfigurieren und starten Sie den Eventsammler des MID WebService. Weitere Informationen finden Sie unter MID-WebService-Event-Sammlerkontext konfigurieren.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

JSON-formatierte Event-Nachrichten werden von Logicmonitor gesendet. MID-Server wandelt die gesammelten Ereignisnachrichten um, indem sie sie mithilfe der Skripteinbindung TransformEvents_MidLogicmonitor analysieren, die sich hier befindet: **Ereignismanagement** > **Integrationen** > **PushConnectors**. Klicken Sie auf der Seite „Push-Connectors“ auf **Logicmonitor Mid Push-Connector**.

Das Standardformat der URL zum Übertragen von Event-Nachrichten von Logicmonitor auf den MID-Server lautet: `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidLogicmonitor`.

Variablen in der Standard-URL

Variable	Beschreibung
MID_Server_IP	IP-Adresse der MID-Webserver-Erweiterung.
{MID_Web_Server_Port}	Listener-Port der MID-Webserver-Erweiterung.
MID_Web_Server_User	Anwendername für die MID-Webserver-Erweiterung.
MID_Web_Server_Password	Passwort des Benutzers des MID-Webservers.

Prozedur

1. Erstellen Sie in der Logicmonitor-Konsole eine benutzerdefinierte HTTP Delivery-Integration.
   a. Navigieren zu **Einstellungen** > **Integrationen** und klicken Sie auf **Hinzufügen** > **Anwenderdefinierte HTTP-Bereitstellungsintegration**.
   b. Füllen Sie im Formular „Manage Custom HTTP Delivery Integration“ die Felder **Name** und **Description** aus und aktivieren Sie das Kontrollkästchen **Use the same URL and data to notify on various alert activity**.
   c. Geben Sie durch die Auswahl der Kontrollkästchen **Acknowledged**, **Cleared** und **Escalated/De-escalated** an, wann eine Benachrichtigung über Alarmaktivitäten versendet werden soll.
   d. Wählen Sie im Menü „HTTP Method“ die Option **HTTP POST** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Füllen Sie die Felder **Username** und **Password** aus, und geben Sie eine URL im Format `http://<MID_Server_IP>:<MID_Web_Server_Port>/api/mid/em/inbound_event?Transform=TransformEvents_MidLogicmonitor` ein.

f. Wählen Sie im Abschnitt „Alert Data“ die Option **Raw** aus, und wählen Sie das Format als **JSON** aus.

g. Fügen Sie die benutzerdefinierte Nutzlast hinzu, die in der Beschreibung des Connectors angegeben ist.

h. Klicken Sie auf **Test Alert Delivery**, um die Verbindung zu überprüfen, oder auf **Save**.

2. Wenn Sie mit dem Erstellen der Integration fertig sind, erstellen Sie eine Eskalationskette für die Warnungseinstellungen.

a. Navigieren zu **Einstellungen** > **Warnungseinstellungen** > **Eskalationsketten** Klicken Sie dann auf **Hinzufügen**.

b. Füllen Sie im Formular „Manage Testing chain“ die Felder **Name** und **Description** aus, und wählen Sie die Rate aus, mit der über die Warnungen benachrichtigt werden soll.

c. Wählen Sie im Abschnitt „Stages“ das Hinzufügungssymbol , um eine Phase hinzuzufügen, und klicken Sie dann auf **Save**.

d. Wenn Sie die neue Phase erstellen, wählen Sie erneut das Symbol zum Hinzufügen aus, um nach dem Benutzer zu suchen und die Integration als Kontaktmethode hinzuzufügen, und klicken Sie dann auf **Save**.

3. Nachdem Sie die Eskalationskette erstellt haben, konfigurieren Sie Warnungsregeln für die von Ihnen erstellte Kette.

a. Navigieren zu **Einstellungen** > **Warnungseinstellungen** > **Warnungsregeln**und klicken Sie auf **Hinzufügen**.

b. Konfigurieren Sie im Fenster „Add Alert“ Bedingungen, die Warnungen auslösen, wenn ein Verstoß gegen die Bedingungen vorliegt.

c. Wählen Sie im Menü „Escalation chain“ die von Ihnen erstellte Eskalationskette aus.

d. Klicken Sie auf **Speichern**.

Hinweis: Um das CI dem **cmdb_ci_vm_object**-Datensatz anstelle von **cmdb_ci_server** zuzuordnen, aktivieren Sie die für Logicmonitor erstellte Event-Regel. Der Sammlername des Logicmonitors, der als Hostname in der Payload eingeht, muss mit der object_id der virtuellen Maschine übereinstimmen, die im Datensatz **cmdb_ci_vm_object** erkannt wurde.

Oracle Cloud Infrastructure-Alarme integrieren

Integrieren Sie Oracle Cloud Infrastructure(OCI)-Alarme mit Ereignismanagement, um Events an das ServiceNow-System zu senden, indem Sie mithilfe der Standardauthentifizierung ein https-Abonnement hinzufügen.

Vorbereitungen

- Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.
- Oracle Cloud Discovery muss ausgeführt werden, damit gewährleistet ist, dass die erstellten Warnungen an die Konfigurationselemente auf der Now Platform gebunden sind. Weitere Informationen finden Sie unter Erkennung der Oracle Cloud-Infrastruktur.
- Erforderliche Rolle: evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Mit dem Oracle Cloud Notifications-Service können Sie Kommunikationskanäle zum Veröffentlichen von Nachrichten mithilfe von Themen und Abonnements einrichten. Wenn eine Nachricht in einem Thema veröffentlicht wird, wird die Nachricht vom Benachrichtigungsservice an alle Abonnements des Themas gesendet.

Wenn eine Oracle Management Cloud-Warnung ausgelöst wird, sich der Schweregrad dieser erhöht oder sie gelöscht wird, empfiehlt es sich, dass Sie aktiv über eine benutzerdefinierte https-URL an die ServiceNow-Instanz benachrichtigt werden. Der Oracle Cloud-Connector wird zum Erstellen von Events im ServiceNow®-System verwendet.

Sie können die Ereignismanagement-Umgebung für die Erfassung von Alarmen aus Oracle Cloud konfigurieren, indem Sie Ihre Instanz der Now Platform als https-Abonnement festlegen.

Prozedur

1. Richten Sie in der Oracle Cloud-Konsole ein https-Abonnement ein.

   a. Wählen Sie im Formular „Create Subscription“ (Abonnement erstellen) im Abschnitt „Configure Subscription“ (Abonnement konfigurieren) in der Liste „Protocol “ (Protokoll) die Option **HTTPS (Custom URL)** (HTTPS (Benutzerdefinierte URL)) aus.

   Hinweis: Wenn das Abonnement erstellt wird, wird das Passwort nicht in Klartext angezeigt.

   b. Geben Sie im Feld „URL“ eine URL im Format `https://<username>:<password>@<instancename>.service-now.com/api/sn_em_connector/em/inbound_event/oraclecloud` ein.
   Beispiel: `https://oracleevents:oracleevents@instance1.service-now.com/api/sn_em_connector/em/inbound_event/oraclecloud`.
   Wenn das Abonnement mit der URL der ServiceNow-Instanz erstellt wird, erhält der Oracle Cloud Push-Connector eine Nutzlast, die das Abonnement bestätigt, und wird in der Oracle Cloud-Konsole in den Status **Aktiv** versetzt.

2. In der Oracle Cloud-Konsole können Sie eine Alarmdefinition erstellen und das Benachrichtigungsziel mit dem Thema festlegen, das das ServiceNow-https-Abonnement enthält.

   a. Navigieren zu **Erkennbarkeit und Management** > **Alarmdefinitionen**.

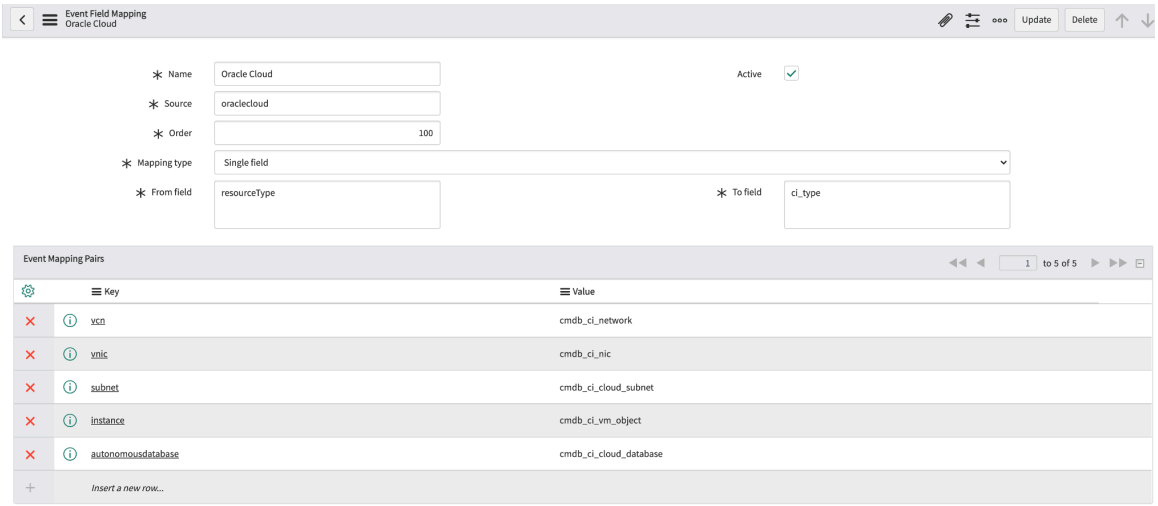
   b. Klicken Sie auf **Create Alarm** (Alarm erstellen) oder wählen Sie einen vorhandenen Alarm aus, für den Sie das Thema festlegen möchten, das das ServiceNow-https-Abonnement enthält.

   c. Wählen Sie im Abschnitt „Destinations“ (Ziele) in der Themenliste das Thema mit dem ServiceNow-https-Abonnement aus.
   Wenn in der Oracle Cloud-Konsole ein Alarm ausgelöst wird, wird derselbe Alarm im Oracle Cloud Push-Connector in der ServiceNow-Instanz empfangen und ein Event wird erstellt.

Ergebnisse

Abhängig von der Oracle Cloud-Alarmressource wird die Warnung mithilfe der folgenden Event-Feldzuordnung an das CI gebunden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Sie können andere Ereignisregeln erstellen oder die Ereignis-Feldzuordnung ändern, um andere Ressourcentypen zuzuordnen.

Sobald das https-Abonnement konfiguriert ist und durch einen Oracle Cloud-Alarm eine Nachricht in Ereignismanagement ausgelöst wird, geschieht Folgendes:

- Durch die Nachricht wird die Oracle Cloud-Alarmmeldung mit dem entsprechenden ServiceNow-Benutzer authentifiziert, der im https-Abonnement angegeben ist.
- Durch die Nachricht werden Informationen aus der ursprünglichen Oracle Cloud-Alarmmeldung extrahiert, damit die erforderlichen Ereignisfelder ausgefüllt werden. Außerdem wird das Event in die Now Platform-Datenbank eingefügt.
- Erfasst spezifischen Inhalt im Feld **Zusätzliche Informationen** des Event-Formulars

Prometheus-Events integrieren

Integrieren Sie Prometheus mit Ereignismanagement, indem Sie einen Standard-Webhook in den Warnungsmanager von Prometheus einfügen.

Vorbereitungen

- Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.
- Vergewissern Sie sich, dass Konfigurationselemente für die von Prometheus verwalteten Hosts im ServiceNow-System vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder cloudbasierter Erkennung erkannt werden.
- Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Prometheus.

Ab Release Xanadu verfügen die mit dem Connector bereitgestellten OOTB-Ereignisregeln (Out-Of-The-Box), die Sie zuvor nicht verwendet haben (d. h. weder aktiviert, deaktiviert noch geändert), jetzt über die **Option Zusätzliche Zuordnung** anwenden Checkbox für Regeln auf „wahr“ gesetzt. Zuvor war dieses Kontrollkästchen deaktiviert. Mit diesem Change können Sie mehr Ereignisregeln oder Automatisierung mit denselben Filterbedingungen für die Ereignisse ausführen.

Hinweis: Diese Funktion gilt nur für aktive Ereignisregeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Fügen Sie in der Prometheus-Instanz einen Webhook hinzu.
   a. Navigieren Sie zu Alertmanager.yml und fügen Sie einen Webhook-Eintrag unter den Empfängern hinzu.
   b. Geben Sie die Endpunkt-URL ein. Verwenden Sie beispielsweise `https://<instance-name>/service-now.com/api/sn_em_connector/em/inbound_event?source=prometheus`.
   c. Geben Sie `basic_auth` unter *`http_config`* ein.
   d. Fügen Sie unter *`basic_auth`* einen Benutzernamen und ein Passwort hinzu und fügen Sie dann den erstellten Webhook-Namen im Empfänger unter *`route`* hinzu.
2. Erstellen Sie in der Prometheus-Instanz eine Warnungsregel.
   a. Erstellen Sie eine Datei für die Warnungsregel und fügen Sie ihren Pfad in prometheus.yml unter *`rules_files`* hinzu.
   b. Erstellen Sie die Warnungsregel gemäß dem Prometheus-Format mit PromQL.
   c. Starten Sie AlertManager und Prometheus neu, um die Änderungen zu übernehmen.

Ergebnisse

Die Übertragung von Warnungen von Prometheus in das Ereignismanagement-Plugin beginnt. Vom Plugin werden Informationen aus der ursprünglichen Prometheus-Warnmeldung extrahiert, sodass die erforderlichen Ereignisfelder gefüllt werden. Außerdem wird das Event in die Datenbank eingefügt. Navigieren Sie in Ihrer Now Platform-Instanz zu **Alle Ereignisse**, um die Events anzuzeigen.

Wenn der Schweregrad nicht in der Nutzlast empfangen wird, ist der Standardschweregrad „Schwerwiegend“. Dieser Wert kann im Abschnitt *`Push Connector Configuration`* von geändert werden **Push-Connectors** > **Prometheus-Push-Connector**. Die gültigen Werte für „Schweregrad“ sind **1- Kritisch**, **2- Schwer**, **3- Gering**, **4- Warnung** und **5- Info**.

Hinweis:

Um Hosts dem *`cmdb_ci_vm_object`*-Datensatz anstelle von *`cmdb_ci_hardware`* zuzuordnen, aktivieren Sie die für Prometheus erstellte Ereignisregel **Prometheus-VM-Bindung**. Weitere Informationen zu Event-Regeln finden Sie unter Event-Regeln.

Sentry-Ereignisse integrieren

Integrieren Sie Sentry mit Ereignismanagement, indem Sie auf der Sentry-Plattform einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Discovery für Sentry-Services wird nicht unterstützt. Sie müssen ein CI manuell in der Tabelle [cmdb_ci_service_auto] erstellen, um die Bindung zu aktivieren, indem Sie die folgenden Schritte ausführen:

1. Wechseln Sie in der Navigationsleiste zu **Konfiguration/Anwendungsservice**.
2. Geben Sie den Namen des Projekts an, das Sie in der Sentry-Anwendung überwachen.
3. Legen Sie den Betriebsstatus auf **Funktionsfähig** fest.
4. Klicken Sie auf **Weiter** und dann auf **Fertig**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie Ereignismanagement für die Erfassung von Ereignissen aus Sentry, indem Sie Sentry als Datenquelle authentifizieren. Legen Sie auf der Sentry-Plattform die Now Platform mithilfe eines Standard-Webhooks als REST-Endpunkt fest.

Prozedur

1. Erstellen Sie in der Sentry-Konsole eine interne Integration.

   a. Navigieren zu **Einstellungen** > **Entwicklereinstellungen**.

   b. Klicken Sie auf **New Internal Integration** (Neue interne Integration).

   c. Füllen Sie auf der Seite „Sentry Integration Details“ (Details der Sentry-Integration) im Abschnitt „Internal Integration Details“ (Details der internen Integration) die Felder aus.

Sentry Integration Details (Details der Sentry-Integration)

Felder	Beschreibung
Name	Name der Integration.
Webhook-URL	Standardformat der URL zum Übertragen von Ereignissen von Sentry an die Instanz der Now Platform. Beispiel: `https://<username>:<password>@<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=sentry`.
Alert Rule Action (Warnungsregelaktion)	Option zum Aktivieren der Integration. **Hinweis:** Wenn diese Option aktiviert ist, ist die Integration in den Regeln für Problemwarnungen und Metrikwarnungen in Sentry verfügbar. Die Warnungen werden an die ServiceNow-Instanz gesendet.
Schema	Schema für UI-Komponenten. Dieses Feld muss leer bleiben.
Übersicht	Beschreibung für die Integration.
Autorisierte JavaScript-Ursprünge	Authentifizierungstoken aus dem Browser zum Aktivieren der Ursprünge der Seiten, von denen Anforderungen erstellt werden. Dieses Feld muss leer bleiben.

   d. Geben Sie im Abschnitt „Permissions“ (Berechtigungen) unter „Issue & Event“ (Problem und Ereignis) die gewünschte Zugriffsebene an.
   Sie können **Read** (Lesen), **Read & Write** (Lesen und Schreiben) oder **Admin** auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Aktivieren Sie im Abschnitt „Webhooks“ das Kontrollkästchen **Issue** (Problem).

f. Klicken Sie auf **Änderungen speichern**.

2. Erstellen Sie in der Sentry-Konsole Warnungsregeln, und konfigurieren Sie diese so, dass Warnungen für Probleme von Sentry an die ServiceNow-Instanz empfangen werden.

a. Navigieren zu **Warnungen** > **Warnungsregel erstellen**.

b. Wählen Sie den Warnungstyp aus, und klicken Sie auf **Set Conditions** (Bedingungen festlegen).

Hinweis: Vom Warnungstyp „Probleme“ werden Problemwarnungen erstellt. Von den anderen Warnungsoptionen werden Metrikwarnungen erstellt.

c. Erstellen Sie auf der Seite „Alert Rule“ (Warnungsregel) entweder eine Problemwarnung oder eine Metrikwarnung.

Warnungsregel

Optionen	Beschreibung
Issue alert (Problemwarnung)	**i.** Geben Sie die Umgebung, das Team und den Warnungsnamen für die Warnung ein. **ii.** Geben Sie unter „Set Conditions“ (Bedingungen festlegen) die Bedingungen **When** (Wann) und **If** (Wenn) ein, die die Warnung auslösen. **iii.** Wählen Sie für die Bedingung **Then** (Dann) die Option **Send a notification via an integration** (Benachrichtigung über eine Integration senden) aus, und wählen Sie die interne Integration aus der Liste aus. **iv.** Legen Sie das Aktionsintervall für die Warnung fest.
Metric Alert (Metrikwarnung)	**i.** Fügen Sie Ihren Transaktionen einen Filter hinzu. **ii.** Wählen Sie die Funktion und das Zeitintervall aus. **iii.** Legen Sie die Schwellenwerte fest, bei denen die Warnung ausgelöst wird. **iv.** Fügen Sie die Aktionen hinzu, die ausgeführt werden sollen, wenn die festgelegten Schwellenwerte erreicht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionen	Beschreibung
	v. Fügen Sie die interne Integration aus der Liste der Liste der Aktionen hinzu, um die Warnungen zu erhalten. **vi.** Fügen Sie einen Regelnamen und ein Team für die Warnung hinzu.

d. Klicken Sie auf **Save Rule** (Regel speichern).

Scout APM-Ereignisse integrieren

Aktivieren Sie die Sammlung von Ereignissen aus Scout APM, indem Sie Scout APM als Datenquelle authentifizieren, um es mit Ereignismanagementzu integrieren.

Vorbereitungen

Das Plugin „Ereignismanagement“ (com.glideapp.itom.snac) muss installiert sein.

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Discovery für Scout APM-Anwendungen wird nicht unterstützt. Zum Aktivieren der Bindung müssen Sie manuell ein CI in einer Instanz ServiceNow in der Tabelle „Serviceinstanz“ [cmdb_ci_service_auto] erstellen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Aktivieren Sie die Scout APM-Überwachung als Anwendungsservice in Ihrer Instanz ServiceNow.
   a. Navigieren zu **Konfiguration** > **Anwendungsservice**.
   b. Geben Sie den Namen der Anwendung an, die Sie überwachen.
   c. Legen Sie den Betriebsstatus auf Funktionsfähig fest.
   d. Wählen Sie **Weiter** aus.
   e. Wählen Sie **Fertig**.
2. Melden Sie sich bei der Scout APM-Konsole an.
3. Erstellen Sie einen Benachrichtigungskanal.

   a. Navigieren zu **Organisation** > **Warnungen und Benachrichtigungen**.

   b. Wählen Sie **New Webhook** (Neuer Webhook) aus.

   c. Geben Sie den Namen des Webhooks und die Webhook-URL an.
   Verwenden Sie das folgende URL-Format: `https://`<USERNAME> :<PASSWORD> @<INSTANCE_NAME> .service-now.com/api/sn_em_connector/em/inbound_event?source=scout

   d. Überprüfen Sie, ob der Webhook funktionsfähig ist, indem Sie **Send Test Alert (Testwarnung senden)**auswählen.
   Ein neues Ereignis wird in Ihrer Instanz ServiceNow in der Tabelle Ereignisse [em_event] mit „Scout APM“ als Datenquelle angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Erstellen Sie im Abschnitt „Organisation“ eine neue Benachrichtigungsgruppe.
   a. Navigieren Sie auf der Seite **Warnungen und Benachrichtigungen** zu **Organisation** > **Benachrichtigungsgruppen**.
   b. Fügen Sie einen Namen für die Gruppe hinzu, und wählen Sie den von Ihnen erstellten Webhook-Kanal aus.
   c. Wählen Sie die Schaltfläche **Benachrichtigungsgruppe erstellen aus**.
5. Erstellen Sie im Abschnitt „Anwendung“ Warnungsbedingungen, und konfigurieren Sie diese so, dass Warnungen für Benachrichtigungen von Scout APM an die Instanz ServiceNow empfangen werden.
   a. Navigieren zu **Anwendungen** > **Warnungsbedingungen**.
   b. Wählen Sie den Typ der Warnungsbedingung aus.
      Weitere Informationen finden Sie in der Scout APM-Dokumentation.
   c. Wählen Sie **Warnungsbedingung erstellen aus**.
   d. Wählen Sie in der Tabelle „Warnungsbedingungen“ die Benachrichtigungsgruppe aus, die Sie erstellt haben.
      Die Warnungsbedingung wird in der Scout-Konsole angezeigt.
6. Konfigurieren Sie Fehlerbenachrichtigungen, um Warnungen für Fehler von der Scout APM-Instanz an die Instanz ServiceNow zu erhalten.
   a. Navigieren zu **Anwendung** > **Fehlerbenachrichtigungen**.
   b. Fügen Sie einen Namen und eine Beschreibung für die Benachrichtigung hinzu.
   c. Wählen Sie die Benachrichtigungsgruppe aus, die Sie erstellt haben.
      Der Scout APM-Benachrichtigungskanal wird mit den Fehlerbenachrichtigungen konfiguriert.
   d. Wählen Sie die Schaltfläche **Benachrichtigungsgruppe hinzufügen**.
      Für jede neue Fehlerbenachrichtigung in der Scout APM-Anwendung wird ein neues Ereignis in der Ereignistabelle [em_event] generiert.

Ergebnisse

Sie können alle Benachrichtigungen in Ihrer Instanz ServiceNow in der Ereignistabelle [em_event] mit „Scout APM“ als Datenquelle anzeigen.

Integrieren Sie Sumo Logic-Ereignisse

Verwenden Sie den Sumo Logic-Push-Connector, um Sumo Logic mit Ereignismanagement zu integrieren, indem Sie der Sumo Logic-Plattform einen Standard-Webhook hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin des Connectors Ereignismanagement auf der Instanz Now Platform installiert ist.

Erforderliche Rolle: evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Umgebung Ereignismanagement für die Sammlung von Ereignissen von Sumo Logic, indem Sie Sumo Logic als Datenquelle authentifizieren. Legen Sie auf der Sumo Logic-Website Ihre Instanz Now Platform mit einem Webhook als REST-Endpunkt fest.

Prozedur

1. Erstellen Sie auf der Sumo Logic-Website ein Benachrichtigungsziel.
2. Wechseln Sie zu Überwachung, und wählen Sie **Anwenderdefinierter Webhook**aus.
3. Füllen Sie das Formular mit dem Namen, der Beschreibung und der URL aus.

   Verwenden Sie dieses URL-Format, um Ereignisse von Sumo Logic an die Instanz ServiceNow zu übertragen.`https://`<username> :<password> @<instance-name> .service-now.com/api/sn_em_connector/em/inbound_event?source=sumologic

   Hinweis: Verwenden Sie Anmeldeinformationen mit der Rolle evt_mgmt_integration als Anwendernamen und Passwort.

   Verwenden Sie im Abschnitt Payload (Nutzlast) die folgende Vorlage:

```
{
    "type": "{{MonitorType}}",
    "node": "{{ResultsJSON._sourceHost}}",
    "metric_name": "{{Name}}",
    "description": "monitor Query: {{Query}}\n Trigger
 Condition:{{TriggerCondition}}\n Trigger Value:{{TriggerValue}}\n
 Trigger Time Range:{{TriggerTimeRange}}\n View Trigger
 Query:{{TriggerQueryURL}}\n View Monitor:{{QueryURL}} \n
 Results:{{ResultsJSON}}",
    "name": "{{Name}}",
    "short_description": "{{Description}}",
    "MonitorType": "{{MonitorType}}",
    "Query": "{{Query}}",
    "QueryURL": "{{QueryURL}}",
    "ResultsJson": "{{ResultsJson}}",
    "NumQueryResults": "{{NumQueryResults}}",
    "Id": "{{Id}}",
    "DetectionMethod": "{{DetectionMethod}}",
    "TriggerType": "{{TriggerType}}",
    "TriggerTimeRange": "{{TriggerTimeRange}}",
    "time_of_event": "{{TriggerTime}}",
    "TriggerCondition": "{{TriggerCondition}}",
    "TriggerValue": "{{TriggerValue}}",
    "TriggerTimeStart": "{{TriggerTimeStart}}",
    "TriggerTimeEnd": "{{TriggerTimeEnd}}",
    "SourceURL": "{{SourceURL}}",
    "alertResponseUrl": "{{alertResponseUrl}}"
  }
```

   Ereignisse vom Typ „Protokollüberwachung“ können ohne CI-Bindung erstellt werden, da Sie den Knotenwert als „node“: „{{ResultsJSON._sourceHost}}“ in der Ereignisnutzlast von Sumo Logic erhalten. Sie können Ereignisse erstellen, aber Sie können sie nicht binden, da Sie sie nicht als Hostnamen für den Protokollüberwachungstyp erhalten. Ein Push-Connector-Parameter „create_log_monitorType_events“ mit dem Wert „falsch“ wurde erstellt. Wenn der Parameterwert „Falsch“ ist, wird die Nutzlast ignoriert, und es werden keine Protokollereignisse erstellt. Wenn Sie den Parameter in true ändern, werden Ereignisse erstellt, und Sie müssen dann Ereignisregeln für die CI-Bindung definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie in der ServiceNow folgenden Tabelle für Schweregradzuordnung mit Sumo Logic-Auslösertyp:

Schweregradzuordnung

Sumo Logic-Auslösertyp	Schweregrad
Kritisch	Kritisch
Warnung	Kleiner
MissingData	Warnung
ResolvedCritical/ResolvedWarning/ ResolvedMissingData	Leeren

Integrieren Sie Sumo Logic in das REST-API-Schlüsseltoken

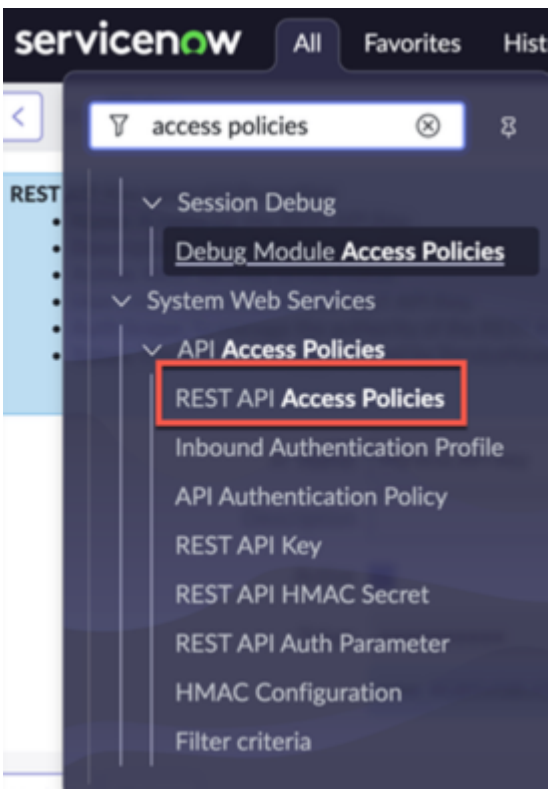
Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und erhöht die betriebliche Effizienz.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**.



2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

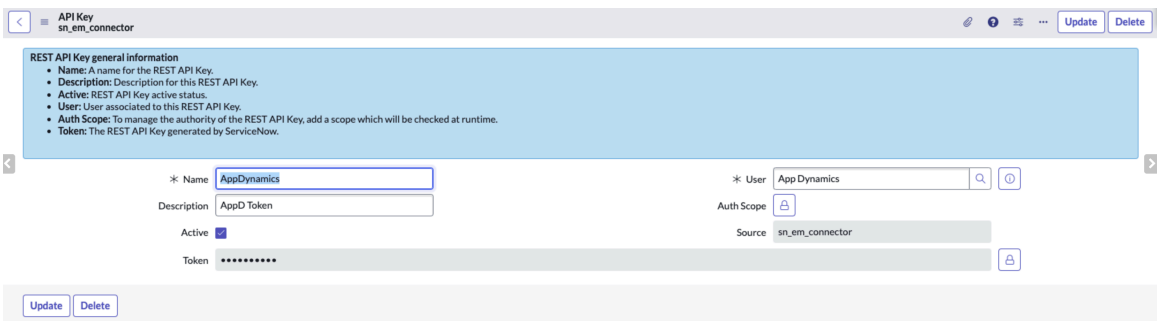
Hinweis: Der Anwender muss mit der Rolle evt_mgmt_integration erstellt werden. Erstellen Sie in der Tabelle „sys_user“ eine neue, um sie hier zu verwenden, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST-API-Schlüssels zu verwalten.
Token	Der von Now Platformgenerierte REST-API-Schlüssel. Kopieren Sie den Schlüssel, der als Teil des REST-API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.
Ablauf	Zeitpunkt, nach dem die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie hinzu: UserAccount.
5. Verwenden Sie das Formularmenü, und wählen Sie **Speichern**aus.

Das System generiert ein Token und speichert es im Feld **Token**. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie den Inhalt, der unter dem Feld angezeigt wird. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Integrieren Sie ThousandEyes-Plattformereignisse

Integrieren Sie ThousandEyes mit Ereignismanagement, indem Sie in der ThousandEyes-Konsole einen Standard-Webhook hinzufügen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Welche Authentifizierung verwendet wird

Die folgenden zwei Authentifizierungsmethoden sind verfügbar:

- OAuth-Authentifizierung: Bietet Authentifizierung auf Unternehmensebene, um die Sicherheit Ihrer Unternehmensumgebung zu gewährleisten. Die Authentifizierung erfolgt mit ThousandEyes Monitor V1- oder V2-Zugriffstoken. Weitere Informationen finden Sie unter Integrieren Sie ThousandEyes mit OAuth-Authentifizierung.
- Standard-Webhook-Authentifizierung: Bietet einen Basisstandard für die Authentifizierung, ohne dass ThousandEyes Active Directory erforderlich ist. Diese Authentifizierung kann besonders für verteilte kleine Teams wie SRE- oder DevOps -Teams nützlich sein. Weitere Informationen finden Sie unter Integrieren Sie ThousandEyes mit der Standardauthentifizierung.

Integrieren Sie ThousandEyes mit der Standardauthentifizierung

Integrieren Sie ThousandEyes mit Ereignismanagement, indem Sie einen Webhook in der ThousandEyes-Plattform hinzufügen.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Discovery für ThousandEyes-Services wird nicht unterstützt, daher müssen Sie manuell ein CI in der ServiceNow-Instanz erstellen, damit die Event-Bindung funktioniert.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus ThousandEyes, indem Sie ThousandEyes als Datenquelle authentifizieren. Legen Sie auf der ThousandEyes-Plattform Ihre Instanz der Now Platform mithilfe eines Webhooks als REST-Endpunkt fest.

Prozedur

1. Führen Sie in der ServiceNow-Instanz die folgenden Schritte aus, um ein CI zu erstellen.
   a. Navigieren Sie in der Navigationsleiste zu **Alle** > **Konfiguration** > **CI-Klassen Manager**.
   b. Klicken Sie auf **Hierarchie** und suchen Sie nach `HTTP(S)-Endpunkt`.
   c. Wählen Sie **CI-Liste** aus und erstellen Sie ein neues CI.
2. Erstellen Sie auf der ThousandEyes-Plattform ein Benachrichtigungsziel.
   a. Navigieren Sie in der Navigationsleiste zu **Warnungen** > **Warnungsregeln**.
   b. Klicken Sie auf eine vorhandene Warnungsregel und wählen Sie die Registerkarte **Notification** (Benachrichtigung) aus.
   c. Auswahlvorgang **Bearbeiten Sie den Webhook** und geben Sie die folgenden Informationen ein.

Webhooks bearbeiten

Feld	Beschreibung
Name	Geben Sie einen Namen für den Webhook ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
URL	Geben Sie die Webhook-URL an. **Hinweis:** Das Standardformat der URL zum Übertragen von Events von ThousandEyes an die ServiceNow-Instanz ist `https://<instance-name>.service-now.com/api/sn_em_connector/em/inbound_event?source=thousandeyes`.
Auth Type	Wählen Sie **Basic** (Standard) aus.

d. Klicken Sie auf **Add New Webhook** (Neuen Webhook hinzufügen).

Ergebnisse

Der Standardschweregrad für die ThousandEyes-Warnung ist **Schwerwiegend -2**und kann im Abschnitt *Push Connector Configuration* von geändert werden **Push-Connectors** > **ThousandEyes-Push-Connector**. Die gültigen Werte für „Schweregrad“ sind **1- Kritisch**, **2- Schwer**, **3- Gering**, **4- Warnung** und **5- Info**.

Die Standardzeitzone der ThousandEyes-Warnung ist GMT. Wenn Sie die Warnung in einer anderen Zeitzone senden möchten, kann dies im Abschnitt *Push Connector Configuration* von geändert werden **Push-Connectors** > **ThousandEyes-Push-Connector**. Das gültige Wertformat ist **GMT+01:00**, **GMT+02:00**, **GMT-05:30**, **GMT-02:00** usw.

Integrieren Sie ThousandEyes mit dem REST-API-Schlüsseltoken

Integrieren Sie mithilfe eines API-Schlüssels, um eine sichere Kommunikation herzustellen und den Datenaustausch über die REST-API zu automatisieren. Dies vereinfacht die Integration, ermöglicht einen nahtlosen Zugriff auf Services und erhöht die betriebliche Effizienz.

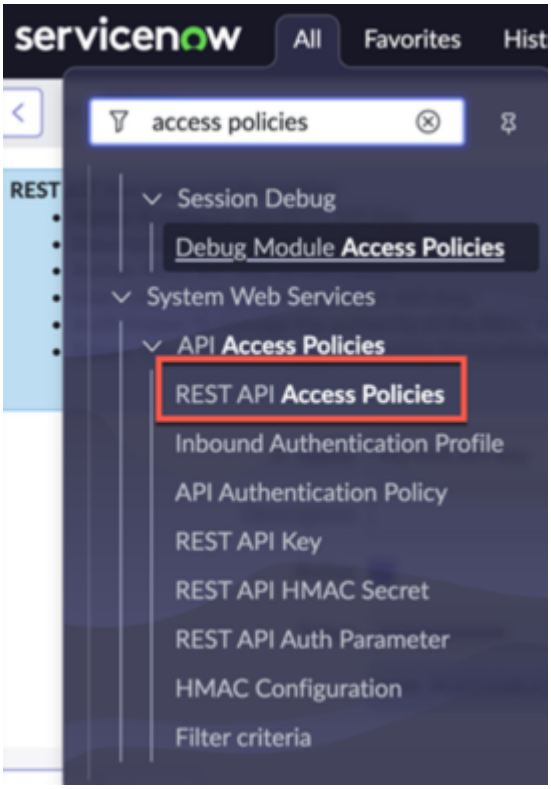
Vorbereitungen

Erforderliche Rolle: evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **System-Webservices** > **API-Zugriffsrichtlinien** > **REST-API-Schlüssel**.



2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

> **Hinweis:** Der Anwender muss mit der Rolle evt_mgmt_integration erstellt werden. Erstellen Sie in der Tabelle „sys_user“ eine neue, um sie hier zu verwenden, um den richtigen Zugriff zu erleichtern.

API-Schlüssel

Feld	Beschreibung
Name	Name zur Identifizierung des REST API-Schlüssels
Beschreibung	Beschreibung für den REST API-Schlüssel.
Aktiv	Status des REST API-Schlüssels.
Anwender	Anwender, der dem REST API-Schlüssel zugeordnet ist. Verwenden Sie das Suchsymbol, um den Anwender auszuwählen.
Authentifizierungsbereich	Option zum Hinzufügen des Authentifizierungsbereichs, um die Berechtigung des REST-API-Schlüssels zu verwalten.
Token	Der generierte REST-API-Schlüssel. Kopieren Sie den Schlüssel, der als Teil des REST-

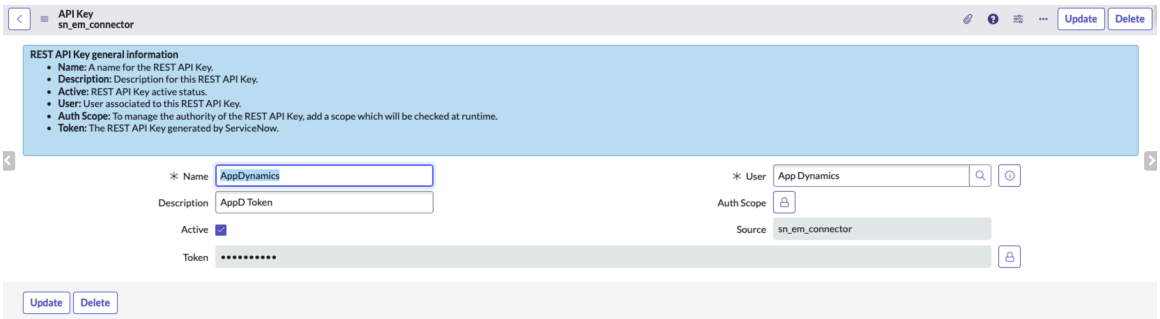
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	API-Aufrufs innerhalb des Header- oder Abfrageparameters verwendet werden soll.
Ablauf	Zeitpunkt, nach dem die Anmeldeinformationen nicht mehr gültig sind. Ein leerer Wert bedeutet keinen Ablauf.

4. Entsperren Sie den Authentifizierungsbereich, und fügen Sie hinzu: UserAccount.
5. Verwenden Sie das Formularmenü, und wählen Sie **Speichern**aus.

   Das System generiert ein Token und speichert es im Feld **Token**. Um das Token anzuzeigen, verwenden Sie das Sperrsymbol, und kopieren Sie den Inhalt, der unter dem Feld angezeigt wird. Dies ist der Wert Ihres Abfrageparameters (oder Headers), wenn Ihr anderes System eine REST-API-Anforderung an ServiceNow sendet.



Ergebnisse

Jetzt können Sie mit dem Senden von Ereignissen beginnen. In Ihrem Überwachungstool können Sie Ereignisse entweder mit dem Header oder dem Abfrageparameter senden `: x-sn-apikey`. Zum Beispiel:

```
https://[INSTANCENAME].service-now.com/api/sn_em_connector/em/inbound_event?source=[SOURCENAME]&sys_id=[SYSID OF PUSH CONNECTOR
 INSTANCE]&x-sn-apikey=[AUTH TOKEN]
```

Integrieren Sie ThousandEyes mit OAuth-Authentifizierung

Erstellen Sie Anmeldeinformationen in der Instanz, und konfigurieren Sie den ThousandEyes-Webhook.

Vorbereitungen

Erforderliche Rolle: web_service_admin

Prozedur

1. Navigieren zu **Alle** > **System-OAuth** > **Applikationsregistrierung** und wählen Sie **Neu**aus.
2. Wählen Sie **OAuth-API-Endpunkt für externe Clients erstellen aus**.
3. Kopieren Sie das automatisch generierte Feld **Client-ID**.
   Die **Client-ID** wird bei der Konfiguration der ThousandEyes-SeviceNow-Integration verwendet.
4. Entsperren Sie das Feld **„Umleitungs-URL“**, und weisen Sie den folgenden Wert zu: **https://app.thousandeyes.com/webhooks-oauth-callback/**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Konfigurieren Sie die Lebensdauer von Zugriffs- und Aktualisierungstoken, indem Sie einen Wert in Sekunden angeben.
6. Öffnen Sie die ThousandEyes-Webhook-Konfiguration, und füllen Sie die folgenden Felder aus:

   Name

   Beliebiger Name

   URL

   Endpunkt des ThousandEyes-Push-Connectors von ServiceNow

   Authentifizierungstyp auswählen

   OAuth

   Gewährungstyp

   Implizit

   Auth-URL

   https://servicenow_instanz>.service-now.com/oauth_auth.do

   Client-ID

   Fügen Sie die in Schritt 3 automatisch generierte Client-ID ein.

7. Wählen Sie **Token abrufen**aus.
8. Sobald der ThousandEyes-Connector zu einer Webseite navigiert ist, auf der eine Verbindung zu Ihrem ServiceNow-Account angefordert wird, wählen Sie **Zulassen aus**.
9. Geben Sie Account-Anmeldeinformationen an, die über die Rolle **„web_service_admin“** verfügen.

Panopta als Datenquelle integrieren

Integrieren Sie die cloudbasierte Überwachungslösung von Panopta in Ereignismanagement. Zum Hinzufügen von Panopta als Datenquelle ist eine Konfiguration in Panopta erforderlich.

Konfigurieren Sie Panopta

Um Panopta als Datenquelle vorzubereiten, folgen Sie dem Verfahren, das unter diesem Link beschrieben wird: Wie kann ich ServiceNow integrieren?

Wenn die Ereignismanagement-Integration in Panopta konfiguriert ist, fügen Sie die Integration einer Ihrer Panopta-Warnungszeitachsen hinzu, damit die ServiceNow-Instanz Incident-Events entsprechend empfängt.

Optionale Ereignismanagement-Konfiguration

Konfigurieren Sie eine Warnungsaktionsregel für den Start im Kontext von Panopta. Weitere Informationen finden Sie unter Webanwendung aus Warnung starten und Warnungsaktionsregel erstellen oder bearbeiten.

Zugehörige Informationen

Konfigurieren Sie Ereignismanagement die -Connectors

Event-Connector für Event Integration Format (EIF) integrieren

Verwenden Sie den Push-Connector, mit dem Events von Produkten (im Allgemeinen von IBM) weitergeleitet werden können, die das EIF-Format (Event Integration) an einen MID-Server unterstützen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector)“ in der Instanz Now Platform installiert ist.

Stellen Sie sicher, dass dem MID Server entweder `EventManagement` oder `ALLE Anwendungen` zugewiesen sind.

Erforderliche Rolle: evt_mgmt_integration

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Ereignismanagement-Umgebung für die Erfassung von Events aus Produkten, die das EIF-Format unterstützen, an einen MID-Server.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Kontext des EIF-Listeners**.
2. Klicken Sie auf **Neu**.
3. Erstellen Sie einen neuen EIF-Listener-Kontext, indem Sie das entsprechende Formular ausfüllen:

   a. Füllen Sie die Felder des Formulars aus.

Formular „Kontext des EIF-Listeners“

Feld	Beschreibung
Name	Eindeutiger Name für den EIF-Listener-Kontext.
Kurzbeschreibung	Kurzbeschreibung des Ausführungskontexts der MID-Server-Erweiterung.
Port	Port für den EIF-Listener zum Empfangen von EIF-Events. Der Standardwert ist **9998**. Wenn der Port jedoch bereits verwendet wird, können Sie stattdessen einen anderen freien Port verwenden.
Status	Status des EIF-Listener. Dieses Feld ist leer, bis der Listener ausgeführt wird. Nachdem der Listener ausgeführt wurde, wird der Wert automatisch auf einen der folgenden Status gesetzt: ▪ Gestartet: Der Listener läuft. ▪ Angehalten: Der Listener läuft nicht. ▪ Offline: Der MID-Server ist nicht verfügbar. ▪ Fehler: Der Listener ist mit einem Fehler fehlgeschlagen.
Ausführen auf	MID-Server-Verzeichnis für die Ausführung dieses Listener.
MID Server	Den Namen des dedizierten MID-Server, wenn Sie **Spezifischer MID Server** im Feld **Ausführen auf** ausgewählt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ausführung auf	Name des MID-Server, auf dem die Erweiterung ausgeführt wird. Dieses Feld wird automatisch mit dem Namen des MID-Server gefüllt, auch wenn er nicht verfügbar ist. Wenn Sie die Erweiterung stoppen, ist dieses Feld leer.

b. Im Formular können Sie auf die zugehörigen Links im Formular „Kontext des EIF-Listeners“ klicken.

Im Formular „Kontext des EIF-Listeners“ verfügbare Befehle

Zugehöriger Link	Beschreibung
Start	Wählen Sie diese Option, wenn der Listener nicht ausgeführt wird. Der Listener wird auf dem konfigurierten MID-Server mit der konfigurierten Portnummer gestartet.
Stoppen	Wählen Sie diese Option, um den ausgeführten Listener auf dem konfigurierten MID-Server anzuhalten.
Neu starten	Klicken Sie hierauf, um den Listener auf dem konfigurierten MID-Server mit der Portnummer zu starten.
Parameter aktualisieren	Wählen Sie diese Option, wenn Sie Änderungen an der Listener-Konfiguration des derzeit ausgeführten Listener vornehmen möchten. Wenn die Parameter gültig sind, trennt sich der Listener und stellt die Verbindung mit den neuen Parametern wieder her.
Parameter testen	Wählen Sie diese Option, um zu testen, ob der Port eine gültige Nummer ist.

4. Wenn Sie fertig sind, klicken Sie mit der rechten Maustaste auf den Formularheader, und wählen Sie **Speichern** aus.
5. Klicken Sie auf **Aktualisieren**.
6. Wenn Sie den eingehenden EIF-Datenverkehr überprüfen möchten, gehen Sie wie folgt vor:
   a. Navigieren zu **MID-Server** > **Server**.
   b. Wählen Sie den MID-Server aus, auf dem die EIF-Erweiterung ausgeführt wird.
   c. Fügen Sie auf der Registerkarte **Konfigurationsparameter** die **mid.log.level**-Eigenschaften hinzu.

Nächste Maßnahme

Wenn der MID-Server nicht gestartet werden kann, können Sie die MID-Server-Protokollfehler überprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schweregrad von Warnungen bezüglich EIF-Events

Wenn die Nutzlast des EIF-Event einen Warnungsschweregrad hat, wird sie in der ServiceNow-Instanz anders zugeordnet.

Schweregrad von EIF-Events	Schweregradzuordnung von ServiceNow-Events
UNBEKANNT	Warnung
Warnung	Kleiner
Kleiner	Schwerwiegend
Kritisch	Kritisch
Fatal (Schwerwiegend)	Kritisch

Erstellen Sie einen Push-Connector-Konfigurationsparameter

Einige Connectors haben keine standardmäßigen Parameter. Daher ist es erforderlich, den Parameter zu erstellen und der Liste der Push-Connector-Konfigurationen im Formularlayout hinzuzufügen, bevor Sie den neuen Parameter hinzufügen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, personalize_form

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Push-Connectors**.
2. Öffnen Sie einen Push-Connector.
3. Klicken Sie im Formular **„Push-Connector“** mit der rechten Maustaste auf den Formularheader, und wählen Sie **Konfigurieren** > **Formularlayout**.
4. Suchen Sie in der Liste **Verfügbar** nach **Push-Connector-Konfigurationen** > **Push-Connector**, und verschieben Sie sie in die Liste **Ausgewählt**.
5. Wählen Sie **Speichern**.
6. Doppelklicken Sie in der Tabelle Push-Connector-Konfigurationen [sn_em_connector_push_config] auf **Neue Zeile einfügen**, um einen neuen Push-Connector-Konfigurationsparameter hinzuzufügen.
7. Wählen Sie **Aktualisieren**.

Ergebnisse

Liste der Push-Connector-Konfigurationen zum Push-Connector-Formularlayout hinzugefügt. Sie können jetzt Push-Connector-Parameter erstellen.

Konfigurieren Sie eine Push-Connector-Instanz .

Konfigurieren Sie eine Push-Connector-Instanz, um die Ereignisse von einem externen System zu empfangen.

Vorbereitungen

Stellen Sie sicher, dass Sie eine Push-Connector-Definition definiert haben.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Connector-Instanz verwenden, um die Ereignisse aus externen Quellen zu empfangen. Sie können die folgenden Arten von Push-Connector-Instanzen erstellen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Instanztyp
- MID-Typ

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Push-Connector-Instanzen**.
2. Wählen Sie die Connector-Instanz aus, die Sie konfigurieren möchten, oder wählen Sie**Neu**,um eine Push-Connector-Instanz zu erstellen.
3. Füllen Sie die Felder im Formular **„Push-Connector-Instanz“** aus.

   Weitere Einzelheiten finden Sie unter Formular der Push-Connector-Instanz.
4. Wählen Sie **Absenden** oder **Aktualisieren** aus.

Ergebnisse
Das Formular der Push-Connector-Instanz wird gespeichert, und jetzt können Sie die Ereignisse von einem externen System empfangen.

Konfigurieren Sie die Event-Erfassung für SNMP-Traps

Der SNMP-Listener wird auf dem MID Server ausgeführt, der als Erfassungsendpunkt für SNMP-Traps fungiert. Der MID Server sendet die Traps zur weiteren Verarbeitung als Event von Ereignismanagement an die ServiceNow-Instanz.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator
Stellen Sie sicher, dass dem MID Server entweder `EventManagement` oder `ALLE Applikationen`zugewiesen sind.

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie den **MID-SNMP-Trap-Listener**, um auf SNMP-Traps zu warten. In dieser Konfiguration fungiert der angegebene MID Server als Erfassungsendpunkt für SNMP-Traps.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **MID-SNMP-Trap-Listener**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie das Formular „SNMP-Trap-Sammlungskontext“ aus.

Option	Beschreibung
Name	Eindeutiger Name für den SNMP-Trap-Sammler.
Kurzbeschreibung	Eine Kurzbeschreibung des Ausführungskontexts der MID Servererweiterung
SNMP-Version	Geben Sie die SNMP-Version an: ◦ v1 und v2c ◦ v3
Minimale Sicherheitsstufe	Die gültigen Sicherheitsstufenwerte sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	◦ Keine – Kein Sicherheitsstufenwert festgelegt. ◦ noAuthnoPriv – Kommunikation ohne Authentifizierung und Datenschutz ◦ authNoPriv – Kommunikation mit Authentifizierung, aber ohne Datenschutz ◦ authPriv – Kommunikation mit Authentifizierung und Datenschutz **Hinweis:** Dieses Feld wird nur angezeigt, wenn `v3` im Feld **SNMP-Version** ausgewählt ist.
UDP-Port	UDP-Port für den SNMP-Trap-Sammler zum Empfangen von SNMP-Traps. Der Standardwert ist *1,162*. Wenn der Port jedoch bereits verwendet wird, können Sie stattdessen einen anderen freien Port verwenden.
Status	Der Status des Trap-Listeners. Dieses Feld ist leer, bis der Listener ausgeführt wird. Nachdem der Listener ausgeführt wurde, wird der Wert automatisch in einen der folgenden Status eingetragen: ◦ **Gestartet**: Der Listener läuft. ◦ **Angehalten**: Der Listener läuft nicht. ◦ **Offline**: Der MID Server ist nicht erreichbar. ◦ **Fehler:** Der Listener ist mit einem Fehler fehlgeschlagen.
Ausführen auf	Der Standort des MID Servers für die Ausführung dieses Listeners. Wählen Sie aus: ◦ Spezifischer MID Server ◦ Spezifisches MID Server-Cluster Die empfohlene Einstellung ist **Spezifischer MID Server**. Netzwerkhardware muss normalerweise für das Senden an eine bestimmte IP-Adresse konfiguriert werden. Wenn der Listener beispielsweise auf einen anderen MID Server im Cluster verschoben wird, wird die Trap nicht empfangen.
MID Server	Geben Sie Folgendes an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	◦ Den Namen des dedizierten MID Servers, wenn Sie im Feld **Ausführen auf Spezifischer MID Server** ausgewählt haben. ◦ Den Namen des dedizierten MID Server-Clusters, wenn Sie im Feld **Ausführen auf Spezifischer MID Server-Cluster** ausgewählt haben. Wenn Sie **Spezifischer MID Server-Cluster** ausgewählt haben, bestimmt ein ServiceNow-Algorithmus, welcher Server im Cluster den Listener ausführt.
EngineID	Wird nur angezeigt, wenn **SNMP-Version = v3**. ◦ Wenn Sie eine SNMP-Inform-Nachricht senden, geben Sie den Standardwert dieses Felds in die Nachricht ein. ◦ Wenn Sie eine SNMP-Trap-Nachricht senden, geben Sie einen anderen Wert als den Standardwert dieses Felds in die Nachricht ein.
Ausführung auf	Der Name des MID Servers, auf dem die Erweiterung ausgeführt wird. Dieses Feld zeigt den Namen des MID Servers an, auch wenn der MID Server nicht erreichbar ist. Wenn Sie die Erweiterung stoppen, ist dieses Feld leer. Dieses Feld wird automatisch ausgefüllt.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Geben Sie im Abschnitt **Anmeldeinformationen für SNMPs** die erforderlichen SNMP v3-Anmeldeinformationen an, die der SNMP-Listener für die Authentifizierung verwendet.

   Hinweis: Der Abschnitt **Anmeldeinformationen für SNMPs** wird nur angezeigt, wenn `v3` im Feld **SNMP-Version** ausgewählt ist.

6. Klicken Sie im Abschnitt **Zugehörige Links** auf **Parameter testen**.
7. Klicken Sie auf **Aktualisieren**.
8. Wahlweise: Wenn der MID Server nicht gestartet werden kann, überprüfen Sie die MID Server-Protokollfehler.

   (Optional) Beim Arbeiten mit Objektbezeichnern (OIDs) kann der OID-Trap-Zähler Probleme beim Aktivieren von Event-Regeln verursachen. Um den Trap-Zähler aus der OID zu entfernen, navigieren Sie zu **MID-Server** > **Eigenschaften** und legen Sie die Eigenschaft **mid.em.snmp_old_key_counter_cut.enabled** auf **true**fest.

Nächste Maßnahme

In **Zugehörige Links** können diese Aktionen für den SNMP-Traps-Listener ausgeführt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im SNMP-Trap-Listener-Formular verfügbare Befehle

Zugehöriger Link	Beschreibung
Starten	Wenn er derzeit nicht ausgeführt wird, wird der Listener gestartet. Der Listener wird auf dem konfigurierten MID Server und der konfigurierten Portnummer gestartet.
Stoppen	Stoppt den laufenden Listener auf dem konfigurierten MID Server. Wenn der Listener nicht ausgeführt wird, wird keine Aktion ausgeführt.
Neu starten	Stoppt und startet den Listener auf dem konfigurierten MID Server und der Port-Nummer.
Testparameter	Testet, ob der Port eine gültige Zahl ist.
Parameter aktualisieren	Wenn Sie Änderungen an der Listener-Konfiguration vornehmen, aktualisieren Sie die Parameter des derzeit ausgeführten Listeners mit dieser Option. Zunächst werden die Parameter auf Gültigkeit getestet. Wenn die Parameter gültig sind, trennt sich der Listener und stellt die Verbindung mit den neuen Parametern wieder her.

Hinweis: Aktualisierungen des SNMP-Trap-Listeners werden erst wirksam, nachdem Sie auf **Neu starten** oder **Parameter aktualisieren** geklickt haben.

Zugehörige Informationen

SNMP Probe MIB Module

SNMP-Traps-Listener für den Empfang von OEM-Traps konfigurieren

SNMP-Traps-Listener für den Empfang von OEM-Traps konfigurieren

Konfigurieren Sie den SNMP-Trap-Listener für den Empfang von Traps von Oracle Enterprise Manager (OEM).

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Ereignismanagement kann Oracle Enterprise Manager Cloud Control-SNMP-Traps als Events verarbeiten. Damit der SNMP-Trap-Listener Traps von OEM erhalten kann, müssen Sie den MID-Server, der den SNMP-Trap-Listener ausführt, als Empfänger des Trap angeben. Nach Erhalt eines OEM-Trap sendet der MID-Server sie zur weiteren Verarbeitung als Event von Ereignismanagement an die ServiceNow-Instanz.

Die `OEM 12c-Trap-` Event-Regel wird mit der Standardbasisinstanz sowie den folgenden Warnungsaktionsregeln bereitgestellt:

- `Oracle EM Launch – Zielstatus`
- `Oracle EM Launch – Event anzeigen`

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **MID-SNMP-Traps-Listener**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder wie in Konfigurieren Sie die Event-Erfassung für SNMP-Traps beschrieben aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie für das Feld **SNMP-Version** Folgendes aus: `v1 und v2c`.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Konfigurieren Sie in Oracle Enterprise Manager Cloud Control den MID-Server als Trap-Listener-Ziel.

SNMP-Trap-Erfassung für hohe Verfügbarkeit konfigurieren

Für SNMP-Traps muss für den MID-Server ein Failover für den Trap-Listener konfiguriert werden.

Aus Failover-Gründen können Sie zwei MID Servers konfigurieren. Da der SNMP-Trap-Listener auf dem MID-Server eingehenden Datenverkehr über die IP-Adresse und den Port des MID-Server empfängt, konfigurieren Sie jeden MID-Server so, dass er dieselben SNMP-Traps empfängt. Zu jedem Zeitpunkt ist nur ein MID-Server aktiv. Daher erhält Event Management keine doppelten Traps.

Nachrichtenschlüssel konfigurieren, um SNMP-Objektbezeichner zu verbreiten

Standardmäßig werden die meisten SNMP-Trap-Events von einem einzelnen Ereignismanagement-Verarbeitungsauftrag verarbeitet. Dies kann die Event-Verarbeitung beeinträchtigen. Konfigurieren Sie Nachrichtenschlüssel auf dem MID-Server, um sicherzustellen, dass mehr als ein Verarbeitungsauftrag aufgerufen wird, um eine optimale SNMP-Trap-Performance zu gewährleisten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Server**.
   Die Seite **MID Server** wird geöffnet.
2. Wählen Sie den entsprechenden MID-Server aus, und wählen Sie auf der MID-Server-Seite die Registerkarte **Konfigurationsparameter** aus.
3. Klicken Sie auf **Neu**.
4. Wählen Sie im Feld **Parametername** die Option *`mid.snmp.event.oid.keys`* aus.
5. Geben Sie im Feld **Wert** eine kommagetrennte Liste von OIDs ein, die für den Nachrichtenschlüssel verwendet werden sollen.
6. Klicken Sie auf **Absenden**.

   Hinweis: Der OID-Trap-Zähler kann Probleme beim Aktivieren von Event-Regeln verursachen. Um den Trap-Zähler aus der OID zu entfernen, navigieren Sie zu **MID-Server** > **Eigenschaften** und legen Sie die Eigenschaft **mid.em.snmp_oid_key_counter_cut.enabled** auf **true**fest.

7. So legen Sie in einem Skript Bedingungen fest, die den zu verwendenden Nachrichtenschlüssel basierend auf den empfangenen SNMP-Traps bestimmen:
   a. Navigieren zu **MID-Server** > **Skripteinbindungen**.
   b. Suchen und wählen Sie **SNMPTrapKeyFilter** aus.
   c. Im Feld **Skript** legen Sie basierend auf dem empfangenen SNMP-Trap-Event Bedingungen fest, für die OIDs verwendet werden sollen.
   d. Aktivieren Sie die Checkbox **Aktiv**, um das Skript zu aktivieren.
   e. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Erfassung per E-Mail konfigurieren

Konfigurieren Sie eine Aktion für eingehende E-Mails, um E-Mail-Benachrichtigungen zu senden, wenn Events und Warnungen ausgelöst werden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie eine Aktion für eingehende E-Mails zum Senden von E-Mails hinzufügen, verwendet Ereignismanagement Aktionen für eingehende E-Mails, um eingehende E-Mails auf die gleiche Weise wie jedes externe Event zu verarbeiten. Der E-Mail-Inhalt wird zum Generieren und Aktualisieren von Events verwendet. Verwenden Sie Regeln zum Generieren von Warnungen oder ändern Sie den Event-Schweregrad. Der Schweregrad wird nach der Auswirkungsberechnung aktualisiert und in der Tabelle em_impact_status gespeichert.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **E-Mail-Eigenschaften**.
2. Wählen Sie im Abschnitt **Konfiguration für eingehende E-Mails** unter **E-Mail-Empfang aktiviert** die Option **Ja** aus, um die Erfassung von Events per E-Mail zu ermöglichen.
3. Um die E-Mail-Informationen zu konfigurieren, die für die Ereignis- und Warnungsverarbeitung an Ereignismanagement übergeben werden, navigieren Sie zu **Systemrichtlinie** > **E-Mail** > **Eingehende Aktionen** Suchen Sie in der Liste der Datensätze mit Aktionen für eingehende E-Mails nach dem Standardformular **zum Erstellen eines Ereignisse**, und öffnen Sie es.

   a. Geben Sie im Formular **„Aktionen für eingehende E-Mails“** diese Werte an.

Feld	Wert
Aktiv	Aktivieren Sie die Checkbox, um die E-Mail-Benachrichtigung zu aktivieren.
Zieltabelle	Wählen Sie **Event [em_event]** aus.
Aktionstyp	Wählen Sie **Datensatz für Aktion** aus.

   b. Wählen Sie die Registerkarte **Beschreibung** aus, und geben Sie eine Beschreibung für die E-Mail-Nachricht ein.

   c. Wählen Sie die Registerkarte **Aktionen** und anschließend diese **Feldaktionen**aus.

   - **[Schweregrad] [An] [<Event-Schweregrad>]**
   - **[Typ] [E-Mail von] [<Teil der E-Mail>]**

     Beispielsweise können Sie **Betreff** als den zu verwendenden Teil der E-Mail auswählen.

4. Fügen Sie ein **Skript** hinzu, um die Eingangsparameter anzupassen und den Text Event-Variablen zuzuordnen.

   Example
   Beispiel:

```
current.source = 'email';
current.event_class = 'email';
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
current.description = email.body_text;
current.time_of_event = new GlideDateTime();
current.insert();
```

5. Senden Sie von der Instanz aus eine E-Mail mit übereinstimmenden Daten, und bestätigen Sie dann, dass die Event- oder Warnungsinformationen in Ereignismanagement angezeigt werden.
   Weitere Informationen zum Senden von E-Mail-Nachrichten zum Erstellen einer -Instanz finden Sie unter Aktionen für eingehende E-Mails .

   Hinweis: Stellen Sie sicher, dass der Benutzer, der die E-Mail sendet, die Rolle **evt_mgmt_integration** hat.

6. Wählen Sie **Absenden**.

Ergebnisse
Die eingehende E-Mail wird an die Tabelle em_event gesendet, und reguläre Ereignismanagement-Prozesse werden fortgesetzt, z. B. werden Event-Regeln und Warnungs-Management-Regeln ausgeführt.

Ereignisweiterleitung

Beschleunigen Sie den Lebenszyklus von Ereignisverarbeitungstests, indem Sie einen Stream von Ereignissen aus Ihrer Produktionsumgebung ServiceNow an Ihre Umgebung außerhalb der Produktion weiterleiten.

Verwenden Sie die Ereignisweiterleitung, um Ereignisse von einer Instanz an eine andere weiterzuleiten, z. B. von einer Produktionsinstanz an eine Instanz außerhalb der Produktion. Mit der Ereignisweiterleitung können Sie Ereignisregeln, Ereignisfeldzuordnungen, Warnungsverwaltungsregeln, Warnungskorrelation usw. testen und bewerten, ohne dass dies Auswirkungen auf Ihre Produktionsumgebung hat.

Nicht alle Überwachungsquellen können Ereignisse an mehrere Zielinstanzen senden. In solchen Fällen können Sie eine geplante Aufgabe konfigurieren, um den Ereignis-Stream regelmäßig von der Instanz ServiceNow, die mit der überwachten Quelle verbunden ist, an andere Instanzen weiterzuleiten.

Richten Sie die Ereignisweiterleitung ein

Erstellen Sie einen Konfigurationsdatensatz für die Ereignisweiterleitung, um den Flow von Ereignissen von einer ServiceNow -Instanz zu einer anderen Instanz zu ermöglichen. Die Weiterleitung von Ereignissen an mehrere Zielinstanzen erfordert das Erstellen separater Konfigurationsdatensätze für jede Zielinstanz.

Vorbereitungen
Sie müssen über Anmeldeinformationen mit der Rolle evt_mgmt_integration verfügen, um Ereignisse in der Zielinstanz zu erstellen. Wenn Sie nicht über diese Anmeldeinformationen verfügen, finden Sie unter Erstellen Sie Anmeldeinformationen für den Standardauthentifizierungs-Server Informationen zum Erstellen von Anmeldeinformationen.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Quellinstanz, die Ereignisse an eine Zielinstanz weiterleitet, muss einen Benutzer mit der Rolle evt_mgmt_integration, ein Passwort für die Anmeldeinformationen und einen neuen Ereignis-Weiterleitungsdatensatz aufweisen. Die Zielinstanz, die Ereignisse von der Quelle empfängt, muss über Anmeldeinformationen mit demselben Anwendernamen und Passwort wie die Quellinstanz verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Ereignisweiterleitungsdatensatz enthält Details zur URL der Zielinstanz ServiceNow, an die Ereignisse weitergeleitet werden sollen, sowie die Anmeldeinformationen, um eine Verbindung herzustellen.

Sie müssen für jede Zielinstanz einen separaten Konfigurationsdatensatz erstellen, um Ereignisse an mehrere Zielinstanzen weiterzuleiten. Anschließend werden Ereignisse an alle Zielinstanzen mit einer aktiven Konfiguration für die Ereignisweiterleitung gesendet.

Prozedur

1. Navigieren Sie in Ihrer Quellinstanz zu **Alle** und geben Sie im Filternavigator `sn_em_connector_event_sync_configuration.list` ein.
2. Wählen Sie auf der Seite **„Ereignissynchronisierungskonfigurationen“Neu**.
3. Geben Sie auf der Seite **„Konfiguration der Ereignissynchronisierung“** im Feld **Instanz-URL** die Ziel-URL ServiceNow für den Empfang von Ereignissen im Format `https://`ein.<your_instance> .service–now.com .
4. Geben Sie im Feld **Anmeldeinformationen** die Anmeldeinformationen für die Zielinstanz an, indem Sie sie eingeben oder danach suchen.
   - Um Ihre Anmeldeinformationen einzugeben, beginnen Sie mit der Eingabe, und wählen Sie dann die Anmeldeinformationen aus der Dropdown-Liste aus.
   - Um nach Ihren Anmeldeinformationen zu suchen, wählen Sie das Symbol „Nachschlagen mit Liste“ ( ), um Ihre Anmeldeinformationen aus der Suchtabelle für Anmeldeinformationen auszuwählen.
5. Wählen Sie **Speichern**.
6. Wählen Sie **Testverbindung** aus, um die Verbindung zur Zielinstanz ServiceNow zu validieren.
   - Wenn die Verbindung erfolgreich war, wird eine Bestätigungsmeldung angezeigt.
   - Wenn die Verbindung nicht erfolgreich ist, überprüfen Sie Ihre Anmeldeinformationen und die Instanz-URL.
7. Aktivieren Sie nach der Validierung das Kontrollkästchen **Aktiv**, um die Ereignisweiterleitung an die Zielinstanz zu aktivieren, und wählen Sie **Absenden**aus.
   Die Konfiguration wird erstellt und auf der Seite **„Konfigurationen der Ereignissynchronisierung“** aufgeführt.
8. Wiederholen Sie bei mehreren Zielen die Schritte für einen separaten Konfigurationsdatensatz für jede Instanz.

Zugehörige Informationen

Führen Sie regelmäßig einen Ereignisweiterleitungsauftrag aus

Führen Sie regelmäßig einen Ereignisweiterleitungsauftrag aus

Planen Sie einen Ereignisweiterleitungsauftrag, um regelmäßig Ereignisse an alle Zielinstanzen mit aktiven Ereignisweiterleitungskonfigurationen zu senden, wenn die Überwachungsquelle keine Ereignisse an mehrere Zielinstanzen senden kann.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können das Verhalten des Auftrags *`event-forwarding`* über zugehörige Systemeigenschaften anpassen. Weitere Informationen finden Sie unter Eigenschaften für die Ereignisweiterleitung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Um die Auswirkungen auf die Leistung zu minimieren, sendet die regelmäßige Aufgabe Ereignisse, die nicht älter als die letzte Stunde sind, als sie nach dem Einrichten der Ereignisweiterleitung zum ersten Mal ausgeführt wurde.

Prozedur

1. Navigieren zu **Alle** > **Geplante Aufgaben** > **Ereignismanagement – Ereignissynchronisierungsauftrag**.
2. Aktivieren Sie auf der Seite **„Geplante Skriptausführung“** das Kontrollkästchen **Aktiv**.
3. Legen Sie im Feld **Wiederholungsintervall** das entsprechende Zeitintervall für die regelmäßige Ausführung der Aufgabe fest.

   Standardmäßig wird die Aufgabe jede Minute ausgeführt.
4. Wählen Sie **Aktualisieren**.

Ergebnisse

Der Ereignisweiterleitungsauftrag wird basierend auf dem von Ihnen festgelegten Wiederholungsintervall regelmäßig ausgeführt. Ereignisse werden an alle Zielinstanzen ServiceNow gesendet, die über aktive Konfigurationsdatensätze für die Ereignisweiterleitung verfügen.

Wenn das Administratorkonto deaktiviert ist, konfigurieren Sie den Benutzer für die geplante Aufgabe. Standardmäßig ist dies „admin“, in diesem Fall muss dies jedoch geändert werden.

Hinweis:

Wenn die Weiterleitung des Ereignisses an die Instanz aus irgendeinem Grund fehlgeschlagen ist, wird im Feld **Letzter Synchronisierungsstatus** die Meldung `Fehlgeschlagen` angezeigt. Im Feld **Letzter Synchronisierungsfehler** wird eine entsprechende Fehlermeldung angezeigt. Die Zielinstanz generiert während der nächsten erfolgreichen Ereignisweiterleitung ein Eigensystem-Überwachungsereignis, das den Fehler der Ereignisweiterleitung für den angegebenen Zeitraum angibt.

Erstellen Sie Anmeldeinformationen für den Standardauthentifizierungs-Server

Erstellen Sie Anmeldeinformationen, um auf eine ServiceNow -Instanz zuzugreifen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.
2. Wählen Sie **Neu**.
3. Wählen Sie **Anmeldeinformationen für Standardauthentifizierung**.
4. Füllen Sie die Felder des Formulars aus.

Anmeldeinformationsformular für die Standardauthentifizierung

Feld	Beschreibung
Name	Geben Sie einen eindeutigen und beschreibenden Namen für diese Anmeldeinformationen ein.
Anwendername	Name zum Identifizieren des Benutzers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Passwort	Passwort zur Verwendung dieser Anmeldeinformationen.
Aktiv	Option zum Aktivieren der Verwendung dieser Anmeldeinformationen.
Reihenfolge	Die Reihenfolge, in der die Plattform diese Anmeldeinformationen bei der Anmeldung bei Geräten testet. Je kleiner die Zahl, desto höher werden die Anmeldeinformationen in der Liste angezeigt. Richten Sie die Reihenfolge der Berechtigungsnachweise ein, wenn Sie eine große Anzahl von Berechtigungsnachweisen verwenden oder wenn die Sicherheitsvorkehrung nach drei fehlgeschlagenen Anmeldeversuchen Benutzer sperrt. Wenn alle Berechtigungsnachweise dieselbe Auftragsnummer haben (oder keine), versucht die Instanz die Berechtigungsnachweise in zufälliger Reihenfolge. Standardwert: `100`

5. Wählen Sie **Absenden**.

Ergebnisse

Die Anmeldeinformationen für die Standardauthentifizierung zur Verwendung mit der Serverinstanz werden erstellt.

Ereignisse werden verarbeitet

Bei der Ereignisverarbeitung werden Ereignisse oder Ereignisströme erfasst, analysiert und automatisch Maßnahmen ergriffen. Der -Prozess umfasst das Anzeigen von Ereignissen, Ereignisbindungen, Ereignisregeln und Ereignisfeldzuordnung.

Ein Event ist eine Benachrichtigung von einem oder mehreren Überwachungstools, die anzeigt, dass etwas von Interesse aufgetreten ist, z. B. eine Protokollnachricht, eine Warnung oder ein Fehler. Events werden verarbeitet und Warnungen werden basierend auf den folgenden Faktoren generiert:

Konfiguration der Ereignissammlung über MID-Server, Skript, SNMP-Trap-Sammlung oder E-Mail-Nachricht.

Eine Event-Regel, Warnungsbindung oder Event-Feldzuordnungskonfiguration für die Verarbeitung von Events aus verschiedenen Quellen. Wenn ein Event-Paket verarbeitet wird, das Events mit einem benutzerdefinierten (nicht unterstützten) Status enthält, werden die Events mit dem benutzerdefinierten Status nicht verarbeitet.

Weitere Informationen finden Sie unter Ereignismanagement erkunden.

Events anzeigen

Ereignismanagement verfolgt einzelne Events zur Verwaltung externer Systeme. Diese Ereignisse sind Benachrichtigungen von Überwachungstools, die auf relevante Ereignisse hinweisen, z. B. Protokollnachrichten, Warnungen oder Fehler. Ereignismanagement sammelt Ereignisse aus externen Quellen und speichert sie in der Tabelle „Ereignis“ [em_event], die eine Liste eingehender Rohereignisse bietet.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator, evt_mgmt_user, oder evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Stellen Sie sicher, dass Sie den Wert des **Klassifizierungsfelds** in Event-Tabellen [em_event] weder manuell noch per Skript oder Event-Regel ändern.

Warum und wann dieser Vorgang ausgeführt wird

Das Event-Überwachungstool generiert die Werte der Quell- und Ressourcenfelder. Ereignismanagement-Implementierer können Event-Typen definieren und Knoten registrieren, um eingehende Events eindeutig zu identifizieren und Warnungen für die spezifischen Anforderungen des Unternehmens zu erstellen. Ereignismanagement verwendet diese Informationen, um zu bestimmen, ob eine Warnung erstellt oder eine vorhandene aktualisiert werden soll.

Eine Event-Quelle kann doppelte Events mit denselben identifizierenden Informationen generieren. Bei Events mit übereinstimmenden Identifizierungsinformationen bestimmt Ereignismanagement anhand des Zeitintervalls zwischen Events, ob die Events ein vorhandenes Problem oder ein neues Problem darstellen.

Zusätzliche Felder sollten im Feld **Zusätzliche Informationen** des Events eingeschlossen werden. Fügen Sie einem Event keine zusätzlichen Felder hinzu, indem Sie der Event-Tabelle [em_event] ein benutzerdefiniertes Feld hinzufügen. Weitere Informationen zum Einbinden zusätzlicher Felder in Events finden Sie unter Benutzerdefinierte Warnungsfelder.

Hinweis: Vermeiden Sie das Schreiben von Business Rules für Event-Tabellen [em_event], da dies zu einer Verschlechterung der Leistung führen kann.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**.

   Die Liste „Alle Events“ zeigt die folgenden Spalten.

Liste „Alle Events“

Spalte	Beschreibung	Ausgefüllt mit
Zeit des Events	Zeit des Auftretens des Events in der Zeitzone des Netzwerkknotens.	Externes Event-Überwachungstool
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen	Externes Event-Überwachungstool
Beschreibung	Grund für Event-Generierung. Anzeige von zusätzlichen Details zu einem Problem. Beispielsweise ein Serverstapel-Trace oder Details aus einem Überwachungstool. Maximale Länge: 4.000 Zeichen	Externes Event-Überwachungstool
Knoten	Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, der/die dem Event zugeordnet ist, z. B. IBM-ASSET. Maximale Länge: 100 Zeichen	Externes Event-Überwachungstool
Typ	Der Metriktyp, auf den sich das Event bezieht, z. B. Datenträger oder CPU, der zur Identifizierung eines Event-Datensatzes verwendet wird, aus dem Warnungen erstellt werden. Maximale Länge: 100 Zeichen	Externes Event-Überwachungstool
Ressource	Knotenressource, die für das Event relevant ist. Beispiel: Datenträger C, CPU-1, der Name	Externes Event-Überwachungstool

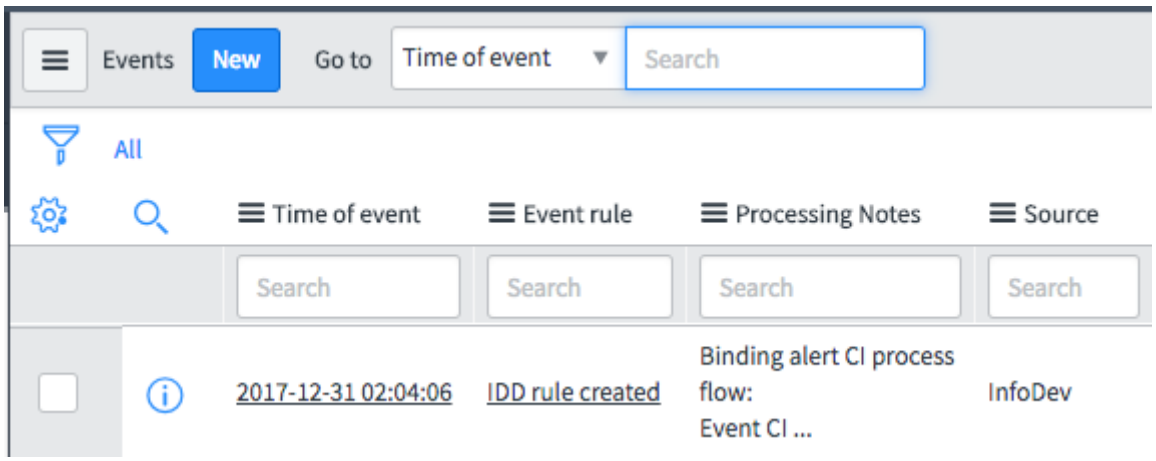
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung	Ausgefüllt mit
	eines Prozesses oder Services. Maximale Länge: 100 Zeichen	
Metrikname	Eindeutiger Name, der beschreibt, welche Metriken erfasst werden und für welche diese Warnung erstellt wurde.	Externes Event-Überwachungstool
Nachrichtenschlüssel	Eindeutiger Event-Bezeichner zur Identifizierung mehrerer Events, die sich auf dieselbe Warnung beziehen. Wenn dieser Wert leer ist, wird er aus den Feldwerten **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** generiert. Maximale Länge: 1.024 Zeichen	Externes Event-Überwachungstool
Status	Der Status des Events: ◦ **Bereit**: Das Event wurde empfangen und wartet auf die Verarbeitung. ◦ **In der Warteschlange**: Das Event wird vom Event-Verarbeitungsauftrag in die Warteschlange gestellt. ◦ **Verarbeitet**: Das Event wurde erfolgreich verarbeitet. ◦ **Fehler**: Beim Verarbeiten des Events ist ein Fehler aufgetreten. Beispielsweise sind die Methode der Event-Erfassung oder der **Schweregrad** des Events leer. ◦ **Ignoriert**: Dieser Wert wird nicht verwendet.	Event
Schweregrad	Obligatorisch. Die Optionen werden normalerweise wie folgt interpretiert: ◦ **Kritisch**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. ◦ **Schwerwiegend**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten. ◦ **Geringfügig**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. ◦ **Warnung**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. ◦ **OK**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig. ◦ **Löschen**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.	Event

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung	Ausgefüllt mit
Warnung	Wenn eine Warnung als Ergebnis des Events erstellt wurde, enthält dieses Feld die eindeutige ID, die von Ereignismanagement zur Identifizieren der Warnung generiert wird.	Eine übereinstimmende Event-Regel oder Event-Feldzuordnung

2. Um ein einzelnes Event anzusehen, klicken Sie auf die gewünschte Zeile in der Spalte **Zeit des Events**.
3. Zum Überprüfen der Event-Regeln, die das Event verarbeitet haben, klicken Sie im Abschnitt **Zugehörige Links** auf **Event-Prozess überprüfen**.
   Für weitere Möglichkeiten zum Anzeigen der Event-Regeln, die auf das Event angewendet wurden, können Sie die Felder `Ereignisregel` und `Verarbeitungsnotizen` in der Event-Liste anzeigen.



Optionale Event-Felder zum Anzeigen der angewendeten Event-Regel

Spalte	Beschreibung
Regel für übereinstimmende Events	Event-Regel, die den aktuellen Event-Regeldefinitionen entspricht. Diese Informationen werden hauptsächlich zum Erstellen von Event-Regelempfehlungen für Events verwendet, die derzeit nicht von Regeln abgedeckt sind. Wenn Event-Regeln geändert wurden, können diese Informationen aus dem unten beschriebenen Feld „Verarbeitungsnotizen“ abgerufen werden. **Hinweis:** Dieses Feld zeigt nicht den Verlauf der Event-Regeln an, die auf das Event angewendet wurden.
Verarbeitungsnotizen	Informationen zur Bindung an den CI-Typ und zu den Event-Regeln, die auf das Event angewendet wurden

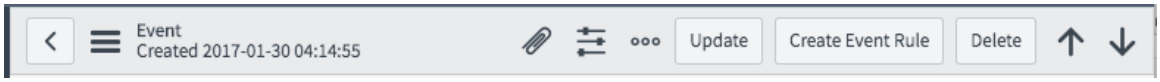
4. So erstellen Sie eine Event-Regel für ein Event, das keiner Event-Regel zugeordnet ist:

   a. Klicken Sie auf das Event.

      Das Event wird im Event-Formular geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



b. Klicken Sie auf **Event-Regel erstellen**.
Die Felder der neuen Event-Regel werden mit Daten aus dem Event ausgefüllt. Sie können die Event-Informationen beispielsweise verwenden, wenn Sie Felder für Warnungen verfassen.

Teambasierte Integrationen in Ereignismanagement

Teambasierte Integrationen ermöglichen Teams die Optimierung der Ereignisverarbeitung in Ereignismanagement, um die Effizienz und die betriebliche Effektivität zu verbessern.

Teambasierte Integrationen bieten die folgenden Fähigkeiten:

- Weisen Sie bestimmten Connectors Teams zu, um einen strukturierten Ansatz für die Integrationsbemühungen zu erreichen.
- Ermöglichen Sie jedem Team, anwenderdefinierte Regeln zu definieren und anzuwenden, um eine gezieltere und einfachere Handhabung der Ereignisverarbeitung zu ermöglichen.
- Leiten Sie Warnungen automatisch an die entsprechenden Teammitglieder weiter, die für die integrierten Systeme verantwortlich sind, je nach Integrations- und Configuration Item (CI)-Besitz.
- Ermöglichen Sie eine nahtlose Integration und Automatisierung durch die automatische Zuweisung von Warnungen an die entsprechenden Teammitglieder auf Grundlage des Eigentums an der Integration und des Konfigurationselements (Configuration Item, CI).

Passen Sie Event-Regeln, Event-Zuordnung und den Vorrang von Teamregeln für teambasierte Integrationen an. Weitere Informationen finden Sie unter Teambasierte Integrationseigenschaften.

Zugehörige Informationen

Event-Regeln

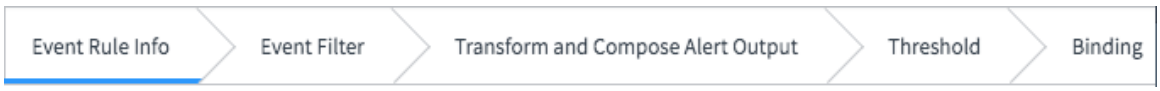
Konfiguration der Event-Feldzuordnung

Warnungszuweisungsgruppen für Teams

Event-Regeln

Verwenden Sie Event-Regeln, um Warnungen für die Nachverfolgung und Nachbesserung zu generieren. Event-Regeln werden in der Event-Regeltabelle [em_match_rule] gespeichert. Konfigurieren und passen Sie Event-Regeln an, um Events und die Generierung von Warnungen zu verwalten.

Event-Regeln ändern die Event-Datensätze in der Event-Tabelle nicht. Änderungen an Event-Daten werden im Instanzspeicher ServiceNow gespeichert.



Verwenden Sie den Event-Regeldesigner zum Erstellen und Konfigurieren von Event-Regeln. Mit den Standard-Ereignisregeln oder Ereignisregeln, die Sie erstellt haben, können Sie folgende Aktionen durchführen:

- Event-Regelfilter anwenden, um zu bestimmen, ob die Regel für ein Event gilt.
- Umwandlung mit **Event-Abgleichsfeldern** und optionalen **Event-Erstellungsfeldern** anwenden, um den Warnungstext zu formatieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Anwenden eines Grenzwerts zum Erstellen anwenderdefinierter Warnungen für schnell wiederkehrende Ereignisse.
- Automatisch Warnungen erstellen oder schließen.
- Warnungen an CI-Informationen aus der CMDB binden.

- Führen Sie mehrere sequenzielle Regeln aus, die für dasselbe Ereignis definiert sind, indem Sie das Kontrollkästchen **Zusätzliche Abgleichsregeln** anwenden aktivieren. Die Ereignisregeln werden in aufsteigender Reihenfolge ausgeführt, wie im Feld **Reihenfolge** festgelegt. Auf Zuweisungsgruppen angewendete Ereignisregeln werden erst ausgeführt, nachdem die globalen Regeln ausgeführt wurden.

Event-Regel erstellen oder bearbeiten

Sie können Event-Regeln erstellen, um Warnungen für die Nachverfolgung und Nachbesserung zu generieren. Verwenden Sie teambasierte Integrationen in Ereignisregeln, um sicherzustellen, dass der Besitz des Connectors und die Ausführung von Regeln Vorrang vor allgemeinen Regeln haben. Teams können Konsistenz und Hierarchie aufrechterhalten und gleichzeitig Flexibilität und Anpassungsoptionen bieten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Zeigen Sie die Liste der verfügbaren Ereignisregeln auf der Seite **Ereignisregeln** an, um zu bestimmen, ob Sie eine Ereignisregel erstellen oder bearbeiten möchten.

Sie können Regeln erstellen, die:

- Informationen in Events verwandeln, um bestimmte Warnungsfeldwerte auszufüllen und Warnungsfelder aus verschiedenen Werten zu erstellen.
- Schwellenwertregeln konfigurieren, die Warnungen nur dann erstellen oder schließen, wenn die eingehenden übereinstimmenden Ereignisse den angegebenen Schwellenwert überschreiten.
- Warnungen mittels CI-Bezeichnern an CIs binden.

Optionen zum Erstellen der Regel sind:

- Erstellen Sie eine Event-Regel und weisen Sie Event-Felder für die Generierung von Warnungen zu.
- Erstellen Sie eine Regel aus einem vorhandenen Ereignis oder einer Gruppe von Ereignissen, die keine Regel aufweisen. In diesem Fall werden die Event-Felder in den Abschnitt „Event-Abgleichsfelder“ der Regel kopiert.
- Bearbeiten Sie eine vorhandene Event-Regel.
- Wählen Sie für Teambasierte Integrationen eine Zuweisungsgruppe aus.

- Führen Sie mehrere sequenzielle Regeln aus, die für dasselbe Ereignis definiert sind, indem Sie das Kontrollkästchen **Zusätzliche Abgleichsregeln** anwenden aktivieren. Die Ereignisregeln werden in aufsteigender Reihenfolge ausgeführt, wie im Feld **Reihenfolge** festgelegt. Auf Zuweisungsgruppen angewendete Ereignisregeln werden erst ausgeführt, nachdem die globalen Regeln ausgeführt wurden.

Sie können eine vorhandene Ereignisregel mit neuen Ereignisdaten aktualisieren. Weitere Informationen finden Sie unter Ereignisregeln aktualisieren.

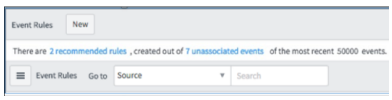
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Ereignisregeln, die nicht zum Ausführen einer Aktion konfiguriert sind, werden übersprungen. Wenn die Regel nicht als Ignorieren, Schwellenwert oder Bindung konfiguriert ist, ist es daher wichtig, entweder das Feld „Übereinstimmung“ oder „Zusammengesetzt“ anzugeben.
- Stellen Sie sicher, dass Sie den Wert des Felds **„Klassifizierung“** in Ereignistabellen [em_event] nicht manuell, per Skript oder per Ereignisregel ändern.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln** und führen Sie eine der folgenden Aktionen aus.

Option	Bezeichnung
Event-Regel aus einem vorhandenen Event erstellen	**a.** Wählen Sie den Link für nicht zugeordnete Ereignisse oder gruppierte Ereignisse, die den Regeln nicht zugeordnet sind.  **b.** Wählen Sie das Event aus, das Sie zum Erstellen der Regel verwenden möchten. Die Event-Felder werden in den Abschnitt „Event-Feldregeln“ der Regel kopiert.
Vorhandene Event-Regel bearbeiten	Wählen Sie in der Liste der Ereignisregeln die Ereignisregel aus, die geändert werden soll. Die Event-Regel wird im Event-Regeldesigner geöffnet, in dem Sie die Werte der Felder ändern können. Wählen Sie **Speichern und** um die Regel zu ändern, wenn die folgende Bannermeldung angezeigt wird und Sie die Ereignisregel konvertieren möchten. `Rule cannot be viewed in the event rule designer. To modify the rule click 'Save and Upgrade'.`
Event-Regel erstellen	Wählen Sie **Neu**.

2. Stellen Sie sicher, dass **Aktiv** ausgewählt ist.
Wenn die Regel deaktiviert ist, findet Event Management eine andere Event-Regel und wendet sie an. Für das Event wird weiterhin eine Warnung erstellt, es sei denn, *Ignore* wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in einer anderen zutreffenden Regel ausgewählt oder wenn der Filter für diese Event-Regel konfiguriert wird.

3. Geben Sie einen eindeutigen und aussagekräftigen Namen ein und füllen Sie das Formular aus.

Event-Regel-Infoformular

Feld	Beschreibung
Quelle	Kategorie, für die diese Übereinstimmungsregel gilt. Die Zuordnungsregel gilt nur für Events mit demselben Event-Klassenwert. Wenn dieser Wert leer ist, wenden Sie die Regel auf alle Events an.
Reihenfolge	Reihenfolge, in der eine Event-Regel ausgewertet wird, wenn mehrere Regeln für denselben Event-Typ definiert sind. Event-Regeln werden in aufsteigender Reihenfolge ausgewertet.
Beschreibung	Geben Sie zusätzliche Informationen ein, die die Event-Regel beschreiben.
Zusätzliche Abgleichsregeln anwenden	Wählen Sie diese Option aus, um zusätzliche Ereignis-Übereinstimmungsregeln gemäß dem Feld Reihenfolge anzuwenden. Die letzte Regel mit Bindungseinstellungen legt die CI-Bindung fest. Wenn diese Option ausgewählt ist, ist die Registerkarte Schwellenwerte inaktiv.
Zuweisungsgruppe	Wählen Sie für teambasierte Integrationen eine Zuweisungsgruppe aus. Wenn in der Ereignisregel keine Zuweisungsgruppe definiert ist, wird diese Ereignisregel als globale Regel betrachtet. Wenn die Regeln ausgeführt werden, werden zuerst die globalen Regeln ausgeführt und dann die Regeln, die zu der Zuweisungsgruppe gehören, zu der die Quellinstanz des Ereignisses gehört.

4. Wahlweise: Definieren Sie die Ereignisregel mithilfe dieser Funktionen des Ereignisregel-Designers.

Option	Bezeichnung
Ereignisfilter	Definieren Sie einen Filter, um einzuschränken, auf welche Events die Event-Regel angewendet werden muss. Weitere Informationen finden Sie unter Events filtern, für die eine Event-Regel gilt.
Warnungsausgabe umwandeln und verfassen	Konfigurieren Sie die Anpassung des Warnungsinhalts. Weitere Informationen finden Sie unter Event-Regel konfigurieren, um den Warnungsinhalt anzupassen.
Schwellenwert	Erstellen oder schließen Sie Warnungen gemäß dem angegebenen Schwellenwert. Weitere Informationen finden Sie unter Schwellenwert festlegen, um die Warnungsgenerierung zu unterdrücken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Bindung	Konfigurieren Sie Event-Regeln, um Warnungen automatisch an CI-Informationen aus der CMDB zu binden. Weitere Informationen finden Sie unter Warnungen an CIs binden.

5. Wählen Sie **Speichern**, **Absenden** oder **Aktualisieren** aus.

Zugehörige Informationen

- Musterabgleich
- Event-Eingabeinformationen verwenden
- Event-Regel konfigurieren, um den Warnungsinhalt anzupassen
- Ereignisregeln aktualisieren
- Ereignisverarbeitung simulieren
- Events filtern, für die eine Event-Regel gilt

Event-Eingabeinformationen verwenden

Der Bereich **Event-Eingabe**, der in den Schritten zur Erstellung einer Event-Regel enthalten ist, bietet einen Verweis auf die Informationen, die Sie zur Konfiguration einer Event-Regel nutzen können.

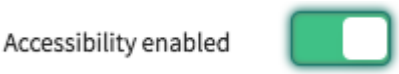
Im Bereich **Warnungsausgabe umwandeln und verfassen** können Sie die Informationen auch in die erforderlichen Felder ziehen, um den Warnungsinhalt anzupassen. Die Felder im rechten Bereich werden als Verweis darauf angezeigt, welche Felder, Ausdrücke und deren Werte beim Arbeiten im Event-Regeldesigner verfügbar sind. Die Felder, die im linken Arbeitsbereich der Warnungsausgabe „Umwandeln und verfassen“ angezeigt werden, werden zu Feldern im generierten Warnungsformular. Darüber hinaus können Sie Warnungs-Tags definieren, die spezifisch für die Anpassung sind.

Allgemeine Komponenten und Navigation

Der Bereich „Event-Eingabe“ besteht aus folgenden Abschnitten:

- Zusätzliche Ereignisinformationen
- Ausdrücke
- Rohinformationen zum Event

Der Bereich „Event-Eingabe“ wird in allen Abschnitten des Event-Regeldesigners angezeigt, mit Ausnahme des Abschnitts „Event-Regelinformationen“. Die Felder im rechten Bereich können nur im Abschnitt „Warnungsausgabe umwandeln und verfassen“ geändert werden. In allen anderen Abschnitten ist der Bereich „Event-Eingabe“ schreibgeschützt und zu Referenzzwecken verfügbar.

Hinweis: Wenn die **Eingabehilfe aktiviert** 

in den Systemeinstellungen ausgewählt ist, ist der Standardbearbeitungsmodus nicht verfügbar .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bearbeitungsmodi

Modus	Beschreibung
Standardbearbeitungsmodus	Text, der im linken Arbeitsbereich ausgewählt wurde, kann nicht bearbeitet werden. Rückgängig machen ist nicht verfügbar. In diesem Modus können Sie den Text oder die Werte nur markieren und umwandeln, indem Sie einen Feldnamen auswählen.
Bearbeitungsmodus reguläre Ausdrücke	Bearbeiten Sie Text im linken Arbeitsbereich, indem Sie ihn nach Bedarf auswählen. Nachdem Sie den Text bearbeitet haben, können Sie nicht mehr in den Standardmodus zurückkehren. **Rückgängig machen** ist nicht verfügbar. **Zurücksetzen** ist jedoch verfügbar, wodurch das Feld auf seinen ursprünglichen Wert zurückgesetzt wird. Sie können Text mit Formatkonventionen für reguläre Ausdrücke verfassen. Geben Sie beispielsweise (. *) ein, um einen Feldnamen zu erstellen. Sie können keine der folgenden Feldwerte eingeben: „$“, um den Wert eines Felds einzubeziehen und den Namen des Felds in Klammern {} anzugeben. Sie können Sonderzeichen in ein Feld einfügen, indem Sie diesen „ausweichen“, d. h. indem Sie dem Zeichen ein „\“ voranstellen. Um beispielsweise einen „\“ in Ihren Text einzufügen, geben Sie „\\“ ein.

Zusätzliche Event-Informationen

Der Abschnitt „Zusätzliche Event-Informationen“ zeigt Standardformularfelder für Events sowie Felder an, die zur Anzeige in Warnungen erstellt wurden und dem Abschnitt **Zusätzliche Informationen** der Warnung hinzugefügt werden.

Beim Konfigurieren von Text in den Feldern im linken Arbeitsbereich können Sie Feldnamen und/oder deren Wert aus diesem Abschnitt in die Felder ziehen.

Ausdrücke

Der Abschnitt „Ausdrücke“ ist nur verfügbar, wenn ein zusätzliches Informationsfeld erstellt wurde. Sie können Ausdrücke aus Event-Rohdaten oder aus zusätzlichen Informationsdaten erstellen.

1. Klicken Sie sich in ein Feld im Bereich der **Event-Eingabe**, um Transformationsaktionen durchzuführen.
2. Erstellen Sie einen Ausdruck, indem Sie Informationen umwandeln und einem Feldnamen zuordnen. Wählen Sie entweder einen Feldnamen aus der vorgeschlagenen Liste aus, oder erstellen Sie je nach Bedarf einen Feldnamen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie sich in ein Feld im Bereich der **Event-Eingabe**. Wählen Sie im linken Arbeitsbereich die erforderlichen Informationen aus.

Erstellen Sie Ausdrücke, indem Sie Informationen umwandeln und einem Feldnamen zuordnen. Wählen Sie einen Feldnamen aus der vorgeschlagenen Liste aus, oder erstellen Sie je nach Bedarf einen Feldnamen.

Rohinformationen zum Event

Der Abschnitt „Rohinformationen zum Event“ ist immer verfügbar. Sein Inhalt sind die Felder aus dem Event-Formular.

Zum Umwandeln von Text klicken Sie auf ein Feld im rechten Bereich, um ihn im Arbeitsbereich auf der linken Seite im Abschnitt „Ausdrücke markieren“ zu öffnen. Sie können Text im Abschnitt **Ausdrücke markieren** auswählen, wo der ausgewählte Text zum Wert eines neu erstellten Felds wird. Benennen Sie das neue Feld. Dieses neue Feld wird dem Abschnitt Ausdrücke hinzugefügt.

Hinweis: Wenn Sie einen regulären Ausdruck für Eingaben erstellen, stellen Sie sicher, dass Sie Eingaben mit den Variablen in sequenzieller Reihenfolge erstellen. Variablen können zwar für die Aufnahme übersprungen werden, die ausgewählte Reihenfolge muss jedoch beibehalten werden.

Steuern, wie Felder angezeigt werden:

- Verwenden Sie die Ausschlussliste [em_event_rule_black_list], um Felder im rechten Bereich auszublenden.
- Verwenden Sie das Formular em_event_rule_order, um die Position der einzelnen Felder zu sortieren.
- Felder, die nicht in der Ausschlussliste enthalten und auch nicht Teil der Tabelle em_event_rule_order sind, erscheinen noch im Event-Regeldesigner, im rechten Bereich und auf der Registerkarte **Warnungsausgabe umwandeln und verfassen**.

Zugehörige Informationen

Event-Regel erstellen oder bearbeiten

Event-Regel konfigurieren, um den Warnungsinhalt anzupassen

Events filtern, für die eine Event-Regel gilt

Schwellenwert festlegen, um die Warnungsgenerierung zu unterdrücken

Events filtern, für die eine Event-Regel gilt

Definieren Sie einen Filter, um einzuschränken, auf welche Events die Event-Regel angewendet werden muss. Konfigurieren Sie den Filter, indem Sie eine Reihe von Bedingungen bereitstellen, die jedes Event erfüllen muss, um von der Anwendung auf die Event-Regel entweder ausgeschlossen oder in sie eingeschlossen zu werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Stellen Sie sicher, dass ein Name für die Event-Regel angegeben ist.
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Zum Erstellen der erforderlichen Bedingungsanweisung können Sie Event-Felder sowie zusätzliche Felder verwenden, die im Feld **Zusätzliche Informationen** des Events definiert sind. Verwenden Sie diese Felder, um Bedingungen zu konfigurieren, die Events ausschließen können. Alternativ können Sie eingehende Events filtern, um sicherzustellen, dass nur die Events einbezogen werden, die die erforderlichen Bedingungen erfüllen.

Hinweis: Beim Abgleich von Event-Regeln wird die Groß-/Kleinschreibung beachtet.

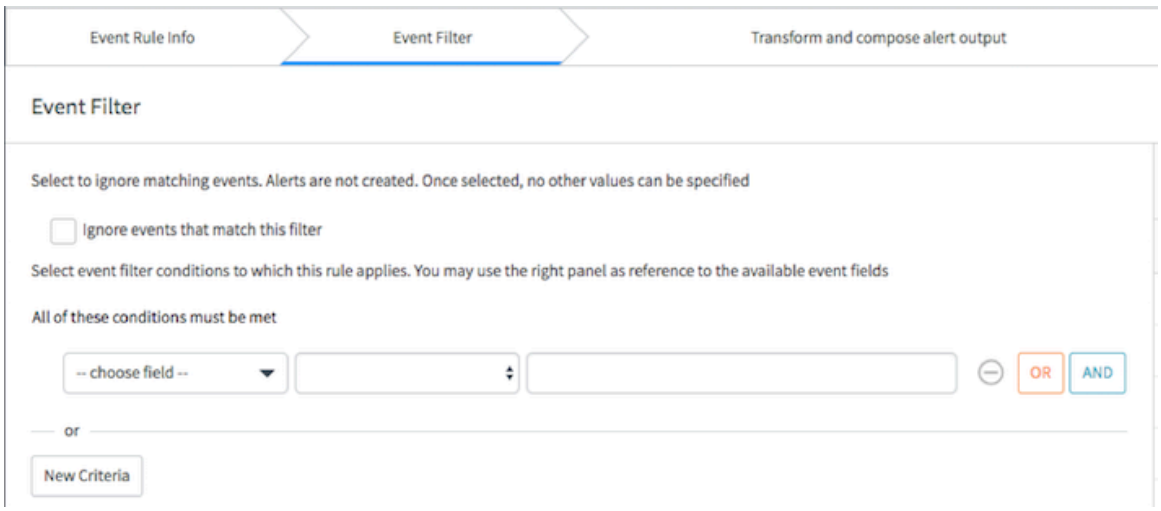
Während der Arbeit auf der Registerkarte „Event-Filter“:

- Wenn Sie in der Event-Regelliste eine empfohlene Regel oder eine vorhandene Regel ausgewählt haben, werden die Filterfelder mit Werten aus diesen Events ausgefüllt. Sie können diese Filterfelder zum Erstellen von Filterbedingungen verwenden.
- Sie können auf eine andere Registerkarte (z. B. **Schwellenwert**) klicken, in diesem Bereich arbeiten und dann im Bereich „Event-Filter“ ohne Verlust von Informationen zur Arbeit zurückkehren.
- Verwenden Sie den rechten Bereich als Referenzquelle dafür, welche Felder zum Erstellen von Filterbedingungen verfügbar sind.

Hinweis: Ereignisfilter, die für die Felder „additional_info“ erstellt wurden, führen nur einen Zeichenfolgenvergleich und keinen numerischen Vergleich durch, auch wenn die in das Wertfeld eingegebenen Informationen so erscheinen, als wären sie numerisch (siehe folgende Grafik):

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.
2. Klicken Sie auf **Neu**, oder öffnen Sie eine Event-Regel.
3. Klicken Sie auf **Event-Filter**.



4. Um Events zu ignorieren, wählen Sie **Events ignorieren, die diesem Filter entsprechen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

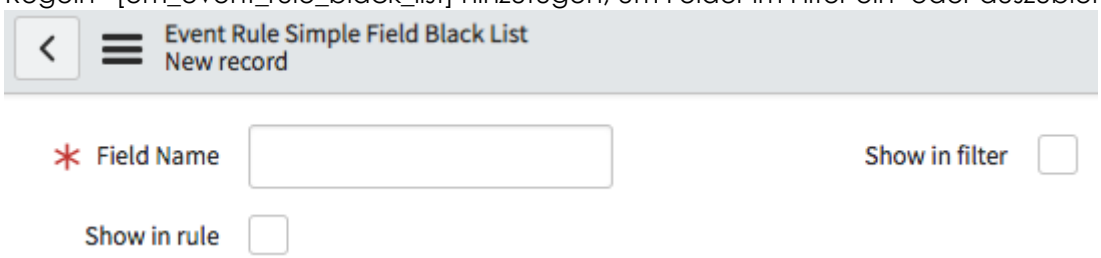
Alle Events, die dieser Event-Regel entsprechen, werden ignoriert. Sie können dem Filter weitere Bedingungen hinzufügen, indem Sie entweder auf **ODER** oder **UND** klicken.

Hinweis: Auch wenn ein Event von einer Event-Regel ignoriert wird, wird es in der Event-Tabelle [em_event] aufgezeichnet. Wählen Sie diese Option aus, um die Erstellung einer Warnung und deren Zuordnung zum Event zu verhindern.

5. Zum Konfigurieren von Bedingungen, für die die Event-Regel gelten muss, klicken Sie auf **Neue Kriterien**.
   Sie können weitere Bedingungen hinzufügen, indem Sie entweder auf **ODER** oder **UND** klicken.

   Hinweis: Das Zeichen **%** wird in Filterbedingungen nicht unterstützt.

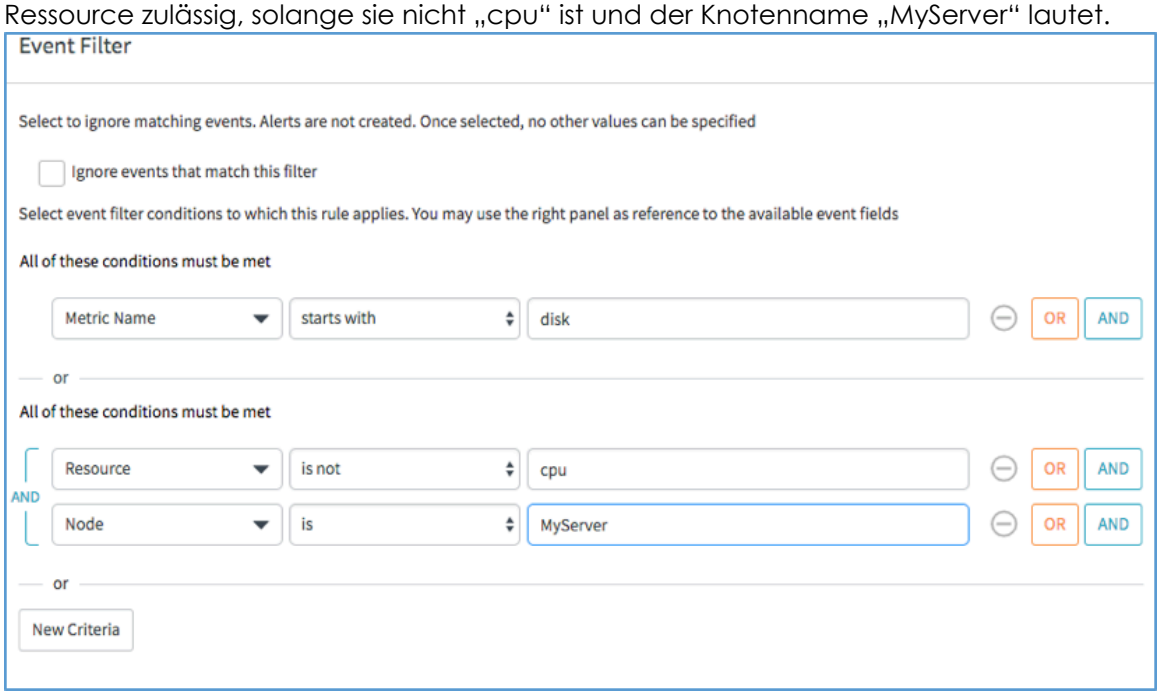
6. Sie können Feldnamen zur Tabelle „Schwarze Listen für einfache Event-Regeln“ [em_event_rule_black_list] hinzufügen, um Felder im Filter ein- oder auszublenden.



   - Um Felder aus dem Filter und dem rechten Bereich zu entfernen, fügen Sie ein neues Feld für schwarze Listen hinzu, in dem die Option **In Regel anzeigen** nicht ausgewählt ist.
   - Um Felder nur aus dem Filter zu entfernen und sie im rechten Bereich angezeigt zu lassen, fügen Sie ein neues Feld für die Ausschlussliste hinzu, in dem die Option **In Regel anzeigen** ausgewählt ist.

7. Klicken Sie entweder auf **Speichern** oder auf **Absenden**.

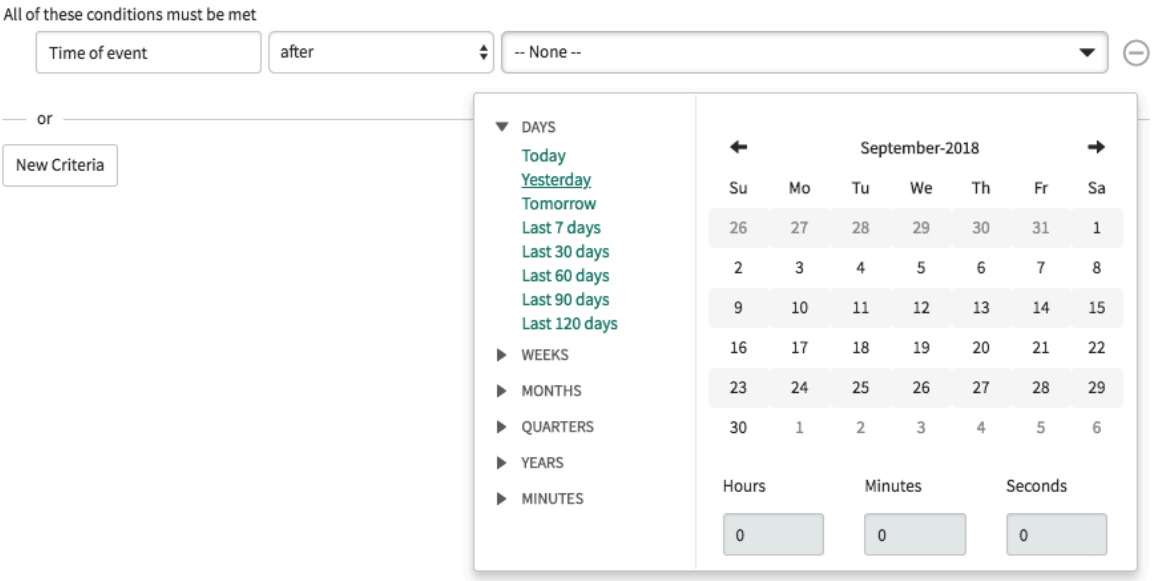
Example:
Beispiel für Filterbedingungen, die zum Ausführen einer Regel angegeben sind, wenn der Metrikname mit dem Wort „Disk“ beginnt. In diesem Beispiel ist jede Ressource zulässig, solange sie nicht „cpu“ ist und der Knotenname „MyServer“ lautet.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für das Filtern von Events anhand von Zeitbedingungen. Wählen Sie im Feld **Feld auswählen oder neu hinzufügen** die `Zeit des Events` aus.

Geben Sie die erforderlichen Zeitbedingungen an, z. B. jederzeit nach gestern.



Zugehörige Informationen

- Event-Regel erstellen oder bearbeiten
- Event-Eingabeinformationen verwenden
- Event-Regel konfigurieren, um den Warnungsinhalt anzupassen
- Schwellenwert festlegen, um die Warnungsgenerierung zu unterdrücken

Events finden, die nicht mit Regeln übereinstimmen

Suchen Sie nach Events, die keinen Regeln entsprechen, und stellen Sie fest, ob Event-Regeln zu deren Verwaltung erforderlich sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

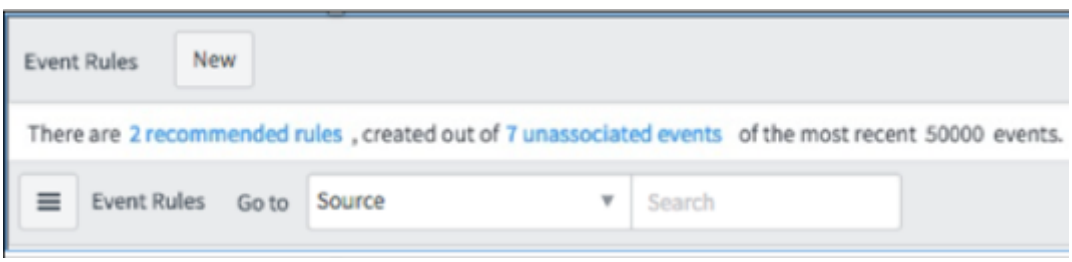
Warum und wann dieser Vorgang ausgeführt wird

Diese Aufgabe beschreibt, wie Sie Ereignisse finden, die nicht mit Regeln übereinstimmen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.
2. Klicken Sie oben im Formular auf den Link für Ereignisse oder gruppierte Ereignisse, die keinen Regeln zugeordnet sind.

Example



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Erstellen Sie eine Event-Regel. Beispielsweise sind Event-Regeln für die Verwaltung von Ereignissen nützlich, die regelmäßig auftreten.

Event-Regeln anzeigen

Sie können alle Event-Regeln in der Event-Regelliste anzeigen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.

Event-Regelliste

Feld	Beschreibung
Name	Der Name der Event-Regel.
Standardbindung überschreiben	Veraltete Bindungskriterien. Wenn im Abschnitt **Bindung** keine Kriterien angegeben wurden oder die angegebenen Bindungskriterien nicht erfüllt werden, werden die veralteten Bindungskriterien berücksichtigt.
Reihenfolge	Reihenfolge, in der eine Event-Regel ausgewertet wird, wenn mehrere Regeln für denselben Event-Typ definiert sind. Event-Regeln werden in aufsteigender Reihenfolge ausgewertet.
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
Aktualisiert	Aktualisierung von Datum und Uhrzeit für die Regel.

Hinweis: Sie können die Event-Regelliste filtern, um die erforderliche Teilmenge der Informationen anzuzeigen. Wenn Sie jedoch nach dem Filtern einen Favoritenlink erstellen und auf den Link klicken, wird in der Liste der Event-Regeln nicht der richtige Filter angezeigt.

Zugehörige Informationen

Events anzeigen

Event-Regel konfigurieren, um den Warnungsinhalt anzupassen

Sie können eine Event-Regel konfigurieren, um den Warnungsinhalt anzupassen. Sie können die Reihenfolge der Felder anpassen und auswählen, welche Felder angezeigt werden. Die Felder, die im linken Arbeitsbereich des Abschnitts **Warnungsausgabe umwandeln und verfassen** einer Event-Regel angezeigt werden, sind die Felder in der generierten Warnung.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Warnungsinhalte anpassen, indem Sie die erforderlichen Event-Felder hinzufügen und den Text in den Feldern ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie einen regulären Ausdruck für Eingaben erstellen, stellen Sie sicher, dass Sie Eingaben mit den Variablen in sequenzieller Reihenfolge erstellen. Variablen können zwar für die Aufnahme übersprungen werden, die ausgewählte Reihenfolge muss jedoch beibehalten werden.

Formatieren Sie den Warnungstext mit einer oder beiden dieser Methoden:

Warnungstext formatieren

Formatierungsmethode	Beschreibung
Umwandeln	Erstellen Sie ein Feld, das in einer Warnung angezeigt wird. Das Feld und sein Wert werden im Abschnitt **„Zusätzliche Informationen“** oder im Abschnitt **„Warnungs-Tags“** angezeigt. Im Bereich **Event-Eingabe** wird das neue Feld im Abschnitt **Ausdrücke** aufgeführt.
Verfassen	Bestimmen Sie, welcher Text im ausgewählten Feld angezeigt werden soll.

Hinweis:

- Bestimmen Sie durch Konfiguration der Ausschlussliste [em_event_rule_black_list], welche Felder im Fenster **Ereigniseingabe** angezeigt werden.

  Ein Feld, das der Ausschlussliste hinzugefügt wurde und bereits in einer vorhandenen Event-Regel enthalten ist, wird nicht aus der Regel entfernt. Stattdessen wird es in den Abschnitt **Manuelle Attribute** in der Regel verschoben.

- Steuern Sie die Reihenfolge der Event-Formularfelder, indem Sie em_event_rule_order konfigurieren.

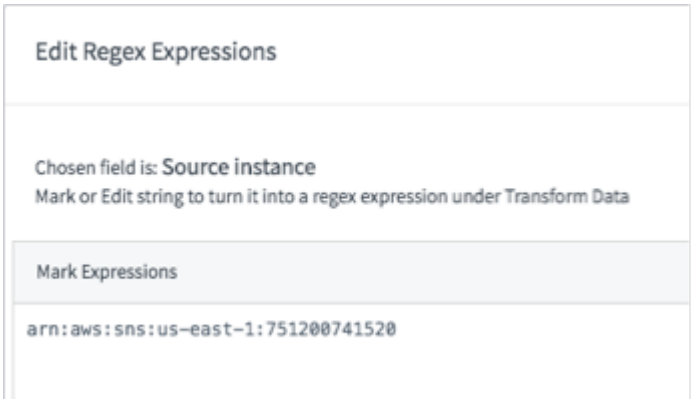
Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.
2. Klicken Sie auf **Neu**, oder öffnen Sie eine Event-Regel.
3. Klicken Sie auf **Warnungsausgabe umwandeln und verfassen**.
   In diesem Abschnitt können Sie den **Umwandlungsmodus** und den **Verfassungsmodus** verwenden.
4. So wandeln Sie Informationen in Felder um – Standardmodus:

   Hinweis: In diesem Schritt erfolgt die Auswahl des Texts im Standardbearbeitungsmodus. In diesem Modus ist Rückgängigmachen verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf das erforderliche Feld im Bereich der Event-Eingabe. Der Wert und der Inhalt des ausgewählten Felds werden im Arbeitsbereich auf der linken Seite angezeigt.

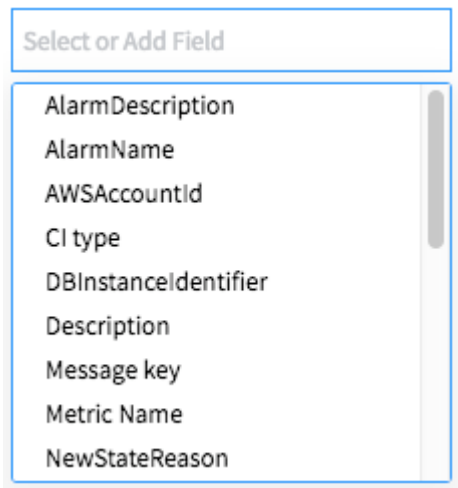


b. Standardbearbeitungsmodus auswählen .

c. Markieren Sie mit dem Bleistift-Cursor den gewünschten Text. Sie können auf Text im Feld doppelklicken, um ein Wort oder den erforderlichen Text und die gewünschten Symbole auszuwählen.

Hinweis: Wenn die **Eingabehilfe aktiviert** Accessibility enabled in den Systemeinstellungen ausgewählt ist, ist der Standardbearbeitungsmodus nicht verfügbar .

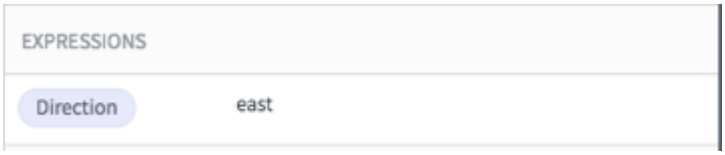
d. Wählen Sie einen Feldnamen aus der Liste aus, oder geben Sie den Namen des erforderlichen Ausdrucks ein. Felder, die in der Liste angezeigt werden, sind vorhandene Ereignisfelder, Felder für zusätzliche Informationen oder zuvor definierte Warnungs-Tags (Felder mit dem Präfix „t_“). Der Feldname wird im Bereich **Ausdrücke** angezeigt, und der ausgewählte Text wird hervorgehoben. Sowohl der Text als auch der Ausdrucksname werden in der gleichen Farbe hervorgehoben. Jeder zusätzliche Ausdruck, den Sie erstellen, und sein Wert wird in einer anderen Farbe hervorgehoben.



Hinweis: Umwandlungsfeldnamen dürfen kein ' (einzelnes Anführungszeichen) enthalten.

e. Klicken Sie auf **Erledigt**. Der Ausdrucksname wird im Abschnitt **Ausdrücke** des **Event-Eingabebereichs** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



f. Wenn Sie auf einen Ausdruck oder seinen Wert im **Event-Eingabebereich** klicken, werden die Details im Arbeitsbereich auf der linken Seite angezeigt.

5. So wandeln Sie Informationen in Felder um – Modus regulärer Ausdruck:

Hinweis:

- Im Modus „regulärer Ausdruck“ ist Rückgängigmachen nicht verfügbar.
- Platzieren Sie beim Erstellen eines regulären Ausdrucks aus Variablen, die im Event hervorgehoben sind, die ausgewählten Variablen in der Reihenfolge, in der sie im Event-Feld angezeigt werden.
- Geben Sie beim Erstellen des regulären Ausdrucks der Event-Regel die Begriffe mithilfe einer genauen Übereinstimmung mit der Eingabe aus den Event-Feldern an. Beispiel: Für den Text `vhxy2stlgwc_8888_hec03v012979` sieht der reguläre Ausdruck

  ```
  ^([^_]+)_
  ```

  so aus, als ob er den Text `vhxy2stlgwc` abfangen soll, der vor dem Unterstrich angezeigt wird. Es funktioniert jedoch nicht, da dieser Text keine exakte Übereinstimmung ist. Verwenden Sie den vollständigen regulären Ausdruck wie folgt:

  ```
  ^([^_]+)_.*
  ```

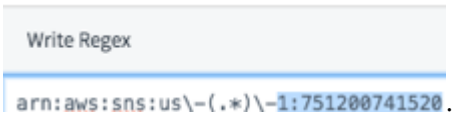
- Als Engine für den regulären Ausdruck wird der Parser Java Matcher verwendet. Stellen Sie sicher, dass Sie einen Java-Parser verwenden, um den regulären Ausdruck zu testen.
- Wenn der reguläre Ausdruck beim Analysieren von Daten nicht mit der gesamten Zeichenfolge übereinstimmt, erfasst die Event-Regel das Event nicht, und es findet keine Analyse statt.
- Die Übereinstimmungsmethode der Java-Engine für reguläre Ausdrücke wird verwendet. Mit dieser Implementierung versucht die Engine für reguläre Ausdrücke, die gesamte Eingabesequenz mit dem angegebenen Muster abzugleichen. Andere Abgleichmethoden, z. B. die Find-Methode, werden nicht unterstützt.
- Standardmäßig sind keine Flags für reguläre Ausdrücke festgelegt, außer dem `Pattern.DOTALL`-Flag. Mit dieser Implementierung von Java für reguläre Ausdrücke entspricht das DOT-Zeichen „.“ einem beliebigen Zeichen, einschließlich Zeilenendezeichen.
- Abgesehen von `Pattern.DOTALL`können andere Flags für reguläre Ausdrücke nicht geändert werden.
- `Lookahead` wird unterstützt. `Lookbehind` wird jedoch nicht unterstützt.

a. Klicken Sie auf das erforderliche Feld im Bereich der Event-Eingabe. Der Wert und der Inhalt des ausgewählten Felds werden im Arbeitsbereich auf der linken Seite angezeigt.

b. Wählen Sie den Bearbeitungsmodus reguläre Ausdrücke

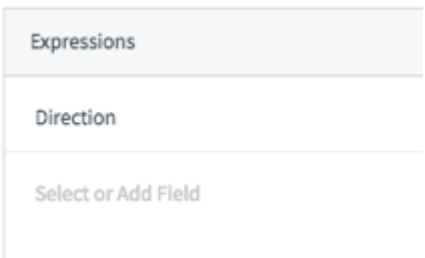
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wählen Sie den erforderlichen Text und die Symbole aus

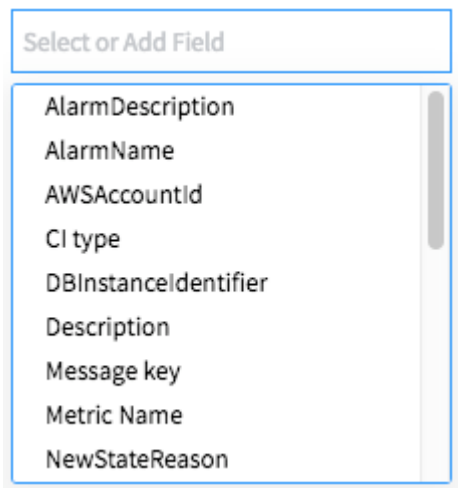


. Ersetzen Sie den hervorgehobenen Text durch (. *), um einen regulären Ausdruck zu erstellen.

d. Klicken Sie im Bereich **Ausdrücke** auf das Feld Feld **auswählen oder hinzufügen**.



e. Wählen Sie einen Feldnamen aus der Liste aus, oder geben Sie den Namen des erforderlichen Ausdrucks ein. Felder, die in der Liste angezeigt werden, sind vorhandene Ereignisfelder, Felder für zusätzliche Informationen oder zuvor definierte Warnungs-Tags (Felder mit dem Präfix „t_“). Der Feldname wird im Bereich **Ausdrücke** angezeigt.



Hinweis: Umwandlungsfeldnamen dürfen kein ' (einzelnes Anführungszeichen) enthalten.

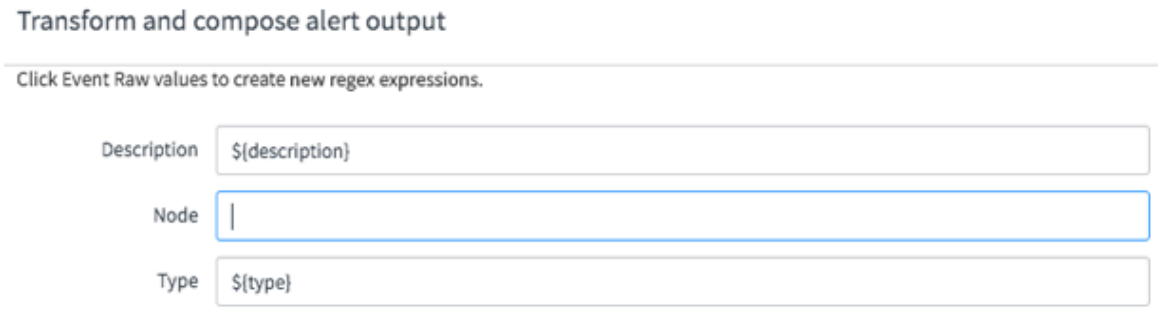
f. Klicken Sie auf **Erledigt**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Platzieren Sie beim Erstellen eines regulären Ausdrucks aus Variablen, die im Event hervorgehoben sind, die ausgewählten Variablen in der Reihenfolge, in der sie im Event-Feld angezeigt werden.
- Geben Sie beim Erstellen des regulären Ausdrucks der Event-Regel die Begriffe mithilfe einer genauen Übereinstimmung mit der Eingabe aus den Event-Feldern an. Beispiel: Für den Text „vhxy2stlgwc_8888_hec03v012979“ sieht der reguläre Ausdruck ^ ([^ _] +) _ so aus, als ob er den Text „vhxy2stlgwc“ abfangen soll, der vor dem Unterstrich angezeigt wird. Es funktioniert jedoch nicht, da dieser Text keine exakte Übereinstimmung ist. Verwenden Sie den vollständigen regulären Ausdruck wie folgt: ^([^_]+)_.*

6. Zum Verfassen von Text klicken Sie sich im Abschnitt „Warnungsausgabe umwandeln und verfassen“ in das erforderliche Feld.



Verfassen Sie Text in den Warnungsfeldern, indem Sie eine der folgenden Aktionen ausführen:

- Ziehen Sie ein Feld aus dem Event-Informationsbereich in das erforderliche Feld.
- Verwenden Sie den Event-Informationsbereich als Referenz für verfügbare Felder. Schreiben Sie die Feldnamendetails im Format ${<fieldname>}, wobei „$“ für „Wert verwenden“ steht. Zwischen den Klammern ersetzt der Name des Event-Felds die Variable <fieldname>.
- Geben Sie Text mit Leerzeichen oder Sonderzeichen ein. Verwenden Sie beispielsweise Leerzeichen oder Unterstriche (_), um den Text im Warnungsfeld lesbar zu machen.

7. Um Felder anzugeben, die in der generierten Warnung angezeigt werden sollen, aktivieren Sie das Kontrollkästchen **Manuelle Attribute**.

Hinweis: Diese Felder und ihre Werte werden im Abschnitt **„Zusätzliche Informationen“** oder im Abschnitt „ **Warnungs-Tags“** für Attribute mit dem Präfix „t_“ angezeigt.

a. Geben Sie in der linken Spalte einen Wert ein.

b. Ziehen Sie in der rechten Spalte entweder einen Wert aus den Feldern Hinzufügen oder Ausdruck, oder geben Sie einen Wert ein.
Wenn Sie einen Wert mit Attributen mit dem Präfix „t_“ eingeben, wird eine Dropdown-Liste mit allen zuvor definierten „t_“-Attributen angezeigt.

8. Klicken Sie auf **Speichern** oder **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Sie können Event-Regeln filtern. Weitere Informationen finden Sie unter Events filtern, für die eine Event-Regel gilt.

Zugehörige Informationen

- Event-Regel erstellen oder bearbeiten
- Event-Eingabeinformationen verwenden
- Warnungstags
- Events filtern, für die eine Event-Regel gilt

Schwellenwert festlegen, um die Warnungsgenerierung zu unterdrücken

Der Event-Schwellenwert ist die Rate, mit der Ereignismanagement eine Warnung generiert. Der Empfang mehrerer Events für ein Gerät in einem kurzen Intervall kann die Erstellung einer Warnung rechtfertigen, da die Bedingung schwerwiegend sein kann. Der Empfang von Events über einen längeren Zeitraum kann jedoch auf eine weniger schwerwiegende Situation hinweisen, die das Erstellen einer Warnung nicht rechtfertigt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Eigenschaften in einer Event-Regel konfigurieren, um Warnungen zu erstellen, die Warnungsgenerierung zu unterdrücken oder vorhandene Warnungen gemäß einem bestimmten Schwellenwert zu schließen. Der Schwellenwert basiert auf dem Wert von Event-Feldern oder der Anzahl der Vorkommen über einen angegebenen Zeitraum.

Hinweis: **Feldname** kann im Feld **Zusätzliche Informationen** des Events der Name eines numerischen Feldes sein. Deshalb gilt: Wenn die `CPU` ein zusätzliches Informationsfeld für ein bestimmtes Event ist, dann kann die `CPU` als **Feldname**verwendet werden.

Angenommen, Sie möchten eine Warnung generieren, wenn die CPU-Auslastung dreimal mit maximal 20 Sekunden zwischen zwei aufeinanderfolgenden Ereignissen 80 % erreicht oder überschreitet. Erstellen Sie eine Event-Regel mit diesen Einstellungen (eine Erklärung für jeden Wert finden Sie in Klammern):

- **Warnoperator erstellen**: *>=* (Operator, um zu bestimmen, ob die Nutzung des **Feldnamens** den angegebenen Wert erreicht oder überschreitet)
- **Feldname**: *CPU* (Events im Zusammenhang mit hoher CPU-Auslastung)
- **Schwellenwert**: *80* (Prozent)
- **Vorkommnisse**: *3* (drei Events, bei denen die CPU-Auslastung bei „> =“ 80 % oder darüber liegt)
- **Über Zeitraum (Sekunden)**: *20* (20 Sekunden oder weniger zwischen Events)

Zum Demonstrieren der Auswertung der vorherigen Einstellungen wird davon ausgegangen, dass die folgenden Events empfangen werden:

Szenario	Ergebnis
Gemeldete verstrichene Zeit und CPU-Auslastung für jedes Event:	In diesem Szenario wird keine Warnung generiert, da ein Event eine CPU-Auslastung aufweist, die unter 80 % liegt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenario	Ergebnis
• Verstrichene Zeit seit dem ersten Event 20, CPU = 85 • Verstrichene Zeit seit dem zweiten Event 40, CPU = 80 • Verstrichene Zeit seit dem dritten Event 60, CPU = 70	
Gemeldete verstrichene Zeit und CPU-Auslastung für jedes Event: • Verstrichene Zeit seit dem ersten Event 20, CPU = 85 • Verstrichene Zeit seit dem zweiten Event 40, CPU = 90 • Verstrichene Zeit seit dem dritten Event 70, CPU = 95	In diesem Szenario wird keine Warnung generiert, da die verstrichene Zeit in einem Event die angegebenen 20 Sekunden überschreitet.
Gemeldete verstrichene Zeit und CPU-Auslastung für jedes Event: • Verstrichene Zeit seit dem ersten Event 20, CPU = 85 • Verstrichene Zeit seit dem zweiten Event 40, CPU = 95 • Verstrichene Zeit seit dem dritten Event 60, CPU = 90	In diesem Szenario wird eine Warnung generiert, da die verstrichene Zeit in allen Events innerhalb der angegebenen Zeit liegt und die CPU-Auslastung über 80 % beträgt.

Hinweis:

- Beim Konfigurieren einer Event-Regel zum Erstellen oder Schließen von Warnungen gemäß einem Schwellenwert werden Events, die zur gleichen Sekunde eintreffen, wie vom Feld *time_of_event* bestimmt, übersprungen. Dies geschieht, da diese Events als Duplikate betrachtet werden.
- Wenn Schwellenwertbedingungen konfiguriert sind, werden Warnungen geschlossen, wenn die Bedingung für **Warnoperator schließen** erfüllt wird, und nicht, wenn ein Event mit **Schweregrad = Klar** oder **Lösungsstatus = Schließen**empfangen wird.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.
2. Erstellen oder öffnen Sie eine Event-Regel.
3. Klicken Sie auf **Schwellenwert**.
4. Wählen Sie **Aktiv** aus.
   Wenn **Aktiv** nicht ausgewählt ist, werden die Felder auf dieser Seite nicht angezeigt.
5. Wählen Sie im Feld **Warnoperator erstellen** einen Operator aus.
   - Wenn Sie **Anzahl** wählen, geben Sie die entsprechenden Werte für **Vorkommnisse** und **Über Zeitraum (Sekunden)** an.
   - Wenn Sie einen anderen Operator als **Anzahl**auswählen, werden die Felder **Feldname** und **Schwellenwert** angezeigt. Geben Sie die erforderlichen Werte in diese Felder ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

> **Hinweis:** Der Wert der Eigenschaft **Schwellenwert** kann der Name eines beliebigen Felds in den **Zusätzlichen Informationen** des Ereignisses sein. Wenn beispielsweise `„CPU“` ein Feld unter **„Zusätzliche Informationen“** für ein bestimmtes Ereignis ist, kann `„CPU“` als **Schwellenwert**verwendet werden.

   - Geben Sie im Feld **Vorkommnisse** den erforderlichen Wert an.
   - Geben Sie im Feld **Über Zeitraum (Sekunden)** den erforderlichen Zeitraum an.

6. Zum automatischen Schließen von Warnungen wählen Sie im Feld **Warnoperator schließen** einen Operator aus.
   Entsprechend Ihrer Auswahl werden zusätzliche Felder angezeigt.
   - Wenn **Anzahl** als Operator für das Feld **Warnoperator erstellen** angegeben ist, dann ist die Auswahl im Feld **Warnoperator schließen** entweder `Keine` oder `Inaktiv`. Geben Sie den erforderlichen Wert an.
   - Wenn Sie **Inaktiv**auswählen, konfigurieren Sie das Feld **Über Zeitraum (Sekunden)**.
   - Wenn Sie im Feld **Operator für Warnungsschließung** einen anderen Operator als **Leerlauf**auswählen, konfigurieren Sie anschließend die Felder **Schwellenwert**, **Tritt ein**und **Über (Sekunden)**.
7. Klicken Sie auf **Speichern** oder auf **Absenden**.

Example:
So erstellen Sie eine Warnung, wenn ein bestimmtes Event fünf Mal in 10 Minuten auftritt – unter **Schwellenwert**:

1. Geben Sie im **Feld Feldname** den Namen eines beliebigen Felds an, das im Feld **Zusätzliche Informationen** im Ereignis vorhanden ist. Der Wert des Felds ist irrelevant.
2. Wählen Sie im Feld **Warnoperator erstellen** `Anzahl` aus.
3. Geben Sie im Feld **Vorkommnisse** `5` an.
4. Geben Sie im Feld **Über Zeitraum** `600` (10 * 60 Sekunden) an.
5. Klicken Sie auf **Speichern** oder auf **Absenden**.

So erstellen Sie eine Warnung, wenn ein bestimmtes Event fünf Mal in 10 Minuten auftritt – mit einem Metrikwert über 55. Nehmen Sie an, dass „metric_value“ ein Feld in den **Zusätzlichen Informationen** des Events ist. Geben Sie Folgendes an:

1. Aktivieren Sie das Kontrollkästchen *Active*.
2. Wählen Sie im Feld **Warnoperator erstellen** `>=` aus.
3. Geben Sie im **Feld** Feldname den Wert **metric_value**an.
4. Geben Sie im Feld **Schwellenwert den Wert**`55 an`.
5. Geben Sie im Feld **Vorkommnisse** `5` an.
6. Geben Sie im Feld **Über Zeitraum** `600` (10 * 60 Sekunden) an.
7. Klicken Sie auf **Speichern** oder auf **Absenden**.

Zugehörige Informationen

- Event-Regel erstellen oder bearbeiten
- Event-Eingabeinformationen verwenden
- Event-Regel konfigurieren, um den Warnungsinhalt anzupassen
- Events filtern, für die eine Event-Regel gilt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungen an CIs binden

Die CI-Bindung oder -Verknüpfung ist der Prozess des Suchens und Verbindens eines Configuration Item (CI) aus Configuration Management Database (CMDB) mit einer Warnung mithilfe der in Ereignisregeln definierten Logik. Dadurch wird sichergestellt, dass Warnungen an die richtigen IT-Komponenten gebunden werden, um die Transparenz zu verbessern und Probleme schneller zu lösen.

Informationen zur CI-Bindung

Durch das Binden von Warnungen an CIs werden eingehende Warnungen mit dem richtigen Configuration Item (CI) verknüpft, das einen bestimmten Host darstellt, z. B. einen Computer, Server, Router oder einen virtuellen Computer in Ihrer IT-Infrastruktur. Dies stellt eine genaue Nachverfolgung von Warnungen sicher, vereinfacht die Fehlerbehebung durch Identifizierung der Ursache von Problemen und verwaltet den Verlauf von Warnungen, die an bestimmte Systeme gebunden sind.

In IT Operations Managementspielt die Beziehung zwischen Warnungen und CIs eine entscheidende Rolle für die effektive Verwaltung von Services und Infrastruktur. Ein CI stellt eine Komponente in Ihrer IT-Umgebung dar, z. B. einen Server, eine Anwendung oder eine Datenbank. Durch die Verknüpfung von Warnungen mit CIs wird sichergestellt, dass Warnungen und Incidents direkt der betroffenen Komponente zugeordnet werden. Dies ermöglicht eine genaue Auswirkungsanalyse und eine schnellere Lösung.

In dynamischen und großen Umgebungen ist es oft schwierig, genau zu bestimmen, welches CI für die Auslösung einer Warnung verantwortlich ist. Warnungen werden aus Ereignis-Rohdaten generiert, die in mehreren Quellen erfasst wurden, diese Daten dürfen jedoch nicht explizit auf ein CI verweisen. Ohne eine zuverlässige Methode zum Binden von Warnungen an CIs sind IT-Teams dem Risiko ausgesetzt:

- Schlechte Transparenz der Auswirkungen auf den Service.
- Längere durchschnittliche Zeit bis zur Lösung (MTTR)
- Ineffiziente Warnungsverwaltungsprozesse.

Ereignisregeln bieten eine strukturierte Möglichkeit, eingehende Ereignisdaten zu analysieren, mit zusätzlichem Kontext anzureichern und dem richtigen CI zuzuordnen. Diese Regeln fungieren als Brücke und wandeln Ereignis-Rohdaten in umsetzbare Warnungen um, die mit CIs verknüpft sind. Ereignisregeln können beispielsweise:

- Eingehende Ereignisdaten analysieren: Der Prozess umfasst die Aufgliederung von Ereignis-Rohdaten, um wichtige Details wie Hostnamen, IP-Adressen oder Service-Tags zu extrahieren. Diese Details werden dann verwendet, um das Ereignis zu analysieren – Quelle, Typ und Auswirkung zu identifizieren – und die Warnung durch Hinzufügen von relevantem Kontext zu ergänzen, z. B. betroffene Services, Prioritäten oder Lösungsschritte, um sicherzustellen, dass sie für IT-Teams umsetzbar ist.
- Muster abgleichen: Hier werden die extrahierten Ereignisdetails – wie Hostnamen, IP-Adressen oder Service-Tags – mit Einträgen in CMDB verglichen, um das entsprechende Configuration Item (CI) basierend auf vordefinierten Regeln oder Logik zu identifizieren. Nach der Übereinstimmung wird die Warnung mit dem CI verknüpft, wodurch Kontext zur betroffenen IT-Komponente für bessere Transparenz und schnellere Lösung bereitgestellt wird.
- CI an Warnung binden: Zu diesem Zeitpunkt wird die Warnung automatisch dem identifizierten CI zugeordnet. Es stellt sicher, dass die Warnung mit der richtigen IT-Komponente im System verbunden ist, erleichtert die Nachverfolgung und Verwaltung und hilft Teams, das Problem schnell zu beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten der CI-Bindung

Bindungstyp	Beschreibung
Implizite Knotenbindung (Standardbindung)	Bindet Warnungen an Host-CIs, indem das Feld **„Knoten“** im Ereignis mit Attributen wie Name, FQDN, IP oder MAC-Adresse abgeglichen wird.
Übereinstimmungsbindung des CI-Felds	Bindet Warnungen an das Feld **„CI-Bezeichner“**, eine JSON-Struktur, die Spaltennamen und Werte enthält (z. B. Name, FQDN, IP oder MAC-Adresse).
CI-Identifizierungsbindung	Bindet Warnungen mithilfe von Ereignisregeln an bestimmte Anwendungen auf Hosts.
Bindung auf Prozessebene	Bindet Warnungen an Anwendungs-CIs durch Abgleich prozessbezogener Attribute.
Bindung auf Geräteebene	Bindet Warnungen an Geräte-CIs, indem Ereignisdaten mit Attributen wie Hostname, IP-Adresse oder MAC-Adresse abgeglichen werden.

Hauptvorteile

- Verbesserte Transparenz von Services: Mit CIs verknüpfte Warnungen vermitteln ein klares Bild davon, welche IT-Komponenten betroffen sind.
- Verbesserte Automatisierung: Die automatisierte CI-Bindung reduziert den manuellen Aufwand und sorgt für Konsistenz.
- Schnellere Lösung: Teams können Probleme schnell diagnostizieren und lösen, indem sie sich auf das betroffene CI konzentrieren.

Beispielanwendungsfall

Szenario: Der E-Mail-Server eines Unternehmens mit dem Namen „MailServer-01“ fällt aus.

Prozess:

1. Warnungsgenerierung: Eine Warnung wird ausgelöst, wenn MailServer-01 nicht mehr reagiert.
2. CI-Bindung: Ereignismanagement sucht automatisch nach MailServer-01 in der CMDB (Configuration Management Database).
   - Falls gefunden, wird die Warnung mit diesem bestimmten Server (CI) verknüpft.
   - Falls der Wert nicht gefunden wird, bleibt die Verknüpfung der Warnung aufgehoben, bis weitere Informationen bereitgestellt werden.

Ergebnis: Die Warnung zeigt jetzt an, dass „MailServer-01“ das betroffene System ist.

- Auswirkung: IT-Teams wissen sofort, welcher Server untersucht werden muss.
- Effizienz: Sie müssen keine anderen Infrastrukturkomponenten oder Systeme überprüfen, was Zeit und Aufwand spart.

Dieser direkte Link hilft, die Problembehandlung zu optimieren, indem er auf die genaue Problemquelle verweist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

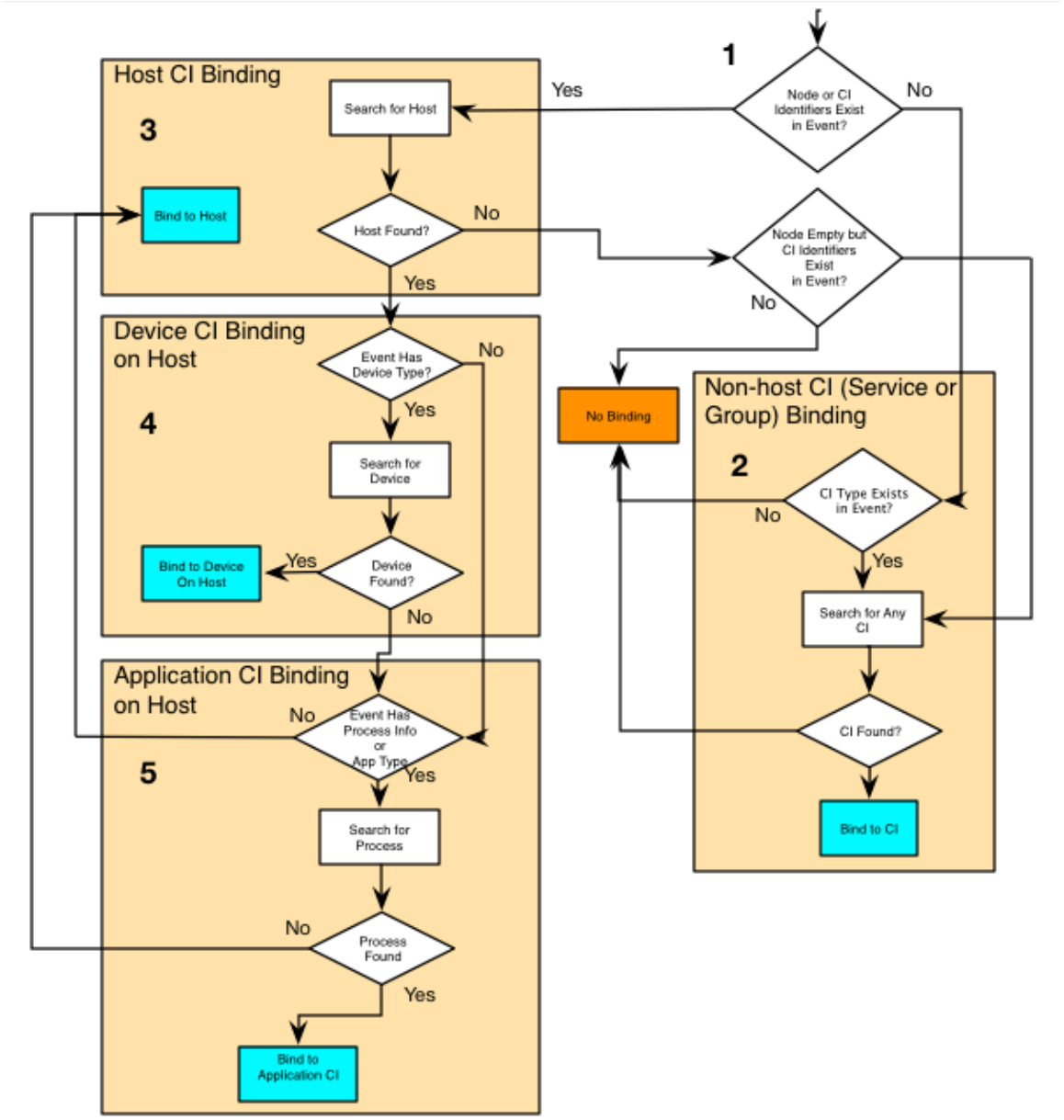
Zugehörige Informationen

Ereignisverarbeitung simulieren

Bindungsprozess-Flow

Lernen Sie, wie Konfigurationselemente (Configuration Items, CI) an Warnungen gebunden werden. Dies umfasst die Verarbeitung der Ereignisauthentifizierung, das Binden von Warnungen mithilfe verfügbarer Felder, wenn kein Knoten vorhanden ist, und das Durchsuchen von CMDB nach übereinstimmenden Hosts. Außerdem wird erläutert, wie Warnungen basierend auf der Host- und CI-Typerkennung mit CIs verknüpft werden.

CI-Bindung an Warnungen: Flow-Diagramm



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozess der Verknüpfung von CIs mit Warnungen

1. Ereigniseingang: Wenn ein Ereignis empfangen wird, sucht Ereignismanagement nach Knoten- oder CI-Bezeichnern.
2. Ist Knotenwert vorhanden?
   - Ja: Wenn ein Knotenwert angegeben wird, durchsucht Ereignismanagement den CMDB Knoten nach einem übereinstimmenden Host.
   - Nein: Wenn kein Knoten gefunden wird, versucht das System, die Warnung mit anderen verfügbaren Details zu binden, z. B.:
     - Warntyp
     - Zusätzliche Informationen
     - CI-Identifier
3. Erkennung von Host und CI-Typ:
   - Beide gefunden: Wenn sowohl ein Host als auch ein CI-Typ identifiziert werden, wird die Warnung mit dem entsprechenden Geräte-CI verknüpft.
   - Nur Host gefunden: Wenn nur ein Host identifiziert wird, verknüpft das System die Warnung mit einem Anwendungs-CI.

Zusätzliche Überlegungen

- Hinweise zur Ereignisverarbeitung: Das Ereignis kann den Bindungsprozess-Flow in sein Feld **Verarbeitungshinweise** aufnehmen und Einblicke in die Bindungsaktionen bieten.
- Bindung an deaktivierte CIs: Standardmäßig werden Ereignisse nicht an CIs mit dem Status „Deaktiviert“ gebunden. Um die Bindung an diese CIs zu aktivieren, legen Sie die Eigenschaft *evt_mgmt.ignore_retired_cis_in_binding* auf „falsch“ fest.
- CI-Status für Bindung angeben: Sie können die Eigenschaft *evt_mgmt.install_status_list_to_ignore_in_binding* konfigurieren, indem Sie CI-Statusnummern angeben, um zu steuern, welche CIs für die Bindung berücksichtigt werden. Zum Beispiel:

CI-Status

Statusnummer	Status
1	Installiert
2	OnOrder
3	InMaintenance
4	PendingInstall
5	PendingRepair
6	InStock
7	Retired
8	Gestohlen
100	Abwesend

Hinweis: Um mehrere Status anzugeben, trennen Sie jede Statusnummer durch ein Komma.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungen an ein bestimmtes Host-CI binden (Standardbindung)

Die Bindung von Warnungen an Configuration Items (CIs) über das Feld **„Knoten“** oder **„CI-Bezeichner“** stellt eine genaue Ereigniszuordnung sicher. Durch Vergleich des **Knoten-** oder **CI-** Bezeichnerwerts eines Ereignisdatensatzes werden Warnungen mit dem richtigen System verknüpft. Dies verbessert die Reaktion, die Ursachenanalyse und die Folgenbewertung durch eine klare Transparenz der betroffenen Assets.

Funktionsweise der Standardbindung

Das System kann die Standardbindung mit dem Feld **„Knoten“** oder dem Feld **„CI-Bezeichner“** aus dem Ereignisdatensatz durchführen.

Wenn ein Ereignis im System ankommt, ist ein Schlüsselfeld wie **„Knoten“** im Ereignisdatensatz verfügbar. Das CI enthält jedoch kein Feld **„Knoten“**. Stattdessen wird der Knotenwert aus dem Ereignis mit verschiedenen Attributen im Host-CI verglichen, z. B. Name, vollständig qualifizierter Domänenname (FQDN), IP- oder MAC-Adresse. Wenn eine Übereinstimmung gefunden wird, wird die Warnung mit dem entsprechenden CI verknüpft. Dies ist die Standardmethode zum Binden von Warnungen an CIs.

Hinweis: In diesem Bindungsprozess muss das CI ein Host sein. Zu Host-CIs gehören Computer, Betriebssysteme, Switches, Router oder alle CI-Typen/Klassen, die die Tabelle [cmdb_ci_hardware] erweitern. Dies bedeutet, dass der CI-Typ oder die Klasse eine Hardwarekomponente sein muss.

Wenn mit dem Knoten keine Übereinstimmung gefunden wird, sucht das System im Feld **„CI-Bezeichner“** im Ereignisdatensatz. Der **CI-Bezeichner** ist eine JSON-Struktur, die Spaltennamen und Werte für den Vergleich enthält (z. B. Name, vollqualifizierter Domänenname, IP oder MAC-Adresse). Beispiel: Wenn das Host-CI **eine Hardware-Seriennummer** ist und eine ausgefüllte Liste mit dem Namen **serial_number**enthält, lautet das JSON-Format: `{"serial_number":"`<Dell Latitude 7420 Laptop> "} . Wenn eine Übereinstimmung gefunden wird, wird die Warnung mit dem entsprechenden CI verknüpft.

Unterschied zwischen Bindung mit Knoten vs. CI-Identifier

Bei der Standardbindung berücksichtigt das System alle Felder im Feld **„Zusätzliche Informationen“** und versucht, ihre Werte mit der CI-Tabelle abzugleichen. Im Feld **„CI-Bezeichner“** können bestimmte Felder für den Abgleich angegeben werden, auch wenn sie nicht unter **„Zusätzliche Informationen“**aufgeführt sind. Dieser Prozess verwendet eine vordefinierte JSON-Struktur, und gilt nur, wenn das CI ein Host ist.

Hinweis: Auch wenn der **Knoten** oder der **CI-Bezeichner** die Warnung erfolgreich an das CI bindet, bestimmen Ereignisregeln darüber hinaus, wie die Bindung erfolgt, indem in Ereignisregeln das Kontrollkästchen **Standardbindung überschreiben** aktiviert ist. Dadurch wird sichergestellt, dass Warnungen basierend auf der Geschäftslogik korrekt gebunden werden und nicht nur aufgrund direkter Übereinstimmungen. Dadurch wird sichergestellt, dass Warnungen basierend auf der Geschäftslogik korrekt gebunden werden und nicht nur aufgrund direkter Übereinstimmungen.

Beispiel: Auflösen eines CI mithilfe von Knoten- und Ereignisregeln

Angenommen, ein Server (Server-123) in Ihrem Netzwerk generiert ein Ereignis. Der Ereignisdatensatz enthält ein **Knotenfeld** mit dem Wert „Server-123.example.com“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Abgleich mit CI-Attributen:
   a. Das System gleicht den Knotenwert mit der CMDB ab.
   b. Er vergleicht „Server-123.example.com“ mit dem FQDN, der IP, der MAC-Adresse oder dem Namen vorhandener Host-CIs.
   c. Wenn eine Übereinstimmung gefunden wird (z. B. lautet der FQDN in der CMDB auch „Server-123.example.com“), wird die Warnung mit diesem CI verknüpft.
2. Ereignisregeln werden angewendet: Selbst wenn der Knoten in Server-123 aufgelöst wird, können zusätzliche Ereignisregeln bestimmen, ob die Warnung anders verknüpft werden soll. Beispielsweise kann eine Ereignisregel festlegen, dass Warnungen von Server-123 mit einem übergeordneten CI (z. B. einem Cluster) anstatt mit dem einzelnen Server verknüpft werden sollen.

Standardbindung wird überschrieben

Das Überschreiben der Standardbindung bietet Flexibilität beim Verknüpfen von Warnungen mit CIs, die über den standardmäßigen knotenbasierten Abgleich hinausgehen. Dies hilft bei der Anpassung der Warnungsbindung an die Geschäftsbedürfnisse, stellt genaue Zuordnungen sicher, verhindert falsch verknüpfte Warnungen und verbessert das Incident-Management und die Ursachenanalyse.

Standardmäßig werden Warnungen an CIs gebunden, indem der Knotenwert in der Warnung mit Attributen wie Name, FQDN, IP oder MAC-Adresse im CI abgeglichen wird. Wenn Sie dieses Verhalten jedoch ändern möchten – entweder durch Verwendung zusätzlicher Kriterien oder durch vollständiges Ignorieren des Knotens – können Sie das Kontrollkästchen **Standardbindung überschreiben** verwenden.

Dies ermöglicht zwei Szenarien:

1. Wenn Bindungstyp = CI-Feldabgleich
   - Wenn das CI ein Host ist, ist der Knoten für die Bindung erforderlich. Weitere Informationen finden Sie unter Binden Sie Host-CIs mithilfe des CI-Feldabgleichs.
   - Wenn das CI kein Host ist, muss der Knoten leer sein. Weitere Informationen finden Sie unter Binden Sie Nicht-Host-CIs mithilfe des CI-Feldabgleichs.
2. Wenn Bindungstyp = CI-Identifizierung Weitere Informationen finden Sie unter Binden Sie Warnungen mithilfe der CI-Identifizierung an CIs.

Diese Flexibilität stellt sicher, dass Warnungen basierend auf bestimmten Geschäftsanforderungen richtig verknüpft werden.

Binden Sie Host-CIs mithilfe des CI-Feldabgleichs

Wenn der CI-Feldabgleich verwendet wird und das CI ein Host ist, wird der Knotenwert aus der Warnung für die Bindung verwendet. Das System vergleicht den Knoten mit Attributen wie Name, FQDN, IP oder MAC-Adresse in der CMDB, um eine Übereinstimmung zu finden. Dadurch wird sichergestellt, dass Warnungen korrekt mit dem entsprechenden Host-CI verknüpft sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein Ereignis im System eingeht, ist ein Schlüsselfeld wie **„Knoten“** im Ereignisdatensatz verfügbar. In CI gibt es kein Feld wie **Knoten**. Der Wert des Knotens aus dem Ereignis wird jedoch mit anderen Werten im Host-CI verglichen, z. B. Name, vollqualifizierter Domänenname (FQDN), IP oder MAC-Adresse. Wenn eine Übereinstimmung gefunden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

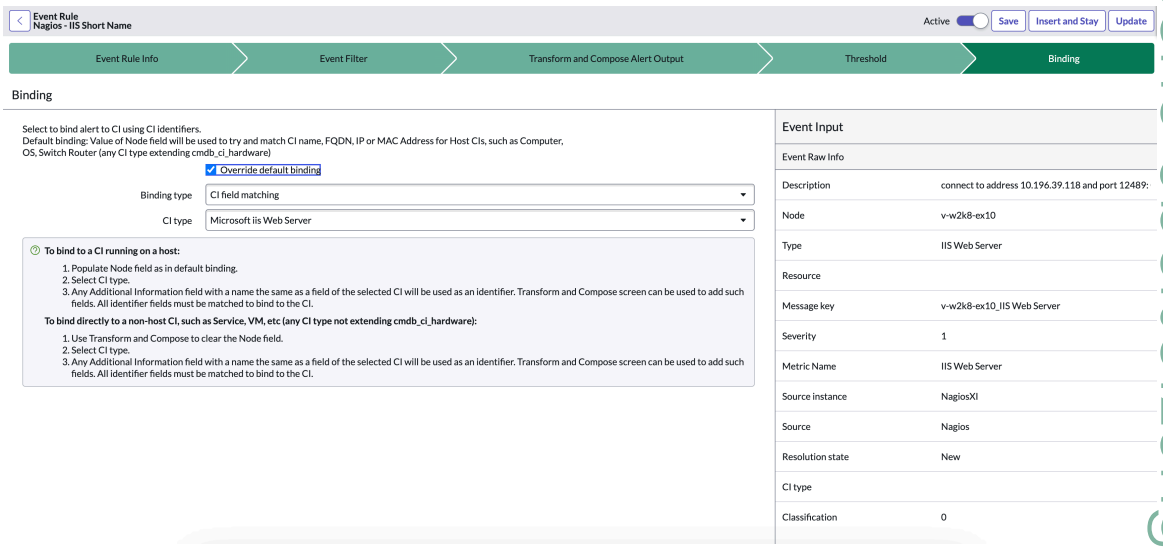
wird, wird die Warnung mit dem entsprechenden CI verknüpft. Dies ist die Standardbindung von Warnungen an CIs. In dieser Bindung muss das CI ein Host sein. Zu Host-CIs gehören Computer, Betriebssysteme, Switches, Router – im Grunde jeder CI-Typ oder jede Klasse, die die Tabelle [cmdb_ci_hardware] erweitert.

Es kann Fälle geben, in denen keine Übereinstimmung gefunden wird, da sich die Spaltennamen im Ereignisdatensatz und in der Tabelle für dasselbe Element unterscheiden. In solchen Fällen können Sie manuell ein zusätzliches Schlüssel-Wert-Paar mit einem Namen erstellen, der der Tabellenspalte entspricht, um sicherzustellen, dass der Übereinstimmungsprozess erfolgreich fortgesetzt wird. Informationen zum Erstellen eines manuellen Felds finden Sie unter Binden Sie CIs mithilfe des CI-Feldabgleichs und der Behandlung von Spaltennamenunterschieden.

Hinweis: Selbst wenn der Knoten die Warnung erfolgreich an das CI bindet, bestimmen Ereignisregeln weiter, wie die Bindung erfolgt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.
2. Wählen Sie **Neu** aus, und füllen Sie die Pflichtfelder der Ereignisregel aus.
3. Wählen Sie die Registerkarte **Bindung**.
4. Aktivieren Sie das Kontrollkästchen **Standardbindung überschreiben**.
5. Wählen Sie im Feld **Bindungstyp CI-Feldübereinstimmung** aus.



6. Wählen Sie im Feld **CI-Typ** den entsprechenden Typ der Hardwarekomponente (z. B. Server, Router oder Speichergerät) aus, die durch den CI-Typ dargestellt wird. Der **CI-Typ** bestimmt die spezifische CMDB-Tabelle, in der das System nach dem übereinstimmenden CI sucht. Wenn der **CI-Typ** beispielsweise **Netzwerkadapter**ist, sucht das System in der Tabelle [cmdb_ci_network_adapter].
7. Wählen Sie **Absenden**.

Zugehörige Informationen

Binden Sie Nicht-Host-CIs mithilfe des CI-Feldabgleichs

Binden Sie Nicht-Host-CIs mithilfe des CI-Feldabgleichs

Wenn mit dem Feld **„Knoten“** keine Übereinstimmung gefunden wird, verwendet das System das Feld **„CI-Identifier“**, um Warnungen anhand von Attributen wie Name, FQDN, IP oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

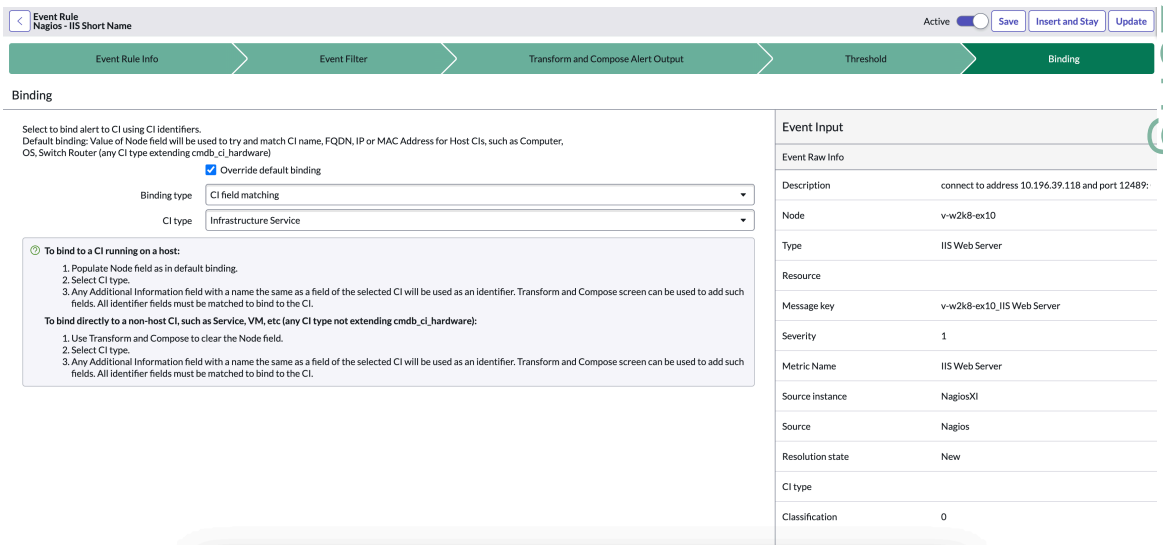
MAC mit Nicht-Host-CIs abzugleichen. Dies stellt eine genaue Warnungszuordnung sicher und verbessert die Transparenz, die Fehlerbehebung und die Ursachenanalyse für verschiedene Infrastrukturkomponenten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn mit dem Feld **Knoten** keine Übereinstimmung gefunden wird, sucht das System im Feld **Zusätzliche Informationen** der Warnung. Wenn Sie einen CI-Typ auswählen, z. B. Dateisystem, sucht das System automatisch nach einem übereinstimmenden Datensatz in der Tabelle [cmdb_ci_file_system]. Sie verwendet die Details im Ereignisregel-Datensatz, insbesondere im Feld **„Zusätzliche Informationen“**, um die Suche einzugrenzen. Wenn beispielsweise das Feld „ **Zusätzliche Informationen** “ Werte wie `{"mount_point": "/snap/amazon-ssm-agent/9565", "name": "/dev/loop0"}`enthält, sucht das System nach einem Datensatz in [cmdb_ci_file_system] Tabelle, die diesen Werten entspricht. Wenn eine Übereinstimmung gefunden wird, bindet das System das CI an die Warnung, um eine genaue Identifizierung und Zuordnung sicherzustellen. Wenn der **CI-TypNetzwerkadapter**ist, sucht das System entsprechend in der Tabelle [cmdb_ci_network_adapter].

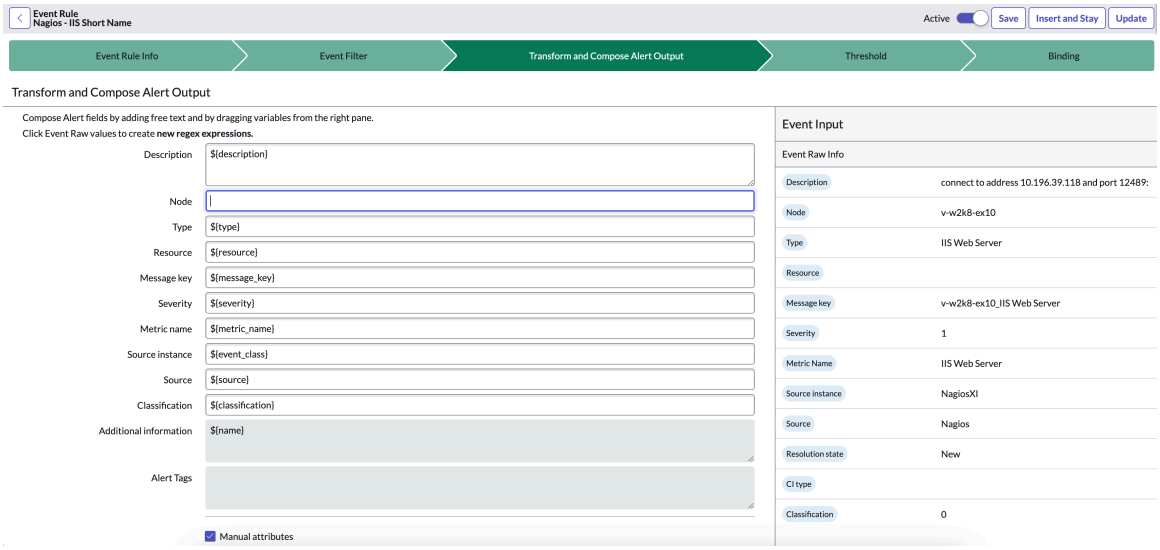
Es kann Fälle geben, in denen keine Übereinstimmung gefunden wird, da sich die Spaltennamen im Ereignisdatensatz und in der Tabelle für dasselbe Element unterscheiden. In solchen Fällen können Sie manuell ein zusätzliches Schlüssel-Wert-Paar mit einem Namen erstellen, der der Tabellenspalte entspricht, um sicherzustellen, dass der Übereinstimmungsprozess erfolgreich fortgesetzt wird. Informationen zum Erstellen eines manuellen Felds finden Sie unter Binden Sie CIs mithilfe des CI-Feldabgleichs und der Behandlung von Spaltennamenunterschieden.

Prozedur
1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.
2. Wählen Sie **Neu** aus, und füllen Sie die Pflichtfelder der Ereignisregel aus.
3. Wählen Sie die Registerkarte **Bindung**.
4. Aktivieren Sie das Kontrollkästchen **Standardbindung überschreiben**.
5. Wählen Sie im Feld **Bindungstyp CI-Feldübereinstimmung** aus.



6. Wählen Sie die Registerkarte **Warnungsausgabe umwandeln und verfassen aus**.
7. Löschen Sie den Wert im **Knotenfeld**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



8. Wählen Sie im Feld **CI-Typ** das Nicht-Host-CI aus.

   Ein Nicht-Host-CI-Typ ist ein beliebiger CI-Typ, der die Tabelle [cmdb_ci_hardware] nicht erweitert, z. B. ein Service oder eine VM. Der **CI-Typ** bestimmt die spezifische CMDB-Tabelle, in der das System nach dem übereinstimmenden CI sucht.

9. Wählen Sie **Speichern**.

Binden Sie CIs mithilfe des CI-Feldabgleichs und der Behandlung von Spaltennamenunterschieden

Binden Sie CIs, indem Sie Felder vom Typ „ **Zusätzliche Informationen“** zum Ereignis mit CI-Attributen abgleichen. Wenn sich die Spaltennamen unterscheiden, erstellen Sie manuell ein zusätzliches Schlüssel-Wert-Paar, um sie an der CI-Tabelle auszurichten und eine genaue CI-Zuordnung sicherzustellen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

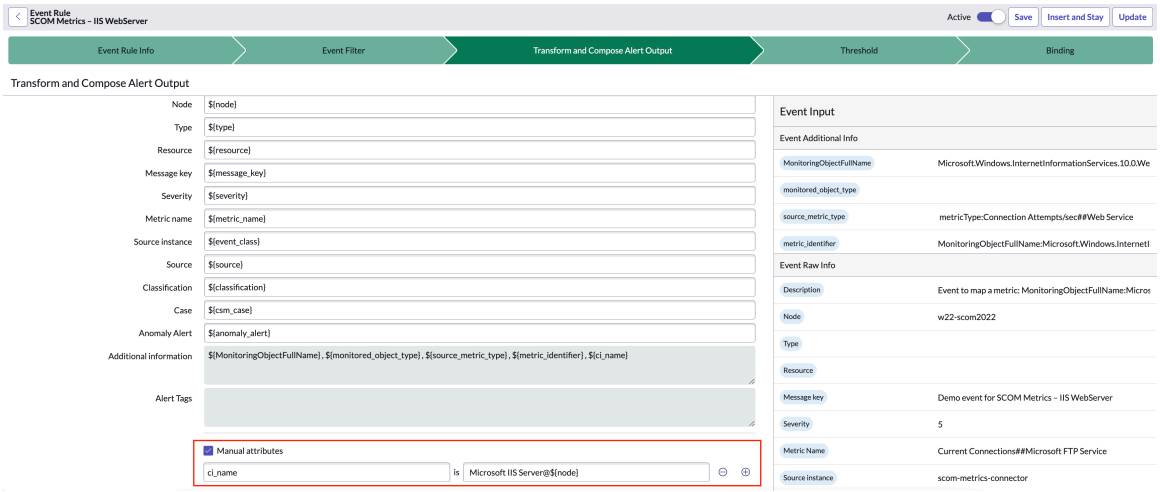
Warum und wann dieser Vorgang ausgeführt wird

Wenn mit dem Feld **Knoten** keine Übereinstimmung gefunden wird, sucht das System im Feld **Zusätzliche Informationen** im Ereignisdatensatz. Es kann Fälle geben, in denen keine Übereinstimmung gefunden wird, da sich die Spaltennamen im Ereignisdatensatz und in der Tabelle für dasselbe Element unterscheiden. In solchen Fällen können Sie manuell ein zusätzliches Schlüssel-Wert-Paar mit einem Namen erstellen, das der Tabellenspalte entspricht, und es dem Feld **Zusätzliche Informationen** hinzufügen, um sicherzustellen, dass der Übereinstimmungsprozess erfolgreich fortgesetzt wird.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.
2. Wählen Sie **Neu** aus, und füllen Sie die erforderlichen Felder aus, oder öffnen Sie einen vorhandenen Ereignisregeldatensatz, um ihn zu ändern.
3. Wählen Sie die Registerkarte **Warnungsausgabe umwandeln und verfassen aus**.
4. Aktivieren Sie die Checkbox **Manuelle Attribute**.
5. Geben Sie in den Feldern **Feldname** und **Feldwert** den entsprechenden Feldnamen ein, und geben Sie das Quellfeld an, aus dem der Wert ausgefüllt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Verwenden Sie das Hinzufügen-Symbol (⊕), um nach Bedarf mehrere Felder hinzuzufügen.

6. Wählen Sie **Speichern**.
   Die Felder werden im Ereignisregel-Datensatz erstellt. Wenn jedoch aus einem Ereignis mithilfe der Ereignisregel eine Warnung generiert wird, werden die manuell hinzugefügten Felder im Feld **Zusätzliche Informationen** der Warnung angezeigt.

Binden Sie Warnungen mithilfe der CI-Identifizierung an CIs

Binden Sie Warnungen mithilfe von Ereignisregeln an bestimmte Anwendungen auf Hosts, um eine genaue Nachverfolgung sicherzustellen und die Geschwindigkeit der Problemlösung zu verbessern. Dies führt zu einer effizienten Behebung und einer besseren Ausrichtung von Warnungen auf die richtigen Ressourcen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

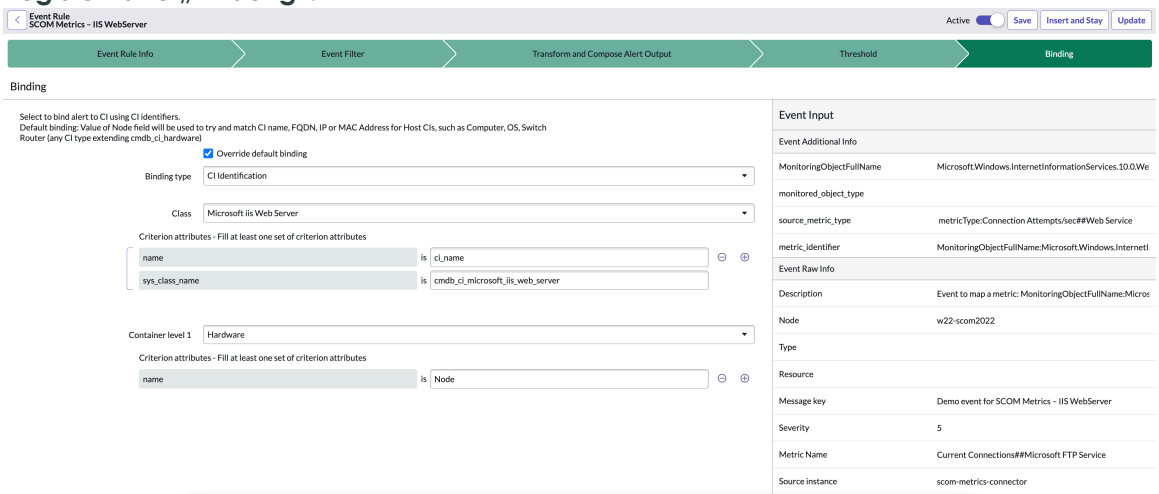
Warum und wann dieser Vorgang ausgeführt wird

Bevor wir durch das Verfahren gehen, wollen wir zunächst anhand eines Beispiels verstehen, wie diese Bindung funktioniert. Angenommen, die sofort einsatzbereite Ereignisregel „SCOM-Metriken – IIS-Webserver“ generiert eine Warnung für einen Microsoft IIS-Webserver, der auf einem Host ausgeführt wird. Anstatt die Warnung nur an den Hostcomputer zu binden, soll sie der spezifischen Anwendung (IIS-Webserver) zugeordnet werden, bei der das Problem aufgetreten ist. Hier erfahren Sie, wie das System eine genaue Bindung sicherstellt.

Angenommen, auf der Registerkarte **„Bindung“** sind die **Klasse** und **die Containerebene 1** zusammen mit ihren jeweiligen Attributen definiert (siehe Abbildung).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Bindung“.



Das Bindungsverfahren führt die folgenden Schritte aus:

1. Identifizieren des Hosts (Containerebene 1)

   Da der Microsoft IIS-Webserver auf einem Host (in diesem Fall Hardware) ausgeführt wird, sucht das System zuerst den Host, der als **Containerebene 1**definiert ist. Das Namensfeld wird verwendet, um den Host zu identifizieren, und sein Wert wird aus dem Feld **„Knoten“** des Ereignisses übernommen. Mit diesem Namen durchsucht das System die CMDB nach einem übereinstimmenden Host-CI.

2. Identifiziert das CI des Microsoft IIS-Webservers auf dem Host

   Sobald der Host identifiziert wurde, sucht das System unter diesem Host nach einem Microsoft IIS-Webserver-CI mit den folgenden Attributen:

   - name = ci_name
   - sys_class_name = cmdb_ci_microsoft_iis_web_server

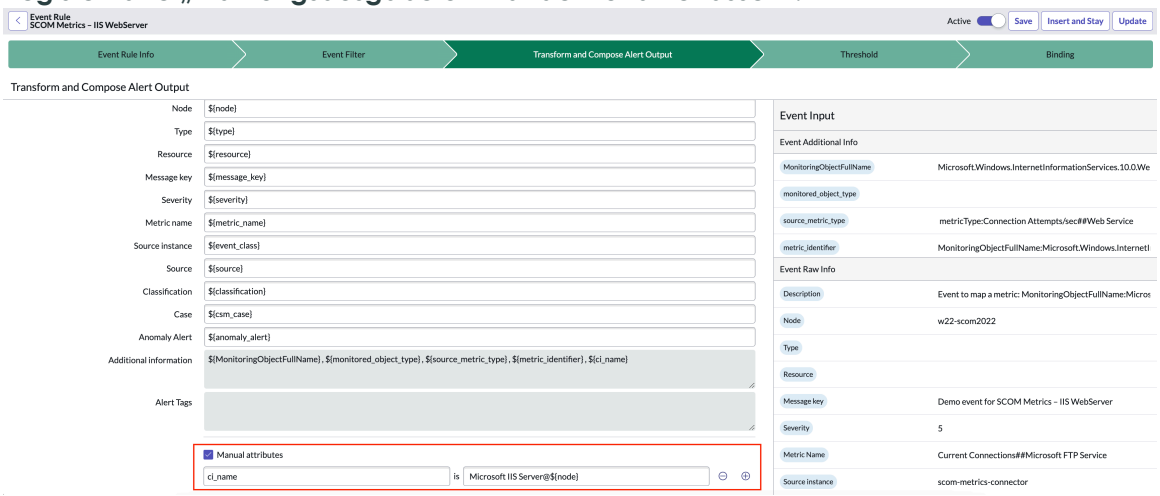
   Hier wird ci_name von dem Schlüssel-Wert-Paar abgeleitet, das auf den Registerkarten **„Transform“ und „Warnungsausgabe“** der Ereignisregel definiert ist. Angenommen, auf der Registerkarte **„Warnungsausgabe umwandeln und verfassen“** der Ereignisregel ist das Kontrollkästchen **Manuelle Attribute** aktiviert und das folgende Schlüssel-Wert-Paar wurde bereits hinzugefügt:

   - **Feldname**: `ci_name`
   - **Feldwert**: `Microsoft IIS Server@${node}`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dadurch wird sichergestellt, dass `ci_name` im Feld **Zusätzliche Informationen** der Warnung angezeigt wird und bei der Konfiguration des Attributfelds der CI-Klasse verwendet wird.

Registerkarte „Warnungsausgabe umwandeln und verfassen“.



Wenn auf dem identifizierten Host ein übereinstimmendes Microsoft IIS-Webserver-CI gefunden wird, wird die Warnung an das richtige Anwendungs-CI und nicht nur an den Host gebunden. Dies gewährleistet eine präzisere Nachverfolgung und Lösung von Incidents, da die Warnung mit dem tatsächlich betroffenen Service verknüpft wird und nicht nur mit dem Computer, auf dem sie ausgeführt wird.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.
2. Wählen Sie **Neu** aus, und füllen Sie die Pflichtfelder der Ereignisregel aus.
3. Wählen Sie die Registerkarte **Bindung**.
4. Aktivieren Sie das Kontrollkästchen **Standardbindung überschreiben**.
5. Wählen Sie im Feld **Bindungstypdie Option CI-Identifizierung**aus.
6. Wählen Sie im Feld **Klasse** eine CI-Klasse aus.
7. **Wählen Sie im Feld Einen Bezeichner auswählen** einen Bezeichner für die Klasse aus.

   Ein Bezeichner für eine Klasse ist ein Satz von Regeln, der dem System hilft, CIs richtig zu erkennen und abzugleichen. Stellen Sie sich dies wie einen Fingerabdruck für jeden CI-Typ vor (z. B. Server, Router oder Anwendung). Der Identifier verwendet Schlüsselattribute – wie Seriennummer, Hostname oder IP-Adresse –, um sicherzustellen, dass eingehende Daten mit dem richtigen CI verknüpft werden, anstatt Duplikate zu erstellen. Weitere Informationen zur CI-Identifizierungsregel finden Sie unter Eine CI-Identifizierungsregel erstellen .

8. Fügen Sie im Feld **„Wert hinzufügen“** den genauen Wert hinzu, oder geben Sie das Quellfeld an, aus dem der Wert für das Feld ausgefüllt werden muss.

   Mit den Symbolen Hinzufügen (⊕) und Löschen (⊖) können Sie Felder hinzufügen oder entfernen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie beim Ausfüllen der CI-Klassenattribute das benötigte Attribut nicht finden, können Sie auf den **Registerkarten „Warnungsausgabe umwandeln und verfassen“** der Ereignisregel verwenden, um das erforderliche Schlüssel-Wert-Paar hinzuzufügen. Weitere Informationen finden Sie unter Event-Regel konfigurieren, um den Warnungsinhalt anzupassen.

Die Transformation und Zusammensetzung der Ereignisregel ist nützlich, wenn relevante Informationen in einem anderen Feld vorhanden sind, aber für die ordnungsgemäße Warnungsverarbeitung extrahiert oder neu zugewiesen werden müssen. Dies ist besonders wichtig, wenn das erforderliche Attribut nicht direkt verfügbar ist und manuell definiert werden muss.

Angenommen, das Feld **Zusätzliche Informationen** einer Warnung enthält den Namen der Warnung im Feld **Knoten**. Für eine korrekte Verarbeitung muss dieser Wert jedoch stattdessen im Feld **Name** angezeigt werden. Da im Ereignis kein Namensattribut vorhanden ist, können Sie manuell eines über die Registerkarten **„Warnungsausgabe umwandeln und verfassen“** in der Ereignisregel erstellen. So geht's:

a. Wählen Sie die Registerkarte **Warnungsausgabe umwandeln und verfassen aus**.

b. Aktivieren Sie die Checkbox **Manuelle Attribute**.

c. Fügen Sie das folgende Schlüssel-Wert-Paar hinzu:

- **Feld**: Name
- **Feldwert**: Knoten

Diese Konfiguration stellt sicher, dass das System den **Knotenwert** extrahiert und dem Namensfeld zuordnet, wodurch er für die CI-Bindung und Warnungskorrelation verfügbar wird.

9. Geben Sie im Bereich *Container level 1* den Host an.
10. Wählen Sie im Feld **Einen Identifier auswählen** einen Identifier für den Container aus.
11. Fügen Sie im Feld **Add value (Wert hinzufügen**) den genauen Wert oder das Feld hinzu, das die Quelle für das Feld **Select an Identifier (Bezeichner auswählen)** des Containers ist.

    Mit den Symbolen Hinzufügen (⊕) und Löschen (⊖) können Sie Felder hinzufügen oder entfernen.
12. Wählen Sie **Speichern**.

Beispiel: Bindung von Warnungen an Nicht-Host-CIs

Binden Sie ein eingehendes Ereignis von einem erkannten Anwendungsservice oder einer erkannten Warnmeldungsgruppe mithilfe einer Ereignisregel und einer Ereignisfeldzuordnung an eine Warnung. In diesem Beispiel wird veranschaulicht, wie dies erreicht wird, indem für jeden Service oder jede Warnmeldungsgruppe eine URL, eine Portnummer oder eine entsprechende IP-Adresse verwendet wird.

Vorbereitungen

Geben Sie die erforderlichen Ereignisfeldwerte an, einschließlich eines eindeutigen Bezeichners für das Nicht-Host-CI.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Führen Sie für Ereignisse, die sich auf ein Nicht-Host-CI beziehen, z. B. Anwendungsservice oder Warnmeldungsgruppe, die folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Lassen Sie das Feld **Knoten** leer.
- Geben Sie den **CI-Typ an,** den Sie in der Ereignisregel binden möchten.
- Stellen Sie sicher, dass das Feld **Zusätzliche Informationen** der Warnung ausreichende Details enthält, um das CI eindeutig zu identifizieren. Der Algorithmus versucht, Attribute in **Zusätzliche Informationen** mit CI-Feldern für diesen Ereignistyp abzugleichen. Wenn eine Übereinstimmung gefunden wird, wird das Ereignis an das CI gebunden.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.
2. Wählen Sie **Neu** aus, und geben Sie die erforderlichen Details für die Ereignisregel ein.
3. Wählen Sie die Registerkarte **Bindung**.
4. Wählen Sie in der Liste **CI-Typ cmdb_ci_service_auto** aus.
5. Fügen Sie im Abschnitt „Ereignis-Übereinstimmungsfelder“ eine neue Zeile mit diesen Werten hinzu:

Feld	Wert
Feld	node
Regulärer Ausdruck	(.*)
Zuordnung	temporärer Knoten

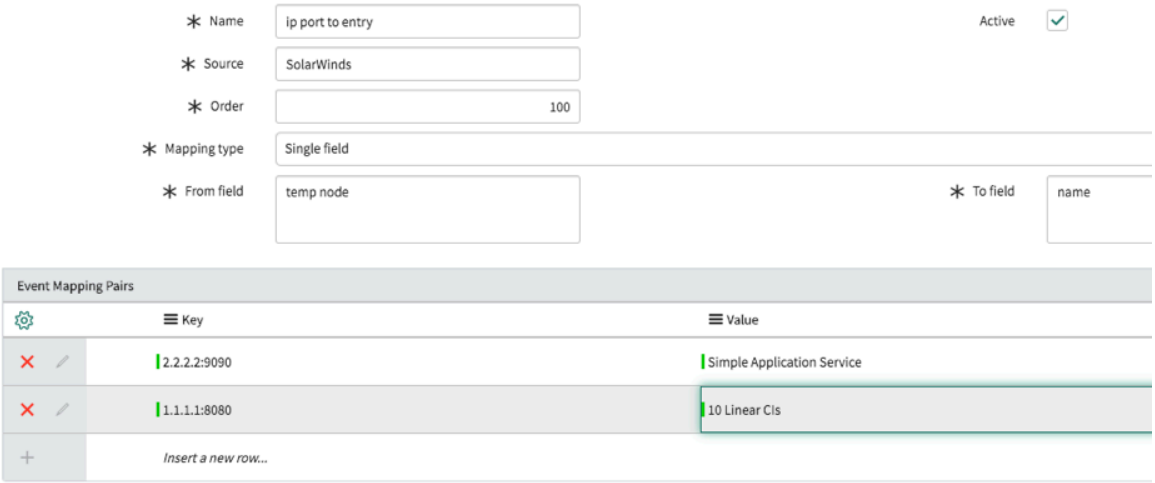
6. Fügen Sie im Abschnitt „Felder zur Ereigniserstellung“ eine neue Zeile mit diesen Werten hinzu:

Feld	Wert
Feld	node
Zusammensetzung	(leer)

7. Wählen Sie **Absenden**.
8. Navigieren zu **Ereignismanagement** > **Regeln** > **Ereignisfeldzuordnung**.
9. Erstellen Sie eine neue Ereignisfeldzuordnung mit diesen Werten:

Feld	Wert
Quelle	Geben Sie die Ereignis-Überwachungssoftware an, die das Ereignis generiert hat.
Zuordnungstyp	Wählen Sie **Einzelfeld** aus.
Feld „Von“	temporärer Knoten
Feld „Bis“	name

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



10. Fügen Sie im Abschnitt „Wertepaare transformieren“ neue Zeilen für jedes Ereigniszuordnungspaar hinzu:
    - Schlüssel: URL oder eine IP-Adresse mit dem entsprechenden Port.
    - Wert: Erkannter Anwendungsservice, technischer Service oder Warnmeldungsgruppenname

    Sie können beispielsweise für jeden Service ein Ereignis-Zuordnungspaar hinzufügen:

Key	Wert
https://service.example.com	Anwendungsservice A
10.0.0.5:8080	Technischer Service B

11. Wählen Sie **Absenden**.

Binden Sie Warnungen an Anwendungsprozess-CIs

Erstellen Sie eine Ereignisregel, um Warnungen an das Host-CI und das Prozess-CI zu binden. Durch die Nutzung von Ereignisregel-Transformationen kann ein eingehendes Ereignis von einem Prozess- oder Anwendungs-CI genau einer Warnung zugeordnet werden, wodurch eine bessere Korrelation und eine effektivere Lösung von Incidents sichergestellt werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig bindet das System Warnungen basierend auf vordefinierten CI-Typen. Möglicherweise müssen Sie Warnungen jedoch an einen anwenderdefinierten CI-Typ binden, der nicht in der vordefinierten Liste enthalten ist. Führen Sie in solchen Fällen die folgenden Schritte aus:

1. Definieren Sie eine anwenderdefinierte CI-Zuordnung: Fügen Sie in der Tabelle „Zuordnung von Prozess zu CI-Typ“ [em_binding_process_map] einen Eintrag hinzu, der Ihrem anwenderdefinierten CI-Typ einen vorhandenen CI-Typ zuordnet.
2. Wählen Sie in der Ereignisregel den CI-Typ aus, für den Sie einen anwenderdefinierten CI-Typ definiert haben.
3. Systemsuchverhalten: Wenn die Ereignisregel ausgelöst wird, verarbeitet das System ein Ereignis. Anstatt den in der Ereignisregel angegebenen CI-Typ zu verwenden,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

verweist es auf die Zuordnung in der Tabelle „Zuordnung von Prozess zu CI-Typ“ [em_binding_process_map]. Wenn eine Übereinstimmung gefunden wird, bindet das System das Ereignis an den anwenderdefinierten CI-Typ anstatt an den vordefinierten.

Dieser Ansatz gewährleistet Flexibilität bei der CI-Bindung, sodass Organisationen anwenderdefinierte Gerätetypen nahtlos in den Ereignismanagement-Workflow integrieren können.

Betrachten Sie zur Veranschaulichung ein Szenario, in dem Sie eine Warnung an ein SQL Server-Anwendungs-CI binden möchten, wenn die CPU-Auslastung in „sqlServer.exe“ 90 % überschreitet, anstatt nur eine Bindung an den Host:

- Stellen Sie sicher, dass das Ereignis den Hostnamen enthält.
- Ordnen Sie den Prozessnamen (sqlServer.exe) der Zuordnungsvariablen „sa_process_name“ im Feld „Ereignisübereinstimmung“ zu. Geben Sie in dieser Phase keinen CI-Typ an.
- Verwenden Sie das Modul „Zuordnung von Prozessen zu CI-Typen“, um eine anwenderdefinierte Zuordnung von einem Prozessnamen zu einem Anwendungs-CI zu definieren.
- Bindungsprozess:
  1. Das System identifiziert zuerst den Host.
  2. Anschließend wird anhand der Beziehungen „Wird ausgeführt auf:Wird ausgeführt“ in der Tabelle „cmdb_rel_ci“ geprüft, ob auf diesem Host eine Anwendung ausgeführt wird.
  3. Wenn ein Transformations-CI-Typ definiert ist, sucht das System in der CMDB nach einem Anwendungs-CI.
  4. Wenn alle Attribute vom Typ „additional_info“ mit den CMDB-CI-Feldern übereinstimmen, wird die Warnung an das Anwendungs-CI anstatt an den Host gebunden.

Prozedur

1. Navigieren Sie zu **Alle**, und suchen Sie nach em_binding_process_map.list.
   Die Seite „Zuordnungen von Prozessen zu CI-Typen“ wird geöffnet.
2. Wählen Sie **Neu**.
3. Geben Sie im Feld **Prozess** den Prozessnamen ein.
4. Wählen Sie im Feld **CI-Typ** den CI-Typ aus.
5. Klicken Sie auf **Absenden**.

CIs mithilfe der Event-Feldzuordnung an Warnungen binden

Anstatt separate Event-Regeln für jedes CI zu erstellen, das Sie an eine Warnung binden möchten, können Sie die Event-Feldzuordnung verwenden, um eine Warnung an mehrere Event-CIs zu binden.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisfeldzuordnung**.
2. Füllen Sie auf der Seite **Event-Feldzuordnung** die Felder wie folgt aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular Event-Feldzuordnung

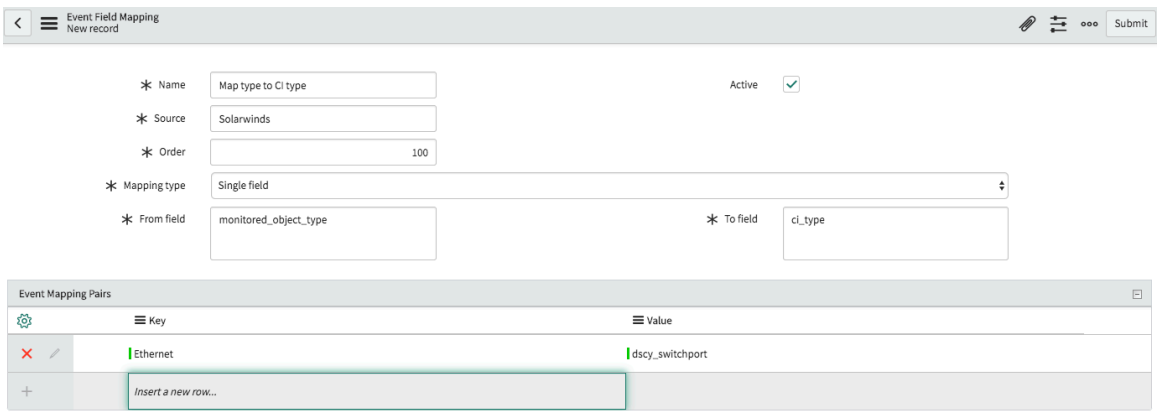
Feld	Beschreibung
Name	Name der Event-Feldzuordnung.
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
Reihenfolge	Zahl zur Festlegung der Reihenfolge, in der diese Aktion verarbeitet werden soll. Aktionen mit niedrigeren Nummern werden zuerst verarbeitet.
Zuordnungstyp	Wählen Sie **Einzelfeld** aus.
Von-Feld	Der Feldname des zu ersetzenden Werts, entweder aus dem Event-Feld des **Events** oder dem Feld **Zusätzliche Informationen**.
An-Feld	Geben Sie **ci_type** ein.
Aktiv	Auswählen, um die Event-Feldzuordnung zu aktivieren.

3. Fügen Sie im Abschnitt **„Wertepaare transformieren“** Folgendes ein:

Abschnitt „Wertepaare transformieren“.

Feld	Beschreibung
Schlüssel	Die Werte des Feldes angegeben im Feld **Von Feld**. Geben Sie für jeden Wert einen eigenen Eintrag ein.
Wert	Der CI-Typ, an den Sie die Warnung binden möchten.

Example:
Es folgt ein Beispiel für eine Event-Feldzuordnung, die den Wert des **Ethernet**-Felds in einer Warnung an das CI **dscy_switchport** bindet:



Zugehörige Informationen

Event-Feldzuordnungen erstellen

Muster für die Event-Gruppenerstellung anzeigen

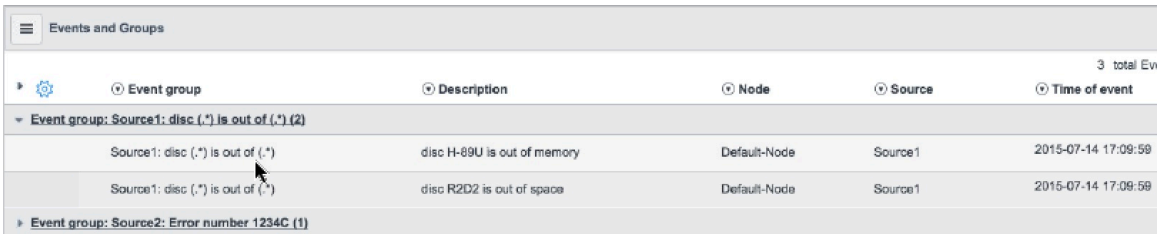
Event-Gruppen sind Event-Sätze, die keine übereinstimmende Event-Regel haben. Sie können die Muster in einer Gruppe von Events anzeigen, um die Auswirkungen der Erstellung einer Regel basierend auf der Event-Quelle und den Beschreibungsmustern zu erfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird
Events werden entsprechend ihrer Quelle und Beschreibung gruppiert.

Prozedur
1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln**.
2. Warten Sie, bis die Gruppenberechnung abgeschlossen ist, und klicken Sie dann auf den erstellten Link.
   Wenn nicht genügend Ereignisse vorhanden sind, erstellt die Berechnung keine Gruppen.
3. Wählen Sie in der Liste der Ereignisse ein Ereignis aus.
4. Um das Muster eines Events zu ändern, doppelklicken Sie auf das Muster, nehmen Sie die gewünschten Änderungen vor, und klicken Sie dann auf **Aktualisieren**.



Ereignisregeln aktualisieren

Aktualisieren Sie Ereignisregeln manuell, um aktuelle Ereignisinformationen widerzuspiegeln, da nach dem Erstellen einer Ereignisregel die Felder **„Zusätzliche Ereignisinformationen“** und **„Rohinformationen zum Ereignis“** nicht automatisch aktualisiert werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur
1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**.
2. Wählen Sie das Ereignis aus.
3. Wählen Sie **Ereignisregel aktualisieren**aus.
4. Wählen Sie die zu aktualisierenden Ereignisregeln aus.
5. Wählen Sie **Auswahl neu laden aus**.

   Wenn Sie mehrere Ereignisregeln ausgewählt haben, wird das zuletzt ausgewählte Element in der Liste im Ereignisregel-Designer geöffnet.

   Hinweis: Wenn die Ausdrücke des regulären Ausdrucks der aktuellen Ereignisregel nach der Aktualisierung nicht mit dem ausgewählten Ereignis übereinstimmen, schlägt die Aktualisierung fehl, und eine Fehlermeldung wird angezeigt, die die Problemfelder angibt. Dieser Schutz stellt sicher, dass Ihre zuvor definierten regulären Ausdrücke für Ereignisregeln durch die Aktualisierung nicht beschädigt werden.

Suchen Sie nach Regeln, die auf ein Ereignis angewendet werden

Zeigen Sie die Regeln an, die auf ein Ereignis angewendet werden, um zu bestimmen, wie dieses Ereignis verarbeitet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Prozedur

1. Navigieren zu **Ereignismanagement** > **Alle Ereignisse**, und klicken Sie dann auf eine Ereignisnummer.
2. Klicken Sie unter **Zugehörige Links** auf **Übereinstimmungsregeln finden**.
3. Überprüfen Sie die Informationen, die im blauen Feld oben auf der Seite angezeigt werden, und prüfen Sie alle **Verarbeitungsnotizen,** um Regeln zu finden, die für ein Ereignis gelten.

Zugehörige Informationen

Events anzeigen

Ereignisverarbeitung simulieren

Sie können die Ereignisverarbeitungslogik für Ereignisse simulieren und die resultierende Warnung anzeigen, um besser zu verstehen, welche Regeln für ein bestimmtes Ereignis ausgeführt werden und wie sich die Ereignisfelder ändern, nachdem die Regel ausgeführt wurde.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**.
2. Öffnen Sie das Ereignis, das Sie simulieren möchten.
3. Wählen Sie im Abschnitt **„Zugehörige Links“Ereignisverarbeitung simulieren.**
4. Wählen Sie in der Infomeldung, die oben auf dem Bildschirm angezeigt wird, den Link zur erstellten simulierten Warnung.
5. Wahlweise: Zeigen Sie an, welche Ereignisregeln und Ereignisfeldzuordnungsregeln angewendet wurden, sowie die Ereignisfeldwerte, indem Sie die Registerkarte **Aktivitäten** auswählen.

Konfiguration der Event-Feldzuordnung

Verwenden Sie Zuordnungsregeln für Event-Felder, um Werte aus bestimmten Feldern Werten in anderen Feldern zuzuordnen.

Ereignismanagement speichert Event-Feldzuordnungen in der Tabelle Event-Feldzuordnung [em_mapping_rule]. Die Zuordnungen gelten nach der Verarbeitung der Event-Regel und vor der Warnungsgenerierung. Die Zuordnungswerte aus der Tabelle Event-Zuordnungspaar [em_mapping_pair] gelten für die Warnung. Der ursprüngliche Schweregrad des Events bleibt unverändert.

Beispiel: Wenn Ereignisse mit dem Feld „**org_severity**“ mit den Werten „*Low*, *Medium*, *High*“ kommen und der **Schweregrad** der Warnung diesen Wert enthalten soll, erstellen Sie eine Ereignisfeldzuordnungsregel, die das Feld **org_severity** dem **Schweregrad**zuordnet. mit diesen Werten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für org_severity, das dem Schweregrad zugeordnet ist

Ursprünglicher Wert für org_severity	Wird dem Warnungs-Schweregradwert zugeordnet
Niedrig	Warnung
Mittel	Schwerwiegend
Hoch	Kritisch

Standardmäßige Event-Feldzuordnungen

Ereignismanagement bietet Standard-Event-Feldzuordnungen für häufig verwendete Systemüberwachungstools. Die Transformationswertpaare aus Ereignisfeldzuordnungen formatieren die eingehenden Ereignisdaten für Ereignismanagement.

Sie können die standardmäßigen Ereignis-Feldzuordnungen und Zuordnungspaare anzeigen, indem Sie zu navigieren **Ereignismanagement** > **Regeln** > **Ereignisfeldzuordnungen** und doppelklicken auf **Name**.

Event-Feldzuordnungen erstellen

Verwenden Sie Ereignisfeldzuordnungen, um Werte aus bestimmten Ereignisfeldern Werten in anderen Feldern zuzuordnen und dadurch umfassendere Informationen in einer Warnung bereitzustellen. Verwenden Sie teambasierte Integrationen in Ereignisregeln, um sicherzustellen, dass der Besitz des Connectors und die Ausführung von Regeln Vorrang vor globalen Regeln haben. Teams können Konsistenz und Hierarchie aufrechterhalten und gleichzeitig Flexibilität und Anpassungsoptionen bieten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie die Regel, um das Event anhand seiner Klasse und der ursprünglichen Werte abzugleichen. Geben Sie außerdem die neuen Werte an, um die ursprünglichen Werte im Ereignis zu ersetzen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisfeldzuordnung**.
2. Wählen Sie **Neu**, oder öffnen Sie eine vorhandene Regel, um sie zu bearbeiten und die Felder auszufüllen.

Ereignisfeldzuordnung

Formular Event-Feldzuordnung

Feld	Beschreibung
Name	Name der Event-Feldzuordnung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
Auftrag	Zahl zur Festlegung der Reihenfolge, in der diese Aktion verarbeitet werden soll. Aktionen mit niedrigeren Nummern werden zuerst verarbeitet.
Zuweisungsgruppe	Wählen Sie für Teambasierte Integrationen eine Zuweisungsgruppe aus. Wenn in der Ereignis-Feldzuordnungsregel keine Zuweisungsgruppe definiert ist, gilt diese Regel als global. Wenn die Regeln ausgeführt werden, werden zuerst die globalen Regeln ausgeführt und dann die Regeln, die zu der Zuweisungsgruppe gehören, zu der die Quellinstanz des Ereignisses gehört.
Zuordnungstyp	Zuordnungsmechanismus, der zum Ändern eines Event-Feldwerts verwendet wird. ◦ **Feld zuordnen und Wert transformieren (Einzelfeld)**: Ordnet den Wert **des Felds „Quelle“** dem entsprechenden Wert in der Tabelle Wertepaare transformieren [em_mapping_pair] zu und füllts das **Zielfeld**aus. Quell- und Zielfelder können Ereignisfelder, Felder für zusätzliche Informationen oder Warnungs-Tags sein. ◦ **Feld erstellen oder aktualisieren und konstanten Wert festlegen (Konstante)**: Legt einen konstanten Wert auf ein **Zielfeld**fest. Das **Feld „Ziel“** kann ein Ereignisfeld, ein Feld für zusätzliche Informationen oder ein Warnungs-Tag sein. ◦ **Feld zuordnen (Feld kopieren)**: Kopiert den genauen Wert eines Quellfelds in das angegebene Zielfeld. Die Felder Quelle und Ziel können das Feld E, das Feld „Zusätzliche Informationen“ oder Warnungs-Tags sein. ◦ **Feld zuordnen und Wert mit regulärem Ausdruck transformieren**: Ordnet den Wert aus dem Feld „Quelle“ generisch dem übereinstimmenden Wert in der Tabelle „Wertepaare transformieren“ zu und füllt das **Feld „Ziel“**aus. Quell- und Zielfelder können Ereignis-, Zusatzinformations- oder Warnungs-Tag-Felder sein. ◦ **Feld mit regulärem Ausdruck zuordnen**: Kopiert den Wert aus einem generisch definierten **Quellfeld** in das **Zielfeld**. Das Feld „Quelle“ muss ein Feld aus dem Feld „Zusätzliche Informationen zum Ereignis“ sein. Das Feld Ziel kann das Feld des Ereignisses, der zusätzlichen Informationen oder des Warnungs-Tags sein. Mit diesem Typ können Sie den Namen des Felds „Quelle“ generisch finden, indem Sie einen regulären Ausdruck (regulären Ausdruck) verwenden. ◦ **Feld zuordnen und Wert aus regulärer Ausdrucksgruppe kopieren**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Kopiert einen Teil des Feldwerts „Quelle“ in das Feld „Ziel“. Quell- und Zielfelder können Ereignisfelder, Felder für zusätzliche Informationen oder Warnungs-Tags sein. Definieren Sie einen regulären Ausdruck, um anzugeben, welcher Teil des **Felds „Quelle“** kopiert werden soll. ◦ **Erweiterte Zuordnung mit Skript**: Implementieren Sie Ihre eigene Logik für die Transformationvon Ereigniswerten mithilfe eines Skripts. Wenn das Kontrollkästchen „Nach Bindung ausführen“ aktiviert ist, wird die Regel nach der CI-Bindungsphase ausgeführt und verwendet das dedizierte Skript, dessen Eingabeparameter auch die sys_id des CI enthalten. **Warnung:** Komplexe Skripts können die Leistung der Ereignisverarbeitung beeinträchtigen. ◦ **Feld aus Referenztabelle zuordnen** Verwenden Sie diesen Regeltyp, um einen **Quellfeldwert** aus der ausgewählten **Referenztabelle** zu extrahieren, indem Sie den Wert des **abzugleichenden Felds**mit dem Wert des **Felds „Übereinstimmende Warnung“** abgleichen und dann den Wert **des Quellfelds** dem **Zielfeld**zuordnen. Das **Feld „Übereinstimmende Warnung“** und das **Feld „Ziel“** können Ereignisfelder, Felder für zusätzliche Informationen oder Warnungs-Tags sein.
Filter	Eine Bedingung für die Ereignisfeldzuordnung. Wählen Sie **Filterbedingung hinzufügen** oder **„ODER“-Klausel hinzufügen** aus, um mehrere Bedingungen zu konfigurieren.
Aktiv	Aktiviert oder deaktiviert die Ereignisfeldzuordnung. Wenn möglich, suchen Sie nach einer anderen Event-Feldzuordnungsregel, und wenden Sie diese an.
Nach Bindung ausführen	◦ Wenn diese Option ausgewählt ist, wird die Regel nach der CI-Bindungsphase ausgeführt. ◦ Verwenden Sie das relevante Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **alert_cmdb_ci** um ein Feld aus dem CI-Datensatz abzurufen. Beispiel: Verwenden Sie „alert_cmdb_ci.assignment_group“, um das Feld „assignment_group“ einer Warnung mit dem Wert der Zuweisungsgruppe des CI auszufüllen (und umzuwandeln). Ein Dot-Walking zu einem zugehörigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Datensatz ist ebenfalls möglich. Verwenden Sie beispielsweise alert_cmdb_ci.asset.model ▪ **alert_cmdb_ci_key** um einen Wert aus der Tabelle „CMDB-Tags“ abzurufen. Beispiel: alert_cmdb_ci_key.subscription notes. **Warnung**: Die Verwendung der Funktion „Nach Bindung ausführen“ kann die Leistung der Ereignisverarbeitung beeinträchtigen. **Hinweis:** Dieses Kontrollkästchen wird nur für die folgenden Zuordnungstypen angezeigt: **Feld zuordnen und Wert transformieren (Einzelfeld)**, **Feld zuordnen (Feld kopieren)**, **Feld zuordnen und Wert mit regulärem Ausdruck transformieren**, **Feld zuordnen und Wert aus regulärer Ausdrucksgruppe kopieren**und **Feld zuordnen aus Referenztabelle**.

◦ Wenn Sie **Feld zuordnen und Wert transformieren (Einzelfeld)**ausgewählt haben, füllen Sie die Felder entsprechend aus.

Zuordnungsfeld und Transformationswertfelder (Einzelfeld).

Feld	Beschreibung
Quellenfeld	Zuzuordnendes Ereignisfeld – enthält alle Felder für Ereignis und zusätzliche Informationen. Hinweis: Für Felder mit zusätzlichen Informationen verwenden Sie: „additional_info“.<field name> ". Wenn das Kontrollkästchen „Nach Bindung ausführen“ aktiviert ist, können Sie die Präfixe „ **alert_cmdb_ci“** und „ **alert_cmdb_ci_key“** verwenden, um CI-bezogene Daten zu empfangen.
Zielfeld	Event-Feld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Wenn dieses Feld mit dem **Feld Quelle**identisch ist, aktualisiert die Zuordnungsregel den Wert im Speicher des Ereignisfelds. Warnungs-Tags können auch mit dem Präfix <t_> definiert werden.
Nach Bindung ausführen	▪ Wenn diese Option aktiviert ist, wird die Ereignisfeldzuordnung nach der CI-Bindung aktiviert. ▪ Verwenden Sie das folgende Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **alert_cmdb_ci** um ein Feld aus dem CI-Datensatz abzurufen. Verwenden Sie beispielsweise „alert_cmdb_ci.assignment_group“, um das Feld „assignment_group“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	einer Warnung mit dem Wert der Zuweisungsgruppe des CI auszufüllen (und zu transformieren). Ein Dot-Walking zu einem zugehörigen Datensatz ist ebenfalls möglich. Verwenden Sie beispielsweise alert_cmdb_ci.asset.model ▪ **alert_cmdb_ci_key** um einen Wert aus der Tabelle „CMDB-Tags“ abzurufen. Beispiel: alert_cmdb_ci_key.subscription notes. **Warnung**: Die Verwendung der Funktion „Nach Bindung ausführen“ kann die Leistung der Ereignisverarbeitung beeinträchtigen.

Schlüsselfelder (Abschnitt „Wertepaare transformieren“)

Feld	Beschreibung
Key	Wert, nach dem von der Zuordnungsregel gesucht wird. Immer wenn das Ereignisfeld diesen Wert enthält, addiert die Zuordnungsregel den im Feld **Quelle** aufgeführten Wert zu dem im Feld **Ziel**aufgeführten Feld. Dieses Feld wird angezeigt, wenn der **Zuordnungstyp „Zuordnungsfeld“ ist und der Transformationswert (Einzelfeld) festgelegt ist**. Wählen Sie nach Bedarf **+** aus, um weitere **Schlüssel** -Felder hinzuzufügen.

Typischer Anwendungsfall: So konfigurieren Sie Folgendes, um das Feld „event_severity“ im Feld „Zusätzliche Informationen“ mit möglichen Werten [z. B. WARNUNG, MINOR, KRITISCH, CLEAR, MAJOR] dem Schweregradfeld zuzuordnen:

- Quellfeld: „event_severity“
- Zielfeld: „severity“
- Wertepaare transformieren:
  - Von Wert „WARNUNG“ bis Wert „4“
  - Von Wert „MINOR“ bis Wert „3“
  - usw.

◦ Wenn Sie **Feld erstellen oder aktualisieren und einen konstanten Wert (Konstante) festgelegt haben**, füllen Sie die Felder entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder erstellen oder aktualisieren und Felder für konstante Werte festlegen (Konstante).

Feld	Beschreibung
Zielfeld	Das **Feld „Ziel“** kann ein Ereignisfeld, ein Feld für zusätzliche Informationen oder ein Warnungs-Tag sein. Typischer Anwendungsfall: Legen Sie für alle Ereignisse, die dem Filter entsprechen, den Warnungsschweregrad auf 1 fest.
Wert	Wert zur Verwendung für das **An-Feld**. Dieses Feld wird angezeigt, wenn der **ZuordnungstypKonstante**ist.

Typischer Anwendungsfall: Legen Sie für alle Ereignisse, die dem Filter entsprechen, den Warnungsschweregrad auf 1 fest.

◦ Wenn Sie **Feld zuordnen (Feld kopieren)**ausgewählt haben, füllen Sie die Felder entsprechend aus.

Feld zuordnen (Feld kopieren) Felder

Feld	Beschreibung
Quellenfeld	**Quellfeldwert**, der in das Feld **Zielfeld** kopiert werden soll. Das **Feld Quelle** kann ein Ereignisfeld, ein Feld für zusätzliche Informationen oder ein Warnungs-Tag sein.
Zielfeld	Ereignisfeld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Das **Feld „Ziel“** kann ein Ereignisfeld, ein Feld für zusätzliche Informationen oder ein Warnungs-Tag sein.
Nach Bindung ausführen	▪ Wenn diese Option aktiviert ist, wird die Ereignisfeldzuordnung nach der CI-Bindung aktiviert. ▪ Verwenden Sie das relevante Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **alert_cmdb_ci** um ein Feld aus dem CI-Datensatz abzurufen. Verwenden Sie beispielsweise „alert_cmdb_ci.assignment_group“, um das Feld „assignment_group“ einer Warnung mit dem Wert der Zuweisungsgruppe des CI auszufüllen (und zu transformieren). Ein Dot-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Walking zu einem zugehörigen Datensatz ist ebenfalls möglich. Verwenden Sie beispielsweise alert_cmdb_ci.asset.model ▪ **alert_cmdb_ci_key** um einen Wert aus der Tabelle „CMDB-Tags“ abzurufen. Beispiel: alert_cmdb_ci_key.subscription notes. **Warnung**: Die Verwendung der Funktion „Nach Bindung ausführen“ kann die Leistung der Ereignisverarbeitung beeinträchtigen.

Typischer Anwendungsfall: Um das IP-Feld aus dem Feld „Zusätzliche Informationen zum Ereignis“ in den Warnungsfeldknoten, zu kopieren, verwenden Sie Folgendes:

- „Quellfeld“: ip
- „Zielfeld“: Knoten

◦ Wenn Sie **Feld zuordnen und Wert mit regulärem Ausdruck transformieren**ausgewählt haben, füllen Sie die Felder entsprechend aus.

Feld zuordnen und Wert mit regulärem Ausdruck transformieren

Feld	Beschreibung
Quellenfeld	Quellfeldwert, der in das Feld **Zielfeld** kopiert werden soll. Das **Feld Quelle** kann ein Ereignisfeld, ein Feld für zusätzliche Informationen oder ein Warnungs-Tag sein.
Zielfeld	Ereignisfeld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Das **Feld „Ziel“** kann ein Ereignisfeld, ein Feld für zusätzliche Informationen oder ein Warnungs-Tag sein.
Nach Bindung ausführen	▪ Wenn diese Option aktiviert ist, wird die Ereignisfeldzuordnung nach der CI-Bindung aktiviert. ▪ Verwenden Sie das relevante Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **alert_cmdb_ci** um ein Feld aus dem CI-Datensatz abzurufen. Verwenden Sie beispielsweise „alert_cmdb_ci.assignment_group“, um das Feld „assignment_group“ einer Warnung mit dem Wert der Zuweisungsgruppe des CI auszufüllen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	(und zu transformieren). Ein Dot-Walking zu einem zugehörigen Datensatz ist ebenfalls möglich. Verwenden Sie beispielsweise alert_cmdb_ci.asset.model ▪ **alert_cmdb_ci_key** um einen Wert aus der Tabelle „CMDB-Tags“ abzurufen. Beispiel: alert_cmdb_ci_key.subscription notes. **Warnung**: Die Verwendung der Funktion „Nach Bindung ausführen“ kann die Leistung der Ereignisverarbeitung beeinträchtigen.

Typischer Anwendungsfall: So ordnen Sie den Schweregrad der Feldfarbe im Feld Zusätzliche Informationen dem Feld Schweregrad zu:

- Quellfeld: „color“
- Zielfeld: „severity“
- Wertepaare transformieren:
  - Von Wert: „.*red“, Zu Wert: „1“. Dies umfasst sowohl „Dunkelrot“, „Hellrot“ als auch andere Werte, die „Rot“ enthalten, und ordnet sie alle „1“ zu.
  - usw.

Schlüsselfelder (Abschnitt „Wertepaare transformieren“)

Feld	Beschreibung
Key	Wert, nach dem von der Zuordnungsregel gesucht wird. Immer wenn das Ereignisfeld diesen Wert enthält, addiert die Zuordnungsregel den im Feld **Quelle** aufgeführten Wert zu dem im Feld **Ziel**aufgeführten Feld. Dieses Feld wird angezeigt, wenn der **Zuordnungstyp „Zuordnungsfeld“ ist und der Transformationswert (Einzelfeld) festgelegt ist**. Wählen Sie nach Bedarf **+** aus, um weitere **Schlüssel** -Felder hinzuzufügen.

◦ Wenn Sie **Feld mit regulärem Ausdruck zuordnen**ausgewählt haben, füllen Sie die Felder entsprechend aus.

Feld mit regulären Ausdrucksfeldern zuordnen

Feld	Beschreibung
Quellenfeld	Generisch definierter Quellfeldwert, der in das **Zielfeld** kopiert werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Das **Feld „Quelle“** muss ein Feld aus dem Feld „Zusätzliche Informationen zum Ereignis“ sein. Mit diesem Typ können Sie den Namen des Felds „Quelle“ generisch finden, indem Sie einen regulären Ausdruck (regulären Ausdruck) verwenden.
Zielfeld	Ereignisfeld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Das **Feld „Ziel“** kann ein Ereignisfeld, ein Feld für zusätzliche Informationen oder ein Warnungs-Tag sein.

Typischer Anwendungsfall: So ordnen Sie das Feld „region“ aus dem Feld „additional_info“ zu, das als „tags.region“ oder „tags|region“ oder „cloud.region“ einem Warnungs-Tag *t_region*, angezeigt wird, und verwenden Sie Folgendes:

- 'Quellfeld': *region
- „Zielfeld“: t_region

◦ Wenn Sie **Feld zuordnen und Wert aus regulärer Ausdrucksgruppe kopieren**ausgewählt haben, füllen Sie die Felder entsprechend aus.

Feld zuordnen und Wert aus regulären Ausdrucksgruppenfeldern kopieren

Feld	Beschreibung
Quellenfeld	Generisch definierter Quellfeldwert, der in das **Zielfeld** kopiert werden soll. Das Feld „Quelle“ muss ein Feld aus dem Feld „Zusätzliche Informationen zum Ereignis“ sein. Mit diesem Typ können Sie den Namen des Felds „Quelle“ generisch finden, indem Sie einen regulären Ausdruck (regulären Ausdruck) verwenden.
Zielfeld	Ereignisfeld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Das **Feld „Ziel“** kann ein Ereignisfeld, ein Feld für zusätzliche Informationen oder ein Warnungs-Tag sein.
Nach Bindung ausführen	▪ Wenn diese Option aktiviert ist, wird die Ereignisfeldzuordnung nach der CI-Bindung aktiviert. ▪ Verwenden Sie das relevante Präfix, um Werte aus dem CI-Datensatz abzurufen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ **alert_cmdb_ci** um ein Feld aus dem CI-Datensatz abzurufen. Verwenden Sie beispielsweise „alert_cmdb_ci.assignment_group“, um das Feld „assignment_group“ einer Warnung mit dem Wert der Zuweisungsgruppe des CI auszufüllen (und zu transformieren). Ein Dot-Walking zu einem zugehörigen Datensatz ist ebenfalls möglich. Verwenden Sie beispielsweise alert_cmdb_ci.asset.model ▪ **alert_cmdb_ci_key** um einen Wert aus der Tabelle „CMDB-Tags“ abzurufen. Beispiel: alert_cmdb_ci_key.subscription notes. **Warnung**: Die Verwendung der Funktion „Nach Bindung ausführen“ kann die Leistung der Ereignisverarbeitung beeinträchtigen.
Gruppenausdruck des regulären Ausdrucks	.*_.*_(.*)_.*

Typischer Anwendungsfall: Um das dritte Oktett aus der IP zu extrahieren und im Feld „Zusätzliche Informationen *third_octet* “ , zu speichern, verwenden Sie:

- „Quellfeld“: ip
- „Zielfeld“: third_octet
- 'Gruppenausdruck des regulären Ausdrucks': .*_.*_(.*)_.*

◦ Wenn Sie **Erweiterte Zuordnung mit Skript**ausgewählt haben, füllen Sie die Felder entsprechend aus.

Erweiterte Zuordnung mit Skriptfeldern

Feld	Beschreibung
Skript	Der Code-Editor bietet Texteditor-Unterstützung für Inline-Skripts. Der Code-Editor verfügt über die folgenden Funktionen für die unterstützten Sprachservices und Inline-Skripts: Syntaxfarbe, Einrückung, Zeilennummerierung und automatische Erstellung von schließenden Klammern und Anführungszeichen, automatische Vorschläge und automatische Vervollständigungen. Bearbeitungstipps:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ Um ein festes Leerzeichen an einer beliebigen Stelle im Code einzufügen, drücken Sie die Taste Tabulator. ▪ Um eine einzelne Codezeile einzurücken, wählen Sie im führenden Leerzeichen der Zeile aus, und drücken Sie die Tabulatortaste. ▪ Um eine oder mehrere Codezeilen einzuziehen, markieren Sie den Code, und drücken Sie die Tabulatortaste. ▪ Um den Einzug zu verringern, drücken Sie Umschalt+Tab. ▪ Um eine Registerkarte am Anfang einer Codezeile zu entfernen, wählen Sie in der Zeile aus, und drücken Sie Umschalt +Tab. ▪ Um Variablen zu deklarieren, verwenden Sie das Schlüsselwort var, damit sie im richtigen JavaScript-Bereich bleiben.
Nach Bindung ausführen	Wenn das Kontrollkästchen „Nach Bindung ausführen“ aktiviert ist, wird die Regel nach der CI-Bindungsphase ausgeführt und verwendet das dedizierte Skript, dessen Eingabeparameter auch die sys_id des CI enthalten. **Warnung:** Komplexe Skripts können die Leistung der Ereignisverarbeitung beeinträchtigen.

◦ Wenn Sie **Feld aus Referenztabelle zuordnen**ausgewählt haben, füllen Sie die Felder entsprechend aus.

Feld aus Referenztabellenfeldern zuordnen

Feld	Beschreibung
Referenztabelle	Die Referenztabelle. Wählen Sie die Tabelle aus, aus der das Feld dem Zielfeld im Ereignis zugeordnet werden soll.
Abzugleichendes Feld	Das Feld aus der Referenztabelle, das mit dem Feld „Übereinstimmende Warnung“ des Ereignisses abgeglichen werden soll. Wird verwendet, um die Datensätze der Referenztabelle herauszufiltern.
Quellenfeld	**Quellfeldwert**, der in das Feld **Zielfeld** kopiert werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Das **Feld Quelle** ist das Feld der Tabelle, die als Referenztabelle ausgewählt wurde.
Übereinstimmendes Warnungsfeld	Ereignisfeld, um übereinstimmende Referenztabellen-Datensätze zu finden. Das **Feld Übereinstimmende Warnung** wird mit dem **Feld Abzugleichendes** Feld abgeglichen. Das Feld Übereinstimmende Warnung kann das Feld Ereignis, das Feld Zusätzliche Informationen oder das Warnungs-Tag sein.
Zielfeld	Ereignisfeld, in dem der Wert von der Zuordnungsregel eingefügt oder aktualisiert wird. Das **Feld „Ziel“** kann ein Ereignisfeld, ein Feld für zusätzliche Informationen oder ein Warnungs-Tag sein.
Nach Bindung ausführen	▪ Wenn diese Option aktiviert ist, wird die Ereignisfeldzuordnung nach der CI-Bindung aktiviert. ▪ Verwenden Sie das relevante Präfix, um Werte aus dem CI-Datensatz abzurufen: ▪ **alert_cmdb_ci** Im **Feld Übereinstimmende Warnung**, um den Wert eines Felds aus einem CI-Datensatz abzurufen. Beispiel: „alert_cmdb_ci.ip_address“ ruft IP-Adressinformationen von gebundenen CIs ab. Wenn das **Feld „Übereinstimmende Warnung“** und das **Feld „Abzugleichende** Felder“ Referenzfelder sind, ist ein Dot-Walking zur sys_id im **Feld „Übereinstimmende Warnung“** erforderlich. Um beispielsweise den Wert „assignment_group“ von gebundenen CIs für den Abgleich mit dem **Feld „Abzugleichendes** Feld“ zu verwenden, geben Sie im **Feld „Übereinstimmende Warnung“**den folgenden Ausdruck ein: alert_cmdb_ci.assignment_group.sys_id ▪ **alert_cmdb_ci_key** um einen Wert aus der Tabelle „CMDB-Tags“ abzurufen. Beispiel: alert_cmdb_ci_key.subscription notes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Warnung: Die Verwendung der Funktion „Nach Bindung ausführen“ kann die Leistung der Ereignisverarbeitung beeinträchtigen.

Typischer Anwendungsfall: Extrahieren Sie „short_description“ aus den „pc_vendor_cat_item“-Datensätzen, die das Feld „name“ mit dem Feld „cat_item_name“ im Feld „Zusätzliche Informationen“ des Ereignisses übereinstimmen, und ordnen Sie es dem Feld „description“ im Ereignis in den folgenden Feldern zu :

- „Referenztabelle“:pc_vendor_cat_item
- „Abzugleichendes Feld“: Name
- „Quellfeld“: short_description
- „Übereinstimmendes Warnungsfeld“:cat_item_name
- „Zielfeld“: Beschreibung

3. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
4. Wählen Sie **Absenden**.

Example:
Die folgenden Werte stellen eine vordefinierte Regel dar, die auf Ereignisse in der Klasse *„From Enterprise 9"* angewendet wird. Wenn die Ereignisse das Element `snmpTrapOID` mit dem Wert `iso.org.dod.internet.private.enterprises.cisco.0.0` enthalten, ändert die Zuordnungsregel den Wert so, dass er in den Warnungen `neu geladen wird`. Wenn die Ereignisse das Element `snmpTrapOID` mit einem Wert von `iso.org.dod.internet.private.enterprises.cisco.0.1` enthalten, ändert die Zuordnungsregel den Wert in den Warnungen in `tcpConnectionClose`.

Feld	Werte
Name	cisco.snmpTrapOID
Quelle	Trap From Enterprise 9
Zuordnungstyp	Feld zuordnen und Wert transformieren (Einzelfeld).
Quellenfeld	snmpTrapOID
Zielfeld	snmpTrapOID
Wertepaare transformieren	• Paar 1 ◦ **Schlüssel**: iso.org.dod.internet.private.enterprises.cisco ◦ **Wert**: reload • Paar 2 ◦ **Schlüssel**: iso.org.dod.internet.private.enterprises.cisco ◦ **Wert**: tcpConnectionClose

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Testen Sie eine Ereignisfeldzuordnung, indem Sie ein Ereignis senden, das ein Feld enthält, das in der Ereignisfeldzuordnung vorhanden ist.

Event-Bezeichner

Event-Felder identifizieren jedes Event eindeutig. Ereignismanagement verwendet diese Informationen, um zu bestimmen, ob eine neue Warnung erstellt oder eine vorhandene aktualisiert werden soll.

- Standardmäßig wird jedes Event durch den **Nachrichtenschlüssel**eindeutig identifiziert.
- Wenn der **Nachrichtenschlüssel** nicht eingetragen ist, werden die Felder **Quelle**, **Typ**, **Knoten**, **Ressource** und **Metrikname** verkettet, um das Feld **Nachrichtenschlüssel** zu füllen.
- Wenn im Event keine Bezeichner angegeben werden, können Sie sie mit Event-Regeln hinzufügen.

Warnungstags

Warnungstags ermöglichen die Konsolidierung für alle normalisierten Felder und verbessern die Administrator-Experience beim Transformieren und Normalisieren von Warnungsfeldern (Schlüssel/Wert). Dies ermöglicht die Wiederverwendung normalisierter Felder in verschiedenen Quellen. Dies verbessert die Warnungsqualität für die Korrelation und bietet zusätzliche Informationen. Box-TBAC-Definitionen (Tag-basierte automatische Korrelation).

Das Feld Warnungs-Tags wird im Warnungsformular angezeigt. Diese Tags werden von Ereignisregeln und in der Ereigniszuordnung erstellt und in der Tabelle der Warnungs-Tags gespeichert. Die zur Erstellung von Schlüssel-Wert-Paaren verwendete Namenskonvention lautet t_<tag name> . Dies ermöglicht die Wiederverwendung von Tags in den Ereignisregeln, indem Anwender die Möglichkeit haben, zuvor definierte Tags auszuwählen. Wenn neue Warnungs-Tags definiert werden, werden automatisch TBAC-Tags (Tag Based Alert Clustering) erstellt. Mit diesen TBAC-Tags können Sie erstellen neue TBAC-Warnungs-Clustering-Definitionen aus der neuen Tag-Quelle.

Event-Feldformat für die Event-Erfassung

Ereignismanagement erfordert, dass alle Events ein Standardformular verwenden, unabhängig davon, wie sie bei der Instanz ankommen.

Geben Sie im Anwendungsnavigationsfilter `em_event.list` ein.

Event-Formular

Name	Beschreibung
em_event.source [Quelle]	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
em_event.node [Knoten]	Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, der/die dem Event zugeordnet ist, z. B. IBM-ASSET. Maximale Länge: 100 Zeichen
em_event_type [Typ]	Optional. Der Metriktyp, auf den sich das Event bezieht, z. B. Datenträger oder CPU, der zur Identifizierung eines Event-Datensatzes verwendet wird, aus dem Warnungen erstellt werden. Maximale Länge: 100 Zeichen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Formular (Fortsetzung)

Name	Beschreibung
em_event.resource [Ressource]	Knotenressource, die für das Event relevant ist. Beispiel: Datenträger C, CPU-1, der Name eines Prozesses oder Services. Maximale Länge: 100 Zeichen
metric_name [Metrikname]	Der Name der Metrik, die gemessen wurde, wie `Freier Speicher DB-Festplatte (MB)`, `Festplatten-Schreibvorgänge/s` oder `Geschriebene Bytes auf Festplatte/s`.
em_event.event_class [Quellinstanz]	Wenn das Feld em_event.node nicht angegeben ist, müssen Warnungen automatisch erstellt werden. Werte für das Feld „em_event.event_class“ stammen entweder von der Quelle, die die Events generiert, oder von der Event-Regel. Name des Computers oder der Software, von dem/der das Event generiert wurde. Beispiel: SolarWinds auf 10.22.33.44. Der entsprechende Feldanzeigename ist **Quellinstanz**.
em_event.message_key [Nachrichtenschlüssel]	Eindeutiger Event-Bezeichner zur Identifizierung mehrerer Events, die sich auf dieselbe Warnung beziehen. Wenn dieser Wert leer ist, wird er aus den Feldwerten **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** generiert. Maximale Länge: 1.024 Zeichen
em_event.ci_type [CI-Typ]	Zeichenfolge, die Informationen zum CI-Typ enthält. Maximale Länge: 100 Zeichen
em_event.severity [Schweregrad]	Optionen für den Event-Schweregrad sind: • **Kritisch**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. • **Schwerwiegend**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten. • **Geringfügig**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. • **Warnung**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. • **OK**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig. • **Löschen**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
em_event.resolution_state [Auflösungsstatus]	Optional. Wenn das Feld leer ist, steht die Auflösung der entsprechenden Warnungen noch aus. Der Event-Status aus der Event-Quelle ist entweder **Neu** oder **Wird geschlossen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Formular (Fortsetzung)

Name	Beschreibung
	• **Neu**, die Lösung für die entsprechenden Warnungen ist offen. • Der Status des **Abschlussereignisses** schließt entsprechende Warnungen.
em_event.time_of_event [Zeit des Events]	Uhrzeit, zu der das Event im Quellsystem aufgetreten ist. Dieses Feld ist ein GlideDateTime-Feld im Format „UTC“ oder „GMT“. Maximale Länge: 40 Zeichen
em_event.state [Status]	Aktueller Verarbeitungsstatus des Events: • **Bereit**: Das Event wurde empfangen und wartet auf die Verarbeitung. • **Verarbeitet**: Das Event wurde erfolgreich verarbeitet. • **Ignoriert**: Dieser Wert wird nicht verwendet. • **Fehler**: Beim Verarbeiten des Events ist ein Fehler aufgetreten. Beispielsweise sind die Methode der Event-Erfassung oder der **Schweregrad** des Events leer.
em_event.alert [Warnung]	Wenn eine Warnung als Ergebnis des Events erstellt wurde, enthält dieses Feld die eindeutige ID, die von Ereignismanagement zur Identifizieren der Warnung generiert wird.
em_event.description [Beschreibung]	Grund für Event-Generierung. Anzeige von zusätzlichen Details zu einem Problem. Beispielsweise ein Serverstapel-Trace oder Details aus einem Überwachungstool. Maximale Länge: 4.000 Zeichen
em_event.additional_info [Zusätzliche Informationen]	Optional. Eine JSON-Zeichenfolge, die weitere Informationen zum Event enthält. Die JSON-Daten werden nur für Zeichenfolgenwerte unterstützt. Andere Werttypen werden nicht unterstützt. Sie müssen Zahlen in Zeichenfolgenwerte konvertieren, indem Sie sie in doppelte Anführungszeichen setzen. Beispielsweise wird dieser Wert nicht unterstützt: {"CPU":100}, während dieser Wert unterstützt wird: {"CPU":"100"}. Ein weiteres Beispiel für eine gültige JSON-Zeichenfolge ist: {"evtComponent":"Microsoft-Windows-WindowsUpdateClient","evtMessage":"Installation Failure: Windows failed. Error 0x80070490"}. Diese Informationen können für die Drittanbieterintegration oder andere Nachwarnungsverarbeitungen verwendet werden. Werte im Feld **Zusätzliche Informationen** eines Events, die nicht im JSON-Schlüssel-/Wert-Format vorliegen, werden auf das JSON-Schlüssel-/Wert-Format normalisiert, wenn das Event verarbeitet wird. Angenommen, der folgende Nur-Text befindet sich im Feld **Zusätzliche Informationen**: "Connection instance is successful" ("Verbindungsinstanz ist erfolgreich"). Wenn das Event verarbeitet wird, wird dieser Nur-Text zu einer JSON-Zeichenfolge und ist in einer Warnung möglicherweise nicht hilfreich. In der resultierenden Warnung steht diese Zeichenfolge im Feld **Zusätzliche Informationen** im JSON-Schlüssel/Wert-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Formular (Fortsetzung)

Name	Beschreibung
	Format, das die Daten enthält: {“additional_content”: “Connection instance is successful"} ({"zusätzlicher_Inhalt": "Verbindungsinstanz ist erfolgreich"}).
processing_notes [Verarbeitungshinweise]	Anzeige des Event-Verarbeitungsprotokolls.

Benutzerdefinierte Warnungsfelder

Sie können benutzerdefinierte Warnungsfelder mit Daten aus dem Feld **Zusätzliche Informationen** des Events befüllen.

Wertvolle Daten, die in den Feldern für **Zusätzliche Informationen** von Events enthalten sind, können beispielsweise für Berichte nützlich sein. Warnungsfelder werden automatisch aus Feldern befüllt, die im Event denselben Namen haben. Dieses Verhalten gilt für die Event-Felder **Zusätzliche Informationen** und für die Felder **Zusätzliche Informationen**, die von der Event-Regel hinzugefügt werden. Verwenden Sie daher den benutzerdefinierten Feldnamen im Feld **Zusätzliche Informationen**, um ein benutzerdefiniertes Warnungsfeld mit dem Wert in den Feldern für **Zusätzliche Informationen** auszufüllen. Sie können zu diesem Zweck auch Event-Regeln verwenden. Werte im Feld **Zusätzliche Informationen** eines Events, die nicht im JSON-Schlüssel-/Wert-Format vorliegen, werden auf das JSON-Format normalisiert, wenn das Event verarbeitet wird.

Das Feld „Kurzbeschreibung“ einer Warnung wird automatisch anhand des Typs, Knotens und der Beschreibung der Warnung geschrieben. Um zu verhindern, dass das Feld „Kurzbeschreibung“ überschrieben wird, öffnen Sie die Tabelle *sys_properties*, suchen die Eigenschaft *evt_mgmt.override_alert_short_description*, ändern den Wert in `false` und klicken dann auf **Aktualisieren**.

Abhängig von den Berechtigungen können Sie möglicherweise nur Felder mit dem Präfix **user**_ erstellen. Wenn dies der Fall ist, erstellen Sie mithilfe der Event-Regeln ein Feld mit **Zusätzlichen Informationen** mit demselben Namen. Um zu verhindern, dass einige Felder in das Warnungsfeld kopiert werden, verwenden Sie die Eigenschaft *evt_mgmt.alert_black_list_fields* und fügen die Feldnamen hinzu, die ausgeschlossen werden müssen. Standardmäßig werden die folgenden Felder nicht kopiert:

- message_key
- category
- additional_info
- sys_updated_on
- sys_updated_by
- sys_created_by
- sys_created_on
- sys_mod_count
- sys_id

Testen und Senden von Ereignissen

Sie können manuell testen und Ereignisse senden, um zu bestätigen, dass Ereignismanagement Ereignisse ordnungsgemäß verwaltet und Warnungen generiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Beispielsweise können Sie Events manuell senden, um:

- zu bestätigen, dass der MID Server eine Event-Connector-Definition und Instanz zum Senden von Events verwendet.
- zu bestätigen, dass Event-Regeln, Event-Feldzuordnungen und andere Konfigurationen Warnungen generieren.
- einen Vorgang oder eine Aktion, der/die kein Event generiert hat, zu verfolgen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Ereignisse**.
2. Klicken Sie auf **Neu**, und füllen Sie anschließend die Felder aus.

Event-Formular

Name	Beschreibung
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
Knoten	Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, der/die dem Event zugeordnet ist, z. B. IBM-ASSET. Maximale Länge: 100 Zeichen
Typ	Der Metriktyp, auf den sich das Event bezieht, z. B. Datenträger oder CPU, der zur Identifizierung eines Event-Datensatzes verwendet wird, aus dem Warnungen erstellt werden. Maximale Länge: 100 Zeichen
Ressource	Eindeutiger Event-Bezeichner zur Identifizierung mehrerer Events, die sich auf dieselbe Warnung beziehen. Wenn dieser Wert leer ist, wird er aus den Feldwerten **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** generiert. Maximale Länge: 1.024 Zeichen
Metrikname	Der Name der Metrik, die gemessen wurde, wie `Freier Speicher DB-Festplatte (MB)`, `Festplatten-Schreibvorgänge/s` oder `Geschriebene Bytes auf Festplatte/s`.
Quellinstanz	Name des Computers oder der Software, von dem/der das Event generiert wurde. Beispiel: SolarWinds auf 10.22.33.44. Der entsprechende Feldanzeigename ist **Quellinstanz**.
Nachrichtenschlüssel	Eindeutiger Event-Bezeichner zur Identifizierung mehrerer Events, die sich auf dieselbe Warnung beziehen. Wenn dieser Wert leer ist, wird er aus den Feldwerten **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** generiert. Maximale Länge: 1.024 Zeichen
Schweregrad	Der Schweregrad des Events. Die Optionen werden normalerweise wie folgt interpretiert: ◦ **Kritisch**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. ◦ **Schwerwiegend**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	◦ **Geringfügig**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. ◦ **Warnung**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. ◦ **Löschen**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen. ◦ **OK**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig.
Auflösungsstatus	Optional. Wenn das Feld leer ist, steht die Auflösung der entsprechenden Warnungen noch aus. Der Event-Status aus der Event-Quelle ist entweder **Neu** oder **Wird geschlossen**. ◦ **Neu**, die Lösung für die entsprechenden Warnungen ist offen. ◦ Der Status des **Abschlussereignisses** schließt entsprechende Warnungen.
Zeit des Events	Uhrzeit, zu der das Event im Quellsystem aufgetreten ist. Dieses Feld ist ein GlideDateTime-Feld im Format „UTC“ oder „GMT“. Maximale Länge: 40 Zeichen
Status	Der aktuelle Verarbeitungsstatus des Events: ◦ **Bereit**: Das Event wurde empfangen und wartet auf die Verarbeitung. ◦ **Verarbeitet**: Das Event wurde erfolgreich verarbeitet. ◦ **Ignoriert**: Dieser Wert wird nicht verwendet. ◦ **Fehler**: Beim Verarbeiten des Events ist ein Fehler aufgetreten. Beispielsweise sind die Methode der Event-Erfassung oder der **Schweregrad** des Events leer.
Warnung	Wenn eine Warnung als Ergebnis des Events erstellt wurde, enthält dieses Feld die eindeutige ID, die von Ereignismanagement zur Identifizieren der Warnung generiert wird.
Beschreibung	Grund für Event-Generierung. Anzeige von zusätzlichen Details zu einem Problem. Beispielsweise ein Serverstapel-Trace oder Details aus einem Überwachungstool. Maximale Länge: 4.000 Zeichen
Zusätzliche Informationen	Eine JSON-Zeichenfolge, die weitere Informationen zum Event enthält. Die JSON-Daten werden nur für Zeichenfolgenwerte unterstützt. Andere Werttypen werden nicht unterstützt. Sie müssen Zahlen in Zeichenfolgenwerte konvertieren, indem Sie sie in doppelte Anführungszeichen setzen. Beispielsweise wird dieser Wert nicht unterstützt: {"CPU":100}, während dieser Wert unterstützt wird: {"CPU":"100"}. Ein weiteres Beispiel für eine gültige JSON-Zeichenfolge ist: {"evtComponent":"Microsoft-Windows-WindowsUpdateClient","evtMessage":"Installation Failure: Windows failed. Error 0x80070490"}. Diese Informationen können für die Drittanbieterintegration oder andere Nachwarnungsverarbeitungen verwendet werden. Werte im Feld **Zusätzliche Informationen** eines Events, die nicht im JSON-Schlüssel-/Wert-Format vorliegen, werden auf das JSON-Schlüssel-/Wert-Format normalisiert, wenn das Event verarbeitet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	wird. Angenommen, der folgende Nur-Text befindet sich im Feld **Zusätzliche Informationen**: "Connection instance is successful" ("Verbindungsinstanz ist erfolgreich"). Wenn das Event verarbeitet wird, wird dieser Nur-Text zu einer JSON-Zeichenfolge und ist in einer Warnung möglicherweise nicht hilfreich. In der resultierenden Warnung steht diese Zeichenfolge im Feld **Zusätzliche Informationen** im JSON-Schlüssel/Wert-Format, das die Daten enthält: {"additional_content": "Connection instance is successful"} ({"zusätzlicher_Inhalt": "Verbindungsinstanz ist erfolgreich"}).

3. Klicken Sie auf **Absenden**.

Event-Verarbeitungsstatistiken anzeigen

Extrahieren Sie Statistiken aus Ihrer Instanz, um sicherzustellen, dass die Leistung nicht beeinträchtigt wird, und extrahieren Sie Metriken im Zusammenhang mit Eventprozessen, um den Status der Eventverarbeitung zu überwachen.

Vorbereitungen

Stellen Sie sicher, dass die Aufgabe *Event Management - Collect xmlstats* aktiv ist. Konfigurieren Sie diese geplante Aufgabe, indem Sie zu navigieren **Systemdefinition** > **Geplante Aufgaben**.

Sie können die Verarbeitung von Event-Statistiken mithilfe dieser Eigenschaften steuern:

- *evt_mgmt.enable_event_processing_stats*. Informationen zur Verwendung dieser Eigenschaft finden Sie unter Verarbeitung von Event-Verarbeitungsstatistiken aktivieren.
- *evt_mgmt.event_processing_stats_period*. Informationen zur Verwendung dieser Eigenschaft finden Sie unter Konfigurieren Sie den Statistikverarbeitungszeitraum.

Erforderliche Rolle: evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Sie können Schlüsselmetriken der Instanz anzeigen, um sicherzustellen, dass die Leistung nicht beeinträchtigt wird, und um den Status der Verarbeitung von Events zu überwachen. Weitere Informationen zum Anzeigen von Statistiken zur Eigensystemüberwachung finden Sie unter Statistiken der Eigensystemüberwachung für Metric Intelligence anzeigen.

Prozedur

1. Führen Sie in einem Browser, in dem die Instanz ausgeführt wird, das XML-Statistikskript aus, indem Sie den folgenden Text an die Instanz-URL anhängen: `xmlstats.do?include=XMLStatsEm`
2. Drücken Sie die **Eingabetaste**.
3. Überwachen Sie die gemeldeten Event-Verarbeitungsmetriken, um sicherzustellen, dass Events gemäß akzeptierten Benchmark-Werten verarbeitet werden.

Ergebnisse

Example: Beispielausgabe nach dem Ausführen des XML-Statistikskripts

```
<xmlstats created="Tue Oct 23 04:01:25 PDT 2018" includes="XMLStatsEm"
 version="2">
<itom_event_management>
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
<event_processing>
<processed count="47" max_process_time="10" mean_process_time="5"
 record_time="2018-10-23 11:00:41"/>
<ready count="7" oldest_ready_event="37" record_time="2018-10-23
 11:00:41"/>
<error count="5" record_time="2018-10-23 11:00:41"/>
<total_created count="5" record_time="2018-10-23 11:00:41"/>
</event_processing>
</itom_event_management>
</xmlstats>
```

Die Metriken zur Event-Verarbeitung im Bericht werden in der folgenden Tabelle beschrieben.

Hinweis: Der Standardverarbeitungszyklus sind Events, die in der letzten Stunde erstellt und in letzter Minute aktualisiert wurden.

Event-Verarbeitungsstatistiken

Metrik	Beschreibung
Event-Verarbeitungsstatistiken	
verarbeitete Anzahl = n	Anzahl der von der Instanz verarbeiteten Events.
max_process_time = n	Längste Zeit, die die Instanz für die Verarbeitung eines Events benötigt.
mean_process_time = n	Durchschnittliche Zeit, die die Instanz zur Verarbeitung der Events in diesem Zyklus benötigt.
Event-fähige Statistiken	
Bereitschaftsanzahl = n	Anzahl der Events, die sich im Status „Bereit“ befinden und zur Verarbeitung verfügbar sind. Der Standardverarbeitungszyklus sind Events, die in der letzten Stunde erstellt und in der letzten Minute aktualisiert wurden.
oldest_ready_event=n	Die längste Zeit, die ein Event benötigt, um im Status „Bereit“ zu bleiben. Wenn diese Metrik einen Wert aufweist, der größer ist als Ihre Benchmarkzahl, untersuchen Sie das Event weiter, um festzustellen, was die Verarbeitung behindert. Der Standardverarbeitungszyklus: Events, die in der letzten Stunde erstellt wurden.
Sonstige Verarbeitungsstatistiken	
Fehleranzahl = n	Anzahl der Events, für die Fehler gemeldet wurden. Der Standardverarbeitungszyklus sind Events, die in der letzten Stunde erstellt und in der letzten Minute aktualisiert wurden.
total_created Anzahl = n	Gesamtanzahl der Events, die während dieses Event-Verarbeitungszyklus verarbeitet wurden. Der Standardverarbeitungszyklus: Events, die in der letzten Stunde erstellt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verarbeitung von Event-Verarbeitungsstatistiken aktivieren

Aktivieren Sie die Verarbeitung von Event-Verarbeitungsstatistiken.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie die Eigenschaft *evt_mgmt.enable_event_processing_stats*, um das XMLStatsEm-Skript zum Ausführen und Sammeln von Statistiken zur Event-Verarbeitung zu aktivieren. Sie können die Ausführung des XMLStatsEm-Skripts deaktivieren, um z. B. ein Leistungsproblem zu beheben.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen Sie nach der Eigenschaft *evt_mgmt.enable_event_processing_stats*.
3. Konfigurieren Sie entweder den Wert einer vorhandenen *evt_mgmt.enable_event_processing_stats*-Eigenschaft, damit das XMLStatsEm-Skript ausgeführt werden kann, oder erstellen Sie eine neue Eigenschaft, wenn sie noch nicht vorhanden ist.
   - Wenn die Eigenschaft vorhanden ist, setzen Sie die Eigenschaft auf **Aktivieren**, um das XMLStatsEm-Skript zum Sammeln von Statistiken zur Event-Verarbeitung zu aktivieren, und klicken Sie auf **Aktualisieren**.
   - Wenn die Eigenschaft nicht vorhanden ist, klicken Sie auf **Neu**, füllen Sie das Formular aus, und klicken Sie auf **Aktualisieren**.

Feld „Systemeigenschaft“

Feld	Beschreibung
Name	Name der Eigenschaft, die Sie erstellen.
Beschreibung	Text, der die Eigenschaft und ihre Funktion beschreibt.
Auswahlmöglichkeiten	Durch Kommas getrennte Werte für eine Auswahlliste. Wenn Sie eine andere Auswahllistenbezeichnung und einen anderen Wert benötigen, verwenden Sie ein Gleichheitszeichen (=), um die Bezeichnung vom Wert zu trennen. Beispiel: Blau = 0000FF, Rot = FF0000, Grün = 00FF00 zeigt Blau, Rot und Grün in der Liste an und speichert den entsprechenden Hex-Wert im Eigenschaftswertfeld.
Typ	Datentyp, der aus einer Liste ausgewählt wird (z. B. Ganzzahl, Zeichenfolge oder true | false).
Wert	Gewünschter Wert für die Eigenschaft. Wenn Sie Eigenschaften mit der Methode *gs.getProperty()* abrufen, behandeln Sie die Ergebnisse als Zeichenfolgen. Beispielsweise gibt eine Wahr|Falsch-Eigenschaft „true“ oder „false“ (Zeichenfolgen) zurück, nicht das boolesche Äquivalent.
Leserollen	Rollen, die über Lesezugriff auf diese Eigenschaft verfügen.
Schreibrollen	Rollen, die über Schreibzugriff auf diese Eigenschaft verfügen.

Zugehörige Informationen

Systemeigenschaft hinzufügen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie den Statistikverarbeitungszeitraum

Legen Sie den Zeitraum (in Sekunden) für die Erfassung von Statistiken zur Event-Verarbeitung fest. Beispielsweise können Sie einen Zeitraum festlegen, der doppelt so lang ist wie der Standardwert von 60 Sekunden, um weitere Statistiken zu erfassen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie die Eigenschaft *evt_mgmt.event_processing_stats_period*, um die XMLStatsEm-Skriptzeit zum Sammeln von Statistiken zur Event-Verarbeitung zu konfigurieren. Legen Sie die Eigenschaftswerte fest, um das Skript über einen längeren oder kürzeren Zeitraum auszuführen. Legen Sie beispielsweise einen kürzeren Zeitraum für die Statistikerfassung fest, damit weniger CPU-Ressourcen verwendet werden.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen Sie nach der Eigenschaft *evt_mgmt.event_processing_stats_period*.
3. Konfigurieren Sie entweder den Wert einer vorhandenen *evt_mgmt.enable_event_processing_stats* Eigenschaft, um das XMLStatsEm-Skript über einen kürzeren oder längeren Zeitraum auszuführen, oder erstellen Sie eine neue Eigenschaft, wenn sie noch nicht vorhanden ist.
   - Wenn die Eigenschaft vorhanden ist, setzen Sie die Eigenschaft auf den erforderlichen Zeitraum fest, um das XMLStatsEm-Skript zum Sammeln von Statistiken zur Event-Verarbeitung zu aktivieren, und klicken Sie auf **Aktualisieren**.
   - Wenn die Eigenschaft nicht vorhanden ist, klicken Sie auf **Neu**, füllen Sie das Formular aus, und klicken Sie auf **Aktualisieren**.

Feld „Systemeigenschaft“

Feld	Beschreibung
Name	Name der Eigenschaft, die Sie erstellen.
Beschreibung	Text, der die Eigenschaft und ihre Funktion beschreibt.
Auswahlmöglichkeiten	Durch Kommas getrennte Werte für eine Auswahlliste. Wenn Sie eine andere Auswahllistenbezeichnung und einen anderen Wert benötigen, verwenden Sie ein Gleichheitszeichen (=), um die Bezeichnung vom Wert zu trennen. Beispiel: Blau = 0000FF, Rot = FF0000, Grün = 00FF00 zeigt Blau, Rot und Grün in der Liste an und speichert den entsprechenden Hex-Wert im Eigenschaftswertfeld.
Typ	Datentyp, der aus einer Liste ausgewählt wird (z. B. Ganzzahl, Zeichenfolge oder true | false).
Wert	Gewünschter Wert für die Eigenschaft. Wenn Sie Eigenschaften mit der Methode *gs.getProperty()* abrufen, behandeln Sie die Ergebnisse als Zeichenfolgen. Beispielsweise gibt eine Wahr|Falsch-Eigenschaft „true“ oder „false“ (Zeichenfolgen) zurück, nicht das boolesche Äquivalent.
Leserollen	Rollen, die über Lesezugriff auf diese Eigenschaft verfügen.
Schreibrollen	Rollen, die über Schreibzugriff auf diese Eigenschaft verfügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Systemeigenschaft hinzufügen

Warnungen verwalten und überwachen

Eine Warnung ist eine Benachrichtigung für ausgewählte Events, die als wichtig eingestuft werden und die der Aufmerksamkeit bedürfen. Ereignismanagement generiert Warnungen basierend auf Event-Regeln.

Die Art und Weise, wie Sie Warnungen überwachen und lösen können, basiert auf den Berechnungen der Warnungsauswirkungen sowie den Konfigurations- und Eigenschafteneinstellungen der Warnungen.

Warnungs-Management

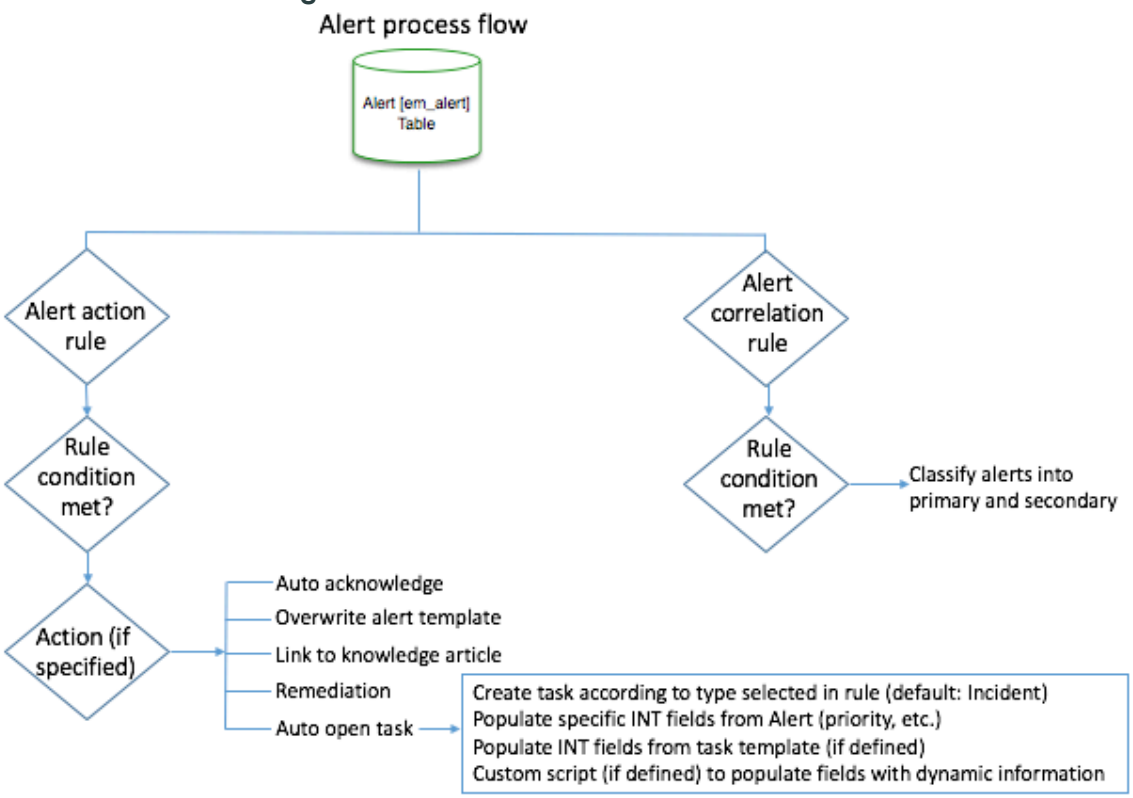
Während Warnungen generiert werden, können Sie weitere Informationen dazu anzeigen, bestätigen und Maßnahmen ergreifen, um sie zu beheben.

Prozess-Flow für Warnungen

Gemäß diesem Prozess-Flow werden Aktionen für Warnungen ausgeführt.

- Ordnen Sie die Warnungsverwaltungsregel einer Warnung zu.
  - Wenn die Quelle des Events mit der in einer vorhandenen Regel angegebenen Quelle übereinstimmt, wird eine Regel abgeglichen. Sie können jede Art von Bedingung für die Quelle der Warnung oder jedes andere Feld und eine Kombination von Feldern definieren.
  - Wenn mehrere Regeln für die gleiche Art von Warnung definiert werden, verwenden Sie die Regel **Reihenfolge**, um die Reihenfolge der Regelanwendung festzulegen.
- Ordnen Sie die Warnungskorrelationsregel einer Warnung zu.

Prozess-Flow für Warnungen



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgaben-/Incident-Felder, die standardmäßig von der Warnung ausgefüllt werden

- `alert.description` wird in `incident.short_description` und `incident.description` kopiert
- `alert.cmdb_ci` wird in `Incident.cmdb_ci` kopiert.
- `alert.severity` wird in `incident.urgency` umgewandelt.

Für automatisch geöffnete Incidents:

- Der `Warnungswert` wird in `incident.contact_type` kopiert.
- Der Wert `sys_user` wird in `Incident.caller_id` kopiert.

Business Rules/Aufgaben, die die Warnungsverarbeitungsaktionen ausführen

Aktion	Name der Business Rule/Aufgabe	Typ
Warnungsvorlage anwenden	Überschreibregel anwenden und validieren	Geschäftsregel
Offener Incident	Event Management – Incidents nach Warnungen erstellen/lösen	Regelmäßige Aufgabe
KB ausfüllen	Event Management – Incidents nach Warnungen erstellen/lösen	Regelmäßige Aufgabe
Bestätigen	Event Management – Incidents nach Warnungen erstellen/lösen	Regelmäßige Aufgabe
Fehlerkorrektur	Automatische Fehlerkorrekturaktionen ausführen	Geschäftsregel
Incident erneut öffnen	Zugehörigen geschlossenen Incident erneut öffnen	Geschäftsregel
Warnung nach geschlossenem Incident schließen	Event Management – Incidents nach Warnungen erstellen/lösen	Regelmäßige Aufgabe
Incident nach geschlossener Warnung schließen	Zugehörigen Incident schließen	Geschäftsregel

Warnungsverwaltungsregeln zum Auflösen von Warnungen

Sie können Ereignismanagement so konfigurieren, dass er automatisch auf Warnungen reagiert. Eine Warnungsverwaltungsregel bestimmt die erforderliche Warnungsantwort, z. B. Öffnen eines Incidents, Erstellen eines Knowledge Base-Artikels, Öffnen einer Aufgabe, Starten einer Korrekturaktion.

Warnungsverwaltungsregeln, die mit Basissystem als Store App (Verwaltung von Warnungsregeln [sn_em_arm]) bereitgestellt werden, um Sie bei der Reaktion auf Warnungen zu unterstützen. Sie können Filter erstellen, um Bedingungen für die Regel anzugeben, sodass die in der Regel angegebene Nachbesserungsaktion nur wirksam wird, wenn die Bedingungen erfüllt sind. Beispiele sind Starten des erforderlichen Subflow oder Öffnen eines Incident auf Grundlage einer Warnung. Der Ausführungsverlauf der Warnung wird automatisch aktualisiert und gibt die aufgerufenen Aktionen an.

Benutzer mit der Rolle „evt_mgmt_admin“ können den Warnungsverwaltungsregel-Designer verwenden, um Warnungsverwaltungsregeln für spezifische Warnungen zu erstellen und anzupassen. Definieren Sie Regeln mit Filtern, um zu bestimmen, für welche

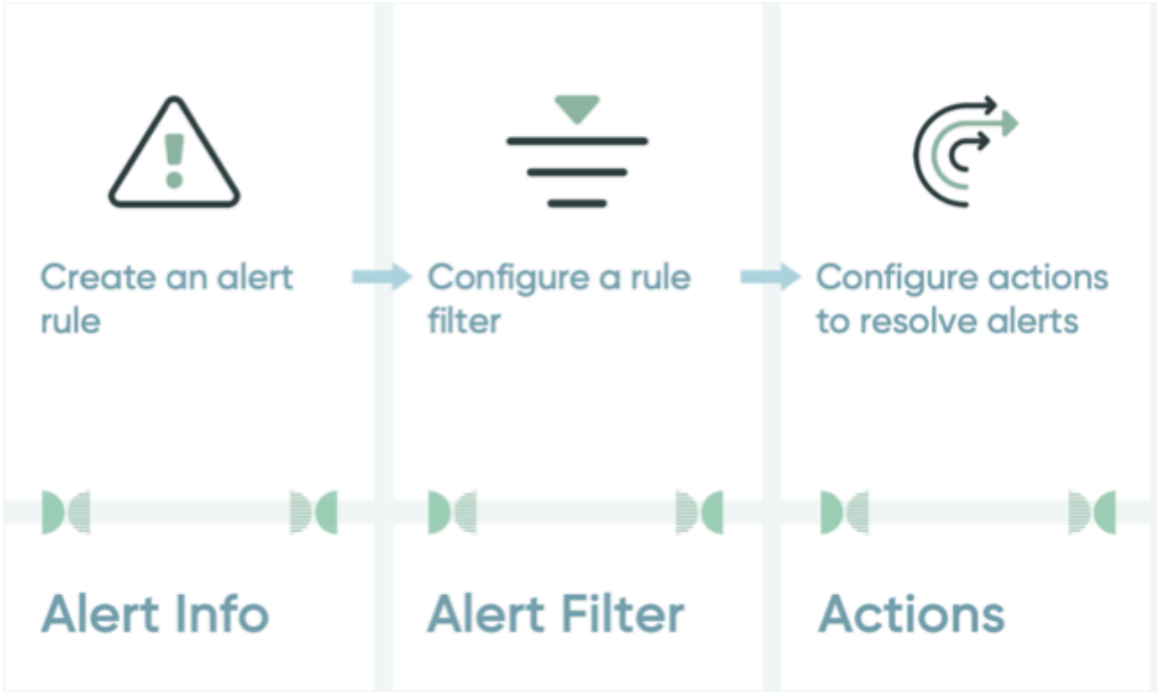
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungen die Regel gilt. Sie können Regeln erstellen, um Anwendungen, URLs, Subflows, Nachbesserungsaktionen oder andere Aktionen auszuführen, z. B. um einen Incident zu öffnen. Weitere Informationen finden Sie unter Warnungsverwaltungsregel erstellen.

Benutzer mit der Rolle „evt_mgmt_operator“ können Warnungsverwaltungsregeln manuell ausführen.

Flow für Warnungsverwaltungsregeln

Der Flow zum Erstellen und Ausführen einer Warnungsverwaltungsregel ist:



Komponenten von Warnungsverwaltungsregeln

Komponente	Beschreibung
Warnungsinformationen	Konfigurieren Sie einen Namen und allgemeine Informationen für die Regel.
Warnungsfilter	Geben Sie einen Filter an, um zu bestimmen, für welche Warnungen die Regel gilt. Sie können die zugehörigen Listenbedingungen angeben.
Aktionen	Geben Sie die Antwort auf die Warnung an, z. B. um einen Subflow auszuführen, eine Fehlerkorrektur durchzuführen, eine Anwendung zu starten oder eine URL in einem Browser zu starten.

Wie Regeln auf aktualisierte Warnungen angewendet werden

Warnungsverwaltungsregeln werden für alle aktualisierten offenen Warnungen ausgeführt. Regeln werden nicht für geschlossene Warnungen ausgeführt, auch wenn sie aktualisiert wurden. Die Filter bestimmen, ob die Aktionen der Regel für die Warnung gelten. Beispiel: Wenn die Bedingung einer Regel angibt, dass eine E-Mail-Nachricht gesendet wird, wenn sich der Schweregrad der Warnung in „Schwerwiegend“ ändert, gilt die Regel für eine Warnung, die durch eine Änderung des Schweregrads von „Warnung“ in „Schwerwiegend“ aktualisiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filter und andere Aktionen verwenden

Filter stellen sicher, dass die Regel nur aufgerufen wird, wenn die konfigurierte Bedingung auftritt, und nicht bei jeder Aktualisierung der Warnung. Sie können beispielsweise eine Regel so konfigurieren, dass Aktualisierungen, die nicht relevant sind (z. B. eine Feldaktualisierung **für Arbeitsnotizen**), die Regel nicht ausführen. Ein weiteres Beispiel ist eine Filterbedingung, die angibt, dass die Warnungsverwaltungsregel nur ausgeführt wird, wenn der Warnungsschweregrad „Kritisch“ lautet.

Sie können die folgenden Aktionen ausführen:

- Geben Sie einen Filter an, um zu bestimmen, für welche Warnungen die Regel gilt.
- Konfigurieren Sie im Abschnitt „Zugehörige Listenbedingungen“ des Formulars zusätzliche Bedingungen, z. B. mit einer *Alert > Parent*-Beziehung, um nach Warnungen zu filtern, die heute empfangen wurden.
- Auf Warnungen reagieren. Erstellen Sie beispielsweise mithilfe von Subflows und Workflows Incidents für primäre Warnungen mit kritischem Schweregrad, oder öffnen Sie eine Suchmaschine in einem Browser, um nach Daten gemäß dem Beschreibungsfeld der Warnung zu suchen.
- Fehlerkorrekturmaßnahmen anwenden. Die Fehlerkorrektur basiert auf Orchestrierungs-Workflows, die zur Ausführung von Fehlerkorrekturmaßnahmen wie dem Erfassen von Systeminformationen oder dem Neustart eines Servers geskriptet werden können.

> **Hinweis:** Um die Leistung von geplanten *Event Management - Evaluate Scoped Alert Rules Management* -Aufgaben zu verbessern, verwenden Sie Subflows anstelle von Workflows.

Geplante Aufgaben, die Warnungsverwaltungsregeln überprüfen

Warnungsverwaltungsregeln werden alle 11 Sekunden durch den standardmäßigen geplanten Auftrag *Event Management - Evaluate Scoped Alert Rules Management0* überprüft. Der Auftrag führt dann die erforderlichen Aktionen aus. Für große Umgebungen können Sie mehr als einen Auftrag hinzufügen. Wenden Sie sich an Kundenservice und Support.

> **Hinweis:** Nur neue Benutzer ab Vancouver erhalten zwei geplante Aufgaben: *Event Management - Evaluate Scoped Alert Rules Management0* und *Event Management - Evaluate Scoped Alert Rules Management1*. Benutzer, die von früheren Familienreleases upgraden, verbleiben bei einer einzigen regelmäßigen Aufgabe *Event Management - Evaluate Scoped Alert Rules Management0*.
>
> Ändern Sie nicht die Eigenschaft *sn_em_arm.alert_management.num_of_jobs*.

Standardmäßig werden der Auftrag zur Gruppierung von Warnungen (**Service Analytics gruppieren Warnungen mit RCA/Warnungszusammenfassung**) und der Auftrag zur Warnungsverwaltung (**Ereignismanagement - Bereichsbezogenes Regel-Management für Warnmeldungen auswerten0**) unabhängig voneinander ausgeführt. Weitere Informationen zum Koordinieren der Warnungsantwort und zur automatisierten Warnungsgruppierung finden Sie unter Warnungsantwort wird mit automatischer Warnungsgruppierung synchronisiert.

Vorhandene Warnungsaktionsregeln migrieren

Vorhandene Warnungsaktionsregeln aus einem früheren Release können zu Warnungsverwaltungsregeln migriert werden. Sie können eine Warnungsaktionsregel nur ändern, nachdem sie zu einer Warnungsverwaltungsregel migriert wurde. Weitere Informationen finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsverwaltungsregel erstellen

Erstellen Sie eine Warnungsverwaltungsregel, um Warnungen nachzuverfolgen und zu lösen, indem Sie die erforderliche Antwort bestimmen, z. B. um einen Incident zu öffnen oder eine Fehlerkorrekturmaßnahme zu starten.

Vorbereitungen

Zum Aktivieren der Fehlerkorrektur mit einem Subflow können Sie einen Subflow verwenden, der mit dem Basissystem verfügbar ist, oder Sie können Ihren eigenen Subflow erstellen. Details finden Sie unter Benutzerdefinierten Subflow erstellen.

Erforderliche Rolle: evt_mgmt_admin, flow_designer

Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie Warnungsverwaltungsregeln zum Nachverfolgen und Beheben von Warnungen.
Während Sie im Warnungsverwaltungsregel-Designer arbeiten, können Sie in mehreren Abschnitten arbeiten, ohne Informationen in einem beliebigen Abschnitt zu verlieren.

Hinweis:

- Warnungsverwaltungsregeln, die nicht für die Ausführung einer Aktion konfiguriert sind, werden übersprungen, und die Regel wird automatisch auf inaktiv festgelegt.
- Wenn eine Warnung durch eine Benutzeraktion (z. B. eine Warnungsverwaltungsregel) an ein CI gebunden ist und sich das CI im Wartungsstatus befindet, müssen Sie das CI manuell an die Warnung binden und es mit dem Status **In Wartung** markieren.

Warnungsverwaltungsregel erstellen, die:

- Nach weiteren Warnungsverwaltungsregeln suchen, die für die ausgewählte Warnung relevant sind.
- Bestimmen, wann die Regel ausgeführt wird.

Warnungsverwaltungsregeln werden nicht unbedingt in der Reihenfolge abgeschlossen, in der sie aufgerufen werden.

Sie können Warnungsverwaltungsregeln so konfigurieren, dass sie:

- Automatisch Incidents, Aufgaben oder Wissensartikel generieren und mit Warnungen verknüpfen
- Automatisch Fehlerkorrektur-Workflows anwenden oder Benutzern ermöglichen, Fehlerkorrekturmaßnahmen manuell vorzunehmen
- Automatisch eine URL entsprechend dem Wert der in der Warnung angegebenen Felder generieren

Zu Ihrer Unterstützung stellt das Basissystem mehrere Warnungsverwaltungsregeln bereit. Sie können sie wie dargestellt verwenden oder als Beispiele verwenden, um benutzerdefinierte Warnungsverwaltungsregeln zu erstellen.

Mit dem Basissystem bereitgestellte Warnungsverwaltungsregeln

Regel	Beschreibung	Aktiv
Sensor-Dashboard in PRTG öffnen	Das Sensor-Dashboard in der Applikation „Paessler PRTG Network Monitor“ (PRTG) wird geöffnet.	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dem Basissystem bereitgestellte Warnungsverwaltungsregeln (Fortsetzung)

Regel	Beschreibung	Aktiv
Oracle EM Launch – Zielstatus und Events anzeigen	Starten Sie Oracle Enterprise Manager, um Folgendes anzuzeigen: • Zielstatus • Event für Warnungen von Oracle EM-Quelle	Ja
Drilldown zu OMI	Drilldown zur HP Operations Manager i (OMi)-Anwendung.	Ja
Incident für die primäre kritische Warnung erstellen	Erstellt einen Incident für primäre kritische Warnungen. Der Incident kann automatisch oder manuell erstellt werden.	Nein
Google-Suche nach „Beschreibung“.	Öffnet die Google-Suche in einem Browser, um anhand der Beschreibung, die in der Warnung angezeigt wird, nach Daten zu suchen.	Ja
Incident erstellen	Erstellt einen Incident für alle Warnungen, die sich nicht im Wartungsstatus befinden. Die Regel wird bei selektiver Aktualisierung automatisch ausgeführt.	Nein
Incident manuell erstellen	Erstellt manuell einen Incident für Warnungen, die sich nicht im Wartungsstatus befinden.	Ja
Kandidat für schwerwiegenden Incident erstellen	Erstellt einen Kandidaten für einen schwerwiegenden Incident für alle Warnungen, die sich nicht im Wartungsstatus befinden und keine sekundären Warnungen sind. Ein Kandidat für einen schwerwiegenden Incident kann zu einem schwerwiegenden Incident befördert werden.	Nein
Major Incident erstellen	Erstellt einen schwerwiegenden Incident für alle Warnungen, die sich nicht im Wartungsstatus befinden und keine sekundären Warnungen sind.	Nein

Nach einem Upgrade Ihrer Instanz von Kingston stehen Ihnen die Warnungsaktionsregeln zur Verfügung, die mit dem Kingston Basissystem bereitgestellt wurden. Wenn Sie jedoch eine der Regeln geändert haben, werden die vorgenommenen Änderungen nicht übertragen.

Standardmäßig werden Warnungsverwaltungsregeln 5 Sekunden nach ihrer Aktualisierung ausgeführt. Um den Wert zu ändern, erstellen Sie die Eigenschaft *evt_mgmt.alert_rule_delay* auf der Seite **„Systemeigenschaften“** (**Systemeigenschaften** > **Alle Eigenschaften**) an.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Regeln** > **Warnungsverwaltungsregeln**.
2. Klicken Sie auf **Neu**, und füllen Sie anschließend die Felder aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular Warnungsverwaltungsregel

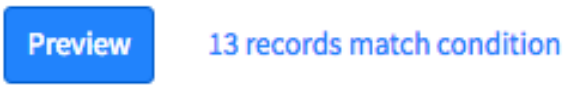
Feld	Beschreibung
Name	Eindeutiger Name für die Regel.
Aktiv	Checkbox zum Aktivieren der Regel. Wenn dieses Kontrollkästchen aktiviert ist, müssen Sie Folgendes angeben: ◦ Im Abschnitt **Warnungsfilter** einen Warnungsfilter ◦ im Abschnitt **Aktionen** mindestens eine dieser Aktionen: ▪ Aktiver Subflow ▪ Workflow ▪ Schnelle Antwort
Reihenfolge	Reihenfolge, in der Regeln ausgewertet werden, wenn mehrere Regeln für dieselbe Warnung definiert sind. Warnungsverwaltungsregeln werden in aufsteigender Reihenfolge ausgewertet. Der Standardwert ist `100`.
Mehrere Warnungsregeln	Anweisung, ob nach zusätzlichen Regeln gesucht werden soll: ◦ **Nach zusätzlichen Regeln suchen**: Führen Sie die aktuelle Regel aus, fahren Sie dann fort, und führen Sie andere übereinstimmende Regeln in der Reihenfolge der Regelpriorität aus, wobei die niedrigere Zahl die höhere Priorität hat. ◦ **Suche nach zusätzlichen Regeln beenden**: Führen Sie nur die aktuelle Regel für die Warnung aus, die dem Filter entspricht. Wenn Sie diese Option auswählen, wird möglicherweise eine Regel ausgeführt, die in einer Regelhierarchie als zweite konfiguriert wird, bevor die Ergebnisse der ersten Regel wirksam werden.
Beschreibung	Beschreibender Text für die Regel

3. Klicken Sie auf **Warnungsfilter** und geben Sie Bedingungen für Warnungen an, auf die diese Regel angewendet wird.

Warnungsfilterphase

Feld	Beschreibung
Regel ist aktiviert, wenn	Die Regel wird ausgeführt, wenn: ◦ **Warnungsänderungen zu Filter**: Änderungen des Inhalts der Warnung bewirken, dass die Warnung dem Filter angepasst wird. Wenn der Filter bei der folgenden Aktualisierung der Warnung abgeglichen wird, wird die Regel nicht angewendet. Wenn die Warnung geschlossen wurde und dann erneut geöffnet wird, wird die Regel beim nächsten Update der Warnung angewendet, und der Filter wird abgeglichen. Danach, wenn die Warnung aktualisiert wird, wird die Regel nicht mehr angewendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ **Warnung entspricht Filter**: der Inhalt der Warnung entspricht dem Filter. Folgend der Aktualisierung der Warnung und wenn der Filter abgeglichen ist, wird die Regel ausgeführt und auf die Warnung angewendet. Die Regel wird für jede übereinstimmende Aktualisierung angewendet.
Warnungsfilter	
Vorschau	Funktion zum Anzeigen einer Vorschau der Warnungen, die der angegebenen Bedingung entsprechen. Ein Hyperlink zeigt an, wie viele Warnungen dem Filter entsprechen.  Wenn Sie auf den Hyperlink klicken, öffnet der Browser eine weitere Registerkarte, die Warnungen in der Tabelle Warnungen [em_alert_list] auflistet. Die Liste zeigt, welche Warnungen der Regel entsprechen, einschließlich geschlossener Warnungen. Warnungen, die bereits von der Regel ausgeführt wurden, werden nicht markiert. Sie können auf eine Warnung klicken, um weitere Details anzuzeigen.
Bedingungen	Bedingungen, die bei Erfüllung den Filter anwenden. Weitere Informationen zum Erstellen von Bedingungen finden Sie unter Bedingungsgenerator verwenden . Zum Hinzufügen einer weiteren Bedingung klicken Sie auf **Neue Kriterien**. **Hinweis:** Die Bedingung **Erstellt am** wird nicht aufgerufen, wenn der Job **Event Management – Warnungsverwaltungsregeln evaluieren** ausgeführt wird. Verwenden Sie stattdessen die Bedingung **Aktualisiert am**, da der Auftrag Warnungen basierend auf dem Zeitpunkt erkennt, zu dem sie aktualisiert wurden, nicht auf dem Zeitpunkt, zu dem sie erstellt wurden.
Zugehörige Listenbedingungen	Bedingungen, um eine Beziehung zu einer anderen Tabelle in den Filter aufzunehmen. **a.** Klicken Sie auf **Tabelle**, und wählen Sie die erforderliche Tabelle aus. **b.** Geben Sie die Bedingungen für diesen Filter an. Weitere Informationen zum Erstellen zugehöriger Listen finden Sie unter Bedingungen für zugehörige Listen hinzufügen .

4. Klicken Sie auf **Aktionen**.
   In diesem Abschnitt können Sie die folgenden Aktionstypen als Antwort auf Warnungen oder zur Behebung von Warnungen konfigurieren:
   - Fehlerkorrektur-Subflows: Führen Sie einen mit dem Basissystem bereitgestellten Subflow aus.
   - Anwendungen starten: Öffnen Sie Anwendungen und Browser, die Sie konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Option „Nachbesserungs-Subflows“ ist veraltet. Verwenden Sie den Flow Designer, um das Auslösen von Flows durch Warnungen zu ermöglichen.

5. Wahlweise: Befolgen Sie im Abschnitt „Nachbesserungs-Subflows“ die folgenden Anweisungen, um Subflows hinzuzufügen:

   a. Doppelklicken Sie unter **Subflow** auf die Zelle.

   b. Klicken Sie auf das Suchsymbol .
   Die Liste der mit dem Basissystem bereitgestellten Subflows wird angezeigt. Weitere Informationen finden Sie unter Ereignismanagement-Subflows im Basissystem.

   c. Wählen Sie in der Subflow-Liste einen Subflow aus.

   d. Wiederholen Sie den Vorgang, und fügen Sie so viele Subflows wie erforderlich hinzu.

(Optional)

   e. Um anzugeben, wann der Subflow ausgeführt werden muss, doppelklicken Sie unter **Ausführung** in die Zelle.

Subflow-Ausführungsoptionen

Name	Beschreibung
Automatisch	Der Subflow wird automatisch ausgeführt, wenn die Regel abgeglichen wird.
Manuell	Subflow bei Bedarf ausführen, wenn die Regel abgeglichen wird.
Beides	Wenn die Regel erfüllt ist, wird der Subflow automatisch ausgeführt, und Sie können den Subflow optional erneut manuell ausführen.

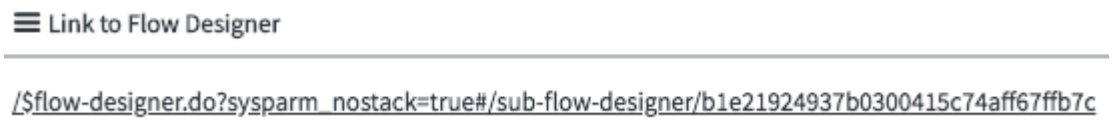
   f. Doppelklicken Sie in die Zelle unter **Grenzwert für automatische Ausführungen**, und geben Sie mit einer ganzen Zahl an, wie oft der Subflow ausgeführt werden soll. Nachdem der Subflow die angegebene Anzahl von Malen ausgeführt wurde, wird er nicht mehr ausgeführt.

   g. Um den auszuführenden Subflow zu aktivieren, doppelklicken Sie in die Zelle unter **Aktiv**, und wählen Sie `true` aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Link in der Zelle unter **Link zum Flow Designer** wird erst angezeigt, nachdem ein Subflow ausgewählt und die Regel gespeichert wurde.



6. Zum Hinzufügen von Anweisungen zum Starten von Anwendungen oder zum Öffnen von Browserfenstern im Bereich „Anwendungen starten“:

   a. Doppelklicken Sie unter **Anzeigenname** auf die Zelle.
   Geben Sie einen Namen für den Link an.

   b. Erstellen Sie im **URL**-Feld die URL anhand der Daten der Warnung im folgenden Format:`http://${source}.com:${port}/${cmdb_ci.name}`
   Das Feld **Aktiv** wird automatisch aktualisiert.

   Jede URL-basierte Aktion kann die Warnungsparameter verwenden, und die URLs können auf Wikis, Messaging-Services, REST APIs usw. verweisen.

7. Klicken Sie auf **Absenden**.

Ergebnisse

Die Warnungsverwaltungsregel wird der Liste der verfügbaren Regeln hinzugefügt, die zum Lösen von Warnungen verwendet werden können.

Zugehörige Informationen

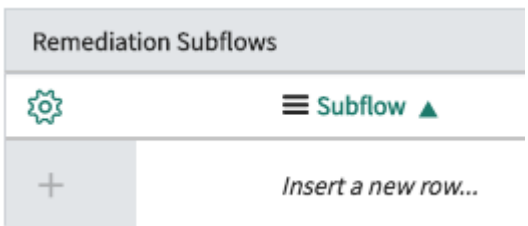
Schnelle Antworten in einer Warnung anwenden

Ereignismanagement-Subflows im Basissystem

Die mit dem Basissystem bereitgestellten Subflows werden im Bereich „Nachbesserungs-Subflows“ der Warnungsverwaltungsregeln angezeigt.

Auf Subflows zugreifen

Navigieren zu **Ereignismanagement** > **Regeln** > **Warnungsverwaltungsregeln** und klicken Sie auf **Neu**. Klicken Sie auf die Registerkarte **Aktionen**. Doppelklicken Sie im Bereich „Nachbesserungs-Subflows“ auf das Feld **Neue Zeile einfügen**.



Klicken Sie auf das Suchsymbol , um Subflows hinzuzufügen. Die Liste der mit dem Basissystem bereitgestellten Subflows wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subflows im Basissystem

Name	Beschreibung
Warnung bestätigen	Subflow, um die Warnung als bestätigt zu markieren. Bestätigen Sie eine Warnung, um anzuzeigen, dass weitere Aufmerksamkeit erforderlich ist.
Wissensartikel anhängen (veraltet)	Subflow zum Anhängen eines Wissensartikels an die Warnung. Dieser Subflow wird für Instanzen bereitgestellt, die aus veralteten Releases (vor dem London-Release) migriert werden. **Hinweis:** Fügen Sie die **Wissensartikelspalte** zur Tabelle „Warnungsverwaltungsregeln“ [em_alert_management_ hinzu und wählen Sie einen Artikel aus, der bei Ausführung der Regel an eine Warnung angehängt werden soll.
Warnung in den Wartungsmodus setzen	Subflow, um den Alarm als in Wartung befindlich zu markieren.
Warnung schließen	Subflow, um die Warnung als geschlossen zu markieren.
Incident erstellen	Subflow zum Erstellen eines Incidents. Felder aus der Warnung werden verwendet, um die übereinstimmenden Felder im erstellten Incident auszufüllen. **Hinweis:** • Wenn ein vorhandener Incident an die Warnung angehängt ist, wird dieser Subflow nicht aktiviert. • Wenn sich die Warnung in Wartung befindet, wird kein Incident erstellt. • Nachdem ein bestimmter Zeitrahmen verstrichen ist, wird der Warnungsverwaltungsauftrag auch dann ausgeführt, wenn der Auftrag zur Warnungsgruppierung nicht abgeschlossen ist. In diesem Fall können Sie durch Aktivieren der Regel *Avoid INTs on secondary alerts* verhindern, dass Incidents für sekundäre Warnungen erstellt werden (dazu muss Eigenschaft *evt_mgmt.avoid_int_enabled* aktiviert sein), da für die primäre Warnung bereits ein Incident vorhanden ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subflows im Basissystem (Fortsetzung)

Name	Beschreibung
Kandidat für schwerwiegenden Incident erstellen	Subflow zum Erstellen eines schwerwiegenden Incidents Felder aus der Warnung werden verwendet, um die übereinstimmenden Felder im erstellten Incident auszufüllen. Ein Kandidat für einen schwerwiegenden Incident kann auf einen schwerwiegenden Incident aktualisiert werden. **Hinweis:** • Wenn ein vorhandener Incident an die Warnung angehängt ist, wird dieser Subflow nicht aktiviert. • Wenn sich die Warnung in Wartung befindet, wird kein Kandidat für schwerwiegenden Incident erstellt. • Wenn die **Rolle in der GruppeSekundär** ist, wird der Kandidat für schwerwiegenden Incident nicht erstellt.
Schwerwiegenden Incident aus Warnung erstellen	Subflow zum Erstellen eines schwerwiegenden Incidents aus einer Warnung Felder aus der Warnung werden verwendet, um die übereinstimmenden Felder im erstellten schwerwiegenden Incident auszufüllen. **Hinweis:** • Wenn ein vorhandener Incident an die Warnung angehängt ist, wird dieser Subflow nicht aktiviert. • Wenn sich die Warnung in Wartung befindet, wird kein Incident erstellt. • Wenn die **Rolle in der GruppeSekundär** ist, wird der Kandidat für schwerwiegenden Incident nicht erstellt.
Schwerwiegenden Incident mit Auswirkung erstellen	Subflow zum Erstellen eines schwerwiegenden Incidents aus einer Warnung, in der auch das Feld **Auswirkung** als Eingabe verwendet wird. Felder aus der Warnung werden verwendet, um die übereinstimmenden Felder im erstellten schwerwiegenden Incident auszufüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subflows im Basissystem (Fortsetzung)

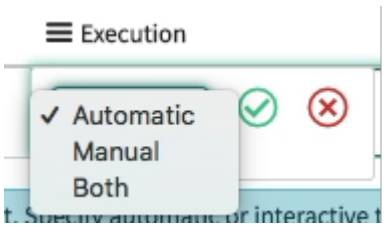
Name	Beschreibung
	Hinweis: • Wenn ein vorhandener Incident an die Warnung angehängt ist, wird dieser Subflow nicht aktiviert. • Wenn sich die Warnung in Wartung befindet, wird kein Incident erstellt. • Wenn die **Rolle in der GruppeSekundär** ist, wird der Kandidat für schwerwiegenden Incident nicht erstellt.
Kandidat für schwerwiegenden Incident mit Auswirkung erstellen	Subflow zum Erstellen eines Kandidaten für schwerwiegenden Incident, in dem auch das Feld **Auswirkung** als Eingabe verwendet wird. Felder aus der Warnung werden verwendet, um die übereinstimmenden Felder im erstellten Incident auszufüllen. Ein Kandidat für einen schwerwiegenden Incident kann auf einen schwerwiegenden Incident aktualisiert werden. **Hinweis:** • Wenn ein vorhandener Incident an die Warnung angehängt ist, wird dieser Subflow nicht aktiviert. • Wenn sich die Warnung in Wartung befindet, wird kein Kandidat für schwerwiegenden Incident erstellt. • Wenn die **Rolle in der GruppeSekundär** ist, wird der Kandidat für schwerwiegenden Incident nicht erstellt.
Aufgabe erstellen (veraltet)	Dieser Subflow verwendet, sofern vorhanden, eine Aufgabenvorlage oder das *EventMgmtCustomIncidentPopulator*Skript für Instanzen, die aus veralteten Releases (vor dem London-Release) migriert werden. Falls konfiguriert, wenden Sie die Aufgabenvorlage an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Subflows im Basissystem (Fortsetzung)

Name	Beschreibung
	Hinweis: Fügen Sie die Spalte **Aufgabenvorlage** zur Tabelle „Warnungsverwaltungsregeln“ [em_alert_management_ hinzu und wählen Sie eine Aufgabenvorlage und eine Aufgabe aus, die bei Ausführung der Regel angewendet werden sollen.
Warnvorlage überschreiben (veraltet)	Dieser Subflow wendet die Alarmvorlage an. Dieser Subflow wird für Instanzen bereitgestellt, die aus veralteten Releases (vor dem London-Release) migriert werden. **Hinweis:** Fügen Sie die Spalte **Aufgabentyp** zur Tabelle „Warnungsverwaltungsregeln“ [em_alert_management_ hinzu und wählen Sie eine Aufgabenvorlage aus, die bei Ausführung der Regel angewendet werden soll.

1. Wählen Sie den von Ihnen benötigten Subflow aus.
2. Informationen zum Anpassen eines Subflows finden Sie unter Benutzerdefinierten Subflow erstellen. Dieses Thema beschreibt auch die Eingabeparameter in einem Subflow.
3. Wenn Sie angeben möchten, wann der Workflow ausgeführt werden muss, doppelklicken Sie auf die Zelle unter **Ausführung**.



.

Benutzerdefinierten Subflow erstellen

Sie können einen Subflow gemäß Ihren Anforderungen erstellen. Anschließend können Sie den benutzerdefinierten Subflow zum Auflösen von Warnungen verwenden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin, flow_designer

Warum und wann dieser Vorgang ausgeführt wird
Kopieren Sie einen vorhandenen Subflow, und passen Sie ihn an. Veröffentlichen Sie den benutzerdefinierten Subflow, damit er zur Lösung von Warnungen verwendet werden kann. Weitere Informationen finden Sie unter Subflow erstellen .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Ihre Instanz ServiceNow Domänentrennung verwendet, müssen Sie sicherstellen, dass der neue benutzerdefinierte Subflow, den Sie erstellt haben, nur auf die Daten der angegebenen Domäne angewendet wird.

Zu Erklärungszwecken wird der Subflow **Incident erstellen** verwendet. Weitere Informationen zum Anpassen eines Subflows finden Sie im Knowledge Base-Artikel KB0722376 .

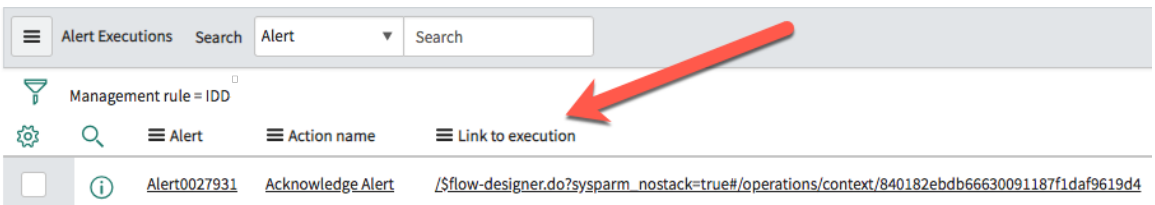
Prozedur

1. Navigieren zu **Alle** > **Prozessautomatisierung** > **Flow Designer**.
2. Klicken Sie im Fenster „Flow Designer“ auf **Subflows**.
3. Klicken Sie auf **Incident erstellen**.
   Der Subflow „Incident erstellen“ wird im Flow Designer im schreibgeschützten Format geöffnet. Die Eingaben im Subflow „Incident erstellen“ werden in der folgenden Tabelle beschrieben.

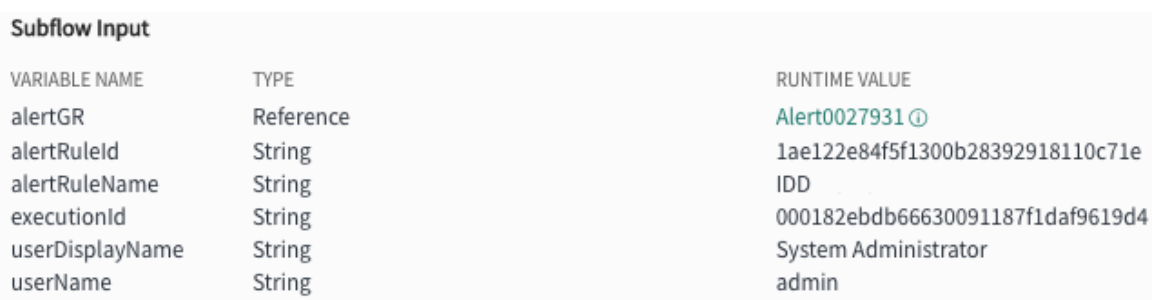
Incident-Eingabeparameter erstellen

Wert	Beschreibung
alertRuleName	Der Name der Warnungsverwaltungsregel, die diesen Subflow angibt, z. B. `IDD`.
alertRuleId	Die sys_id der Warnungsverwaltungsregel, z. B. `1ae122e84f5f1300b28392918110c71e`.
alertGR	Der Warnungsdatensatz, der dem Filter entspricht, der in der Warnungsverwaltungsregel definiert ist, z. B. `Alert0027931`
executionId	Die ID der abzurufenden Ausführung, z. B. `000182ebdb66630091187f1daf9619d4`
userName	Der Name des aktuellen Benutzers, z. B. `Systemadministrator`
userDisplayName	Der Name, den der aktuelle Benutzer zur Anzeige angegeben hat, z. B. `admin`

Beispiel: In einer Warnungsverwaltungsregel, die Warnungen verarbeitet hat, klicken Sie im Bereich „Warnungsausführungen“ auf den **Link zur Ausführung** der erforderlichen Warnung.



Der Flow Designer wird geöffnet. Klicken Sie auf **Subfloweingaben und -ausgaben**. Die Namen der Eingabevariablen des Subflows werden mit ihren jeweiligen Werten angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie im Header des Subflows auf „Weitere Aktionen“ , und wählen Sie **Subflow kopieren**.
5. Im Feld **Neuer Subflow-Name** geben Sie den Namen des neuen Subflows ein.
6. Um den Anwendungsbereich des Subflows zu beschränken, wählen Sie im Feld **Anwendung** die erforderliche Anwendung aus, andernfalls wählen Sie `Global`.
7. Klicken Sie auf **Kopieren**.
   Der neue Subflow wird erstellt und als Registerkarte im Subflow-Designer-Editor geöffnet. Die von der Vorlage bereitgestellten Eingaben werden angezeigt.

   Eingaben sind fest und es kann nichts hinzugefügt werden.

   Im Editor können Sie Subflow-Eingaben oder -Ausgaben je nach Bedarf löschen.
8. Zum Löschen einer Eingabe klicken Sie auf das .
   Eingaben sind fest und es kann nichts hinzugefügt werden.
9. Erstellen Sie Subflow-Ausgaben, indem Sie die Namen und Datentypen definieren.
   a. Klicken Sie auf das , um eine Ausgabe hinzuzufügen.
   b. Definieren Sie den Namen und den Datentyp.
10. Klicken Sie auf **Speichern**, um den Subflow im Entwurfsstatus zu speichern.
11. Um den Subflow zu speichern und zu veröffentlichen, sodass er im Regel-Designer der Warnungsverwaltung verwendet werden kann, klicken Sie auf **Veröffentlichen**.

Ergebnisse

Schließen Sie den geänderten Subflow in eine Warnungsverwaltungsregel ein, um Warnungen gemäß Ihren benutzerdefinierten Anforderungen aufzulösen.

Zugehörige Informationen

Subflows

Informationen zur Warnungsausführung

Warnungsausführungsinformationen bieten einen Verweis auf die durchgeführten Warnungsverwaltungsregelaktionen. Diese Informationen werden nur dann im Datensatz der Warnungsverwaltungsregel angezeigt, wenn eine Warnung dem Filter in der Regel entspricht und eine Aktion ausgeführt wurde. Sie können auf einen beliebigen Link in der Liste Warnungsausführungen klicken, um das referenzierte Element zu öffnen.

Warnungsausführungen

Im Datensatz der Warnungsverwaltungsregel zeigt die Liste „Warnungsausführungen“ wichtige zugehörige Datensätze für die Regel an.

Hinweis: Die Liste „Warnungsausführungen“ im Datensatz „Warnungsverwaltungsregeln“ zeigt Warnungsausführungsinformationen und eine Liste der Warnungsverwaltungsregeln an, mit denen die ausgewählte Warnung übereinstimmt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsausführungsliste

Informationen in der Warnungsausführungsliste

Die Spalten in der Warnungsausführungsliste werden mit Details der Warnungen gefüllt, die der Warnungsverwaltungsregel und den ausgeführten Aktionen entsprechen. Die aufgelisteten Warnungen entsprechen dem Filter der Regel.

Informationen zur Warnungsausführung anzeigen

Sie können auf einen beliebigen Link in der Warnungsausführungsliste klicken, um die Warnungsausführungsinformationen des referenzierten Elements zu öffnen. Diese Informationen werden nur dann im Datensatz der Warnungsverwaltungsregel angezeigt, wenn eine Warnung dem Filter in der Regel entspricht und eine Aktion ausgeführt wurde.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Zu den Informationen in der Warnungsausführungsliste zählen:

- Die Liste der Warnungen, die dem Filter der Regel entsprechen.
- Die Aufgaben, einschließlich Incidents, die geöffnet wurden.
- Welche Nachbesserungs-Workflows und welche Subflows ausgeführt wurden.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Warnungsverwaltungsregeln**.
2. Klicken Sie in der Liste der Warnungsverwaltungsregeln auf die Regel.
   Wenn eine Warnung mit dem Filter in der Regel übereinstimmt und eine Aktion ausgeführt wurde, wird im Datensatz der Warnungsverwaltungsregeln die Liste der Warnungsausführungen angezeigt. Die Liste wird unabhängig von der Phase der ausgewählten Warnungsverwaltungsregel angezeigt.

Warnungsausführungsliste

Spalte	Beschreibung
Warnung	Warnungsnummer der Warnungen, die der Warnungsverwaltungsregel entsprechen
Aktionsname	Name der Aktion, die ausgeführt wurde, um die Warnung zu lösen (Subflow oder Workflow).
Link zur Ausführung	Link zu dem Aktionsausführungsprotokoll, das bei Ausführung der Aktion erstellt wurde.
Zugehörige Aufgabe	Link zu der Aufgabe, die erstellt wurde, als die Warnung gelöst wurde. Beispiel: Wenn die Aktion für eine Regel das Erstellen eines Incidents ist, enthält dieses Feld die Incident-Nummer mit einem Link zum Öffnen des Incidents.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	Es wird ein Link zur Workflow-Nachbesserungsaufgabe bereitgestellt, die zur Überwachung der Nachbesserung erstellt wird.
Log	Hinweis oder Information, die das Ergebnis der Ausführungsaktion anzeigt, z. B. wie die Ausführung erfolgte, „`1 von 2 Ausführungen`“. Wenn die Warnung geschlossen wird, wird die Anzahl der Ausführungen (die erste Zahl) auf 0 zurückgesetzt. Diese Informationen geben nicht an, dass der Subflow erfolgreich ausgeführt wurde, sondern dass der Aufruf des Subflows erfolgreich war und der Subflow ordnungsgemäß konfiguriert ist.
Automatische Ausführung	Angabe, wie die Aktion ausgeführt wurde: automatisch (true) oder manuell (false).
Erstellt	Datum und Uhrzeit der Erstellung des Eintrags.

Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel

Vorhandene Warnungsaktionsregeln aus einem früheren Release können zwar ausgeführt, aber nicht geändert werden. Migrierte Warnungsaktionsregeln werden zu Warnungsverwaltungsregeln, und alle Definitionen der Warnungsaktionsregeln werden in das Warnungsverwaltungsregelformat migriert. Migrierte Regeln können geändert werden.

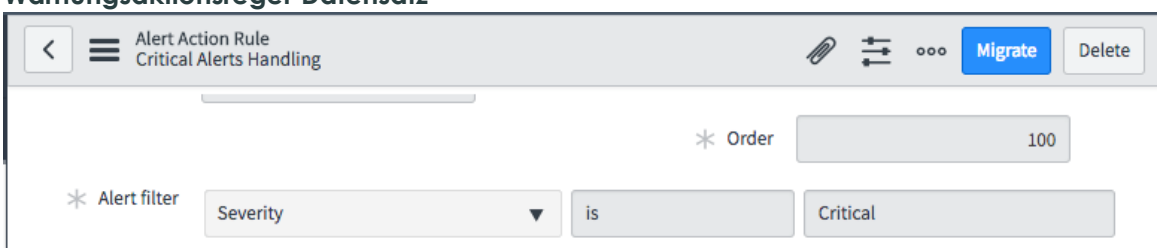
Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Vorhandene Warnungsaktionsregeln sind aktive, schreibgeschützte Regeln. Eine Warnungsaktionsregel kann nur geändert werden, nachdem sie in eine Warnungsverwaltungsregel migriert wurde.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Warnungsaktionsregeln**.
2. Wählen Sie eine Warnungsaktionsregel zum Migrieren oder Löschen aus.

Warnungsaktionsregel-Datensatz



3. Klicken Sie auf **Migrieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie auf **Migrieren**geklickt haben, finden Sie die Liste der migrierten Regeln zusammen mit den neuen Warnungsverwaltungsregeln, indem Sie zu navigieren **Ereignismanagement** > **Regeln** > **Warnungs-Management**.

Nach einer erfolgreichen Migration werden alle Definitionen der Warnungsaktionsregeln in das Warnungsverwaltungsregelformat migriert.

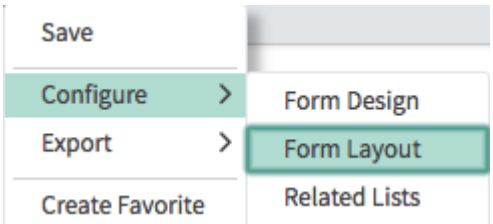
Ergebnisse

Wenn eine Alarmaktionsregel erfolgreich migriert wurde, kann die Alarmaktionsregel nicht mehr geändert werden. Die neue Warnungsverwaltungsregel kann jedoch geändert werden.

Nächste Maßnahme

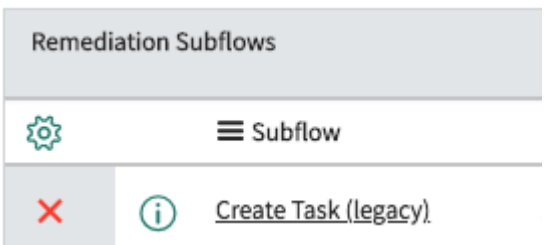
Wenn die migrierte Alarmaktionsregel über eine Aufgabenvorlage verfügt, können Sie den Designer der Alarmverwaltungsregel so anpassen, dass der Name der Aufgabenvorlage angezeigt wird.

1. Klicken Sie im Header der Warnungsverwaltungsregel auf **Zusätzliche Aktionen** ☰.
2. Auswahlvorgang **Konfigurieren** > **Formularlayout**.



3. Wählen Sie im Bereich **Verfügbar Aufgabenvorlage**, und verschieben Sie sie in den Bereich **Ausgewählt**. Positionieren Sie sie wie erforderlich.

4. Wählen Sie im Feld **Aufgabenvorlage** die zu verwendende Vorlage aus.
5. Wählen Sie auf der Registerkarte „Aktionen“ im Bereich „Nachbesserungs-Subflows“ den (veralteten) Subflow „Aufgabe erstellen“ (veraltet) aus, um die Aufgabenvorlage auszuführen.



Zugehörige Informationen

Schnelle Antworten in einer Warnung anwenden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsantwort wird mit automatischer Warnungsgruppierung synchronisiert

Standardmäßigwerden die Aufträge für die Warnungsgruppe und das Warnungsmanagement unabhängig voneinander ausgeführt. Daher können Sie die Warnungsantwort mit der automatisierten Warnungsgruppierung synchronisieren.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig werden der Auftrag zur Gruppierung von Warnungen (**Service Analytics-Gruppe Warnungen mit RCA/Warnungszusammenfassung**) und der Warnungsverwaltungsauftrag (**Ereignismanagement - Bereichsbezogenes Regel-Management für Warnmeldungen auswerten0**) unabhängig voneinander ausgeführt. Um die Warnungsantwort mit der automatisierten Warnungsgruppierung zu synchronisieren (um z. B. zu vermeiden, dass in einer sekundären Warnung ein Incident erstellt wird), müssen Sie evt_mgmt.avoid_int_enabled auf **true**, setzen, um sicherzustellen, dass die Aufgabe Warnungsmanagement nach der Warnung ausgeführt wird Gruppenauftrag ist abgeschlossen. Diese Eigenschaft ist über die Seite Ereignismanagement Eigenschaften () zugänglich.**Alle** > **Ereignismanagement** > **Administration** > **Ereignismanagement-Eigenschaften**). Darüber hinaus müssen Sie die entsprechende Warnungsverwaltungsregel konfigurieren (z. B. für die Incident-Erstellung), um alle sekundären Warnungen herauszufiltern.

Hinweis: Wenn die Warnmeldungsgruppe beim Start des Warnungsverwaltungsauftrags nicht generiert wurde, da nur eine einzige Warnung vorlag, wird ein Incident erstellt. Wenn eine neue Warnung folgt, wird automatisch ein Gruppen-Incident erstellt, und die Warnung neue Warnung wird während der Ausführung des nächsten Gruppierungsauftrags für Warnungen sekundär.

Prozedur
1. Navigieren zu **Alle** > **Ereignismanagement** > **Einstellungen** > **Eigenschaften**.
2. Wählen Sie im Kontrollkästchen Ja/Nein dieOption **Ja** aus, um Incidents bei sekundären Warnungen zu vermeiden, und warten Sie, bis der Gruppierungsauftrag ausgeführt wurde.
3. Wählen Sie im Kontrollkästchen Ja/Neindie Option **Nein** aus, um die Incident-Erstellung für sekundäre Warnungen zu aktivieren.
4. Wählen Sie **Speichern**.
5. Um sekundäre Warnungen herauszufiltern, navigieren Sie zu **Alle** > **Ereignismanagement** > **Regeln** > **Warnungsverwaltungsregeln**.
6. Wählen Sie die relevante Regel aus, z. B. **Incident erstellen**.
7. Öffnen Sie im Formular „Warnungsverwaltungsregel“ die Registerkarte **Warnungsfilter**.
8. Wählen Sie im Bereich Bedingung die Option **Und**aus.
9. Bedingung hinzufügen:
   - **Rolle in Gruppe**
   - **ist nicht**
   - **Sekundär**
10. Wählen Sie **Aktualisieren**.

Aktionen zum Beheben von Warnungen konfigurieren

Führen Sie Befehle zum Beheben von Warnungen für CIs von Linux- und Windows-Remote-Systemen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Installieren Sie das Plugin „*IntegrationHub Enterprise spokes*“.

Unter Linux: Vergewissern Sie sich, dass der Remote-Linux-Host über die MID-Server-IP-Adresse erreichbar ist, über die Aktionsskripts ausgeführt werden.

Für Windows:

- Stellen Sie sicher, dass PowerShell v3.0 bis 5.0 unterstützt und auf dem Zielserver Windows installiert wird.
- Aktivieren Sie PowerShell-Remoting auf dem Remote-Zielserver Windows.
- Stellen Sie sicher, dass der Remote-Zielserver Windows mit dem FQDN von MID-Server erreichbar ist, der Aktionsskripts ausführt.

Fügen Sie den Aliassen für Anmeldeinformationen, die mit dem Basissystem bereitgestellt werden, Anmeldeinformationen hinzu:

- linuxAdmin
- windowsAdmin

Erforderliche Rolle: evt_mgmt_admin oder flow_designer

Prozedur

1. Greifen Sie auf eine der folgenden Arten auf Korrekturaktionen zu:
   - Über Schnellaktionen in einer Warnung, wie in Schnelle Antworten in einer Warnung anwenden beschrieben.
   - Die Registerkarte Playbook in Service Operations-Arbeitsbereich, wie unter Aktionen ausführen, um Warnungsprobleme zu lösen beschrieben.
2. Konfigurieren Sie zusätzliche Eingaben im Feld **Zusätzliche Information** der Warnung, und verwenden Sie dazu folgendes Format:

   ```
   {"remediation_action_resource":"<mandatory input>"}
   ```

   Die Pflichteingabe pro Aktion wird in der folgenden Tabelle beschrieben.

Aktionsname	Pflichteingabe im Feld „Zusätzliche Information“
Windows-Prozess beenden	Prozess-ID
Linux-Service neu starten	Servicename
Linux-Prozess beenden	Prozess-ID
Windows-Prozesse abrufen	N/V
Windows-Dienst beenden	Anzeigename für Service
Windows-Dienst neu starten	Anzeigename für Service
Windows-Dienste abrufen	N/V
Linux-Service beenden	Servicename
Windows-Dienst starten	Anzeigename für Service
Windows-Dienst anhalten	Anzeigename für Service
Linux-Services abrufen	N/V

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsname	Pflichteingabe im Feld „Zusätzliche Information“
Linux Top-Befehl für Arbeitsspeicher ausführen	N/V
Verwendeten Speicherplatz anzeigen	N/V
Linux Top-Befehl ausführen	N/V
Linux-Service starten	Servicename
Verwendeten Speicherplatz anzeigen	N/V

Ergebnisse

Nach der Ausführung einer Warnungsaktion werden die Ergebnisse im Feld *Work Notes* der Warnung vermerkt.

Zugehörige Informationen

- Beheben von WMI-/PowerShell-Problemen auf dem Remotecomputer
- WMI, PowerShell und Windows-Firewalls
- MID-Server: Beheben von WMI-/PowerShell-Problemen – Anmeldeinformationen
- Aktivieren/Testen von PowerShell-Remoting auf einem Windows-Host

Domänentrennung über Subflows aufrufen

Ereignismanagement unterstützt die Domänentrennung sowohl im Basissystem als auch in benutzerdefinierten Subflows. Nachdem Sie einen Subflow angepasst haben, fügen Sie ihn der Aufnahmelistentabelle für Domänentrennungs-Subflows (*em_ds_subflow_white_list*) hinzu.

Zugehörige Informationen

- Ereignismanagement-Domain Separation konfigurieren

CI-Fehlerkorrektur

Warnungs- und Configuration Item (CI)-Fehlerkorrekturen helfen bei der Behebung von zugrunde liegenden Problemen, die Warnungen generieren. Die Fehlerkorrektur basiert auf Orchestrierungs-Workflows, die zur Ausführung von Fehlerkorrekturmaßnahmen wie dem Erfassen von Systeminformationen oder dem Neustart eines Servers geskriptet werden können.

Ereignismanagement bietet einen Rahmen für die Konfiguration und Implementierung eines systemweiten Fehlerkorrekturplans zur Lösung, Minimierung oder Verhinderung von Problemen, die Events und Warnungen generieren. Konfigurieren Sie Warnungsverwaltungsregeln für die Fehlerkorrektur von Warnungen und CI-Fehlerkorrekturregeln für die Fehlerkorrektur einer Reihe von CIs.

Warnungs-Fehlerkorrektur

Verwenden Sie Warnungsverwaltungsregeln, um bestimmte Warnungen einem Fehlerkorrektur-Workflow zuzuordnen. Sie können einen Workflow manuell auf Warnungen anwenden. Alternativ können Sie die Warnungsverwaltungsregel konfigurieren, die einen Workflow automatisch für Warnungen ausführt, die den Regelkriterien entsprechen. Der Workflow kann auch geskriptet werden, um eine Benutzergenehmigung anzufordern, bevor nachfolgende Workflow-Aufgaben ausgeführt werden. Der Workflow wird zur Benutzergenehmigung angehalten, auch wenn er automatisch ausgelöst wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Fehlerkorrektur

Konfigurieren Sie die Fehlerkorrektur umfassender, indem Sie CI-Fehlerkorrekturregeln erstellen, um die Fehlerkorrektur manuell auf bestimmte CIs anzuwenden.

Nachbesserungsaufgaben

Wenn ein Fehlerkorrektur-Workflow ausgeführt wird, wird eine Fehlerkorrekturaufgabe erstellt, um Details zu erfassen, wie z. B. die Zeit, zu der der Workflow gestartet wurde, die Warnung, die den Fehlerkorrektur-Workflow ausgelöst hat (falls relevant) und das CI, das korrigiert wurde. Zeigen Sie diese Aufgaben an, um Korrekturaktivitäten in der Organisation nachzuverfolgen.

Zugehörige Informationen

Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel

CI-Fehlerkorrektur erstellen oder bearbeiten

Erstellen Sie eine CI-Fehlerkorrekturregel, mit der Benutzer manuell einen Orchestration Workflow zur Lösung von Problemen mit bestimmten CIs anwenden können, die Warnungen zugeordnet sind. Definieren Sie diese CIs in den CI-Filterbedingungen der Regel.

Vorbereitungen

Erstellen Sie den Workflow, um CIs zu beheben. Wählen Sie in den Workflow-Einstellungen **Fehlerkorrektur-Aufgabe [em_remediation_task]** im Feld **Tabelle** aus.

Senden Sie dann die Workflow-Definition, und fügen Sie den Workflow-Eigenschaften die folgenden Bedingungen hinzu:

- **[Fehlerkorrektur ausführen] [ist] [true]**
- **[Workflow-] [Liste] [<Name des neuen Workflows, den Sie erstellt haben>]**

  Beispiel: Wenn der Name des Workflows `CI-Fehlerkorrektur` ist, fügen Sie diese Bedingung hinzu:

  [Workflow] [ist] [CI-Fehlerkorrektur]

Nachdem Sie den Workflow konfiguriert haben, stellen Sie sicher, dass Sie ihn veröffentlichen. Weitere Informationen finden Sie unter Einen Workflow erstellen .

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Eine CI-Fehlerkorrekturregel ordnet eine Reihe von CIs zu, bei denen Probleme mit einem Fehlerkorrektur-Workflow auftreten können. Der Fehlerkorrektur-Workflow kann entweder das zugrunde liegende Problem lösen oder zur Behebung des Problems beitragen, das die Warnung generiert hat. Beispielsweise können Sie proaktiv einen Workflow mit den entsprechenden Antwortaktionen für vorhersehbare Warnungen konfigurieren. Weitere Informationen finden Sie in unserem kurzen Video Event Management-Fehlerkorrektur .

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **CI-Fehlerkorrekturen**.
2. Klicken Sie auf **Neu**, oder wählen Sie eine CI-Fehlerkorrektur zur Bearbeitung aus.
3. Füllen Sie die Felder aus, und klicken Sie auf **Senden** oder **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CI-Fehlerkorrekturformular

Kontrolldiagramm	Beschreibung
CI-Filter	Bedingungen, die den CIs entsprechen, auf die Sie diese Fehlerkorrektur anwenden möchten.
Orchestrierungs-Workflow	Der Fehlerkorrektur-Workflow, der auf CIs angewendet werden soll, die den Filterbedingungen entsprechen.

Ergebnisse

In Servicezuordnungen, die über das Dashboard Ereignismanagement geöffnet werden, kann diese Fehlerkorrektur auf alle CIs angewendet werden, die den Filterbedingungen entsprechen.

Fehlerkorrekturaufgaben anzeigen

Ereignismanagement erstellt automatisch eine Fehlerkorrekturaufgabe, um jede Fehlerkorrektur zu erfassen, die auf ein CI oder eine Warnung angewendet wurde. Sie erhalten damit eine Gesamtansicht der Fehlerkorrekturaktivitäten in der Organisation.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user

Prozedur

Navigieren zu **Alle** > **Ereignismanagement** > **Korrekturaufgaben**.

Spalte	Beschreibung
Zahl	Nummer, die der Aufgabe zugewiesen ist.
Konfigurationselement	Element oder Service, der von dieser Aufgabe betroffen ist.
Priorität	Priorität, die dieser Aufgabe zugewiesen wurde, basierend auf Auswirkung und Dringlichkeit.
Status	Status der Aufgabe, der offen oder geschlossen sein kann.
Zugewiesen an	Person, der diese Aufgabe zugewiesen wurde.
Kurzbeschreibung	Beschreibung der Aufgabe
Aufgabentyp	Dieser Aufgabentyp ist eine Fehlerkorrekturaufgabe.

Funktionsweise von Warnungen mit CIs in der Wartung

Wenn sich ein CI in der Wartung befindet, werden die Auswirkungsstruktur, die Servicezuordnung und die Registerkarte „Warnungen“ basierend auf verschiedenen Faktoren aktualisiert.

Ereignismanagement Teil 2 | Impact Tree Sehen Sie sich dieses kurze Video an, um zu erfahren, wie Warnungen mit CIs funktionieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

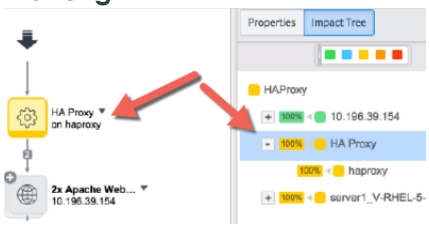
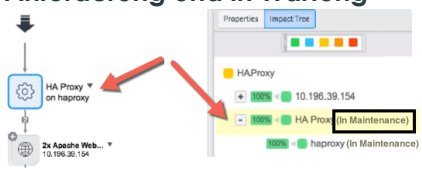
Ein CI wird in folgenden Fällen gewartet:

- Eine Change-Anforderung ist für das CI geplant.
- Das Feld **Installationsstatus** im CI-Datensatz wird auf **In Wartung**gesetzt.

Hinweis: Informationen zum Anpassen der Funktionsweise von Warnungen mit CIs in der Wartung finden Sie unter Wartungsregeln erstellen.

Darstellung von CIs in der Wartung in Event Management	Beschreibung und der optimale Zeitpunkt für die Lösung der Warnung
CI mit einer aktiven Change-Anforderung Wenn eine aktive Change-Anforderung für das CI geplant ist oder wenn der **Installationsstatus** des CI **auf In Wartung**lautet, werden alle Warnungen für das betroffene CI von der Berechnung der Auswirkung ausgeschlossen. Auf der Registerkarte „Warnungen“ werden alle entsprechenden Warnungen vorübergehend ebenfalls ausgeblendet. Im Auswirkungsbaum wird das CI in Grün mit dem Hinweis **(In Wartung)** angezeigt. In der Auswirkungsstruktur und in der Servicezuordnung werden CIs vorübergehend grün angezeigt. Für einen Service werden alle Warnungen bezüglich CIs im Service auch auf der Registerkarte „Warnungen“ ausgeblendet. Der gesamte Service wird im Auswirkungsbaum in Grün angezeigt. Für einen Host mit einer aktiven Change-Anforderung werden die Host-Applikationen als eine Einheit betrachtet. Alle untergeordneten Anwendungen werden, bis die Change-Anforderung nicht mehr aktiv ist, so behandelt wie der Host.	Eine aktive Change-Anforderung hat die folgenden Werte: • Der **Status** ist **Geplant** oder **Implementieren**. • Die aktuelle Zeit liegt zwischen geplantem Startdatum und geplantem Enddatum der Change-Anforderung. ODER • Die aktuelle Zeit liegt zwischen tatsächlichem Startdatum und tatsächlichem Enddatum der Change-Anforderung. Sie können den Fortschritt der Change-Anforderung überwachen. Warten Sie, bis die Change-Anforderung in den Status **Überprüfen** oder **Geschlossen** verschoben wird. Anschließend können Sie alle Warnungen für das betroffene CI und alle Warnungen behandeln, die zwischen Start- und Enddatum generiert wurden. Verwenden Sie die Auswirkungsstruktur, die Topologie und die Registerkarte „Warnungen“, um den berechneten Auswirkungsschweregrad anzuzeigen. **Hinweis:** Das Kontrollkästchen **Wartung** für eine Warnung ist aktiviert, wenn das Feld **Installationsstatus** des CI-Datensatzes **In Wartung**lautet. Dieses Kontrollkästchen **Wartung** gibt an, dass die Warnung auf der Registerkarte **Warnungen** ausgeblendet werden muss.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Darstellung von CIs in der Wartung in Event Management	Beschreibung und der optimale Zeitpunkt für die Lösung der Warnung
CI ohne aktive Change-Anforderung und nicht in der Wartung  Wenn keine aktive Change-Anforderung für ein CI vorhanden ist und sich das CI nicht in der Wartung befindet, wird die Auswirkungsberechnung fortgesetzt. Die Auswirkungsstruktur, die Servicezuordnung und die Registerkarte „Warnungen“ zeigen den berechneten Auswirkungsschweregrad für Warnungen an.	Eine inaktive Change-Anforderung hat die folgenden Werte: • Der **Status** ist **Neu**, **Bewerten**, **Autorisieren**, **Prüfen**, **Schließen** oder hat überhaupt keine Änderungen. • Der **Status** ist **Geplant** oder **Implementieren**. Die aktuelle Zeit liegt jedoch vor oder nach dem geplanten oder tatsächlichen Datumsbereich in der Change-Anforderung. Sie können den Fortschritt der Change-Anforderung überwachen. Wenn ein CI eine inaktive Change-Anforderung aufweist, können Sie die entsprechenden Warnungen nach Bedarf bearbeiten.
CI ohne aktive Change-Anforderung und in Wartung  Wenn für das CI keine aktive Change-Anforderung geplant ist und der **Installationsstatus** des CI **auf In Wartung**lautet, werden alle Warnungen für dieses CI von der Berechnung der Auswirkung ausgeschlossen. Im Auswirkungsbaum wird das CI in Grün mit dem Hinweis **(In Wartung)** angezeigt. In der Auswirkungsstruktur und in der Servicezuordnung werden CIs vorübergehend grün angezeigt.	Alle Warnungen in einem CI mit einer inaktiven Change-Anforderung und **In Wartung** haben keine Auswirkungsberechnung.

Zugehörige Informationen

Wartungsregeln erstellen

SLAs für Anwendungsservices und CIs

Ereignismanagement unterstützt die Erstellung von SLAs für Anwendungsservices und CIs.

Sie können die Qualität der von Ihrer Organisation angebotenen Services überwachen und verwalten. Beispielsweise können Sie eine SLA einrichten, die ausgelöst wird, wenn der maximale Warnungsschweregrad eines Anwendungsservice oder CI **kritisch** ist, und die Zeit messen, die erforderlich ist, um den Anwendungsservice oder das CI wieder in den Status **OK** zu versetzen , wenn die Bedingungen erfüllt sind, die die Warnung verursacht haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SLAs und die Aufgabentabelle

Sie können SLAs nur für Tabellen erstellen, die die Aufgabentabelle erweitern. Die Anwendung Ereignismanagement stellt eine Tabelle mit dem Namen Ereignismanagement-SLA [em_ci_severity_task] bereit, die die Aufgabentabelle erweitert. Verwenden Sie diese Tabelle in Ihren SLAs, um den Schweregrad anzugeben, der die SLA auslösen und stoppen soll. Während der Berechnung der Warnungsauswirkung werden Änderungen im Schweregrad von Anwendungsservices und CIs automatisch in der SLA-Tabelle Ereignismanagement aktualisiert. Scheduled Jobs halten die Informationen in dieser Tabelle auf dem neuesten Stand.

Wie die Ereignismanagement-SLA-Tabelle ausgefüllt wird

Die SLA-Tabelle Ereignismanagement wird für Anwendungsservices und CIs unterschiedlich ausgefüllt:

- Bei Anwendungsservices füllt das System die SLA-Tabelle Ereignismanagement automatisch aus, wenn ein Anwendungsservice erstellt oder der maximale Schweregrad geändert wird.
- Für CIs müssen Sie zuerst identifizieren, welche CIs für SLAs verfügbar gemacht werden können, indem Sie einen SLA-Konfigurationsdatensatz erstellen. Das System füllt dann automatisch die SLA-Tabelle Ereignismanagement mit dem CI-Schweregrad „geändert“ aus.

Hinweis: Doppelte CIs werden der SLA-Tabelle Ereignismanagement nicht hinzugefügt, auch wenn dasselbe CI mehr als einem SLA-Konfigurationsfilter entspricht.

Erstellen Sie eine SLA-Konfiguration für CIs

Erstellen Sie eine SLA-Konfiguration in der Anwendung Ereignismanagement, um zu bestimmen, welche CIs für SLAs verfügbar sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Der SLA-Konfigurationsdatensatz ist ein Filter für eine Tabelle im System. Wählen Sie eine Tabelle mit den CIs aus, für die Sie eine SLA erstellen möchten.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **SLA-Konfiguration**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).

SLA-Konfigurationsformularfelder

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Tabelle	Wählen Sie eine Tabelle mit den CIs aus, für die Sie eine SLA erstellen möchten. Sie können auch die Tabelle „Configuration Item to Host View“ [query_based_service_basic_view] verwenden, die von Dynamische CI-Gruppen verwendet wird.
Filter	Konfigurieren Sie den Filter für die Datensätze.

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Example:
Hier ein Beispiel:

Wenn Sie eine SLA auf allen Linux-Servern für schwerwiegende und kritische Warnungen ausführen möchten, erstellen Sie zuerst eine SLA-Konfiguration in der Linux-Server-Tabelle [cmdb_ci_linux_server]. Erstellen Sie dann die SLA-Definition mit diesem Filter:

- `CI.class` ist ein `Linux-Server`
- Der `Schweregrad` ist „`Schwerwiegend`" oder „`Kritisch`"

Nächste Maßnahme
Erstellen Sie eine SLA-Definition für die CIs, die dieser SLA-Konfiguration entsprechen.

Beschränken Sie die Datensätze für den SLA-Konfigurationsfilter

Wenn der SLA-Konfigurationsfilter zu viele Datensätze zurückgibt, können Sie eine Eigenschaft hinzufügen, um die maximale Anzahl von Datensätzen festzulegen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig ist die Größe von Datensätzen für dynamische CI-Gruppen auf 10.000 Elemente beschränkt. Das Überschreiten dieses Grenzwerts kann die Systemstabilität beeinträchtigen. Wenn die Filterkonfiguration für eine angegebene dynamische CI-Gruppe zu viele Datensätze zurückgibt, können Sie die Anzahl der zurückgegebenen Datensätze beschränken, indem Sie den Wert der Eigenschaft „sa.qbs.max_num_of_cis" festlegen. Weitere Informationen finden Sie unter Dynamische CI-Gruppe erstellen .

Prozedur

1. Geben Sie `sys_properties.list` im Anwendungsnavigator ein.
2. Fügen Sie die folgenden Eigenschaften hinzu:
   `sa.qbs.max_num_of_cis`
3. Legen Sie den Wert auf eine ganze Zahl fest, die die maximale Anzahl zurückzugebender Datensätze darstellt.

Erstellen Sie eine SLA-Definition für ein CI oder einen Anwendungsservice

Sie können SLAs für CIs und Anwendungsservices genau wie für andere Aufgabendatensätze in der Instanz erstellen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Service-Level-Management** > **SLA** > **SLA-Definitionen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular „SLA-Definition" aus.
   Eine Beschreibung der einzelnen Felder finden Sie unter Erstellen Sie eine SLA-Definition für ein CI oder einen Anwendungsservice.
4. Wählen Sie für das Feld **Tabelle** die Option **Event Management SLA [em_ci_severity_task]** aus .
5. Konfigurieren Sie den **Startbedingungsfilter,** indem Sie Bedingungen hinzufügen, z. B .:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SLA-Filterbedingungen

Für alle CIs mit **kritischem Schweregrad**		
Typ	**ist**	**CI** **Hinweis:** Ereignismanagement-SLAs funktionieren nur für CI-Klassen von der Serviceinstanz [cmdb_ci_service_auto].
Schweregrad	**ist**	**Kritisch**
Für einen bestimmten Service, z. B. E-Mail, wenn der **Schweregrad kritisch** ist		
Anwendungsservice	**ist**	**E-Mail**
Schweregrad	**ist**	**Kritisch**

6. Konfigurieren Sie Bedingungen für Pause, Stopp und Zurücksetzen.
7. Klicken Sie auf **Absenden**.

Warnungslebenszyklus-Konfiguration

Ereignismanagement bietet verschiedene Module, Vorlagen und Eigenschaften für die Konfiguration von Warnungen und die Aktionen, die für diese Warnungen ausgeführt werden.

Konfigurieren des aktiven Alarmintervalls

Die Eigenschaft „Aktives Intervall“ (**evt_mgmt.active_interval**) bestimmt, wie Ereignismanagement ein neues Ereignis behandelt, das Ereignissen ähnelt, die in einer vorhandenen geschlossenen Warnung angezeigt werden. Basierend auf dem aktiven Intervall, dem Ereignis und den vorhandenen Informationen zu geschlossenen Warnungen wird die Warnung erneut geöffnet, und die Ereignisinformationen werden der vorhandenen Warnung hinzugefügt, oder es wird eine neue Warnung erstellt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn das neue Ereignis empfangen wird und die Warnung bereits geschlossen ist, vergleicht Ereignismanagement die Zeit seit der letzten Warnungsaktualisierung (**sys_updated_on**) mit dem Wert der aktiven Intervalleigenschaft. Anschließend aktualisiert das System entweder die vorhandene Warnung oder erstellt eine neue Warnung (wenn die ursprüngliche Warnung geschlossen wird), wie in der folgenden Tabelle erläutert. Eine offene Warnung wird von Ereignismanagement automatisch aktualisiert, ohne den Wert der aktiven Intervalleigenschaft zu überprüfen.

Szenario	Ergebnis
Das neue Ereignis tritt auf, bevor das aktive Intervall für die vorhandene geschlossene Warnung abläuft.	Das Ereignis wird als eine Wiederholung eines vorhandenen Problems identifiziert. Die Warnung wird mit den Ereignisinformationen aktualisiert, und die Warnung wird erneut geöffnet.
Das neue Ereignis tritt nach Ablauf des aktiven Intervalls für die vorhandene geschlossene Warnung auf.	Eine neue Warnung wird erstellt, da das Ereignis als neues Problem identifiziert wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenario	Ergebnis
	Die Ereignisinformationen werden der neuen Warnung hinzugefügt.

Ändern Sie das aktive Intervall, indem Sie das **aktive Intervall (in Sekunden)** bearbeiten , innerhalb dessen ein neues Ereignis einen Eigenschaftswert der geschlossenen Warnung erneut öffnet .

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Ereignismanagement-Eigenschaften**.
2. Ändern Sie die Anzahl der Sekunden für die Eigenschaft **Aktivintervall (Zeitintervall in Sekunden, innerhalb dessen von einem neuen Ereignis ein geschlossener Alarm erneut geöffnet wird)**.
3. Klicken Sie auf **Speichern**.

Fluktuierende Warnungen konfigurieren

Legen Sie Fluktuationseigenschaften fest, um zu bestimmen, wann eine Warnung in den Status „Fluktuierend“ übergeht oder diesen verlässt. Flattern kann auf Konfigurationsprobleme (d. h. zu niedrig festgelegte Schwellenwerte), störende Services oder tatsächliche Netzwerkprobleme hinweisen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Flattern tritt auf, wenn von der Event-Quelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden. Flattern bewirkt, dass der Status der Ressource wiederholt zwischen dem Schweregrad *OK* und einem Schweregrad schwankt, der Aufmerksamkeit erfordert, z. B. *Critical*.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Ereignismanagement-Eigenschaften**.
2. Bearbeiten Sie die folgenden Eigenschaften nach Bedarf.

Eigenschaft	Beschreibung
evt_mgmt.update_alert_restricted_fields_-elapsed_time	Mindestzeitraum in Sekunden, der vergehen muss, bevor eine Warnung für identische Ereignisse aktualisiert werden kann. Wenn eine Warnung innerhalb dieses Intervalls aktualisiert wird, unterdrückt das System die Aktualisierung, um zu verhindern, dass häufig identische Benachrichtigungen gesendet werden. Standardmäßig ist dieses Intervall auf 86.400 Sekunden (24 Stunden) festgelegt.
evt_mgmt.flap_interval	Fluktuationsintervall in Sekunden. Dies ist der Zeitraum, innerhalb dessen eine Warnung in den Fluktuationsstatus übergeht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Eine Warnung tritt in den Status „Fluktuierend“ ein, wenn seine aktuelle **Anzahl der Fluktuationen** den gegebenen *evt_mgmt.flap_frequency* Eigenschaftswert innerhalb der von der angegebenen Eigenschaft *evt_mgmt.flap_interval* festgelegten Zeit erreicht oder überschreitet.
evt_mgmt.flap_frequency	Fluktuationshäufigkeit (die zum Übergehen in den Status „Fluktuierend“ erforderliche Warnungshäufigkeit).
evt_mgmt.flap_quiet_interval	Intervall für Verlassen des Fluktuationsstatus (Zeit in Sekunden, die vergehen muss, bis eine Warnung den Status „Fluktuierend“ verlässt). Eine Warnung verlässt den Status „Fluktuierend“, wenn das Zeitintervall zwischen dem letzten Auftreten des Events und der **letzten Aktualisierungszeit** der Warnung den Eigenschaftswert *evt_mgmt.flap_quiet_interval* erreicht oder überschreitet. Eine Warnung kann den Status „Fluktuierend“ auch unter folgenden Bedingungen verlassen: ◦ Wenn ein eingehendes Event nach Ablauf der Zeit *flap_quiet_interval* eintritt. Die neue Warnung wird generiert, und ihr Statuswert hängt vom Schweregrad des eingehenden Events ab. ◦ Nach einem Hintergrundauftrag, der alle fünf Minuten ausgeführt wird, wird sichergestellt, dass keine Warnungsaktualisierungen stattgefunden haben und die Zeit *flap_quiet_interval* verstrichen ist. Wenn keine Updates vorhanden sind, zeigt die Warnung den vorherigen Statuswert vor der Ausführung des Hintergrundauftrags an.

3. Klicken Sie auf **Speichern**.

Nächste Maßnahme

Sie können überwachen **Ereignismanagement** > **Alle Warnungen** Liste für Warnungen, die sich im Fluktuationsstatus befinden. Details finden Sie unter Warnungen im Status „Fluktuierend“ anzeigen.

Zugehörige Informationen

Mit fluktuierenden Warnungen arbeiten

Warnungen im Status „Fluktuierend“ anzeigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungspriorität

Bestimmen Sie die Reihenfolge, in der Warnungen behandelt werden, anhand der Punktzahl der Warnungspriorität. Mehrere Faktoren bestimmen die Priorität der Warnung, und dieser Wert ändert sich mit Änderungen an den zugrunde liegenden Faktoren.

Multifaktor-Entscheidungen

Der Wert der Warnungsprioritätspunktzahl setzt sich aus dem Wert der Kategorie und ihrer relativen Gewichtung zusammen. Sie können die Faktoren, aus denen die Punktzahl besteht, wie in den folgenden Abschnitten beschrieben, gemäß *Category order*, *Category value mapping* und *CI type weight factor mapping* konfigurieren. Die Kategorien sind:

- *Accumulated categories* - Diese Kategorien kumulieren Elemente mit verschiedenen Untertypen, die möglicherweise einen anderen Status oder Gewichtsfaktor haben. Beispielsweise Services, die nach unterschiedlicher Relevanz berücksichtigt werden, oder Services, die nach Kosten berücksichtigt werden.
- *Choice-list categories* - Eine Liste von Elementen Sie können jedes Element einem anderen Wert zuordnen, wodurch die Priorität für dieses Element geändert wird. Beispielsweise kann der kritische Schweregrad, der standardmäßig den Wert 1 hat, 4 zugeordnet werden, um ihm eine höhere Gewichtung in der berechneten Warnungspriorität zu geben.

Kategorienliste

Kategorie	Beschreibung
Kumulierte Kategorien	
Anzahl der betroffenen Business Services	Diese Kategorie wird von der Geschäftsrelevanz des Services berücksichtigt. Eine Warnung, die sich auf einen Service auswirkt, hat eine niedrigere Priorität als eine Warnung, die sich auf viele Services auswirkt. Wenn beispielsweise ein Router ausgefallen ist, kann dies Auswirkungen auf viele Services haben, und eine höhere Priorität stellt sicher, dass diese Warnung vor einer anderen behandelt wird, die sich auf weniger Services auswirkt. Eine Warnung, die sich auf viele nicht kritische Services auswirkt, muss mit Priorität behandelt werden. Wenn sich eine Warnung jedoch nur auf einige wenige Services auswirkt, dies aber wichtige Services sind, hat diese Warnung eine höhere Priorität.
CI-Typ	Diese Kategorie unterscheidet verschiedene CI-Typen. Beispielsweise kann eine Warnung auf einem CI-Typ, der ein Router oder Switch ist, eine höhere Priorität haben als eine Warnung auf einem anderen CI-Typ, z. B. einem Server oder einer Anwendung.
Anzahl sekundärer Warnungen	Warnungen, die ähnliche Eigenschaften wie andere Warnungen aufweisen, werden normalerweise gruppiert, z. B. Warnungen mit demselben Nachrichtenschlüssel. Eine übergeordnete Warnung mit vielen sekundären Warnungen hat eine höhere Priorität als eine übergeordnete Warnung mit nur wenigen sekundären Warnungen. Alle sekundären Warnungen einer übergeordneten Warnung werden gezählt. Wenn eine sekundäre Warnung geschlossen wird, ist sie nicht mehr mit der übergeordneten Warnung korreliert. Wenn eine übergeordnete Warnung geschlossen wird,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kategorienliste (Fortsetzung)

Kategorie	Beschreibung
	sind alle sekundären Warnungen nicht mehr korreliert, und ihr Prioritätswert wird entsprechend berechnet.
Auswahllisten-Kategorien	
Warnungsstatus	Für eine Warnung im Status *Closed* wird keine Prioritätspunktzahl berechnet. Die verfügbaren Status mit ihren Standardwerten sind: • Offen = Zuordnungswert 1 • Erneut öffnen = Zuordnungswert 2 • Flattern = Zuordnungswert 3
Warnungsschweregrad	Die Prioritätspunktzahl spiegelt den Schweregrad der zugrunde liegenden Warnung wider, z. B. hat eine Warnung mit dem Schweregrad *Critical* einen höheren gewichteten Wert als eine Warnung mit dem Schweregrad *Minor*. Für eine Warnung mit dem Schweregrad *OK* wird keine Priorität berechnet. Die verfügbaren Stufen sind: • Kritisch • Hoher • Geringer • Warnung
Rolle	Die Prioritätspunktzahl spiegelt die Rolle der Warnung wider. Die Prioritätspunktzahl ist höher für eine Warnung mit der Rolle *Parent* hat, darauf folgt Rolle *None*, und das geringste Gewicht hat eine Warnung mit Rolle *Secondary*. Eine übergeordnete Warnung mit vielen sekundären Warnungen hat einen höheren Wert als eine übergeordnete Warnung mit weniger sekundären Warnungen. Die verfügbaren Rollen sind: • Übergeordnet • Keine • Sekundär

Struktur der Warnungsprioritätspunktzahl

Gewichteter Wert für jede Kategorie

Jede Kategorie verfügt über eine eigene Platzierung in der Alarmprioritätspunktzahl, entsprechend ihrer Reihenfolge und ihrem Limit. Wie nachfolgend unter Warnungsprioritätspunktzahl ändern beschrieben, können Sie Reihenfolge und Grenzwert konfigurieren. Es gibt nur positive Zahlen.

Mit Ausnahme der folgenden werden alle Kategoriewerte aus der Tabelle *em_alert_priority_category_mapping* zugeordnet:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CI-Typ: Aus der Tabelle *em_alert_priority_ci_type* zugeordnet
- Sekundär: Der Wert entspricht der Anzahl der sekundären Warnungen und wird aus keiner Tabelle zugeordnet.

Hinweis: Um einen optimalen Arbeitsspeicherschutz zu gewährleisten, haben Warnungsgruppen mit mehr als 1000 Warnungen möglicherweise keine genaue Prioritätspunktzahl.

Beispielkomponenten für die Warnungsprioritätspunktzahl 7302020.003

Kategorie	Punktzahl
Services	(7,0, 1000000,0) Beispiel: Es gibt 2 betroffene Services, deren geschäftliche Relevanz wie folgt bewertet wird: • Service1: Geschäftsrelevanz-Prioritätspunktzahl = **3** • Service2: Geschäftsrelevanz-Prioritätspunktzahl = **4** Die Summe der geschäftlichen Relevanzprioritätspunktzahlen ist **7**, daher beträgt der berechnete Prioritätswert 7.000.000 (7 * 1.000.000). **Hinweis:** Die Business-Relevanz-Prioritätspunktzahl ist der zugeordnete Wert (**Wert nach Zuordnung**) in den Anwendungsservice-Einträgen der Tabelle „Zuordnungen der Warnungsprioritätskategorie“ (em_alert_priority_category_mapping
Schweregrad	(3,0, 100000,0)
CI-Typ	(20,0, 100,0)
Rolle	(2,0, 10,0)
Sekundär	(0, 0,01)
Status	(3,0, 0,001)

Mit den Punktzahlen aus der vorherigen Tabelle wird die Warnungsprioritätspunktzahl wie folgt berechnet:

```
(Services value * 1,000,000) + (Severity value * 100,000) + (CI type value
* 100) + (Role value * 10) + (Secondary value) + (State value * 0.001)
```

Durch Ersetzen der Werte der Kategorien aus der vorherigen Tabelle in der Formel ergibt sich:

```
(7 * 1,000,000) + (3 * 100,000) + (20 * 100) + (2 * 10) + (0 * 0.001) + (3
* 0.001) = 7,302,020.003
```

Im Bereich **Prioritätsaufgliederung** der Registerkarte **Weitere Informationen** wird als Warnungsprioritätswert 7302020.003 angezeigt. In der Liste „Warnungen“ wird dieser Wert als 7302 (Anzahl der Tausender) angezeigt.

Auswirkung von Kategoriebegrenzungen

Durch Grenzwerte für Kategorien können sich Überlaufwerte auf die nächste Kategorie auswirken, die in der Prioritätsreihenfolge höher angeordnet ist. Jede aufgelaufene Kategorie hat ein vordefiniertes Limit. Wenn die Anzahl diesen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Grenzwert überschreitet, wird 1 zur nächsthöheren Kategorie addiert. Wenn beispielsweise die Anzahl der CI-Typen den Grenzwert überschreitet, wird 1 zur nächsten Kategorie (Schweregrad) addiert, die eine höhere Priorität hat: `yyy-zzz wird zu yy (y + 1) - 000`.

In Liste „Alle Warnungen“ anzeigen

In der Liste **Alle Warnungen** wird die Warnungsprioritätspunktzahl in der Spalte **Priorität** angezeigt. Nur zu Anzeigezwecken wird die tatsächlich berechnete Warnungsprioritätspunktzahl durch 1000 geteilt, während in der Datenbank für Berechnungs- und Sortierzwecke der vollständige berechnete Wert verwendet wird.

Die detaillierte Berechnung der Warnungspriorität der ausgewählten Warnung wird auf der Registerkarte **Weitere Informationen** im Bereich **Prioritätsaufgliederung** angezeigt.

Berechnung der Warnungsprioritätspunktzahl

Die Berechnung der Warnungspriorität basiert auf allen Warnungen einer Gruppe und nicht nur auf der primären Warnung der Gruppe. Die Priorität wird für Warnungen berechnet, die diese Bedingungen erfüllen:

- Status ungleich **Geschlossen**
- Schweregrad ungleich **OK**

Warnungen, die zur Prioritätsberechnung in der Warteschlange stehen, werden in der Tabelle `em_alert_trigger_queue` aufgelistet. In der Tabelle „Geplante Aufgaben“ sind zwei Jobs für `Event Management - Warteschlangenpriorität Warnungen` vorhanden. Diese beiden Jobs können parallel ausgeführt werden. Sie können *`Einfügen und bleiben`* verwenden, um einen anderen Job zu erstellen. Der Job `Event Management - Warnungspriorität` wird einmal pro Minute ausgeführt und berechnet Prioritäten in Batches von 1000 offenen Warnungen. Es gibt mehrere Faktoren, die den Wert der Priorität einer Warnung bestimmen. Eine Änderung des Schweregrads löst eine sofortige Aktualisierung der Warnungsprioritätspunktzahl aus. In diesem Fall wird nur der Schweregradteil der Priorität geändert, zusammen mit den Schweregradinformationen im Bereich **Prioritätsaufgliederung** der Registerkarte **Weitere Informationen**.

Auslöser, die eine Neuberechnung auslösen

Auslöser, die eine Neuberechnung der Warnungsprioritätspunktzahl bewirken können, sind:

Liste der Auslöser für die Neuberechnung

Wiederholung	Auswirkung auf die Warnungsprioritätspunktzahl
Neue Warnung	Die Generierung einer neuen Warnung ist ein Auslöser für die Berechnung der Warnungsprioritätspunktzahl.
Vorhandene Warnung, die von „Geschlossen“ in einen anderen Status übergeht	Die Priorität wird für eine geschlossene Warnung nicht berechnet. Wenn der Warnungsstatus also von „Geschlossen“ in „Offen“, „Erneut öffnen“ oder „Fluktuierend“ geändert wird, ist diese Änderung ein Ausler fösür die Neuberechnung der Warnungsprioritätspunktzahl.
Rollenänderung zwischen primär, sekundär oder keine	Änderungen an der Rolle sind ein Auslöser für die Neuberechnung der Warnungsprioritätspunktzahl. Beispiel:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste der Auslöser für die Neuberechnung (Fortsetzung)

Wiederholung	Auswirkung auf die Warnungsprioritätspunktzahl
	• Eine Warnung, deren Typ in `Primär`geändert wurde, löst eine Neuberechnung der Warnungsprioritätspunktzahl aus. • Eine Warnung, deren Typ in `Keine` geändert wurde, löst die Neuberechnung der Warnungsprioritätspunktzahl aus. • Eine Warnung, deren Typ in `Sekundär`geändert wurde, löst eine Neuberechnung der Warnungsprioritätspunktzahl aus.
CI-Typ	Wenn ein CI an einen Alarm gebunden wird, ist diese Änderung ein Auslöser für die Neuberechnung der Alarmprioritätspunktzahl. Dieser Auslöser zur Neuberechnung der Priorität erfolgt nur einmal, wenn das CI an den Alarm gebunden ist.
Änderung der Anzahl sekundärer Warnungen	Eine Änderung der Anzahl sekundärer Warnungen löst eine Neuberechnung der Warnungsprioritätspunktzahl aus.
Schweregrad	Eine Änderung des Schweregrads löst eine Neuberechnung der Warnungsprioritätspunktzahl aus. Zum Beispiel löst die Änderung von `OK` zu `Schwerwiegend` eine Neuberechnung der Punktzahl aus. Im Gegensatz zu den anderen oben aufgeführten Auslösern löst eine Änderung des Schweregrads eine sofortige Aktualisierung des Schweregrads der Berechnung der Warnungsprioritätspunktzahl aus.

Warnungsprioritätspunktzahl ändern

Sie können die Wichtigkeit einiger Kategorien der Warnungspriorität ändern, indem Sie deren Reihenfolge und/oder Gewichtung wie unten beschrieben ändern. Beispiel: Wenn der CI-Typ eine höhere Bedeutung hat als die Anzahl der betroffenen Services, können Sie deren Reihenfolge ändern. Infolgedessen wird die Anzahl der Services jetzt mit 100 multipliziert, während der CI-Typ jetzt mit 1000000 multipliziert wird.

Hinweis: Durch die Änderungen, die Sie mit diesem erweiterten Verfahren vornehmen, ändert sich die Standardmethode zur Berechnung der Warnungsprioritätspunktzahl. Wenn diese konfigurierbaren Werte geändert werden, ändert sich bei Warnungen, die andernfalls möglicherweise keine hohe Punktzahl haben würden, möglicherweise die Reihenfolge, in der die Warnungen abgearbeitet werden.

Kategoriereihenfolge ändern

Navigieren Sie zur Tabelle *em_alert_priority_category_order*. In der Spalte **Reihenfolge** können Sie die Reihenfolge der erforderlichen Kategorie ändern.

Kategoriewertzuordnung

Die Tabelle *em_alert_priority_category_mapping* zeigt den Konfigurationswert für jede Kategorieauswahl. Jeder Wert in einer Dropdown-Liste von Kategorien kann durch Konfigurieren dieser Tabelle einem anderen Wert zugeordnet werden.

CI-Typ-Gewichtsfaktorzuordnung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren Sie zur Tabelle *em_alert_priority_ci_type*. Sie können einen neuen CI zum Beispiel `DualCoreCPU` hinzufügen und in der Spalte **Priorität** die Priorität der gewünschten Kategorie ändern. Darüber hinaus können Sie den vorhandenen Typ bearbeiten und seinen Prioritätswert ändern. Diese Tabelle wird dazu verwendet, den Wert jedes CI-Typs zuzuordnen. Beispielsweise kann ein Mainframe mit CI_type: cmdb_ci_mainframe eine Priorität von 80 haben, während ein Server mit CI_type: cmdb_ci_server eine Priorität von 60 aufweisen könnte. Mit der Zuordnung können Sie die Priorität der verschiedenen CI-Typen anpassen.

Warnungszuweisungsgruppen für Teams

Warnungszuweisungsgruppen weisen Warnungen umgehend und automatisch den richtigen Teams zu und verbessern so die allgemeinen Fähigkeiten zur Verwaltung von Incidents.

Administratoren bestimmen die Priorität von Warnungszuweisungsgruppen und stellen so sicher, dass Warnungen an die entsprechenden Teammitglieder weitergeleitet werden.

Die Zuweisungsgruppe für Warnungen wird durch den Wert der Eigenschaft *evt_mgmt.alert_auto_assignment_field* bestimmt. Als Administrator können Sie die Zuweisungsgruppe basierend auf den Warnungsfeldern festlegen, indem Sie den Eigenschaftswert verwenden und die Reihenfolge der durch Kommas getrennten Felder ändern, indem Sie den Eigenschaftswert bearbeiten.

Zugehörige Informationen

- Die Priorität für die Warnungszuweisungsgruppe wird zugewiesen
- Teambasierte Integrationseigenschaften
- Event-Regel erstellen oder bearbeiten
- Event-Feldzuordnungen erstellen

Die Priorität für die Warnungszuweisungsgruppe wird zugewiesen

Weisen Sie Warnungszuweisungsgruppen eine Priorität zu, um sicherzustellen, dass Warnungen an die entsprechenden Teammitglieder weitergeleitet werden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Geben Sie im Feld **Suche**`den Wert evt_mgmt.alert_auto_assignment_field` ein, und wählen Sie den Eigenschaftsdatensatz aus.
3. Geben Sie im Feld **Wert** die Zuweisungsgruppenvorrangangabe ein.
   Legen Sie die Priorität der Zuweisungsgruppe entsprechend der Reihenfolge der durch Kommas getrennten Felder fest, z. B. cmdb_ci.support_group, IntegrationGroup.
4. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

- Teambasierte Integrationseigenschaften

Express-Liste -Ansichten werden für Benutzer und Benutzergruppen konfiguriert

Steuern Sie zentral, was Anwender überwachen, indem Sie Ansichten in Express-Liste vordefinieren und sie Anwendern und Anwendergruppen zuweisen.

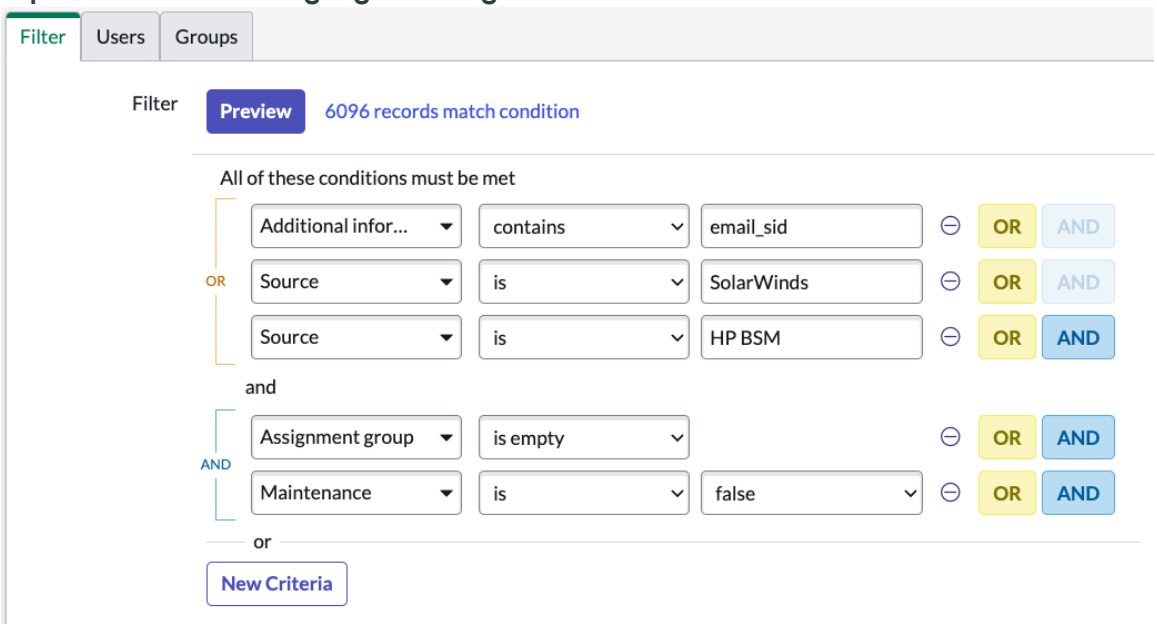
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Als Ereignismanagement -Administrator können Sie Express-Liste -Ansichten erstellen, um sicherzustellen, dass sich Benutzer auf bestimmte Services, Prioritäten oder Warnungen konzentrieren. Ereignismanagement ermöglicht Ihnen, die Filter, die Spaltenreihenfolge und Filterattribute für eine Express-Liste -Ansicht zu definieren und die Ansicht dann einzelnen Anwendern und Anwendergruppen zuzuweisen.

Anwender, die zu einer Gruppe gehören, können nur die vordefinierten Ansichten sehen, die Sie dieser Gruppe zugewiesen haben, und ihre eigenen gespeicherten Ansichten. Wenn ein Benutzer zu mehreren Gruppen gehört, kann er die Ansichten sehen, die Sie allen diesen Gruppen zugewiesen haben. Benutzer können zwischen Ansichten wechseln und alle Ansichten mit Ausnahme der zugewiesenen Standardansicht ändern und speichern. Sie können jedoch keine Einstellungen in einer der ihnen zugewiesenen Ansichten überschreiben und ihre Standardansicht ändern oder freigeben.

Mit dem Filterbedingungsgenerator können Sie UND- und ODER-Bedingungen zwischen Attributen konfigurieren.

Express-Liste Filterbedingungen anzeigen



Beispielsweise kann der Administrator Bedingungen konfigurieren, die es dem Benutzer ermöglichen, nur Warnungen anzuzeigen, die keiner Zuweisungsgruppe zugewiesen sind oder sich in Wartung befinden. Im Beispiel müssen die Warnungen auch den Wert email_sid enthalten und aus einer der angegebenen Quellen stammen.

Zugehörige Informationen

- Erstellen Sie eine vordefinierte Ansicht Express-Liste für -Benutzer
- Verwenden Sie eine zugewiesene Express-Liste Ansicht

Erstellen Sie eine vordefinierte Ansicht Express-Liste für -Benutzer

Konfigurieren Sie eine Express-Liste -Ansicht für Benutzer, um sicherzustellen, dass sie sich auf bestimmte Services, Prioritäten oder Warnungen konzentrieren. Sie können die Filter, die Spaltenreihenfolge und die Filterattribute für diese Ansicht festlegen und sie einzelnen Anwendern oder Anwendergruppen zuweisen.

Vorbereitungen

Weitere Informationen zu vordefinierten Express-Liste -Ansichten finden Sie unter Express-Liste -Ansichten werden für Benutzer und Benutzergruppen konfiguriert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Express-Listenansichten**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular **„Express-Listenansicht“** aus.

Express-Liste Tabelle anzeigen

Feld	Beschreibung
Name	Eindeutiger Name der Ansicht Express-Liste.
Primäres Feld „Sortieren nach“	Das Feld, nach dem Express-Listesortiert werden soll. Standard: Generierungszeit des ersten Ereignisses.
Sekundäres Feld „Sortieren nach“	Das Feld, nach dem die Ergebnisse des primären Felds „Sortieren nach“ sortiert werden sollen. Dieses Feld ist optional.
Auftrag	Die Reihenfolge der Ansicht Express-Liste, wenn mehrere Ansichten vorhanden sind.
Reihenfolge des primären Felds „Sortieren nach“	Die Sortierreihenfolge des primären Felds „Sortieren nach“: Aufsteigend oder Absteigend.
Reihenfolge des sekundären Felds „Sortieren nach“	Die Sortierreihenfolge des sekundären Felds „Sortieren nach“, falls festgelegt: Aufsteigend oder Absteigend.
Standard	Option, um diese Ansicht Express-Liste als Standardansicht für den zugewiesenen Anwender oder die zugewiesene Gruppe festzulegen. Wenn mehrere Standardansichten vorhanden sind, bestimmt der im Feld Reihenfolge festgelegte Wert deren Reihenfolge.

4. Legen Sie Filterbedingungen für die Ansicht Express-Liste fest.

Hinweis: Wenn Sie in Ihre Ansicht Express-Liste auch nur einen einzigen nicht unterstützten Filter aufnehmen, verhindert der Operator Ereignismanagement, dass er die Einstellungen von Filtern in dieser Ansicht ändert, einschließlich der unterstützten. Wenn Sie möchten, dass Bediener ihre persönliche Ansicht anpassen, stellen Sie sicher, dass Sie nur unterstützte Filter einbeziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie auf der Registerkarte **Filter** ein Feld, einen Operator und einen oder mehrere Werte für eine Bedingung aus.

Hinweis: Das Standardfeld ist Status.

b. Wahlweise: Führen Sie die folgenden Aufgaben aus.

Aufgabe	Verfahren
Fügen Sie eine Filterbedingung hinzu	**i.** Wählen Sie entweder den UND- oder den ODER-Operator aus. **ii.** Wählen Sie ein Feld, einen Operator und mindestens einen Wert für die Bedingung aus.
Fügen Sie eine Warnungs-Tag-Filterbedingung hinzu	**i.** Wählen Sie im Abschnitt „Warnungs-Tags-Filter“ **Neue Zeile einfügen...**aus. **ii.** Wählen Sie für jeden Tag-Filter das erforderliche Tag, den Operator und den Wert aus.
Fügen Sie einen zusätzlichen Satz von Filterbedingungen für Warnungs-Tags hinzu	**i.** Wählen Sie im Abschnitt „Warnungs-Tags-Filter “ **Neues Kriterium**aus. **ii.** Fügen Sie die erforderlichen Tag-Filterbedingungen hinzu.
Zeigen Sie die Anzahl der Ergebnisse an, die eine Abfrage mit den konfigurierten Bedingungen zurückgibt	Wählen Sie **Vorschau**.

5. Weisen Sie der Ansicht Express-Liste Benutzer und Gruppen zu.

Aufgabe	Verfahren
Weisen Sie der ausgewählten Ansicht Express-Liste einen Anwender zu	**a.** Wählen Sie auf der Registerkarte **Benutzerdie Option Neue Zeile einfügen...**aus. **b.** Wählen Sie das Suchsymbol ( ), und suchen Sie in der Tabelle **„Benutzer“** nach dem entsprechenden Benutzer. **c.** Wählen Sie den Benutzer aus, und wählen Sie dann das Speichern-Symbol ( ).
Weisen Sie der ausgewählten Ansicht Express-Liste eine Benutzergruppe zu	**a.** Wählen Sie auf der Registerkarte **Gruppendie Option Neue Zeile einfügen...**aus. **b.** Wählen Sie das Suchsymbol ( ), und suchen Sie in der Tabelle **Gruppen** nach der entsprechenden Gruppe. **c.** Wählen Sie die Gruppe und dann das Speichern-Symbol ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Verfahren
	Hinweis: Benutzer, die zu einer Gruppe gehören, können nur die Ansichten sehen, die Sie dieser Gruppe zugewiesen haben. Wenn ein Benutzer zu mehreren Gruppen gehört, kann er die von Ihnen konfigurierten Ansichten für alle diese Gruppen sehen.

6. Wählen Sie im Formularmenü **Speichern**aus.
   Die folgenden Registerkarten werden angezeigt:
   - Auf der Registerkarte **Express-Listentabellenfelder** werden die Felder angezeigt, die als Tabellenspalten in Express-Listeangezeigt werden sollen.
   - Auf der Registerkarte **Feldattribute für die Express-Listenansicht** werden die Filterattribute für die offenen Warnungen in Express-Listeangezeigt.
7. Wahlweise: Fügen Sie der Ansicht Express-Liste Tabellenfelder und Feldattribute hinzu.

Aufgabe	Verfahren
Fügen Sie der Tabelle Express-Liste eine Spalte hinzu	**a.** Wählen Sie auf der Registerkarte **Express-Listentabellenfelder** die **Option Neu**aus. **b.** Füllen Sie die Felder des Formulars aus. ▪ Feld: Die hinzuzufügende Spalte. ▪ Express-Liste Ansicht: Der Name der Ansicht, der die Spalte hinzugefügt werden soll. ▪ Mindestbreite: Mindestbreite der Spalte. ▪ Reihenfolge: Die Position der Spalte in der Tabelle. ▪ Aktiv: Option zum Aktivieren der Spalte. **c.** Wählen Sie **Absenden**.
Fügen Sie dem Filterbereich in ein Attribut hinzu Express-Liste	**a.** Wählen Sie auf der Registerkarte **Express-Listenansicht – Feldattribute die-Option Neu**aus. **b.** Füllen Sie die Felder des Formulars aus. **i.** Feld: Das Attribut, das dem Filterbereich hinzugefügt werden soll. **ii.** Express-Liste Ansicht: Der Name der Ansicht, der das Attribut hinzugefügt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Verfahren
	iii. Reihenfolge: Die Position des Attributs im Bereich. **iv.** Aktiv: Option zum Aktivieren des Attributs. **c.** Wählen Sie **Absenden**.

8. Wahlweise: Schließen Sie Felder oder Feldattribute aus der Ansicht Express-Liste aus, indem Sie sie deaktivieren.

Aufgabe	Verfahren
Deaktivieren Sie ein Feld	**a.** Wählen Sie auf der Registerkarte **Express-Listentabellenfelder** das Informationssymbol (ⓘ) links neben einem Felddatensatz. **b.** Löschen Sie im Feldformular **Aktiv**. **c.** Wählen Sie **Aktualisieren**.
Deaktivieren Sie ein Feldattribut	**a.** Wählen Sie auf der Registerkarte **„Feldattribute für Express-Listenansicht“** das Informationssymbol (ⓘ) links neben einem Feldattributdatensatz. **b.** Löschen Sie im Feldformular **Aktiv**. **c.** Wählen Sie **Aktualisieren**.

Hinweis: Sie können den aktualisierten Status eines Felds oder eines Feldattributs in der Tabelle anzeigen, indem Sie das Symbol für Listensteuerelemente (≡) und dann **Liste neu laden**wählen.

9. Wenn Sie mit der Ansicht Express-Liste zufrieden sind, wählen Sie **Aktualisieren**aus.

Weisen Sie Benutzer und Gruppen den vordefinierten Ansichten Express-Liste zu

Weisen Sie einzelne Anwender und Anwendergruppen vorkonfigurierten Ansichten Express-Liste zu, um sicherzustellen, dass sie sich auf bestimmte Services, Prioritäten oder Warnungen konzentrieren.

Vorbereitungen

Weitere Informationen zu vordefinierten Express-Liste -Ansichten finden Sie unter Express-Liste -Ansichten werden für Benutzer und Benutzergruppen konfiguriert.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Express-Listenansichten**.
2. Wählen Sie die vordefinierte Ansicht Express-Liste aus, die Sie einem Benutzer oder einer Gruppe zuweisen möchten.
3. Weisen Sie der ausgewählten Ansicht Express-Liste Anwender oder Gruppen zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgabe	Verfahren
Weisen Sie der ausgewählten Ansicht Express-Liste einen Anwender zu	**a.** Wählen Sie auf der Registerkarte **Benutzer**die Option **Neue Zeile einfügen...**aus. **b.** Wählen Sie das Suchsymbol ( ), und suchen Sie in der Tabelle **„Benutzer“** nach dem entsprechenden Benutzer. **c.** Wählen Sie den Benutzer aus, und wählen Sie dann das Speichern-Symbol ( ).
Weisen Sie der ausgewählten Ansicht Express-Liste eine Benutzergruppe zu	**a.** Wählen Sie auf der Registerkarte **Gruppe**die Option **Neue Zeile einfügen...**aus. **b.** Wählen Sie das Suchsymbol ( ), und suchen Sie in der Tabelle **Gruppen** nach der entsprechenden Gruppe. **c.** Wählen Sie die Gruppe und dann das Speichern-Symbol ( ). **Hinweis:** Anwender, die zu einer Gruppe gehören, können nur die vordefinierten Ansichten sehen, die Sie dieser Gruppe zugewiesen haben, und ihre eigenen gespeicherten Ansichten. Wenn Anwender zu mehreren Gruppen gehören, können sie die Ansichten sehen, die Sie allen diesen Gruppen zugewiesen haben.

4. Wählen Sie **Aktualisieren**.

Warnungsauswirkungsberechnung

Die Auswirkungsberechnung zeigt das Ausmaß eines Ausfalls von CIs, Services, Warnungen und Warnungsgruppen an. Vom System werden Faktoren wie Auswirkungsregeln und CI-Beziehungen zur Berechnung des Schweregrads einer generierten Warnung verwendet. Der Schweregrad wird in der Auswirkungsstruktur, in Zuordnungen für Anwendungsservices und in Dashboards angezeigt.

Berechnungen der Auswirkung sind für Warnmeldungsgruppen von Anwendungsservices verfügbar. Die folgenden Faktoren werden zur Berechnung der Gesamtauswirkung eines Ausfalls verwendet.

- Auswirkungsregeln
- Anzahl der zugehörigen aktiven Warnungen.
- Vergangener Verlauf des betroffenen CI.
- Beziehungen zwischen CIs für einen bestimmten Anwendungsservice oder Anwendungsservices.
- Wenn das CI-Element ein Netzwerk oder Speichergeräte enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

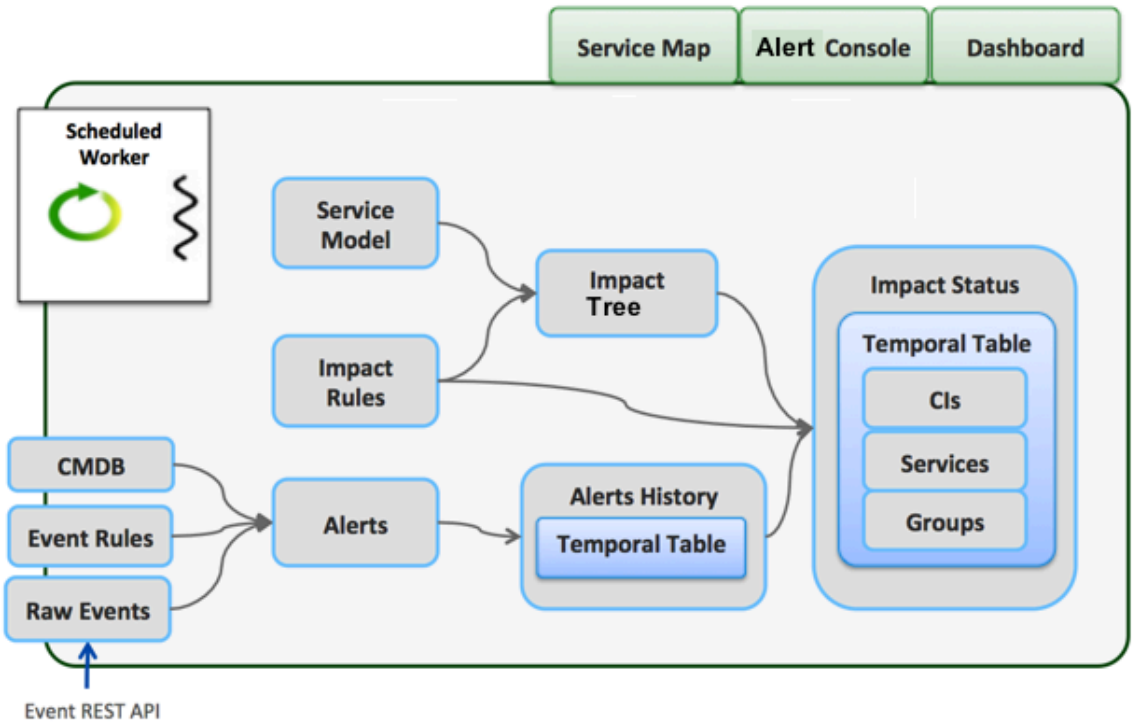
- Warnungen zu CIs in der Wartungsphase werden aus der Auswirkungsberechnung ausgeschlossen.

Hinweis:

- CIs gelten nicht nur dann als in Wartung, wenn eine aktive Change-Anforderung geplant ist, sondern auch, wenn das **Statusfeld** des CIs auf **In Wartung** gesetzt ist.
- Wenn ein untergeordnetes CI in Wartung gesetzt wird, wird auch das übergeordnete CI in Wartung gesetzt.

Wenn eine Verbindung zwischen Services besteht, werden auch die Auswirkungen eines Services auf den anderen berechnet.

Auswirkungsberechnungen verwenden Informationen aus verschiedenen Quellen, um den Schweregrad der Warnung festzulegen.



Berechnung der Auswirkung

Die Berechnung der Auswirkung hängt von den CI-Beziehungen für einen Anwendungsservice oder Anwendungsservices ab. Zusätzliche Faktoren wie Change-Anforderungen, Netzwerkpfade, Speicherpfade und zugehörige CIs wirken sich auf die Auswirkungsberechnung aus.

Services

Der folgende Flow für die Auswirkungsberechnung wird für Warnungen ausgeführt, bei denen der Ausfall kein Netzwerk oder keinen Netzwerkspeicher betrifft. Ereignismanagement führt die folgenden Schritte aus:

1. Erstellen einer Servicezuordnung Verwenden Sie die Tabellen Zuordnungen von Servicekonfigurationselementen [svc_ci_assoc] und CI-Beziehungen [cmdb_rel_ci], um untergeordnet/übergeordnet-Beziehungen im Anwendungsservice oder in den Anwendungsservices zu erstellen.
2. Wenn kein CMDB-Pfad vom Service zum CI vorhanden ist, in der Tabelle „svc_ci_assoc“ jedoch eine Zuordnung angezeigt wird, zeigen Sie eine

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängigkeitsbeziehung zwischen dem Anwendungsservice und dem CI an. Andernfalls zeigen Sie keine Verbindung an.

3. Wenn bei Anwendungsservices die dem Service zugewiesenen CIs auch mit dem Service in der CMDB verbunden sind, behält die Zuordnung die Hierarchie zwischen den CIs bei, wie sie in der CMDB angezeigt werden. Die CI-Servicezuweisungen werden im Abschnitt Anwendungsservice für Servicekonfigurationselemente angezeigt. Wenn in der CMDB keine Verbindung zum Service besteht, werden die CIs direkt unter den Anwendungsservices in der Zuordnung angezeigt.
4. Erstellen Sie die Auswirkungsstruktur. Markieren Sie das Ausmaß eines Ausfalls nach unten zu 100 %, 60 %, 40 % oder 20 %. Wenn die Elemente in zwei oder mehr Clustern betroffen sind, ist die Auswirkung um 100 % geringer.

Change-Anforderungen und der Status „In Wartung“

Wenn eine aktive Change-Anforderung für das CI geplant ist oder wenn der **Installationsstatus** des CI **auf In Wartung**lautet, werden alle Warnungen für das betroffene CI von der Berechnung der Auswirkung ausgeschlossen. Auf der Registerkarte „Warnungen“ werden alle entsprechenden Warnungen vorübergehend ebenfalls ausgeblendet. Im Auswirkungsbaum wird das CI in Grün mit dem Hinweis **(In Wartung)** angezeigt. In der Auswirkungsstruktur und in der Servicezuordnung werden CIs vorübergehend grün angezeigt.

Hinweis:

- CIs gelten nicht nur dann als in Wartung, wenn eine aktive Change-Anforderung geplant ist, sondern auch, wenn das **Statusfeld** des CIs auf **In Wartung** gesetzt ist.
- Wenn ein untergeordnetes CI in Wartung gesetzt wird, wird auch das übergeordnete CI in Wartung gesetzt.

Für einen Service werden alle Warnungen bezüglich CIs im Service auch auf der Registerkarte „Warnungen“ ausgeblendet. Der gesamte Service wird im Auswirkungsbaum in Grün angezeigt. Für einen Host mit einer aktiven Change-Anforderung werden die Host-Applikationen als eine Einheit betrachtet. Alle untergeordneten Anwendungen werden, bis die Change-Anforderung nicht mehr aktiv ist, so behandelt wie der Host. Weitere Informationen finden Sie unter Funktionsweise von Warnungen mit CIs in der Wartung.

Netzwerkpfade

Zur Berücksichtigung der Netzwerkredundanz verwendet Ereignismanagement eine separate Auswirkungsberechnung. Sie können Änderungen der Netzwerktopologie oder des Pfads im Anwendungsservice anzeigen. Der folgende Flow für die Auswirkungsberechnung wird für Warnungen ausgeführt, bei denen der Ausfall einen Netzwerkpfad betrifft. Ereignismanagement führt die folgenden Schritte aus:

1. Erstellen Sie eine Anwendungsservice-Zuordnung für das betroffene Netzwerk.
   - Verwenden Sie die Host-ID und die Ziel-IP-Informationen aus der Warnung und den Netzwerkpfad aus der Tabelle „Netzwerkpfade“ [sa_network_paths].
   - Verwenden Sie die Elemente im Netzwerkpfad, die von der Configuration Item-Tabelle [cmdb_ci] abgeleitet sind. Verwenden Sie auch die Elemente, die dem Pfad zugeordnet sind, aus der Tabelle „Infra-Pfad zu Elementen“ [sa_infra_path_assoc].

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie Beziehungen fest. Das Anwendungs-CI weist die Beziehung „Abhängig von::Verwendet von“ für ein Element im Pfad auf, das in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] definiert ist. In der Beziehung ist das Anwendungs-CI das übergeordnete Element und das Element im Netzwerkpfad das untergeordnete Element.

2. Berechnen Sie einen separaten Schweregrad für jedes reguläre Element im Pfad. Jedes reguläre Element im Pfad fügt seinen eigenen Schweregrad zu seinen Vorfahren bis zum Anwendungs-CI hinzu, von dem der Pfad stammt.
3. Berechnen Sie alle redundanten Elemente im Pfad mit der Redundanzregel, indem Sie den Schweregrad der betroffenen CIs um eine Ebene reduzieren. Beispiel: Wenn der Schweregrad *Critical* ist, verringert die Redundanzregel den Schweregrad um eine Ebene auf *Major*.
4. Erstellen Sie die Auswirkungsstruktur. Markieren Sie das Ausmaß eines Ausfalls nach unten zu 100 %, 60 %, 40 % oder 20 %. Wenn die Elemente in zwei oder mehr Clustern betroffen sind, ist die Auswirkung um 100 % geringer.

Speicherpfade

Zur Berücksichtigung der Netzwerkredundanz verwendet Ereignismanagement eine separate Auswirkungsberechnung. Sie können sehen, wie die Auswirkungsstruktur aktualisiert wird, wenn sich die Netzwerkspeichertopologie vom Anwendungsservice ändert. Ereignismanagement führt die folgenden Schritte für Warnungen aus, die Speicher-CIs enthalten:

1. Erstellen Sie eine Anwendungsservice-Zuordnung für das betroffene Speichergerät:
   - Verwenden Sie das Speichergerät in der Tabelle „sa_fs_to_storage_path“. Die Speichergerätedefinition verwendet die Dateisysteminformationen im Pfad.
   - Verwenden Sie die Elemente im Netzwerkpfad, die von der Configuration Item-Tabelle [cmdb_ci] abgeleitet sind. Verwenden Sie auch die Elemente, die dem Pfad aus der Tabelle „Infra-Pfad zu Elementen“ [sa_infra_path_assoc] zugeordnet sind.
   - Legen Sie Beziehungen fest. Das Anwendungs-CI weist die Beziehung „Abhängig von::Verwendet von“ für ein Element im Pfad auf, das in der Tabelle „CI-Beziehung“ [cmdb_rel_ci] definiert ist. In der Beziehung ist das Anwendungs-CI das übergeordnete Element und das Element im Speicherpfad das untergeordnete Element.
2. Berechnen Sie einen separaten Schweregrad für jedes reguläre Element im Pfad. Jedes reguläre Element im Pfad fügt seinen eigenen Schweregrad zu seinen Vorfahren bis zum Original-Anwendungs-CI des Pfads hinzu.
3. Berechnen Sie redundante Elemente im Pfad mit der Redundanzregel, indem Sie den Schweregrad der betroffenen CIs um eine Ebene reduzieren. Beispiel: Wenn der Schweregrad *Critical* ist, verringert die Redundanzregel den Schweregrad um eine Ebene auf *Major*.
4. Erstellen Sie die Auswirkungsstruktur. Markieren Sie das Ausmaß eines Ausfalls nach unten zu 100 %, 60 %, 40 % oder 20 %. Wenn die Elemente in zwei oder mehr Clustern betroffen sind, ist die Auswirkung um 100 % geringer.

Zugehörige CIs

Während Warnungen für ein CI generiert werden, werden zusätzliche Auswirkungsberechnungen für zugehörige CIs ausgeführt. Beispielsweise

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden Berechnungen der zusätzlichen Auswirkung für eine Anwendungsserviceabhängigkeit von einem CI ausgeführt, das nicht Teil des Anwendungsservice ist. Diese zugehörigen CIs werden nicht als Teil des Services erkannt. Stattdessen werden die zugehörigen CIs durch Definition einer Infrastrukturbeziehung angegeben.

Der folgende Flow zur Berechnung der Auswirkung gilt für Warnungen mit CIs, die eine Abhängigkeit von zugehörigen CIs aufweisen, die außerhalb des Anwendungsservice liegen. Ereignismanagement führt die folgenden Schritte aus:

1. Beziehungen zwischen Anwendungsservice-CIs und zugehörigen CIs ableiten. Verwenden Sie Beziehungen, Auswirkungsregeln und andere Daten aus der Tabelle „Infrastrukturbeziehungen“ [em_impact_infra_rel_def].
2. Fügen Sie der Auswirkungsstruktur und der Warnungsliste im Dashboard Ereignismanagement zugehörige CIs hinzu.
   - Verwenden Sie Daten aus der Tabelle „Infrastrukturbeziehung“ [em_impact_infra_rel_def], um Containment-Links zum Host anzuzeigen.
   - Verwenden Sie die Tabellen „Auswirkungsstatus“ [em_impact_status] und „Warnungsverlauf“ [em_alert_history], um den Status zu bestimmen.

Auswirkungsregeln

Auswirkungsregeln, die für die Auswirkungsberechnung verwendet werden, schätzen den Umfang oder den Schweregrad eines Ausfalls basierend auf betroffenen CIs.

Die Tabelle „Auswirkungsregel“ [em_impact_rule] enthält Auswirkungsregeln, die die entsprechenden CIs, Anwendungsservices und Einstellungen für die Auswirkung anzeigen. Die folgenden Standardauswirkungsregeln sind verfügbar.

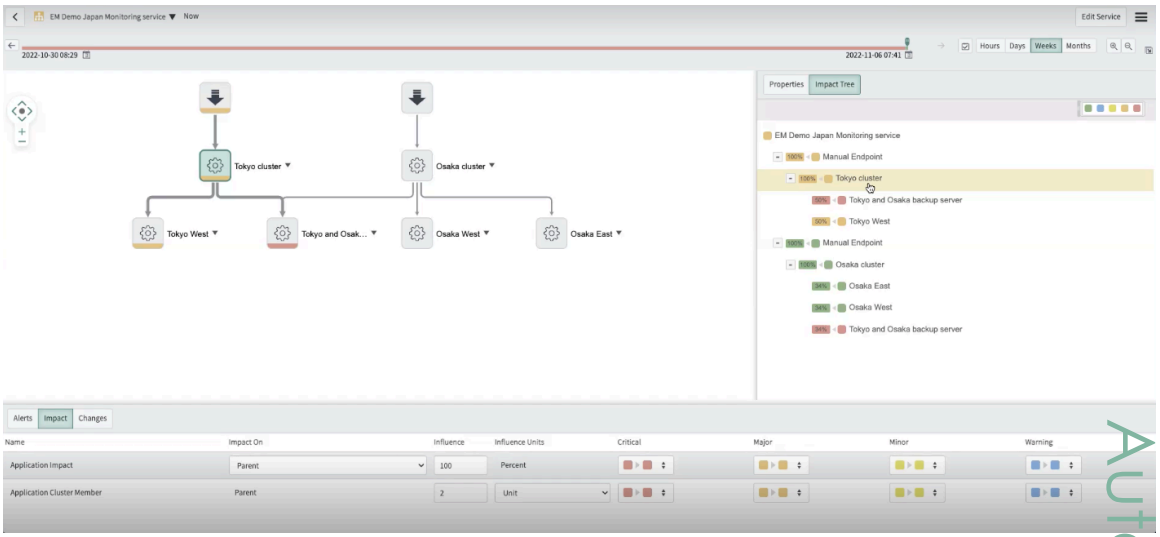
Mitglied in Anwendungscluster

Bestimmung, wie sich die Mitglieder des Anwendungsclusters auf die Gesamtwirkung des Clusters auswirken. Wenn beispielsweise ein Cluster mit drei Mitgliedern **einen Einfluss von 90 %** benötigt, um den Schweregrad für den gesamten Cluster auf **„Schwerwiegend“**festzulegen, hat jedes Mitglied **30 % Einfluss** (90 % geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn alle drei Mitglieder den Schweregrad **Schwerwiegend** aufweisen.

Sie können unterschiedliche Auswirkungsregeln pro Cluster konfigurieren, und daher unterscheidet sich die Weitergabe der untergeordneten CI an das übergeordnete Element (für dasselbe untergeordnete CI). Daher können Sie Gruppen von CIs (auch als manuelle Cluster bezeichnet) manuell erstellen und die Auswirkungsregel auf Clusterebene für nachgelagerte Elemente in Richtung der untergeordneten Elemente des Clusters konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel, in dem das gleiche untergeordnete CI seine Auswirkung auf das übergeordnete Cluster von jedem Cluster unterschiedlich verbreitet



Im obigen Beispiel gibt es zwei Einstiegspunkte. Der Tokyo-Cluster auf der rechten Seite verfügt über drei CIs. Der Tokyo-Cluster auf der linken Seite verfügt über zwei CIs. Die Sicherungsserver für Tokyo und Tokyo haben gemeinsam übergeordnete Elemente – Tokyo-Cluster und Tokyo-Cluster. Auf der rechten Seite sehen Sie die Auswirkungsstruktur, in der für den Tokyo-Cluster zwei Anwendungsclustermitglieder mit jeweils 50 % Einfluss und für den Tokyo-Cluster drei Anwendungscluster mit jeweils 34 % Einfluss vorhanden sind.

Für die manuelle Clusterkonfiguration gibt es zwei Zeilen: „Auswirkung auf die Anwendung“ und „Mitglied im Anwendungscluster“. Die untergeordneten Elemente werden angezeigt, da das Feld Auswirkung auf als Übergeordneter Service und nicht als Anwendungsservice ausgewählt wurde. In der Zeile „Mitglied in Anwendungscluster“ ist das Feld „Einfluss“ auf „2“ festgelegt. Dies impliziert, dass es mindestens zwei untergeordnete Elemente gibt, die versagen (und dass sie den Fehler an ihre übergeordneten weitergeben). Der Tokyo-Cluster ist auf drei Personen konfiguriert. Der Prozentsatz ist für die Sicherungsserver in Tokyo und Tokyo für jeden Cluster unterschiedlich (50 % bzw. 34 %). Wie Sie sehen können, wirkt sich der Fehler des Sicherungsservers in Tokyo und Tokyo, auch wenn er „Rot – Kritisch“ ist, unterschiedlich auf die übergeordneten Elemente aus. Der Okay-Cluster bleibt grün, obwohl der Tokyo-Clusterfehler „Orangen schwerwiegend“ ist.

Klicken Sie auf einen Service oder ein CI, um die zugehörigen Warnungen anzuzeigen. Wenn Sie beispielsweise auf den allgemeinen Anwendungsservice klicken, werden die zugehörigen Warnungen im Warnungsbereich unter der Zuordnungsansicht angezeigt, wenn Sie **Warnungen**auswählen. Die aufgeführten Warnungen beziehen sich auf den ausgewählten Service. Warnungen von untergeordneten Services werden aufgelistet, wenn diese Services ausgewählt werden.

Die folgenden Auswirkungsfelder werden angezeigt, wenn Sie **Auswirkung**auswählen.

Einschluss

Bestimmt die Auswirkung auf Entitäten mit einer Beziehung vom Typ „Contains“ (Enthält). Diese Regel ist schreibgeschützt.

Infrastrukturabhängigkeiten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bestimmung der Definition der Wirkungsausbreitung für CIs in Infrastrukturbeziehungen.

CI-Anwendungsservice

Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Anwendungsservices sind.

CI-Auswirkung

Gilt für Anwendungsservices. Bestimmung der Beziehung zwischen Servicemitgliedern. Die Auswirkung von untergeordneten auf übergeordnete CIs ist immer 100 %. Zum Beispiel wird der Schweregrad der Auswirkungen auf die übergeordnete Ebene vom untergeordneten CI mit dem höchsten Schweregrad abgeleitet.

Übergeordnetes CI in Anwendung

Auswirkungen werden nur für die übergeordnete Entität festgelegt.

Netzwerkpfad

Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines klassischen Netzwerks sind.

Mitglied in OS-Cluster

Bestimmung, wie sich die Mitglieder des Host-Clusters auf Basis eines Prozentsatzes oder der Anzahl der Clustermitglieder auf den Gesamtstatus des Clusters auswirken. Wenn ein Cluster mit drei Hosts beispielsweise **60 % Einfluss** erfordert, um den Schweregrad **„Schwerwiegend“**festzulegen, hat jedes Mitglied **20 % Einfluss** (60% geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn zwei oder mehr Clustermitglieder den Schweregrad **Schwerwiegend** aufweisen. Das gesamte Cluster gilt auch als inaktiv.

Speicherpfad

Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Speichernetzwerks sind.

Eigenschaften

Neben Auswirkungsregeln können Sie Eigenschaften für die Auswirkungsberechnung konfigurieren.

Konfigurieren Sie diese Eigenschaften nach Bedarf:

Eigenschaften der Auswirkungsberechnung

Eigenschaftsname	Beschreibung
`evt_mgmt.impact_calculation.alert_group_support`	Aktiviert die Unterstützung von Warnungsgruppen
`evt_mgmt.impact_maintenance.sleep_time_sec`	Mindestzeit in Sekunden für die Überprüfung der CI-Wartung: überprüft sowohl das Feld „Status“ des CI als auch alle Change-Anforderungszeitpläne für das CI
`evt_mgmt.impact_calculation.alert_copy_delay`	Die Verzögerung nach dem Erstellen oder Aktualisieren einer Warnung, bevor sie für die Auswirkungsberechnung und -gruppierung verwendet wird. Wird dazu verwendet, verspätete Eingänge oder langsame Geschäftsregeln zu kompensieren, die in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften der Auswirkungsberechnung (Fortsetzung)

Eigenschaftsname	Beschreibung
	Tabelle em_alert definiert sind. Standard = 2000 ms. Wird verwendet, wenn Warnungen und Events nacheinander verarbeitet werden (wenn die Eigenschaft `evt_mgmt.max_objs_in_alert_query` nicht definiert oder auf **1** festgelegt ist)
`evt_mgmt.impact_calculation.alert_copy_delay_msec_in_batch_msec`	Die Verzögerung nach dem Erstellen oder Aktualisieren einer Warnung, bevor sie für die Auswirkungsberechnung und -gruppierung verwendet wird. Wird dazu verwendet, verspätete Eingänge oder langsame Geschäftsregeln zu kompensieren, die in der Tabelle em_alert definiert sind. Standard = 30000 ms. Wird in großen Kundenumgebungen mit hohem Datenverkehr verwendet, wenn Warnungen und Ereignisse in Batches verarbeitet werden (wenn die Eigenschaft `evt_mgmt.max_objs_in_alert_query` auf einen Wert größer als **1**festgelegt ist).

Servicezuordnungen verstehen

Servicezuordnungen zeigen aktive Warnungen für CIs und die Beziehungen zwischen CIs an. Durch das Anzeigen dieser Informationen können Sie die Quelle von Warnungen besser verstehen und Abhilfemaßnahmen ergreifen. Die Servicezuordnung ist für alle Anwendungsservices verfügbar.

Über Servicezuordnungen

Eine Servicezuordnung zeigt Warnungen mit betroffenen CIs und CI-Abhängigkeiten an. Beispielsweise werden Änderungen an einer Verbindung zwischen einem Host und einem Hypervisor auf der Servicezuordnung angezeigt. Wenn sich Definitionen von Servicezuordnungen ändern, werden Servicezuordnung, Warnung und Auswirkungsinformationen entsprechend aktualisiert. Seit Release Quebec wurde die Transparenz erhöht. Wenn die Warnung an den Einstiegspunkt gebunden ist, identifiziert die Servicezuordnung ein Problem am Einstiegspunkt.

Hinweis: Für die Einstiegspunkte in der Servicezuordnung werden keine Warnungen angezeigt.

Sie können eine Servicezuordnung über diese Orte öffnen:

- In der Liste der Anwendungsservices können Sie Servicezuordnungen für Anwendungsservices anzeigen.
- In der Liste „Überwachte Services“ können Sie Servicezuordnungen für überwachte Services anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Symbole werden in Servicezuordnungen verwendet. Die Formen der Symbole unterscheiden sich bei Anwendungsservices geringfügig.

Symbole der Servicezuordnung

Symbol	Beschreibung
( )	Stellt Anwendungen wie MicrosoftMicrosoft Azure Event Hubs IIS- oder SQL-Server dar
( )	Stellt physische sowie virtuelle VM-Computer und -Server dar
( )	Stellt den Startpunkt des Netzwerks dar. Beispielsweise werden Layer-3-Geräte oben auf der Zuordnung angezeigt, und verbundene Software und Services werden am Ende der Zuordnung angezeigt.
( )	Zeigt die Anzahl der redundanten CIs an
( )	Zeigt die Arbeitsauslastung zwischen Computern an.
( )	Der graue Connector zeigt eine Beziehung zwischen CIs an.
()	Jedes CI ohne aktives Warnungsfeld stellt ein Netzwerk-CI dar. Ein graues Feld stellt ein CI ohne aktive Warnungen dar. Informationen zum CI sind ausgeblendet.
( )	Blendet mehrere CIs aus, die als redundant gekennzeichnet sind
()	Ein betroffenes CI zeigt die Farbe an, die den Schweregrad des dem CI zugeordneten Alarms darstellt. • **Kritisch (rot)**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. • **Schwerwiegend (orange)**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten. • **Geringfügig (gelb)**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. • **Warnung (blau)**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. • **OK (grün)**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig. • **Keine Farbe**: Keine aktiven Warnungen.
( )	Stellt Fiber Channel, Festplatten oder andere Datenspeichergeräte dar
( )	Stellt zugehörige Webservices für das Netzwerk dar, z. B. NGINX- oder JBoss-Webserver.

Hinweis: Einstellungen für Sitzungszeitüberschreitungen gelten nicht für diesen Bildschirm. Die Sitzung bleibt verbunden, auch wenn keine menschliche Interaktion stattfindet. Wenn diese Einstellung ein Problem darstellt, melden Sie sich entweder ab oder schließen die aktive Registerkarte im Browser.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Warnungsauswirkungsberechnung

Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen

Anzeigen der Auswirkungsstruktur

Die Auswirkungsstruktur zeigt die Beziehungen zwischen CIs und die relative prozentuale Auswirkung für jedes untergeordnete CI an. Diese Informationen sind für erkannte Services und Anwendungsservices verfügbar.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

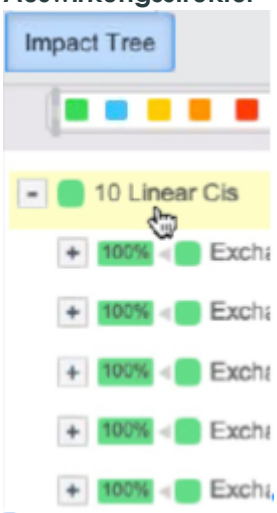
Die Auswirkungsstruktur zeigt das Ergebnis von Auswirkungsregeln für über- und untergeordnete CI-Beziehungen. Die Struktur stellt eine Servicezuordnung mit CIs aus der Zuordnung von Servicekonfigurationselementen [svc_ci_assoc] dar. Wenn zugehörige CIs verbunden, aber nicht Teil der Servicezuordnung sind, kann die Auswirkung für die zugehörigen CIs auch in der Auswirkungsstruktur angezeigt werden.

Die Zahlen oder Prozentsätze in einem übergeordneten CI fassen den Gesamtschweregrad basierend auf Warnungen von untergeordneten CIs zusammen. Der übergeordnete Schweregrad basiert auf Auswirkungsregelberechnungen.

Im folgenden Video-Tutorial erfahren Sie mehr über Auswirkungsstrukturen.

Ereignismanagement Teil 2 | Auswirkungsstruktur

Auswirkungsstruktur



Prozedur

1. Öffnen Sie die Servicezuordnung für den Service aus der Liste Anwendungsservice.
   a. Navigieren zu **Ereignismanagement** > **Services** > **Anwendungsservices**.
   b. Klicken Sie neben dem **Service auf Service anzeigen**.
2. Klicken Sie auf der Servicezuordnung auf ein CI mit einer Farbe des Schweregrads.
3. Klicken Sie auf die Registerkarte **Auswirkung**.
4. Erweitern Sie auf der Registerkarte **Auswirkungsstruktur** im Seitenbereich das übergeordnete CI, und klicken Sie auf das CI, das Warnungen generiert hat.
5. Verwenden Sie die Farbe des Schweregrads, um CIs zu finden, die Warnungen enthalten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kritisch (rot)**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor.
- **Schwerwiegend (orange)**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten.
- **Geringfügig (gelb)**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten.
- **Warnung (blau)**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist.
- **OK (grün)**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig.

6. Führen Sie einen oder mehrere der folgenden Schritte aus.

Option	Bezeichnung
Anpassen der Auswirkungsregeln	**a.** Klicken Sie auf die Registerkarte **Auswirkung**. **b.** Überprüfen Sie die Auswirkungsregeln, und passen Sie sie bei Bedarf an.
Nachbesserung einer Warnung	**a.** Klicken Sie auf die **Warnungen**. **b.** Klicken Sie mit der rechten Maustaste auf die Warnung, und wählen Sie **Korrektur ausführen** aus.

Netzwerkpfade, die in der Auswirkungsstruktur angezeigt werden, können eine große Menge an Ressourcen verbrauchen, was die Systemleistung beeinträchtigt. Um zu verhindern, dass Netzwerkpfade in der Auswirkungsstruktur angezeigt werden, navigieren Sie zu **Systemeigenschaften** > **Alle Eigenschaften** und legen Sie die Eigenschaft *evt_mgmt.network_path_excluded* auf **true** fest.

Informationen zum Anzeigen der Auswirkungsstruktur mit Service Operations-Arbeitsbereich finden Sie unter Zeigen Sie mit die Auswirkungsstruktur an Service Operations-Arbeitsbereich.

Anpassen der Auswirkungsregeln für ein CI

Konfigurieren Sie Auswirkungsregeln, um die Berechnung der Auswirkung für Discovery-Services und manuelle Servicesanzupassen. Die Auswirkungsregeln aktualisieren die allgemeine Warnung und zeigen die Auswirkung auf zugehörige CIs an. Wenn Sie Auswirkungsregeln ändern, gelten die Updates für den Schweregrad von Warnungen an Stellen wie dem Dashboard Ereignismanagement und dem Betreiber-Arbeitsbereich.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können die Auswirkungsregeln von CIs in der Zuordnung Anwendungsservice eines Service anzeigen und anpassen.

Hinweis: Das Ereignismanagement-Dashboard wird für neue Instanzen im Paris-Release nicht unterstützt. Instanzen, die von einem Release vor Orlando aktualisiert wurden und das Ereignismanagement Dashboard verwenden, können dies jedoch weiterhin tun.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie die Anwendungsservicezuordnung entweder über das Dashboard Ereignismanagement oder über die Liste Anwendungsservice.

Option	Bezeichnung
Über das Ereignismanagement-Dashboard	**a.** Navigieren zu **Ereignismanagement** > **Dashboard**. **b.** Doppelklicken Sie auf die Kachel der Anwendungsservices.
Über die Liste Anwendungsservice	**a.** Navigieren zu **Ereignismanagement** > **Services** > **Anwendungsservices**. **b.** Klicken Sie neben den Anwendungsservices **auf Karte anzeigen**.

2. Klicken Sie in der Anwendungsservicezuordnung auf ein CI.
3. Klicken Sie unterhalb der Karte auf die Registerkarte **Auswirkung**, und passen Sie dann die Auswirkungsregeln entsprechend an.

Auswirkungsregeln

Feld	Beschreibung
Name	Der Name der Auswirkungsregel. ◦ **Mitglied in Anwendungscluster**: Bestimmung, wie sich die Mitglieder des Anwendungsclusters auf die Gesamtwirkung des Clusters auswirken. Wenn beispielsweise ein Cluster mit drei Mitgliedern **einen Einfluss von 90 %** benötigt, um den Schweregrad für den gesamten Cluster auf **„Schwerwiegend“**festzulegen, hat jedes Mitglied **30 % Einfluss** (90 % geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn alle drei Mitglieder den Schweregrad **Schwerwiegend** aufweisen. **Hinweis:** Informationen zum Konfigurieren eines manuellen Clusters finden Sie unter Konfigurieren Sie einen manuellen Cluster ◦ **CI Anwendungsservice**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Anwendungsservices sind. ◦ **CI-Auswirkung**: Gilt für Anwendungsservices. Bestimmung der Beziehung zwischen Servicemitgliedern. Die Auswirkung von untergeordneten auf übergeordnete CIs ist immer 100 %. Zum Beispiel wird der Schweregrad der Auswirkungen auf die übergeordnete Ebene vom untergeordneten CI mit dem höchsten Schweregrad abgeleitet. ◦ **Übergeordnetes CI in Anwendung**: Auswirkungen werden nur für die übergeordnete Entität festgelegt. ◦ **Inclusion**: Bestimmt die Auswirkung auf Entitäten mit einer Beziehung vom Typ „Contains“ (Enthält). Diese Regel ist schreibgeschützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ **Infrastrukturabhängigkeiten**: Bestimmung der Definition der Wirkungsausbreitung für CIs in Infrastrukturbeziehungen. ◦ **Netzwerkpfad**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines klassischen Netzwerks sind. ◦ **Mitglied in OS-Cluster**: Bestimmung, wie sich die Mitglieder des Host-Clusters auf Basis eines Prozentsatzes oder der Anzahl der Clustermitglieder auf den Gesamtstatus des Clusters auswirken. Wenn ein Cluster mit drei Hosts beispielsweise **60 % Einfluss** erfordert, um den Schweregrad **„Schwerwiegend“**festzulegen, hat jedes Mitglied **20 % Einfluss** (60% geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn zwei oder mehr Clustermitglieder den Schweregrad **Schwerwiegend** aufweisen. Das gesamte Cluster gilt auch als inaktiv. ◦ **Speicherpfad**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Speichernetzwerks sind.
Auswirkung auf	Der gültige Servicetyp für diese Auswirkungsregel. ◦ **Anwendungsservice**: Die Auswirkungsregel gilt für einen Anwendungsservice. ◦ **Übergeordnet**: Die Auswirkungsregel gilt für das übergeordnete CI.
Einfluss	Der Wert, der die Festlegung der Auswirkungsregel für das übergeordnete Element zulässt. Legen Sie einen Wert für das übergeordnete Elementfest. Dieses Feld arbeitet mit dem Feld **Einflusseinheiten** zusammen.
Einflusseinheiten	Die Maßeinheit, die die Auswirkung auf das übergeordnete Element anzeigt. Legen Sie den höchsten Wert für das übergeordnete CI fest. Legen Sie niedrigere Werte für jedes untergeordnete CI fest. Wenn Warnungen für mehrere untergeordnete CIs auftreten, berechnet Ereignismanagement die Summe der **Einflusseinheiten** für jedes untergeordnete Element. Wenn die Summe den übergeordneten **Einflusseinheitswert** überschreitet, erhält das übergeordnete Element den höchsten Schweregrad im Satz. Dieses Feld arbeitet mit dem Feld **Einfluss** zusammen. ◦ **Prozent**: Wenn der Prozentsatz den **Einflusswert** überschreitet, wenden Sie die Auswirkung auf das übergeordnete Element an. ◦ **Nummer**: Wenn die Nummer den **Einflusswert** überschreitet, wenden Sie die Auswirkung auf das übergeordnete Element an. Beispielsweise können Sie die übergeordneten **Einflusseinheiten** auf **100 %** und die untergeordneten CIs auf diese Werte festlegen: ▪ Untergeordnetes Element 1: 34% ▪ Untergeordnetes Element 2: 34% ▪ Untergeordnetes Element 3: 34% ▪ Untergeordnetes Element 4: 70 % Wenn Warnungen für die untergeordneten Elemente 3 und 5 den Schweregrad „Kritisch“ aufweisen, wird der Schweregrad des übergeordneten Elements auf „Kritisch“ festgelegt, da die Summe größer als 100 % ist (34% + 70 % = 104%).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Auswirkung wenn kritisch	Die alternative Auswirkung, die verwendet wird, wenn der berechnete Schweregrad „Kritisch“ ist. Wenn die Spalte rechts von **Auswirkung, wenn kritisch** einen höheren Schweregrad aufweist, aktualisieren Sie alle Spalten ganz rechts mit dem gleichen oder einem niedrigeren Schweregrad als **Auswirkung, wenn kritisch**. Um sicherzustellen, dass die Topologie und die Auswirkungsstruktur die Auswirkung genau anzeigen, aktualisieren Sie jede Spalte immer entsprechend. ◦ **Kritisch**: Rot (höchster Schweregrad). ◦ **Schwerwiegend**: Orange. ◦ **Geringfügig**: Gelb. ◦ **Warnung**: Blau (niedrigster Schweregrad).
Auswirkung wenn größer	Die alternative Auswirkung, die verwendet wird, wenn der berechnete Schweregrad **Schwerwiegend** ist. Wenn die Spalte rechts von **Auswirkung, wenn schwerwiegend** einen höheren Schweregrad aufweist, aktualisieren Sie alle Spalten ganz rechts mit dem gleichen oder einem niedrigeren Schweregrad als **Auswirkung, wenn schwerwiegend**. Um sicherzustellen, dass die Topologie und die Auswirkungsstruktur die Auswirkung genau anzeigen, aktualisieren Sie jede Spalte immer entsprechend. ◦ **Kritisch**: Rot (höchster Schweregrad). ◦ **Schwerwiegend**: Orange. ◦ **Geringfügig**: Gelb. ◦ **Warnung**: Blau (niedrigster Schweregrad).
Auswirkung, wenn geringfügig	Die alternative Auswirkung, die verwendet wird, wenn der berechnete Schweregrad **Geringfügig** ist. Steuert die Feldwerte rechts von diesem Feld. Wenn die Spalte **Auswirkung, wenn Warnung** einen höheren Schweregrad aufweist, verwenden Sie den Wert **Auswirkung, wenn geringfügig** für beide Felder. Um sicherzustellen, dass die Topologie und die Auswirkungsstruktur die Auswirkung genau anzeigen, aktualisieren Sie jede Spalte immer entsprechend. ◦ **Kritisch**: Rot (höchster Schweregrad). ◦ **Schwerwiegend**: Orange. ◦ **Geringfügig**: Gelb. ◦ **Warnung**: Blau (niedrigster Schweregrad).
Auswirkung, wenn Warnung	Die alternative Auswirkung, die verwendet wird, wenn der berechnete Schweregrad **Warnung** ist. Um sicherzustellen, dass die Topologie und die Auswirkungsstruktur die Auswirkung genau anzeigen, müssen die Spalten auf der linken Seite höhere Schweregrade aufweisen. ◦ **Kritisch**: Rot (höchster Schweregrad). ◦ **Schwerwiegend**: Orange. ◦ **Geringfügig**: Gelb. ◦ **Warnung**: Blau (niedrigster Schweregrad).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Überprüfen Sie die Änderungen in der Auswirkungsstruktur. Wenn Sie beispielsweise eine Zahl oder einen Prozentsatz für den Einfluss von untergeordneten CIs geändert haben, überprüfen Sie die Aktualisierungen der Auswirkungsstruktur entsprechend.

Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen

Sie können Servicezuordnungen anzeigen, um aktive Warnungen für CIs und die Beziehungen zwischen CIs anzuzeigen. Durch das Anzeigen dieser Informationen können Sie die Quelle von Warnungen besser verstehen und Abhilfemaßnahmen ergreifen. Die Servicezuordnung ist für alle Anwendungsservices verfügbar.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Servicezuordnung über diese Orte öffnen:

- In der Liste der Anwendungsservices können Sie Servicezuordnungen für Anwendungsservices anzeigen.
- In der Liste „Überwachte Services“ können Sie Servicezuordnungen für überwachte Services anzeigen.

Prozedur
1. Öffnen Sie eine Anwendungsservice-Zuordnung:
   a. Navigieren zu **Ereignismanagement** > **Services** > **Anwendungsservices**.
   b. Klicken Sie neben dem Service auf **Zuordnung anzeigen**.
2. Führen Sie einen oder mehrere der folgenden Schritte aus.

Option	Aktion
Anzeige von Warnungen für ein CI nach Typ und Schweregrad	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie unterhalb der Karte auf die Registerkarte **Warnungen**, und überprüfen Sie die aufgelisteten Warnungen.
Anzeige von Änderungen an einem CI in einem erkannten Service	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie unterhalb der Zuordnung auf die Registerkarte **Änderungen**.
Warnungsbindungen an CIs anzeigen	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie auf das Menüsymbol für zusätzliche Aktionen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	, um den Indikator **Betroffene CIs** anzuzeigen. **c.** Klicken Sie unterhalb der Zuordnung auf die Registerkarte **Betroffene CIs**.
Anzeige von Dateieigenschaften	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie im Seitenbereich auf die Registerkarte **Eigenschaften**, und überprüfen Sie Informationen zum CI. **c.** Wenn Sie detailliertere Informationen anzeigen möchten, scrollen Sie zum Ende des Bereichs, und klicken Sie auf **Detaillierte Eigenschaften**.
Auswirkungsregeln für ein CI anzeigen	In der Servicezuordnung: **a.** Klicken Sie auf ein CI mit einem Schweregrad. **b.** Klicken Sie unterhalb der Servicezuordnung auf die Registerkarte **Auswirkung**, und überprüfen Sie die aufgeführten Auswirkungsregeln.
Anzeigen von Warnungsdetails für Netzwerke oder Speicher für einen Service	In der Servicezuordnung: **a.** Klicken Sie mit der rechten Maustaste auf einen Pfad zwischen CIs. **b.** Wählen Sie **Netzwerkpfad anzeigen** oder **Speicherpfad anzeigen**.
Anzeigen weiterer Informationen für CIs	Im Header der Servicezuordnung:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	a. Klicken Sie auf das Menüsymbol für zusätzliche Aktionen . **b.** Um auf Wunsch weitere Informationen anzuzeigen, können Sie die **Zuordnungsindikatoren** auswählen.
Nachbessern eines CIs	Klicken Sie in der Topologie mit der rechten Maustaste auf das CI, und wählen Sie dann **Optionen für die Fehlerkorrektur**.

Zugehörige Informationen

Warnungsauswirkungsberechnung

Servicezuordnungen verstehen

Erstellen einer Infrastrukturbeziehung für zugehörige CIs

Infrastrukturbeziehungen zeigen CIs, die mit einem Anwendungsservice verbunden sind, aber keine erforderlichen Teile des Services sind. Infrastrukturbeziehungen sind nur für Anwendungsservices verfügbar.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie eine CI-Infrastrukturbeziehung erstellen, werden die Informationen in der Tabelle „Infrastrukturbeziehungen“ [em_impact_infra_rel_def] gespeichert. Wenn Warnungen generiert werden, begleitet das zugehörige CI die Anwendungsservice-Informationen im Dashboard Ereignismanagement und in der Auswirkungsstruktur. Zusätzliche Informationen für die zugehörigen CIs werden nur in einer zugehörigen Abhängigkeitsansichtszuordnung für den Anwendungsservice angezeigt. Die folgenden Standard-Infrastrukturbeziehungen sind verfügbar.

Standard-Infrastrukturbeziehungen

Infrastrukturbeziehung	Auswirkungsregel	Beschreibung
cmdb_ci_appl	Mitglied in OS-Cluster	Zeigt die Auswirkung von Warnungen zwischen Hardware- und Softwareanwendungen an.

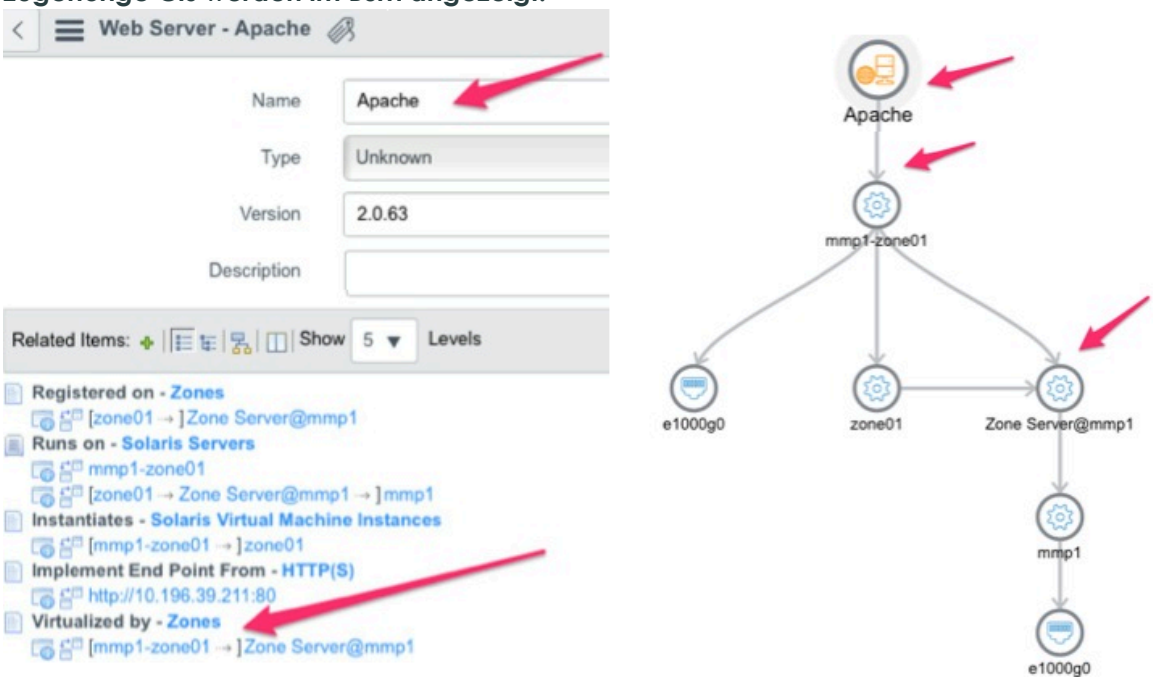
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-Infrastrukturbeziehungen (Fortsetzung)

Infrastrukturbeziehung	Auswirkungsregel	Beschreibung
cmdb_ci_esx_server	Infrastrukturabhängigkeiten	Zeigt die Auswirkung von Warnungen zwischen VCenter und ESX-Clustern an.
cmdb_ci_kvm	Infrastrukturabhängigkeiten	Zeigt die Auswirkung der Warnung auf die Linux-Kernel-basierte Virtual Machine-Konnektivität (KVM) an.
cmdb_ci_vm_zones	Infrastrukturabhängigkeiten	Zeigt die Auswirkung von Warnungen auf die Solaris-VM-Zonen an.

Beispielsweise fügt Ereignismanagement basierend auf der Infrastruktur-Beziehungsdefinition cmdb_ci_vm_zones ZoneServer@mmp1 dem Anwendungsservice hinzu. Die Containment-Regel verwaltet den Schweregrad der Auswirkung auf Warnungen.

Zugehörige CIs werden im BSM angezeigt.



Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Infrastrukturbeziehungen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

Formular Infrastrukturbeziehungen

Feld	Beschreibung
Untergeordneter Typ	Die Tabelle, die Daten zur untergeordneten Entität enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übergeordneter Typ	Die Tabelle, die Daten zur übergeordneten Entität enthält.
Beziehungstyp	Die Beziehung zwischen den untergeordneten und übergeordneten Entitäten.
Auswirkungsrichtung	Die Auswirkungsrichtung, die in der Anwendungsservicezuordnung angezeigt werden soll. ◦ **Vom untergeordneten zum übergeordneten Element**: Wenn sich eine Warnung auf ein untergeordnetes Element bezieht, die Auswirkung auf das übergeordnete Element anzeigen. ◦ **Vom übergeordneten zum untergeordneten Element**: Wenn sich eine Warnung auf ein untergeordnetes Element bezieht, die Auswirkung auf das übergeordnete Element anzeigen.
Auswirkungsregel	Die Auswirkungsregel zum Berechnen von Infrastrukturbeziehungen: ◦ **BS-Clustermitglied** : Bestimmung, wie sich die Mitglieder des Host-Clusters auf Basis eines Prozentsatzes oder der Anzahl der Clustermitglieder auf den Gesamtstatus des Clusters auswirken. Wenn ein Cluster mit drei Hosts beispielsweise **60 % Einfluss** erfordert, um den Schweregrad **„Schwerwiegend“**festzulegen, hat jedes Mitglied **20 % Einfluss** (60% geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn zwei oder mehr Clustermitglieder den Schweregrad **Schwerwiegend** aufweisen. Das gesamte Cluster gilt auch als inaktiv. ◦ **Mitglied in Anwendungscluster** : Bestimmung, wie sich die Mitglieder des Anwendungsclusters auf die Gesamtwirkung des Clusters auswirken. Wenn beispielsweise ein Cluster mit drei Mitgliedern **einen Einfluss von 90 %** benötigt, um den Schweregrad für den gesamten Cluster auf **„Schwerwiegend“**festzulegen, hat jedes Mitglied **30 % Einfluss** (90 % geteilt durch 3). Der Schweregrad des gesamten Clusters kann nur dann in **Schwerwiegend** geändert werden, wenn alle drei Mitglieder den Schweregrad **Schwerwiegend** aufweisen. ◦ **Infrastrukturabhängigkeiten** : Bestimmung der Definition der Wirkungsausbreitung für CIs in Infrastrukturbeziehungen. ◦ **CI-Anwendungsservice**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Anwendungsservices sind. ◦ **Übergeordnetes CI in Anwendung**: Auswirkungen werden nur für die übergeordnete Entität festgelegt. ◦ **Inclusion**: Bestimmt die Auswirkung auf Entitäten mit einer Beziehung vom Typ „Contains“ (Enthält). Diese Regel ist schreibgeschützt. ◦ **Netzwerkpfad**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines klassischen Netzwerks sind. ◦ **Speicherpfad**: Bestimmung der Auswirkungen auf übergeordnete oder untergeordnete Entitäten, die Teil eines Speichernetzwerks sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ **CI-Auswirkung** : Gilt für Anwendungsservices. Bestimmung der Beziehung zwischen Servicemitgliedern. Die Auswirkung von untergeordneten auf übergeordnete CIs ist immer 100 %. Zum Beispiel wird der Schweregrad der Auswirkungen auf die übergeordnete Ebene vom untergeordneten CI mit dem höchsten Schweregrad abgeleitet.

4. Klicken Sie auf **Absenden**.

Auswirkung des untergeordneten Services auf den übergeordneten Service anzeigen

In der Zuordnungsansicht eines Anwendungsservices wird der Schweregrad eines untergeordneten Services an den übergeordneten Service weitergegeben.

Vorbereitungen

Erforderliche Rolle:

- für Anwendungsservices, evt_mgmt_admin
- für erkannte Services, service_mapping_admin

Warum und wann dieser Vorgang ausgeführt wird

In der Zuordnungsansicht eines Anwendungsservices können Sie sehen, dass der Schweregrad eines untergeordneten Services an den übergeordneten Service weitergegeben wird.
Ein Anwendungsservice wird durch den Schweregrad von Warnungen beeinflusst, die ihm direkt zugeordnet sind, und von Warnungen auf den CIs, die sich im Service befinden. Wenn der Schweregrad eines untergeordneten Services höher als der des übergeordneten Services ist, wird für den übergeordneten Service in der Zuordnungsansicht der Schweregrad des untergeordneten Services angezeigt. In der Kartenansicht werden die CIs in der Liste **Auswirkungsstruktur** angezeigt. Die Farbe der CIs zeigt den Schweregrad der Warnung an. Der untergeordnete Service ist auch von Anwendungsservices betroffen, die sich unter ihm befinden.

Beispiel, in dem der übergeordnete Service den Schweregrad des untergeordneten Services anzeigt

Wenn eine Schleife entsteht, z. B. durch Verbindung eines übergeordneten Services mit einem untergeordneten Service, kann diese Beziehung in der Zuordnungsansicht angezeigt werden. Die Auswirkung dieser Schleife wird nicht berechnet, und die Beziehung wird in der Auswirkungsstruktur nicht angezeigt. Beispiel: Es gibt drei CIs, A, B und C, wobei C ein Subservice von B und B ein Subservice von A ist. Die Beziehung des mit C verbundenen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

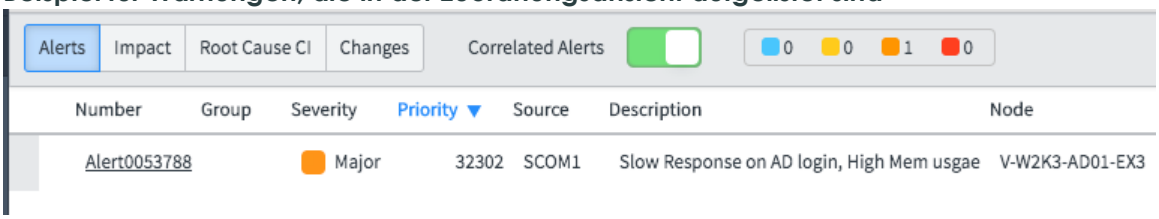
Services von A wird in der Zuordnungsansicht angezeigt. Diese Beziehung wird jedoch nicht in der Auswirkungsstruktur angezeigt.

Hinweis: Eine Nachricht wird im Systemfehlerprotokoll im folgenden Format angezeigt, wobei sich die sys_id des Services und der Knoten entsprechend ändern: `Schleife in Service-ID: [sysId] und Knoten: [sysId] gefunden. Diese Beziehung wird entfernt, um Auswirkungsschleifen zu vermeiden.`

Beispiel: `Schleife gefunden in Service-ID: 409d4fd59f030200fe2ab0aec32e705c und Knoten: df5cf6159f030200fe2ab0aec32e70a2. Diese Beziehung wird entfernt, um Auswirkungsschleifen zu vermeiden.`

Klicken Sie auf einen Service oder ein CI, um die zugehörigen Warnungen anzuzeigen. Wenn Sie beispielsweise auf den allgemeinen Anwendungsservice klicken, werden die zugehörigen Warnungen im Warnungsbereich unter der Zuordnungsansicht angezeigt. Die aufgeführten Warnungen beziehen sich auf den ausgewählten Service. Warnungen von untergeordneten Services werden aufgelistet, wenn diese Services ausgewählt werden.

Beispiel für Warnungen, die in der Zuordnungsansicht aufgelistet sind



Prozedur

Öffnen Sie eine Anwendungsservice-Zuordnung:

a. Navigieren zu **Ereignismanagement** > **Services** > **Anwendungsservices**.

b. Wählen Sie neben dem Service **Service anzeigen**.

c. Wählen Sie im rechten Bereich **Auswirkungsstruktur**aus.

d. Wählen Sie im unteren Bereich **Auswirkung**.

Ergebnisse

In der Servicezuordnung können Sie visuell überprüfen, ob für die Serviceintegrität des untergeordneten Service ein Rollup zum übergeordneten Service durchgeführt wird. Unter des Symbols eines betroffenen CI befindet sich ein farbiger Balken, der den Schweregrad der Warnung darstellt. Diese Farbleiste wird auch in der unteren Leiste des übergeordneten Services angezeigt. Für die manuelle Clusterkonfiguration können Sie Anwendungsauswirkung und Mitglied im Anwendungscluster ändern.

Zugehörige Informationen

Zuordnungssegmente auf andere Anwendungsservices übertragen

Konfigurieren Sie einen manuellen Cluster

Warnungsauswirkungen bei der Selektierung von Warnungen anpassen

Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen

Ursachenanalyse (RCA)

Verkürzen Sie die durchschnittliche Zeit bis zur Reparatur (MTTR), indem Sie die Ursache einer Warnung ermitteln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

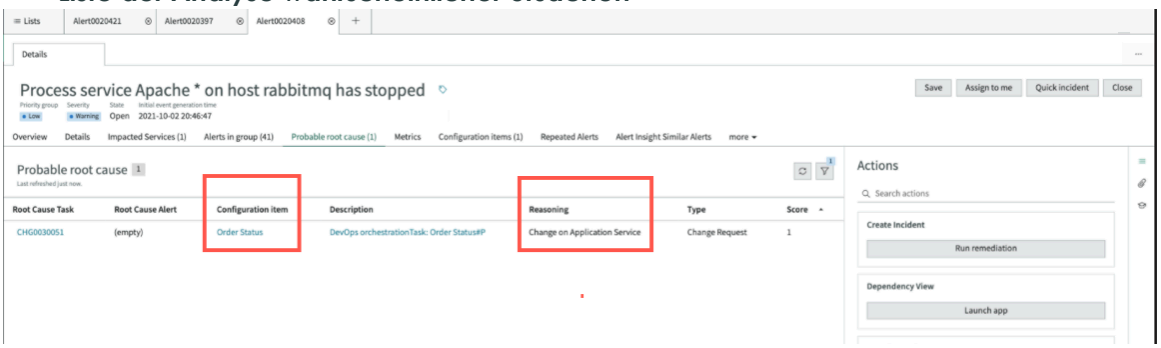
Die Ursachenanalyse (RCA) bietet eine Liste der wahrscheinlichen Ursachen für Warnungen. Diese Funktion verwendet vorhandene Daten in IT Service Management, um die Ursache eines Problems zu ermitteln.

RCA berücksichtigt drei Faktoren: Warnungen, Configuration Item (CI)-Topologie und Change-Anforderungen auf den CIs. Sie extrahiert CIs aus Warnungen oder Warnungsgruppen und analysiert die CI-Beziehungen in der CMDB. Anschließend werden verschiedene konfigurierbare Filter verwendet, um relevante Change-Anforderungen in den CIs als mögliche Ursachen zu berücksichtigen.

Change-Anforderungen können sich auf einen Zeitrahmen oder ein CI, den zugehörigen Anwendungsservice oder die darauf installierte Software beziehen. Beispielsweise muss ein CI aktualisiert oder ein Sicherheitspatch installiert werden. Eine Change-Anforderung für ein CI kann sich auf andere CIs auswirken.

RCA ordnet die Warnungen und Change-Anforderungen den CIs zu. Anschließend wird die Ursachenpunktzahl berechnet, eine logische Punktzahl, die zum Sortieren wahrscheinlicher Ursachen verwendet wird. Die Berechnung dieser Punktzahl basiert auf Change-Anforderungen für CIs und auf Warnungen für ein wichtiges CI, das als Topologieursprungs-CI bezeichnet wird. Die Punktzahl der Ursache bestimmt, wie RCA die Liste der wahrscheinlichen Ursachen ausfüllt.

Liste der Analyse wahrscheinlicher Ursachen



Standardmäßig zeigt die Liste die fünf wahrscheinlichsten Ursachen mit der höchsten Punktzahl an. Sie listet die mit den einzelnen Warnungen verbundenen CIs und den Grund auf, aus dem sie von RCA als mögliche Ursachen identifiziert wurden.

Die Bewertung für wahrscheinliche Ursachen wird durch die folgenden Kriterien in der angegebenen Reihenfolge bestimmt (niedrigere Nummer = höhere Priorität):

1. Change für ein CI, das aus einer Topologie stammt
2. Change für ein zugehöriges CI, das aus einer Topologie stammt
3. Change für ein CI
4. Change für ein zugehöriges CI/Change für einen Anwendungsservice/Change für Software
5. Warnung für das CI, das aus einer Topologie stammt

Zum Deaktivieren der Funktion „Analyse der wahrscheinlichen Ursache“ müssen Sie die Eigenschaft *sa_analytics.disable_prc* erstellen und den Wert auf `true` festlegen. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

RCA-Einstellungen anpassen

Ändern Sie die Standardeinstellungen, die das RCA-Verhalten bestimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Standardfiltereinstellungen steuern, welche Change-Anforderungen von RCA als mögliche Ursachen angesehen werden. Sie können bestimmte Standardeinstellungen ändern, um z. B. RCA Standard-Change-Anforderungen zu ignorieren.

Sie können auch die Anzahl der in der Liste angezeigten wahrscheinlichen Ursachen ändern. Standardmäßig zeigt die Liste die fünf wahrscheinlichsten Ursachen mit der höchsten Punktzahl für die Ursache an.

Standardmäßig ist die RCA-Berechnung aktiviert. Sie können sie deaktivieren, indem Sie den Standardwert *sa_analytics.disable_prc* in „True“ ändern.

Prozedur
1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Führen Sie je nach Bedarf eine oder beide der folgenden Aktionen aus.
   - Ändern Sie die Standardfiltereinstellungen:
     a. Wählen Sie **Neu**aus.
     b. Geben Sie im Feld **Name** den Namen der Eigenschaft an, für die Sie die Standardeinstellung ändern möchten.

        Die neue Eigenschaft muss denselben Namen haben wie die zugehörige Eigenschaft in der Tabelle.

Eigenschaft	Beschreibung	Typ	Standardwert
sa_analytics.rca.default_category	Die Kategorien von Change-Anforderungen, die RCA als mögliche Ursache betrachtet.	String	" "
sa_analytics.rca.default_type	Die Typen von Change-Anforderungen, die RCA als mögliche Ursache betrachtet.	String	„Standard, Normal, Notfall“
sa_analytics.rca.default_state	Die Status von Change-Anforderungen, die RCA als mögliche Ursache betrachtet.	String	„-1,0,3,7,8,157“
sa_analytics.rca.default_interval_in_hours	Der Zeitraum in Stunden, in dem Change-Anforderungen aufgetreten sind, die RCA als mögliche Ursache ansieht.	int	168

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Geben Sie einen gültigen Wert für die Eigenschaft ein.

Hinweis: Der Wert, den Sie für die neue Eigenschaft festlegen, überschreibt den Standardwert für die zugehörige Eigenschaft.

◦ Ändern Sie die Anzahl der in der Liste angezeigten wahrscheinlichen Ursachen:

a. Suchen Sie die Eigenschaft *sa_analytics.rca_task_table_max_records*.

Name der Eigenschaft	Beschreibung	Typ	Standardwert
sa_analytics.rca_task_table_max_records	Die maximale Anzahl der in der Liste angezeigten wahrscheinlichen Ursachen:	int	5

b. Ersetzen Sie den Standardwert durch einen neuen gültigen Wert.

◦ Deaktivieren Sie RCA, indem Sie die Eigenschaft *sa_analytics.disable_prc* erstellen.

a. Wählen Sie **Neu**.

b. Füllen Sie das Formular mit den folgenden Werten aus.

Eigenschaftsname	Beschreibung	Typ	Wert
sa_analytics.disable_prc	Die wahrscheinliche Ursache wird deaktiviert.	Boolean	wahr

3. Klicken Sie auf **Absenden**.

Warnungsähnlichkeit

Das Finden von Warnungen, die der von Ihnen untersuchten Warnung ähnlich sind, kann helfen, Zeit bei der Fehlerbehebung zu sparen, indem Sie sehen, wie ähnliche Warnungen gelöst wurden.

Ähnliche Warnungen suchen

Die Ähnlichkeit von Warnungen wendet Natural Language Processing (NLP) basierend auf maschinellem Lernen (ML) Now Platform an, wie in Predictive Intelligence implementiert.

Die ML-Logik filtert irrelevante Informationen heraus und bietet weitere Informationen zum Verständnis der Ursache von Warnungen. Sie können Lösungen zur Lösung ähnlicher Warnungen und die wahrscheinliche Ursache anzeigen.

ML hilft bei der Suche nach ähnlichen Warnungen basierend auf dem Text in diesen Warnungsdatensatzfeldern:

- Konfigurationselement.Klasse
- Metrikname
- Beschreibung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche Warnungsinformationen

Wählen Sie im Warnungsarbeitsbereich die erforderliche Warnung aus, und klicken Sie auf **Insight**, um zusätzliche Informationen zur Warnung anzuzeigen.

Wählen Sie in der Liste Warnungen die erforderliche Warnung aus, und verwenden Sie die Registerkarten „Warnungseinblick“ auf der rechten Seite des Warnungsdatensatzes, um zusätzliche Informationen zur Warnung anzuzeigen. Zum Beispiel können Sie die letzten Warnungen für das aktuelle CI und ähnliche CIs anzeigen, um die beste Lösung für das Nachbessern und Lösen dieser Warnung zu finden.

Die Registerkarten für Warnungseinblick sind:

- Betroffene Services
- Flatternd
- Verlauf
- Aktivitäten
- Weitere Informationen
- Wiederholte Warnungen
- Ähnliche Warnungen
- CI-Incidents
- CI-Change Requests
- CI-Probleme
- Zugehörige Incidents
- Zugehörige Change Requests
- Zugehörige Probleme

Weitere Informationen zu den Registerkarten für Warnungseinblick finden Sie unter Informationen zu Warnungseinblick.

Ähnliche Warnungen suchen

Sie können Warnungen finden, die der derzeit untersuchten Warnung ähnlich sind. Sparen Sie Zeit bei der Fehlerbehebung, indem Sie ähnliche Warnungen überprüfen, um zu sehen, wie sie gelöst wurden.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Predictive Intelligence aktiv ist. Informationen zur Aktivierung dieses Plugins finden Sie unter Plugins aktivieren .

Stellen Sie sicher, dass die Eigenschaft `evt_mgmt.similarity_use_ml` auf `true` festgelegt ist.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

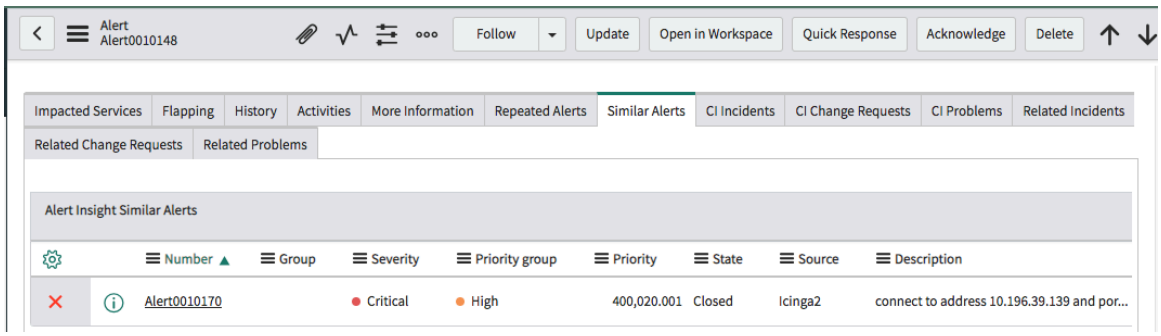
Sparen Sie Zeit beim Lösen der aktuellen Warnung, indem Sie überprüfen, wie ähnliche Warnungen gelöst wurden. Stellen Sie eine Lösungskonsistenz bereit, indem Sie ähnliche Warnungen auf dieselbe Weise lösen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

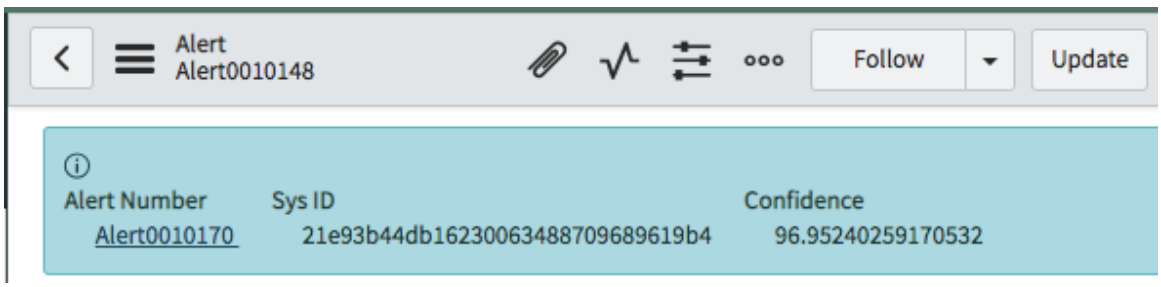
Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Klicken Sie in der Liste der Warnungen auf den Warnungsdatensatz, den Sie untersuchen möchten.
3. Klicken Sie im Warnungsdatensatz auf die Registerkarte **Ähnliche Warnungen**.
   Warnungen, die der untersuchten Warnung ähnlich sind, werden aufgelistet.



   Standardmäßig werden bis zu 10 ähnliche Warnungen aufgelistet. Sie können diesen Wert ändern, indem Sie die Eigenschaft `evt_mgmt.similarity_max_similar_alerts_shown` festlegen.

4. Wenn Sie einen Schwellenwert konfiguriert haben, klicken Sie im Bereich „Zugehörige Links“ auf **Ähnlichkeitsdetails anzeigen**.
   Die Sys-ID und das Confidence-Level jeder ähnlichen Warnung werden angezeigt. Das Confidence-Level zeigt an, wie die ähnliche Warnung mit den von Ihnen festgelegten Parametern übereinstimmt. Beispielsweise zeigt ein hoher Confidence-Prozentwert eine höhere Wahrscheinlichkeit einer Ähnlichkeit der Warnungen mit den von Ihnen festgelegten Werten an.



   Sie können den Wert des Schwellenwerts ändern, indem Sie die Eigenschaft `evt_mgmt.similarity_use_threshold` festlegen.

Ähnlichkeitslösungen

Mithilfe von Ähnlichkeitslösungen können Sie Machine Learning (ML) verwenden, um den Text in einem Datensatz für gelöste Warnungen mit einem Datensatz für offene Warnungen zu vergleichen, um den Lösungsansatz erneut zu verwenden.

Ähnlichkeitslösung trainieren

Zum Trainieren einer Ähnlichkeitslösung sammeln Sie Wörter, um eine Sammlung zu erstellen, die Machine Learning (ML) verwenden kann, um Text in den Feldern **Kurzbeschreibung**, **Beschreibung**, **Quelle**, **Typ**, **Ressource** und **Metrikname** in einer gelösten Warnung zu vergleichen, um zu sehen, ob die Wörter in der festgelegten Übereinstimmung mit den Wörtern in einer offenen Warnung übereinstimmen. Die gelöste Warnung, die einer offenen Warnung ähnelt, ist ein Beispiel dafür, wie die offene Warnung gelöst werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um eine Lösung zu trainieren, muss der Filter mindestens einen Datensatz zurückgeben. Wenn Ihr Filter keine Datensätze zurückgibt, aktualisieren Sie ihn.

Hinweis: Die bevorzugte Anzahl von Datensätzen für das Trainieren einer Lösung besteht aus 30.000 bis 300.000 Datensätzen. Wenn Sie mehr als 300.000 Datensätze einreichen, werden die neuesten 300.000 Datensätze zum Trainieren der Lösung verwendet. Verwenden Sie nur authentische Datensätze aus der Datenbank.

- Stellen Sie sicher, dass die Datensätze, die Sie trainieren, nicht zu alt und relevant für Ihren Geschäftbedarf sind. Sorgen Sie dafür, dass die Wörter in der Sammlung stets aktuell sind.
- Verwenden Sie keine hartcodierten Datumsangaben als Filter, da diese Filter nicht aktualisiert werden, wenn die Lösungen neu trainiert werden, es sei denn, Sie aktualisieren sie vor jedem neuen Training manuell. Verwenden Sie stattdessen relative Datumsfilter, wie z. B. letzte 3 Monate, letzte 6 Monate oder letzte 12 Monate.
- Führen Sie nach Bedarf Trainings durch, bis eine akzeptable Ähnlichkeitslösung bereitgestellt wird. Diese Praxis bietet Ihnen Zeit zum Überprüfen und Aktualisieren Ihrer Lösungsdefinition.

Felder, die in die Lösung einbezogen werden sollen

Notieren Sie sich Felder, die wahrscheinlich Wörter und Ausdrücke enthalten, die dem System helfen, ähnliche Datensätze für Ihre Lösung zu identifizieren.

Die Ähnlichkeitsfelder, die Sie auswählen, sollten eine Teilmenge Ihres Eingabefelds „Auswahlen“ sein. Beispiel: Wenn Sie „Felder“ aus Incident-Datensätzen auswählen, die sich im Status „Offen“ befinden, wählen Sie **Hinweis schließen** nicht als Ähnlichkeitsfeld aus. Da offene Datensätze keine **Hinweis schließen**-Felder enthalten, kann der Text nicht ähnlich sein.

Die Ähnlichkeitsfelder stehen Benutzern beim Erstellen von Datensätzen zur Verfügung.

Über die Ähnlichkeitspunktzahl

Die Ähnlichkeitspunktzahl ist ein Maß für den Ähnlichkeitsgrad zwischen zwei Warnungsdatensätzen von 0 bis 100. Warnungsdatensätze, deren Ähnlichkeitspunktzahl über dem von Ihnen angegebenen Schwellenwert liegt, werden von der Lösung zurückgegeben.

Überprüfen Sie Ähnlichkeitsbeispiele und ihre Punktzahlen mithilfe der Funktion **Schulungsfortschritt anzeigen**, um zu bestimmen, ob der Lösungsschwellenwert erhöht oder verringert werden soll. Sie können den Schwellenwert im Feld **Threshold for Similarity Score** (Schwellenwert für Ähnlichkeitspunktzahl) ändern.

Fortschritt der Trainingslösung anzeigen

Die Trainingsdauer variiert je nach Anzahl der Datensätze und Klassen innerhalb des Trainingssatzes. Je mehr Datensätze und Klassen Sie verwenden, desto länger dauert das Training. Zum Beispiel kann das Trainieren eines Satzes mit 100.000 Datensätzen und mehreren hundert Klassen ungefähr fünf Stunden dauern.

Um den Fortschritt der Trainingslösung zu zeigen, führt die ML-Lösung automatisch die folgenden Tätigkeiten aus, wenn Sie **Trainingsfortschritt anzeigen** auf der Seite „Lösungen“ wählen. Weitere Informationen finden Sie unter Fortschritt beim Lösungstraining anzeigen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lösungstrainingsaktivitäten

Aktivität	Beschreibung
Dateien zum Trainieren abrufen.	Das System lädt die Trainingsdatensätze herunter und sendet sie an den nächstgelegenen Trainingsservice.
Daten vorbereiten.	Das System entfernt doppelte Datensätze aus dem Trainingssatz.
Lösung trainieren.	Der Trainingsservice trainiert die Lösung.
Trainierte Lösung hochladen.	Der Trainingsservice lädt die Lösung als Anhangsdatensätze hoch.

Eine Ereignismanagement Ähnlichkeitslösung erstellen

Erstellen und trainieren Sie eine Lösung, die maschinelles Lernen auf eine Sammlung von Wörtern anwendet und ähnliche Warnungen in Ihrem Instanzdatensatz vorschlägt. Sie können beispielsweise den Text in einer gelösten Warnung mit einer offenen Warnung vergleichen, um die Lösung wiederzuverwenden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Das von Ihnen verwendete Verschlüsselungsschema kann sich darauf auswirken, ob Sie Lösungen trainieren können.

- Wenn Ihre Daten durch Full Disc Encryption (FDE) verschlüsselt sind, können Sie Lösungen trainieren.
- Wenn das Feld, das Sie für das Training verwenden, mit Feldverschlüsselungverschlüsselt ist, stellen Sie sicher, dass der Worker-Benutzer des gemeinsam genutzten Services über die richtige Verschlüsselungsmodulrolle verfügt, die für die Verschlüsselung verwendet wurde.
- Wenn Sie Edge Encryption verwenden, wird das Trainieren nicht unterstützt.

Hinweis: Diese Funktion unterstützt nur die englischsprachige Verarbeitung.

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence** > **Ähnlichkeit** > **Lösungsdefinitionen**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

ML-Lösungsdefinitionsformular

Feld	Beschreibung
Lösungsvorlage	Verwendung zum Definieren einer Wortsammlung.
Bezeichnung	Eindeutiger Name für die Ähnlichkeitslösung.
Name	Feld, das automatisch mit einem vom System zugewiesenen Namen gefüllt wird, der dem Bezeichnungsnamen beim Erstellen der Lösung ähnlich ist.
Tabelle	Tabelle, die die Datensätze enthält, die für die Wortsammlung verwendet werden sollen, z. B. Incident-Tabelle oder Asset-Tabelle. Wenn Sie einen Tabellenwert zuweisen, erscheint

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	ein Link, der die Anzahl der Datensätze zeigt, die mit Ihren aktuellen Bedingungen übereinstimmen.
Filter	Bedingungen, die Sie auf die Trainingsdatensätze anwenden möchten. Um eine Lösung zu trainieren, muss der Filter mindestens einen Datensatz zurückgeben. Wenn Ihr Filter keine Datensätze zurückgibt, aktualisieren Sie ihn.
Eingabefelder	Notieren Sie sich Felder, die den Text und Kontext enthalten, die Sie in Ihre Wortsammlung aufnehmen möchten. Der Felddatentyp kann eine Zeichenfolge, Referenz, Auswahl oder HTML sein, z. B. **Kurzbeschreibung** und **Beschreibung**. **Hinweis:** **Journaltyp** ist kein unterstützter Datentyp. Gute Kandidaten für Ihre Eingabefelder enthalten Text, der für die Lösung relevant ist. Wenn Sie zum Beispiel eine Lösung konfigurieren, um ähnliche Incident-Datensätze zu finden, können Sie die Felder **Kurzbeschreibung**, **Beschreibung**, **Lösungsnotizen** und **Notizen schließen** auswählen.
Schulungshäufigkeit	Trainings werden standardmäßig einmal vom System durchgeführt. Da Ihre Daten mit der Zeit altern können, wodurch die Genauigkeit Ihres Vorhersagemodells beeinträchtigt wird, sollten Sie regelmäßige Trainings in Betracht ziehen, wenn Ihre Lösungsdefinition relativ stabil ist.
Domäne	Wählen Sie in Instanzen mit aktiver Domänentrennung die Domäne aus, deren Zieldatensätze Sie für Ihre Wortsammlung verwenden möchten. Erstellen Sie einen separaten Datensatz für die Ähnlichkeitslösungsdefinition für jede Domäne, deren Feldwerte Sie für Ihre Wortsammlung verwenden möchten.
Ähnlichkeitsfelder	Notieren Sie sich Felder, die wahrscheinlich Wörter und Ausdrücke enthalten, die dem System helfen, ähnliche Datensätze für Ihre Lösung zu identifizieren. Wenn Sie Ihre **Ähnlichkeitsfeldauswahl** ändern möchten, klicken Sie auf das Schlosssymbol ( ), um es zu öffnen, und nehmen Sie Aktualisierungen vor. Klicken Sie erneut auf das Symbol, um das Feld zu schließen und die Aktualisierungen zu speichern.
Ähnlichkeitsfenster	Der Zeitraum, in dem Sie nach ähnlichen Datensätzen suchen möchten. Wenn Sie eine kleinere Zahl an insgesamt eingehenden Datensätzen haben, ist möglicherweise ein größeres Fenster am besten. Wenn das Fenster jedoch zu groß ist, rufen Sie möglicherweise Datensätze ab, die nicht nützlich sind. Wenn das Fenster zu klein ist, können Sie möglicherweise nicht genügend ähnliche Datensätze abrufen. Wenn Sie beispielsweise nach ähnlichen Incident-Datensätzen suchen, die geöffnet sind, können Sie **Letzter Tag** auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Diese Auswahl bezieht sich auf die neuesten Datensätze, von denen viele noch offen sein könnten.
Ähnlichkeitsfensterfilter	Filterbedingungen für Ihr Ähnlichkeitsfenster. Diese Filter definieren die Datensatz-Bedingungen, unter denen Ihre Ähnlichkeitsergebnisse ermittelt werden. Wenn Sie zum Beispiel nach ähnlichen Incident-Datensätzen suchen, die offen sind, können Sie Ihre Suche filtern, indem Sie Bedingungen erstellen wie: **[Incident-Status] [ist] [In Bearbeitung]** Diese Filter werden zusätzlich zu den **Eingabefeld**-Filtern angewendet.
Aktualisierungshäufigkeit für Fenster	Aktualisierungshäufigkeit des Ähnlichkeitsfensters. Beispiel: Wenn Ihr Fenster offene Incident-Datensätze enthält, können Sie die Aktualisierungshäufigkeit **Alle 15 Minuten**auswählen. Neue Incidents treten häufig im Laufe des Tages auf, sodass diese Häufigkeit die Wahrscheinlichkeit erhöht, dass neu geöffnete Datensätze in die Aktualisierung einbezogen werden. **Hinweis:** Wenn das Ähnlichkeitsfenster aus Datensätzen besteht, z. B. Wissensartikel-Datensätze, die in der Regel nicht häufig erstellt werden, können Sie eine höhere Aktualisierungshäufigkeit wählen, z. B. **Jeden Tag**.

4. Klicken Sie auf **Speichern**, um den Lösungsdefinitionsdatensatz zu speichern, damit Sie später darauf zurückgreifen können, oder auf **Senden und trainieren**, um den Lösungsdefinitionsdatensatz zu erstellen und zu trainieren.
5. Wenn Sie die Lösung zum Trainieren übermittelt haben, klicken Sie im Fenster **Trainingsaktivierung** zur Bestätigung auf **OK**.

Ergebnisse
Das System plant das Trainieren der Lösung beim nächstgelegenen Trainingsservice. Sie und andere Benutzer, die die Kategorie „Predictive Intelligence-Benachrichtigungen“ abonniert haben, erhalten eine Benachrichtigung, wenn das Training abgeschlossen ist, einschließlich aller Fehler, die im Training aufgetreten sind. Nach Abschluss des Trainings lädt das System die Lösung als Anhangsdatensatz hoch.

Nächste Maßnahme
Schauen Sie sich die Beispiele der trainierten Ähnlichkeitslösung im zugehörigen Link **Ähnlichkeitsbeispiele** des Formulars „ML-Lösungsdefinition“ an.

Fortschritt des Lösungstrainings Ereignismanagement anzeigen

Zeigen Sie den Fortschritt oder Statistiken des Lösungstrainings an, um zu bestimmen, ob eine Lösung verfügbar ist oder wie lange der nächste Trainingszyklus vermutlich dauert.

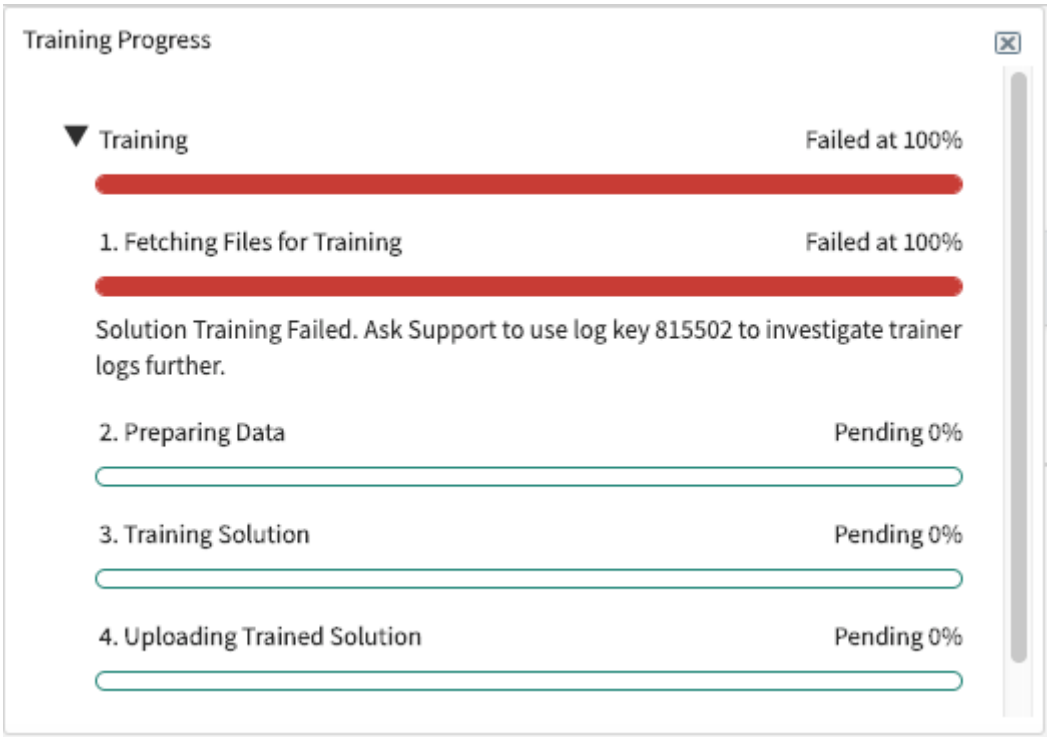
Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence** > **Ähnlichkeit** > **Lösungen**.
2. Wählen Sie in der Liste der ML-Lösungen die Lösung aus, deren Fortschritt oder Statistiken Sie anzeigen möchten.
3. Klicken Sie auf den zugehörigen Link **Trainingsfortschritt anzeigen**.
   Die ML-Lösung führt automatisch Aktivitäten aus, die im Popup-Fenster „Trainingsfortschritt“ angezeigt werden.

   Das System zeigt ein Popup-Fenster mit dem Trainingsfortschritt an. Im folgenden Beispiel ist der Fortschritt fehlgeschlagen.



   Bei einem erfolgreichen Training wären alle Balken vollständig blau und der Fortschritt für jeden Schritt würde 100 % betragen.

Nächste Maßnahme

Weitere Informationen finden Sie unter Ereignismanagement Ähnlichkeitsbeispiele prüfen.

Ereignismanagement Ähnlichkeitsbeispiele prüfen

Überprüfen Sie die Ähnlichkeitsbeispiele und Punktzahlen, die das System während der Lösungsschulung bereitstellt, um den Vergleich des ausgewählten Warnungsdatensatzes mit vorhandenen Warnungsdatensätzen zu überprüfen. Beispielsweise können Sie den Schwellenwert der Ähnlichkeitspunktzahl ändern, um die Genauigkeit Ihrer Ähnlichkeitsempfehlungen zu erhöhen.

Vorbereitungen

Ähnlichkeitslösung in einem ServiceNow Rechenzentrum trainieren Weitere Informationen finden Sie unter Eine Ereignismanagement Ähnlichkeitslösung erstellen.

Erforderliche Rolle: evt_mgmt_admin

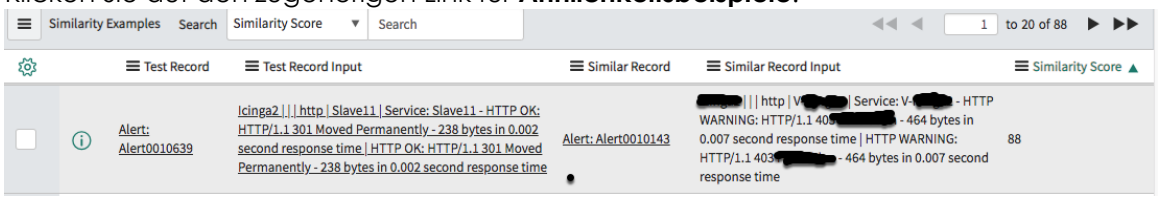
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Passen Sie den aktuellen Schwellenwert an, um nützliche Ergebnisse zu erhalten. Beispielsweise hat eine niedrige Ähnlichkeitspunktzahl mehr Abdeckung, aber weniger Genauigkeit.

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence** > **Ähnlichkeit** > **Lösungen**.
2. Suchen Sie Ihre Lösung in der Liste der ML-Lösungen, und klicken Sie auf das Informationssymbol (ⓘ).
3. Klicken Sie auf **Datensatz öffnen**.
4. Klicken Sie auf den zugehörigen Link für **Ähnlichkeitsbeispiele**.



5. Überprüfen Sie die Ähnlichkeitsbeispiele und ihre Schwellenwert-Punktzahlen, um das Niveau der Genauigkeit und Abdeckung zu bestimmen, die auf die Ergebnisse der Lösungsähnlichkeit angewendet werden sollen.
   Je höher die Ähnlichkeitspunktzahl ist, desto präziser ist sie und desto weniger Abdeckung bietet sie. Je niedriger die Ähnlichkeitspunktzahl ist, desto mehr Abdeckung und desto weniger Präzision bietet sie.
6. Bestimmen Sie abhängig von Ihrer Überprüfung, ob der Schwellenwert für die Ähnlichkeitslösung erhöht oder verringert werden soll.

   Die Lösung gibt nur Ähnlichkeitsergebnisse zurück, deren Punktzahl über dem Schwellenwert liegt. Wenn der aktuelle Schwellenwert keine nützlichen Ergebnisse liefert, passen Sie den Schwellenwert an.

7. Navigieren zu **Predictive Intelligence** > **Ähnlichkeit** > **Lösungen**.
8. Suchen Sie in der Liste der ML-Lösungen Ihre Lösung, und klicken Sie auf das Referenzsymbol (ⓘ).
9. Klicken Sie auf **Datensatz öffnen**.
10. Geben Sie im Abschnitt „Lösungsstatistiken“ im Feld **Schwellenwert für Ähnlichkeitspunktzahl** einen neuen Wert ein.
    Angenommen, die aktuelle Punktzahl beträgt 80. Basierend auf Ihrer Ähnlichkeitsbeispielüberprüfung möchten Sie das Feld möglicherweise aktualisieren, indem Sie eine höhere Punktzahl von 90 eingeben. Dadurch werden weniger Ergebnisse zurückgegeben, aber diese sind dem geprüften Warnungsdatensatz ähnlicher. Eine niedrige Ähnlichkeitspunktzahl hat mehr Abdeckung, aber weniger Genauigkeit.
11. Klicken Sie mit der rechten Maustaste auf den Header des Formulars, und klicken Sie auf **Speichern**.
    Ihre Lösung verwendet den neuen Ähnlichkeitsschwellenwert. In dem Beispiel gibt die Lösung nur Ähnlichkeitsergebnisse zurück, deren Punktzahl über 90 liegt.

Lösungsversion Ereignismanagement aktivieren

Das System aktiviert die neueste Version der Lösung, Sie können jedoch auch eine zuvor trainierte Lösungsversion von Ereignismanagement aktivieren, wenn sie angemessener ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Da Sie möglicherweise mehrere Lösungen erstellt haben, können Sie die Lösung aktivieren, die am besten geeignet ist.
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Predictive Intelligence** > **Ähnlichkeit** > **Lösungen**.
2. Klicken Sie in der Liste der ML-Lösungen auf das Referenzsymbol (ⓘ) für die trainierte Lösung, die Sie aktivieren möchten.
3. Klicken Sie auf **Datensatz öffnen**.
   Sie können der Lösung mithilfe der Eigenschaft `evt_mgmt_similarity_solution_title` einen Titel zuweisen. Der Standardwert ist `ml_x_global_alert_similarity`. Diese Eigenschaft ändert den Wert im Feld **Lösungsname**.
4. Klicken Sie im Lösungsdatensatz auf **Aktivieren**.
   Das System aktiviert diese Lösungsversion und deaktiviert jede andere Lösungsversion.

Eigensystemüberwachung für Ereignismanagement

Verwenden Sie die Ereignismanagement Eigensystemüberwachung zur Nachverfolgung von Ereignismanagement Merkmalen und Problembehebung.

Überwachen Sie Ereignismanagement, um Probleme zu erkennen und zu beheben

Aktivieren Sie die Eigensystemüberwachung, um Systemprobleme Ereignismanagement zu erkennen und zu beheben. Einige Konfigurationen sind erforderlich, damit die Eigensystemüberwachung aussagekräftige Daten anzeigen kann. Nach der Konfiguration und Aktivierung der Aufgaben zeigt Service Operations-Arbeitsbereich Daten an, die nach einem wiederkehrenden Zeitplan automatisch erfasst und berechnet werden.

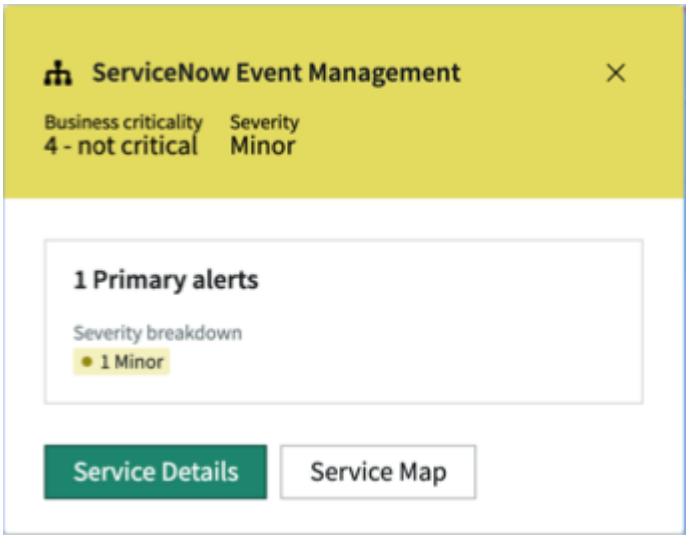
Hinweis: Ereignismanagement Dashboard wird für neue Instanzen im Paris Release nicht unterstützt. Instanzen, die von einem Release vor Orlando aktualisiert wurden und das Ereignismanagement Dashboard verwenden, können dies jedoch weiterhin tun.

Die Funktion „Eigensystemüberwachung“ erstellt CIs in der CMDB zur Darstellung der Komponenten der Eigensystemüberwachung. Verwenden Sie die bereitgestellten Überwachungen, um den Status von Services und Ereignismanagement Funktionen zu überwachen und nachzuverfolgen.

Ereignismanagement Eigensystemüberwachung kann:

- Warnungen auslösen, wenn ein Problem mit Ereignismanagement auftritt
- Zeigen Sie die **ServiceNow Ereignismanagement-** Anwendungsservices in Service Operations-Arbeitsbereichan . Verwenden Sie Service Operations-Arbeitsbereich, um Warnungen nach Anwendungsservice, technischem Service und Warnungsgruppen anzuzeigen. Sie können auf eine Kachel doppelklicken, um allgemeine Informationen zum Service anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Klicken Sie auf **Servicedetails**, um Details des Services anzuzeigen.
- Klicken Sie **auf Servicezuordnung**, um eine Zuordnungsdarstellung der Anwendungsservices **von ServiceNow Ereignismanagement** und die Beziehungen zwischen CIs in den Anwendungsservices **von ServiceNow Ereignismanagement** anzuzeigen.

Prozess-Workflow Eigensystemüberwachung

Wenn die Eigenschaft *`Event Management – self-health monitoring`* aktiviert ist:

1. Die Anwendungsservices **von ServiceNow Ereignismanagement** werden automatisch erstellt.
2. Aufträge werden automatisch zur Ausführung von Skripts geplant, die konfigurieren, was überwacht werden muss.
3. Die Tabelle „Überwachungsstatus [em_monitor_state]“ wird nach jeder Event-Ausführung aktualisiert, die von den Konfigurationsskripts ausgelöst wird.
4. Die generierten Warnungen werden überwacht.

   Der Service zeigt den Status der überwachten Entität an. Beispielsweise werden Warnungen im Dashboard Ereignismanagement, Service Operations-Arbeitsbereich oder in der Liste „Alle Warnungen“ angezeigt.

Sie können mit **Quick Response** auf der Standard-Plattform-Schnittstelle die Warnungen nach dem zugrunde liegenden Problem beheben. Details finden Sie unter Schnelle Antworten in einer Warnung anwenden.

Geplante Aufträge zur Verarbeitung von Skripts

Die standardmäßig geplanten Aufgaben, nachdem die Eigenschaft *`Event Management – self-health monitoring`* aktiviert wurde, sind:

- Die geplante Aufgabe `Ereignismanagement „Integritätsüberwachung einfügen“,` die die Skripts ausführt.
- Die geplante Aufgabe `Ereignismanagement „ – Integritätsüberwachung aktualisieren“,` die die Aktualisierungsskripts ausführt. Dieser Auftrag wird einmal pro Minute ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Systemüberwachung starten oder anhalten

Sie können das Starten oder Anhalten der Eigensystemüberwachung steuern, indem Sie die Eigenschaft der Eigensystemüberwachung konfigurieren. Bei der ersten Aktivierung der Eigenschaft zur Eigensystemüberwachung werden automatisch die ServiceNow-Anwendungsservices Ereignismanagement erstellt.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie die Eigenschaft zur Selbstsystemüberwachung, um Anwendungsservices und Ereignismanagementzu überwachen und nachzuverfolgen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Ereignismanagement-Eigenschaften**.
2. Suchen Sie die Eigenschaft *Enable Event Management self-health monitoring* (*evt_mgmt.self_health_active*).
   Wählen Sie einen dieser Werte aus:

Aktivieren Sie die Eigenschaft Event Management-Eigensystemüberwachung

Feld	Beschreibung
Aktiviert	Die ServiceNow-Anwendungsservices Ereignismanagement werden für die Überwachung der Eigenintegrität erstellt. Events werden empfangen und Warnungen werden generiert.
Nur Warnungen	Die Anwendungsservices von ServiceNow Ereignismanagement und die zugehörigen CIs werden nicht erstellt. Warnungen werden erstellt, sind jedoch nicht an ein CI gebunden.
Deaktiviert	Die Anwendungsservices von ServiceNow Ereignismanagement sind nicht funktionsfähig. Events werden nicht empfangen, und es werden keine Warnungen generiert.

3. Klicken Sie auf **Speichern**.

Ergebnisse
Die ServiceNow-Anwendungsservices Ereignismanagement werden entsprechend dem für die Eigenschaft *evt_mgmt.self_health_active* ausgewählten Wert festgelegt.

Konfigurieren Sie die geplante Aufgabe Ereignismanagement - Integritätsüberwachung einfügen

Legen Sie fest, was die regelmäßige Aufgabe Ereignismanagement „ - Integritätsüberwachung einfügen“ überwachen soll. Nachdem der Auftrag ausgeführt wurde, können Sie die Anwendungsservices **von ServiceNow Ereignismanagement** anzeigen.

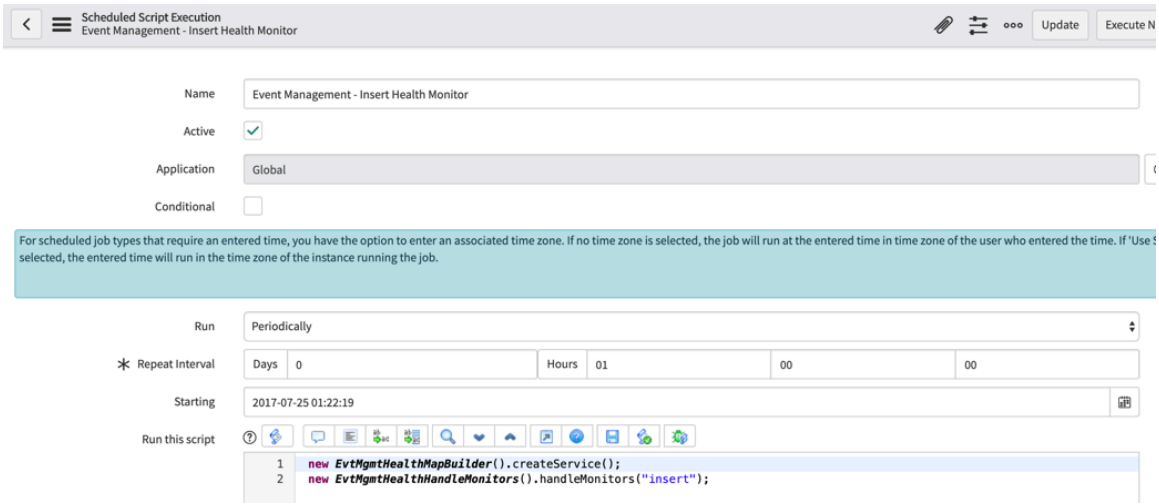
Vorbereitungen
Stellen Sie sicher, dass die Eigenschaft *Enable Event Management — self-health monitoring* auf der Seite mit den Ereignismanagement-Eigenschaften () aktiviert ist.**Ereignismanagement** > **Ereignismanagement-Eigenschaften**) an.

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Systemdefinition** > **Geplante Aufgaben**.
2. Suchen und wählen Sie den Auftrag **Event Management - Systemüberwachung einfügen**.



3. Ändern Sie die im Feld **Dieses Skript ausführen** angegebenen Skripts , um zu festzulegen, welche Skripts überwacht werden sollen.

Eigensystemüberwachung mit Domänentrennung

Verwenden Sie Domain Separation, um die Selbstintegrität zum Anzeigen Ereignismanagement von Integritätsproblemen zu aktivieren, die auf Daten, Regeln und Einstellungen der angemeldeten Benutzerdomäne basieren. Die ausgewählte Domäne darf keine untergeordneten Domänen enthalten.

Vorbereitungen

Stellen Sie sicher, dass das Plugin „Domain Support – Domain Extension Installer“ (com.glide.domain.msp_extensions.installer) aktiviert ist und dass MID-Server, mit dem Sie eine Verbindung herstellen, für Ereignismanagementkonfiguriert ist.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Eigensystemüberwachung ist domänenbezogen. Wenn das Plugin „Domain Support – Domain Extension Installer“ (com.glide.domain.msp_extensions.installer) aktiviert wurde, zeigt die Selbstintegrität Integritätsprobleme basierend auf Daten, Regeln und Einstellungen der angemeldeten Benutzerdomäne an. Wenn Regeln und Einstellungen für eine untergeordnete Domäne nicht definiert sind, werden die Einstellungen der übergeordneten Domäne rekursiv angewendet.

Hinweis: Um in einer domänengetrennten Instanz Eigensystem-Überwachungsereignisse zu generieren, müssen Sie die Domäne dieser generierten Ereignisse angeben. Dazu geben Sie die `sys_id` der erforderlichen Domäne in der Eigenschaft *`evt_mgmt.domain_self_monitoring`* an.

Wenn das Plugin „Domain Support – Domain Extension Installer“ (com.glide.domain.msp_extensions.installer) nicht aktiviert ist, wird das Hinzufügen oder Entfernen eines Connectors oder MID-Server sofort in der Zuordnung angezeigt.

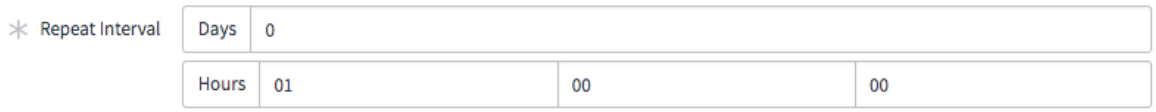
Wenn das Plugin „Domänensupport - Domänenerweiterungs-Installer“ (com.glide.domain.msp_extensions.installer) aktiviert ist, werden die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Updates regelmäßig gemäß den Intervallspezifikationen des geplanten Auftrags Ereignismanagement„Systemüberwachung einfügen“ durchgeführt.

Prozedur

1. Navigieren zu **Alle** > **Systemzeitplaner** > **Geplante Aufgaben**.
2. Suchen und wählen Sie in der Liste **Zeitplan** den Auftrag Ereignismanagement„Systemüberwachung einfügen“ aus.
3. Wählen Sie im Auftrag Ereignismanagement – Integritätsüberwachung einfügen unter „Zugehörige Links“ **Konfigurieren Sie die Auftragsdefinition aus**.
4. Legen Sie die erforderliche regelmäßige Aktualisierungszeit im Feld **Wiederholungsintervall** fest, indem Sie die erforderlichen Werte angeben.
   Der Standardwert ist 1 Stunde.

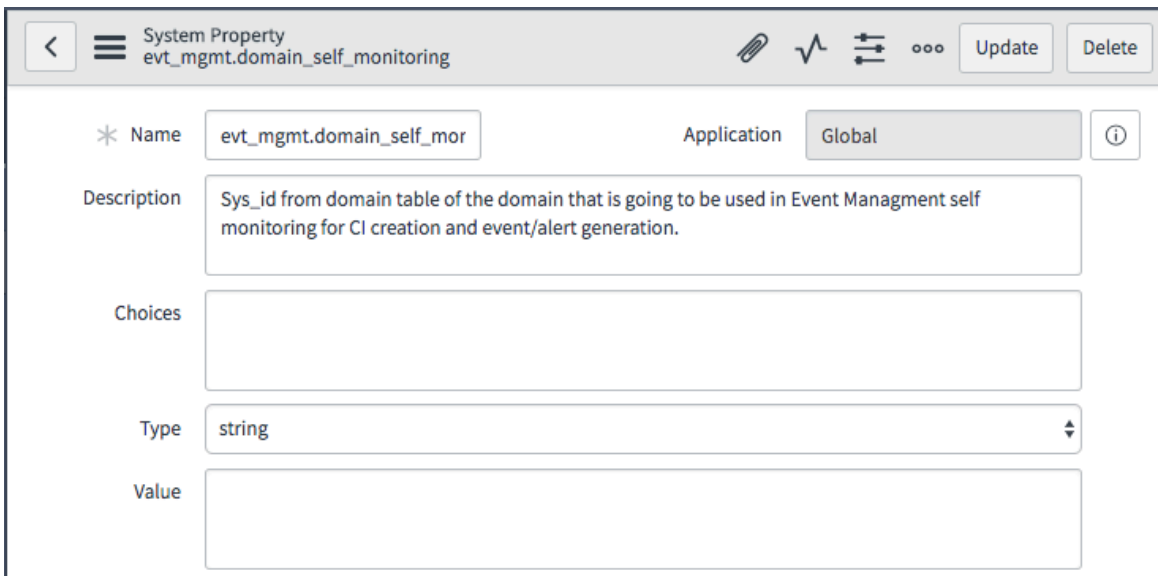


5. Wählen Sie **Aktualisieren**.

Ergebnisse

Weitere Konfiguration ist für die CI-Erstellung, den Empfang von Events und die Generierung von Warnungen erforderlich. Die `sys_id` der Domäne muss im Feld **Wert** der Eigenschaft *`evt_mgmt.domain_self_monitoring`* angegeben werden.

1. Navigieren Sie zu **Systemeigenschaften Alle Eigenschaften**.
2. Suchen Sie nach der Eigenschaft *`evt_mgmt.domain_self_monitoring`*, und wählen Sie sie aus.



3. Geben Sie im Feld **Wert** die `sys_id` der Domäne an.
4. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Einrichtung der Domänentrennung und grundlegende Verwaltung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigensystemüberwachung konfigurieren

Sie können eine Eigensystemüberwachung konfigurieren, um Ereignismanagement Komponenten nachzuverfolgen und um sicherzustellen, dass sie den angegebenen Schwellenwert nicht überschreiten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Tabelle „Überwachungskonfigurationen [em_monitor_conf]“ enthält die Datensätze, die bestimmen, welche Ereignismanagement Komponenten überwacht werden. Jeder Datensatz enthält das Skript für die Systemüberwachung, das für Ihre Überwachung relevant ist. Wenn Sie beabsichtigen, ein neues Systemüberwachungsskript zu erstellen, müssen Sie eine Überwachung konfigurieren, die dem Zweck des benutzerdefinierten Skripts entspricht. Sie können die Überwachungskonfigurationsdatensätze so konfigurieren, dass sie die für Sie wichtigen Elemente nachverfolgen. Beispielsweise können Sie den Schwellenwertaspekt im Datensatz *`Connector's Idle state monitoring`* ändern, indem Sie angeben, dass die Häufigkeit des Überwachungsauftrags 90 Sekunden anstatt 120 Sekunden beträgt.

Hinweis: Jeder der Überwachungskonfigurationsdatensätze kann deaktiviert werden.

Wenn eine Überwachungskonfiguration einen Schwellenwert angibt, bestimmt der Konfigurationswert, welcher Warnungsschweregrad angezeigt werden soll. Schwellenwerte geben die Verzögerungszeitwerte in Minuteneinheiten an.

Hinweis: Zusätzliche Informationen zur Eigensystemüberwachung werden auf Dashboard Ereignismanagement Übersicht angezeigt.

Nach Aktivierung der Eigenschaft *`Event Management - self-health monitoring`* werden Aufträge automatisch zur Ausführung von Skripts geplant, die konfigurieren, was überwacht werden muss:

- Die geplante Aufgabe Ereignismanagement `„Integritätsüberwachung einfügen“` führt die Skripts aus. Bestimmen Sie, was überwacht werden muss, indem Sie das Skript in diesem Auftrag hinzufügen oder ändern, der einmal pro Stunde ausgeführt wird.
- Die geplante Aufgabe Ereignismanagement `„ - Integritätsüberwachung aktualisieren“` führt die Aktualisierungsskripts aus. Dieser Auftrag wird einmal pro Minute ausgeführt.

Verwenden Sie das folgende Verfahren, um zu konfigurieren, ob eine Überwachungskonfiguration ausgeführt werden kann, und die Häufigkeit der Überwachungsaufgabe festzulegen. Sie können die Schwellenwerte angeben, die bei Überschreitung eine Warnung auslösen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Eigensystemüberwachung**.
2. Wählen Sie in der Liste „Überwachungskonfigurationen“ einen Überwachungskonfigurationsdatensatz aus, und ändern Sie das erforderliche Feld. Füllen Sie die Felder des Formulars aus.

Überwachungskonfigurationsformular

Feld	Beschreibung
Aktiv	Kontrollkästchen zum Aktivieren der Überwachungskonfiguration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Überwachungsauftragshäufigkeit [Sekunden]	Häufigkeit, mit der der Überwachungsauftrag ausgeführt wird.
Schwellenwert für „Kritisch“	Jeder Punkt über dem Wert gilt als kritische Konsequenz.
Schwellenwert für „Schwerwiegend“	Jeder Punkt über dem Wert, jedoch unter dem Wert des **kritischen Schwellenwerts**, gilt als schwerwiegende Konsequenz.
Schwellenwert für „Gering“	Bei Überschreitung gilt der Wert als geringfügige Konsequenz.
Warnungsschwellenwert	Wenn der Wert überschritten wird, wird eine Warnung ausgegeben.

3. Klicken Sie auf **Aktualisieren**.

Ergebnisse
Die Werte im geänderten Datensatz der Überwachungskonfiguration werden mit den tatsächlichen Werten verglichen, wie sie in empfangenen Events auftreten. Warnungen werden gemäß den Konfigurationseinstellungen erstellt.

Example:
Beispiel 1: Verwenden Sie das folgende Verfahren, um das Feld **Kritischer Schwellenwert** der **Überwachung des Ruhezustands des Connectors** von 30 Sekunden auf 35 Sekunden zu ändern. Dieses Feld bestimmt die Anzahl der Sekunden, die vergehen, bevor eine Warnung generiert wird, wenn der Leerlaufstatuswert eines **kritischen Schwellenwerts** eines Connectors überschritten wird. In diesem Beispiel wird das Feld **Kritischer Schwellenwert** von 30 Sekunden auf 35 Sekunden geändert.

1. Navigieren zu **Ereignismanagement** > **Einstellungen** > **Selbstintegritätskonfiguration**.
2. Wählen Sie in der Liste „Überwachungskonfigurationen“ die **Connector-Leerlaufüberwachung** aus.
3. Ändern Sie im Feld **Kritischer Schwellenwert** den Wert auf `35`.
4. Klicken Sie auf **Aktualisieren**.

Ergebnis Der Schwellenwert des Felds **Kritischer Schwellenwert** wurde von `30` auf `35`erhöht. Dadurch wird die Anzahl der Sekunden erhöht, die vergehen, bevor eine Warnung für diesen Schwellenwert generiert wird.

Beispiel 2: Dieses Beispiel beschreibt die Konfiguration des Schweregradschwellenwerts bei Verwendung der **Connectors-Statusüberwachung**. Die **Connector-Statusüberwachung** hat eine Konfiguration „true“ (= Wert 1) oder „false“ (= Wert 0) für den Schweregradschwellenwert. Für diese Überwachung wird für einen Schwellenwert mit dem Wert `1` dieser Schweregrad angezeigt. Nur ein Schweregradschwellenwert kann den Wert `1` haben. Dieses Beispiel geht davon aus, dass der angezeigte erforderliche Schweregrad `Geringfügig` ist.

1. Navigieren zu **Ereignismanagement** > **Einstellungen** > **Selbstintegritätskonfiguration**.
2. Wählen Sie in der Liste „Überwachungskonfigurationsliste“ **Connector-Status** aus.
3. Geben Sie im Feld **Schwellenwert für „Gering“**den Wert `1` ein.
4. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnis Die Überwachung gibt eine Warnung aus, wenn der Schwellenwert des Felds **Schwellenwert für „Gering“** überschritten wird.

Nächste Maßnahme

Erstellen Sie eine benutzerdefinierte Überwachung. Eine Vorlage wird bereitgestellt, die Sie bei der Erstellung eines Skripts unterstützt, das die angegebenen Komponenten überwachen kann. Weitere Informationen finden Sie unter Erstellen Sie eine Eigensystemüberwachung, um ein benutzerdefiniertes Skript für die Systemüberwachung zu verwenden.

Erstellen Sie eine Eigensystemüberwachung, um ein benutzerdefiniertes Skript für die Systemüberwachung zu verwenden

Sie können eine Eigensystemüberwachung erstellen, um ein benutzerdefiniertes Skript für die Systemüberwachung zur Überwachung spezifischer Ereignismanagement Komponenten zu verwenden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Zur Erweiterung der Eigensystemüberwachungen, die im Basissystem enthalten sind, können Sie eine Eigensystemüberwachung erstellen, um die von Ihnen angegebenen Komponenten zu überwachen. Die mit dem Basissystem bereitgestellten Eigensystemüberwachungsskripts sind in der folgenden Tabelle aufgelistet.

Eigensystemüberwachungsskripts, die mit dem Basissystem bereitgestellt werden

Systemüberwachungsskript	Verwendet von einer Überwachung für folgende Zwecke:
Verzögerung bei der Event-Verarbeitung überprüfen	Die Dauer [in Minuten] von Events überwachen, die im Status „Bereit“ blieben und nicht verarbeitet wurden.
Connector-Überwachung	Überwachung: • Gibt an, ob die Zeit, die ein Connector im Leerlauf war, den konfigurierten Schwellenwert [in Minuten] überschritten hat. • Der aktive Status von Connectors.
Status der Event-Verarbeitung abrufen	Überwachung der Zeit, in der sich die Events im Status „Bereit“ befinden. Warnungen werden gesendet, wenn diese Zeit den Schwellenwert überschreitet.
MID-Server-Schwellenwertwarnungen	MID Serverzustand überwachen. Wenn Änderungen am MID-Server-Status erkannt werden, werden Events gesendet.

Sie können Warnungsverwaltungsregeln erstellen, um auf die von der Eigensystemüberwachung erkannten Probleme zu reagieren und sie zu beheben. Warnungen werden basierend auf dem angegebenen Schweregrad und Schwellenwert generiert. Navigieren zu **Ereignismanagement** > **Administration** > **Eigensystemüberwachung** für die Überwachungen, die mit der Basisinstanz bereitgestellt werden, um die durch die Eigenintegrität erkannten Probleme zu überwachen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen	Beschreibung
Überwachung des Connectors im Ruhezustand	Überwachung, um zu überprüfen, ob sich einer der Connectors im Ruhezustand befand und den konfigurierten Schwellenwert [in Minuten] überschritten hat. Ausgewähltes Eigensystemüberwachungsskript: `Connector-Überwachung`.
Connectors-Status	Überwachung zur Nachverfolgung des aktiven Status der Connectors. Wählen Sie nur einen Schwellenwert aus, um zu konfigurieren, welcher Schweregrad aufgerufen werden soll. Verwenden Sie 1 zum Auswählen des Schwellenwertfelds oder 0, um das Schwellenwertfeld zu ignorieren. Weitere Informationen finden Sie unter Connector-Statusbeispiel. Ausgewähltes Eigensystemüberwachungsskript: `Connector-Überwachung`.
Verzögerung bei der Event-Verarbeitung	Die Dauer [in Minuten] von Events überwachen, die im Status „Bereit“ blieben und nicht verarbeitet wurden, Dieser Zeitraum initiiert eine Warnung für das Event, das das CI verarbeitet, mit Schweregrad gemäß den konfigurierten Schwellenwerten [Minuten]. Ausgewähltes Systemüberwachungsskript: `Verzögerung bei der Event-Verarbeitung überprüfen`.
Event-Verarbeitungsauftrag	Überwachung des Status der Event-Verarbeitungsaufgaben. Eine Warnung wird generiert, wenn die Leerlaufzeit eines Auftrags den konfigurierten Schwellenwert überschreitet. Ausgewähltes Systemüberwachungsskript: `Event-Verarbeitungsstatus überprüfen`.
MID-Server MID-Server Schwellenwertwarnungen	Überwachen Sie die Integrität MID-Server MID-Server von . Events werden gesendet, wenn Probleme mit der MID-Server-Verfügbarkeit und Ressourcenschwellenwerten erkannt werden. Systemüberwachungsskript ausgewählt: `MID Server-Schwellenwertwarnungen`.

Hinweis: Um zu verhindern, dass eine Eigensystemüberwachung den Connector-Status erkennt, können Sie das Kontrollkästchen **Aktiv** der Überwachung jederzeit deaktivieren und dann auf **Aktualisieren** klicken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Administration** > **Eigensystemüberwachung**und klicken Sie auf **Neu**.
2. Füllen Sie die Felder des Formulars aus.

Überwachungskonfigurationsformular

Feld	Beschreibung
Name	Beschreibender und aussagekräftiger Name für die Überwachung.
Beschreibung	Textbeschreibung, die die Überwachung beschreibt.
Aktiv	Kontrollkästchen, um die Überwachung zu aktivieren.
Überwachungsauftragshäufigkeit [Sekunden]	Häufigkeit, mit der der Überwachungsauftrag ausgeführt werden soll. Standardwert: `120` Sekunden
Letzte Ausführung	Datum und Uhrzeit der letzten Ausführung Diese Werte werden automatisch aktualisiert.
Skript	Überwachungsskript. Klicken Sie auf das Suchsymbol. Die vorhandenen Skripts werden auf dem Bildschirm „Systemüberwachungsskripts“ aufgelistet, oder klicken Sie auf **Neu**, um ein benutzerdefiniertes Skript für die Systemüberwachung zu erstellen. Weitere Informationen zum Erstellen eines benutzerdefinierten Systemüberwachungsskripts finden Sie unter Schritt 3.
Hinweis: Zu allen folgenden Schwellenwertkonfigurationsfeldern: Alle überwachten Werte werden mit den Schwellenwerten verglichen. Wenn ein überwachter Wert einen Schwellenwert überschreitet, wird eine Warnung mit dem entsprechenden Schweregrad ausgegeben.	
Schwellenwert für „Kritisch“	Jeder Punkt über dem Wert gilt als kritische Konsequenz.
Schwellenwert für „Schwerwiegend“	Jeder Punkt über dem Wert, jedoch unter dem Wert des kritischen Schwellenwerts, gilt als schwerwiegende Konsequenz.
Schwellenwert für „Gering“	Bei Überschreitung gilt der Wert als geringfügige Konsequenz.
Warnungsschwellenwert	Wenn der Wert überschritten wird, wird eine Warnung ausgegeben.
Zusätzliche Informationen	Weitere Informationen zur Überwachung.

3. Zum Erstellen eines benutzerdefinierten Systemüberwachungsskripts klicken Sie im Formular „Überwachungskonfiguration“ neben dem Feld **Skript** auf das Suchsymbol, um das Skript Systemüberwachung zu öffnen, und klicken Sie auf **Neu**.
4. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Systemüberwachungsskript“

Feld	Beschreibung
Aktiv	Kontrollkästchen, um die Überwachung zu aktivieren.
Beschreibung	Textbeschreibung, die das benutzerdefinierte Skript beschreibt.
Name	Beschreibender und aussagekräftiger Name für das benutzerdefinierte Skript.
Skript	Benutzerdefiniertes Skript, das bei Aufruf von einer Überwachung ausgeführt wird. Eine Skriptvorlage wird als Leitfaden bereitgestellt. Sie können Eigensystemüberwachungsskripts, die mit dem Basissystem bereitgestellt werden als Beispiele für das Erstellen des Skripts verwenden und die Skript-Editor-Tools verwenden. Stellen Sie sicher, dass das benutzerdefinierte Skript Folgendes enthält: Führen Sie die Überwachungsfunktion aus, die entsprechend der Einstellung „Häufigkeit der Überwachungsaufträge“ *runUpdateHealthMonitorScripts(scriptId)* aufgerufen wird. Fügen Sie diese Funktion hinzu, um die Überwachungslogik auszuführen. Geben Sie die Konfigurationsfunktion an, die stündlich *runInsertHealthMonitorScripts(scriptId)* aufgerufen wird. Fügen Sie die Konfigurationslogik hinzu, und fügen Sie bei Bedarf ein CI hinzu. Geben Sie im Suchfeld des Navigationsbereichs `em_monitor_state.list` ein . Geben Sie in der Tabelle „Überwachungsstatus“ [em_monitor_state] die Initialisierung des Überwachungsdatensatzes im erforderlichen Datensatz an. Verwenden Sie die Hilfsfunktionen, die in den Skripteinbindungen *EvtMgmtHealthMonitorCommon* und *EvtMgmtEventAlertGenerator* definiert sind: ◦ EvtMgmtHealthMonitorCommon ◦ healthMonitorCommon.shouldRun ◦ healthMonitorCommon.calculateSeverity ◦ EvtMgmtEventAlertGenerato ◦ openAlert ◦ closeAlert

Sie können die Tabelle „Überwachungskonfigurationen“ [em_monitor_conf] für die Konfiguration der Systemüberwachung, die Tabelle „Systemüberwachungsskripts“ [em_monitor_scripts] für Skripts und die Tabelle „Überwachungsstatus“ [em_monitor_state] für die Anzeige der Ergebnisse der Überwachung verwenden, wie in *runInsertHealthMonitorScripts* initialisiert.

Weitere Informationen zu Skripteinbindungen und APIs finden Sie unter: Mit Ereignismanagement installierteSkripteinbindungen

5. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Sie können eine Eigensystemüberwachung erstellen, um ein benutzerdefiniertes Skript für die Systemüberwachung zur Überwachung spezifischer Ereignismanagement Komponenten zu verwenden.

Zeigen Sie die Zuordnung von Self-Integritäts-Anwendungsservices Ereignismanagement an

Sie können Anwendungsservice-Zuordnungen für Ereignismanagement anzeigen, um eine Visualisierung der Daten zu Configuration Items (CIs) zu erhalten, aus denen dieser Service besteht, sowie der Beziehungen und Verbindungen zwischen diesen CIs.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

In der Topologiezuordnung der Anwendungsservices Ereignismanagement werden nur MID-Server mit bestandener Validierung und aktive Connectors angezeigt.

Warum und wann dieser Vorgang ausgeführt wird
Die Ereignismanagement -Komponenten, die von den Self-Health-Anwendungsservices überwacht werden, sind in der folgenden Tabelle aufgeführt:

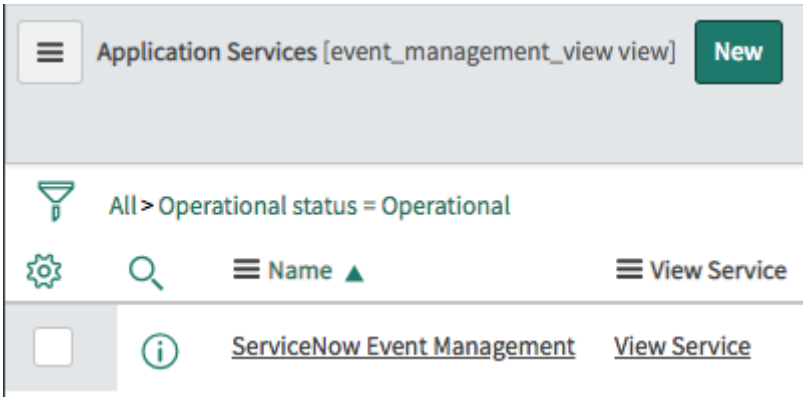
Komponenten, die vom Anwendungsservice Eigensystemüberwachung überwacht werden

Komponente	Was wird überwacht
Event-Connectors	Für jeden Connector: • Status: „Erfolg“ oder „Fehler“ • Verzögerung: Verstrichene Zeit seit „letzter Laufzeit“ (über dem Schwellenwert)
Event-Verarbeitungsaufträge	Für jeden Event-Verarbeitungsauftrag • Anzahl der tatsächlich ausgeführten Aufträge im Vergleich zur Anzahl der zur Ausführung konfigurierten Aufträge. • Verzögerung einer der Event-Verarbeitungsaufträge über die als Schwellenwert festgelegte Zeit. • Dauer von Events im Status „Bereit“ im Vergleich zum angegebenen Schwellenwert. • Verzögerung einer Event-Regelverarbeitung über den festgelegten Schwellenwert hinaus. Bei einer Verzögerung wird eine Warnung generiert und die Event-Regel deaktiviert.
MID-Server	MID Server, die validiert wurden, werden angezeigt. Der MID Serverstatus und die Tabelle `Ecc_agent_issue` werden überwacht. Ein Event wird ausgelöst, wenn diese Tabelle aktualisiert wird. Der MID Serverstatus wird entweder **Nach oben** oder **Nach unten** angezeigt. Informationen zur Integrität des MID-Servers finden Sie unter MID-Server-Heartbeat

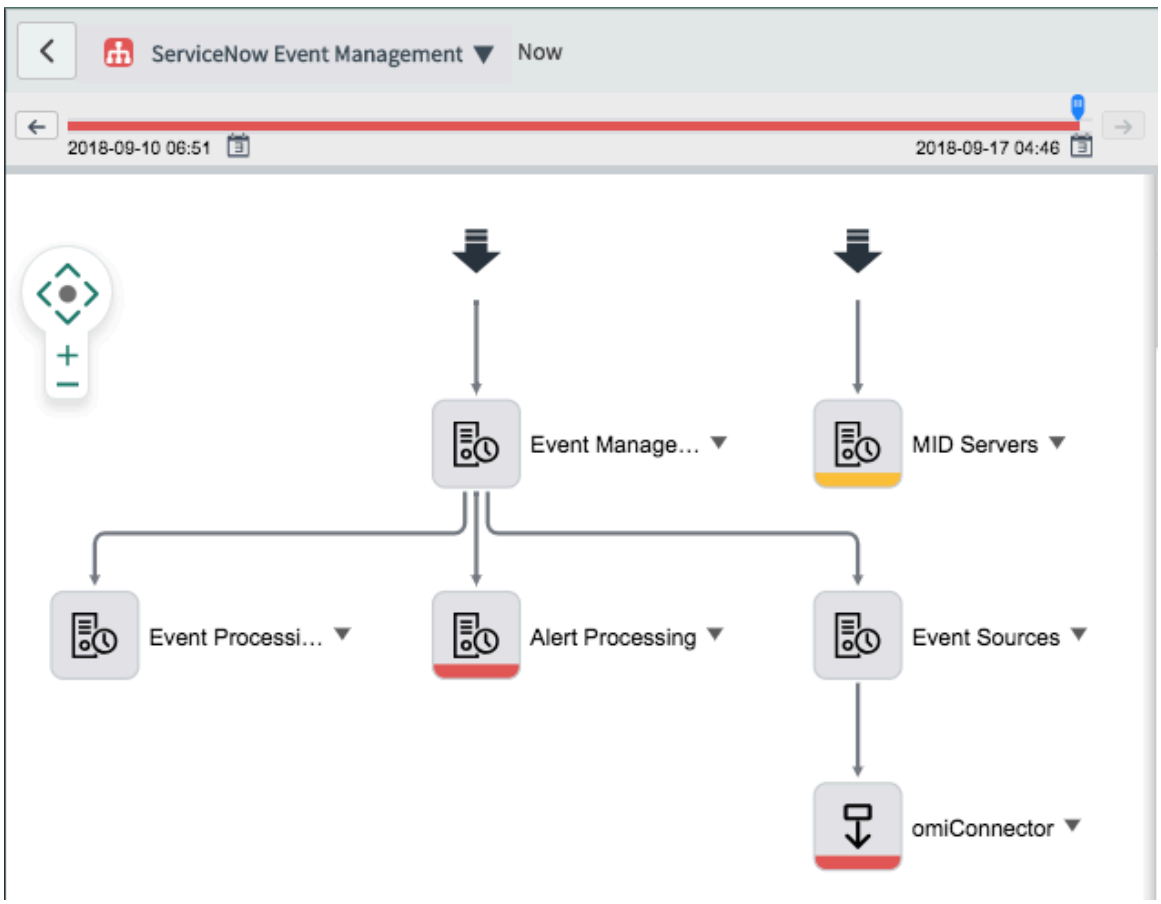
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Anwendungsservices**.
2. Klicken Sie auf die Anwendungsservices **ServiceNow Ereignismanagement**.
3. Suchen Sie auf der Seite **Anwendungsservices** nach **ServiceNow Event Management**, und klicken Sie auf **Service anzeigen**.



Auf der Karte werden die zugehörigen MID Server und das Objekt Ereignismanagement angezeigt, wie im folgenden Bild dargestellt; diese MID Server haben den Status **NACH OBEN**. MID Server werden aktualisiert, wenn sie erstellt oder deaktiviert werden.



Unter dem Objekt Ereignismanagement befinden sich Event-Verarbeitung, Warnungsverarbeitung und Event-Quellen (z. B. Connectors). Nur **aktive** Connectors werden angezeigt. Wenn ein Connector erstellt wird, wird der Connector erst angezeigt, nachdem er aktiviert wurde. Der Status aktiver Connectors wird aktualisiert, und der Status nicht aktiver Connectors wird nicht angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im vorherigen Bild wird die Integrität der Ereignismanagement Komponenten angezeigt. Die Komponente „omniConnector“ weist einen roten Balken auf, der angibt, dass eine kritische Warnung aufgetreten ist, die diesen Connector betrifft. Darüber hinaus wirkt sich diese kritische Warnung auf das übergeordnete Warnungsverarbeitungsobjekt aus, das daher einen roten Balken aufweist.

Ergebnisse
Sie können das Konfigurationselement mit einer kritischen Warnung auswählen und die Auswirkung vom übergeordneten Element zum Anwendungsservice ändern.

Wartungsregeln erstellen

Verwenden Sie Wartungsregeln, um CIs im Wartungsstatus zu kennzeichnen. Im Wartungsstatus werden diese CIs von der Auswirkungsberechnung ausgeschlossen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Regeln definieren, um CIs, die den angegebenen Kriterien entsprechen, als Wartungsstatus zu kennzeichnen. Die markierten CIs füllen die Tabelle „Auswirkungswartungs-CIs“ [em_impact_maint_ci].

Hinweis: Beim Ausführen von Wartungsregeln wird der Status „cmdb_ci“ übereinstimmender CIs nicht geändert. Übereinstimmende CIs werden jedoch in der Tabelle „em_impact_maint_ci“ von diesen Regeln gekennzeichnet, und dieser Status wird für Auswirkungs- und Warnungsberechnungen berücksichtigt.

Das Feld, das von dieser Regel als im Wartungsstatus gekennzeichnet ist, ist das CMDB-Statusfeld.

Hinweis: Zum Aktivieren einer Wartungsregel wählen Sie das Feld **Aktiv** in der Wartungsregel aus. Deaktivieren Sie das Feld **Aktiv**, um eine Wartungsregel zu deaktivieren.

Die mit der Wartungsregeln bereitgestellten Skripts sind:

Standard-Wartungsregel	Beschreibung
CI im Change-Zeitfenster	Wenn das CI ein aktives Change-Zeitfenster hat, werden die übereinstimmenden CIs als im Wartungsstatus gekennzeichnet. Die Regel führt eine Abfrage für die Change-Anforderungstabelle [change_request] aus, um zu bestimmen, ob die Regel angewendet wird. Alle diese Bedingungen in der Tabelle „change_request“ müssen erfüllt sein: • **Status** ist eine der folgenden Optionen: Geplant, Implementieren, In Bearbeitung oder Offen/Neu (Status in (-2, -1, 1, 2)). • **Genehmigung** ist „Genehmigt“ (genehmigung = „genehmigt“).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standard-Wartungsregel	Beschreibung
	• Das Change-Anforderungsfenster ist aktiv, d. h. die aktuelle Zeit liegt zwischen dem **Geplanten Startdatum** und dem **Geplanten Enddatum**, oder die aktuelle Zeit liegt zwischen dem **Tatsächlichen Startdatum** und dem **Tatsächlichen Enddatum**. • Der Change-Anforderungsdatensatz ist kein Wartungsdatensatz (on_hold = „false“). **Hinweis:** Alle diese Bedingungen müssen vorhanden sein, damit das CI von dieser Regel in den Wartungsstatus versetzt wird. Beispiel: Wenn der **Status** des Change-Anforderungsgenehmigung `Change wartet auf Genehmigung` ist, wird die Änderung der Tabelle „em_impact_maint_ci“ hinzugefügt.
Wartungsstatus des CIs	CIs, deren CMDB-Statusfeld **In Wartung** ist, werden von dieser Regel als im Wartungsstatus gekennzeichnet. Standardmäßig sind stillgelegte CIs nicht in CIs enthalten, die sich **In Wartung** befinden. So schließen Sie stillgelegte CIs ein: **1.** Navigieren Sie zu **Alle Eigenschaften**. **2.** Wählen Sie **Neu**. **3.** Konfigurieren Sie die *evt_mgmt.maintenance_rule_include_retired* Eigensch mit **Wert = true**. **Hinweis:** Das Einbeziehen von Tausenden stillgelegter CIs kann die Systemleistung beeinträchtigen.

Automatische Übersetzung

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Wartungsregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

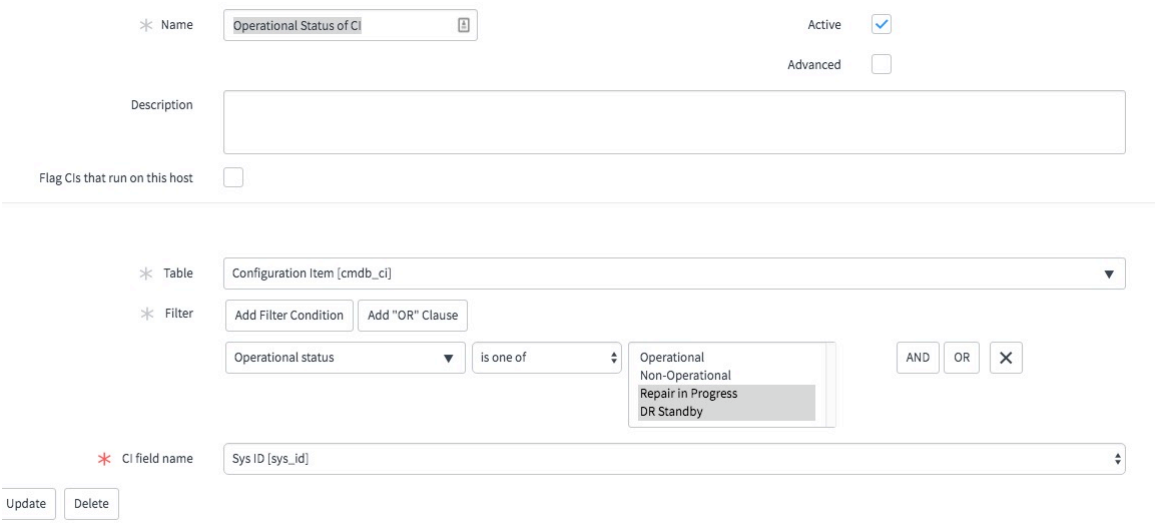
Spaltenüberschrift	Beschreibung
Name	Der Name der Wartungsregel.
Aktiv	Wählen Sie diese Option, um die Wartungsregel zu aktivieren.
Erweitert	Wählen Sie diese Option, um die Anzeige des optionalen Skriptabschnitts zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spaltenüberschrift	Beschreibung
Beschreibung	Informationen, die diese Wartungsregel beschreiben.
CIs kennzeichnen, die auf diesem Host ausgeführt werden	Wählen Sie diese Option, um alle Anwendungen, die auf dem erkannten Host ausgeführt werden, als in Wartung befindlich zu kennzeichnen.
Tabelle	Wählen Sie die Tabelle aus, die das erforderliche CI enthält.
Filter	Legen Sie fest, wie die Daten ausgewählt werden.
CI-Feldname	Wählen Sie das CI aus der Liste aus. Die Liste wird entsprechend Ihrer Auswahl im Feld **Tabelle** ausgefüllt. Wenn eine CMDB-Tabelle oder eine von CMDB abgeleitete Tabelle ausgewählt wurde, geben Sie `sys_id` für den **CI-Feldnamen** an. Andernfalls geben Sie das erforderliche CI-Feld an, das Sie verwenden möchten. Siehe Beispiele.

4. Klicken Sie auf **Absenden**.

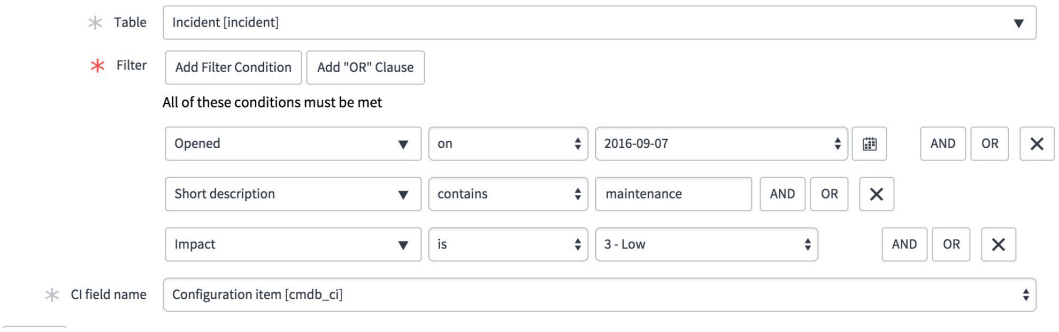
Example:
Beispiel für eine Wartungsregel, die eine CMDB-Tabelle verwendet.
Angenommen, ein Unternehmen definiert ein CI als in Wartung, wenn der Betriebsstatus des CIs entweder **Reparatur in Bearbeitung** oder **DR-Standby** lautet.



Beispiel für eine Wartungsregel, die eine andere als eine CMDB-Tabelle verwendet.

Angenommen, ein Unternehmen verwendet Incident-Datensätze zur Nachverfolgung der Wartung. Jede Wartungsanforderung wird in einen Incident übersetzt, wenn sie eine Beschreibung hat, die mit „CI-Wartung wird durchgeführt“ beginnt. Solange der Status eines solchen Incidents offen ist, gibt dieser Status an, dass die Wartung in Bearbeitung ist. Geben Sie für das Feld **CI-Feldname** einen CI-Namen aus der ausgewählten Tabelle an, in diesem Fall **Incident**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beispiel für eine Wartungsregel, die die erweiterte Skriptfunktion verwendet.

Wählen Sie auf der Seite „Wartungsregel“ die Option **Erweitert**. Passen Sie das bereitgestellte Beispielskript an:

```
var now_GR = new GlideRecord('cmdb_ci');
gr.addQuery('name', 'your_name_here');
gr.query();
while (gr.next()){
 result.push(gr.sys_id +'');}
```

Der Rückgabewert für dieses Beispielskript ist eine Textzeichenfolge, die ein Array von CI-IDs darstellt, z. B. [„sys_id1“, „sys_id2“, „sys_id3“].

Sie können dieses Skript als Beispiel verwenden, um Ihr eigenes benutzerdefiniertes Skript vorzubereiten.

```
(function findCisInMaint(){
var result = [];


//Your code goes here, this is an example of setting CIs in maintenance
var gr = new GlideRecord('cmdb_ci');
gr.addQuery('name', 'your_name_here');
gr.query();
while (gr.next()){
 result.push(gr.sys_id +''); //The array should be a string array, make sure to add strings
}


//Make sure to create a string representation of the array
return JSON.stringify(result);

})();
```

Zugehörige Informationen

Funktionsweise von Warnungen mit CIs in der Wartung

Warnung in Wartung setzen

Incidents im Zusammenhang mit einer Warnung lösen

Wenn Sie einen Incident lösen, der einer Warnung zugeordnet ist, wird gemäß der Eigenschaft *evt_mgmt.incident_closes_alert* ggf. auch die Warnung geschlossen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Prozedur

1. Öffnen Sie einen Incident.
2. Klicken Sie auf **Incident lösen**.

   Die entsprechende Warnung wird geschlossen, gelöst oder in Ruhe gelassen, wie in der Systemeigenschaft *evt_mgmt.incident_closes_alert* angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Warnung wird möglicherweise nicht sofort geschlossen, wenn der Incident geschlossen wird. Je nach Wert des Parameters *evt_mgmt.alert_rule_close_delay* kann die Warnung 5 Sekunden nach der letzten Warnungsaktualisierung geschlossen werden. Dieser Wert (in Sekunden) ist im Parameter definiert. Um die Eigenschaft zu verwenden, müssen Sie die Eigenschaft mit demselben Namen erstellen und ihr den erforderlichen Wert zuweisen. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Warnungen schließen

Schließen Sie eine Warnung durch ein Event oder eine Benutzeraktion. Beim Schließen der Warnung werden auch alle zugehörigen Incidents geschlossen, die nicht bereits gelöst oder geschlossen sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin oder evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird
Beim Schließen der Warnung werden auch alle zugehörigen Incidents geschlossen, die nicht bereits gelöst oder geschlossen sind. Dieses Standardverhalten kann durch Ändern des Werts der Eigenschaft *evt_mgmt.alert_closes_incident* konfiguriert werden.

Prozedur

1. Warnungen können Sie folgendermaßen schließen: Über das Warnungsformular, über Warnungen im Arbeitsbereich oder über das Dashboard Ereignismanagement (für Instanzen, die von einem Release vor Orlando aktualisiert wurden).
   - Um eine Warnung aus dem Warnungsformular zu schließen, navigieren Sie zu **Ereignismanagement** > **Alle Warnungen**. Klicken Sie in der Liste „Alle Warnungen“ auf die gewünschte Warnung.
   - Zum Schließen einer Warnung aus dem Arbeitsbereich aktivieren Sie das entsprechende Kontrollkästchen in der Warnungsliste, und klicken Sie auf die Schaltfläche **Schließen**. Sie können auch eine Warnung auswählen und dort in der Registerkarte „Details“ auf **Schließen** klicken.
   - Um ein Ereignis aus dem Dashboard Ereignismanagement zu schließen, navigieren Sie zu **Ereignismanagement** > **Dashboard**. Klicken Sie im Bereich „Warnungen“ auf die erforderliche Warnung.
2. Klicken Sie in der Ansicht „Warnungseigenschaften“ auf **Schließen**.
   Wenn Sie auf **Schließen** klicken, wird die Warnung ohne Bestätigung geschlossen.

   Weist die Warnung gelöste oder geschlossene Incidents auf, dann wird dem Incident eine Arbeitsnotiz darüber hinzugefügt, dass die zugehörige Warnung geschlossen wurde.

   Wenn die Warnung einen offenen Incident aufweist, der nicht mit anderen offenen Warnungen verknüpft ist, wird der Incident gemäß der Eigenschaft *evt_mgmt.alert_closes_incident* geschlossen, gelöst oder unverändert belassen.

Warnungen erneut öffnen

Weitere Events können zum erneuten Öffnen von Warnungen führen; außerdem können Sie eine Warnung erneut öffnen, indem Sie ihren Status ändern. Wenn eine Warnung erneut geöffnet wird, werden zugeordnete Incidents gemäß ihrem Status und der Eigenschaft *evt_mgmt.alert_reopens_incident* ggf. ebenfalls aktualisiert oder erneut geöffnet.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Warnung erneut geöffnet wird, wird der zugehörige Incident wie folgt verarbeitet:

- Wenn der Incident nicht *Resolved* oder *Closed* ist, wird eine Arbeitsnotiz darüber hinzugefügt, dass die zugehörige Warnung erneut geöffnet wurde.
- Wenn es sich bei dem Incident um *Resolved* oder *Closed* handelt, wird abhängig vom Wert der Eigenschaft *evt_mgmt.alert_reopens_incident* entweder der Incident erneut geöffnet, ein neuer Incident erstellt oder es wird nichts unternommen.
  - Falls er erneut geöffnet wird, werden dem Incident Arbeitsnotizen hinzugefügt.
  - Wenn ein neuer Incident erstellt wird, werden alle entsprechenden Warnungsverwaltungsregeln, Warnungsaktionsregeln und Aufgabenvorlagen auf den Incident angewendet. Wenn keine übereinstimmende Warnungsaktionsregel oder Vorlage vorhanden ist, werden Felder aus dem vorhandenen Incident in einen neuen Incident kopiert.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Suchen Sie anhand der Warnungsnummer.
3. Klicken Sie im Feld **Status** auf **Erneut öffnen**.
4. Klicken Sie auf **Aktualisieren**.

Warnungseinblick-Eigenschaften

Wählen Sie diese Eigenschaften, um Warnungseinblick zu konfigurieren.

Erforderliche Rolle: evt_mgmt_admin

Die folgenden alert_insight-Eigenschaften befinden sich unter „sys_properties“.

Eigenschaft	Verwendung
Zeitrahmen	
evt_mgmt.alert_insight_alert_history_min	Legen Sie den Zeitrahmen (in Minuten) fest, um wiederholte und ähnliche Warnungsdaten abzurufen. Standard: `43200` (30 Tage) **Hinweis:** Warnungen werden unabhängig von ihrem Status (offen/erneut geöffnet/ fluktuierend/geschlossen) abgerufen.
evt_mgmt.alert_insight_closed_alert_window	Legen Sie den Zeitrahmen (in Minuten) fest, um bereits geschlossene Warnungen abzurufen. Es ist die Zeit nach dem Datum der letzten Aktualisierung der Warnung. Standard: `4320` (3 Tage)
Ähnlichkeit	
evt_mgmt.alert_insight_alert_same_as_filter	Diese Eigenschaft ist eine kommagetrennte Zeichenfolge, die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung
	definiert, welches der Warnungsfelder verwendet wird, um Warnungen als ähnlich zu betrachten. Standard: `source,type,resource,metric_name`
Zugehörige CIs	
evt_mgmt.alert_insight_related_cis_topology_levels Die Beziehungstypen sind: • CMDB-basiert (Metadatenregeln und vorgeschlagene Beziehungen) • Innerhalb von Anwendungsservices • Innerhalb von Warnungsgruppen	Für den Beziehungstyp „Innerhalb des Anwendungsservice“ legt diese Eigenschaft die Tiefe oder die maximale Ebene der Beziehung abgerufener CIs fest. Standard: `3`
Punktzahl	
evt_mgmt.alert_insight_group_mapping	Diese Eigenschaft legt die Punktzahl für Warnungsgruppenbeziehungen fest. `Standardwert`: 2
evt_mgmt.alert_insight_level_1_mapping	Diese Eigenschaft legt die Punktzahl für Beziehung der Ebene 1 fest. Standard: `3`
evt_mgmt.alert_insight_level_2_mapping	Diese Eigenschaft legt die Punktzahl für Beziehung der Ebene 2 fest. `Standardwert`: 2
evt_mgmt.alert_insight_level_3_mapping	Diese Eigenschaft legt die Punktzahl für Beziehung der Ebene 3 fest. Standard: `1`
Maximale Anzahl zugehöriger Aufgaben	
evt_mgmt.alert_insight_max_tasks	Maximale Anzahl zugehörige Aufgaben, die für Warnungseinblick abgerufen werden sollen. Standard: `10`.

Berücksichtigung von Metadatenregeln

Die über- und untergeordnete Beziehung von CIs wird berücksichtigt. Abhängige Beziehungsregeln bestehen aus Hosting- und Containment-Regeln, wobei jeder Typ die Daten aus einer anderen Perspektive des CIs modelliert.

Abhängige Beziehungsregeln verwalten:

- Um auf Regeln auf Klassenebene zuzugreifen, verwenden Sie den CI-Klassenmanager. Navigieren zu **Alle** > **Konfiguration** > **CI-Klassen Manager**.
- Verwenden Sie den Metadaten-Editor, um auf gruppierte Regeln zuzugreifen. Navigieren zu **Alle** > **Konfiguration** > **Identifikation/Ausgleich** > **Metadaten-Editor**.

Containment-Regeln stellen die Konfigurationshierarchie der CIs dar und beschreiben, welches CI welche anderen CIs enthält.

Hosting-Regeln repräsentieren die Platzierung von CIs in einer Unternehmensdefinition und beschreiben, worauf CIs ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ändern Sie die Warnungseinblick-Eigenschaften, um die Anzeige von Warnungsinformationen und -analysen im Bereich „Warnungseinblick“ zu konfigurieren.

Konfiguration zugehöriger CIs

Die folgenden Eigenschaften steuern, welche CMDB-Beziehungen für zugehörige CIs berücksichtigt werden sollen. Die CMDB-Beziehungen umfassen reguläre CMDB-Beziehungsregeln, Metadatenregeln (Containment-Regeln und Hosting-Regeln) und vorgeschlagene Beziehungen.

Eigenschaft	Verwendung
evt_mgmt.related_cis_get_all_relation_types	Abrufen aller Beziehungstypen, außer Metadatenregeln. Standardwert: `false`
evt_mgmt.related_cis_use_containment_rules	Verwendung von Metadaten-Containment-Regeln. Standardwert: `true`
evt_mgmt.related_cis_use_hosting_rules	Verwendung von Metadaten-Hosting-Regeln. Standardwert: `true`
evt_mgmt.related_cis_use_suggested_relations_rules	Verwendung von Regeln für vorgeschlagene Beziehungen. Standardwert: `false`
evt_mgmt.related_cis_validate_relation_rules	Diese Eigenschaft steuert, ob die Beziehung des CIs gemäß Metadatenregeln validiert werden soll. Standardwert: `true`

Punktzahl

Punktzahlen werden nach Beziehungstyp oder -tiefe konfiguriert. Punktzahlen werden kumuliert. Je höher die Punktzahl, desto relevanter ist das zugehörige CI zum aktuellen CI.

Beispiel:Für ein CI, das auf Ebene `2` im gleichen Anwendungsservice des aktuellen CI gefunden wurde, lautet die Punktzahl `2`. Das gleiche CI befindet sich in der gleichen Warnungsgruppe, daher gibt es eine zusätzliche Punktzahl von `3`. Die kumulierte Punktzahl ist daher `2 + 3 = 5`.

Zugehörigkeitstyp

Die Spalte Zugehörigkeitstyp in den Registerkarten **Zugehörige Incidents**, **Zugehörige Change-Anforderungen** und **Zugehörige Probleme** zeigen den Beziehungstyp an, über den das CI der ausgewählten Warnung und das zugehörige CI verfügen.

Um Beziehungen vom Typ „Zugehörigkeit“ anzuzeigen, navigieren Sie zu **Alle** > **Konfiguration** > **Identifikation/Ausgleich** > **Metadaten-Editor**.

Die Beziehung zwischen über- und untergeordneten Elementen zwischen Konfigurationselementen wird berücksichtigt:

Event-Tabellen rotieren und Warnungstabellen bereinigen

Das Wachstum von Datentabellen beeinträchtigt die Leistung. Behalten Sie die Instanzleistung durch Rotieren der Event-Tabellen und Bereinigen der Warnungstabellen für die Beibehaltung von Status- und Warnungsverlauf bei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wachstum von Event-Tabellen kontrollieren

Standardmäßig verwendet die Ereignismanagement-Event-Tabelle [em_event] die Tabellenrotation. Der Zeitplan für die Tabellenrotation stellt sicher, dass neue Daten in eine der Tabellen in der Rotationsgruppe geschrieben werden. Entsprechend dem Wert der Einstellung **Basisrotation bereinigen** wird die Basistabelle gelöscht, und dann beginnt eine neue Schreibrunde für die Tabellen in einer täglichen Rotation. Standardmäßig erfolgt diese Tabellenlöschung nach sieben Rotationen.

Informationen zum Sichern von Events in einer benutzerdefinierten Tabelle finden Sie unter Ereignismanagement-Konfigurationspräferenzen.

Wachstum von Warnungstabellen kontrollieren

Standardmäßig bereinigt ein Scheduled Job die Warnungstabelle [em_alert]. Die Bereinigung der Warnungstabelle wird für die Beibehaltung des Status und des Warnungsverlaufs empfohlen.

Zugehörige Informationen

Tabellenrotation

Event-Tabellenrotation

Tabellenrotation wird standardmäßig von Ereignismanagementverwendet, um das Wachstum von Event-Tabellen [em_event] innerhalb der Rotationstabellengruppe zu kontrollieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Tabellenrotation stellt sicher, dass die Ereignistabellen eine angemessene Größe erreichen.
Gemäß dem Zeitplan für jede Tabellenrotation werden neue Daten in eine der Tabellen in der Rotationsgruppe geschrieben. Eine Tabellenrotationsgruppe enthält die ursprüngliche Tabelle sowie mehrere zusätzliche Tabellen. Nachdem im Rotationsverfahren die letzte Tabelle einer Rotation geschrieben wurde, überschreibt die Rotation die erste Tabelle der Rotation. Standardmäßig ist die Tabellenrotation für Ereignismanagement das Rotieren von em_table in eine Offload-Tabelle, und die Basistabellenbereinigung erfolgt nach sieben Tabellenrotationen.

Prozedur

1. Navigieren zu **Systemdefinition** > **Tabellenrotationen**.
2. Klicken Sie auf **Neu**, oder wählen Sie die zu ändernde Tabellenrotationsgruppe aus.
3. Füllen Sie die Felder aus.
4. Klicken Sie auf **Absenden** oder **Aktualisieren**.

Zugehörige Informationen

Tabellenrotation

Tabellenrotation anwenden

Event-Tabellen rotieren und Warnungstabellen bereinigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status und Warnungsverlauf löschen

Sie können die automatische Tabellenbereinigung konfigurieren, um die Leistung zu verbessern. Die automatische Tabellenbereinigung wird für die Beibehaltung des Status und des Warnungsverlaufs empfohlen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Datensätze älter als 90 Tage sind, werden sie standardmäßig gelöscht. Wenn Datensätze für einen längeren Zeitraum aufbewahrt werden, werden größere Datenmengen gespeichert, und die Leistung kann beeinträchtigt werden.

Hinweis: Standardmäßig wird zur Kontrolle des Wachstums der Event-Tabelle [em_event] Tabellenrotation verwendet. Informationen zum Sichern von Events in einer benutzerdefinierten Tabelle finden Sie unter Ereignismanagement-Konfigurationspräferenzen.

Prozedur

1. Navigieren zu **Alle** > **Automated Test Framework** > **Administration** > **Tabellenbereinigung**.
2. Verkürzen Sie bei Bedarf den Aufbewahrungszeitraum (in Sekunden) für Datensätze der Tabelle „Warnungen“ [em_alert]: (Standard: 7.776.000).

Zugehörige Informationen

Event-Tabellen rotieren und Warnungstabellen bereinigen

Event-Tabellenrotation

Tabellen „Warnungsverlauf“ und „Auswirkungsstatus“ bereinigen

Bereinigung der Warnungstabelle

Tabellen „Warnungsverlauf“ und „Auswirkungsstatus“ bereinigen

Planen Sie Aufträge, um alte Warnungsdatensätze in den Tabellen „Warnungsverlauf“ [em_alert_history] und „Auswirkungsstatus“ [em_impact_status] zu markieren und zu entfernen und so zu verhindern, dass die Tabellen mit Daten überladen werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Planen Sie die folgenden Aufträge, um alte Warnungsdatensätze zu entfernen:

- **Auffüllen**: Bestimmt, wann Warnungen zum Löschen markiert werden sollen
- **Clean**: Löscht die Warnungen

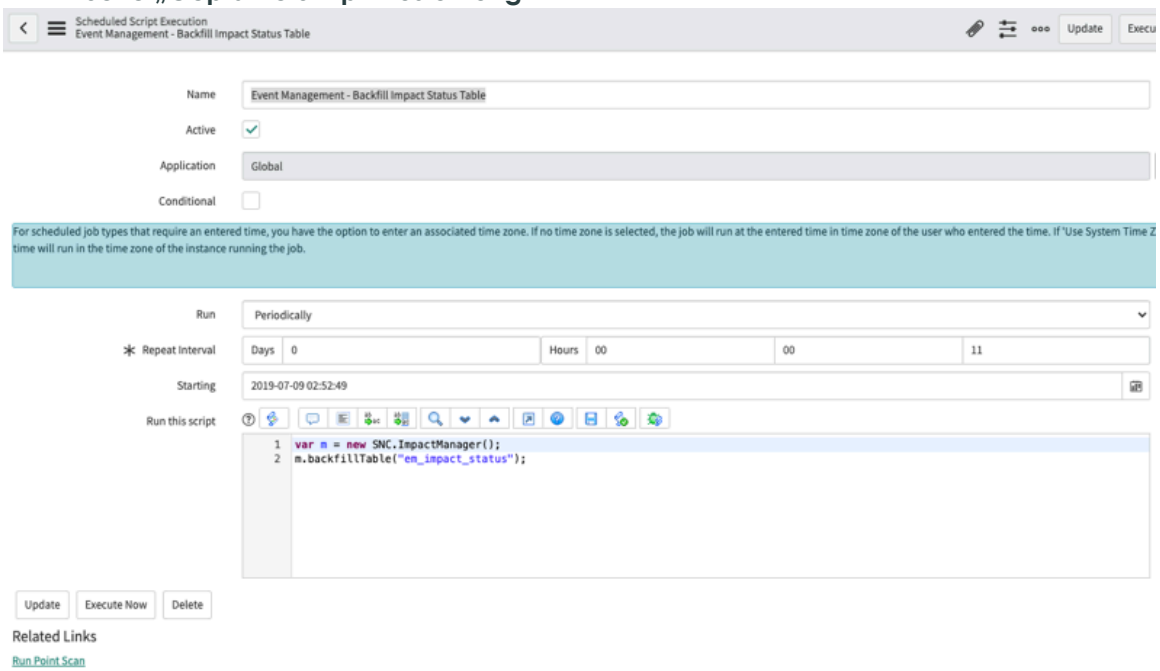
Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.
   Die Seite **Scheduled Jobs** wird angezeigt.
2. So bestimmen Sie, wie oft Warnungen in der Tabelle **Auswirkungsstatus** zum Löschen markiert werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Suchen Sie nach der Aufgabe **Event Management – Auswirkungsstatustabelle für Auffüllung** und wählen Sie sie aus.
Die Seite **Geplante Skript-Ausführung** wird angezeigt.

Seite „Geplante Skript-Ausführung“



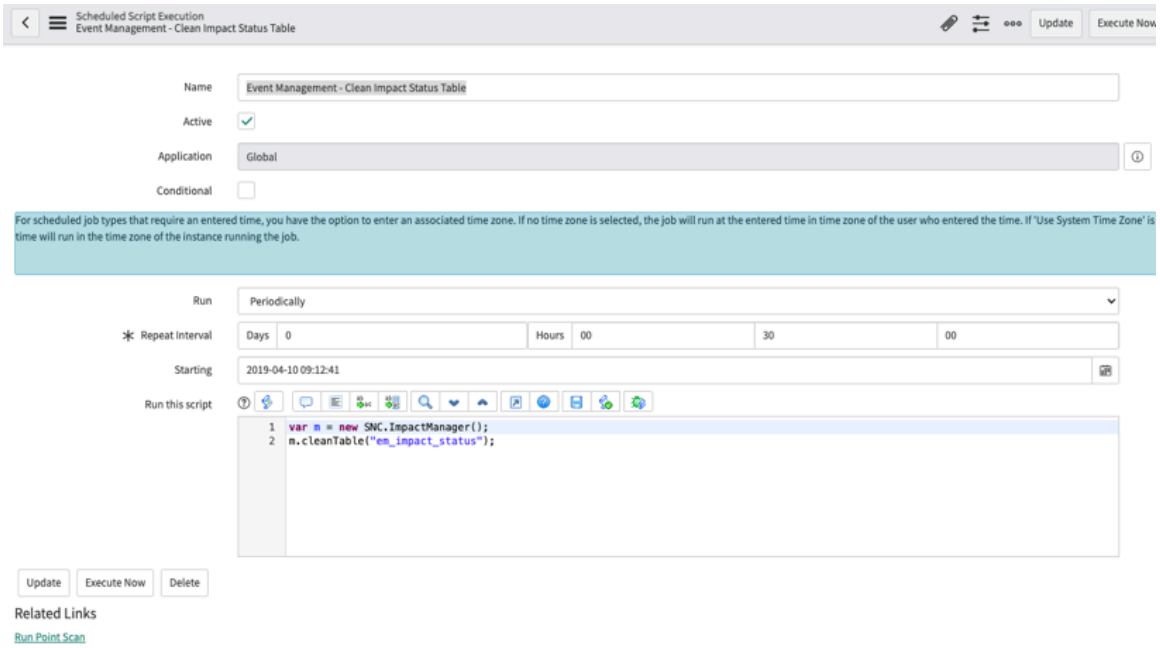
b. Konfigurieren Sie im Feld **Wiederholungsintervall**, wie oft der Auftrag ausgeführt werden soll.
Um den Auftrag sofort auszuführen, wählen Sie **Jetzt ausführen** aus.

c. Wählen Sie **Aktualisieren**.

3. So entfernen Sie alte Warnungen aus der Tabelle **Auswirkungsstatus**:

a. Suchen Sie nach der Aufgabe **Event Management – Tabelle mit Auswirkungsstatus bereinigen** und wählen Sie sie aus.
Die Seite **Geplante Skript-Ausführung** wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



b. Konfigurieren Sie im Feld **Wiederholungsintervall**, wie oft der Auftrag ausgeführt werden soll.
Um den Auftrag sofort auszuführen, wählen Sie **Jetzt ausführen** aus.

c. Wählen Sie **Aktualisieren**.

4. Wiederholen Sie die Schritte 2 und 3, um die Auffüll- und Bereinigungsaufträge für die **Tabelle „Warnungsverlauf“** auszuführen.

Bereinigung der Warnungstabelle

Die Funktion „Scheduled Jobs“ führt ein Skript aus, das Warnungen in der Warnungstabelle [em_alert] schließt, die bestimmte Bedingungen erfüllen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn das Event Management-Plugin aktiviert ist, wird standardmäßig ein Job zur Ausführung des Skripts `Event Management – Warnungen automatisch schließen` geplant, um Warnungen in der Warnungstabelle, die die angegebenen Bedingungen erfüllen, automatisch zu schließen.

Aufgrund des hohen Datenverkehrs zur Tabelle können Sie die Warnungstabelle [em_alert] nicht als Ganzes prüfen. Auditieren Sie stattdessen die ausgewählten relevanten Felder in der Tabelle.

Prozedur

1. Legen Sie die Tabelle auf `audit = true` fest.

2. Legen Sie `audit = true` für die relevanten Felder fest.
Um übermäßig viele Audit-Datensätze zu vermeiden, prüfen Sie nur die Felder, die für die Prüfung erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Das Skript `Event Management – Warnungen automatisch schließen` wird automatisch ausgeführt und zu geplanten Zeiten wiederholt. Dabei schließt es Warnungen, die die angegebenen Bedingungen erfüllen.

Zugehörige Informationen

Event-Tabellen rotieren und Warnungstabellen bereinigen

Event-Tabellenrotation

Status und Warnungsverlauf löschen

Warnungsgruppierung

Die Warnungsgruppierung ist der Prozess des Organisierens und Konsolidierens zugehöriger Warnungen in Gruppen basierend auf gemeinsamen Merkmalen oder Kriterien. Dies vereinfacht die Warnungsverwaltung durch die Reduzierung von Rauschen. So können Sie Probleme effizienter priorisieren, nachverfolgen und beheben. Gruppierte Warnungen bieten einen klareren Überblick über zugehörige Incidents und ermöglichen eine schnellere Ursachenanalyse und Behebung.

Informationen zur Gruppierung von Warnungen

Sehen Sie sich dieses kurze Video an, um zu erfahren, wie Warnungsgruppierungen Warnungen basierend auf bestimmten Kriterien in Clustern organisieren.

Video, in dem erläutert wird, wie Warnungsgruppierungen Warnungen basierend auf bestimmten Kriterien in Clustern organisieren.

Funktionsweise der Warnungsgruppierung

Die Gruppierung von Warnungen erhöht die betriebliche Effizienz und optimiert das Warnungsmanagement durch die Kategorisierung von Warnungen. So funktioniert es:

1. Ereigniskonsolidierung: Ereignismanagement sammelt Warnungen aus mehreren Quellen und bietet eine zentralisierte Ansicht von Benachrichtigungen und Warnungen. Diese Konsolidierung ermöglicht es Teams, Warnungen effizienter zu verwalten und kritische Probleme leichter zu erkennen.
2. Kontextbezogene Ergänzung: Warnungen werden mit Daten aus der Configuration Management Database (CMDB) angereichert, die detaillierte Informationen zu Anwendungen und Infrastrukturkomponenten enthalten. Dieser Kontext ermöglicht Teams, die Bedeutung von Warnungen besser zu verstehen und Antworten basierend auf ihrer Auswirkung zu priorisieren.
3. Intelligente Korrelation: Ereignismanagement nutzt verschiedene Arten von Algorithmen für maschinelles Lernen, um zugehörige Warnungen automatisch zu gruppieren. Diese intelligente Gruppierung reduziert das Warnungsrauschen, indem ähnliche Warnungen kombiniert werden. So können sich Teams auf wichtige Probleme konzentrieren, anstatt mit mehreren Benachrichtigungen überhäuft zu werden.

Vorteile der Warnungsgruppierung

- Durch die Zusammenfassung von Warnungen auf Grundlage vordefinierter Muster werden automatisierte Warnmeldungsgruppen erstellt.
- Korrelieren von Warnungen mithilfe von Zeitstempeln und CI-Identifizierung, um automatisierte Warnungsgruppen zu bilden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CMDB -basierte Warnungsgruppierung durch Korrelation von Warnungen basierend auf CI-Beziehungen in der CMDB bilden.
- Korrelieren von Warnungen basierend auf der Textähnlichkeit von Warnungen mithilfe von NLP (Natural Language Processing).

Zugehörige Informationen

Warnungsantwort wird mit automatischer Warnungsgruppierung synchronisiert

Warnungsgruppierung und Anwendungsfälle

Die Methoden zur Gruppierung von Warnungen reichen von anwenderdefinierten Ansätzen (manuell, regelbasiert und Tag-Cluster) bis zu erweiterten, gut abstimmbaren Algorithmen (automatisch, CMDB, textbasiert, Log Analytics und Netzwerkdatenverkehr).

Warnungsgruppierungstypen und Anwendungsfälle

Typ	Beschreibung	Anwendungsfall
Log Analytics-Gruppierung	Warnungen werden basierend auf der Analyse der Protokolldaten gruppiert. Dies beinhaltet die Korrelation von Protokolleinträgen, um zugehörige Incidents und Probleme zu identifizieren. Durch die Nutzung von Protokollmustern und -sequenzen kann diese Methode komplexe Probleme mit mehreren Schritten in der gesamten IT-Umgebung erkennen.	Ein Online-Gaming-Unternehmen verbessert die Serverstabilität durch die Implementierung proaktiver Protokollanalysen. Sie überwachen Protokolle von Spielservern in Echtzeit und verwenden Analysetools, um Fehlermuster zu erkennen, die vor Abfällen auftreten. Die Analyse zeigt beispielsweise, dass bestimmte Fehlermuster etwa 30 Minuten vor einem Serverabsturz auftreten. Durch die Einrichtung automatisierter Warnungen für diese Muster kann das Unternehmen Korrekturmaßnahmen initiieren, z. B. den Neustart von Services oder die Neuzuteilung von Ressourcen, bevor ein Absturz auftritt. Dieser proaktive Ansatz verhindert Unterbrechungen, minimiert Ausfallzeiten und verbessert die Spielerfahrung, indem Probleme behoben werden, bevor sie sich auf die Akteure auswirken.
Regelbasierte Gruppierung	Warnungen werden nach vordefinierten Regeln und Kriterien gruppiert,	In einem Rechenzentrum, in dem eine E-Commerce-Website verwaltet wird,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen und Anwendungsfälle (Fortsetzung)

Typ	Beschreibung	Anwendungsfall
	die von Anwendern festgelegt wurden. Diese Regeln können bestimmte Bedingungen enthalten, z. B. Schwellenwerte oder Ereignistypen. Diese Methode ist effektiv für konsistente und wiederholbare Muster, erfordert jedoch die Wartung der Regeln.	hilft eine regelbasierte Warnungsgruppierung bei der Bewältigung von hohem Datenverkehr bei Ereignissen wie Flash-Sales. Warnungen zu Serverproblemen (z. B. hohe CPU-Auslastung) werden als übergeordnete Warnungen bezeichnet. Diese übergeordneten Warnungen sind mit untergeordneten Warnungen verknüpft, die zugehörige Probleme melden, z. B. langsame Datenbankabfragen. Die Regeln stellen sicher, dass serverbezogene Warnungen mit ihren Symptomen gruppiert werden, damit das IT-Team Probleme mit der Serverüberlastung schnell erkennen und beheben kann. Dieser Ansatz verbessert die Effizienz der Problemlösung und minimiert Ausfallzeiten.
Automatisierte Gruppierung	Hochentwickelte Algorithmen identifizieren und gruppieren zugehörige Warnungen automatisch auf Grundlage von Mustern und Ähnlichkeiten in den Warnungsdaten. Diese Methode nutzt maschinelles Lernen und KI, um sich an neue und unbekannte Probleme anzupassen und ein proaktives Warnungsmanagement zu ermöglichen. Ereignismanagement gruppiert Warnungen, die ähnlich, aber nicht unbedingt identisch sind, basierend auf der zeitlichen Nähe zur letzten Ereignisgenerierung.	Ein großes Finanzinstitut verwendet maschinelles Lernen, um Warnungen von zahlreichen Servern und Anwendungen zu verwalten. Das System analysiert historische Warnungsdaten, um Muster zu erkennen, z. B. Datenbankserverausfälle, die häufig von Clientverbindungsfehlern begleitet werden. Dann werden zugehörige Warnungen automatisch gruppiert. Wenn beispielsweise eine neue Datenbankserverfehlerwarnung erkannt wird, wird sie mit vorherigen Verbindungsfehlerwarnungen gruppiert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen und Anwendungsfälle (Fortsetzung)

Typ	Beschreibung	Anwendungsfall
	Warnungen mit demselben CI und demselben Musterbezeichner werden in einer Gruppe zusammengefasst. Die automatische Warnungsgruppierung besteht aus den folgenden Komponenten. • Warnungszusammenfassung – Lerner (**Service Analytics Warnungszusammenfassung – Lerner – Täglich**): Dieser Offline-Auftrag wird täglich ausgeführt, um vergangene Warnungen zu verarbeiten und statistische Analysen durchzuführen, um Warnungsmuster zu erstellen. Details finden Sie unter Konfigurieren Sie die musterbasierte Warnungsgruppierung. • Echtzeitwarnungszusammenfassungsauftrag (**Service Analytics-Gruppenwarnungen mit RCA/ Warnungszusammenfassung**): Dieser Auftrag wird jede Minute ausgeführt, um Warnungszusammenfassungsgruppen basierend auf Warnungsmustern, CMDB-Beziehungen, Textähnlichkeit, anwenderdefinierten Warnungs-Clustering-Tags und Netzwerkdatenverkehrsverbindung zu generieren zwischen Prozessen.	Diese automatisierte Gruppierung hilft den IT- und Sicherheitsteams, Probleme schnell zu erkennen und zu beheben, die Antwortzeiten zu verbessern und die Ausfallzeiten zu reduzieren.
CMDB-basierte Gruppierung	Warnungen werden basierend auf Configuration Item (CI)-Beziehungen und Abhängigkeiten von der Configuration Management Database (CMDB) gruppiert. Dieser Ansatz stellt sicher, dass Warnungen, die	Ein Telekommunikationsunternehmen verwendet CMDB-Daten, um Warnungen im Zusammenhang mit seiner Netzwerkinfrastruktur zu verwalten. Warnungen, die sich auf einen bestimmten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen und Anwendungsfälle (Fortsetzung)

Typ	Beschreibung	Anwendungsfall
	sich auf bestimmte Infrastrukturkomponenten oder Services beziehen, gruppiert werden, was eine kontextbezogene Warnungsverwaltung ermöglicht.	Netzwerkrouter und die zugehörigen Geräte beziehen, werden auf Grundlage ihrer CMDB-Beziehungen gruppiert, sodass das Netzwerkteam alle zugehörigen Probleme erkennen und die Ursache effizient beheben kann.
Textbasierte Gruppierung	Warnungen werden gruppiert, indem der Textinhalt der Warnungen analysiert wird, um Ähnlichkeiten und zugehörige Probleme zu identifizieren. NLP-Techniken (Natural Language Processing) werden verwendet, um Gemeinsamkeiten in der Warnungsbeschreibung, dem Metriknamen und der CI-Klasse zu finden. Dadurch ist diese Methode für unstrukturierte Daten effektiv.	In einer Organisation, die Zoom-Räume für virtuelle Besprechungen verwendet, erhält das IT-Team zahlreiche Warnungen, wenn der Zoom-Raum-Server ausfällt. Jede Warnung kann darauf hinweisen, dass ein anderer Zoom-Raum ausgefallen ist, z. B. Zoom-Raum Nr. 10 ist ausgefallen, Zoom-Raum Nr. 11 ist ausgefallen usw., wobei der einzige Unterschied in der Raumnummer besteht. Bei Organisationen mit einer CMDB können diese Warnungen mithilfe von CMDB-Beziehungen gruppiert werden, da das System die Warnungen basierend auf der Auswirkung des Servers auf alle zugehörigen Zoom-Räume korrelieren kann. Für Organisationen ohne CMDB kann jedoch die textbasierte Gruppierung verwendet werden. Das System wendet die Verarbeitung natürlicher Sprache auf Gruppenwarnungen mit ähnlichen Beschreibungen an, damit das IT-Team schnell erkennen kann, dass mehrere Zoom-Räume von demselben zugrunde liegenden Serverproblem betroffen sind. Dieser Ansatz ermöglicht es dem IT-Team, die Ursache des Problems effizient zu beheben, Ausfallzeiten zu reduzieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen und Anwendungsfälle (Fortsetzung)

Typ	Beschreibung	Anwendungsfall
		und die Antwortzeiten zu verbessern.
Tag-Clustergruppierung	Warnungen werden mithilfe von Tags oder Bezeichnungen kategorisiert und gruppiert, die allgemeine Attribute wie Anwendung, Servertyp oder geografischer Standort darstellen. Diese Methode ermöglicht eine flexible und dynamische Gruppierung basierend auf sich entwickelnden Tagging-Strategien.	Eine Organisation ohne CMDB verwaltet einen Linux-Server, auf dem verschiedene Services ausgeführt werden. Das IT-Team verwendet in jeder Warnung ein **Knotenfeld**, um den Server zu identifizieren, und gruppiert alle Ereignisse, die sich auf Services auf demselben Server beziehen, basierend auf diesem Knotenwert. Beispielsweise gruppieren sie Warnungen wie „Service A ausgefallen“ und „Service B – hohe CPU-Auslastung“, wenn sie denselben Knotenwert verwenden. Dieser Ansatz hilft dem IT-Team, serverbezogene Probleme effizienter zu beheben. Durch das Clustering von Warnungen für denselben Knoten, dieselbe Anwendung oder dieselbe IP-Adresse optimiert das Team seine Antwortmaßnahmen und löst Probleme effektiver, auch ohne CMDB.
Manuelle Gruppierung	Benutzer wählen und gruppieren zugehörige Warnungen manuell, je nach Fachwissen und Verständnis des Systems. Dieser Ansatz ermöglicht eine präzise Steuerung, kann jedoch zeitaufwändig sein und automatisierte Korrelationen fehlen.	Ein Systemadministrator erhält mehrere Warnungen zu verschiedenen Services, die auf einem einzelnen Server fehlschlagen. Der Administrator gruppiert diese Warnungen manuell und erkennt, dass sie alle auf einen einzelnen Hardwarefehler auf diesem Server zurückzuführen sind. Er priorisiert die Behebung des Hardwareproblems, um alle Services wiederherzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die manuelle und regelbasierte Gruppierung von Warnungen unterscheidet sich von der auf Algorithmen basierenden Gruppierung hauptsächlich dadurch, wie die übergeordnete Warnung ausgewählt wird. Bei manueller, regelbasierter oder Log Analytics-Gruppierung wird eine der echten Warnungen als übergeordnete Warnung festgelegt. In den Modi „Automatisch“, „CMDB“, „Textbasiert“, „Tag-Cluster“ und „ Netzwerkverkehrwird eine virtuelle Warnung, die die älteste und schwerwiegendste Warnung in der Gruppe darstellt, als übergeordnete Warnung erstellt.

Hinweis: In domänengetrennten Umgebungen werden Warnmeldungsgruppen nur für Warnungen innerhalb derselben Domäne erstellt.

Informationen zu geplanten Aufgaben und Parametern finden Sie unter Geplante Aufgaben und Parameter für die Gruppierung von Warnungen. Ausführliche Informationen zu den verschiedenen Gruppierungstypen finden Sie unter Warnungsgruppierungstypen und -erstellungsmethoden.

Geplante Aufgaben und Parameter für die Gruppierung von Warnungen

Automatisieren Sie die Warnungsorganisation, indem Sie -Aufträge konfigurieren, um Warnungen basierend auf vordefinierten Kriterien und Parametern zu gruppieren.

Um Warnungen in automatisierten, CMDB-, textbasierten, Tag-Cluster- und Netzwerkdatenverkehrskorrelations-Gruppen zu gruppieren, wird die geplante Aufgabe mit der Bezeichnung **„Service Analytics-Gruppenwarnungen mit RCA/ Warnungszusammenfassung“** normalerweise einmal pro Minute ausgeführt. Dieser Auftrag verarbeitet die Gruppierung von Warnungen basierend auf der angegebenen Methode. Darüber hinaus können Sie mehrere geplante Aufgaben parallel ausführen, um die Gruppierung von Warnungen effizienter zu verwalten. Weitere Informationen finden Sie unter Führen Sie mehrere geplante Aufgaben für die Gruppierung von Warnungen aus.

Um zu definieren, welche Warnungen gruppiert werden, werden die folgenden Parameter verwendet:

- *sa_analytics.aggregation_enabled*: Dieser Parameter aktiviert die von der geplanten Aufgabe erstellte Warnungsgruppierung. Legen Sie die Eigenschaft *Enable alert aggregation for Automated, CMDB, and Text-Based groups* auf „`true`“ fest, um diese Funktion zu aktivieren.

  Hinweis: Diese Eigenschaft gilt auch für die Gruppierung von Tag-Clustern und Netzwerkdatenverkehrkorrelationen.

- *sa_analytics.agg.query_dynamic_window*: Standardmäßig ist diese auf 10 Minuten (600 Sekunden) festgelegt. Sie definiert den maximal zulässigen Zeitunterschied zwischen den Zeitpunkten der letzten Ereignisgenerierung von zwei Warnungen, die zusammen gruppiert werden können.
- *sa_analytics.agg.query_max_group_lifetime*: Dieser Parameter gibt den maximalen Zeitraum von der Generierung der ersten Warnung bis zur letzten Warnung in einer Gruppe an, mit einem Standardwert von 30 Minuten (1800 Sekunden). Wenn Ereignisse mit einer Verzögerung eintreffen, die diesen Zeitraum überschreitet, kann mit dem Parameter *sa_analytics.agg.group_expiration_time* die Gruppierungszeit auf über 30 Minuten verlängert werden.

Hinweis: Einige Parameter, wie z. B. **sa_analytics.agg.query_dynamic_window**, **sa_analytics.agg.query_max_group_lifetime**und **sa_analytics.agg.group_expiration_time**, werden nicht standardmäßig bereitgestellt. Um diese Eigenschaften zu verwenden, müssen Sie Eigenschaften mit denselben Namen erstellen und ihnen die erforderlichen Werte zuweisen. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Wie Warnungen gruppiert werden

Bei der Tag-Cluster-Gruppierung werden Warnungen basierend auf dem Zeitrahmenparameter, der in den Einstellungen für das Warnungs-Tag-Clustering definiert ist, einer Gruppe hinzugefügt. Für die automatisierte, CMDB- und textbasierte Gruppierung des Netzwerkdatenverkehrs werden Warnungen wie folgt zusammengefasst.

Berücksichtigen Sie die folgenden Warnungen mit demselben CI. (Sie können alle derselben CMDB-Gruppe hinzugefügt werden).

- Warnung 1: Erste Ereignisgenerierung um 01:00:00 Uhr
- Warnung 2: Generierung des ersten Ereignisses um 01:11:00
- Warnung 3: Generierung des ersten Ereignisses um 01:13:00
- Warnung 4: Generierung des ersten Ereignisses um 01:16:00
- Warnung5: Generierung des ersten Ereignisses um 01:25:00
- Warnung6: Erste Ereignisgenerierung um 01:34:00 Uhr
- Warnung 7: Generierung des ersten Ereignisses um 01:43:00

Warnung1 und Warnung2 werden aufgrund des Zeitabstands von mehr als 10 Minuten nicht gruppiert. Alert2 und Alert3 erstellen um 01:13:00 eine Gruppe. Das dynamische 10-Minuten-Fenster beginnt um 01:13:00 Uhr mit:

- Alert4 wird der Gruppe um 01:16:00 hinzugefügt. Dadurch wird das 10-Minuten-Fenster neu gestartet.
- Alert5 und Alert6 werden der Gruppe hinzugefügt, da ihre Ereigniszeiten innerhalb des 10-Minuten-Fensters liegen.
- Warnung7 wird der Gruppe nicht hinzugefügt, da sie 9 Minuten nach Warnung6 eintrifft und somit das Limit *sa_analytics.agg.query_max_group_lifetime* von maximal 30 Minuten Gruppenlebensdauer ab der ursprünglichen Gruppenerstellung (01:13:00 + 30 Minuten = 01:43:00) überschreitet. .

Konfigurieren Sie die geplante Aufgaben-basierte Warnungsgruppierung

Richten Sie Regeln und Parameter ein, um zugehörige Warnungen automatisch zu gruppieren, um die Warnungsverwaltung zu optimieren und das Warnungsrauschen zu reduzieren.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Die geplante Aufgabe „Serviceanalysen: Gruppenwarnungen mit RCA/ Warnungszusammenfassung“ hilft beim Gruppieren von Warnungen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Warnungskorrelationsregeln**.
2. Aktivieren Sie auf der Seite „Warnungskorrelationseigenschaften“ die relevanten Eigenschaften.
   - Aktivieren Sie die CMDB-Korrelation (*sa_analytics.agg.query_cmdb_correlation_enabled*).
   - Aktivieren Sie die Korrelation des Netzwerkdatenverkehrs (*sa_analytics.agg.query_network_traffic_correlation_enabled*).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Aktivieren Sie die ML-basierte Automatisierungskorrelation (*sa_analytics.specific_patterns_enabled*).
- Aktivieren Sie die textbasierte Korrelation (*sa_analytics.text_based_group_enabled*).
- Eigenschaft „Gruppieren nach“ mit einer kommagetrennten Liste von Feldnamen, die übereinstimmende Werte für alle Warnungen aufweisen müssen, damit Warnungen zusammen gruppiert werden können. Die Eigenschaft kann Warnungsfeldnamen (z. B. „assignment_group“), CI-Feldnamen (z. B. alert_cmdb_ci.location), Feldnamen für zusätzliche Warnungsinformationen (z. B. „additional_info.state“) oder Warnungs-Tags (z. B. t_data_center) enthalten. Wenn die angegebenen Feldwerte zwischen Warnungen übereinstimmen, können diese Warnungen in einer Gruppe zusammengefasst werden (*sa_analytics.agg.group_alert_with_same_group_by_fields*).
- Maximale Anzahl von Beziehungen zwischen CIs in einer Topologie, die eine CMDB-Gruppe bilden (*sa_analytics.agg.query_cmdb_graph_walk_nodes*).
- Alle CMDB-Beziehungen für CMDB-Gruppenkorrelation verwenden (*evt_mgmt.related_cis_get_all_relation_types*).

3. Wählen Sie **Speichern**.

   Um Warnungen ohne CI als textbasierte oder ML-basierte Gruppen zu gruppieren, legen Sie *sa_analytics.enable_no_ci_grouping* auf `true` fest. Stellen Sie sicher, dass der Funktionsbezeichner sowohl den Knoten- als auch den Metriknamen enthält. Weitere Informationen zum Konfigurieren des Feature-Bezeichners finden Sie unter Geben Sie Musterbezeichner-Attribute für die Warnungsgruppierung an, und verwalten Sie sie.

4. Wahlweise: Legen Sie *evt_mgmt.alert_groups_reasoning.enable_worknotes* auf `„Keine“` fest, um zu verhindern, dass Arbeitsnotizen für Gruppenbegründungen angezeigt werden.

   (Optional) Standardmäßig wird auf der Registerkarte **Aktivitäten** eine Arbeitsnotiz mit dem Gruppierungsgrund angezeigt, wenn eine Gruppe erstellt oder aktualisiert wird.

Zugehörige Informationen

Automatisierte Warnungsgruppierung

CMDB -basierte Warnungsgruppierung

Textbasierte Warnungsgruppierung

Gruppierung von Tag-Clustern von Warnungen

Führen Sie mehrere geplante Aufgaben für die Gruppierung von Warnungen aus

Führen Sie mehrere geplante Aufgaben parallel aus, um Warnungen zu gruppieren. Dies verhindert eine Überlastung des Systems bei Überschreitungen (Warnungsstorme).

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die aktuelle geplante Aufgabe wird mit einem einzelnen Thread ausgeführt. Während Warnungsüberschreitungen (Warnungsstürze) dauert die Verarbeitung erheblich länger. Um diese Auswirkungen zu beheben, können jetzt mehrere Aufgaben Warnungen innerhalb der geplanten Aufgabe verarbeiten. Dies verbessert die Skalierbarkeit und die Gesamtleistung in Zeiten mit hohem Volumen.

Die Anzahl der Aufträge, die bei der Warnungsverarbeitung ausgeführt werden sollen, ist in einer neuen Eigenschaft *sa_analytics.agg.alert_grouping.num_of_jobs* definiert. Die Auftragsnummer wird als Parameter an die entsprechende Methode gesendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: In diesem Szenario wird das Verfahren zum Erhöhen der horizontalen Skalierung von keiner horizontalen Skalierung (einzelner Auftrag) auf 2 Aufträge gezeigt.

Sie können mehrere geplante Aufgaben parallel effizient verwalten und ausführen, um Warnungen mithilfe bestimmter Eigenschaften zu gruppieren. Mit diesen Eigenschaften können Sie die Gruppierungskriterien an Ihre Anforderungen anpassen, um sicherzustellen, dass Warnungen basierend auf Zuweisungsgruppen, Domain Separation-Feldern oder „Gruppieren nach"-Feldern verarbeitet werden. Die verfügbaren Eigenschaften sind:

- *sa_analytics.agg.group_alert_with_same_assignment_group_only*: Gruppiert Warnungen, die dieselbe Zuweisungsgruppe verwenden. Standardmäßig ist der Wert auf „false" festgelegt. Wenn Sie diese Eigenschaft auf „true" festlegen möchten, erstellen Sie eine Eigenschaft mit demselben Namen, und legen Sie den Wert auf „true" fest.
- *sa_analytics.agg.group_alert_with_same_domain_only*: Gruppiert Warnungen, die zu derselben Domäne gehören. Standardmäßig ist der Wert auf „true" festgelegt.
- *sa_analytics.agg.group_alert_with_same_group_by_fields*: Eigenschaft „Gruppieren nach" mit kommagetrennter Liste von Feldnamen, die übereinstimmende Werte für alle Warnungen aufweisen müssen, damit Warnungen zusammen gruppiert werden können. Die Eigenschaft kann Warnungsfeldnamen (z. B. „assignment_group"), CI-Feldnamen (z. B. alert_cmdb_ci.location), Feldnamen für zusätzliche Warnungsinformationen (z. B. „additional_info.state") oder Warnungs-Tags (z. B. t_data_center) enthalten. Wenn die angegebenen Feldwerte zwischen Warnungen übereinstimmen, können diese Warnungen in einer Gruppe zusammengefasst werden.

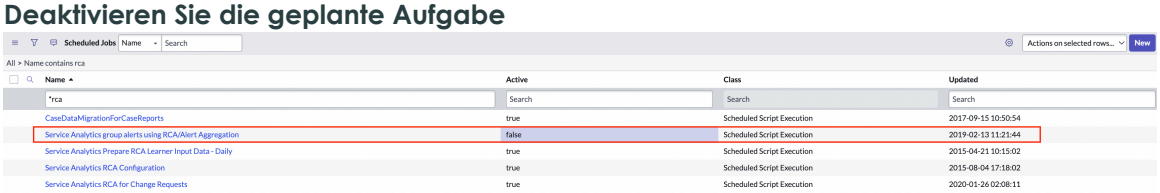
Hinweis: Um eine effiziente horizontale Skalierung sicherzustellen, muss mindestens eine dieser Eigenschaften definiert werden, um eine Form der Trennungs- oder Gruppierungslogik einzurichten. Dies ist erforderlich, um sicherzustellen, dass alle Warnungen, die zu derselben Gruppe gehören, von bestimmten Aufgaben korrekt verarbeitet werden, wodurch eine logische Trennung der Warnungen entsteht.

Wenn mindestens eine dieser Eigenschaften nicht auf „wahr" festgelegt wird, werden die Warnungen nicht ordnungsgemäß getrennt. Wenn Sie beispielsweise keine Gruppierungslogik definieren (legen Sie eine Eigenschaft auf „wahr" fest) und sowohl die Zuweisungsgruppe als auch die Domänentrennung auf „falsch" festgelegt sind, funktioniert die horizontale Skalierung nicht, und alle Warnungen werden von einer einzigen geplanten Aufgabe verarbeitet .

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.
2. Suchen Sie die geplante Aufgabe: Service Analytics-Gruppenwarnungen mit RCA/ Warnungszusammenfassung.
3. Legen Sie für alle vorhandenen Service Analytics-Gruppenwarnungen für geplante Aufgaben mit RCA/Warnungszusammenfassung den Wert in der Spalte **Aktiv** auf **false**fest.

Deaktivieren Sie die geplante Aufgabe



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Erstellen Sie eine neue Eigenschaft *sa_analytics.agg.alert_grouping.num_of_jobs*, oder aktualisieren Sie, falls sie bereits vorhanden ist, die Eigenschaft auf die gewünschte Anzahl mehrerer geplanter Aufgaben für die Warnungsgruppierung, z. B. 2 oder 4.
5. Klonen Sie die Definition der geplanten Aufgabe aus der Tabelle „Geplante Aufgaben“ [sys_auto] in die gewünschte Anzahl mehrerer geplanter Aufgaben für die Warnungsgruppierung.
6. Rufen Sie in den neuen Aufträgen im Abschnitt „Dieses Skript ausführen“ die neue JS-Funktion „queryS0“ (anstelle der alten Funktion „query()“) auf, und übergeben Sie ihr die Auftragsnummer als Eingabeparameter.

   Hinweis: Auftragsnummern müssen bei 0 beginnen und werden aufeinanderfolgenden Reihenfolgen folgen: 0, 1, 2, 3, 4...

7. Korrigieren Sie Hashes in den Tabellen [sa_analytics_status] und [sa_hash], indem Sie den frühesten Hash mit demselben Präfix auswählen, ihn klonen und das Hash-Namensuffix hinzufügen, z. B. „_groupingX“, wobei „X“ für die Auftragsnummer steht.

   Wenn Sie von keiner horizontalen Skalierung (einzelner Auftrag) auf 2 Aufträge hochskalieren und den Hash-Namen `last_alert_process_time`klonen möchten, klonen Sie ihn, um den gleichen Wert wie in `„last_alert_process_time“`beizubehalten:

   - `last_alert_process_time_grouping0`
   - `last_alert_process_time_grouping1`

   Wenn Sie die horizontale Skalierung von keiner horizontalen Skalierung (einzelner Auftrag) auf 4 Aufträge für den Hashnamen `last_alert_process_time`durchführen möchten, klonen Sie ihn, um den gleichen Wert wie in `„last_alert_process_time“`beizubehalten:

   - `last_alert_process_time_grouping0`
   - `last_alert_process_time_grouping1`
   - `last_alert_process_time_grouping2`
   - `last_alert_process_time_grouping3`

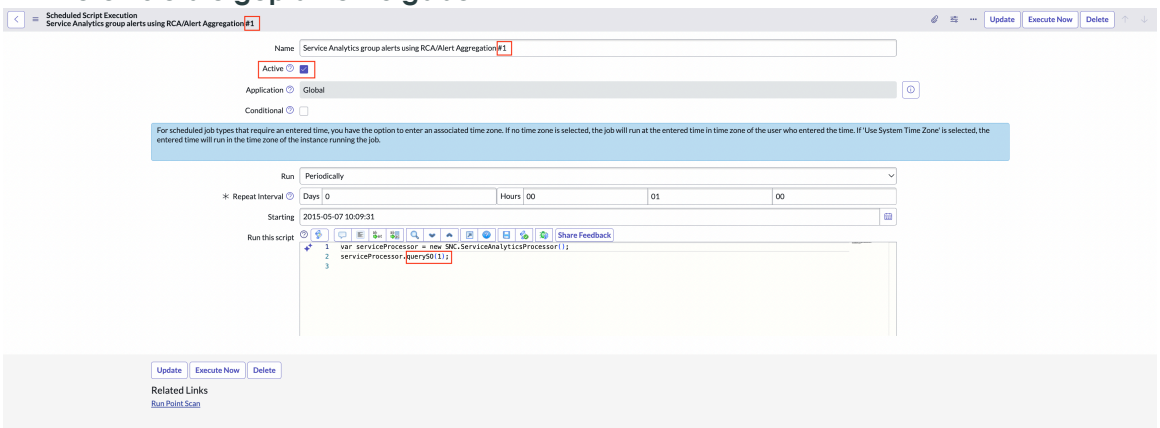
Zu klonende Hashes

Hash-Name	Tabelle
Abfrage_Auftrag_letzte_Ausführung	sa_hash
last_alert_process_time	sa_analytics_status
last_staging_table_update_time	sa_analytics_status
last_staging_table_truncate_time	sa_analytics_status
Analytics_trigger_g1	sa_hash

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Aktivieren Sie die neuen Aufträge, indem Sie für jeden Auftrag das Kontrollkästchen **Aktiv** aktivieren.

Aktivieren Sie die geplante Aufgabe



Ergebnisse

Die geplante Aufgabe „Service Analytics-Gruppe Warnungen mit RCA/ Warnungszusammenfassung“ ist so eingerichtet, dass mehrere Aufgaben gleichzeitig für die Gruppierung von Warnungen ausgeführt werden.

Konfigurieren Sie die Reihenfolge der Warnungskorrelationslogik

Verbessern Sie das Warnungsmanagement, indem Sie Benutzern ermöglichen, die Reihenfolge der Korrelationslogik anzupassen. Mit dieser Funktion können Sie Korrelationsmethoden an ihre spezifischen Anforderungen anpassen und so die Priorisierung von Warnungen und die Reaktionseffizienz verbessern.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen Sie nach der Eigenschaft *sa_analytics.agg.query.group_logic_order*.

   Der Standardwert ist „CMDB,NETWORK_TRAFFIC,TAG_BASED,PATTERN,TEXTBASE“. Dies ist eine durch Kommas getrennte Liste der Gruppierungstypen in der Reihenfolge ihrer Ausführung.

   Hinweis: Wenn einer der Gruppierungstypen in der Eigenschaft nicht angegeben ist, muss er manuell hinzugefügt werden. Warnungskorrelationsregeln sind auslöserbasiert und werden sofort angewendet, wenn eine Warnung erstellt oder aktualisiert wird, bevor andere Gruppierungsalgorithmen verwendet werden.

   - CMDB: CMDB-Gruppierung
   - NETWORK_TRAFFIC: Gruppierung des Netzwerkdatenverkehrs
   - TAG_BASED: Tag-Clustergruppierung
   - MUSTER: Automatisierte CI-basierte Mustergruppierung
   - TEXTBASE: Textbasierte Gruppierung
3. Verwenden Sie die Eigenschaft *sa_analytics.agg.query.group_logic_order*, um die Reihenfolge der Korrelationsmethoden basierend auf Ihren Einstellungen zu definieren oder zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filter für automatische Warnungsgruppen konfigurieren

Filtern Sie Warnungen und Warnungsgruppen, um Warnungsrauschen zu reduzieren. Nur Warnungen, die dem Filter entsprechen, werden in die Gruppe des ausgewählten Gruppentyps (Automatisiert, CMDB oder Text) aufgenommen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Ihr Filter Warnungen angibt, deren Configuration Item-Klasse nicht Linux ist, werden nur Warnungen mit Nicht-Linux-Konfigurationselementen in der Gruppe des ausgewählten Gruppentyps enthalten.

Hinweis: Nachdem der Filter erstellt wurde, gilt er nur für neue Warnungen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Automatischer Gruppenfilter**.
2. Wählen Sie auf der Seite „Automatische Gruppenfilter“ entweder einen vorhandenen Gruppenfilter aus oder erstellen Sie einen neuen Filter.
3. Wenn Sie einen neuen Filter erstellen:

   a. Wählen Sie **Neu**.

   b. Geben Sie im Feld **Name** einen Namen für den Filter ein.

   c. Wählen Sie den Warnungsgruppentyp aus:
      - Automatisiert
      - Test
      - CMDB

      Sie können mehr als einen Gruppentyp mit einer einzelnen Filterbedingung zuweisen.

      Jeder Gruppentyp kann nur einen einzigen aktiven Filter aufweisen.

4. Erstellen Sie im Abschnitt **Warnungsfilter** Bedingungen, die eine Warnung erfüllen muss, damit sie in die Gruppe aufgenommen wird.
5. Speichern Sie den Warnungsgruppenfilter.
   - Wählen Sie für einen vorhandenen Warnungsgruppenfilter **Absenden** aus.
   - Wählen Sie für einen neuen Warnungsgruppenfilter **Aktualisieren** aus.

Ergebnisse
Die Filterbedingung wird auf der Seite „SA-gruppierte Warnungsfilter“ in der Spalte **Warnungsfilter** angezeigt.

Warnungsgruppenfilter auf zusammengefasste Gruppen anwenden

Reduzieren Sie Rauschen, indem Sie nur zusammengefasste Warnungsgruppen suchen, die einem konfigurierten Filter entsprechen. Zusammengefasste Gruppen sind Gruppen, die für Warnungen mit identischen CIs und Musterbezeichnern erstellt wurden.

Vorbereitungen
Hinweis: Dieses Verfahren ist nur für die erweiterte Konfiguration relevant.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Automatische Gruppenfilter**.
2. Fügen Sie auf der Seite „Automatische Gruppenfilter“ die Spalte **Aggregiert** hinzu.
   a. Wählen Sie das Symbol „Liste personalisieren“ ( ) in der oberen rechten Ecke.
   b. Verschieben Sie den Eintrag **Aggregiert** aus der Liste **Verfügbar** in die Liste **Ausgewählt**.
   c. Wählen Sie die Aufwärts-/Abwärtspfeile aus, um festzulegen, wo der Eintrag **Zusammengefasst** im Formular angezeigt werden soll.
   d. Wählen Sie **OK**.
3. Doppelklicken Sie auf der Seite Automatische Gruppenfilter auf den Wert in der Spalte **Aggregiert**.

   Zusammengefasste Gruppen gelten nur für automatisierte Warnungsgruppen. Wenn die Option „Zusammengefasst“ angezeigt wird, wurde sie automatisch für eine automatisierte Warnungsgruppe aktiviert.

   Hinweis: Wenn sich der Wert des Felds **Automatisiert** ändert, ändert sich auch der Wert des Felds **Aggregiert**. Sie können den Wert des Felds **„Aggregiert“** nur ändern, wenn der Wert des Felds **„Automatisiert** “ „wahr“ ist.

4. Wählen Sie **true** aus, damit der angegebene Filter auf Gruppen mit identischen CIs und Muster-IDs angewendet wird, oder wählen Sie **false,** um den Filter zu ignorieren und zusammengefasste Gruppen für alle Warnungen im System zu erstellen.

Zugehörige Informationen

Geben Sie Musterbezeichner-Attribute für die Warnungsgruppierung an, und verwalten Sie sie

Warnungsgruppierungstypen und -erstellungsmethoden

Machen Sie sich mit den verschiedenen Arten der Warnungsgruppierung vertraut, verstehen Sie ihre Beschreibungen, und erfahren Sie mehr über ihre Erstellungsmethoden, um die Problemidentifizierung zu verbessern und das Warnungsmanagement zu optimieren.

-Warnungsgruppen anzeigen und verwalten

Navigieren zu **Ereignismanagement** > **Alle Warnungen** um alle Warnmeldungsgruppen anzuzeigen. Das Symbol in der Spalte **Gruppe** gibt den Warnungsgruppentyp an, während Warnungen, die keiner Gruppe zugeordnet sind, keinen Eintrag in der Spalte **Gruppe** haben. Doppelklicken Sie auf die Spalte **Gruppe**, um das Dialogfeld „Gruppierte Warnungen“ zu öffnen, in dem Sie alle Warnungen in der Gruppe anzeigen und manuell Warnungen hinzufügen oder entfernen können.

Hinweis: Eine Warnung kann jeweils nur einer Warnmeldungsgruppe angehören.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten der Warnungsgruppierung

Warnungsgruppierungstypen

Typ	Syn	Beschreibung	Erstellungsmethode	Zusätzliche Information
Log Analytics	L	Log Analytics -Gruppen werden gebildet, wenn das System mehrere zugehörige Log Analytics -Warnungen identifiziert und basierend auf ihren signifikanten Verbindungen gruppiert.	Wird im Rahmen der Log Analytics-Ereignisverarbeitung erstellt.	Arten von Health Log Analytics-Warnungen
Regelbasiert	R	Regelbasierte Gruppen bestehen aus zugehörigen Warnungen, die auf Grundlage der Compliance mit Warnungskorrelationsregeln organisiert sind. Diese bestimmen, wie Warnungen anhand ihrer Beziehungen gruppiert werden.	Wird über die Business-Regel (Korrelationsregel berechnen) in der Tabelle „em_alert“ erstellt, wenn eine Warnung erstellt oder aktualisiert wird.	Warnungskorrelationsregel erstellen
Automatisiert	A	Automatisierte Gruppen werden durch Warnungszusammenfassung gebildet und enthalten eine virtuelle Warnung als primäre Warnung der Gruppe. Eine automatisierte Gruppe vom Typ „Aggregiert“ wird erstellt, wenn mindestens zwei Warnungen denselben CI-Typ und Metriknamen verwenden.	Über geplante Aufgabe erstellt.	Automatisierte Warnungsgruppierung
CMDB	C	CMDB-Gruppen werden auf Grundlage von CI-Beziehungen in der CMDB gebildet, insbesondere für CIs, die nicht in regelbasierten oder automatisierten Gruppen enthalten sind.	Über geplante Aufgabe erstellt.	CMDB -basierte Warnungsgruppierung
Basierend auf Netzwerkdatenverkehr	N	Warnmeldungsgruppen für Netzwerkverkehr werden durch die Analyse der Verbindungen des Netzwerkverkehrs zwischen Prozessen auf allen Hosts gebildet. Diese Methode nutzt durch ML-Service-Mapping identifizierte Servicekandidaten, um Warnungen im Zusammenhang mit Problemen mit dem Netzwerkdatenverkehr zu gruppieren.	Über geplante Aufgabe erstellt.	Warnungsgruppierung basierend auf Netzwerkdatenverkehr

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgruppierungstypen (Fortsetzung)

Typ	Syn	Beschreibung	Erstellungsmethode	Zusätzliche Information
Text	T	Textgruppen werden gebildet, indem Warnungen basierend auf ähnlichem Text aus häufig verwendeten Wörtern in den folgenden Feldern gruppiert werden. • Beschreibung • Metrikname • CI-Klasse	Über geplante Aufgabe erstellt.	N/V
Tag-Cluster	Tag	Tag-Clustergruppen werden durch die Gruppierung von Warnungen gemäß anwenderdefinierten tagbasierten Warnungs-Clustering-Definitionen gebildet.	Über geplante Aufgabe erstellt.	Gruppierung von Tag-Clustern von Warnungen
Manuell	M	Manuell nach Anwendern gruppierte Warnungen, um zugehörige Probleme zu organisieren.	Manuell vom Anwender erstellt.	Erstellen Sie manuell eine Warnmeldungsgruppe

Informationen zu geplanten Aufgaben und Parametern finden Sie unter Geplante Aufgaben und Parameter für die Gruppierung von Warnungen. Ausführliche Informationen zum Konfigurieren der Reihenfolge der Warnungskorrelationslogik finden Sie unter Konfigurieren Sie die Reihenfolge der Warnungskorrelationslogik.

Log Analytics-Warnungsgruppierung

ServiceNow Health Log Analytics identifiziert Muster in Protokolldaten und lernt das Musterverhalten. Wenn die Engine für künstliche Intelligenz anomales Verhalten erkennt, wird ein Ereignis an die Anwendung ServiceNow Ereignismanagement gesendet.

Log Analytics-Warnungsgruppen werden von der Anwendung Health Log Analytics erstellt. Weitere Informationen finden Sie unter Typs von Health Log Analytics Warnungen.

Regelbasierte Warnungsgruppierung

Die regelbasierte Warnungsgruppierung wird durch Warnungskorrelationsregeln erstellt. Mit diesen Regeln können Sie Warnungen manuell als primär oder sekundär klassifizieren und eine Beziehung zwischen ihnen herstellen. Verwenden Sie Warnungskorrelationsregeln, um zugehörige Warnungen zu gruppieren. Die Regel wird nur für neue Warnungen oder Warnungen ausgeführt, deren Status von „Schließen/Fluktuierend“ in „Öffnen/Erneut öffnen“ geändert wurde.

Beispiel: Wenn die regelbasierte Warnungsgruppierung angewendet wird, werden sekundäre Warnungen, die angeben, dass virtuelle Computer oder Anwendungen auf dem Offline-Server ebenfalls ausgefallen sind, unter der primären Warnung gruppiert, die die Stammwarnung für den offline ist. Sie können regelbasierte Warnungsgruppierungen in Express-Liste von Service Operations-Arbeitsbereich (ITOM) anzeigen. Weitere Informationen finden Sie unter Links zwischen Warnungen in regelbasierten Warnmeldungsgruppen anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Primäre und sekundäre Warnungen

- Primäre Warnung: Identifiziert die Ursache einer Warnmeldungsgruppe und stellt ihre sekundären Warnungen dar.
- Sekundäre Warnung: Sie beziehen sich auf dasselbe Problem und sind unter der primären Warnung gruppiert. Der Zweck sekundärer Warnungen besteht darin, zu bestimmen, welche Warnungen unterdrückt werden sollen, wodurch das Warnungsrauschen reduziert wird und Sie sich auf die primäre Warnung konzentrieren können.

Wie primäre und sekundäre Warnungen interagieren

Bei der regelbasierten Warnungsgruppierung wird eine der echten Warnungen als primäre Warnung festgelegt. Primäre und sekundäre Warnungsfilterbedingungen geben an, welche Warnungen als primär und welche als sekundär klassifiziert werden. Die Filterkriterien werden auf die Tabelle „Warnung“ [em_alert] angewendet.

In dieser Warnungsgruppierung sind sowohl primäre als auch sekundäre Warnungen sichtbar, sekundäre Warnungen werden jedoch unter der primären Warnung gruppiert. Die Eigenschaft **Sekundäre Warnung geöffnet lassen, auch wenn die primäre Warnung geschlossen wird. für manuelle oder regelbasierte** (*evt_mgmt.rule_based_manual_closure*) Steuerungen, ob sekundäre Warnungen offen bleiben oder geschlossen werden, wenn die primäre Warnung geschlossen wird.

Wenn die Eigenschaft nicht ausgewählt ist (d. h. auf Nein festgelegt ist), wird nach dem Schließen der primären Warnung die übergeordnete Referenz aus den sekundären Warnungen entfernt (die Gruppierung wird aufgelöst), und die sekundären Warnungen werden geschlossen und werden zu eigenständigen Warnungen. Wenn Sie das Kontrollkästchen für die Eigenschaft aktivieren (d. h. auf Ja setzen) und die primäre Warnung geschlossen ist, wird die übergeordnete Referenz aus den sekundären Warnungen entfernt (die Gruppierung wird aufgelöst), wodurch sie zu eigenständigen offenen Warnungen werden.

Warnungshierarchie

Nur eine Ebene sekundärer Warnungen ist zulässig. In Situationen, in denen eine Sekundärwarnung über eine eigene Sekundärwarnung verfügt, wird die Hierarchie von der Event Management-Anwendung abgeflacht, damit es weiterhin nur zwei Ebenen gibt.

Ein Beispiel: Nehmen wir an, Warnung A ist die primäre Warnung und Warnung B ist die sekundäre Warnung. Wenn Warnung C zu einer sekundären Warnung von Warnung B wird, wird die Hierarchie von der Anwendung abgeflacht: A bleibt die primäre Warnung, B und C werden zu sekundären Warnungen (eine Ebene unter A).

Als weiteres Beispiel nehmen wir an, dass drei Korrelationsregeln vorhanden sind, was zu den folgenden Ergebnissen führt:

- Regel 1 (mit Reihenfolgenwert 1): B wird zur primären Warnung für A.
- Regel 2 (mit Reihenfolgenwert 2): A wird zur primären Warnung für C und D.
- Regel 3 (mit Reihenfolgenwert 3): E wird zur primären Warnung für A.

Wenn die Warnungen B, C, D und E ausgelöst werden, erscheinen sie alle getrennt in der Warnungsliste, da keine Korrelationen zwischen ihnen bestehen.

Wenn Warnung A ausgelöst wird:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Durch Regel 1 wird A zu einer sekundären Warnung unter Warnung B.
2. Durch Regel 2 werden C und D zu sekundären Warnungen unter Warnung A, und die Hierarchie wird reduziert, sodass A, C und D zu sekundären Warnungen der primären Warnung B werden.
3. Regel 3 wird nicht angewendet, da mehrere übergeordnete Elemente nicht zulässig sind. A hat bereits B als primäres Element.

Wenn alle Warnungen ausgelöst werden, wird daher nur B als primäre Warnung für A, D und C angezeigt, während E eine eigenständige Warnung bleibt.

Warnungskorrelationsregel erstellen

Erstellen Sie eine Warnungskorrelationsregel, um primäre und sekundäre Warnungen festzulegen. Die primäre Warnung wird als Ursache für die Warnungsgruppe identifiziert, und die sekundären Warnungen werden unter der primären Warnung gruppiert.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Warnungskorrelationsregeln**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.
   Weitere Informationen zu diesen Feldern finden Sie unter Formular für Warnungskorrelationsregel.
4. Wählen Sie **Absenden**.

Ergebnisse

Eine regelbasierte Warnmeldungsgruppe wird erstellt, wenn eine neue Warnung generiert wird oder wenn der Status einer vorhandenen Warnung von Geschlossen oder Fluktuierend in Offen oder Erneut geöffnet wechselt, sofern die Filterkriterien übereinstimmen.

Automatisierte Warnungsgruppierung

Die automatisierte Warnungsgruppierung ist ein Prozess, der Verlaufsdaten verwendet, um ähnliche Warnungen automatisch in Gruppen zu organisieren. Diese Warnungen können Systemprobleme wie Serverfehler oder Netzwerkausfälle sein. Durch die Gruppierung zugehöriger Warnungen können Teams Muster schnell erkennen, wiederkehrende Probleme verwalten und das Rauschen durch zu viele einzelne Warnungen reduzieren.

Stellen Sie sich vor, Sie überwachen das Verkehrssystem einer Stadt. Sie erhalten viele Warnungen, z. B. Berichte über Unfälle, Verkehrsstaus und Straßensperrungen. Die automatisierte Warnungsgruppierung funktioniert wie ein intelligenter Assistent, der diese Warnungen basierend auf Mustern organisiert, sodass Sie verwandte Probleme gemeinsam anzeigen und effizienter reagieren können. Diese automatisierten Warnmeldungsgruppen werden unter Express-Liste innerhalb von Service Operations-Arbeitsbereichangezeigt.

So aktivieren Sie diese Gruppierung

Um die auf maschinellem Lernen basierende Automatisierung für die Warnungskorrelation zu aktivieren, legen Sie die Eigenschaft **ML-basierte Automatisierungskorrelation aktivieren** (sa_analytics.specific_patterns_enabled) auf „wahr“ fest.

Wenn das Installationsprogramm für Domain Support – Domain Extensions aktiviert ist, werden Warnungszusammenfassungsmuster basierend auf der Domänenebene erstellt, die in der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft „sa_analytics.agg.learner_domain_level“ definiert ist. Standardmäßig ist diese Domänenebene auf zwei festgelegt, was der zweiten Ebene in der Domänenhierarchie entspricht. Beispielsweise kann in einem Unternehmen Ebene 1 das Unternehmen selbst darstellen, während Ebene 2 Abteilungen oder Teams innerhalb des Unternehmens darstellen kann. Warnungen werden basierend auf dieser zweiten Ebene gruppiert, ähnlich wie nach Abteilung oder Team. Für weitere Details Domain Separation und Ereignismanagement.

Funktionsweise

Die automatisierte Warnungsgruppierung nutzt maschinelles Lernen (ML) und Verlaufsdaten, um Muster in Warnungen zu identifizieren. Er untersucht bestimmte Merkmale, die als Musterbezeichner bezeichnet werden, z. B. den Typ des Problems, das betroffene System, das CI oder die Metrik, die innerhalb eines ähnlichen Zeitraums mehrmals aufgetreten ist, um zu bestimmen, ob Warnungen zusammenhängen. Der Alert Aggregation Learninger verwendet Algorithmen, um Warnungen basierend auf Mustern zu gruppieren. Konkret werden musterbasierte Algorithmen und Wahrscheinlichkeitsmethoden verwendet, um eingehende Warnungen zu analysieren und zugehörige Warnungen zu identifizieren.

Stellen Sie sich das so vor, als würden Sie feststellen, dass an einer bestimmten Kreuzung häufig zu Hauptverkehrszeiten Unfälle passieren. Das System gruppiert ähnliche Warnungen (z. B. wiederkehrende Verkehrsstaus an derselben Stelle) basierend auf bestimmten Bezeichnern (z. B. Standort oder Typ des Problems). Das System führt die folgenden Schritte aus, um Warnungen effektiv zu gruppieren:

- Verlaufsdaten analysieren: Das System untersucht vergangene Warnungen, um Muster und Beziehungen zu ermitteln.
- Maschinelles Lernen anwenden: ML-Algorithmen analysieren historische Warnungsdaten, um Muster und Beziehungen zwischen Warnungen zu identifizieren. Das System kann aus vergangenen Incidents lernen und seine Fähigkeit verbessern, ähnliche Warnungen im Laufe der Zeit zu gruppieren.
- Ähnliche Warnungen gruppieren: Warnungen mit übereinstimmenden Mustern werden automatisch in einer Gruppe zusammengefasst.

Angenommen, Sie verwalten das Verkehrssystem einer Stadt und erhalten mehrere Warnungen:

- 8:00 Uhr: Unfall auf der Hauptstraße
- 8:05 Uhr: Verkehrsstau in der Nähe der Main Street
- 8:10 Uhr: Straßensperrung auf der Main Street

Die automatisierte Warnungsgruppierung funktioniert wie ein intelligenter Assistent, indem sie diese Warnungen analysiert und ein Muster erkennt. Es gruppiert sie, da sie sich alle auf die Main Street beziehen und wahrscheinlich aus demselben Unfall stammen. Dadurch können Sie schnell das Gesamtbild erkennen und sich auf die Behebung der Ursache (des Unfalls) konzentrieren, anstatt jede Warnung einzeln zu behandeln.

Vorteile

- Wiederkehrende Probleme finden: Erkennen Sie schnell Muster (z. B. ständige Überhitzung eines Servers).
- Zeitersparnis: Behandeln Sie Gruppen zusammengehöriger Warnungen anstelle einzelner.
- Antwort verbessern: Fokus auf die Behebung der Ursache anstatt die Behandlung vereinzelter Probleme.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Musterbezeichner verstehen

Ein Musterbezeichner ist ein Satz von Kriterien oder Attributen (z. B. Warnungstyp, betroffenes System usw.), die zum Gruppieren ähnlicher Warnungen verwendet werden. Es hilft, wiederkehrende Probleme zu identifizieren, und erleichtert Teams die Reaktion und Lösung laufender Probleme.

Wie Musterbezeichner Warnungen gruppieren

Verwenden Sie ein Netzwerküberwachungssystem, das Warnungen für verschiedene Probleme generiert, z. B. hohe CPU-Auslastung, Speicherverluste oder Verbindungstimeouts.

Musterbezeichner: Name der Metrik und CI

- Warnung 1: Hohe CPU-Auslastung auf Server A um 10:00 Uhr
- Warnung 2: Hohe CPU-Auslastung auf Server A um 10:05 Uhr
- Warnung 3: Speicherverlust auf Server B um 10:10 Uhr
- Warnung 4: Hohe CPU-Auslastung auf Server A um 10:15 Uhr

In diesem Fall kann der Musterbezeichner auf den Metriknamen (z. B. hohe CPU-Auslastung) in Kombination mit dem Configuration Item (CI) (z. B. Server A) festgelegt werden. Die Warnungen 1, 2 und 4 werden in einer Gruppe zusammengefasst, da sie dieselbe Metrik (hohe CPU-Auslastung) und dasselbe CI (Server A) verwenden, was auf ein wiederkehrendes Problem hinweist, das möglicherweise weitere Untersuchungen erfordert. Warnung 3 wird jedoch nicht in diese Gruppe aufgenommen, da sie eine andere Metrik (Speicherverlust) und ein anderes CI (Server B) aufweist.

Hinweis: Der Satz von Warnungsfeldern, die für den Musterbezeichner verwendet werden, wird auch als Funktionsbezeichner-Attribute oder einfach Attribute bezeichnet.

Konfigurieren Sie effektive Musterbezeichner

Um effektive Muster-Identifier für die Warnungsgruppierung zu konfigurieren, führen Sie die folgenden drei Schritte aus, um eine genaue und aussagekräftige Analyse der Warnungen sicherzustellen.

Schritt	Aktion	Beschreibung
Event-Regel erstellen	Definieren Sie eine Ereignisregel. Informationen zum Erstellen einer Ereignisregel finden Sie unter Event-Regel erstellen oder bearbeiten.	Richten Sie eine Ereignisregel ein, um die relevanten Warnungsfelder für den Musterbezeichner auszufüllen.
Verwalten Sie den Musterbezeichner	Fügen Sie dem Musterbezeichner das relevante Warnungsfeld hinzu. Informationen zum Hinzufügen von Feldern zum Musterbezeichner finden Sie unter Geben Sie Musterbezeichner-Attribute	Nachdem Sie die relevanten Warnungsfelder hinzugefügt haben, wählen Sie **Bereitstellen**, um den Musterbezeichner zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritt	Aktion	Beschreibung
	für die Warnungsgruppierung an, und verwalten Sie sie.	
Wählen Sie relevante Bezeichner aus	Wählen Sie Warnungsfelder aus, die das Problem eindeutig identifizieren. Wenn das Problem beispielsweise darin besteht, dass ein Service offline ist oder keine Verbindung zur Datenbank besteht, suchen Sie in der Warnung nach bestimmten Werten, die darauf hinweisen. Fügen Sie diese Feldtypen dem Musterbezeichner hinzu. Standardmäßig wird das Feld **Metrikname** als Musterbezeichner bereitgestellt.	• Vermeiden Sie übermäßig eindeutige Felder (z. B. Datum), die die Musteridentifizierung erschweren. • Vermeiden Sie zu allgemeine Felder, die dazu führen, dass zu viele Warnungen gruppiert werden, sodass Muster nicht mehr unterscheidbar sind.

Warnungsgruppierung und gelernte Muster

Erfahren Sie, wie Warnungsmuster im System erkannt, gruppiert und angezeigt werden.

Konzept	Beschreibung
Muster-Discovery	Wenn eine Reihe von Warnungsfeldern übereinstimmt, werden die Warnungen in einem „gelernten Muster“ gruppiert. Beispielsweise werden Warnungen mit derselben Prioritätsgruppe und Ressource in einem Muster gruppiert.
Musterberichterstellung	Diese Muster werden im Bericht „Erlernte Muster“ unter angezeigt **Ereignismanagement** > **Administration** > **Erlernte Muster**.

Musterattribute und Zeitrahmen verwalten

Erfahren Sie, wie Sie Muster-Identifier-Attribute verwalten, neue Sätze bereitstellen und wie das System Probleme identifiziert.

Konzept	Beschreibung
Aktive Musterbezeichner-Attribute	Es kann jeweils nur ein Attributsatz aktiv sein. **Hinweis:** Der neue Satz ersetzt den aktuellen nach der Bereitstellung.
Zweck und Zeitrahmen	Die Mustergruppierung identifiziert Probleme innerhalb der letzten 30 Tage,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konzept	Beschreibung
	gesteuert durch die Eigenschaft **sa_analytics.agg.learner_period_days**.
Identifizierung des Problems	Um ein Problem zu identifizieren, verwendet das System eine Kombination aus Configuration Items (CIs) und Musterbezeichnern (manchmal auch als Funktionsbezeichner bezeichnet). Standardmäßig ist ein Musterbezeichner als Metrikname definiert, dies kann jedoch geändert werden. Zwei Warnungen gelten als ähnlich, wenn sie dasselbe CI und denselben Musterbezeichner verwenden, auch wenn sich Felder wie Quelle, Schweregrad, Beschreibung und andere unterscheiden können. Weitere Informationen finden Sie unter Geben Sie Musterbezeichner-Attribute für die Warnungsgruppierung an, und verwalten Sie sie. **Hinweis:** Der Alert Aggregation Learner identifiziert auch Muster von Warnungen innerhalb manueller Warnmeldungsgruppen. In einigen Fällen können Sie Muster aus Warnungen erstellen, bei denen die CIs in einem bestimmten Feld denselben Wert verwenden. Um beispielsweise Muster aus Warnungen mit demselben CI- **Standort** -Feld zu erstellen, geben Sie `den Standort` in die Eigenschaft *`sa_analytics.agg.learner_group_by_property`* ein. Weitere Informationen finden Sie unter Konfigurieren Sie die geplante Aufgaben-basierte Warnungsgruppierung. Wenn Sie mit CI-basierten Gruppen arbeiten, vergewissern Sie sich, dass der Musterbezeichner sowohl den Knoten- als auch den Metriknamen enthält. Einzelheiten zur Konfiguration des Funktionsbezeichners finden Sie unter Bericht zu gelernten Mustern. **Hinweis:** Warnungen ohne CI können dennoch als textbasierte oder CI-basierte Warnungsgruppen gruppiert werden, wobei ein Knoten als CI behandelt wird. Um diese Funktionalität zu aktivieren, legen Sie die Eigenschaft „sa_analytics.enable_no_ci_grouping“ auf „wahr“ fest.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die musterbasierte Warnungsgruppierung

Konfigurieren Sie den Warnungszusammenfassungs-Lerner (Service Analytics Warnungszusammenfassungs-Lerner – täglich), einen Offline-Auftrag, der täglich ausgeführt wird, um frühere Warnungen zu verarbeiten. Es identifiziert Muster zugehöriger Warnungen mithilfe einer Kombination aus musterbasierten und Wahrscheinlichkeitstechniken und ermöglicht so eine schnellere Erkennung und Lösung wiederkehrender Probleme.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Der Learner der Warnungszusammenfassung verfolgt das manuelle Hinzufügen und Entfernen von Warnungen aus automatisierten Warnungsgruppen. Wenn Sie vorherige Hinzufügungen oder Entfernungen von Warnungen rückgängig machen, wird der automatische Prozess entsprechend angepasst.

Sie können das Hinzufügen und Entfernen von Anwendern zu automatisierten Warnmeldungsgruppen überprüfen und Aktionen rückgängig machen, um zu verhindern, dass sie automatisch wiederholt werden. Der Alert Aggregation Learninger identifiziert auch Muster in manuellen Warnungsgruppen und ermöglicht so die automatische Bildung neuer Warnungsgruppen basierend auf diesen Mustern, wenn neue Streams von Warnungen eingehen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Warnungskorrelationseigenschaften**.
2. Aktivieren Sie die folgenden Eigenschaften.
   - Aktivieren Sie die Warnungszusammenfassung für automatisierte, CMDB- und textbasierte Gruppen (*sa_analytics.aggregation_enabled*).

     Hinweis: Wenn diese Option deaktiviert ist, werden alle anderen Gruppen deaktiviert.

   - Aktivieren Sie die ML-basierte Automatisierungskorrelation (*sa_analytics.specific_patterns_enabled*).
3. Wahlweise: Führen Sie die folgenden Schritte aus, um den Zeitraum für den Warnungszusammenfassungs-Lerner zur Verarbeitung von Warnungen zu konfigurieren:
   a. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
   b. Wählen Sie auf der Seite „Systemeigenschaften“ die Eigenschaft *sa_analytics.agg.learner_period_days* aus.

      Wenn die Eigenschaft nicht vorhanden ist, müssen Sie sie definieren.

   c. Legen Sie den **Wert** der Eigenschaft auf die Anzahl der Tage fest, nach der der Lernerauftrag für die Warnungszusammenfassung verarbeitet werden soll.

      Hinweis: Werte über 30 Tage erhöhen die Auftragsverarbeitungszeit. Verwenden Sie für eine optimale Leistung Werte von 30 Tagen oder weniger.

Geben Sie Musterbezeichner-Attribute für die Warnungsgruppierung an, und verwalten Sie sie

Der Alert Aggregation Learninger analysiert Warnungen und identifiziert Muster anhand eines definierten Satzes von Warnungs- und Configuration Item (CI)-Attributen. Durch die Konfiguration dieser Attribute als Musterbezeichner können Sie steuern, welche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Merkmale zum Gruppieren von Warnungen verwendet werden. Diese Anpassung erstellt aussagekräftige Warnungsgruppen und verbessert das Warnungsmanagement und die Antwortzeiten, indem sie das Rauschen reduziert und die Fokussierung auf kritische Probleme ermöglicht.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Ereignismanagement** > **Administration** > **Muster-Identifier verwalten**.
2. Wählen Sie auf der Seite „Musterattribute der SA-Warnungszusammenfassung“ **Neu**, um einen neuen Musterbezeichner zu erstellen, oder öffnen Sie einen vorhandenen Musterbezeichner.
   Die Seite „Musterattribut für SA-Warnungszusammenfassung“ wird geöffnet.
3. Wählen Sie das Symbol für Attribute des Funktionsbezeichners entsperren ( ), und verschieben Sie Attribute aus der Liste **Verfügbar** in die Liste **Ausgewählt**.

   Hinweis: Eigenschaften aus CMDB-CI über Dot-Walking werden nicht ausgefüllt.

   Das Attribut **Configuration Item** wird automatisch als Bezeichner betrachtet und sollte dem Abschnitt Funktionsbezeichner-Attribute nicht explizit hinzugefügt werden. Das Muster ist definiert als eine Kombination aus dem Configuration Item und den von Ihnen ausgewählten Funktionsbezeichner-Attributen.
4. Durch Auswahl des Symbols für Bezeichnerattribute der Sperrfunktion ( ).
5. Wählen Sie **Absenden** für einen neuen Musterbezeichner oder **Aktualisieren** für einen vorhandenen Musterbezeichner aus.
6. Navigieren Sie zurück zur Seite „Musterattribut für SA-Zusammenfassung von Warnmeldungen“, indem Sie den Musterbezeichner öffnen.
7. Aktivieren Sie die Musterbezeichner-Attribute, indem Sie **Bereitstellen**auswählen.

Nächste Maßnahme

- Stellen Sie sicher, dass eine entsprechende Ereignisregel vorhanden ist: Stellen Sie sicher, dass eine Ereignisregel eingerichtet ist, um eingehenden Warnungen die neu definierten Muster-Identifier-Attribute zuzuweisen oder auszufüllen. Ereignisregeln definieren, wie Attribute basierend auf bestimmten Bedingungen Warnungen zugewiesen werden.
- Führen Sie den Auftrag „Service Analytics-Attributfüller für historische Warnungen“ aus: Nachdem die neue Ereignisregel vorhanden ist, wird dieser Auftrag verwendet, um die Muster-Identifier-Attribute für vorhandene Warnungen, die vor der Definition der neuen Attribute erstellt wurden, nachträglich auszufüllen. Stellt sicher, dass auch vergangene Warnungen (Verlaufswarnungen) mit den Attributen gefüllt sind, die für eine ordnungsgemäße Gruppierung erforderlich sind.

Bericht zu gelernten Mustern

Mit dem Bericht „Erlernte Muster“ können Sie die Effizienz der Warnungszusammenfassung bewerten und wiederkehrende Warnungsmuster identifizieren. Sie ermöglicht eine proaktive Lösung von Problemen und verbessert die allgemeine Systemleistung, indem Einblicke in häufige Warnungen gewährt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Navigieren und Sortieren des Berichts

Um auf den Bericht „Erlernte Muster“ zuzugreifen, navigieren Sie zu **Ereignismanagement** > **Berichterstellung** > **Erlernte Muster**.

Sortieroptionen: Sie können Muster nach Musterpunktzahl, Häufigkeit und Größe sortieren, um zu priorisieren, welche Warnungen zuerst bearbeitet werden.

Metriken und Daten im Bericht

Der Bericht zeigt wichtige Metriken an, die den gelernten Mustern zugeordnet sind, einschließlich:

- Häufigkeit: Die Anzahl der Vorkommen von Musterbezeichnerattributen (CI/MetricName).
- Musterbezeichnerattribute: Beschreibt, wie bei der Warnungsgruppierung relevante Musterattribute kombiniert werden, um ein gelerntes Muster zu erstellen. Diese Muster können in mehreren Warnungen erneut auftreten und weisen häufig auf dasselbe zugrunde liegende Problem hin.
- Präsentationsformat: Metriken werden in einem Tabellenformat angezeigt, das nach gelernten Mustern organisiert ist.

Mit diesem Bericht können Sie:

- Fokus auf Warnungen mit höherer Häufigkeit: Zuordnen von Ressourcen für Warnungen mit höherer Häufigkeit, um die Lösung zahlreicher Warnungen zu beschleunigen.
- Größere Muster mit niedrigerer Häufigkeit anvisieren: Zuordnen von Ressourcen zu größeren gelernten Mustern mit niedrigerer Häufigkeit für gezielte Analysen.

Mustergruppendetails und Bezeichnerattribute

- Erweitern Sie eine Mustergruppe, um Details zu allen Bezeichnerattributen anzuzeigen, die dem Muster zugeordnet sind.
- Sortieren Sie die Einträge in den einzelnen Mustern nach Konfigurationselement und Funktionsbezeichner.

Spalte	Beschreibung
Konfigurationselement	CI, das den kombinierten Musterbezeichner-Attributen zugeordnet ist.
Funktionsbezeichner	Funktionsbezeichner, der für die kombinierten Musterbezeichnerattribute verwendet wird.
Häufigkeit	Häufigkeit, mit der die kombinierten Musterbezeichnerattribute im Datensatz angezeigt werden.
Größe	Anzahl der Vorkommen der kombinierten Musterbezeichnerattribute (z. B. Konfigurationselement und Funktionsbezeichner) innerhalb eines erlernten Musters.
Punktzahl	Berechnete Punktzahl, die die Häufigkeit und Größe des gelernten Musters kombiniert. Die Formel für diese Punktzahl lautet: `Punktzahl = Häufigkeit x (Größe + 1)`.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	Dieser Wert hilft bei der Priorisierung von Mustern basierend auf ihrer Häufigkeit und Größe, sodass Sie sich leichter auf Muster mit hoher Priorität konzentrieren können.
CI-Link	Link in der Spalte **Konfigurationselement**, um Details der CI-Informationen anzuzeigen.

Schließen Sie Muster aus gelernten Mustern aus

Schließen Sie CI-basierte oder CI-klassenbasierte Warnungen und Muster aus, wenn Sie auf Warnungen stoßen, die einem erlernten Muster durch den Auftrag „Erlernte Muster“ falsch hinzugefügt wurden. Beispielsweise kann ein Muster eine Warnung enthalten, die zur gleichen Zeit wie andere Warnungen aufgetreten ist, aber nicht mit diesen zusammenhängt. Dadurch wird die Genauigkeit beibehalten, was zu einer besseren Warnungsgruppierung und einer verbesserten Verwaltungseffizienz führt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

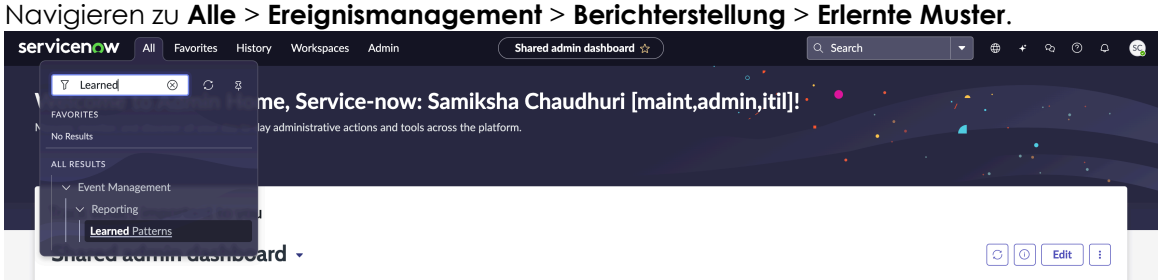
Warum und wann dieser Vorgang ausgeführt wird

Sie wählen die falsche Warnung in einem Muster aus, um das gesamte Muster auszuschließen, zu dem sie gehört.

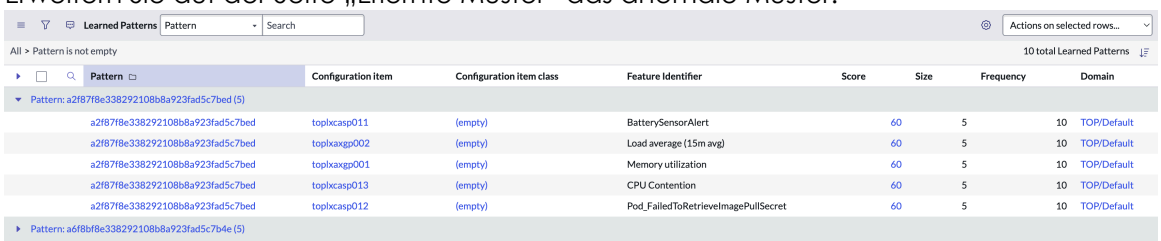
Hinweis: Wenn Sie eine falsche Warnung ausschließen, werden alle anderen Muster, die diese Warnung enthalten, ebenfalls ausgeschlossen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Berichterstellung** > **Erlernte Muster**.



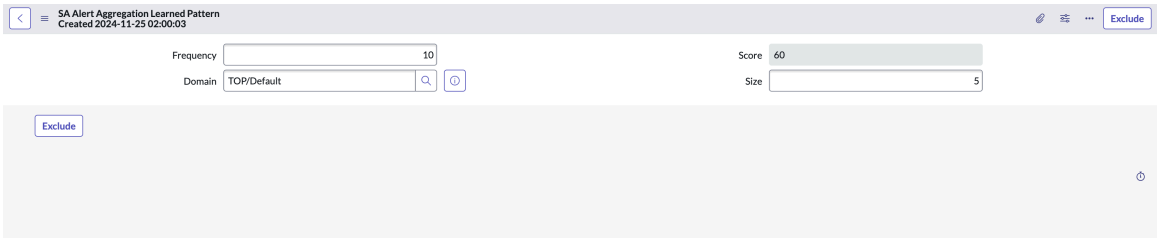
2. Erweitern Sie auf der Seite „Erlernte Muster“ das anomale Muster.



3. Wählen Sie den Musternamen aus, um ihn für den Ausschluss zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie auf der Seite „Erlerntes Muster der SA-Warnungszusammenfassung“ die **Option Ausschließen aus**.



Ergebnisse

Das gesamte Muster wird aus dem Bericht „Erlernte Muster“ entfernt und auf der Seite „Ausgeschlossene Muster“ unter aufgeführt **Ereignismanagement** > **Administration** > **Ausgeschlossene Muster**.

Wenn das Muster andere Warnungen enthält, können Sie es wiederherstellen, indem Sie diese Warnungen als gelerntes Muster zurückfordern. Weitere Informationen finden Sie unter Ausgeschlossene Muster wiederherstellen.

Ausgeschlossene Muster wiederherstellen

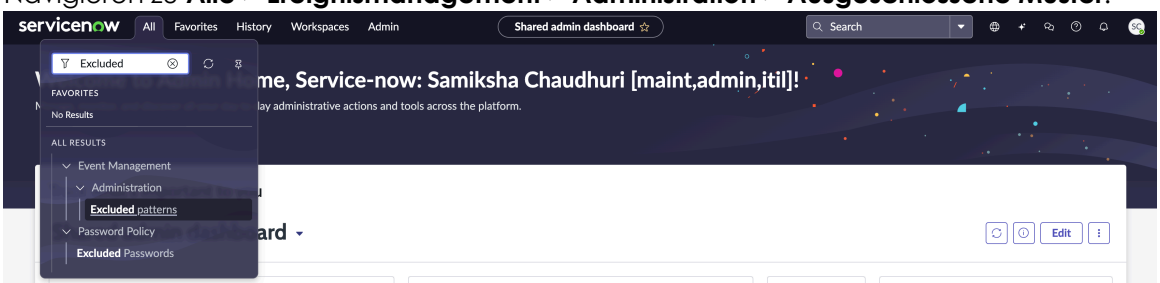
Durch das Wiederherstellen ausgeschlossener Muster im Bericht zu gelernten Mustern können Sie wertvolle Einblicke wieder integrieren, die durch falsche Warnungen verloren gegangen sind. Diese Flexibilität ermöglicht eine genaue Warnungszusammenfassung und verbessert die Überwachung. Wenn Sie beispielsweise ein Muster aufgrund einer falschen Warnung ausgeschlossen haben, können Sie es ohne diese Warnung wiederherstellen, um sicherzustellen, dass relevante Daten für Analysen und Entscheidungen zugänglich bleiben.

Vorbereitungen

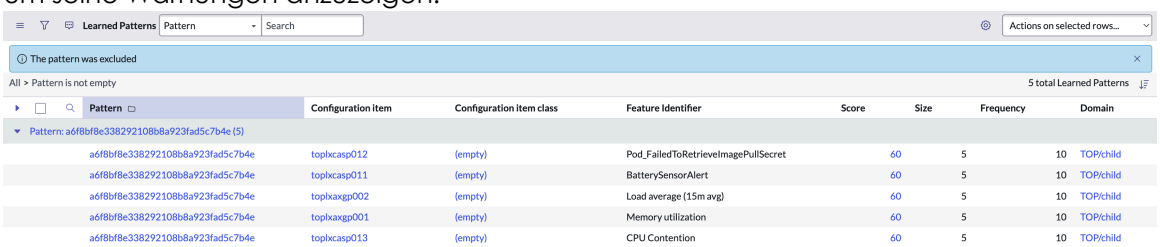
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Ausgeschlossene Muster**.



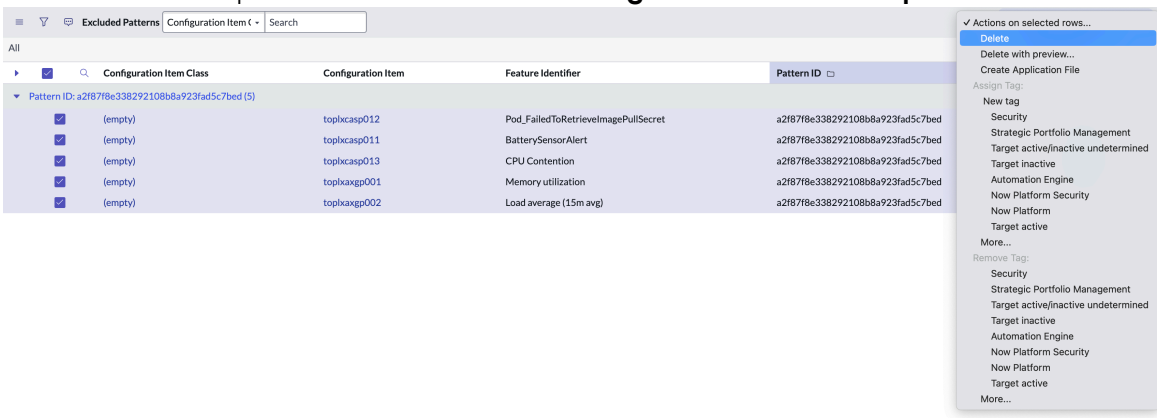
2. Erweitern Sie auf der Seite „Ausgeschlossene Muster“ ein Muster oder wählen Sie eins aus, um seine Warnungen anzuzeigen.



3. Wählen Sie die Muster aus, die Sie wiederherstellen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilendie Option Löschen aus**.

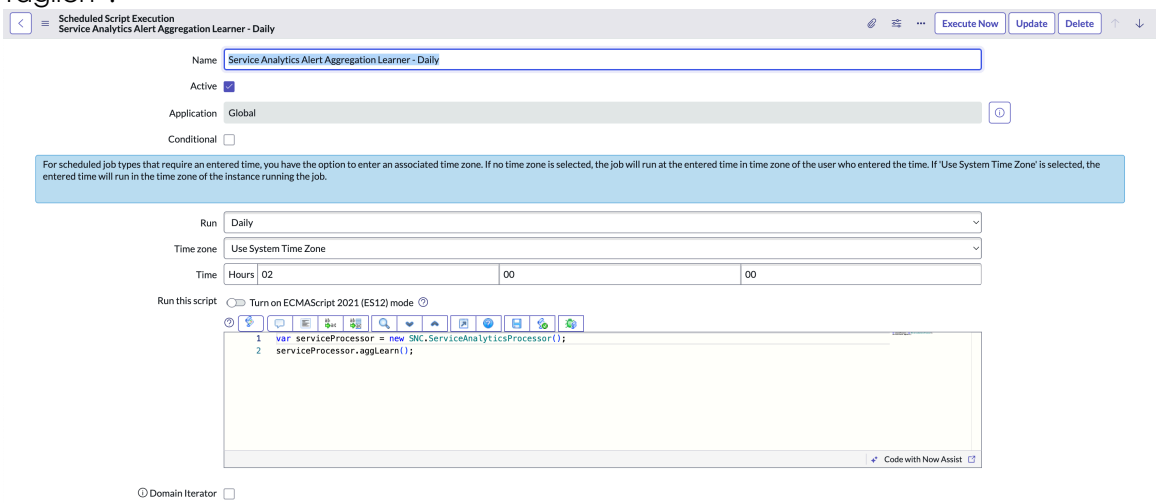


5. Wählen Sie im Bestätigungsfenster **Löschen**.
6. Führen Sie die regelmäßige Aufgabe „Erlernte Muster“ aus.

   a. Auswahlvorgang **Systemdefinition** > **Geplante Aufgabe**.

   b. Suchen Sie auf der Seite „Geplante Aufgaben“ nach der Aufgabe „Service Analytics-Warnungszusammenfassung – Lerner – Täglich“.

   c. Öffnen Sie den Auftrag „Service Analytics-Warnungszusammenfassung – Lerner – Täglich“.



   d. Wählen Sie **Jetzt ausführen**.

Ergebnisse

Das Muster wird mit seinen wiederhergestellten Warnungen auf der Berichtsseite „Erlernte Muster“ angezeigt. Um auf diese Seite zuzugreifen, navigieren Sie zu **Ereignismanagement** > **Berichterstellung** > **Erlernte Muster**.

CMDB -basierte Warnungsgruppierung

CMDB Die -basierte Warnungsgruppierung hilft Organisationen bei der Verwaltung von Warnungen, indem sie sie entsprechend den zugehörigen Configuration Items (CIs) in der Configuration Management Database (CMDB) organisieren. Diese Methode gruppiert Warnungen basierend auf CI-Beziehungen in Anwendungen oder Infrastrukturkomponenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dadurch können Teams die Auswirkungen von Problemen besser verstehen, effektiver auf Warnungen reagieren und die Serviceverfügbarkeit aufrechterhalten.

CMDB -Warnungsgruppen werden basierend auf den aktuellen Beziehungen zwischen CIs in einer Organisation erstellt. Wenn also mehrere Warnungen für verschiedene CIs ausgelöst werden (z. B. wenn bei einem Server Probleme auftreten), werden Warnungen basierend auf CI-Beziehungen gruppiert.

Standardmäßig werden alle vorhandenen Verbindungen zwischen CIs zum Gruppieren von Warnungen verwendet. Aufgrund der Komplexität von IT-Systemen gibt es jedoch viele Arten von Beziehungen, und Organisationen können filtern, welche bei der Zusammenfassung von Warnungen berücksichtigt werden sollen. Sie können beispielsweise Beziehungstypen nach vorgeschlagenen Beziehungen filtern, die in der Tabelle „CMDB-Gruppen-CI-Beziehungen“ [em_suggested_relation_type] angezeigt werden. Sie können auch anhand der Hosting- und Containment-Regeln (abhängige Beziehungsregeln) filtern.

Wenn beispielsweise ein Server mehrere Anwendungen hostet und mit diesem Server ein Problem auftritt, können alle Warnungen, die sich auf den Server und die von ihm gehosteten Anwendungen beziehen, in einer Gruppe zusammengefasst werden. Dies hilft dem IT-Team, die Ursache des Problems schnell zu identifizieren und zu beheben, anstatt jede Warnung isoliert zu behandeln. Wenn verschiedene Prozesse auf einem Server ausgeführt werden, können Teams durch Gruppieren von Warnungen basierend auf diesen Prozessen erkennen, wie sich Probleme in einem Bereich auf andere auswirken können, was zu einem umfassenderen Verständnis der Situation führt.

Die -Warnungsgruppen CMDB werden effektiv in der Express-Liste innerhalb von Service Operations-Arbeitsbereichangezeigt, wodurch Teams zugehörige Warnungen einfach überwachen und verwalten können. Diese Funktion erhöht die betriebliche Effizienz, indem sie eine klare Ansicht der Warnungen bietet, die basierend auf den aktuellen Beziehungen zwischen Configuration Items (CIs) miteinander verbunden sind.

Anwendungsfälle für CMDB -basierte Warnungsgruppierung

Anwendungsfälle für die Gruppierung CMDB verbessern die Warnungsverwaltung, indem sie Warnungen basierend auf Konfigurationselement-Beziehungen korrelieren, die Transparenz verbessern und eine effizientere Problembehandlung ermöglichen.

Häufige CMDB -Gruppierungsanwendungsfälle

Im Kontext der CMDB -Gruppierung stehen Organisationen bei der Verwaltung von Warnungen im Zusammenhang mit Configuration Items (CIs) vor mehreren Herausforderungen.

Gängige Anwendungsfälle

Anwendungsfall	Herausforderungen	Lösungen
Gemeinsam genutztes Configuration Item (CI) Szenario: Eine Organisation überwacht einen Datenbankserver, bei dem mehrere Probleme auftreten. Dies führt zu zahlreichen Warnungen im Zusammenhang	• Verzögerte Reaktion: Teams können isoliert auf Warnungen reagieren und dabei möglicherweise zugehörige Warnungen übersehen, was zu verzögerten Lösungen führt.	• Fassen Sie Warnungen, die sich auf dasselbe CI beziehen, in einer einzigen Gruppe zusammen, um eine einheitliche Ansicht zu schaffen. • Ermöglichen Sie eine schnellere Lösung von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gängige Anwendungsfälle (Fortsetzung)

Anwendungsfall	Herausforderungen	Lösungen
mit verschiedenen Anwendungen, die diese Datenbank verwenden.	• Ineffiziente Ressourcenzuteilung: Zeit und Ressourcen werden möglicherweise für die Untersuchung einzelner Warnungen verschwendet, die tatsächlich miteinander zusammenhängen. • Fehlender Kontext: Warnungen, die sich auf dasselbe CI beziehen, können über verschiedene Warnungsgruppen verteilt sein, was es schwierig macht, einen vollständigen Überblick zu erhalten.	Warnungen, indem Sie alle zugehörigen Warnungen gemeinsam behandeln.
Hosting-/Containment-Beziehungen Szenario: Ein physischer Server hostet mehrere virtuelle Computer (VMs), und für einen Hardwarefehler auf dem Server wird eine Warnung generiert. Aufgrund der Abhängigkeit der VMs vom Server werden auch mehrere Warnungen für die VMs ausgegeben.	• Transparenz in Abhängigkeiten: Teams haben möglicherweise keinen Einblick in die Art und Weise, wie CIs miteinander verbunden sind, was zu ineffizienten Problembehandlungsprozessen führt. • Lösung komplexer Warnungen: Das Verständnis der betroffenen CIs und ihrer Beziehungen kann kompliziert sein, was zu längeren Lösungszeiten führt. • Ressourcenverbrauch: Eine Missverwaltung von Warnungen kann zu doppelten Aufgaben in Teams führen, wodurch Zeit und Ressourcen verschwendet werden.	• Gruppieren Sie Warnungen mithilfe der Hosting-/Containment-Regeln CMDB, um Warnungen im Zusammenhang mit dem physischen Server und den gehosteten VMs in einer einzigen Warnungsgruppe zusammenzufassen. • Stellen Sie eine umfassende Ansicht aller Warnungen im Zusammenhang mit dem Ausfall des physischen Servers bereit. • Konzentrieren Sie die Korrekturmaßnahmen auf den physischen Server, während Sie die VMs überwachen, um sicherzustellen, dass alle Aspekte effizient behandelt werden.
Anwendungsbeziehungen Szenario: Eine Unternehmensanwendung basiert auf mehreren Mikroservices, und bei einem dieser Services tritt ein	• Anwendungsabhängigkeiten verstehen: Für Teams kann es schwierig sein, die Interaktion von Anwendungskomponenten nachzuverfolgen, was es schwierig macht, Probleme	• Implementieren Sie eine Gruppierung basierend auf Applicative Flow-Beziehungen, um Warnungen im Zusammenhang mit dem betroffenen Microservice

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gängige Anwendungsfälle (Fortsetzung)

Anwendungsfall	Herausforderungen	Lösungen
Problem auf, das Warnungen in mehreren Komponenten generiert, was die Diagnose erschwert.	in komplexen Systemen zu lokalisieren. • Langsame Lösung von Incidents: Ohne ein klares Verständnis des Anwendungs-Flows kann die Lösung von Warnungen langsam und arbeitsintensiv sein. • Inkonsistente Überwachung: Warnungen im Zusammenhang mit Anwendungen werden möglicherweise nicht konsistent überwacht oder priorisiert, was zu potenziellen Fehlern führt.	und seinen abhängigen Komponenten zusammenzufassen. • Verwenden Sie Abhängigkeitszuordnungen, um die Interaktion verschiedener Services zu visualisieren. • Optimieren Sie den Lösungsprozess, indem Sie gruppierte Warnungen im Zusammenhang mit der Anwendung bearbeiten und so die Antwortzeiten verbessern.

CMDB -Warnungsgruppierung – Eigenschaften und Funktionalität

Erfahren Sie mehr über die wichtigsten Eigenschaften und Funktionen der Warnungsgruppierung CMDB, die eine effiziente Warnungsorganisation auf Grundlage von Beziehungen ermöglichen und die Gesamteffektivität der Warnungsverwaltung verbessern.

Eigenschaften für die Verwaltung der Erstellung von CMDB -Warnungsgruppen

Verwenden Sie die in den folgenden Tabellen aufgeführten Eigenschaften, um die Erstellung der Warnmeldungsgruppe CMDB zu steuern. Weitere Informationen finden Sie unter Konfigurieren Sie die geplante Aufgaben-basierte Warnungsgruppierung.

Eigenschaft	Einstellung
CMDB-Korrelation aktivieren *sa_analytics.agg.query_cmdb_correlation_enabled*	Aktivieren Sie diese Eigenschaft, um CI-Beziehungen automatisch für die Warnungszusammenfassung, die Korrelation von Warnungen und die Erstellung von CMDB -Warnungsgruppen zu verwenden.
Maximale Anzahl von Beziehungen zwischen CIs in einer Topologie, die eine Gruppe CMDB bilden *sa_analytics.agg.query_cmdb_graph_walk_nodes*	Legen Sie die maximale Anzahl aktivierter Beziehungen zwischen CIs in einer Topologie fest, die eine Gruppe CMDB bilden. Wenn Sie diese Eigenschaft beispielsweise auf 3 festlegen, wird ein CI, das einer Warnung zugeordnet ist, automatisch mit ähnlichen CIs innerhalb von maximal drei Hops gruppiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Einstellung
	Hinweis: Diese Eigenschaftseinstellung wirkt sich auf alle Arten von Beziehungen aus, die für die Warnungszusammenfassung verwendet werden. Die Verwendung eines Werts über 4 kann sich negativ auf die Leistung des Warnungszusammenfassungsauftrags auswirken.
Verwenden Sie alle CMDB -Beziehungen für CMDB die -Gruppenkorrelation *evt_mgmt.related_cis_get_all_relation_types*	Legen Sie den Wert auf „true“ fest, wenn Sie alle Beziehungstypen für CMDB die -Gruppierung verwenden möchten. Die Standardeinstellung für neue Benutzer lautet, dass die Option auf „true“ festgelegt ist. Dies bedeutet, dass alle Beziehungstypen für die Gruppierung verwendet werden. Legen Sie die Eigenschaft auf „false“ fest, um die Beziehungen zu filtern.

Eigenschaften für die Verwaltung der automatischen Erstellung von CMDB -Warnungsgruppen für erweiterte Anwendungsfälle

In einigen Anwendungsfällen müssen Sie möglicherweise bestimmte CI-Beziehungen von der automatischen Erstellung von Warnmeldungsgruppen ignorieren oder ausschließen. In diesem Fall muss die Eigenschaft *evt_mgmt.related_cis_get_all_relation_types* auf „false“ festgelegt werden, und die Eigenschaften in der folgenden Tabelle müssen ebenfalls konfiguriert werden.

Hinweis: Wenn die Eigenschaft *evt_mgmt.related_cis_get_all_relation_types* auf „false“ festgelegt ist und die Beziehung nicht in der Tabelle [em_suggested_relation_type] angegeben ist, wird die Beziehung nicht für die Warnungszusammenfassung berücksichtigt.

Eigenschaften für die Verwaltung der automatischen Erstellung von CMDB -Warnungsgruppen für erweiterte Anwendungsfälle

Eigenschaft	Einstellung
Aktivieren Sie „Vorgeschlagene Beziehungen“ für Korrelation CMDB *sa_analytics.agg.query_cmdb_suggested_relationships_enabled*	Lassen Sie diese Eigenschaft aktiviert, um beim Bilden von Warnmeldungsgruppen für [CMDB alle in der Tabelle CMDB definierten Gruppen-CI-Beziehungen [em_suggested_relation_type] zu verwenden. Um eine neue Beziehung einzubeziehen, fügen Sie sie dieser Tabelle hinzu. Diese Eigenschaft ist standardmäßig aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften für die Verwaltung der automatischen Erstellung von CMDB -Warnungsgruppen für erweiterte Anwendungsfälle (Fortsetzung)

Eigenschaft	Einstellung
Verwenden Sie die Beziehung CMDB basierend auf Host-Containment-Metadatenregeln *evt_mgmt.related_cis_use_containment_rules*	Containment-Regeln geben an, welche Klassen von Konfigurationselementen in einem anderen Element über eine bestimmte Beziehung beim Erstellen einer Servicevorlage enthalten sein dürfen. Lassen Sie diese Eigenschaft beim Bilden von CMDB -Warnungsgruppen aktiviert, um alle im Metadaten-Editor definierten Host-Containment-Regeln zu verwenden. Weitere Einzelheiten finden Sie unter Abhängige CMDB-Beziehungsregeln . Diese Eigenschaft ist standardmäßig aktiviert.
Aktivieren Sie die Filterung nach abhängigen Beziehungsregeln *evt_mgmt.related_cis_use_hosting_rules*	Hosting-Regeln definieren, welche Klassen von Configuration Items auf anderen Klassen von Configuration Items gehostet werden. Lassen Sie diese Eigenschaft beim Bilden von CMDB -Warnungsgruppen aktiviert, um Hosting-Regeln anzuwenden, die definieren, welche Klassen von Konfigurationselementen in anderen Klassen gehostet werden. Diese Eigenschaft ist standardmäßig ausgeblendet und aktiviert. **Hinweis:** Wenn Sie den Standardwert ändern müssen, fügen Sie die Eigenschaft hinzu, da sie standardmäßig nicht in der Instanz vorhanden ist. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .
Ignorieren CMDB Sie die Bildung von Warnmeldungsgruppen aufgrund von anwendbaren Flow-Beziehungen auf CI *sa_analytics.agg.ignore_cmdb_application_flow*	Legen Sie diese Eigenschaft auf „true“ fest, um zu verhindern, dass CMDB -Gruppen basierend auf Anwendungs-Flow-Beziehungen für CI-Beziehungen in Anwendungsservices entstehen. Diese Eigenschaft ist standardmäßig ausgeblendet und aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften für die Verwaltung der automatischen Erstellung von CMDB -Warnungsgruppen für erweiterte Anwendungsfälle (Fortsetzung)

Eigenschaft	Einstellung
	Hinweis: Wenn Sie den Standardwert ändern müssen, fügen Sie die Eigenschaft hinzu, da sie standardmäßig nicht in der Instanz vorhanden ist. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .
sa_analytics.applicative_flow_rc_enable	Diese Eigenschaft ist standardmäßig ausgeblendet und aktiviert.

Ereignismanagement speichert für jedes verarbeitete CI eine Zuordnung zugehöriger CIs in der Tabelle Ereignismanagement CI-Diagrammwiederverwendung [em_ci_graph_reuse]. Sie können den Speicherzeitraum anpassen, indem Sie die Eigenschaft *sa_analytics.agg.query_cmdb_graph_reuse_period* ändern. Der Standardwert ist ein Tag (86.400 Sekunden). Dieser Prozess verbessert die Suchleistung von Beziehungen in CMDB. Um den Speicherprozess während erweiterter Anwendungsfallkonfigurationen zu deaktivieren, legen Sie den Eigenschaftswert auf 0 fest.

Hinweis: Wenn Sie den Standardwert ändern müssen, fügen Sie die Eigenschaft *sa_analytics.agg.query_cmdb_graph_reuse_period* hinzu, da sie standardmäßig nicht in der Instanz vorhanden ist. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Zeigen Sie die Abhängigkeitszuordnung für Warnungen CMDB vom Typ an

Die Abhängigkeitszuordnung veranschaulicht, wie und warum Warnungen gruppiert werden, was die Fehlerbehebung und das Problem-Management vereinfacht. Es zeigt Verbindungen zwischen CIs innerhalb einer -Warnungsgruppe CMDB auf und verbessert so die Transparenz ihrer Beziehungen. Wenn ein CI nicht Teil der Gruppe ist, aber eine Verbindung zu anderen Warnungs-CIs herstellt, bleibt es außerdem in der Zuordnung sichtbar, was die Behebung von Warnungen und das proaktive Management unterstützt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user, evt_mgmt_operator

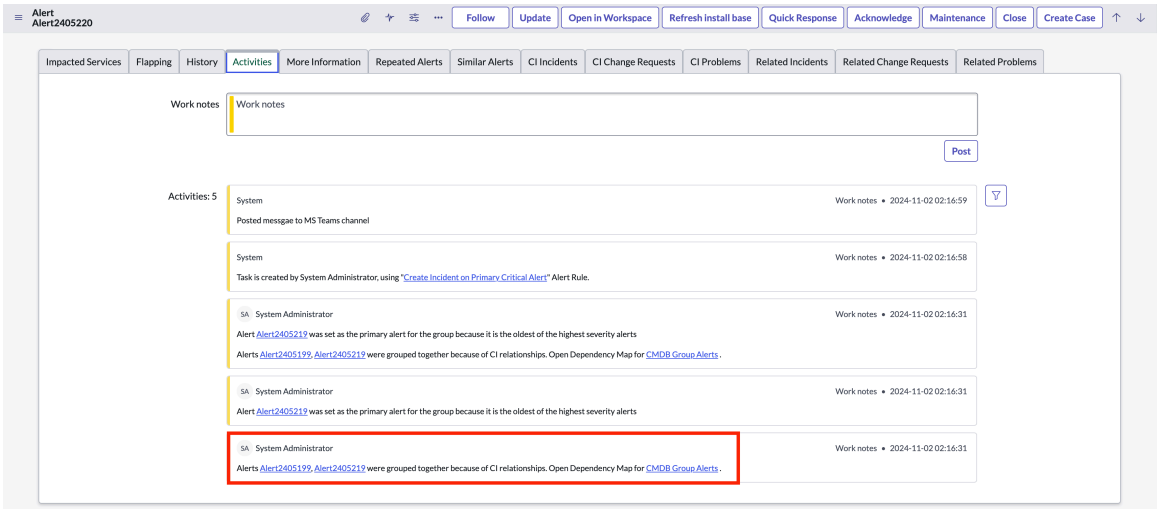
Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Suchen Sie nach der Gruppe CMDB.
3. Öffnen Sie eine Gruppenwarnung CMDB.
4. Scrollen Sie nach unten, und wählen Sie die Registerkarte **Aktivitäten** aus.

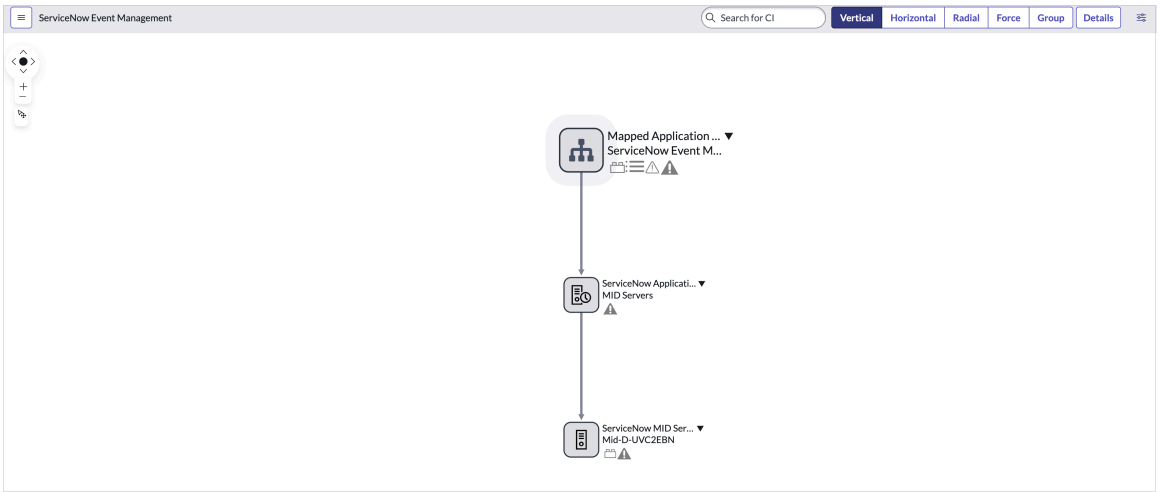
   Unter Umständen wird eine ähnliche Meldung wie die folgende angezeigt:

   ```
   Alert2405199 und Alert2405219 wurden aufgrund von CI-Beziehungen
   zusammen gruppiert. Öffnen Sie die Abhängigkeitszuordnung für CMDB-
   Gruppenwarnungen. Abhängigkeitszuordnung für CMDB-Gruppenwarnungen
   ```
   öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie den Link, um die Abhängigkeitsansicht der CMDB -Warnungen anzuzeigen.



Fügen Sie CMDB Gruppen-CI-Beziehungen eine CI-Beziehung hinzu

Fügen Sie eine CMDB -Gruppen-CI-Beziehung für eine CI-Klasse hinzu, um eine genaue Generierung von Warnmeldungsgruppen zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Konfigurieren Sie die Eigenschaft *sa_analytics.agg.query_cmdb_suggested_relationship_enabled*, um die Warnungsgruppierung mithilfe vorgeschlagener Beziehungen zu verbessern. Weitere Informationen zu Eigenschaften finden Sie unter CMDB -Warnungsgruppierung – Eigenschaften und Funktionalität.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **CMDB-Gruppe – CI-Beziehungen**.

   a. Klicken Sie auf **Neu**.

   b. Füllen Sie das Formular aus.

Felder „Vorgeschlagene Beziehungen“

Feld	Beschreibung
Basisklasse	Die Basisklasse in der Beziehung fungiert je nach Typ der hergestellten Beziehung entweder als übergeordnete Klasse oder als untergeordnete Klasse.
Beziehung	Der Beziehungstyp, der definiert, wie zwei oder mehr Entitäten verbunden werden.
Abhängige Klasse	Die Klasse, die auf eine andere Klasse in der Beziehung angewiesen ist und je nach Beziehungstyp entweder als übergeordnetes Element oder als untergeordnetes Element dient.

2. Klicken Sie auf **Absenden**.

Example: CMDB Gruppen-CI-Beziehung

Basisklasse	Beziehung	Abhängige Klasse/Zielklasse
Oracle	Ist gehostet auf	Linux-Server
Oracle	Ist gehostet auf	Solaris-Server

Hinweis: Dieselbe übergeordnete Klasse und Beziehung können mehr als einmal angezeigt werden.

Löschen Sie eine CI-Beziehung aus CMDB Gruppen-CI-Beziehungen

Löschen Sie eine CI-Beziehung der Gruppe CMDB, um die verfügbaren Beziehungen für die Gruppierung CMDB von -Warnungen einzuschränken und so das Rauschen zu reduzieren und die Relevanz von Warnungen zu verbessern.

Vorbereitungen

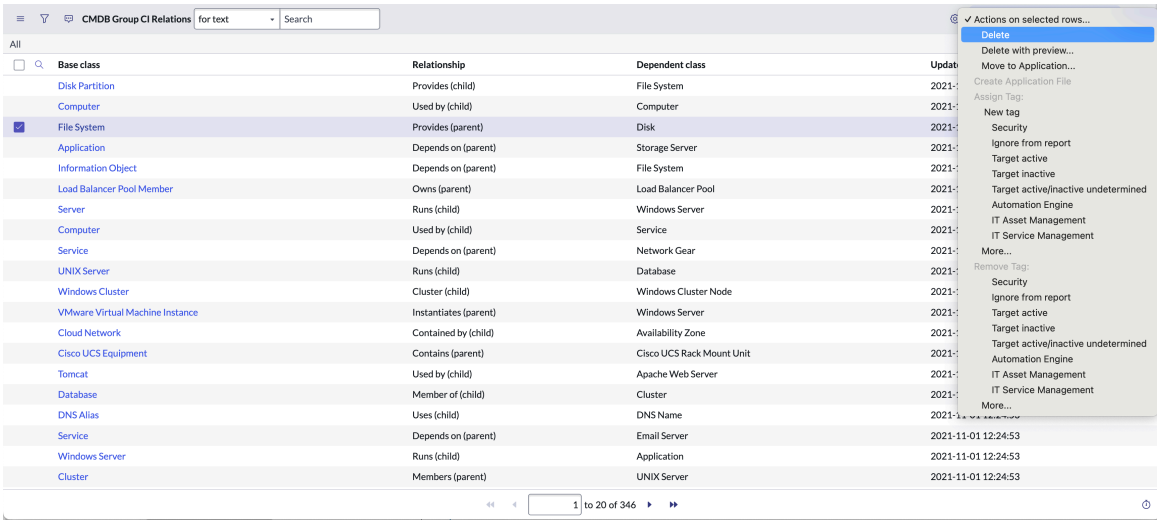
Erforderliche Rolle: evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **CMDB-Gruppe – CI-Beziehungen**.
2. Aktivieren Sie das Kontrollkästchen neben der CI-Beziehung, die Sie löschen möchten.
3. Wählen Sie das Menü Aktionen und dann **Löschen**aus.



4. Wählen Sie im Bestätigungsfenster **Löschen**.
   Die CI-Beziehung wird gelöscht.

Warnungsgruppierung basierend auf Netzwerkdatenverkehr

Die Methode zur auf Netzwerkdatenverkehr basierenden Warnungsgruppierung gruppiert Warnungen, indem der Netzwerkverkehr zwischen Prozessen auf allen Hosts analysiert wird. Er nutzt durch ML Service Mapping identifizierte Servicekandidaten, um Warnungen im Zusammenhang mit Problemen mit dem Netzwerkdatenverkehr zu gruppieren. Dadurch wird sichergestellt, dass Warnungen von direkt verbundenen Prozessen innerhalb desselben Servicekandidaten gruppiert werden, was eine kontextbezogenere Ansicht von Netzwerk-Incidents bietet.

Servicekandidaten sind potenzielle Sammlungen von Prozessen in Ihrer IT-Umgebung, die basierend auf ihren Netzwerkverbindungen und Interaktionen identifiziert werden. Sie stellen verschiedene Services oder Funktionen dar, die Ihre IT-Systeme bereitstellen, auch wenn sie in der Konfigurationsdatenbank Ihres Systems nicht vollständig beschrieben werden. Beispielsweise können Servicekandidaten alle an der E-Mail-Zustellung beteiligten Prozesse zusammenfassen, auch wenn die Konfigurationsdetails unvollständig sind.

ML-Service-Mapping nutzt maschinelles Lernen, um diese Servicekandidaten automatisch zu erkennen und zuzuordnen. Identifiziert, wie verschiedene Prozesse und Komponenten basierend auf ihrem Netzwerkdatenverkehr und ihren Interaktionen verbunden und gruppiert sind. Dies hilft beim Verständnis und der Organisation der IT-Services und ihrer Komponenten, was die Verwaltung und Behebung von Problemen erleichtert. Beispielsweise kann ML Service Mapping die Verbindungen zwischen E-Mail-Servern und E-Mail-Clients basierend auf ihren Netzwerkinteraktionen automatisch identifizieren und zuordnen.

Hinweis: Die auf dem Datenverkehr basierende Warnungsgruppierung ist für Neukunden ab dem Release Yokohama aktiviert. Bestandskunden müssen die Eigenschaft Korrelation des Netzwerkdatenverkehrs aktivieren (*sa_analytics.agg.query_network_traffic_correlation_enabled*) manuell aktivieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionsweise

- Hostidentifizierung: Warnungen im Zusammenhang mit Netzwerkproblemen werden aus verschiedenen Quellen generiert.
- Identifizierung des Netzwerkkontexts: Der Korrelationsprozess verwendet horizontale Discovery-Ergebnisse und ML-Service-Mapping, um die relevantesten Servicekandidaten und Netzwerkverbindungen zu identifizieren.

  Dieser Prozess verwendet die Ergebnisse der regelmäßigen Aufgabe **Ereignismanagement – Service-Candidate-Prozess zu Prozesszuordnung ausfüllen – Täglich**, die einmal pro Tag ausgeführt wird und zum Speichern von Prozess-zu-Prozess-Verbindungen für Host-CIs in dem Format verwendet wird, das für den Warnungsgruppierungsalgorithmus erforderlich ist .

- Warnungsgruppierung: Warnungen werden basierend auf direkten Prozess-zu-Prozess-Verbindungen im Kontext desselben Servicekandidaten gruppiert. Die Gruppierung wird in Echtzeit aktualisiert, wenn neue Warnungen empfangen werden.

Vorteile

- Verbesserte Genauigkeit: Durch die Nutzung von Netzwerkdatenverkehrverbindungen und Servicekandidaten bietet diese Methode eine hohe Genauigkeit bei der Gruppierung von Warnungen und minimiert Falschmeldungen.
- Erweiterte Abdeckung: Warnungen werden auch in Umgebungen mit geringer CMDB-Reife effektiv gruppiert und deckt so ein breiteres Spektrum von Warnungen und Problemen ab.
- Optimierte Lösung: IT-Teams können zugehörige Probleme schnell in einem Massenvorgang identifizieren und lösen, wodurch das Volumen der zu verwaltenden Warnungen reduziert und die betriebliche Effizienz verbessert wird.

Aktivieren Sie die auf Netzwerkdatenverkehr basierende Warnungsgruppierung

Aktivieren Sie die auf dem Datenverkehr im Netzwerk basierende Warnungsgruppierung, um automatisch zu korrelieren und das Warnungsrauschen zu reduzieren, indem Sie zugehörige Ereignisse basierend auf den Mustern des Netzwerkdatenverkehrs gruppieren. Dies trägt zu einer effizienteren Reaktion auf Warnungen bei und rationalisiert das Warnungsmanagement.

Vorbereitungen

Stellen Sie sicher, dass die Anwendung Service Mapping Plus (sn_sm_scoped_app) installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Warnungskorrelationsregeln**.
2. Stellen Sie sicher, dass die Eigenschaft Korrelation des Netzwerkdatenverkehrs aktivieren (*sa_analytics.agg.query_network_traffic_correlation_enabled*) ausgewählt ist.

Auf Datenverkehr basierende Warnungsgruppierung deaktivieren

Deaktivieren Sie die auf Netzwerk-Datenverkehr basierende Warnungsgruppierung, um zu verhindern, dass Warnungen nur nach Netzwerkaktivität gruppiert werden. So reduzieren

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie das Rauschen bei Datenverkehrsspitzen und stellen sicher, dass kritische Probleme hervorstechen und eine schnellere Lösung ermöglichen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Warnungskorrelationsregeln**.
2. Deaktivieren Sie das Kontrollkästchen für die Eigenschaft Korrelation des Netzwerkdatenverkehrs aktivieren (*sa_analytics.agg.query_network_traffic_correlation_enabled*).
3. Legen Sie die Eigenschaft *sa_analytics.enable_process_mapping_calculation* auf „falsch“ fest.

Verfolgen Sie Arbeitsnotizen und überprüfen Sie den Servicekandidaten

Verfolgen und verfolgen Sie Arbeitsnotizen, während Sie den Servicekandidaten überprüfen, um sicherzustellen, dass alle Aktionen und Aktualisierungen erfasst werden. Dies trägt zu Klarheit und Kontinuität im Überprüfungsprozess bei und verringert das Risiko, dass Details übersehen werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin und sm_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.

   Hinweis: Scrollen Sie nach unten zu einer Warnung mit **Netzwerkverkehr** als Gruppe, klicken Sie mit der rechten Maustaste in die Spalte **Gruppe**, und wählen Sie **Übereinstimmungen anzeigen**aus. Hier werden alle Warnungen im Zusammenhang mit **dem Netzwerkverkehr**angezeigt.

2. Wählen Sie für die Warnung, deren Arbeitsnotizen Sie anzeigen möchten, die Warnungsnummer aus.
3. Scrollen Sie auf der Warnungsseite nach unten, und wählen Sie die Registerkarte **Aktivitäten**.
   Sie können die Arbeitsnotizen für die ausgewählte Warnung anzeigen.
4. Wählen Sie in den Arbeitsnotizen den Service-Candidate aus, um Details anzuzeigen.
   Die Seite „Anwendungsservice-Candidate“ wird geöffnet.
5. Wählen Sie **Vorschau des Zuordnungsdiagramms** aus, um die Zuordnung der Servicekandidaten in Form eines Diagramms anzuzeigen.
   Die Zuordnung der Servicekandidaten bietet eine visuelle Darstellung der Verbindung verschiedener Servicekandidaten. So lassen sich Beziehungen leichter verstehen, potenzielle Probleme identifizieren und Abhängigkeiten effektiver analysieren.

Gruppierung von Tag-Clustern von Warnungen

Mit der Gruppierung von Tag-Clustern können Sie auf einfache Weise Warnungsgruppen erstellen. Es handelt sich um eine Methode der Warnungsgruppierung ohne Code, bei der Warnungen korreliert werden, ohne die CMDB oder Modelltraining verwenden zu müssen. Diese einfachere Art der Gruppierung ähnlicher Warnungen reduziert das allgemeine Rauschen einer großen Menge von Warnungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Gruppierung von Tag-Clustern für Warnungen wird unmittelbar nach der Aktivierung der Anwendung Tag-Based Alert Clustering Engine (Engine für tagbasiertes Alarm-Clustering) aktiviert, die unter ServiceNow Storeverfügbar ist. Diese Gruppierung wird gemäß der in Konfigurieren Sie die Reihenfolge der Warnungskorrelationslogikangegebenen Korrelationslogikreihenfolge angewendet. Tags zur Gruppierung von Warnungen werden auf M2M-Basis (Viele-zu-Viele) an Definitionen angehängt. Mehrere Tags können mit einer einzelnen Definition verknüpft werden, und ein Tag kann Teil mehrerer Definitionen sein. Gruppen, die aus Warnungsgruppierungsdefinitionen für Tag-Cluster gebildet werden, werden als Tag-Cluster-Gruppentyp klassifiziert.

Die Gruppierung von Tag-Clustern von Warnungen unterstützt die Domänentrennung, sodass verschiedene Domänen über eigene unterschiedliche Konfigurationen und Logiken für die Gruppierung von Warnungen verfügen.

Erstellen Sie zuerst Gruppierungs-Tags für Warnungen, um die Kriterien für die Gruppierung von Warnungen zu definieren. Sie können die Tags so festlegen, dass eine exakte Übereinstimmung, eine ungefähre Übereinstimmung („Fuzzy-Übereinstimmung“) oder eine Zeichenmusterübereinstimmung erforderlich ist.

Sie können auch vorkonfigurierte Tags verwenden, um das Clustering von Warnungen zu beschleunigen. Diese vordefinierten Tags werden Warnungen zugeordnet und basieren auf Informationen aus Quellen wie dem Feld „Warnung“, den Warnungs-Tags oder den zusätzlichen Warnungsinformationen. Wenn die erforderlichen Daten fehlen und die ausgewählte Tag-Quelle Warnungs-CI oder Warnungs-CI-Schlüssel ist, wird das Tag mit dem Wert Configuration Item (CI) aus Configuration Management Database (CMDB)ausgefüllt. Vordefinierte Tags sind leicht anhand ihrer Beschreibung zu identifizieren, die vordefinierte Tags enthält.

Sie können ein oder mehrere Tags an eine Warnungs-Clustering-Definition anhängen, die die Bedingungen für die Warnungskorrelation angibt. Sie können entweder eine eigene Definition für Warnungs-Clustering erstellen oder eine vordefinierte verwenden, die von der Anwendung bereitgestellt wird. Vordefinierte Definitionen sind mit zugehörigen Tags versehen.

Wichtig: Stellen Sie sicher, dass Sie vordefinierte Definitionen aktivieren, bevor Sie verwenden. In neuen Systemen sind standardmäßig mehrere Definitionen aktiv. Die verbleibenden müssen aktiviert werden. Weitere Informationen finden Sie unter Aktivieren Sie eine vordefinierte Definition für Warnungs-Clustering.

Sobald einer Definition ein oder mehrere Warnungs-Clustering-Tags zugeordnet sind, sammelt das System Warnungen und prüft, ob ihre Tags mit allen in der Definition angegebenen Tag-Werten übereinstimmen. Warnungen mit übereinstimmenden oder ähnlichen Tag-Werten werden zusammen gruppiert. Neue eingehende Warnungen werden einer vorhandenen Gruppe hinzugefügt, wenn ihre Tags mit den Tags in der Definition übereinstimmen, die zum Erstellen der Gruppe verwendet wurde.

Bei der Tag-Cluster-Gruppierung werden Warnungen basierend auf dem Zeitrahmen, der in den Einstellungen für das Warnungs-Clustering definiert ist, einer Gruppe hinzugefügt. Die Zeit zwischen der ersten Warnung (virtuelle Warnung) und den nachfolgenden Warnungen wird ausgewertet. Wenn zwei neue Warnungen empfangen werden und ihre Zeitdifferenz innerhalb des definierten Zeitrahmens liegt, werden sie der Gruppe hinzugefügt. Die Generierungszeit des ersten Ereignisses wird verwendet, um die Relevanz des Zeitrahmens zu bestimmen.

Zugehörige Informationen

- Alarm-Clustering-Tags erstellen
- Alarm-Clustering-Definitionen erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktivieren Sie eine vordefinierte Definition für Warnungs-Clustering

Hängen Sie ein vordefiniertes Tag an eine Tag-basierte Warnungs-Clustering-Definition an

Event-Regel konfigurieren, um den Warnungsinhalt anzupassen

Warnungstags

Alarm-Clustering-Tags erstellen

Erstellen Sie optimierte Warnungskorrelationen mit Warnungs-Clustering-Tags, indem Sie Warnungen, die identische oder ähnliche Tags verwenden, basierend auf Ihrer konfigurierten Übereinstimmungsmethode gruppieren. Dies reduziert das Rauschen, verbessert die Priorisierung von Incidents und die betriebliche Effizienz, was zu einer schnelleren Problemlösung und kürzeren Reaktionszeiten führt.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Engine für tagbasiertes Alarm-Clustering** > **Tags für Warnungs-Clustering**.
2. Klicken Sie auf **Neu**.
3. Geben Sie die Werte im Ereignismanagement-Formular „Tag-basiertes Warnungs-Clustering-Tag“ ein.
4. Wählen Sie **Absenden**.

Ergebnisse
Das Tag wird in der Tabelle „Tag-basierte Warnungs-Clustering-Tags“ angezeigt.

Alarm-Clustering-Definitionen erstellen

Definieren Sie Bedingungen für das Warnungs-Clustering, um ein oder mehrere Tags für das Warnungs-Clustering auszulösen, mit denen Sie Warnungsgruppen aus weniger Warnungen erstellen können. Durch das Erstellen von Warnungsgruppen aus weniger Warnungen wird das Rauschen reduziert. Dadurch können Sie kritische Incidents leichter identifizieren, Antworten priorisieren und Probleme effektiv verwalten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Um eine Tag-Definition zu erstellen, müssen Anwender mithilfe von Filtern definieren, für welche Warnungen die Definition gilt, und Gruppierungskriterien definieren, indem sie angeben, welche Feldwerte verglichen werden sollen, um eine Gruppe zu erstellen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Engine für tagbasiertes Alarm-Clustering** > **Warnungs-Clustering-Definitionen**.
2. Wählen Sie **Neu**.
3. Konfigurieren Sie die Felder im Ereignismanagement-Formular „Tag-basierte Warnungs-Clustering-Definition“.
4. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Die Definition wird in der Tabelle Definitionen für tagbasiertes Warnungs-Clustering unter Service Operations-Arbeitsbereich (ITOM) > Gruppierungsautomatisierung angezeigt. Mit dieser Definition erstellte Warnungsgruppen werden als Tag-Clustergruppen kategorisiert.

Aktivieren Sie eine vordefinierte Definition für Warnungs-Clustering

Aktivieren Sie vor der Verwendung die mit der Anwendung „Engine für tagbasiertes Alarm-Clustering“ bereitgestellten vordefinierten Warnungs-Clustering-Definitionen. Die Verwendung dieser vorkonfigurierten Definitionen minimiert die Setup-Zeit und gewährleistet einen effizienteren Konfigurationsprozess, was eine schnellere Implementierung und eine optimierte Warnungsverwaltung ermöglicht.

Vorbereitungen

Wichtig: Wenn Sie bereits die Anwendung „Engine für tagbasiertes Alarm-Clustering“ verwenden, sind alle vordefinierten Definitionen inaktiv und müssen aktiviert werden. Im Gegensatz dazu sind für Neukunden standardmäßig mehrere Definitionen aktiv, sodass die Funktionen zur Erstellung von Warnungs-Clustern ohne zusätzliche Einrichtung sofort verwendet werden können.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Engine für tagbasiertes Alarm-Clustering** > **Clustering-Definitionen**.
2. Wählen Sie eine vordefinierte Definition aus.

   Hinweis: Eine vollständige Liste der verfügbaren vordefinierten Definitionen finden Sie unter Liste der vordefinierten Definitionen für tagbasiertes Warnungs-Clustering.

3. Aktivieren Sie im Formular „Definition für tag-basiertes Warnungs-Clustering“ das Kontrollkästchen **Aktiv**.
4. Wählen Sie **Speichern**.

Ergebnisse
In der Tabelle Definitionen für tag-basiertes Warnungs-Clustering zeigt das Feld **Aktiv** für die aktivierte Definition den Wert **wahr**an. Sie können dieser Definition jetzt ein Warnungs-Clustering-Tag zuordnen, um eine effektive Gruppierung von Warnungen basierend auf den definierten Kriterien zu ermöglichen.

Hängen Sie ein vordefiniertes Tag an eine Tag-basierte Warnungs-Clustering-Definition an

Beginnen Sie schneller mit Warnungs-Clustering, indem Sie ein vordefiniertes Warnungs-Clustering-Tag an eine Tag-basierte Warnungs-Clustering-Definition in Ereignismanagementanhängen. Durch das Zuordnen eines vordefinierten Tags stellen Sie sicher, dass Warnungen, die die angegebenen Kriterien erfüllen, effektiv gruppiert werden, was zu einer schnelleren Identifizierung und Reaktion auf zugehörige Incidents führt.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Anwendung „Engine für tagbasiertes Alarm-Clustering“ enthält eine Reihe von vordefinierten Tags für das Clustering von Warnungen. Fügen Sie einer Tag-basierten Warnungs-Clustering-Definition ein Tag hinzu, um die Bedingungen anzugeben, die für die Warnungskorrelation erfüllt sein müssen. Dies ermöglicht eine effektive Gruppierung von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungen auf Grundlage gemeinsamer Merkmale. Dadurch werden Genauigkeit und Effizienz der Reaktion auf und Verwaltung von Incidents verbessert.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Engine für tag-basiertes Alarm-Clustering** > **Warnungs-Clustering-Definitionen**.
2. Wählen Sie eine Definition aus.
3. Wählen Sie im Abschnitt „Definitionen für Tag-basiertes Warnungs-Clustering – Tags M2M“ **Neue Zeile einfügen aus**.
4. Verwenden Sie das Suchfeld, um ein vordefiniertes Warnungs-Clustering-Tag zu finden, und aktivieren Sie dann das grüne Häkchen, um Ihre Auswahl zu bestätigen.

   Hinweis: Vordefinierte Tags sind an ihrer Beschreibung erkennbar, zu der auch „sofort einsatzbereit“ gehört. Eine vollständige Liste der verfügbaren vordefinierten Tags finden Sie unter Liste der vordefinierten Tags für Warnungs-Clustering.

5. Wählen Sie **Speichern**.

Ergebnisse

Das vordefinierte Tag für Warnungs-Clustering ist jetzt an die Tag-basierte Warnungs-Clustering-Definition angehängt. Diese Zuordnung ermöglicht die effektive Gruppierung von Warnungen basierend auf den angegebenen Kriterien, was die Warnungsverwaltung und die Reaktionseffizienz verbessert.

Textbasierte Warnungsgruppierung

Bei der textbasierten Warnungsgruppierung werden Warnungen anhand bestimmter Textmuster oder Stichwörter im Warnungsinhalt organisiert und korreliert. Dieser Ansatz gruppiert Warnungen, die ähnliche Textmerkmale aufweisen, z. B. Fehlermeldungen oder Ereignisbeschreibungen, dynamisch, was eine flexiblere und anpassungsfähigere Verwaltung von Warnungen ermöglicht.

Die EM Alert Clustering-Lösung ist eine Methode, die verwendet wird, um Warnungen basierend auf Ähnlichkeiten in bestimmten Feldern zu korrelieren und Cluster oder Gruppen zu bilden. In ServiceNow Ereignismanagementwerden Cluster auf Grundlage der Felder Beschreibung, Metrikname und Configuration item.Class-Felder erstellt. Diese Lösung organisiert Warnungen in textbasierten Gruppen, und wenn eine neue Warnung eingeht, identifiziert die ML-Vorhersage das entsprechende Cluster und gruppiert Warnungen innerhalb desselben Clusters.

Hinweis: Der ML-Vorhersageauftrag ist asynchron und weist Clustern Echtzeitwarnungen zu, was zu geringfügigen Verzögerungen führen kann. Diese Verzögerung kann dazu führen, dass textbasierte Gruppen einige Minuten später erstellt werden, da die Aufgabe zur Gruppierung von Warnungen einmal pro Minute ausgeführt wird. Wenn Vorhersageergebnisse während einer Ausführung nicht verfügbar sind, werden sie im nächsten Gruppierungsauftrag erneut überprüft.

Damit die textbasierte Logik ausgeführt werden kann, muss das Plugin Predictive Intelligence (com.glide.platform_ml) installiert und die Definition der EM Alert Clustering-Lösung aktiviert sein.

Es gibt bestimmte Einstellungen oder Grenzwerte zur Steuerung des Verhaltens der textbasierten Warnungsgruppierung. Diese Schwellenwerte definieren die Kriterien für die Gruppierung von Warnungen basierend auf Textmustern oder Attributen. Die textbasierten Schwellenwerte sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Clusterqualitätsschwellenwert: Der Clusterqualitätsschwellenwert (*sa_analytics.alert_grouping_tb_cluster_quality_threshold*) bestimmt die Mindestqualität, die erforderlich ist, damit ein Warnungscluster als gültig angesehen wird. Dieser Schwellenwert stellt sicher, dass nur Cluster mit einem Mindestmaß an Ähnlichkeit und Zuverlässigkeit verwendet werden. Cluster, die diesen Schwellenwert erfüllen, gelten als gültig. Dadurch wird die Genauigkeit der Gruppierungen verbessert und Rauschen durch irrelevante Cluster oder Cluster mit niedriger Qualität reduziert. Der Schwellenwert liegt zwischen 1 und 100, der Standardwert ist 70.
- Warnungsrangschwellenwert: Der Warnungsrangschwellenwert (*sa_analytics.alert_grouping_tb_alert_rank_threshold*) definiert den Mindestrang, der erforderlich ist, damit eine Warnung in eine Gruppe aufgenommen wird. Dieser Schwellenwert stellt sicher, dass nur Warnungen mit einem bestimmten Ähnlichkeitsgrad in einer Gruppe zusammengefasst werden, wobei Warnungen mit niedrigerem Rang herausgefiltert werden, um die Qualität der Warnungsgruppe zu erhalten. Der Standardwert ist 0,3, wobei niedrigere Werte auf eine bessere Ähnlichkeit hindeuten.

Hinweis: Um diese Eigenschaften zu verwenden, müssen Sie Eigenschaften mit denselben Namen erstellen und ihnen die erforderlichen Werte zuweisen. Weitere Informationen zum Erstellen einer Eigenschaft finden Sie unter Systemeigenschaft hinzufügen .

Die Definition der EM Alert Clustering-Lösung befindet sich in der Tabelle [ml_capability_definition_clustering]. Um darauf zuzugreifen, navigieren Sie zu **Predictive Intelligence** > **Clustering** > **Lösungsdefinitionen**.

Informationen dazu, ob die Lösungsdefinition aktiv ist, finden Sie unter Überprüft die Lösung für textbasiertes Clustering. Zum Deaktivieren der Definition der EM-Warnungs-Clustering-Lösung deaktivieren Sie die textbasierte Warnungsgruppierung, indem Sie die Eigenschaft *sa_analytics.text_based_group_enabled* auf `„false“` festlegen und das Kontrollkästchen **Aktiv** in der Definition der EM-Warnungs-Clustering-Lösung deaktivieren.

Beispiel für textbasierte Warnungsgruppierung

Szenario	Beispiel
Probleme mit der Netzwerkverbindung: Es gibt weit verbreitete Probleme mit der Netzwerkverbindung, die mehrere Abteilungen betreffen.	Warnungen von verschiedenen Netzwerküberwachungstools können Probleme wie Netzwerksegmentausfall, hoher Paketverlust oder Konnektivitätsprobleme im Subnetz melden. Die textbasierte Warnungsgruppierung nutzt die EM Alert Clustering-Lösung und die ML-Vorhersage, um die Warnungsverwaltung zu optimieren. Die EM Alert Clustering-Lösung verwendet Natural Language Processing-Algorithmen (NLP), um häufige Textmuster in Warnungen wie Netzwerksegmentausfall oder hoher Paketverlust zu analysieren und zu identifizieren. Anschließend werden diese Warnungen basierend auf ihrer Textähnlichkeit gruppiert und zugehörige Probleme gruppiert. Die ML-Vorhersage verbessert diesen Prozess zusätzlich,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenario	Beispiel
	indem sie neue Warnungen in Echtzeit auswertet und anhand ihrer Textmuster den entsprechenden vorhandenen Clustern zuordnet. Diese dynamische Gruppierung bietet eine konsolidierte Ansicht der Konnektivitätsprobleme, sodass Netzwerktechniker schnell diagnostizieren und die Ursache der Probleme effizienter beheben können.

Überprüft die Lösung für textbasiertes Clustering

Ereignismanagement verwendet NLP-Algorithmen (Natural Language Processing), um allgemeine Textmuster in Warnungen zu identifizieren und durch Clustering Warnungsgruppen zu erstellen. Dieser Ansatz ermöglicht nicht nur die effiziente Organisation ähnlicher Warnungen, sondern reduziert auch das Rauschen und hilft, sich auf wichtige Probleme zu konzentrieren, wodurch das Warnungsmanagement insgesamt verbessert wird.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Predictive Intelligence (com.glide.platform_ml) installiert ist.

Stellen Sie sicher, dass der Parameter *sa_analytics.text_based_group_enabled* auf `true` festgelegt ist.

Hinweis: Wenn das Plugin Predictive Intelligence nicht installiert ist, wird die textbasierte Logik nicht ausgeführt, auch wenn *sa_analytics.text_based_group_enabled* auf „wahr“ festgelegt ist. Dies liegt daran, dass die textbasierte Gruppierung auf der Gruppierung von Warnungen basierend auf der Beschreibung, dem Metriknamen und der CI-Klasse basiert. Ohne das Plugin kann kein Clustering durchgeführt werden, und daher werden unabhängig vom aktiven Status keine textbasierten Gruppen erstellt.

Stellen Sie sicher, dass mindestens 100 Warnungen in der Warnungstabelle [em_alerts] vorhanden sind.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Predictive Intelligence** > **Clustering** > **Lösungsdefinitionen**.
   Die Seite „Clustering-Definitionen“ wird geöffnet.
2. Wählen Sie EM Warnungsmeldung Clustering-Lösung aus.
3. Stellen Sie sicher, dass die Checkbox **Aktiv** aktiviert ist.
4. Wählen Sie **Aktualisieren und neu trainieren** aus.
   Weitere Informationen zu ML-Lösungen finden Sie unter Trainingsaufträge für ML-Lösungen überprüfen .

Manuelle Warnungsgruppierung

Die manuelle Gruppierung von Warnungen umfasst das Organisieren und Kategorisieren von Warnungen basierend auf anwenderdefinierten Kriterien und direkten Eingriffen.

Sie können Warnungen manuell auswählen und gruppieren, um Incidents besser zu verwalten und zu lösen, indem Sie die Gruppierung basierend auf bestimmten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anforderungen, Relevanz oder Kontext anpassen. Dieser Ansatz stellt eine effektive Kategorisierung von Warnungen sicher und verbessert das allgemeine Incident-Management sowie die Reaktionseffizienz.

Erstellen Sie manuell eine Warnmeldungsgruppe

Erstellen Sie manuell eine Warnmeldungsgruppe, um zugehörige Warnungen zu organisieren und zu verwalten, wenn Sie keine geplanten Aufgaben verwenden. Dies bietet Flexibilität, um Warnungen bei Bedarf für eine effektive Lösung zu gruppieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

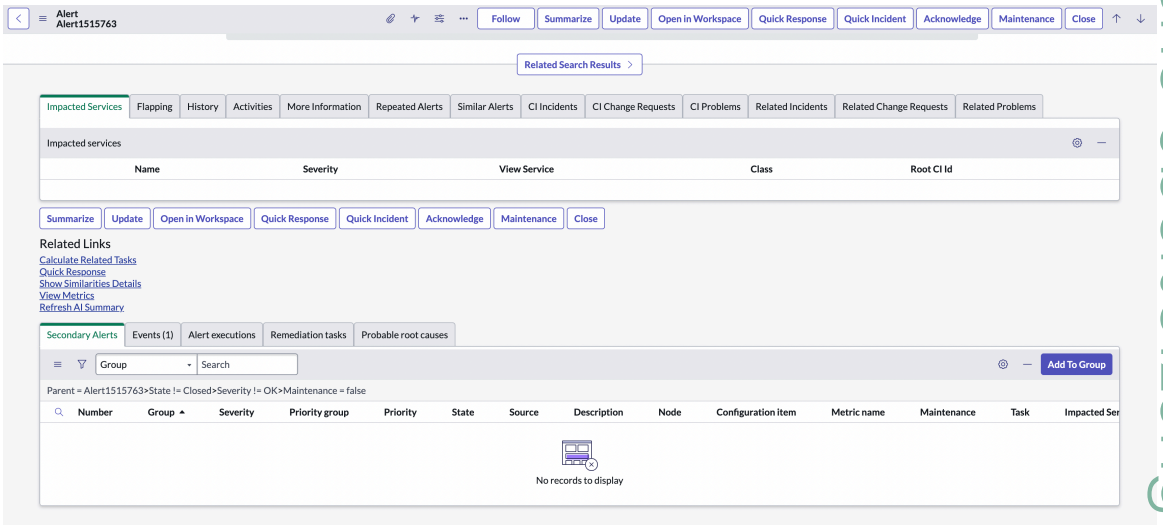
Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Wählen Sie die Warnungsnummer aus, um die Warnung zu öffnen.

   Die Warnung wird verwendet, um eine Warnmeldungsgruppe zu erstellen, die als primäre Warnung festgelegt wird und der Sie sekundäre Warnungen hinzufügen können.

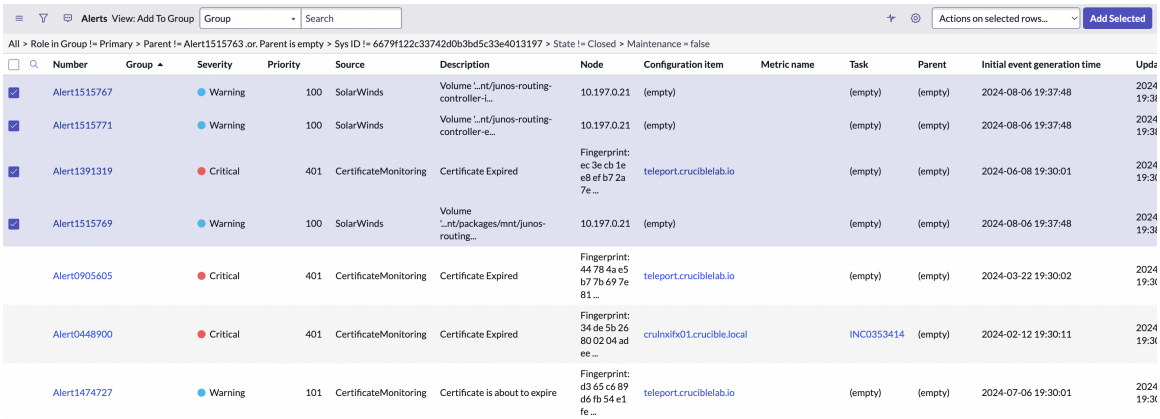
   Hinweis: Eine geschlossene Warnung kann nicht als übergeordnete Warnung zugewiesen werden.

3. Scrollen Sie nach unten, und wählen Sie auf der Registerkarte **Sekundäre Warnungendie Option Zu Gruppe hinzufügen**aus.

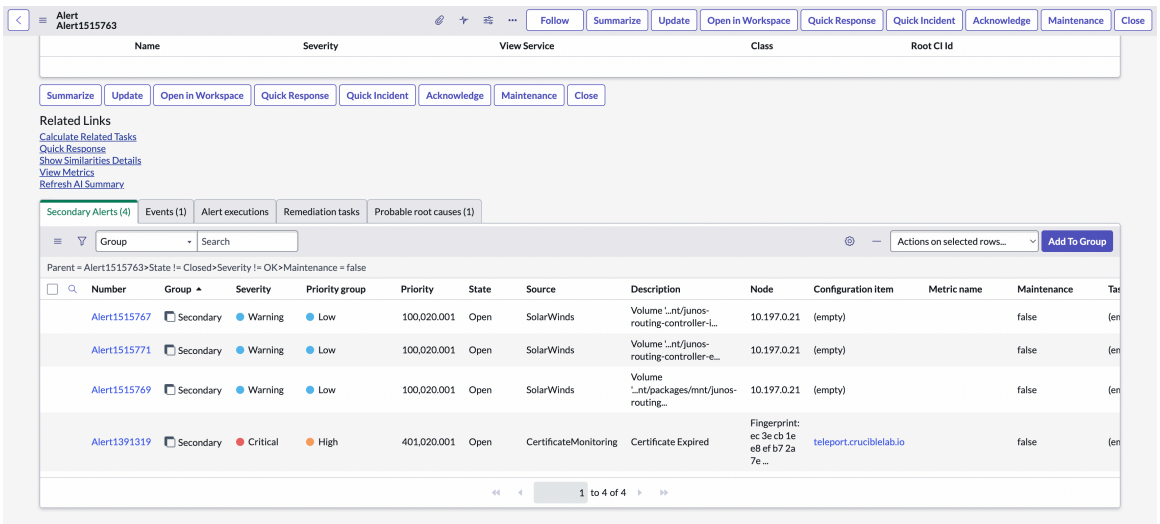


4. Aktivieren Sie die Kontrollkästchen für alle Warnungen, die Sie der Gruppe als sekundäre Warnungen hinzufügen möchten, und wählen Sie **Ausgewählte hinzufügen**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Zeigen Sie auf der Registerkarte **Sekundäre Warnungen** die Warnungen an, die als sekundär hinzugefügt wurden.



Fügen Sie eine sekundäre Warnung manuell einer vorhandenen Warnmeldungsgruppe hinzu

Fügen Sie alle relevanten Warnungen, die bei der Überprüfung einer automatisierten Warnungsgruppe erkannt wurden, als sekundäre Warnungen hinzu, um die Vollständigkeit und den Nutzen der Gruppe für die Problembehandlung bei Incidents zu verbessern.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Warnung, die Sie zum Hinzufügen zu einer neuen Gruppe auswählen, ist möglicherweise bereits Teil einer anderen Gruppe. Durch Hinzufügen zur neuen Gruppe wird er automatisch aus der aktuellen Gruppe entfernt und seine Gruppenzuordnung geändert. Alternativ können Sie das übergeordnete Element der Warnung aktualisieren, um sie in eine andere Gruppe zu verschieben. Durch Angabe eines neuen übergeordneten Elements wird die Warnung an die Gruppe des neuen übergeordneten Elements übertragen und aus der vorherigen Gruppe entfernt. Dies kann durch Aktualisieren des Felds **Übergeordnet** im Warnungsformular oder durch Ändern der Spalte **Übergeordnet** in der Warnungsliste erfolgen.

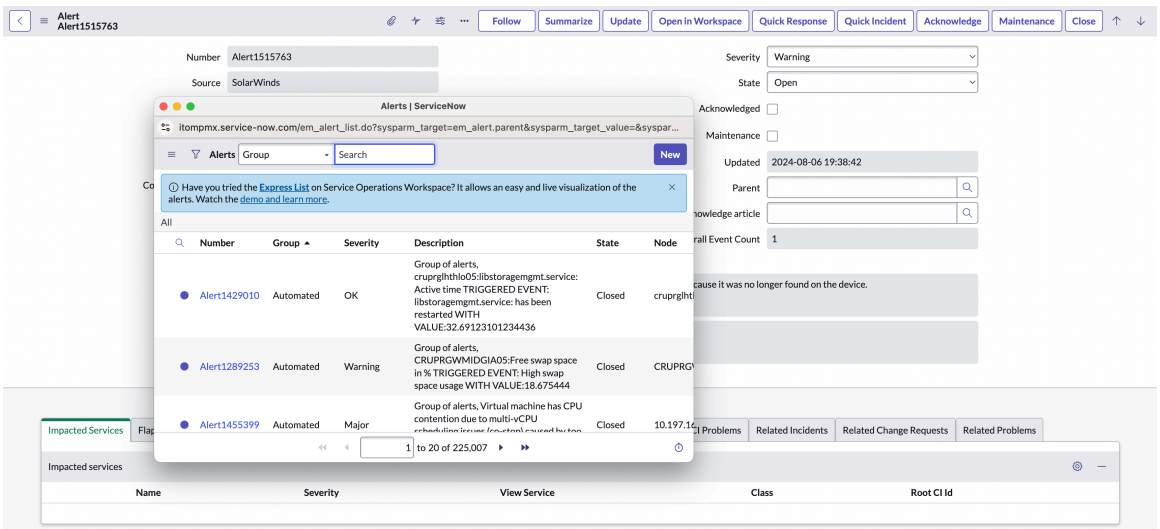
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie einer Gruppe eine Warnung hinzufügen, wird diese Aktion als Feedback für die Gruppierung von Warnungen im Rahmen des Prozesses protokolliert. Derzeit ist die Feedback-Option verfügbar, löst jedoch nach der Protokollierung keine weiteren Aktionen aus. Zukünftige Verbesserungen dieser Funktion werden berücksichtigt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Wählen Sie die Warnungsnummer aus, um die Warnung zu öffnen.
3. Suchen Sie im Feld **Übergeordnet** nach der Warnung, die Sie der ausgewählten Warnung als übergeordnetes Element zuweisen möchten.



4. Wählen Sie die Nummer der übergeordneten Warnung aus.
5. Wählen Sie **Aktualisieren**.

Ergebnisse

Die Warnung wird als sekundäre Warnung zur ausgewählten übergeordneten Warnung hinzugefügt.

Warnungen aus einer Warnungsgruppe entfernen

Entfernen Sie eine Warnung, wenn Sie die Genauigkeit und Nützlichkeit der Gruppe bei der Fehlerbehebung für einen Incident verbessern möchten. Wenn diese Aktion die Gruppe mit einer oder keinen Warnungen verlässt, wird die Gruppe gelöscht und nicht mehr als Warnungsgruppe angezeigt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator

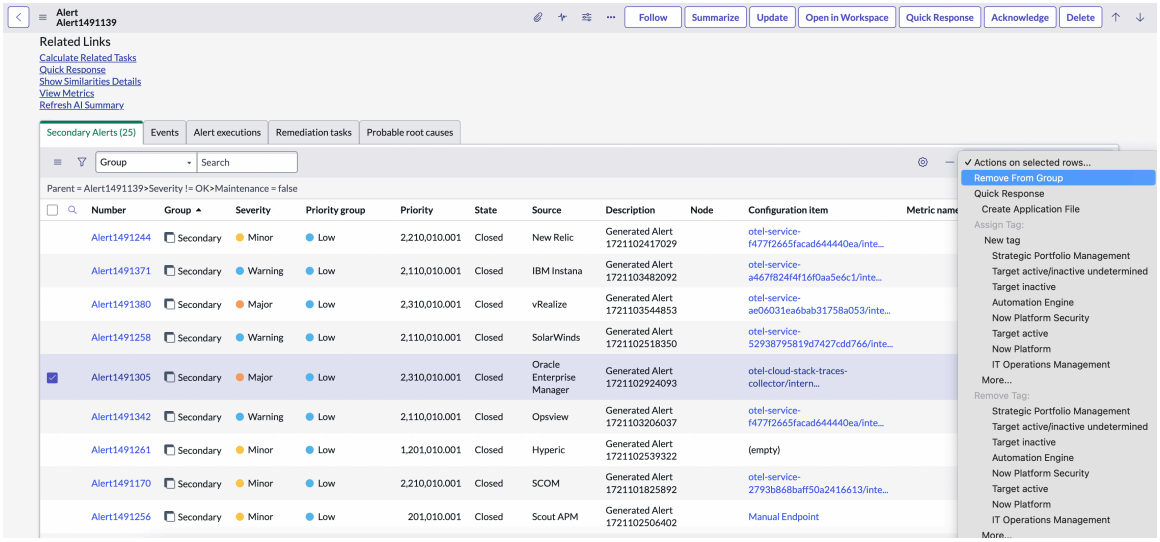
Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Wählen Sie die Warnungsnummer aus, um die Warnmeldungsgruppe zu öffnen.
3. Scrollen Sie nach unten, um die Registerkarte **Sekundäre Warnungen** anzuzeigen.
4. Aktivieren Sie das Kontrollkästchen neben der Warnung, die Sie aus der Gruppe entfernen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Menü Aktionen für ausgewählte Zeile die Option **Aus Gruppe entfernen aus**.



Ergebnisse

Die Warnung wird aus der Gruppe entfernt.

Arbeitsnotizen konfigurieren, um Begründungen für Warnungsgruppierungen zu erfassen

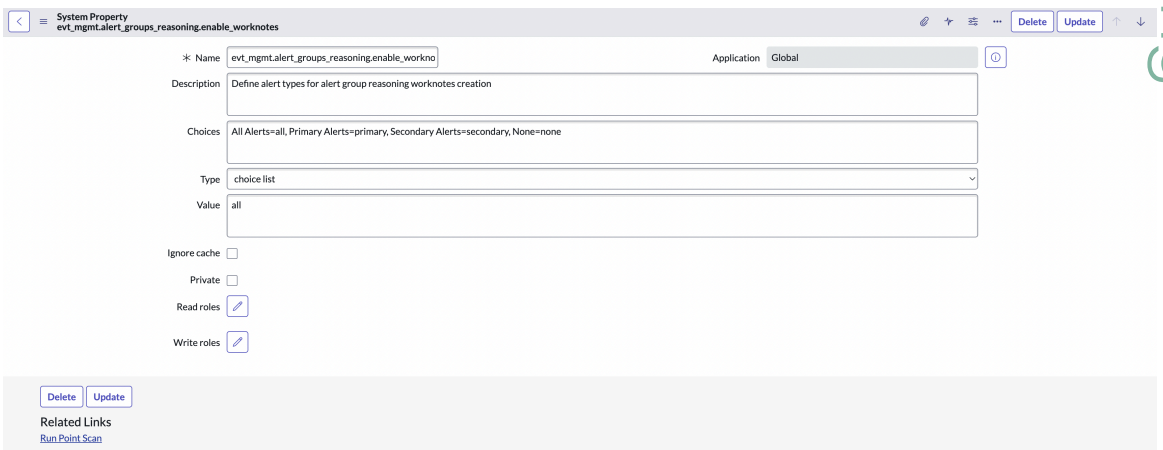
Wenn Warnungen einer Gruppe hinzugefügt werden, wird im Feld Arbeitsnotizen der Warnung eine Nachricht aufgezeichnet, um zu erklären, warum die Warnung in die Gruppe aufgenommen wurde. Definieren Sie Warnungstypen zum Erstellen dieser Arbeitsnotizen im Zusammenhang mit der Argumentation von Warnungsgruppen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Suchen Sie nach der Eigenschaft *evt_mgmt.alert_groups_reasoning.enable_worknotes*.
3. Öffnen Sie die Eigenschaft.



4. Definieren Sie im Feld **Auswahlmöglichkeiten** Warnungstypen für die Erstellung von Arbeitsnotizen im Zusammenhang mit der Argumentation von Warnmeldungsgruppen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaftswerte

Wert	Beschreibung
Alle Warnungen	Für jede Warnung werden Arbeitsnotizinformationen generiert.
Primäre Warnungen	Arbeitsnotizdaten werden nur für primäre Warnungen generiert.
Sekundäre Warnungen	Arbeitsnotizdaten werden nur für sekundäre Warnungen generiert.
Keine	Es werden keine Arbeitsnotizdaten generiert.

5. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Warnungsgruppierungstypen und -erstellungsmethoden

Anwendungsservice in Ereignismanagement

Ein Anwendungsservice ist eine Reihe untereinander verbundener Anwendungen und Hosts, die so konfiguriert sind, dass sie einer Organisation einen Service bereitstellen.

Allgemeine Informationen zu Anwendungsservices finden Sie unter Anwendungsservices .

Erstellen Sie manuell einen Anwendungsservice in Ereignismanagement

Sie können Anwendungsservices manuell erstellen. Ereignismanagement kann Anwendungsservices verwenden, um die Serviceleistung zu überwachen und Integritätsprobleme zu identifizieren.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Anwendungsservices stellen eine Reihe verbundener Anwendungen und Hosts dar, die so konfiguriert sind, dass sie einer Organisation einen Service bereitstellen. Anwendungsservices können intern sein, beispielsweise ein E-Mail-System einer Organisation, oder auf Kunden ausgerichtet sein, z. B. die Website einer Organisation. Verwenden Sie Anwendungsservices, um Services in Ihrer Organisation zu organisieren, zu warten und zu überwachen.

Anwendungsservices unterstützen die folgenden CI-Typen nicht:

- cmdb_ci_endpoint
- cmdb_ci_translation_rule
- cmdb_ci_config_file
- cmdb_ci_qualifier
- cmdb_ci_application_cluster

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Anwendungsservices**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie ein Serviceformular

Feld	Beschreibung
Name	Geben Sie einen eindeutigen Anwendungsservicenamen ein.
Eigentum von	Geben Sie einen Inhaber an, der für diesen Anwendungsservice im Unternehmen verantwortlich ist.
Einstiegspunkte hinzufügen:	
CI-Typ	Wählen Sie den CI-Typ (CI-Klasse) für das hinzuzufügende CI aus. Jedes CI gehört zu einem CI-Typ, der eine Reihe von Attributen enthält, die für diese Art von CI konfiguriert wurden. cmdb_ci_appl für Anwendungen.
CI-Name	Wählen Sie das CI aus der Liste der CIs des ausgewählten CI-Typs aus.

Die Liste der CI-Typen enthält nur zulässige CI-Typen. Sie können beispielsweise keinen Anwendungscluster hinzufügen.

4. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Einzelheiten zur Gruppierung von Anwendungsservices finden Sie unter Anwendungsservices gruppieren.

Einzelheiten zum Steuern des Benutzerzugriffs auf Anwendungsservices finden Sie unter Benutzerzugriff auf Anwendungsservices steuern.

Konvertieren Sie manuelle Services in Anwendungsservices

Sie können vorhandene manuelle Services in Anwendungsservices konvertieren. Ereignismanagement kann Anwendungsservices verwenden, um die Serviceleistung zu überwachen und Integritätsprobleme zu identifizieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Manuelle Services werden nicht mehr unterstützt, und dieser Servicetyp sowie erkannte Services wurden durch Anwendungsservices ersetzt. Alle vorhandenen manuellen Services müssen in Anwendungsservices konvertiert werden.
Während des Konvertierungsvorgangs:

- Der manuelle Serviceeintrag wird von der Tabelle für manuelle Services [cmdb_ci_service_manual] in die Tabelle für zugeordnete Anwendungsservices [cmdb_ci_service_discovered] durch Änderung der Datensatzklasse verschoben.
- Alle ursprünglichen manuellen Serviceattribute, z. B. Name, Besitzer und Betriebsstatus, werden in den Anwendungsservices beibehalten.
- Die Configuration Items (CIs) des manuellen Service bleiben nach der Konvertierung in den Anwendungsservices erhalten.
- Das System fragt die CMDB nach den neuesten CI-Changes ab und wendet die CI-Auswirkungsregeln an.

Anwendungsservice unterstützt diese CI-Typen nicht:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

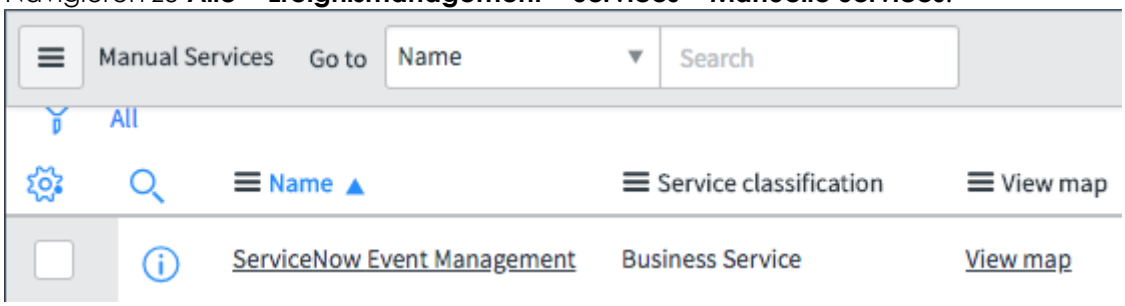
- cmdb_ci_endpoint
- cmdb_ci_translation_rule
- cmdb_ci_config_file
- cmdb_ci_qualifier
- cmdb_ci_application_cluster

Wenn die vorherigen CI-Typen im manuellen Service verwendet werden, den Sie konvertieren möchten, schlägt die Konvertierung fehl. CIs dieses Typs sollten vor der Konvertierung entfernt werden. Sie können ersetzt werden, indem den Anwendungsservices nach der Konvertierung neue CIs hinzugefügt werden.

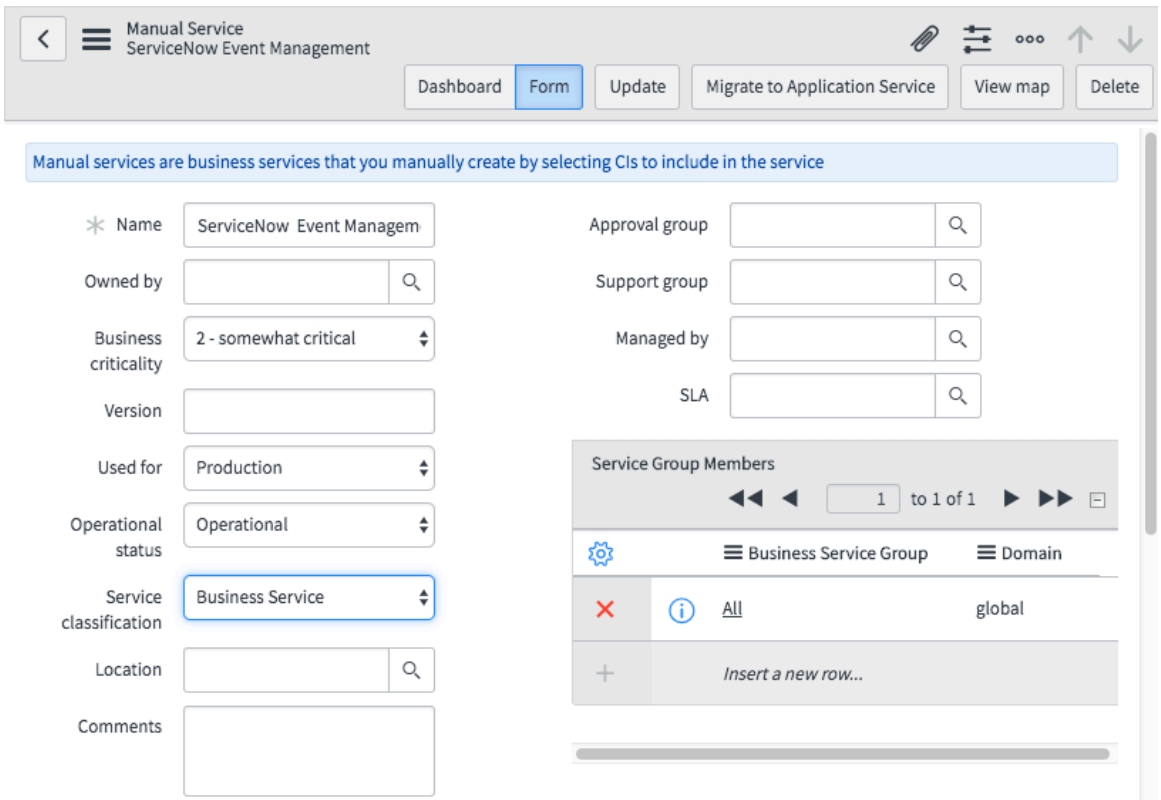
Wenn Ihre Instanz ServiceNow Domain Separation verwendet, schlägt die Konvertierung fehl, wenn sich CIs aus mehreren Domänen im gleichen Service befinden. Ersetzen oder entfernen Sie relevante CIs vor der Konvertierung. Die konvertierten Anwendungsservices enthalten nur CIs, die derselben Domäne wie die Anwendungsservices zugewiesen sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Manuelle Services**.



2. Wählen Sie den manuellen Service aus, den Sie in Anwendungsservices konvertieren möchten.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Zu Anwendungsservice migrieren**.
4. Klicken Sie auf **OK**.

Ergebnisse

- Die CIs aus dem manuellen Service werden den konvertierten Anwendungsservices hinzugefügt.
- Nachdem der Konvertierungsprozess abgeschlossen ist, wird das Formular für Anwendungsservices geöffnet.

Konvertieren Sie manuelle Services mithilfe der API in Anwendungsservices

Sie können eine JavaScript-API verwenden, um vorhandene manuelle Services in Anwendungsservices zu konvertieren. Ereignismanagement kann Anwendungsservices verwenden, um die Serviceleistung zu überwachen und Integritätsprobleme zu identifizieren.

Manuelle Services werden nicht mehr unterstützt, und dieser Servicetyp sowie erkannte Services wurden durch Anwendungsservices ersetzt. Alle vorhandenen manuellen Services müssen in Anwendungsservices konvertiert werden. Stellen Sie sicher, dass jede Automatisierung manueller Services (wie Geschäftsregeln und regelmäßige Aufgaben) erstellt und getestet wird, bevor Sie sie in Anwendungsservices konvertieren.

Hinweis: Manuelle Services sind statisch und behalten nach der Konvertierung in Anwendungsservices ihre ursprüngliche Struktur. Um importierte manuelle Services mit dem vorhandenen CMDB-Status zu aktualisieren, füllen Sie entweder die ursprünglichen manuellen Services, um sicherzustellen, dass alle CIs dem richtigen Service zugewiesen sind, oder führen Sie nach der Konvertierung die Option zum **Mit CMDB-Changes aktualisieren** aus.

Während des Konvertierungsvorgangs:

- Der manuelle Serviceeintrag wird von der Tabelle für manuelle Services [cmdb_ci_service_manual] in die Tabelle für zugeordnete Anwendungsservices [cmdb_ci_service_discovered] durch Änderung der Datensatzklasse verschoben.
- Alle ursprünglichen manuellen Serviceattribute, z. B. Name, Besitzer und Betriebsstatus, werden in den Anwendungsservices beibehalten.
- Die Configuration Items (CIs) des manuellen Service bleiben nach der Konvertierung in den Anwendungsservices erhalten.
- Das System fragt die CMDB nach den neuesten CI-Changes ab und wendet die CI-Auswirkungsregeln an.

Die maximale Anzahl von CI-Verbindungen, die Anwendungsservices während dieses Vorgangs hinzugefügt werden, wird durch die Eigenschaft „sa.service.max_ci_service_population“ gesteuert. Standardmäßig ist der Wert 1000 festgelegt (1000 Verbindungen). Eine höhere Anzahl von CI-Verbindungen kann zu Leistungsproblemen führen. Um die maximale Anzahl der hinzugefügten CI-Verbindungen anzupassen, fügen Sie die Eigenschaft „sa.service.max_ci_service_population“ hinzu (siehe Systemeigenschaften hinzufügen).

Wenn Sie versuchen, mehr CIs zu verarbeiten, als in der Eigenschaft „sa.service.max_ci_service_population“ angegeben sind, schlägt der Vorgang fehl.

Führen Sie den Konvertierungsprozess in kleinen Blöcken von jeweils ungefähr 10 aus, um den problematischen Service im Falle eines Konvertierungsproblems leichter zu lokalisieren.

Anwendungsservices unterstützen die folgenden CI-Typen nicht:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- cmdb_ci_endpoint
- cmdb_ci_translation_rule
- cmdb_ci_config_file
- cmdb_ci_qualifier
- cmdb_ci_application_cluster

Wenn die vorherigen CI-Typen im manuellen Service verwendet werden, den Sie konvertieren möchten, schlägt die Konvertierung fehl. CIs dieses Typs sollten vor der Konvertierung entfernt werden. Sie können ersetzt werden, indem den Anwendungsservices nach der Konvertierung neue CIs hinzugefügt werden.

Wenn Ihre Instanz ServiceNow Domain Separation verwendet, schlägt die Konvertierung fehl, wenn sich CIs aus mehreren Domänen im gleichen Service befinden. Ersetzen oder entfernen Sie relevante CIs vor der Konvertierung. Die konvertierten Anwendungsservices enthalten nur CIs, die derselben Domäne wie die Anwendungsservices zugewiesen sind.

Die JavaScript-API lautet:

```
BusinessServiceManager.migrateManualToApplicationService(String
 service_id)
```

Parameter

Name	Typ	Beschreibung
service_id	Zeichenfolge	Sys-ID des zu konvertierenden manuellen Service

Ergebnisse

Typ	Beschreibung
Boolescher Wert	`„true“` für eine erfolgreiche Konvertierung, `„false“` für eine fehlgeschlagene Konvertierung

Wenn die `sys_id` eines vorhandenen manuellen Services `451047c6c0a8016400de0ae6df9b9d76`ist, führen Sie die folgende API aus, um sie in Anwendungsservices zu konvertieren:

```
var bsManager = new SNC.BusinessServiceManager();
var res =
 bsManager.migrateManualToApplicationService("451047c6c0a8016400de0ae6df9
b9d76");
```

Zugehörige Informationen

BusinessServiceManager – Global

Konfiguration von CIs in einem manuellen Service als manueller Cluster

Konfigurieren oder ändern Sie ein CI als bestimmtes CI oder generische CI-Klasse in einem manuellen Service (der nicht automatisch erkannt wurde) als manuell definiertes Cluster. Ein manueller Cluster bietet Redundanzfähigkeiten im Cluster und bietet kontinuierliche Vorgänge oder Services des gesamten Clusters, falls ein oder mehrere CIs in diesem Cluster ausfallen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit dem manuellen Cluster können Sie CIs unter einem logischen Cluster in einem Service gruppieren. In der Auswirkungsstruktur können Sie die relative Auswirkung eines Clustermitglieds auf den Cluster festlegen.

Sobald das CI als manueller Cluster definiert ist, zeigt die Berechnung der Auswirkung das Ausmaß eines Ausfalls für die untergeordneten CIs an. Bei der Berechnung der Auswirkung werden Faktoren wie Auswirkungsregeln und CI-Beziehungen verwendet, um den Schweregrad einer generierten Warnung zu berechnen. Auswirkungsregeln, die zur Berechnung der Auswirkung verwendet werden, schätzen das Ausmaß oder den Schweregrad eines Ausfalls basierend auf den betroffenen CIs und bestimmen, wie die Auswirkung für über- oder untergeordnete Entitäten gilt, die Teil eines Anwendungsservice sind.

Das Ausmaß eines Ausfalls kann 100 % Ausfall, 60 % betroffen, 40 % beeinträchtigt oder 20 % beeinträchtigt sein.

Redundanz wird in Auswirkungsregeln definiert. Sie können beispielsweise definieren, dass das übergeordnete CI kritisch ist, wenn mindestens zwei untergeordnete CIs kritisch sind. Die Auswirkung von untergeordneten auf übergeordnete CIs beträgt nicht immer 100 %. Wenn die CIs aller drei untergeordneten Elemente betroffen sind, reduziert sich die Auswirkung auf 100 %.

In einer Servicezuordnung können Sie ein bestimmtes CI oder eine generische CI-Klasse in einem manuellen Service als manuell definiertes Cluster konfigurieren oder ändern. Bei der Konfiguration als generische CI-Klasse werden alle CIs der ausgewählten Klasse in diesem Service gleich konfiguriert.

Zugehörige Informationen

Warnungsauswirkungsberechnung

Konfigurieren Sie einen manuellen Cluster

Stellen Sie Redundanzfähigkeiten eines gesamten Clusters bereit, falls ein oder mehrere CIs in diesem Cluster ausfallen. Durch Anzeigen der relativen Auswirkungen eines Clustermitglieds auf die Clusterinformationen können Sie die Quelle von Warnungen besser verstehen und Korrekturmaßnahmen ergreifen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

In einem manuellen Service, der nicht automatisch erkannt wurde, können Sie ein bestimmtes CI oder eine generische CI-Klasse manuell unter einem logischen Cluster gruppieren. Die relative Auswirkung eines Clustermitglieds auf den Cluster kann in der Auswirkungsstruktur konfiguriert werden.

Weitere Informationen finden Sie unter Warnungsauswirkungsberechnung.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Manuelle Cluster**.
2. Wählen Sie **Neu**.
3. Wählen Sie im Abschnitt **„Service mit diesem manuellen Cluster auswählen“** einen Anwendungsservice aus, der den neuen manuellen Cluster enthalten soll, basierend auf einem bestimmten CI oder einer allgemeinen CI-Klasse.
   Die Clusternummer wird automatisch generiert und im Feld **Nummer** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie das Symbol „Nachschlagen mit Liste“ ( ) im Feld **Service**.

b. Wählen Sie in der Tabelle „CMDB-CI-Service“ [cmdb_ci_service_discovered] einen manuell erstellten Service aus.
Informationen zum Definieren eines neuen Anwendungsservice finden Sie unter Erstellen Sie manuell einen Anwendungsservice in Ereignismanagement.

c. Wahlweise: Zeigen Sie eine Vorschau des Datensatzes an, indem Sie das Symbol Vorschau auf diesen Datensatz ( ) wählen.

4. Wählen Sie im Abschnitt **„Bestimmtes CI oder generische CI-Klasse auswählen“** im Feld **Definiert als** aus, ob der manuelle Cluster als bestimmtes CI eines manuellen Clusters oder als generische CI-Klasse eines manuellen Clusters definiert werden soll, die auf alle CIs angewendet wird dieser Klasse.
   - Spezifisches CI: Wählen Sie im Feld **Konfigurationselement** das Symbol „Nachschlagen mit Liste“ (“), und wählen Sie dann das Konfigurationselement aus.
   - Generische CI-Klasse: Wählen Sie im Feld **Klasse des Konfigurationselements** die Klasse des Konfigurationselements aus.
5. **Geben Sie im Abschnitt Eine Beschreibung** angeben entweder eine Beschreibung im Feld **Beschreibung** an, oder lassen Sie das Feld leer, um eine automatisch generierte Beschreibung aufzunehmen, wenn Sie **Speichern** oder **Absenden**wählen.

   Das Feld **Beschreibung** wird automatisch aktualisiert, wenn Sie **Speichern** oder **Absenden**wählen. Die automatisch generierte Beschreibung besteht aus dem Namen des Configuration Item und dem Servicenamen. Beispiel: `CI`<Alert Processing> in Betrieb<linuxApplService> (*** automatisch generiert ***) .

   Um eine automatische Aktualisierung des Beschreibungsfelds zu verhindern und Ihre Änderungen beizubehalten, löschen Sie das Suffix (*** automatisch generiert ***), das als Teil der Beschreibung angezeigt wird.
6. Aktivieren Sie den Cluster, indem Sie das Kontrollkästchen **Aktivieren** aktivieren.
7. Wählen Sie **Absenden**.

Ergebnisse
Der manuelle Cluster wird in der Tabelle „EM Impact Manueller Cluster“ [em_impact_manual_cluster] gespeichert. Die Berechnung der Auswirkung wird automatisch neu berechnet.

Zugehörige Informationen

Konfiguration von CIs in einem manuellen Service als manueller Cluster

Ändern Sie einen manuellen Cluster

Ändern Sie einen vorhandenen manuellen Cluster, indem Sie den Service, das spezifische CI, die generische CI-Klasse oder die Beschreibung ändern, falls eine falsche Erstkonfiguration, Änderungen im Netzwerk oder andere Probleme vorliegen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Manuelle Cluster**.
2. Wählen Sie in der Liste einen manuellen Cluster aus.
3. Ändern Sie den Service, der das manuelle Cluster enthält, indem Sie im Abschnitt **„Service auswählen, der diesen manuellen Cluster enthält“** einen anderen auswählen.
   Die Clusternummer wird im Feld **Nummer** angezeigt.
   a. Wählen Sie das Symbol „Nachschlagen mit Liste“ ( ) im Feld **Service**.
   b. Wählen Sie in der Tabelle „CMDB-CI-Service“ [cmdb_ci_service_discovered] einen manuell erstellten Service aus.
   c. Wahlweise: Zeigen Sie eine Vorschau des Datensatzes an, indem Sie das Symbol Vorschau auf diesen Datensatz ( ) wählen.
4. Ändern Sie im Abschnitt **„Bestimmtes CI oder generische CI-Klasse auswählen“** im Feld **Definiert als** den manuellen Cluster entweder als spezifisches CI eines manuellen Clusters oder als generische CI-Klasse eines manuellen Clusters, die auf alle CIs dieser Klasse angewendet wird .
   - Spezifisches CI: Wählen Sie im Feld **Konfigurationselement** das Symbol „Nachschlagen mit Liste“ (“), und wählen Sie dann das Konfigurationselement aus.
   - Generische CI-Klasse: Wählen Sie im Feld **Klasse des Konfigurationselements** die Klasse des Konfigurationselements aus.
5. Wahlweise: Ändern Sie im Abschnitt **„Beschreibung bereitstellen** “ die Beschreibung im Feld **Beschreibung**.

   (Optional) Das Feld **Beschreibung** wird automatisch aktualisiert, wenn Sie **Speichern** oder **Absenden**wählen. Die automatisch generierte Beschreibung besteht aus dem Namen des Configuration Item und dem Servicenamen. Beispiel: `CI`<Alert Processing> in Betrieb<linuxApplService> (*** automatisch generiert ***) .

   Um eine automatische Aktualisierung des Beschreibungsfelds zu verhindern und Ihre Änderungen beizubehalten, löschen Sie das Suffix (*** automatisch generiert ***), das als Teil der Beschreibung angezeigt wird.
6. Aktivieren oder deaktivieren Sie den Cluster, indem Sie das Kontrollkästchen **Aktivieren** aktivieren oder deaktivieren.
7. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

Ergebnisse

Der manuelle Cluster wird in der Tabelle „EM Impact Manueller Cluster“ [em_impact_manual_cluster] gespeichert. Die Berechnung der Auswirkung wird automatisch neu berechnet.

Zugehörige Informationen

Konfiguration von CIs in einem manuellen Service als manueller Cluster

Erstellen Sie eine Warnungsabfrage

Eine Warnungsabfrage ist eine Reihe von Warnungen, die bestimmte Kriterien für einen bestimmten Service erfüllen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Navigieren zu **Ereignismanagement** > **Administration** > **Ereignismanagement-Eigenschaften** und stellen Sie sicher, dass die Eigenschaft **Unterstützung für Warnungsabfragen aktivieren** (*evt_mgmt.impact_calulation.alert_group_support*) auf **Ja**festgelegt ist.

Erforderliche Rolle: evt_mgmt_admin oder evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Der Hauptgrund für die Verwendung von Warnungsabfragen ist eine Modellierungslösung, die auf Daten basiert, die in der Warnung selbst enthalten sind, als Alternative zur Verwendung von erkannten, Anwendungsservices oder technischen Services.
Erstellen Sie eine Warnungsabfrage, um ähnliche Warnungen zu kombinieren, die die spezifischen Kriterien erfüllen.

In diesem Video erfahren Sie mehr über die Grundlagen Ereignismanagement von , einschließlich Warnungsabfragen:

Erste Schritte mit Ereignismanagement

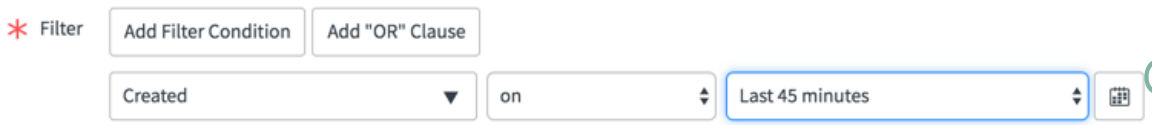
Prozedur

1. Navigieren zu **Ereignismanagement** > **Services** > **Warnungsabfragen**.
2. Wählen Sie **Neu**.
3. Im Formular **„Warnungsabfrage** “in den Feldern.

   Eine Beschreibung der Feldwerte finden Sie unter Formular „Warnungsabfrage“..

   Hinweis: Im Feld **Filter**:

   - Beziehen Sie bei der Definition eines Warnungsabfragefilters nur Felder ein, die in der Tabelle „Warnungsverläufe“ [em_alert_history] angezeigt werden. Die Berechnung der Auswirkung basiert auf Warnungsverlaufsdaten, und Felder wie „Gesamtanzahl der Ereignisse“, „Priorität“ und „Prioritätsgruppe“ werden nicht in die Tabelle „Warnungsverläufe“ [em_alert_history] kopiert.
   - Geben Sie keine dynamische Zeitbedingung an. Geben Sie im Filter beispielsweise nicht die Bedingung `Erstellt` der `Letzte 45 Minuten` an, da die Berechnung der Auswirkung durch eine Änderung der Warnung oder Warnungsabfrage ausgelöst wird. Für die dynamische Zeitbedingung hat sich jedoch keine dieser Bedingungen geändert.

   - Einige Filter können die Auswirkungsberechnung verlangsamen. Um dieses Problem zu lösen, passen Sie Ihre Warnungsabfrage an, indem Sie einen entsprechenden Index hinzufügen (siehe Indexvorschläge für langsame Abfragen) .
4. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Erstellen Sie manuell eine Warnmeldungsgruppe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicegruppe erstellen

Erstellen Sie Servicegruppen, um ähnliche Services zu kombinieren. Organisieren Sie Services nach Gruppen, um Aktionen für mehrere Services gleichzeitig auszuführen und den Benutzerzugriff auf Services zu steuern.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Servicegruppen werden im Dashboard Service Operations-Arbeitsbereich angezeigt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Servicegruppen**.
2. Klicken Sie auf **Neu**.
3. Im Feld **Name** geben Sie den Namen der neuen Servicegruppe ein.
4. Wahlweise: Um die neue Gruppe in eine andere Gruppe einzubetten, geben Sie den Namen der anderen Gruppe im Feld **Übergeordnete Gruppe** ein.
   Benutzer mit Zugriff auf eine übergeordnete Servicegruppe haben automatisch Zugriff auf alle untergeordneten Gruppen.
5. Klicken Sie auf **Absenden**.

Zugehörige Informationen

Einer Servicegruppe eine Rolle zuweisen

Gruppen-Anwendungsservices

Einer Servicegruppe eine Rolle zuweisen

Weisen Sie der Anwendungsservicegruppe die Rolle Ereignismanagement zu, um sicherzustellen, dass Gruppenmitglieder Warnungen verwalten und darauf reagieren können.

Vorbereitungen
Konfigurieren Sie eine Servicegruppe, damit Benutzer Anwendungsservices, Anwendungsservices oder Warnmeldungsgruppen verwalten können.
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Zuständigkeiten der Servicegruppe**.
2. Klicken Sie auf **Neu**.
3. Wählen Sie im Feld **Anwendungsservicegruppe** den Namen der Servicegruppe aus.
4. Wählen Sie im Feld **Rolle** eine Ereignismanagement-Rolle aus:
   - evt_mgmt_admin
   - evt_mgmt_integration
   - evt_mgmt_operator
   - evt_mgmt_user
5. Klicken Sie auf **Absenden**.
6. Um Benutzer zu finden, die der Rolle zugewiesen sind, navigieren Sie zu **Anwenderadministration** > **Anwender** > **Rollen** und suchen Sie nach der Rolle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Mit Ereignismanagement installierte Rollen

Service-Mapping aktivieren und für die Erkennung von oben nach unten konfigurieren

Eine Discovery von oben nach unten bietet eine Liste von CIs und ihren Beziehungen. Diese Informationen sind nützlich für die Verwaltung von Softwarediensten und Hardwareproblemen, die mit Warnungen verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
In Ereignismanagement werden Service-Mapping-Beziehungen in Warnungen angezeigt. Sie können das zugehörige CI und andere Informationen im Dashboard Ereignismanagement anzeigen. Die Zuordnungsbeziehungen werden in einer Servicezuordnung mit der generierten Warnung, allen an die Warnung gebundenen CIs und allen zugehörigen CIs angezeigt.

Prozedur

Verwenden Sie Service-Mapping, um Top Down-Discovery-Informationen abzurufen. Service-Mapping, das eng mit Ereignismanagementverwandt ist, bietet Tools zum Erkennen der Beziehungen zwischen Netzwerk, Hardware, Software, Speicher und anderen Geräten.

Zugehörige Informationen

Service-Mapping

Service-Mapping anfordern

E-Mail-Benachrichtigung bei Änderung des Anwendungsservice-Schweregrads konfigurieren

Konfigurieren Sie eine E-Mail-Benachrichtigung, um Benutzer über Änderungen des Anwendungsservice-Schweregrads zu informieren.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Konfigurieren Sie eine E-Mail-Benachrichtigung, um Benutzer über Änderungen des Anwendungsservice-Schweregrads zu informieren. Dabei können Sie einstellen, wann die Benachrichtigung gesendet wird, wer sie empfängt und was sie enthält.

Prozedur

1. Navigieren zu **Alle** > **Systemeigenschaften** > **E-Mail-Eigenschaften**.
2. Wählen Sie im Abschnitt **Konfiguration für ausgehende E-Mails** unter **E-Mail-Versand aktiviert** die Option **Ja** aus, um das Senden von Schweregradinformationen per E-Mail zu ermöglichen.
3. Klicken Sie auf **Speichern**.
4. Navigieren zu **Systembenachrichtigung** > **E-Mail** > **Benachrichtigungen**.
5. Klicken Sie auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Geben Sie im Formular **E-Mail-Benachrichtigungsaktionen** diese Werte an.

Feld	Wert
Name	Geben Sie einen beschreibenden Namen ein, z. B. *Application Service severity change*.
Tabelle	Wählen Sie den erforderlichen Servicetyp und die entsprechende Tabelle aus: Warnungsgruppe, erkannter Service, technischer Service oder Anwendungsservice.
Aktiv	Aktivieren Sie die Checkbox, um die E-Mail-Benachrichtigung zu aktivieren.

b. Klicken Sie auf die Registerkarte **Empfänger**.
Im Bereich **Benutzer** suchen und wählen Sie den erforderlichen Benutzer (der Benutzer benötigt keine Systemadministrator-Anmeldeinformationen). Wiederholen Sie diesen Schritt für alle Benutzer, die für den Empfang dieser Benachrichtigung erforderlich sind.

c. Klicken Sie auf die Registerkarte **Wann senden**, suchen Sie im **Feld Auswahlfeld** nach *Severity*, und wählen Sie den Eintrag aus.

d. Klicken Sie auf die Registerkarte **Was darin enthalten ist**, und geben Sie im Feld **Betreff** einen aussagekräftigen Text ein, der dem Empfänger der E-Mail-Benachrichtigung klar macht, was der Inhalt der E-Mail ist.

e. Erstellen Sie im Nachrichtenbereich **Nachricht-HTML** mithilfe der Funktionen **Variablen auswählen** die Bedingungen, unter denen die E-Mail-Benachrichtigung gesendet werden soll.
Konfigurieren Sie beispielsweise diese Variablen, um den Schweregrad zu ändern:

```
severity changed
```

```
Severity: ${severity}
```

```
on application service
```

```
Name: ${name}
```

6. Klicken Sie auf **Absenden**.

Kontextbezogene Farben und Symbole konfigurieren

Verwenden Sie das Formular **Kontextbezogene Farben und Symbole**, um Farbe, Text und Symbole so zu konfigurieren, dass verschiedene Standardkontexte oder benutzerdefinierte Kontexte vorhanden sind, die durch eine Kontext-ID identifiziert werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können die Farben oder Symbole von Elementen im Formular **Kontextbezogene Farben und Symbole** anpassen, um die angezeigten Farben oder Symbole von Schweregraden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in zugehörigen Ereignismanagement-Bildschirmen zu beeinflussen, entweder wenn der Eingabehilfemodus aktiviert oder deaktiviert ist. Weitere Informationen zur Barrierefreiheit finden Sie unter Barrierefreiheitsfunktionen .

In jedem Farbauswahlfeld haben Sie die Möglichkeit, den Wert der Farbe als eines der folgenden CSS-Formate (Cascading Style Sheet) einzugeben, die bestimmen, wie HTML-Elemente angezeigt werden sollen:

- Name: vordefinierte Farbnamen, z. B. Rot, Grün, Oliv, Blau, Dunkelblau oder Hellblau
- RGB-Dezimalzahl: RGB(102, 153, 204)
- RGB-Hex-Wert: #223344

Auf den folgenden Websites finden Sie Informationen zu CSS-Farbdeklarationen (einschließlich Hex- oder RGB-Schreibweise):

- HTML-Farben (W3CSchools) für weitere Informationen zu Hex-Wert und RGB Schreibweise.
- HTML-Farbnamen (W3CSchools) für gültige Farbnamen.

Die mit der Basisinstanz bereitgestellten Kontext-IDs sind:

- information_severity
- warning_severity
- minor_severity
- major_severity
- critical_severity
- topology_connection

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Kontextbezogene Farben und Symbole**.
2. Klicken Sie auf **Neu** oder auf eine vorhandene Konfiguration.
3. Konfigurieren Sie die folgenden Felder.

Element	Beschreibung
Kontextdetails	
Kontext-ID	Geben Sie eine eindeutige ID für den Kontext ein, z. B. „clear_severity“.
Kontextname	Lesbarer Name für den Kontext. Dieser Text kann von Sprachausgabeprogrammen vorgelesen werden.
Batch	Batch, zu dem dieser Kontext gehört.
Beschreibung	Beschreibung der Verwendungen für den Kontext.
Farben	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Element	Beschreibung
Hinweis: Für jeden Eintrag in den Farbfeldern wird nach der Eingabe eines Farbcodes ein Block rechts vom Feld mit der angegebenen Farbe angezeigt. Die Verwendung ungültiger Farbcodes löst eine entsprechende Fehlermeldung aus.	
CSS-Farbe	Der entsprechende CSS-Farbcode für den Kontextfarbnamen.
CSS-Farbe bei Interaktion	CSS-Farbcode, der beim Daraufzeigen oder Fokussieren angezeigt wird.
Verfügbare CSS-Farbe	Verfügbarer CSS-Farbcode, der anzeigt, wenn der Eingabehilfemodus aktiviert ist.
Verfügbare CSS-Farbe bei Interaktion	Eingabehilfe-CSS-Farbcode, der beim Daraufzeigen oder Fokussieren angezeigt wird.
Symbole	
Symbol	Symbol, das anzeigt, ob der Kontext ein Symbol enthält.
Eingabehilfesymbol	Symbol, das anzeigt wird, wenn der Kontext ein Symbol enthält und wenn der Eingabehilfemodus aktiviert ist. Um ein eigenes Symbol hinzuzufügen oder eine Liste der verfügbaren Symbole anzuzeigen, rufen Sie Ein oder mehrere Bilder hochladen auf .

4. Klicken Sie auf **Absenden**.

Lizenznutzung für Event Management anzeigen

Ereignismanagement wird basierend auf der Anzahl der CIs lizenziert, die im letzten Jahr an Warnungen gebunden wurden. Für Warnungen, die nicht an CIs gebunden sind, berechnet das System die Anzahl der Knoten (Server), die im letzten Jahr Ereignisse an die Instanz direkt oder über ein Überwachungstool einer Drittpartei senden konnten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin oder evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird
Der Auftrag **„Ereignismanagement – Knotenanzahlspeicher“** berechnet die Anzahl der eindeutigen Knoten, die Ereignisinformationen entweder direkt oder über Drittparteien an Ereignismanagement senden und im letzten Jahr für die Lizenzierung berechtigt waren. Die Informationen dieses Auftrags werden in der Tabelle Lizenznutzung [em_unique_nodes] gespeichert, um für alle Benutzer sichtbar zu sein. An Warnungen gebundene CIs werden bei der Lizenzierung berücksichtigt. Wenn keine CIs vorhanden sind, die an Warnungen gebunden sind, wird das Event-Knotenfeld verwendet. Ein Knoten ist ein Verweis auf einen Server, nicht auf die Instanzen der darauf befindlichen Software. Ihre Knotenanzahl hängt von der Infrastruktur (z. B. Server) ab, die Ereignisse sendet.

Prozedur

Navigieren zu **Alle** > **Ereignismanagement** > **Berichterstellung** > **Lizenznutzung**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Tabelle wird automatisch basierend auf den Warnungen im System gefüllt. Der Anwender hat keine Berechtigung zum Bearbeiten der Tabelle. Wird verwendet, um die Nutzung der Lizenzierung Ereignismanagement zu berechnen.

Spalte	Beschreibung
CMDB CI	Das CI, das an die Warnung gebunden ist, die aus dem Event generiert wird. Wenn für dieses Feld ein Wert vorhanden ist, ist das **Knotenfeld** leer.
Knoten	Der Zeichenfolgenwert des **Knotenfelds** des Events. Wenn für dieses Feld ein Wert vorhanden ist, ist das Feld **CMDB CI** leer.
Typ	Einer der folgenden Werte: • Unbekannt – Ein CI ist nicht an die generierte Warnung gebunden. • Server – Die Quelle des Events war ein Server. • PaaS – Die Quelle des Events war „Platform as a Service“.
Ist lizenzierbar	Einer der folgenden Werte: • True – Das aufgelistete Event wird auf die Lizenznutzung angerechnet. • False – Das aufgelistete Event wird nicht auf die Lizenznutzung angerechnet

Ereignismanagement verwenden

Als Ereignismanagement Operator haben Sie die Aufgabe, Warnungen zu finden und zu analysieren sowie Aktionen zur Lösung des zugrunde liegenden Problems zu ergreifen.

Dieser Leitfaden kann Sie regelmäßig unterstützen.

Warnungsinformationen anzeigen

Zeigen Sie eine Liste aller Warnungen für Anwendungsservices an, und verwalten Sie dann einzelne Warnungen nach Bedarf.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Mehrere zugehörige Events können zu einer einzigen Warnung korrelieren. Ereignismanagement erstellt Warnungen nur, wenn mindestens ein Event die Bedingungen erfüllt, die in Eventregeln, Warnungsaktionsregeln und Warnungskonfigurationseinstellungen definiert sind.

Beim Aktualisieren einer Warnung werden von leeren Feldwerten keine Werte überschrieben, die vom Ereignis der Warnung übernommen wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Klicken Sie auf die Warnungsnummer, um eine Warnung anzuzeigen oder zu verwalten.
3. Überprüfen Sie die Informationen im Warnungsformular.
   Sie können auf die Registerkarten im Formular klicken, um weitere Informationen zu erhalten.
   - Um Informationen zur Fluktuation anzuzeigen, klicken Sie auf die Registerkarte **Fluktuierend**.
   - Um den Warnungsverlauf anzuzeigen, klicken Sie auf die Registerkarte **Verlauf**.

Warnungsformular

Feld	Beschreibung
Nummer	Wenn eine Warnung als Ergebnis des Events erstellt wurde, enthält dieses Feld die eindeutige ID, die von Ereignismanagement zur Identifizieren der Warnung generiert wird.
Quelle	Event-Überwachungssoftware, von der das Event generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
Knoten	Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, der/die dem Event zugeordnet ist, z. B. IBM-ASSET. Maximale Länge: 100 Zeichen
Typ	Der Metriktyp, auf den sich das Event bezieht, z. B. Datenträger oder CPU, der zur Identifizierung eines Event-Datensatzes verwendet wird, aus dem Warnungen erstellt werden. Maximale Länge: 100 Zeichen
Ressource	Knotenressource, die für das Event relevant ist. Beispiel: Datenträger C, CPU-1, der Name eines Prozesses oder Services. Maximale Länge: 100 Zeichen
Konfigurationselement	JSON-Zeichenfolge, die ein Konfigurationselement darstellt. Beispiel: `{"name":"SAP ORA01","type":"Oracle"}` ({"Name": "SAP ORA01", "Typ": "Oracle"}). Der CI-Bezeichner, der das Event generiert hat, wird im Feld **Zusätzliche Informationen** angezeigt. Maximale Länge: 1.000 Zeichen Hinweis: Referenz-Popups und Click-throughs sind für schreibgeschützte Felder standardmäßig ausgeblendet. Für **Konfigurationselement** und andere schreibgeschützte Felder können Sie die Einstellung „Schreibgeschützt“ optional ändern. Weitere Informationen finden Sie unter Popups für schreibgeschützte Felder konfigurieren . Klicken Sie auf das , um die Warnung in der Abhängigkeitsansicht zu öffnen.
Aufgabe	Die entsprechende Aufgabe für die Warnung, z. B. Incident, Change oder Problem.
Metrikname	Eindeutiger Name, der beschreibt, welche Metrikdaten erfasst werden.
Beschreibung	Eine Beschreibung der Warnung.
Nachrichtenschlüssel	Eindeutiger Event-Bezeichner zur Identifizierung mehrerer Events, die sich auf dieselbe Warnung beziehen. Wenn dieser Wert leer ist, wird er aus den Feldwerten **Quelle**, **Knoten**, **Typ**, **Ressource** und **Metrikname** generiert. Maximale Länge: 1.024 Zeichen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schweregrad	Der Schweregrad des Events. Der Wert für dieses Feld wird aus dem Event kopiert, es sei denn, das Event schließt die Warnung. In diesem Fall wird der vorherige Schweregrad für die Berichterstellung beibehalten. ◦ **Kritisch**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. ◦ **Schwerwiegend**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten. ◦ **Geringfügig**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. ◦ **Warnung**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. ◦ **OK**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig. ◦ **Löschen**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
Status	Der Status der Warnung. ◦ **Öffnen**: Die Warnung erfordert eine Benutzeraktion. ◦ **Erneut öffnen**: Die zuvor geschlossene Warnung erfordert eine Benutzeraktion. ◦ **Flatternd**: Nachdem die Warnung geschlossen wurde, gehen sehr viele identische Events aus derselben Quelle ein, die zu zahlreichen erneuten Öffnungen der Warnung führen. Benutzeraktion ist erforderlich. ◦ **Geschlossen**: Die Warnung ist geschlossen, und es ist keine weitere Benutzeraktion erforderlich.
Bestätigt	Wählen Sie **Bestätigt** aus, um anzugeben, dass ein Benutzer die Warnung bestätigt hat.
Reserviert	Ein Kontrollkästchen, mit dem angezeigt wird, ob sich die von der Warnung betroffene Ressource in Wartung befindet.
Aktualisiert	Der Zeitpunkt der letzten Aktualisierung der Informationen zur Warnung.
Übergeordnet	◦ Wenn dieses Feld leer ist, können Sie eine Warnungsnummer angeben. Die aktuelle Warnung wird zu einer sekundären Warnung zu dieser übergeordneten Warnung. ◦ Wenn eine Warnungsnummer angezeigt wird, ist die aktuelle Warnung bereits eine sekundäre Warnung zu dieser aktuellen Warnung, der übergeordneten Warnung.
Feedback	Dieses Feld wird in Warnungsformularen nur angezeigt, wenn die zu ändernde Warnung eine übergeordnete Warnung ist. Ihre Antwort bietet Feedback zur Genauigkeit und Nützlichkeit der Gruppe. Mögliche Werte sind: ◦ Kein – Es wurde kein Wert ausgewählt. ◦ Kein Feedback – Für diese Warnung gibt es kein Feedback.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Ja – die Warnungsgruppe ist genau und nützlich. ◦ Nein – die Warnungsgruppe ist nicht genau und nützlich. **Hinweis:** Derzeit ist die Feedback-Option verfügbar, löst jedoch nach der Protokollierung keine weiteren Aktionen aus.
Wissensartikel	Der der Warnung zugeordnete Wissensartikel (sofern vorhanden).
Gesamtanzahl der Events	Der Zähler wird jedes Mal erhöht, wenn ein Event an die Warnung gebunden wird. Der Zählwert wird beibehalten, auch nachdem das tatsächliche Event gelöscht wurde. Primäre Warnungen (virtuelle Warnungen) werden basierend auf ihren sekundären Warnungen aktualisiert. Die tatsächliche Anzahl der Events, die sich auf die Warnung auswirken, wird angezeigt. **Hinweis:** Erstellen Sie keine Warnungsgruppe basierend auf der Event-Anzahl. Wenn eine Warnungsgruppe auf der Event-Anzahl basiert, wird die Auswirkung der Gruppe nicht ordnungsgemäß berechnet, da das Feld „Event-Anzahl“ nicht für die Auswirkungsberechnung in die Tabelle „em_alert_history“ kopiert wird.
Quellinstanz	Der Name des Computers oder der Software, die/der das Event generiert hat. Beispiel: SolarWinds auf 10.22.33.44.
Benutzername und Rolle	Der Benutzer und die Rolle der Person, die die neuesten Warnungsaktualisierungen vorgenommen hat.
Bestätigt	Das Kontrollkästchen **Bestätigt** nach dem neuesten Update mit den meisten Warnungen. ◦ *True*: **Bestätigt** ist ausgewählt. ◦ *False*: Das Kontrollkästchen **Bestätigt** wird deaktiviert.
Abschnitt **Korrelierte Warnungen**	Die sekundären Warnungen, die mit dieser Warnung korrelieren, wobei diese Warnung die primäre Warnung ist. Weitere Informationen finden Sie unter Regelbasierte Warnungsgruppierung.
Abschnitt **Primäre Warnungen**	Die primäre Warnung, die mit dieser Warnung korreliert, wobei diese Warnung eine sekundäre Warnung ist. Weitere Informationen finden Sie unter Regelbasierte Warnungsgruppierung.

Zusätzliche Registerkarten.

Feld	Beschreibung
Registerkarte „Betroffene Services“	
Betroffene Services	Die betroffenen Services, die zu dieser Warnung gehören, werden aufgelistet. Weitere Informationen finden Sie unter Anzeigen der Auswirkungsstruktur.
Registerkarte „Flatternd“	
Anzahl der Fluktuationen	Die Anzahl, wie oft es innerhalb des Flatterintervalls seit der Startzeit im **Flattern – Startfenster** zu Flatterbewegungen bei

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Warnungen gekommen ist, d. h. zwischen einem geschlossenen und einem nicht geschlossenen Zustand gewechselt wurde.
Flattern – Startfenster	Die anfängliche Startzeit zur Messung der Fluktuationsereignisse.
Flattern – Zeit des letzten Update	Das letzte Vorkommen der Fluktuation. Dies ist die Verarbeitungszeit der Plattform, nicht die Zeit des Quellsystems.
Flattern – letzter Status	Der Status der Warnung vor dem Übergang in den Status „Fluktuierend“.
Registerkarte „Verlauf“	
Generierungszeit des ersten Events	Die Zeit, zu der das Event, von dem die Warnung zuerst generiert wurde, aufgetreten ist. Dies ist die Verarbeitungszeit der Plattform, nicht die Zeit des Quellsystems.
Generierungszeit des letzten Events	Das letzte Mal, dass das mit der Warnung verknüpfte Event aufgetreten ist. Dies ist die Verarbeitungszeit der Plattform, nicht die Zeit des Quellsystems.
Erstellt	Uhrzeit, zu der die Warnung erstellt wurde.
Arbeitsnotizen	Die zusätzlichen Notizen zur Warnung.
Registerkarte Aktivitäten	
Aktivität	Ein Datensatz der durchgeführten Arbeit. Der Text hat einen Datums- und Zeitstempel.
Registerkarte „Weitere Informationen“	
Prioritätsaufgliederung	Zeigt die Berechnung der Warnungsprioritätspunktzahl an.
Zusätzliche Informationen	Eine JSON-Zeichenfolge, die weitere Informationen zum Event enthält. Die JSON-Daten werden nur für Zeichenfolgenwerte unterstützt. Andere Werttypen werden nicht unterstützt. Sie müssen Zahlen in Zeichenfolgenwerte konvertieren, indem Sie sie in doppelte Anführungszeichen setzen. Beispielsweise wird dieser Wert nicht unterstützt: {"CPU":100}, während dieser Wert unterstützt wird: {"CPU":"100"}. Ein weiteres Beispiel für eine gültige JSON-Zeichenfolge ist: {"evtComponent":"Microsoft-Windows-WindowsUpdateClient","evtMessage":"Installation Failure: Windows failed. Error 0x80070490"}. Diese Informationen können für die Drittanbieterintegration oder andere Nachwarnungsverarbeitungen verwendet werden. Werte im Feld **Zusätzliche Informationen** eines Events, die nicht im JSON-Schlüssel-/Wert-Format vorliegen, werden auf das JSON-Schlüssel-/Wert-Format normalisiert, wenn das Event verarbeitet wird. Angenommen, der folgende Nur-Text befindet sich im Feld **Zusätzliche Informationen**: "Connection instance is successful" ("Verbindungsinstanz ist erfolgreich"). Wenn das Event verarbeitet wird, wird dieser Nur-Text zu einer JSON-Zeichenfolge und ist in einer Warnung möglicherweise nicht hilfreich. In der resultierenden Warnung steht diese Zeichenfolge im Feld **Zusätzliche Informationen** im JSON-Schlüssel/Wert-Format, das die Daten enthält: {“additional_content”: “Connection instance is successful"} ({"zusätzlicher_Inhalt": "Verbindungsinstanz ist erfolgreich"}).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Sie können auf eine Warnung wie folgt reagieren:

Optionen zur Reaktion auf Warnungen

Option	Beschreibung
Absenden	Speichern Sie die am Formular vorgenommenen Änderungen, und kehren Sie zur Liste der **Warnungen** zurück.
Bestätigen Sie die Warnung.	Klicken Sie auf **Bestätigen**. Wenn die Warnung erneut geöffnet wird, wird diese Schaltfläche erneut angezeigt, damit Sie die Warnung erneut bestätigen können.
Erstellen eines Incidents.	Klicken Sie auf **Incident erstellen**. Weitere Informationen finden Sie unter Incident oder Security Incident aus einer Warnung erstellen.
Wenn Security Incident Response aktiviert ist, erstellen Sie eine Reaktion auf einen Security Incident.	Klicken Sie auf **Security Incident erstellen**.
Legen Sie fest, dass sich die Warnung in Wartung befindet.	Klicken Sie auf das Kontrollkästchen **Wartung**. Weitere Informationen finden Sie unter Alle Warnungen nach Wartungsstatus anzeigen.
Schließen Sie die Warnung.	Klicken Sie auf **Schließen**. Weitere Informationen finden Sie unter Warnungen schließen.

Zugehörige Informationen

Aus Events und Warnungen erstellte Security Incidents

Prioritätsgruppe

Zur besseren Selektierung und Fokussierung werden Warnungen mit einer höheren Priorität an den Anfang der Warnungsliste gesetzt. Diese Platzierung macht Sie auf die Warnungen aufmerksam, die eine höhere Priorität als andere Warnungen haben.

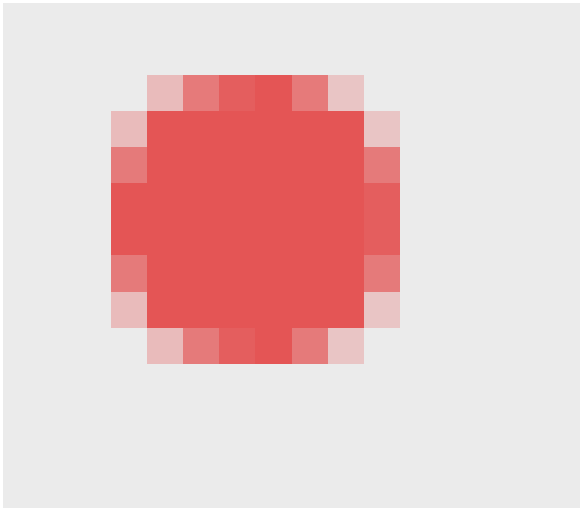
Die Prioritätsgruppe gibt an, welche Warnungen zuerst Aufmerksamkeit erfordern. Die Priorität wird für alle offenen Warnungen berechnet, woraufhin diese einer von vier Prioritätskategorien zugeordnet werden.

Schwellenwerte
Schwellenwerte für die berechnete Priorität werden verwendet, um zu bestimmen, welcher Kategorie die Warnung zugeordnet wird. Warnungen mit einer Priorität, die über dem Wert der Eigenschaft *evt_mgmt.top_priority_group_threshold* liegt, werden als **Dringend**kategorisiert, was die höchste Priorität ist. Der Standardwert für den Schwellenwert ist 1M.

Prioritätsgruppenkategorien
Die Prioritätsgruppen, in die Warnungen fallen, sind in der folgenden Tabelle aufgelistet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

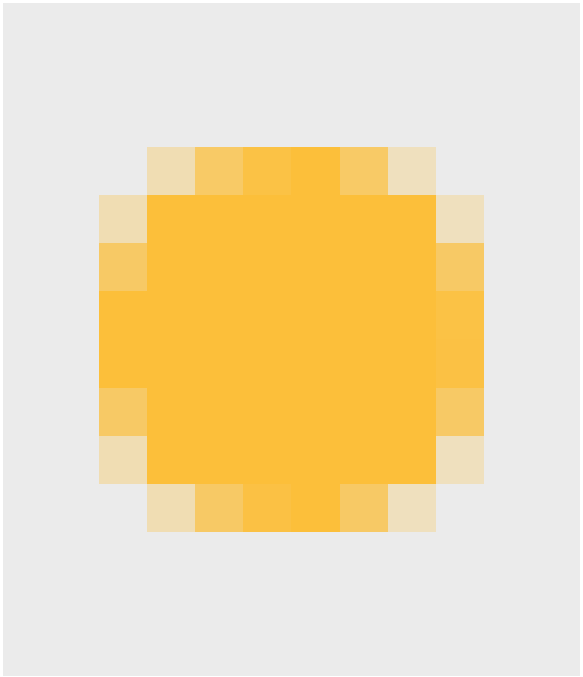
Warnungsprioritätsgruppen

Prioritätsgruppe	Symbol
Dringend	
Hoch	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsprioritätsgruppen (Fortsetzung)

Prioritätsgruppe	Symbol
Mittel	
Niedrig	

Automatische Übersetzung

Der Wert der Warnungsprioritätsgruppe ist aussagekräftiger als der Warnungsschweregrad an sich. Beispiel: Eine Warnung mit dem Schweregrad „Schwerwiegend“ muss möglicherweise nicht vor einer Warnung gelöst werden, deren Priorität „Kritisch“ ist. Der kombinierte Gruppenprioritätswert berücksichtigt die Gewichtung jedes Faktors, sodass Sie besser wissen, welche Warnung zuerst bearbeitet werden muss.

Die Warnungsprioritätsgruppe ist in Warnungslisten auf der Seite „Dashboard“, „Alert Intelligence“ und „Alle Warnungen“ verfügbar. Beispielsweise wird in der Liste **Alle Warnungen** die Warnungsprioritätsgruppe wie in der folgenden Abbildung dargestellt angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Number	Group	Severity	Priority group	Priority
Demo0001011		Warning	Low	100
Demo0001006		Warning	Moderate	100
Alert0010004		Minor	High	200

Auslöser, die eine Neuberechnung auslösen

Änderungen an offenen Warnungen lösen die Neuberechnung der Priorität aus. Anschließend wird die Warnung erneut in die entsprechende Prioritätsgruppe eingeteilt. Geschlossene Warnungen werden bei der Berechnung der Warnungsprioritätsgruppe nicht berücksichtigt.

Zugehörige Informationen

Warnungspriorität

Informationen zur Warnungsausführung

Warnungsausführungsinformationen bieten einen Verweis auf die durchgeführten Aktionen in Bezug auf die Warnung. Zu den angezeigten Informationen gehören, welche Warnungsverwaltungsregeln für die Warnung ausgeführt wurden, Incidents, die geöffnet wurden, und welche Nachbesserungs-Workflows ausgeführt wurden.

Warnungsausführungen

In einem Warnungsformular zeigt die Registerkarte „Warnungsausführung“ wichtige zugehörige Datensätze für die Warnung an. Beispielsweise wird angezeigt, welche Aktionen ausgeführt wurden und welche Warnungsverwaltungsregeln ausgeführt wurden. Wenn ein Incident geöffnet wurde, werden die zugehörigen Aufgaben angezeigt.

Warnungsausführungen

Felder im Abschnitt „Warnungsausführungen“

Feld	Beschreibung
Warnung	Verweis auf die Warnung, die unter dieser Regel ausgeführt wurde.
Aktionsname	Gibt an, wie die Warnung gelöst wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder im Abschnitt „Warnungsausführungen“ (Fortsetzung)

Feld	Beschreibung
Link zur Ausführung	Verknüpfte Aktion, die zur Behebung der Warnung durchgeführt wurde.
Zugehörige Aufgabe	Link zu der Aufgabe, die erstellt wurde, als die Warnung gelöst wurde.
Protokoll	Link zu dem Protokoll, das die Aktionen zur Lösung der Warnung ausführlich beschreibt.
Automatische Ausführung	Gibt an, ob die Regel automatisch (true) oder manuell (false) war.

Aktionsname
Dies gibt an, was beispielsweise aufgetreten ist, wenn ein Incident erstellt wurde.

Protokoll
Das Protokoll zeigt, welche Warnungsverwaltungsregel die Aktion initiiert hat. Es zeigt z. B. die automatische Ausführung (1 von 3) oder die manuelle Ausführung (2 von 4) an.

Warnungen im Status „Fluktuierend“ anzeigen

Sie können Warnungen anzeigen, die sich im Status „Fluktuierend“ befinden.

Vorbereitungen
Bevor Sie mit diesem Verfahren beginnen, bitten Sie Ihren Administrator, Eigenschaften für fluktuierende Warnungen zu konfigurieren.
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird
Flattern tritt auf, wenn von der Event-Quelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden. Flattern bewirkt, dass der Status der Ressource wiederholt zwischen dem Schweregrad *OK* und einem Schweregrad schwankt, der Aufmerksamkeit erfordert, z. B. *Critical*.

Die Häufigkeit von Events aus einer identischen Quelle innerhalb eines bestimmten Zeitintervalls bestimmt, ob sich eine Warnung im Status „Fluktuierend“ befindet oder ob ein neues Problem aufgetreten ist. Basierend auf den Eigenschaftswerten *evt_mgmt.flap_frequency* und *evt_mgmt.flap_interval*:

- Wenn das gleiche Problem wiederholt auftritt, ordnet Ereignismanagement das neue Event der vorhandenen Warnung zu, und der Status der Warnung wird auf **Flatternd** festgelegt.
- Wenn das Problem nach Ablauf des Zeitintervalls auftritt, erstellt Ereignismanagement eine Warnung.

Beispielsweise können Sie auf eine Warnung reagieren, indem Sie einen problematischen Server neu starten. Nachdem mehrere Minuten lang keine Events generiert wurden, wird davon ausgegangen, dass das Problem behoben ist, und die Warnung wird geschlossen. Wenn das Problem durch den Neustart nicht behoben wurde, kann dieser Server später weitere Events generieren. Dann werden zusätzliche Warnungen für dasselbe Problem generiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Klicken Sie auf die Nummer einer Warnung, die sich im Status **Flatternd** befindet.
3. Klicken Sie in der Warnung auf die Registerkarte **Flatternd**.

Registerkarte „Flatternd“ auf Warnungsformular

Feld	Beschreibung
Registerkarte **Flatternd**	
Anzahl der Fluktuationen	Die Anzahl, wie oft es innerhalb des Flatterintervalls seit der Startzeit im **Flattern – Startfenster** zu Flatterbewegungen bei Warnungen gekommen ist, d. h. zwischen einem geschlossenen und einem nicht geschlossenen Zustand gewechselt wurde.
Flattern – Startfenster	Die anfängliche Startzeit zur Messung der Fluktuationsereignisse.
Flattern – Zeit des letzten Update	Das letzte Vorkommen der Fluktuation. Dies ist die Verarbeitungszeit der Plattform, nicht die Zeit des Quellsystems.
Flattern – letzter Status	Der Status der Warnung vor dem Übergang in den Status „Fluktuierend“.

4. Wenn das Feld **Übergeordnet** leer ist, behandeln Sie diese Warnung als neues Problem.

Zugehörige Informationen

Fluktuierende Warnungen konfigurieren

Alle Warnungen nach Wartungsstatus anzeigen

Der **Wartungsstatus** gibt an, dass das CI gewartet wird. Beispielsweise gibt es ein Software-Upgrade, und die Probleme können aus dieser Aktivität resultieren, daher werden alle Wartungswarnungen verworfen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Der Wartungsstatus der Warnung kann sich aus einem der folgenden Gründe ändern:

- Ein Benutzer hat das Kontrollkästchen **Wartung** in der Warnung aktiviert oder die Warnung in der Listenansicht ausgewählt und dann auf die UI-Aktion **Wartung** geklickt.
- Eine neue Warnung, die an ein CI gebunden war, das sich in der CMDB-Tabelle im Wartungsstatus befindet.
- Wenn alle vorherigen zugehörigen Events der Warnung in Wartung sind, kann das Warnungsfeld **Wartung** automatisch auf *true*„Wartung läuft “gesetzt werden. Wenn das Feld **Wartung für** Warnungen *false* ist, der zugehörige CI-Status jedoch in *In Maintenance* geändert wird, nachdem die Warnung erstellt wurde, wird die Warnung bei nachfolgenden Events nicht in den Wartungsmodus versetzt. Beispiel: Wenn für einen Router eine Warnung generiert wird und der Router später zur Wartung heruntergefahren wird, wird dennoch davon ausgegangen, dass ein Problem vor Beginn der Wartung aufgetreten ist, und das Problem darf nicht ignoriert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn für eine Warnung in Genf ein Wartungs-Flag festgelegt wurde, wirkt sich dies nach dem Upgrade in Helsinki auf die Auswirkung als reguläre Warnung aus.
- Wenn eine Warnung durch eine Benutzeraktion (z. B. eine Warnungsverwaltungsregel) an ein CI gebunden ist und sich das CI im Wartungsstatus befindet, müssen Sie das CI manuell an die Warnung binden und es mit dem Status **In Wartung** markieren.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Überprüfen Sie die Spalte **Wartung** für jede Warnung.
   Der Wert *true* gibt an, dass das CI gewartet wird.

Hinweis: Wenn das Feld **Wartung** auf dem Warnungsformular nicht angezeigt wird, personalisieren Sie die Liste, um das Feld hinzuzufügen. Weitere Informationen finden Sie unter Persönliche Listen .

Innerhalb einer Warnung zusammenarbeiten

Sie können mit Kollegen zusammenarbeiten und Arbeitsnotizen schreiben, während Sie in einer Warnung arbeiten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird
Sie können in einer kompakten Ansicht von Connect arbeiten, die die Standardbenutzeroberfläche überlagert, oder in einem Vollbild-Arbeitsbereich. Die Konversationen werden nicht in die Warnung kopiert.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Klicken Sie auf die gewünschte Warnung.
3. Klicken Sie im Warnungsbildschirm auf **Folgen**.
   Die Bezeichnung der Schaltfläche ändert sich in **Verfolgt** und zeigt die aktuelle Verbindung mit dem Status der Zusammenarbeit an.
4. Um die Connect-Seitenleiste als Vollbild anzuzeigen, klicken Sie auf der Schaltfläche **Folgen** auf den Abwärtspfeil, und wählen Sie **Connect Full öffnen**.
   Sie können Text im Feld **Arbeitsnotiz** eingeben. Dieser Text wird nicht in die Warnung kopiert.
5. Zur Zusammenarbeit mit Kollegen oder dem Support klicken Sie auf das Symbol **Benutzer hinzufügen**.
6. Um die Connect-Zusammenarbeitssitzung abzuschließen, klicken Sie auf **Verfolgt**.

Incident oder Security Incident aus einer Warnung erstellen

Wenn eine Warnung eskaliert und einer Person zugewiesen werden muss, die das zugrunde liegende Problem lösen kann, können Sie einen Incident öffnen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird
Wenn Security Incident Response aktiviert ist, können Sie einen Security Incident erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Incidents und Sicherheits-Incidents manuell über das Warnungsformular erstellen. Um doppelte Aufgaben zu vermeiden, überprüft das System die Bedingungen aller Aufgabenvorlagen, bevor ein Incident erstellt wird.

Sie können den erstellten Incident mithilfe der *EvtMgmtCustomIncidentPopulator.populateFieldsFromAlert*Skripteinbindung anpassen. Die Anpassung umfasst das Zuordnen von Feldern von der Warnung zum Incident oder das Abbrechen der Incident-Erstellung gemäß benutzerdefinierten Bedingungen. Weitere Informationen finden Sie unter Benutzerdefinierte Warnungsfelder.

Sie können Incident-Felder mithilfe von benutzerdefinierten Warnungsfeldwerten aus zusätzlichen Informationsfeldern ausfüllen. Verwenden Sie die Skripteinbindung *EvtMgmtCustomIncidentPopulator*, um die Werte nach dem Kopieren der Daten in die Warnung in den Incident zu kopieren. Weitere Informationen finden Sie unter Benutzerdefinierte Warnungsfelder.

Hinweis: Wenn Security Incident Response aktiviert ist, enthält das Basissystem eine Warnungsaktionsregel namens **Create security incidents for critical alerts** (Sicherheitsvorfälle für kritische Warnungen erstellen). Diese Warnungsaktionsregel erstellt Sicherheitsvorfälle, wenn kritische Sicherheitsereignisse gemeldet werden.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Klicken Sie auf die **Nummer** der Warnung.
3. So erstellen Sie einen Incident:
   - Zum Erstellen eines Incidents klicken Sie auf **Quick Incident**.
   - Zum Erstellen von Security Incidents klicken Sie auf **Security Incident erstellen**. Sie müssen das Security-Plugin (SecOps) installieren, um diese Option zu aktivieren.
4. Klicken Sie auf **Aktualisieren**.

Ergebnisse

Der erstellte Incident wird im Feld **Aufgaben** im Warnungsformular angezeigt.

Zugehörige Informationen

Aus Events und Warnungen erstellte Security Incidents

Warnung in Wartung setzen

Sie können Warnungen manuell in die Wartung setzen, um sie in der Warnungsliste und im Agent Workspace auszublenden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Das Platzieren der Warnung in Wartung setzt nicht das CI in Wartung. Das **Statusfeld** im CI-Datensatz bleibt unverändert.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Führen Sie eine der folgenden Aktionen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Um mehrere Warnungen in Wartung zu versetzen	Aktivieren Sie die Kontrollkästchen neben den einzelnen Warnungen, und klicken Sie dann oben in der Liste auf die UI-Aktion **Wartung**.
Um eine Warnung in Wartung zu versetzen	Öffnen Sie die Warnung, und aktivieren Sie entweder das Kontrollkästchen **Wartung**, und klicken Sie auf **Aktualisieren**, oder klicken Sie oben in der Liste auf die UI-Aktion **Wartung**.

Zugehörige Informationen

Wartungsregeln erstellen

Informationen zu Warnungseinblick

Warnungseinblick hilft bei der schnelleren Suche nach Warnungen, sodass eine Lösung schneller gefunden und die wahrscheinliche Ursache der ausgewählten Warnung offengelegt werden kann.

Warnungseinblick verwenden, um eine Lösung zu finden und die Ursache der Warnung zu finden

Ergebnisse der Datenanalyse liefern weitere Informationen über die Warnung, die über die Informationen im Warnungsformular hinausgehen. Dies hilft bei der schnelleren Suche nach Warnungen, sodass eine Lösung schneller gefunden und die wahrscheinliche Ursache der Warnung offengelegt werden kann.

Die angezeigten Informationen stammen aus wiederholten Warnungen, ähnlichen Warnungen, Incidents, Problemen und Change Requests für dasselbe CI, ähnliche CIs und andere CIs, die durch CMDB-Beziehungen oder Gruppierungen verbunden sind.

Schnelle Antworten in einer Warnung anwenden

In einer Warnung können Sie die Funktion *Schnelle Antwort* verwenden, um Fehlerkorrekturen auf die Warnung anzuwenden oder eine Webanwendung zu starten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

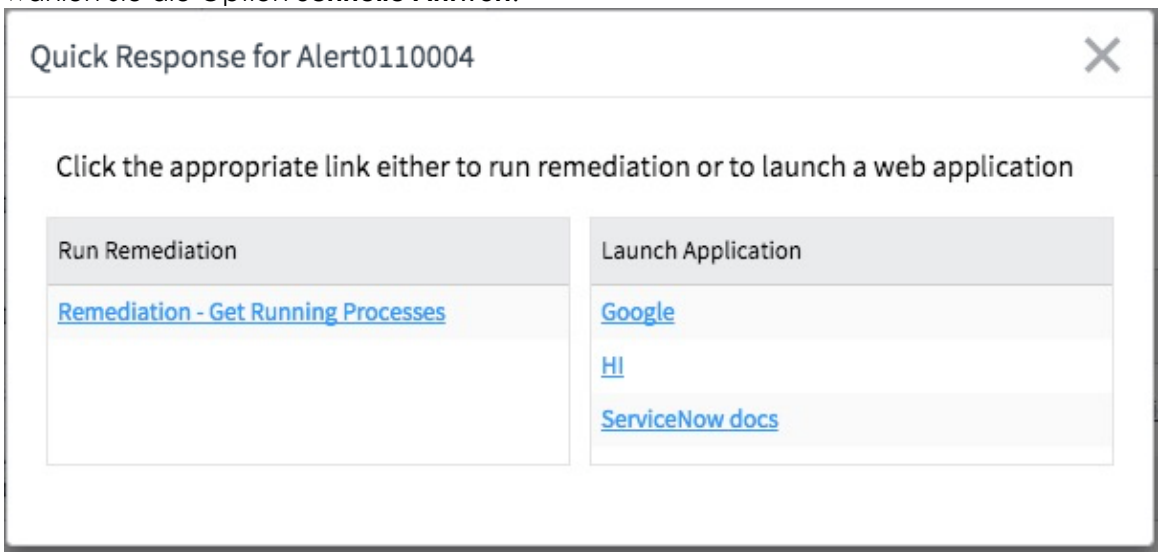
Mit der Funktion **Schnelle Antwort** können Sie schnelle Aktionen in der ausgewählten Warnung durchführen. Mit dieser Aktion können Sie Nachbesserungen anwenden oder Anwendungen starten. Wenn Sie ein Upgrade von Istanbul oder einer früheren Version durchgeführt haben, können Sie sich diese Funktion als Kombination aus den Funktionen **Fehlerkorrektur** und **Anwendung starten** vorstellen.

Wenn Sie beim Aufrufen einer schnellen Antwort einen Link für die Fehlerkorrektur auswählen, wird ein Workflow ausgeführt, und zwar anhand den in der Warnungsverwaltungsregel angegebenen Kriterien. Klicken Sie auf den entsprechenden Link vom Typ „Anwendung starten“, um die in der Warnungsverwaltungsregel festgelegte Webanwendung zu starten. Weitere Informationen finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Klicken Sie mit der rechten Maustaste auf die jeweilige Warnung in der Warnungsliste und wählen Sie die Option **Schnelle Antwort**.



3. Klicken Sie auf der Seite „Schnelle Antwort“ auf den entsprechenden Link, um die gewünschte Aktion auszuführen.
   Wenn der benötigte Link nicht verfügbar ist, führen Sie eine der folgenden Aktionen aus.

Option	Bezeichnung
Bei Fehlerkorrekturen definieren Sie eine Korrekturaufgabe, und zwar abhängig von einer Warnungsregel und basierend auf der ausgewählten Warnung	**a.** Navigieren Sie zu **Warnungsregeln**. **b.** Wählen Sie die gewünschte Warnungsverwaltungsregel zur Bearbeitung aus. **c.** Klicken Sie auf **Fehlerkorrektur**. **d.** Klicken Sie auf **Fehlerkorrektur aktivieren**. **e.** Wählen Sie im Feld **Ausführung** entweder „automatisch“ oder „manuell“ aus. **f.** Geben Sie im Workflow-Feld **Orchestration** den gewünschten Workflow für die Fehlerkorrektur an. ▪ Bei **Orchestration** wählen Sie in den Workflow-Einstellungen die **Korrekturaufgabe [em_remediation_task]** im Feld **Tabelle** aus. ▪ Veröffentlichen Sie den Orchestration Workflow, wenn Sie ihn fertig konfiguriert haben. **g.** Klicken Sie auf **Aktualisieren**. Weitere Informationen finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Erstellen Sie bei „Anwendung starten“ einen Link auf eine Webanwendung, indem Sie basierend auf der ausgewählten Warnung eine Warnungsregel verwenden	**a.** Navigieren Sie zu **Warnungsregeln**. **b.** Wählen Sie die gewünschte Warnungsverwaltungsregel zur Bearbeitung aus. **c.** Klicken Sie auf **Startprogramm**. **d.** Klicken Sie auf **Aktivieren**. **e.** Geben Sie im Feld **Anzeigename** einen Namen für den Link ein. **f.** Im Feld **URL** erstellen Sie anhand von Daten aus der Warnung die URL, und zwar im folgenden Format: `${source}.com:${port}/${cmdb_ci.name}` **g.** Klicken Sie auf **Aktualisieren**. Weitere Informationen finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

Nächste Maßnahme

Informationen dazu, wie Sie Korrekturaufgaben oder Links zu Webanwendungen erstellen, finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

Zugehörige Informationen

Webanwendungen aus einer Warnung starten

Serviceintegritätüberwachung

Auf Betreiber-Arbeitsbereichkönnen Sie Warnungen nach Anwendungsservices, technischem Service und Warnmeldungsgruppe anzeigen. Für Services können Sie auch eine Servicezuordnung öffnen, um Beziehungen zwischen CIs im Service anzuzeigen.

Vorbereitungen

Bitten Sie einen Administrator, mindestens einen Anwendungsservice, einen technischen Service oder eine Warnmeldungsgruppe zu erstellen, wenn keines dieser Elemente vorhanden ist.

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Die Kacheln Betreiber-Arbeitsbereich stellen einen Service, eine Warnungsgruppe oder ein CI dar. Die Kachelfarbe stellt den Gesamtschweregrad der Warnung dar.

Hinweis: Das Ereignismanagement-Dashboard wird für neue Instanzen im Paris-Release nicht unterstützt. Für Instanzen, die ausgehend von einem Release vor Orlando aktualisiert wurden und in denen das Ereignismanagement-Dashboard verwendet werden kann, ist dies jedoch weiterhin möglich.

Diese Kachelsymbole sind verfügbar:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard-Kachelsymbole

Symbol	Bedeutung
	Stellt den Status eines zugeordneten Anwendungsservice dar.
	Stellt den Status einer Warnungsgruppe mit einer Reihe von entsprechenden offenen Warnungen dar.
	Stellt den Status einer dynamischen CI-Gruppe dar.

Jede Kachel stellt den höchsten Schweregrad einer Warnung für den Service, die Warnungsgruppe oder das CI dar. Beispielsweise wird eine Kachel rot angezeigt, wenn eine Warnung kritisch ist. Eine grüne Kachel zeigt entweder Informationswarnungen oder keine derzeit aktiven Warnungen an. Wenn sich die Warnungsschweregrade ändern, werden die Kachelfarben entsprechend aktualisiert. Die folgenden Schweregrade sind verfügbar:

- **Rot**: Schweregrad „Kritisch“ (höchster Schweregrad) Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor.
- **Orange**: Schweregrad „Schwerwiegend“ Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten.
- **Gelb**: Schweregrad „Gering“ Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten.
- **Blau**: Schweregrad „Warnung“ (niedrigster Schweregrad) Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist.
- **Frün**: Information. Kein Schweregrad Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig.

Prozedur

Zur Integration mit Operational Intelligence aktivieren Sie das Plugin „Operational Intelligence“ (com.snc.sa.metric).
Führen Sie die Schritte im Thema Erste Schritte mit Metrikdaten aus. Informationen zu Metriken werden auf der Registerkarte **Metriken** im Service Operations-Arbeitsbereich angezeigt.

Zugehörige Informationen

Metrikwerte im Explorer für Einblicke anzeigen

Erkannten Service-Verlauf anzeigen

Der Verlauf der erkannten Services zeigt die Häufigkeit der erkannten Services für einen bestimmten Zeitraum an.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Der Verlauf der erkannten Services wird nur angezeigt, wenn mehrere erkannte Services über einen bestimmten Zeitraum auftreten. Ein erkannter Service ist ein Service, der von Service Mapping erkannt wird. Der Verlauf erkannter Services ist für Anwendungsservices nicht verfügbar. Wenn für einen bestimmten Service keine erkannten Services generiert werden, wird der Verlauf der erkannten Services ausgeblendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Service Operations-Arbeitsbereich**.
2. Klicken Sie auf eine Servicekachel, und klicken Sie auf **Servicezuordnung**.
3. Klicken Sie auf die Schaltfläche **Verlaufszuordnung**.
   Die Verlaufszeitleiste wird angezeigt. Änderungen am Service werden durch ein Uhrensymbol ( ) angezeigt.

4. Zum Anzeigen einer Zuordnung, die Änderungen am Schweregrad des Services darstellt, klicken Sie auf das Symbol „Mehr“ ( ), und wählen Sie **Erweiterte Zuordnung**.

Die angezeigte Farbe entspricht dem Schweregrad der erkannten Services, und die Länge der Leiste in jeder Farbe entspricht der Dauer, die die erkannten Services diesen Schweregrad beibehalten haben.

In der folgenden Tabelle sind die Schweregradfarben erläutert:

Farben für Serviceschweregrade

Schweregrad	Symbolfarbe
Kritisch	
Hoher	Orange
Geringer	Gelb
Warnung	Blau

5. Um die Informationen zu ändern, die auf der erweiterten Zuordnung des erkannten Serviceverlaufs angezeigt werden, klicken Sie auf ein Verlaufssymbol.

   - **Kalendersymbol**: Informationen für derzeit aktive erkannte Services anzeigen.
   - **Stunden**: Informationen zu erkannten Services anzeigen, die in der letzten Stunde aufgetreten sind.
   - **Tage**: Informationen zu erkannten Services anzeigen, die in den letzten 24 Stunden aufgetreten sind.
   - **Wochen**: Informationen zu erkannten Services anzeigen, die in der letzten Woche aufgetreten sind.
   - **Monate**: Informationen zu erkannten Services anzeigen, die im letzten Monat aufgetreten sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen Sie Warnungen für Anwendungsservices

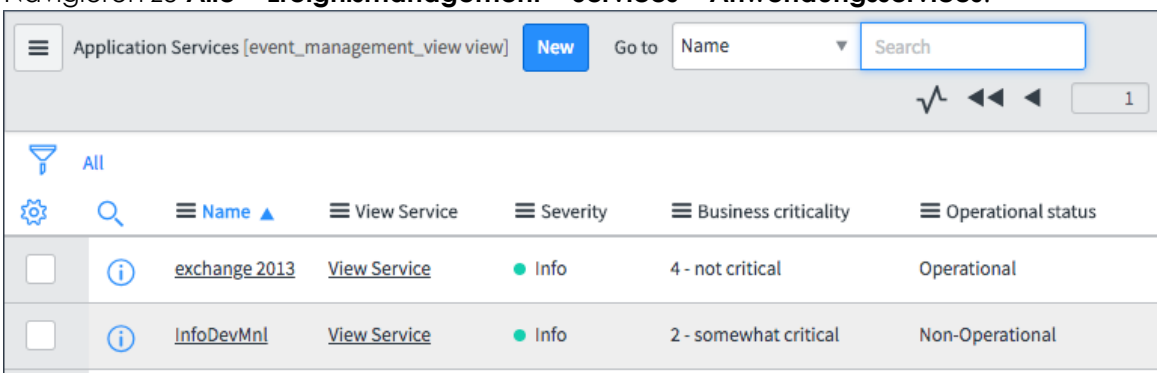
Um nur Informationen für Anwendungsservices anzuzeigen, navigieren Sie zur Liste der Anwendungsservices. In dieser Liste können Sie Servicezuordnungen öffnen, um Warnungen für die CIs in jedem Service anzuzeigen und zu verwalten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Anwendungsservices**.



2. Klicken Sie in der Zeile der erforderlichen Anwendungsservices **auf Zuordnung anzeigen**.
3. Führen Sie einen oder mehrere der folgenden Schritte aus.

Option	Aktion
Warnungsdetails für ein CI anzeigen	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie unterhalb der Karte auf die Registerkarte **Warnungen**, und überprüfen Sie die aufgelisteten Warnungen.
Auswirkung auf übergeordnetes CI anzeigen	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie unterhalb der Servicezuordnung auf die Registerkarte **Auswirkung**, und überprüfen Sie die aufgeführten Auswirkungsregeln. **c.** Auswirkungsregeln bei Bedarf anpassen
Ändern Sie die Zuordnungsanzeige, das Zuordnungslayout oder die Zuordnungsindikatoren	Im Header der Servicezuordnung: **a.** Klicken Sie auf das Menüsymbol. **b.** Konfigurieren Sie die entsprechenden Einstellungen.
Navigieren Sie zu anderen Anwendungsservices	Im Header der Servicezuordnung: **a.** Klicken Sie auf den Abwärtspfeil neben dem Servicenamen oder das Ordnersymbol für alle Services. **b.** Suchen Sie nach anderen Anwendungsservices, und wählen Sie sie aus ( ).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	Die Symbolfarbe stellt die höchste Auswirkung oder den höchsten Schweregrad für aktive Warnungen in den Anwendungsservices dar. ◦ **Kritisch**: Rot (höchster Schweregrad). ◦ **Schwerwiegend**: Orange. ◦ **Geringfügig**: Gelb. ◦ **Warnung**: Blau (niedrigster Schweregrad).
Eigenschaften für ein CI anzeigen	In der Servicezuordnung: **a.** Klicken Sie auf eine CI-Kachel. **b.** Klicken Sie im Seitenbereich auf die Registerkarte **Eigenschaften**, und überprüfen Sie Informationen zum CI. **c.** Wenn Sie detailliertere Informationen anzeigen möchten, scrollen Sie zum Ende des Bereichs, und klicken Sie auf **Detaillierte Eigenschaften**.

Überwachte Services anzeigen

Zeigen Sie alle Services an, die Ereignismanagement unterstützt, z. B. Warnmeldungsgruppen, erkannte Services, Anwendungsservices und technische Services. Je nach Typ des Services können Sie Details zur Servicedefinition anzeigen oder einen Drilldown in den Service durchführen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user

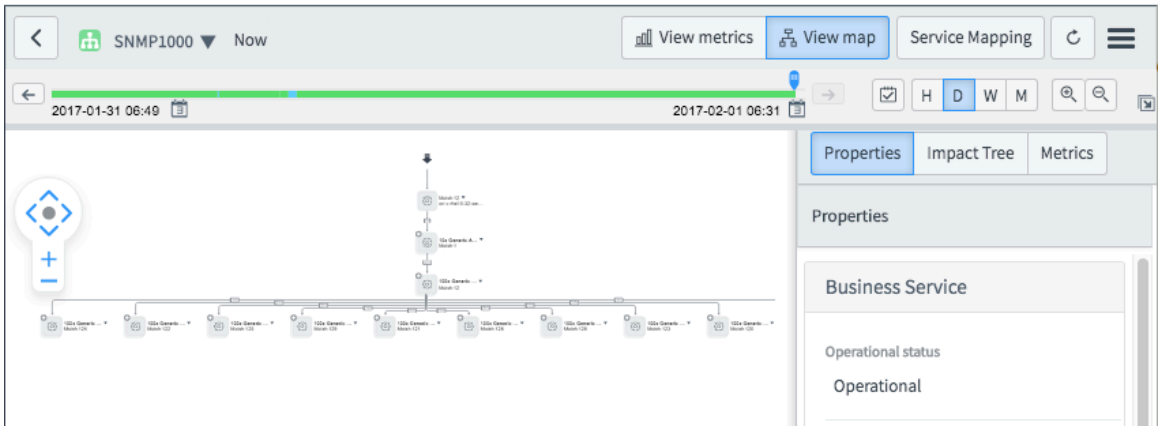
Hinweis: Anwendungsservices, die vor der Aktivierung des Plugins Ereignismanagement erstellt wurden, werden in der Spalte **Service anzeigen** der Liste „Überwachte Services“ nicht aufgeführt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Überwachte Services**.
2. Klicken Sie auf **Service anzeigen**, um die für diesen Service relevante Ansicht zu öffnen. Wenn Sie einen Drilldown zum Inhalt des Services durchführen, wird je nach Service-Typ entweder eine Zuordnung, eine Warnungsliste oder eine CI-Liste angezeigt.

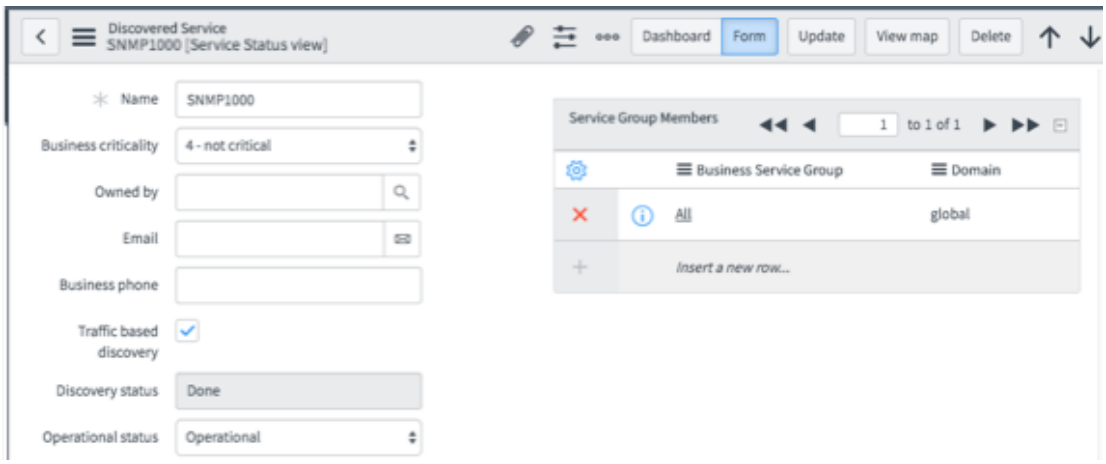
   Wenn Sie beispielsweise für SNMP1000 auf **Service anzeigen** klicken, können Sie einen Drilldown zum Inhalt des Services durchführen, und die zugehörige Topologiezuordnung wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Zum Anzeigen von Servicedefinitionsdetails eines Services klicken Sie auf den Namen des Services auf der Seite **Überwachte Services**.

   Beispiel: Klicken Sie in der Spalte **Name** auf SNMP1000 ( ).



Zugehörige Informationen

Serviceintegritätüberwachung

Übersichts-Dashboard „Event Management“ verwenden

Das Ereignismanagement Übersichtsmodul verwendet Performance Analytics zur Präsentation von Daten aus Ihrer Instanz, um Ihre Prozesse besser darzustellen und zu verstehen und kontinuierliche Verbesserungen zu erzielen.

Vorbereitungen

Standard-Zeilenanzahl, die von einer Indikatorquelle abgerufen werden darf ist 50.000. Um diese Anzahl zu ändern, bearbeiten Sie die Eigenschaft com.snc.pa.dc.max_row_count_indicator_source: **Performance Analytics** > **System** > **Eigenschaften**.

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Mit der Administratorrolle Ereignismanagement können Sie Bericht-Widgets hinzufügen, löschen und neu anordnen. Die anderen Ereignismanagement Rollen können Bericht-Widgets anzeigen und aktualisieren.

Hinweis: Event Management unterstützt keine Mobilgeräte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Übersicht**.
   Die Standardanzeige des Übersichts-Dashboards Ereignismanagement hängt davon ab, ob die Basisinstanz ein Upgrade von einem früheren Release ist und welche Plugins aktiviert sind:
   - Ereignismanagement wurde von einem früheren Release aktualisiert oder ist in der Instanz aktiviert, siehe Dashboard Ereignismanagement Übersicht.
   - Ereignismanagement und das Plugin Performance Analytics - Content Pack - Ereignismanagement (com.snc.pa.em) sind aktiviert, siehe Ereignismanagement Insight-Dashboard.

   Hinweis: Wenn Ereignismanagement von einem früheren Release aktualisiert wurde und das Plugin Performance Analytics - Content Pack - Ereignismanagement (com.snc.pa.em) aktiviert ist, siehe Ereignismanagement Bewertungslisten.
2. Verschieben oder fügen Sie Widgets nach Bedarf hinzu.
3. Klicken Sie auf Elemente in Widgets, um weitere Informationen zu erhalten.

Zugehörige Informationen

Performance Analytics und Reporting

Ereignismanagement Insight-Dashboard

Das Insight-Dashboard Ereignismanagement kann angezeigt werden, wenn sowohl das Plugin Ereignismanagement (com.glideapp.itom.snac) als auch das Plugin Performance Analytics - Content Pack - Ereignismanagement (com.snc.pa.em) aktiviert sind.

Ereignismanagement Insights-Dashboard

Hinweis: Event Management unterstützt keine Mobilgeräte.

1. Navigieren zu **Ereignismanagement** > **Übersicht** um das Übersichtsmodul anzuzeigen.
2. Wählen Sie Ereignismanagement Insights aus der Dropdown-Liste aus.

Folgende Registerkarten sind im Dashboard Ereignismanagement Insights verfügbar:

- Datenqualität
- Überwachung Servicerelevanz
- Auswirkungszeit Schweregrad-Überwachung
- Warnungslebenszyklus

Sie können auf Elemente in Widgets klicken, um weitere Informationen zu erhalten.

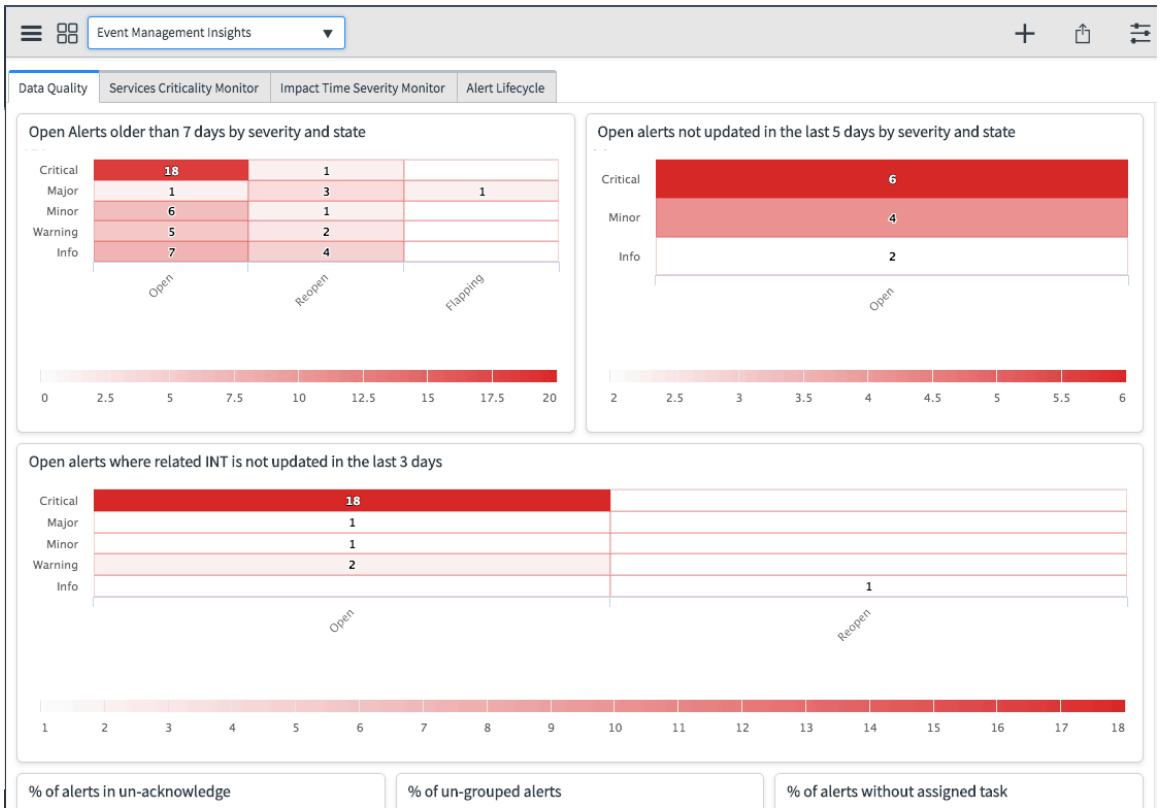
Datenqualität

Die Registerkarte „Datenqualität“ in der Basisinstanz wird angezeigt:

- Offene Warnungen, die nach Schweregrad und Status älter als 7 Tage sind
- Offene Warnungen, die in den letzten 5 Tagen nicht nach Schweregrad und Status aktualisiert wurden
- Offene Warnungen, bei denen das zugehörige INT in den letzten 3 Tagen nicht aktualisiert wurde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- % der Warnungen mit aufgehobener Bestätigung
- % der nicht gruppierten Warnungen
- % der Warnungen ohne zugewiesene Aufgabe

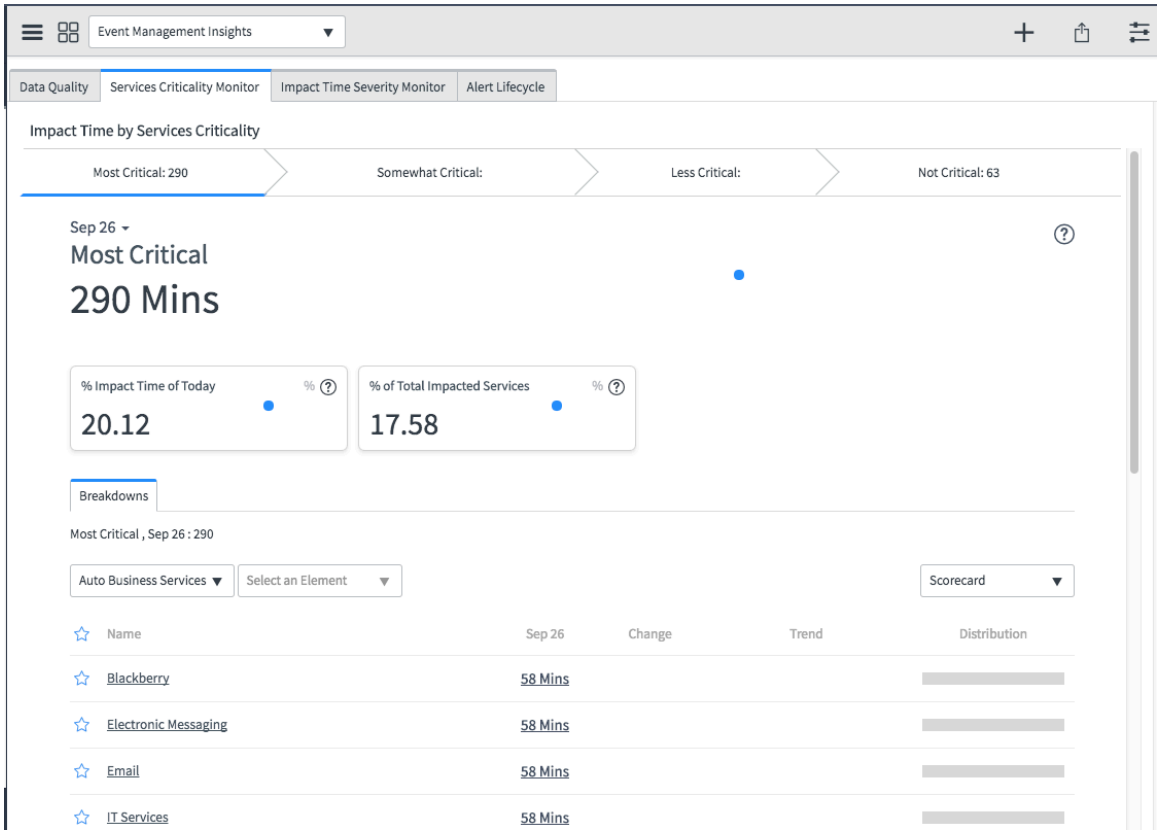


Überwachung Servicerelevanz

Die Registerkarte „Überwachung der Servicerelevanz“ in der Basisinstanz zeigt die Auswirkungszeit nach Servicerelevanz gruppiert nach:

- Sehr kritisch
- Teilweise relevant
- Weniger relevant
- Nicht relevant

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

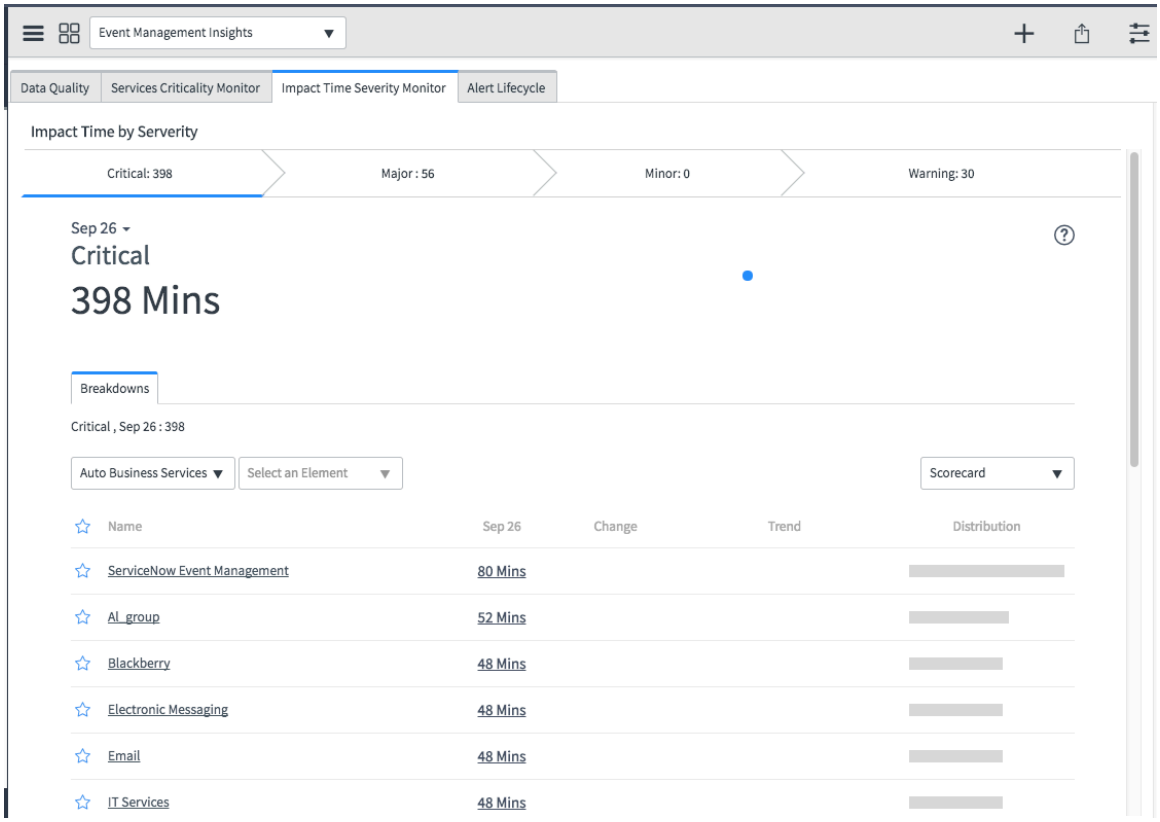


Auswirkungszeit Schweregrad-Überwachung

Die Registerkarte „Auswirkungszeit-Schweregradüberwachung“ zeigt die Auswirkungszeit nach Schweregrad gruppiert nach:

- Kritisch
- Hoher
- Geringer
- Warnung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Warnungslebenszyklus

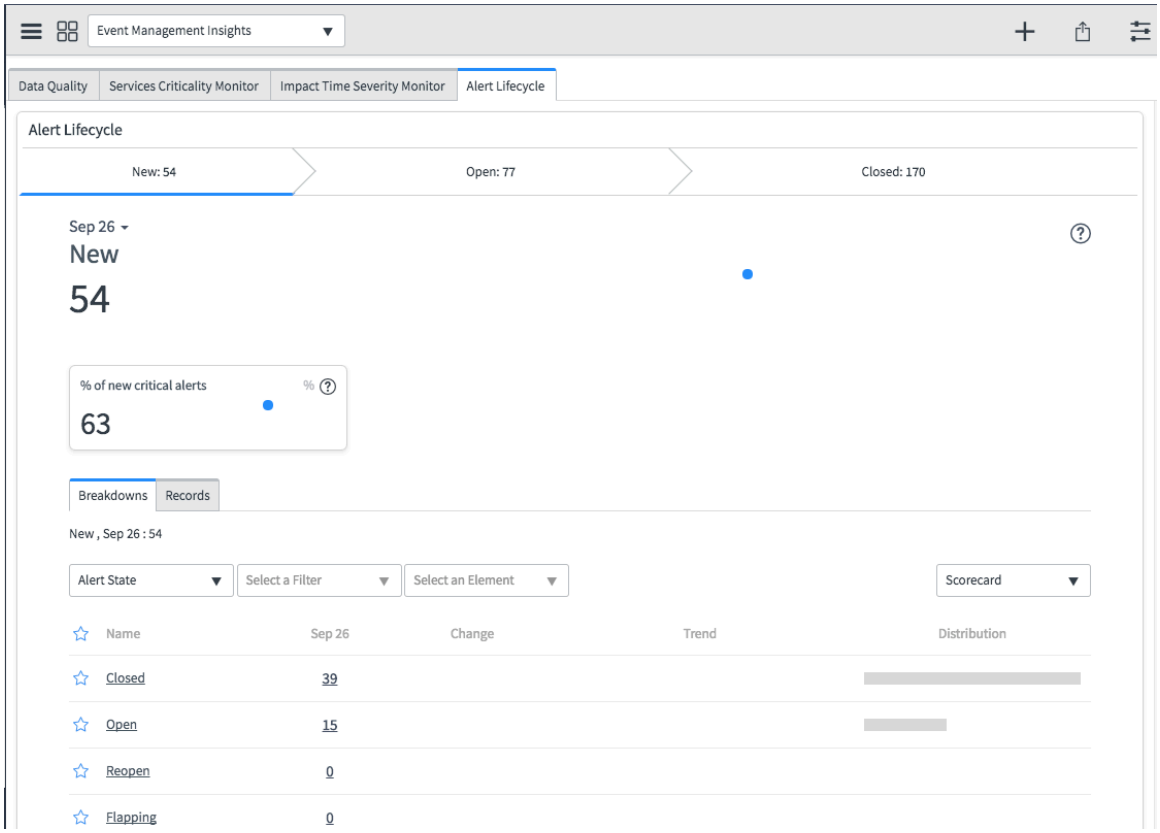
Die Registerkarte „Warnungslebenszyklus“ zeigt die Widgets des Warnungslebenszyklus, gruppiert nach:

- Neu
- Offen
- Abgeschlossen

In jedem dieser Widgets können Sie entweder Aufgliederungen oder die zugrunde liegenden Datensätze anzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ereignismanagement Bewertungslisten

Das Bewertungslisten-Dashboard Ereignismanagement kann angezeigt werden, wenn sowohl das Plugin Ereignismanagement (com.glideapp.itom.snac) als auch das Plugin Performance Analytics - Content Pack - Ereignismanagement (com.snc.pa.em) aktiviert sind.

Ereignismanagement Bewertungslisten-Dashboard

Hinweis:

- Ereignismanagement unterstützt keine Mobilgeräte.
- Sie müssen die relevanten Performance Analytics-Aufträge konfigurieren, damit das Bewertungslisten-Dashboard Daten anzeigen kann. Einzelheiten finden Sie unter Performance Analytics-Datensammlung .

1. Navigieren zu **Ereignismanagement** > **Übersicht** um das Übersichtsmodul anzuzeigen.
2. Wählen Sie Ereignismanagement Bewertungsliste aus der Dropdown-Liste aus.

Die Registerkarten sind im Ereignismanagement Bewertungslisten-Dashboard verfügbar:

- EM-Übersicht
- Service-Bewertungslisten
- Warnungsbewertungsliste
- Systemüberprüfungsüberwachung

Sie können auf Elemente in Widgets klicken, um weitere Informationen zu erhalten.

EM-Übersicht

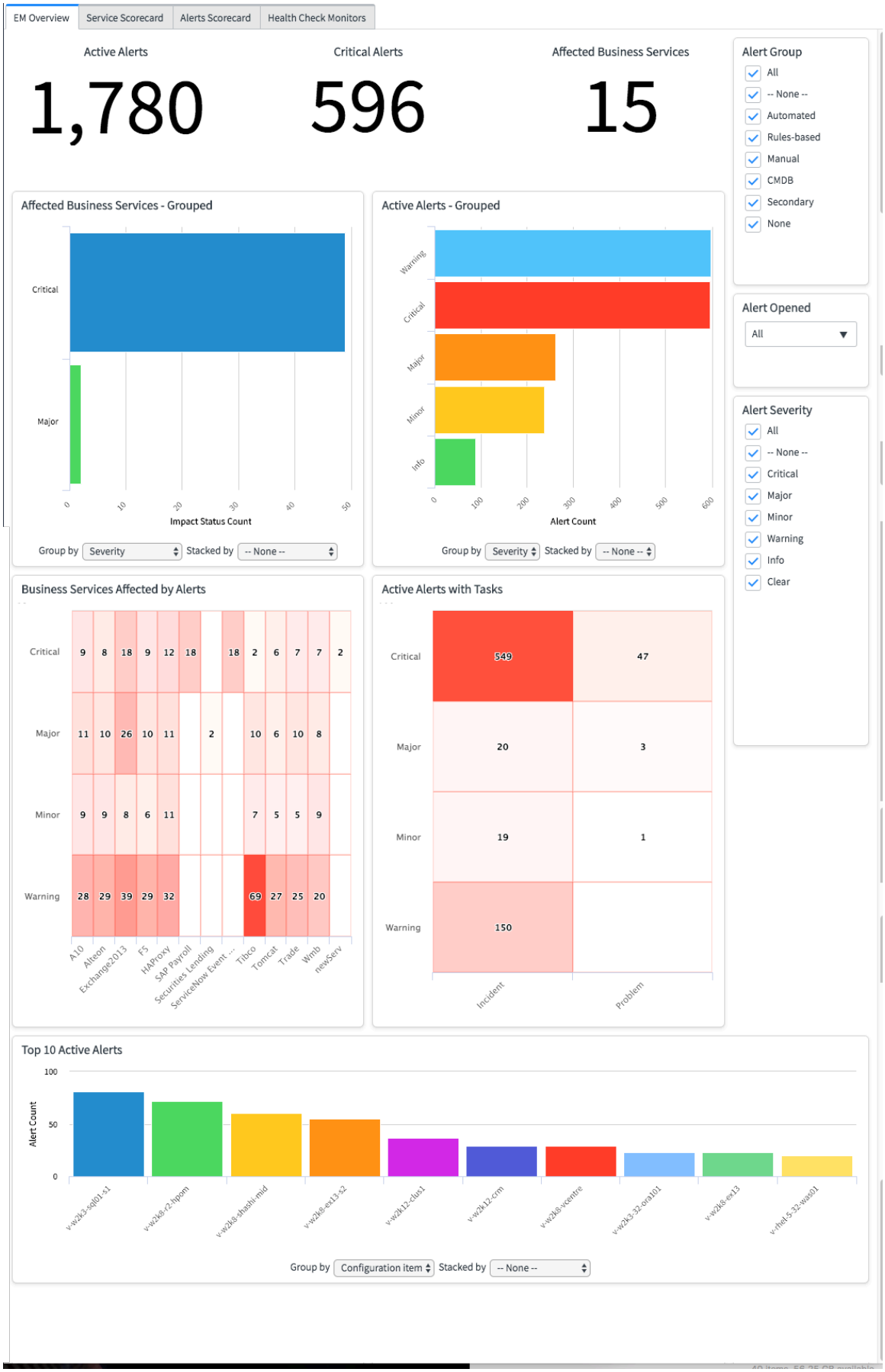
Die Registerkarte EM-Übersicht zeigt Folgendes:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Widget	Beschreibung
Aktive Warnungen	Anzahl aktiver Warnungen.
Kritische Warnungen	Anzahl der Warnungen, deren Schweregrad kritisch ist.
Betroffene Anwendungsservices	Anzahl der Services, die sich auf den Anwendungsservice auswirken.
Betroffene Anwendungsservices – Gruppiert	Grafische Darstellung der Anzahl der Services, die sich auf den Anwendungsservice auswirken. Sie können das Diagramm mit den Steuerelementen im Widget konfigurieren.
Aktive Warnungen - Gruppiert	Grafische Darstellung der Anzahl der aktiven Warnungen. Sie können das Diagramm mit den Steuerelementen im Widget konfigurieren.
Von Warnungen betroffene Anwendungsservices	Anzahl der Anwendungsservices, die sich auf Warnungen auswirken. Sie können das Diagramm mit den Steuerelementen im Widget konfigurieren.
Aktive Warnungen mit Aufgaben	Anzahl aktiver Warnungen mit Aufgaben. Sie können das Diagramm mit den Steuerelementen im Widget konfigurieren.
Top 10 aktive Warnungen	Zehn aktivste Warnungen im Überprüfungszeitraum. Sie können das Diagramm mit den Steuerelementen im Widget konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Automatische Übersetzung

Service-Bewertungsliste

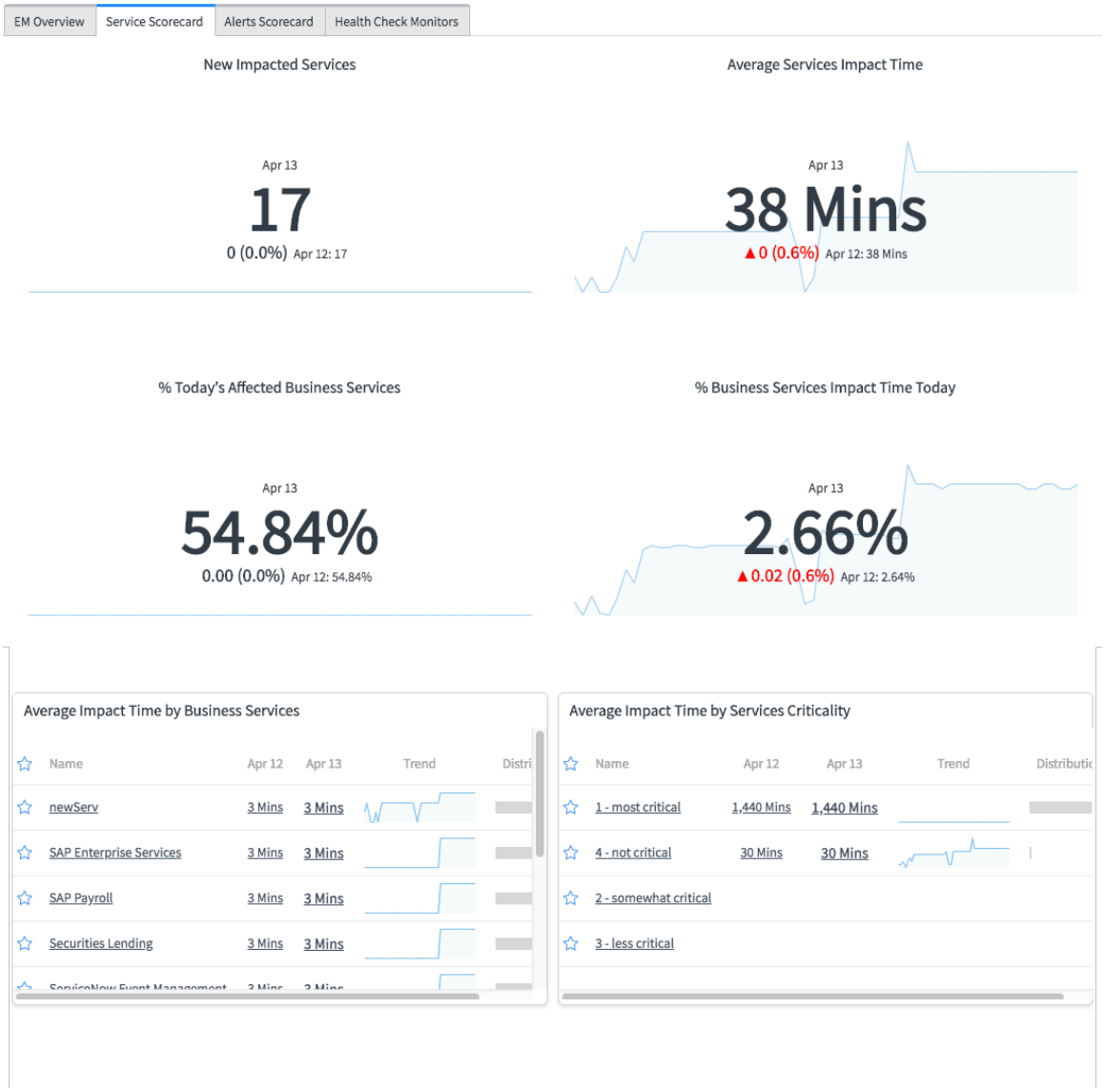
Die Registerkarte „Service-Bewertungsliste“ zeigt Folgendes:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardberichte im Dashboard „Service-Bewertungsliste“

Widget	Beschreibung
Neu betroffene Services	Zeigt die Anzahl der Services an, die von einer Warnung betroffen waren.
Durchschnittliche Auswirkungszeit Services	Zeigt die durchschnittliche Zeit (in Minuten) an, die Warnungen auf Services wirken.
Betroffene Anwendungsservices von heute	Zeigt den Prozentsatz der Anwendungsservices an, die im Laufe des Tages betroffen waren.
% Auswirkungszeit Anwendungsservices heute	Zeigt den Prozentsatz der Anwendungsservices an, die im Laufe des Tages von Warnungen betroffen waren.
Durchschnittliche Auswirkungszeit nach Anwendungsservices	Zeigt die durchschnittliche Zeit (in Minuten) an, während der Anwendungsservices von Warnungen betroffen sind.
Durchschnittliche Auswirkungszeit nach Services-Relevanz	Zeigt die durchschnittliche Zeit (in Minuten) an, während der Anwendungsservices von der Servicerelevanz betroffen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

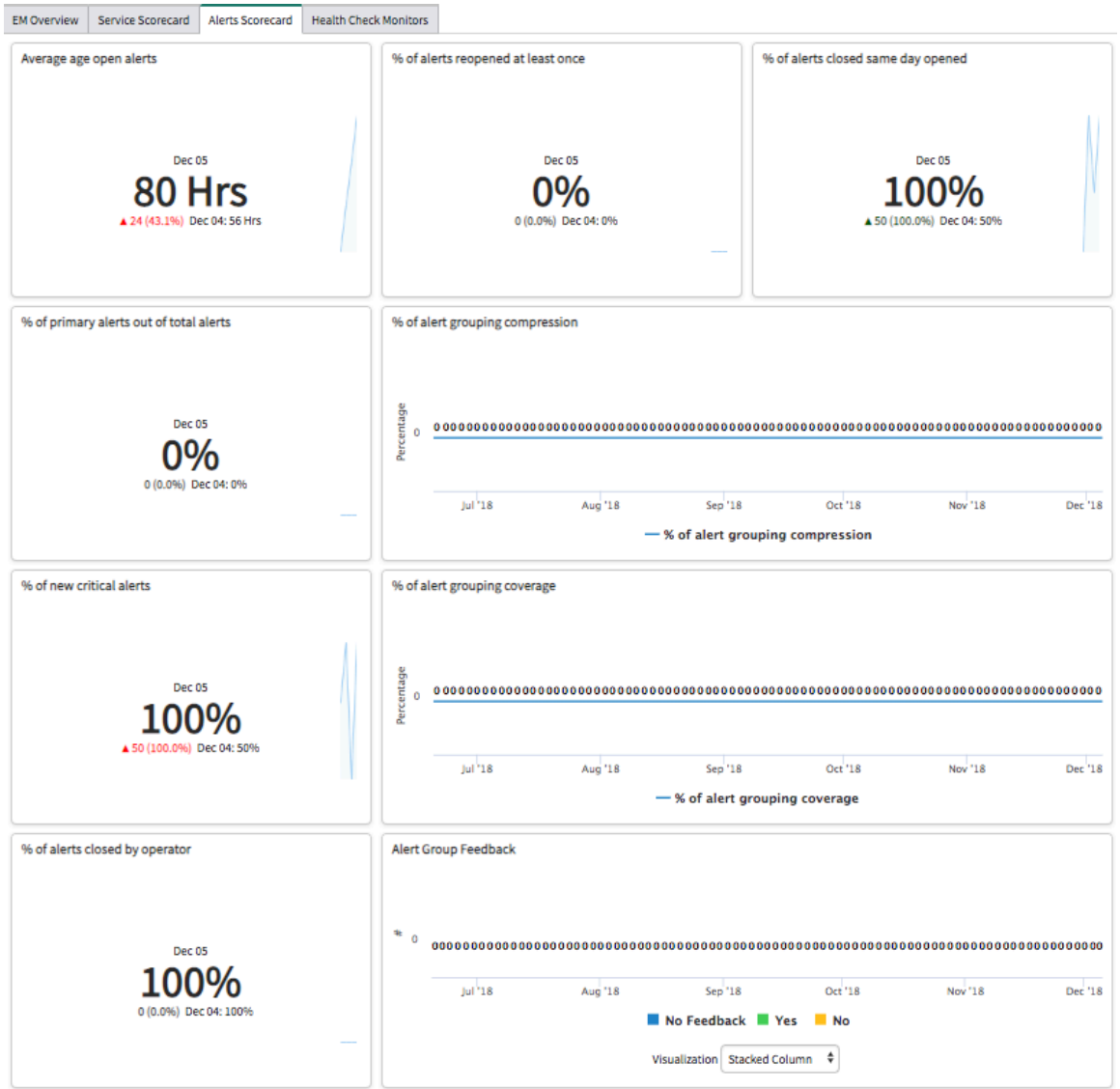


Warnungsbewertungsliste

Die Registerkarte „Warnungsbewertungsliste“ zeigt Folgendes:

- Durchschnittsalter offener Warnungen
- % der mindestens einmal erneut geöffneten Warnungen
- % der am selben Tag geöffneten und geschlossenen Warnungen
- % der primären Warnungen von allen Warnungen
- % der Warnungsgruppenkomprimierung
- % der neuen kritischen Warnungen
- % der Warnungsgruppierungsabdeckung
- % der vom Operator geschlossenen Warnungen
- Warnungsgruppenfeedback

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

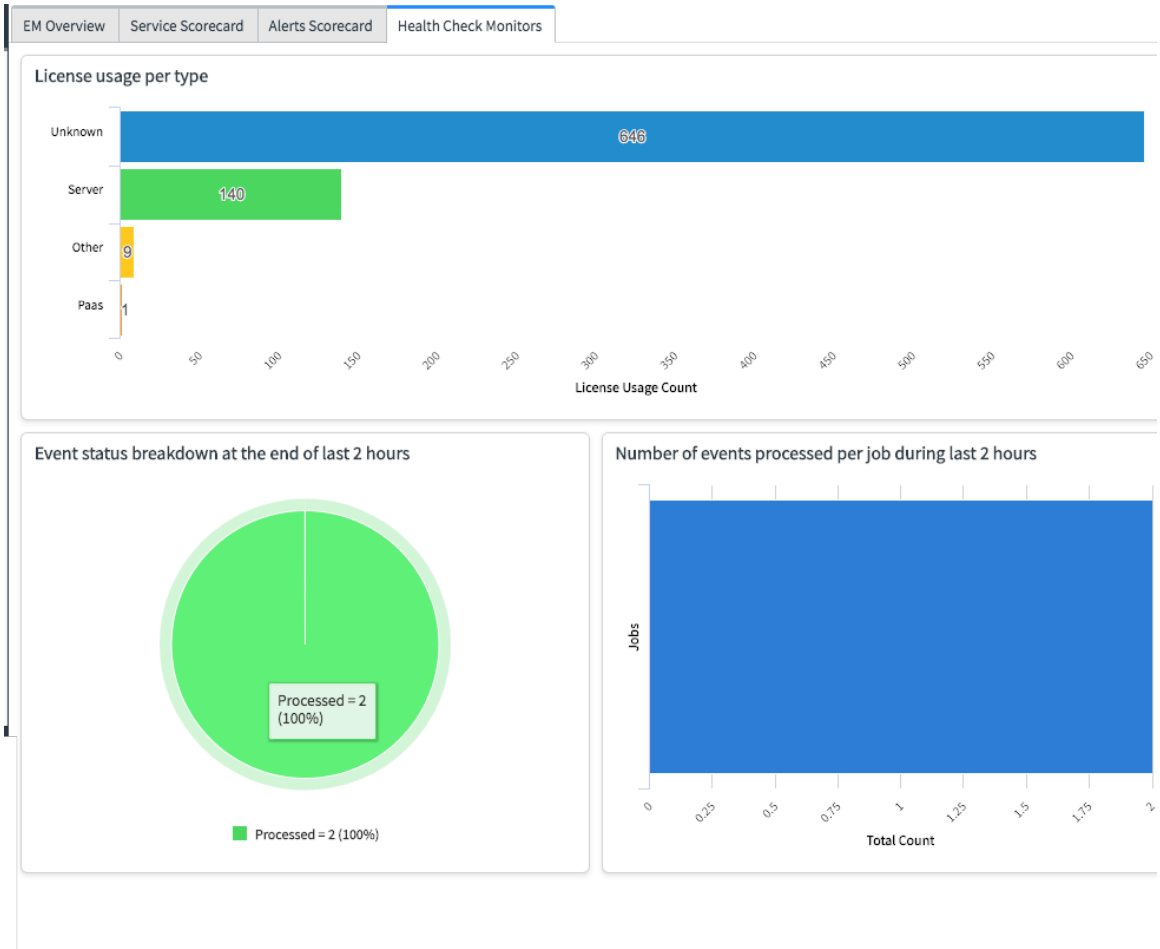


Systemüberprüfungsüberwachung

Die Registerkarte „Systemüberprüfungsüberwachung“ zeigt Folgendes:

- Lizenznutzung nach Typ
- Event-Status-Aufgliederung am Ende der letzten 2 Stunden
- Anzahl der pro Auftrag in den letzten 2 Stunden verarbeiteten Events

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Wenn eine große Anzahl von Events vorhanden ist, ist die Event-Status-Aufgliederung am Ende des Berichts über die letzten 2 Stunden nicht verfügbar.

Dashboard Ereignismanagement Übersicht

Das Dashboard Ereignismanagement Übersicht kann angezeigt werden, wenn Ereignismanagement von einem früheren Release aktualisiert oder in der Instanz zum ersten Mal aktiviert wird.

Ereignismanagement-Dashboard „Übersicht“

Hinweis: Event Management unterstützt keine Mobilgeräte.

Navigieren zu **Ereignismanagement** > **Übersicht** um das Übersichtsmodul anzuzeigen.

Sie können auf Elemente in Widgets klicken, um weitere Informationen zu erhalten.

Die in diesem Dashboard verfügbaren Übersichtsmodule sind:

- Ereignismanagement-Übersicht
- Systemüberprüfungsüberwachung

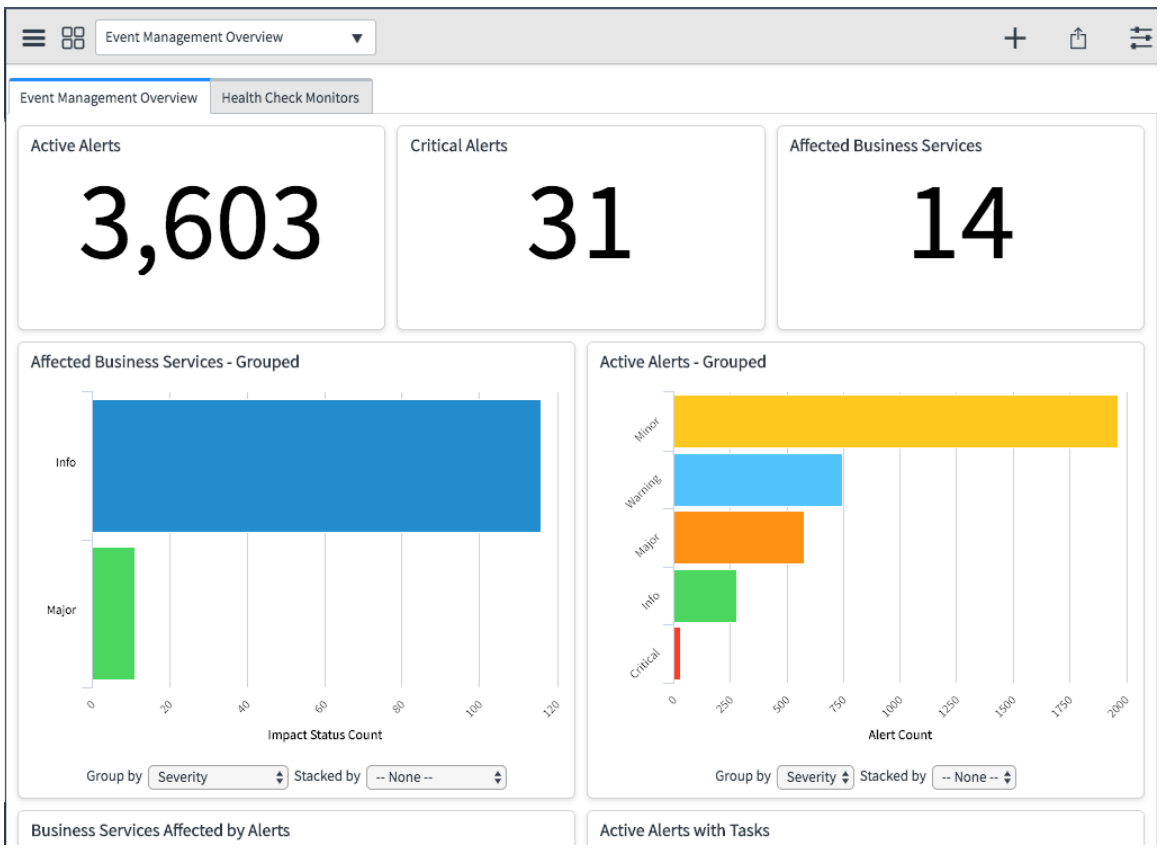
Ereignismanagement Registerkarte Übersicht

Standard-Widgets auf der Registerkarte Ereignismanagement Übersicht sind:

Widget	Beschreibung
Aktive Warnungen	Zeigt die Anzahl aktiver Warnungen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Widget	Beschreibung
Kritische Warnungen	Zeigt die Anzahl von Warnungen an, deren Schweregrad „Kritisch“ ist.
Betroffene Anwendungsservices	Zeigt die Anzahl der Services an, die sich auf den Anwendungsservice auswirken.
Betroffene Anwendungsservices – Gruppiert	Grafische Darstellung der Anzahl der Services, die sich auf den Anwendungsservice auswirken. Sie können das Diagramm mit den Steuerelementen im Widget konfigurieren.
Aktive Warnungen - Gruppiert	Grafische Darstellung der Anzahl der aktiven Warnungen. Sie können das Diagramm mit den Steuerelementen im Widget konfigurieren.
Von Warnungen betroffene Anwendungsservices	Zeigt die Anzahl der Anwendungsservices an, die sich auf Warnungen auswirken. Sie können das Diagramm mit den Steuerelementen im Widget konfigurieren.
Aktive Warnungen mit Aufgaben	Zeigt die Anzahl aktiver Warnungen mit Aufgaben an. Sie können das Diagramm mit den Steuerelementen im Widget konfigurieren.
Top 10 aktive Warnungen	Zeigt die 10 Warnungen an, die während des Überprüfungszeitraums am aktivsten waren. Sie können das Diagramm mit den Steuerelementen im Widget konfigurieren.

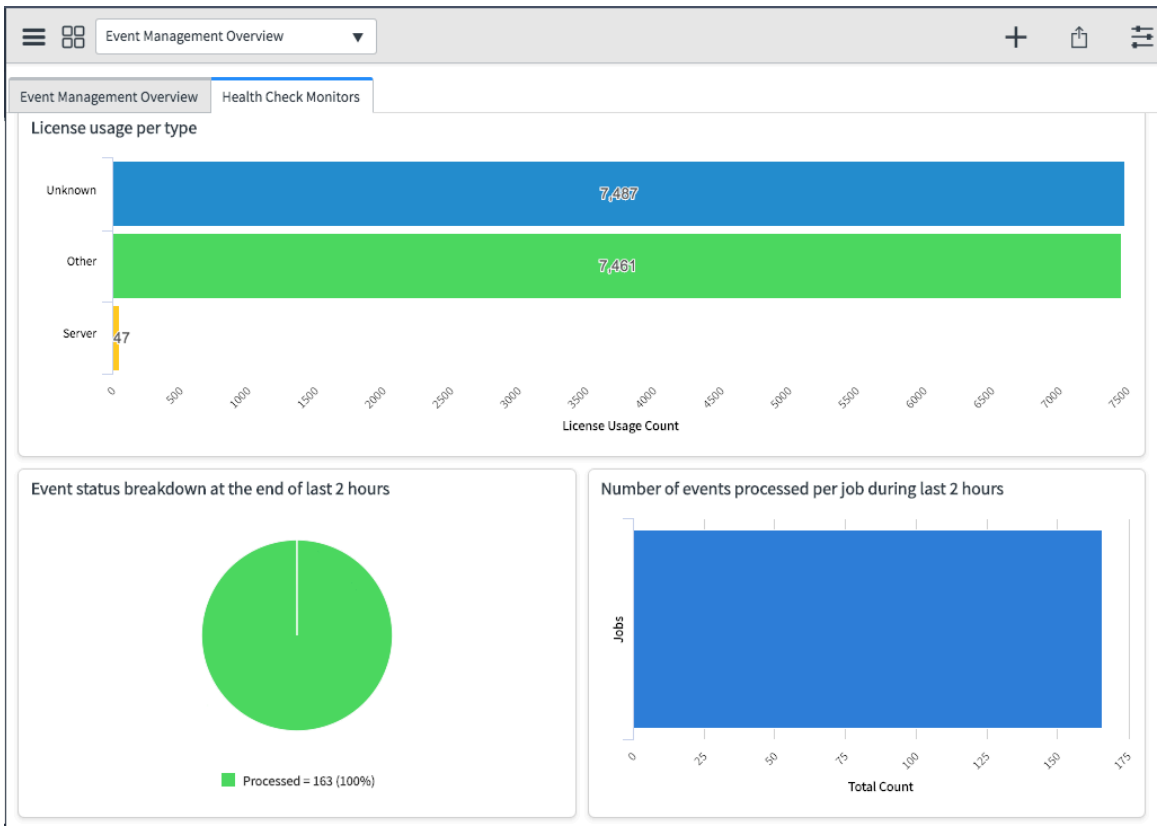


Registerkarte „Systemprüfungsüberwachung“

Standard-Widgets auf der Registerkarte „Systemprüfungsüberwachung“ sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Widget	Beschreibung
Lizenznutzung nach Typ	Zeigt die Anzahl der CIs und Knoten an, die für die Lizenznutzung gezählt wurden.
Event-Status-Aufgliederung am Ende der letzten 2 Stunden	Zeigt den Status von Events in den letzten 2 Stunden an. **Hinweis:** Wenn eine große Anzahl von Events vorhanden ist, ist dieser Bericht nicht verfügbar.
Anzahl der pro Auftrag in den letzten 2 Stunden verarbeiteten Events	Zeigt die Anzahl der pro Auftrag in den letzten 2 Stunden verarbeiteten Events



Webanwendungen aus einer Warnung starten

Sie können eine Webanwendung aus einer Warnung starten, wenn die in einer Warnungsaktionsregel festgelegten Bedingungen erfüllt sind.

Vorbereitungen

Erstellen und konfigurieren Sie eine Warnungsaktionsregel, damit sie eine URL vorbereitet, wenn die von Ihnen angegebenen Bedingungen erfüllt sind. Beispielsweise können Sie mit dieser Funktion abhängig von der Lösung der Warnungsparameter einen Artikel in der Knowledge Base öffnen oder eine URL erstellen.

Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator oder evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Klicken Sie mit der rechten Maustaste auf eine Warnung, und zwar unter „Alle Warnungen“ oder in der Liste der Warnungen im Dashboard Ereignismanagement (für Instanzen, die von einem Release vor Orlandoaktualisiert wurden). Wählen Sie anschließend **Schnelle**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Antwort aus. Klicken Sie auf den jeweiligen Link, um die in der Warnungsaktionsregel konfigurierte Webanwendung zu starten. Weitere Informationen finden Sie unter Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Alle Warnungen**.
2. Klicken Sie mit der rechten Maustaste auf die jeweilige Warnung, und wählen Sie die Option **Schnelle Antwort**.
   Ein Fenster wird angezeigt, das eine Liste der verfügbaren, in der Warnungsaktionsregel konfigurierten Webanwendungen sowie den der Warnung entsprechenden Filter enthält. Zeigen Sie zum Anzeigen der Ziel-URL auf den Cursor über dem Namen der Anwendung.

   Hinweis: Kann mindestens ein Parameter der Warnungsaktionsregel nicht gelöst werden, wird der zugehörige Anwendungsname schwarz angezeigt. Nach Lösung der Warnungsparameter wird der Anwendungsname zu einem Link.

3. Klicken Sie auf den Namen einer Anwendung, um die URL in Ihrem Browser zu öffnen (in einer neuen Registerkarte oder einem neuen Fenster).

Example:

Ein häufiger Anwendungsfall ist der Start im Kontext des Quellverwaltungssystems.
Zu anderen Beispielen zählt die Suche in Knowledge Bases, ob innerhalb von ServiceNow oder extern. Jede URL-basierte Aktion kann die Warnungsparameter verwenden, und die URLs können auf Wikis, Messaging-Services, REST APIs usw. verweisen.

Zugehörige Informationen

Migrieren einer Warnungsaktionsregel zu einer Warnungsverwaltungsregel

Schnelle Antworten in einer Warnung anwenden

Ereignismanagement Operator-Tutorial

Als Ereignismanagement Operator haben Sie die Aufgabe, Warnungen zu finden und zu analysieren sowie Aktionen zur Lösung des zugrunde liegenden Problems zu ergreifen.

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Tutorial durchlaufen

Bevor Sie als Operator arbeiten können, sollten Sie sich anhand des Tutorials mit verschiedenen Konzepten von Ereignismanagement vertraut machen, um zu verstehen, was Operatoren bei der täglichen Arbeit tun.

Starten Sie das Tutorial, indem Sie auf die erste Lektion klicken:

Lektion 1	Übersicht über Events und Warnungen
Lektion 2	Übersicht über die Anwendungsservices

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lektion 3	Ereignismanagement Operator-Arbeitsbereiche
Lektion 4	Was Operatoren tun

Eine Übersicht zu Warnungen für Ereignismanagement Operatoren

Als Ereignismanagement Operator müssen Sie wissen, wie eine Warnung aus einem Event generiert wird, worauf Sie bei Warnungen achten müssen und wie Warnungen gruppiert werden können.

Dies ist die erste Lektion im Ereignismanagement Tutorial.

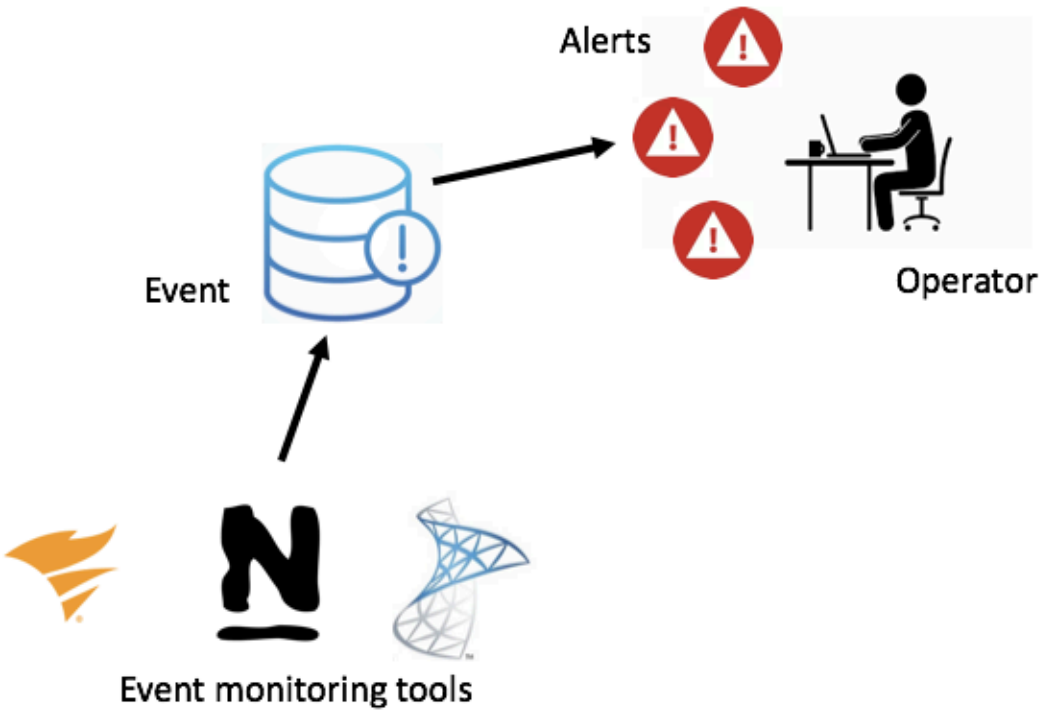
Lektion 1	○	**Übersicht über Events und Warnungen**
Lektion 2	○	Übersicht über die Anwendungsservices
Lektion 3	○	Ereignismanagement Operator-Arbeitsbereiche
Lektion 4	○	Was Operatoren tun

Ihre Organisation verfügt bereits über ein Tool für die Event-Überwachung, z. B. Microsoft System Center Operations Manager (SCOM), Nagios, SolarWinds usw. Wenn ein Problem in Ihrem Netzwerk auftritt, z. B. wenn ein Computer oder eine Datenbank ausfällt, senden die Event-Überwachungstools verschiedene Events an Ihre ServiceNow Instanz. Die Anwendung Ereignismanagement verarbeitet die Events gemäß den vom Administrator konfigurierten Einstellungen und generiert dann Warnungen. Eine Warnung ist ein Indikator dafür, dass Probleme eine Aktion erfordern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsgenerierung



Als Ereignismanagement-Bediener besteht Ihre Rolle darin, Warnungen anzuzeigen und je nachdem, wie Ereignismanagement in Ihrer Organisation implementiert ist, eine Aktion zur Behebung des zugrunde liegenden Problems durchzuführen oder jemanden zu diesem Zweck zu benachrichtigen. Später in diesem Tutorial werden die Phasen eines typischen Warnungsverwaltungsprozesses erläutert.

Warnungspriorität und Schweregrad

Die zwei häufigsten Merkmale einer Warnung sind Priorität und Schweregrad.

- Die Priorität einer Warnung ist eine Punktzahl, mit der Sie bestimmen können, wie wichtig die Auswirkung für Anwendungsservices ist. Mehrere Faktoren bestimmen die Prioritätspunktzahl der Warnung. Ihr Ereignismanagement Administrator kann den Algorithmus konfigurieren, den die Anwendung Ereignismanagement zur Berechnung der Priorität verwendet.
- Der Schweregrad einer Warnung ist ein Indikator dafür, wie schwerwiegend das zugrunde liegende Problem ist. Das Tool zur Event-Überwachung in Ihrer Organisation übermittelt normalerweise Schweregradwerte mit dem Event, die dann für die Warnung übernommen werden. Die folgenden standardmäßigen Typen von Schweregraden werden in diesem Tutorial vorgestellt:

Schweregrad	Beschreibung
Kritisch	Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schweregrad	Beschreibung
Schwerwiegend	Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung hat sich verschlechtert.
Geringfügig	Ein partieller, nicht kritischer Verlust der Funktionalität oder eine Leistungsverschlechterung ist aufgetreten.
Warnung	Aufmerksamkeit ist erforderlich, obwohl die Ressource noch funktionsfähig ist.
OK	Kein Schweregrad Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig.
Löschen	Die Warnung benötigt keine Aktion mehr.

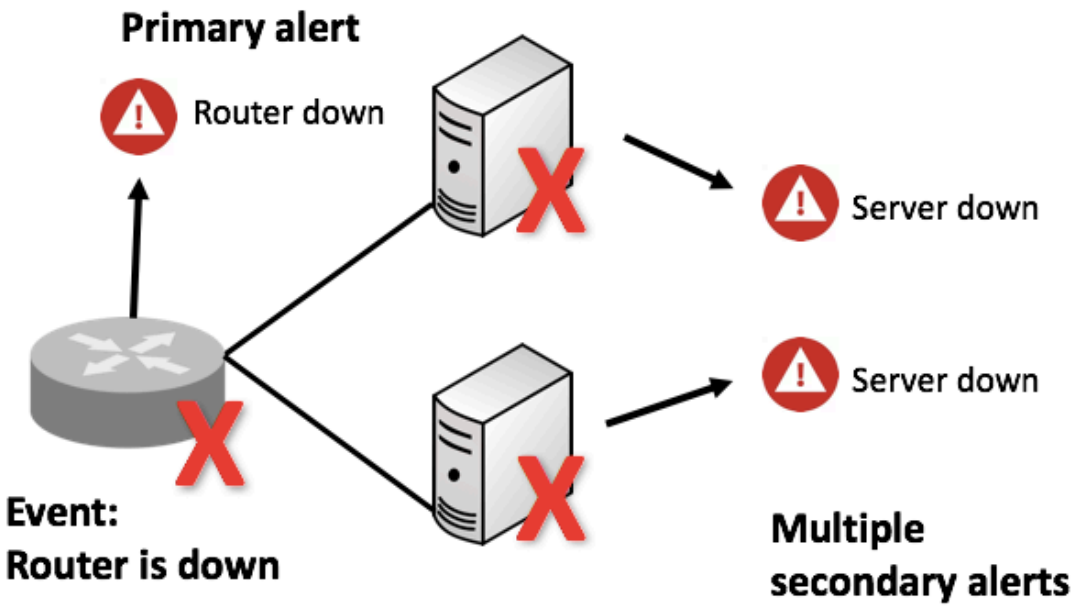
Korrelierte Warnungen

Einige Warnungen sind miteinander verknüpft. Wenn beispielsweise ein Router ausfällt, werden ggf. mehrere separate Warnungen generiert, eine für jeden mit dem Router verbundenen Server. Alle diese Warnungen sind miteinander verbunden oder korreliert. Um Sie bei der Verwaltung korrelierter Warnungen zu unterstützen, kann Ereignismanagement diese automatisch gruppieren. Dabei wird eine zweistufige Hierarchie eingerichtet, mit einer Stammwarnung, der so genannten primären Warnung, und anderen zugehörigen Warnungen, den sogenannten sekundären Warnungen. Wenn Sie Warnungen anzeigen, werden primäre Warnungen standardmäßig hervorgehoben. So wissen Sie immer sofort, auf welche Warnung Sie sich konzentrieren müssen, ohne von den sekundären Warnungen abgelenkt zu werden.

Wenn in unserem Beispiel ein Router in Ihrem Netzwerk ausfällt, ist die Netzwerkkommunikation auch für verbundene Server betroffen, vorausgesetzt, diese können keine anderen Router erreichen. Der Routerausfall wird zur primären Warnung, und die auf dem Server generierten Warnungen sind sekundäre Warnungen, die unter der Routerwarnung korreliert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sekundäre Warnungsgenerierung



Abhängig von der Ereignismanagement-Implementierung in Ihrer Organisation werden Warnungen ggf. automatisch gruppiert, und zwar abhängig von den vom Administrator eingerichteten Korrelationsregeln. Ihre Instanz kann auch lernen, wie sie die Korrelation von Warnungen basierend auf diesen Regeln verbessern kann. Als Operator sollten Sie dennoch stets die Genauigkeit der Korrelation verifizieren und bei Bedarf zusätzliche Warnungen manuell mit der primären Warnung korrelieren. Später im Tutorial erfahren Sie, wie Sie dies tun können.

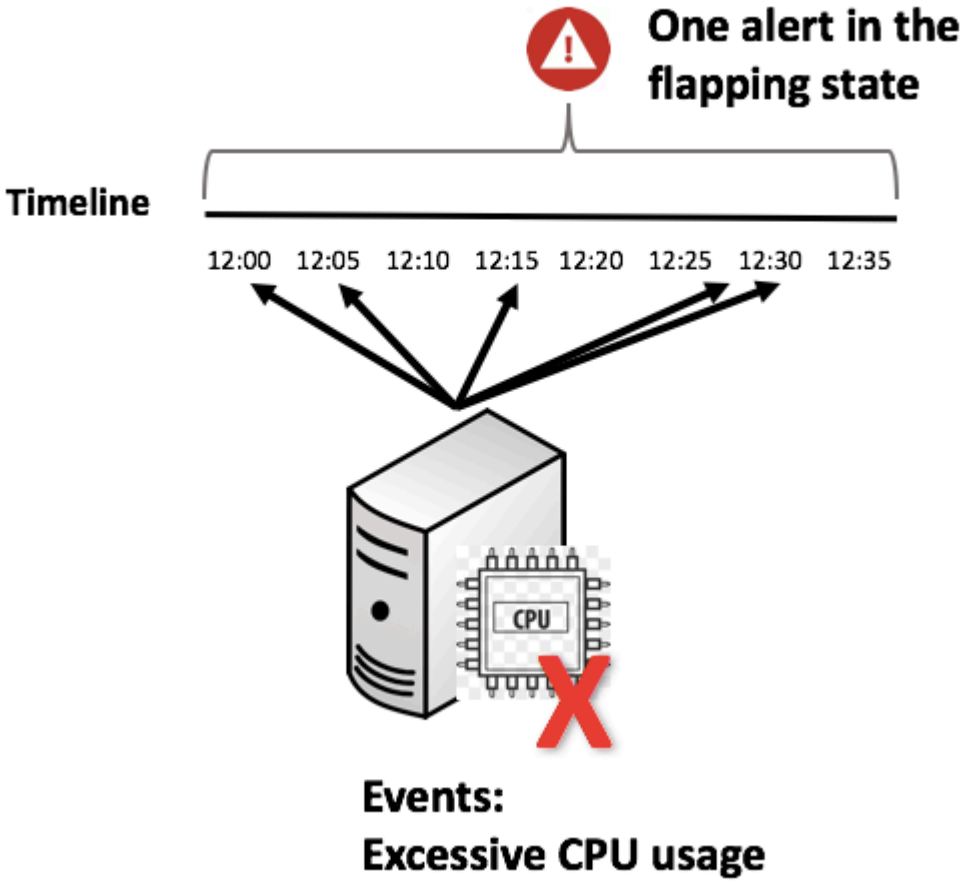
In diesem Tutorial erfahren Sie, wie Warnungen manuell korreliert werden.

Fluktuierende Warnung

Eine Warnung kann „flattern“, wobei sie in schneller Abfolge mehrere Ereignisse vom Typ „Öffnen“ / „Schließen“ erhält. Flattern weist darauf hin, dass Ereignismanagement nicht weiß, ob die zugrundeliegenden Events echt sind oder nicht. Die Events können auf kleine Probleme mit der CI-Konfiguration hindeuten, oder aber auf größere Probleme, z. B. einen Netzwerkausfall.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fluktuierende Warnung



Nehmen wir zum Beispiel einen Server an, der einen Webservice hostet. Wenn der Server zu viele aktive Prozesse aufweist, wird ggf. ein Event aufgrund übermäßiger CPU-Auslastung ausgelöst. Da die CPU-Auslastung je nach Web-Serviceanfragen schnell schwanken kann, werden eventuell mehrere Ereignisse ausgelöst, wodurch die Warnung in den Status „Fluktuierend“ versetzt wird. Als Operator müssen Sie möglicherweise einen Incident erstellen, um den Server neu zu starten; vielleicht muss auch die CPU neu konfiguriert oder eine Hardwareänderung am Gerät vorgenommen werden.

Ein weiteres Beispiel ist ein lockeres Netzwerkkabel, das vorübergehende, wiederholte Netzwerkausfälle verursacht. Die vom Administrator konfigurierten Schwellenwerte sind für diese Art von Warnung möglicherweise nicht optimal, daher geht Ereignismanagement von einer fluktuierenden Warnung aus.

Tutorial fortsetzen

Fahren Sie mit der nächsten Lektion fort: Anwendungsservices für -Operatoren Ereignismanagement ..

Anwendungsservices für -Operatoren Ereignismanagement .

Als Ereignismanagement -Operator müssen Sie verstehen, was Anwendungsservices sind.

Dies ist die zweite Lektion im Ereignismanagement Tutorial.

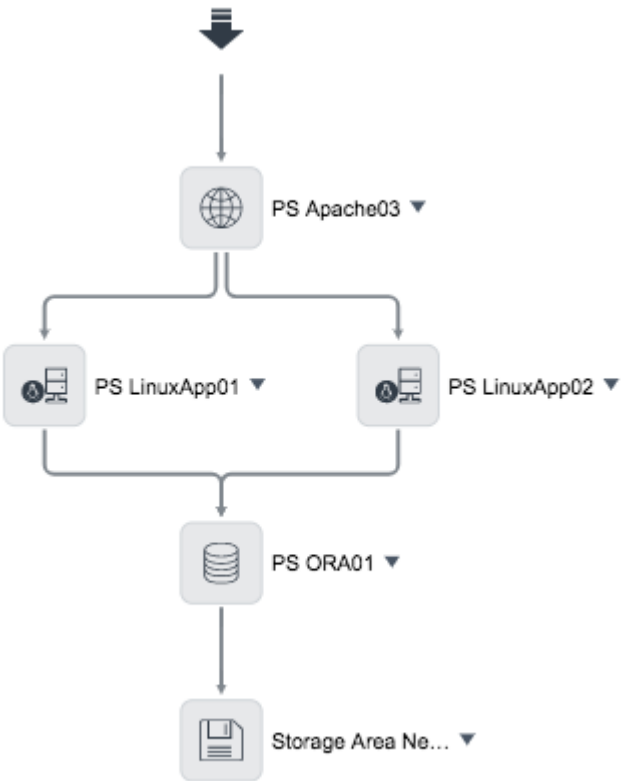
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lektion 1	✓	Übersicht über Events und Warnungen
Lektion 2	○	**Übersicht über die Anwendungsservices**
Lektion 3	○	Ereignismanagement Operator-Arbeitsbereiche
Lektion 4	○	Was Operatoren tun

Ein Anwendungsservice ist eine Sammlung von Komponenten, z. B. Netzwerkgeräten, Computern und Anwendungen, die Ihrer Organisation einen Service bieten. Bei den Services kann es sich um ein E-Mail-System handeln, oder um eine Website, die Bestellungen oder Anforderungen in einer Datenbank nachverfolgt. Ihr Administrator muss die Anwendungsservices bereits in Ihrer Instanz ServiceNow angegeben haben.

Jede Komponente, aus der ein Anwendungsservice besteht, wird als Konfigurationselement oder CI (Configuration Item) bezeichnet. Diese Servicezuordnung bietet eine visuelle Darstellung für einen Anwendungsservice:

Servicezuordnung



In diesem Beispiel sehen Sie einen Webportal Anwendungsservice mit diesen CIs:

- **PS Apache03**: Ein Apache-Webserver, der eine Unternehmenswebsite hostet.
- **PS LinuxApp01** und **PS LinuxApp02**: Zwei Linux-Server, welche sich die Arbeitsauslastung vom Webservers teilen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **PS ORA01**: Ein Datenbankserver, auf den beide Linux-Server zugreifen müssen.
- **Storage Area Network 001**: Massenspeichergerät, von dem andere CIs abhängen

Sie können solche Servicezuordnungen auf dem Dashboard „Service Operations Workspace“ sehen. Später in diesem Tutorial erfahren Sie mehr über das Dashboard und darüber, wie ein Anwendungsservice aussieht, wenn eine Warnung einem CI zugeordnet ist.

Arten von Anwendungsservices

Ereignismanagement klassifiziert Anwendungsservices in die folgenden Typen:

Technische Services

Ein technischer Service ist eine dynamische Gruppierung von CIs, die auf einigen allgemeinen Kriterien basiert. Beispielsweise kann ein technischer Service aus allen Webservern oder allen Oracle-Datenbanken für einen bestimmten Standort bestehen, z. B. Nordamerika.

Anwendungsservices

Ein Anwendungsservice kann aus erkannten Services und/oder manuellen Services bestehen. Ein erkannter Service ist ein Anwendungsservice, den die Anwendung Service-Mapping findet (wenn Ihre Organisation Service-Mappingverwendet). Ein manueller Service ist ein Anwendungsservice, den Ihr Administrator konfiguriert, indem er CIs auswählt bzw. hinzufügt und die Beziehungen zwischen CIs angibt.

Warnungsgruppen

Warnungen, die entweder manuell oder automatisch gruppiert werden.

Warnungsauswirkung

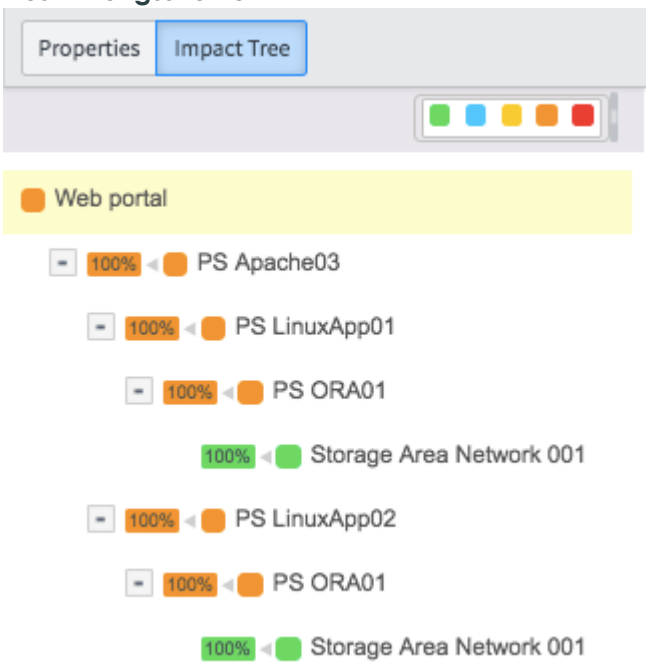
Anwendungsservices sind entscheidend für den Betrieb Ihrer Organisation. Wenn ein Problem bei einem CI auftritt, kann der gesamte Anwendungsservice betroffen sein. Ein Teil Ihrer Rolle als Operator besteht darin, Warnungen auf CIs zu analysieren und zu sehen, wie sie sich auf den Anwendungsservice als Ganzes auswirken. Dann ergreifen Sie eine Aktion, um das zugrunde liegende Problem zu korrigieren oder zu lösen. Ihr Administrator kann Auswirkungsregeln konfigurieren, welche in die Berechnungen zum Schweregrad einer Warnung einfließen.

Später erfahren Sie mehr darüber, wie Sie das Dashboard „Service Operations Workspace“ verwenden können. Dabei zeigen wir Ihnen, wie Sie eine Auswirkungsstruktur für einen Anwendungsservice anzeigen, um die Beziehung zwischen dem Schweregrad einer Warnung und dem gesamten Anwendungsservice zu verstehen.

In diesem Beispiel sehen Sie eine **schwerwiegende** Warnung zu einer Oracle-Datenbank (**PS ORA01**), die ebenfalls schwerwiegende Warnungen für die übergeordneten CIs und den Webportal Anwendungsservice auslöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auswirkungsstruktur



Tutorial fortsetzen

Fahren Sie mit der nächsten Lektion fort: Ereignismanagement Operator-Umgebung.

Ereignismanagement Operator-Umgebung

Als Ereignismanagement -Operator ist Dashboard „Service Operations Workspace“Ihre primäre Arbeitsumgebung.

In dieser dritten Lektion im Ereignismanagement Tutorial erhalten Sie einen Überblick über Ihre Arbeitsbereiche, um immer schnell die benötigten Informationen finden zu können.

Tutorial-Lektionen		
Lektion 1	✓	Übersicht über Events und Warnungen
Lektion 2	✓	Übersicht über die Anwendungsservices
Lektion 3	○	Ereignismanagement Operator-Umgebung
Lektion 4	○	Was Operatoren tun

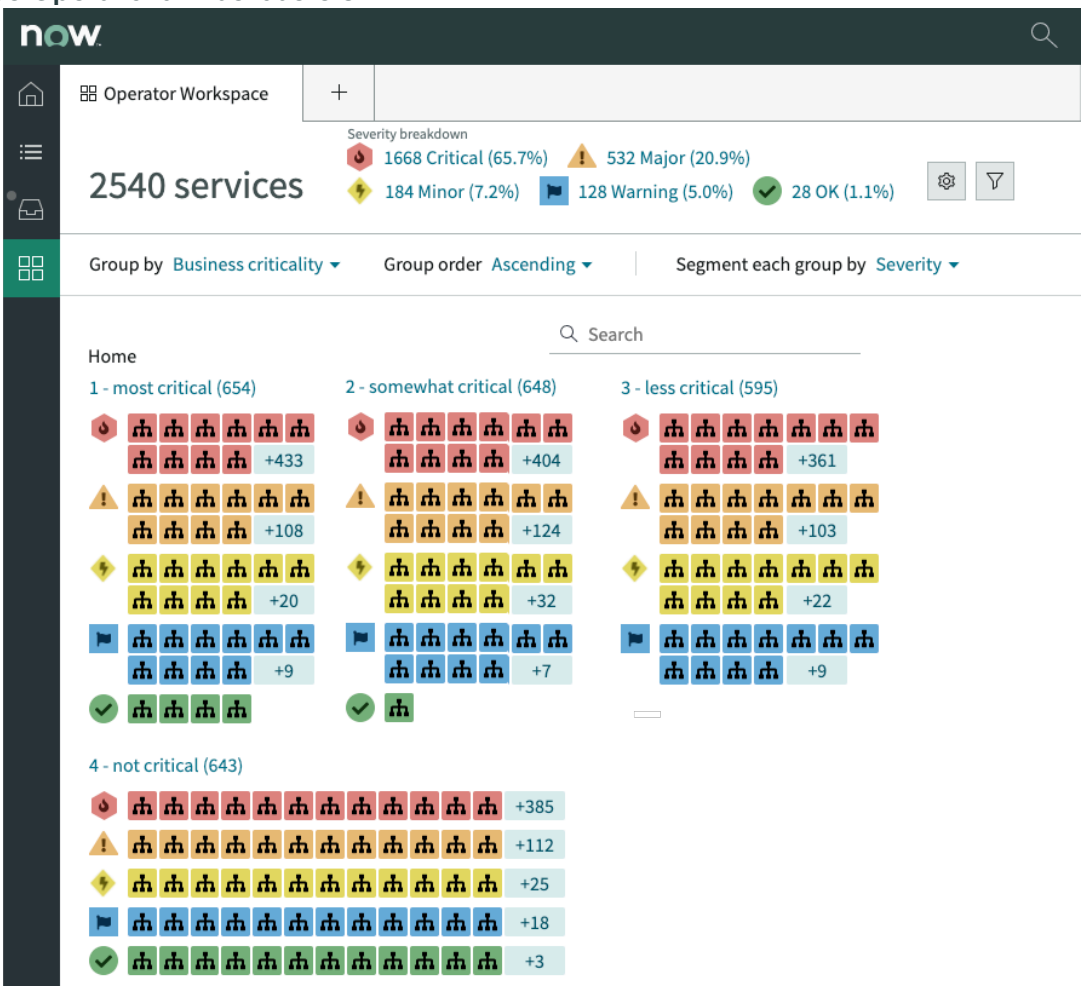
Dashboard „Service Operations-Arbeitsbereich“.

Ihr Hauptarbeitsbereich ist das Dashboard „Service Operations-Arbeitsbereich“, das eine Ansicht bietet, die sich auf die Beziehung von Warnungen zu Anwendungsservices konzentriert. Von hier aus können Sie Detailinformationen für die einzelnen Anwendungsservices anzeigen, um die betroffenen CIs anzuzeigen und sich ein Bild von den Gesamtauswirkungen der Ursache der Warnung zu machen. Um das Dashboard zu öffnen, wechseln Sie zu: **Ereignismanagement** > **Service Operations-Arbeitsbereich**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service Operations-Arbeitsbereich



Die Hauptbereiche des Dashboards sind:

Banner

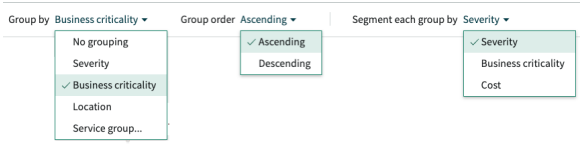
Das Banner enthält Steuerungen zum Ein- oder Ausblenden von Anwendungsservices basierend auf den von Ihnen ausgewählten Kriterien:

Klicken Sie auf einen Schweregrad, um Anwendungsservices basierend auf den ihnen zugeordneten Warnungen ein- oder auszublenden.

Verwenden Sie die Steuerungen **Gruppe** und **Segment**, um die Ansicht zu organisieren.

Hinweis: Ihr Administrator weist eine Anwendung den Kritikalitäts- und Kostenwert für Ihre Anwendungsservices zu.

Gruppen- und Segmentfilter



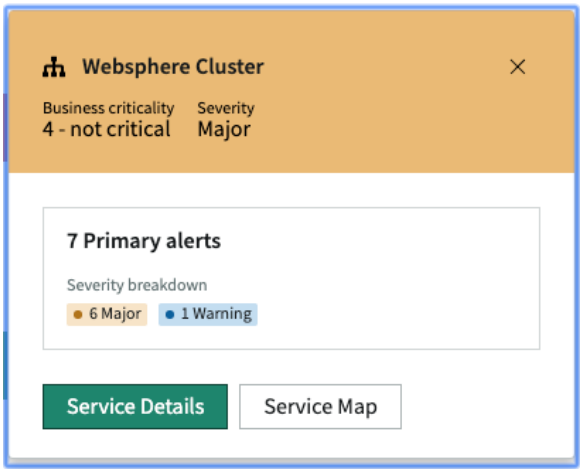
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungsservices

Dashboard „Service Operations Workspace“ zeigt Kacheln an, die Anwendungsservices darstellen. Die Farbe einer Kachel repräsentiert den Schweregrad der Warnungen, die dem Anwendungsservice zugeordnet sind.

Klicken Sie auf eine Kachel, um eine Zusammenfassung der Warnungen anzuzeigen, die mit dem Anwendungsservice verknüpft sind. Klicken Sie, um Details oder die Servicezuordnung anzuzeigen.



Warnungen

Klicken Sie auf das Listensymbol ( ). Klicken Sie auf der Registerkarte „Listen“ auf die anzuzeigende Warnung.

Sie können die Liste filtern oder sortieren, um eine bestimmte Warnung zu finden. Sortieren Sie nach beliebigen Warnungsdetails, z. B. nach **Priorität**. Dabei werden mehrere Faktoren für den **Schweregrad** der Warnung berücksichtigt; dieser Wert wird vom Tool für die Event-Überwachung bereitgestellt.

Öffnen Sie eine beliebige Warnung, indem Sie auf die Nummer klicken.

Bei der Analyse einer Warnung erfahren Sie später, was die einzelnen Spalten bei einer Warnung bedeuten.

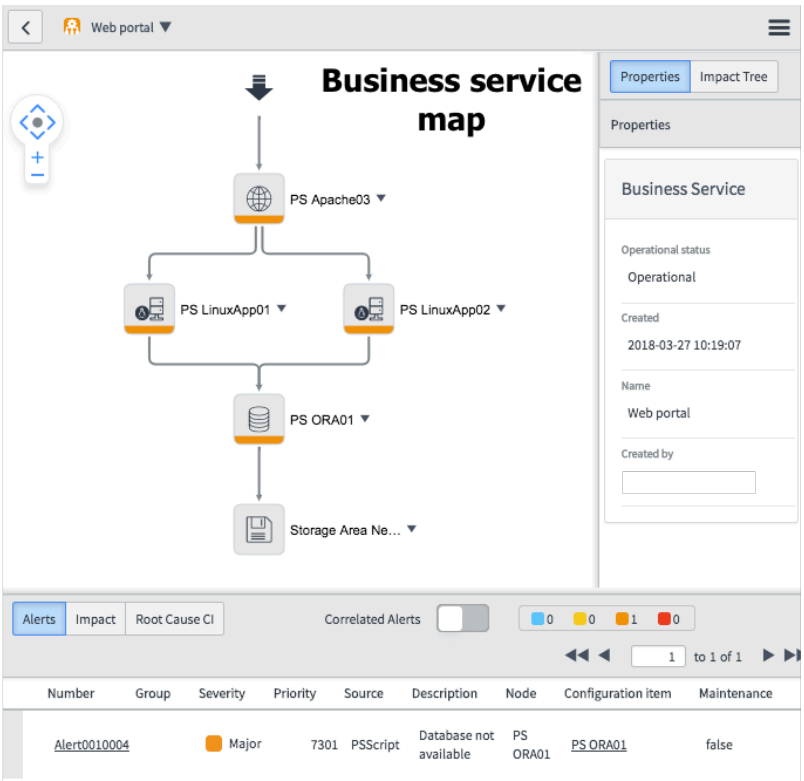
Anwendungsservice-Zuordnungsansichten im Dashboard „Service Operations-Arbeitsbereich“

Doppelklicken Sie auf den Namen einer Anwendungsservice-Kachel, um eine der Anwendungsservice-Zuordnungsansichten zu öffnen. Welche Ansicht angezeigt wird, hängt vom Anwendungsservice-Typ ab.

Automatische Übersetzung

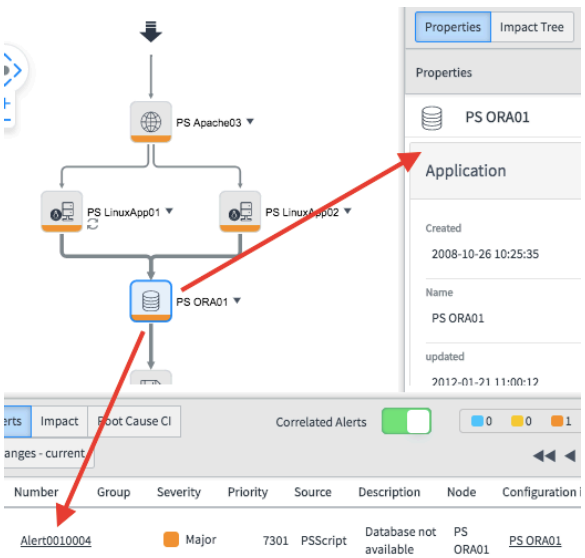
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für einen Anwendungsservice vom Typ manuell oder Standard wird diese Ansicht angezeigt:



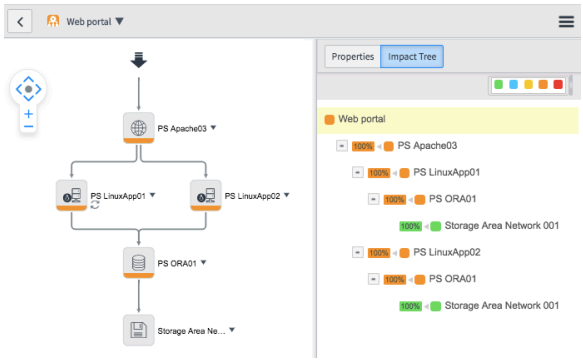
Die in einer vorherigen Lektion vorgestellte Anwendungsservicezuordnung wird im Hauptbereich angezeigt. Folgendes ist in dieser Ansicht möglich:

Klicken Sie auf eines der CIs, um nur Warnungen für dieses CI anzuzeigen, und die Details zu diesem CI im Bereich **Eigenschaften** anzuzeigen.



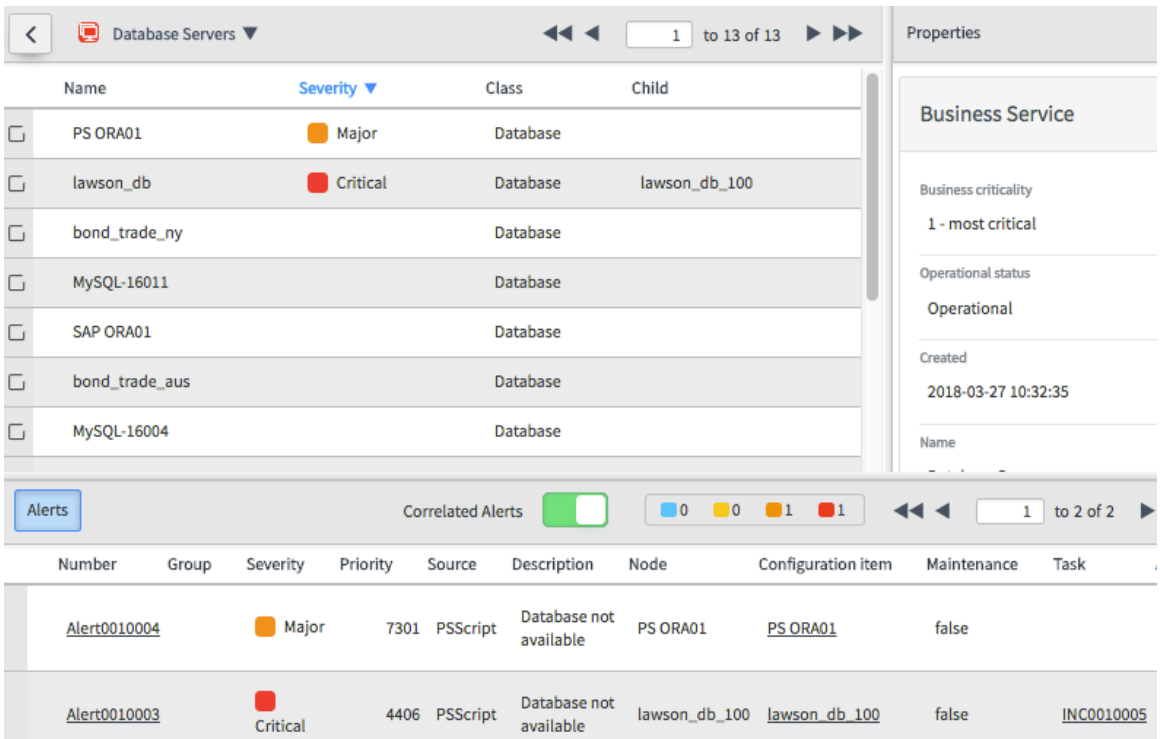
Klicken Sie auf **Auswirkungsstruktur**, um den Status aller CIs anzuzeigen sowie ihre Auswirkungen aufeinander beim Empfangen einer Warnung. Sie werden später im Tutorial mehr über die Auswirkungsstruktur erfahren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



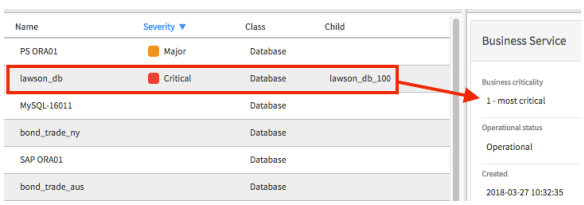
Öffnen Sie eine beliebige Warnung aus der Liste **Warnungen** unten, indem Sie auf die Nummer klicken.

Für einen technischen Anwendungsservice wird diese Ansicht angezeigt:



Folgendes ist in dieser Ansicht möglich:

Klicken Sie auf ein CI, um Details dazu anzuzeigen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Öffnen Sie eine beliebige Warnung aus der Liste **Warnungen** unten, indem Sie auf die Nummer klicken.

Tutorial fortsetzen

Fahren Sie mit der nächsten Lektion fort: Was Ereignismanagement Operatoren tun.

Was Ereignismanagement Operatoren tun

Als Operator Ereignismanagement umfasst Ihr typischer Workflow drei Phasen: Analyse einer Warnung und ihrer Auswirkungen auf Anwendungsservices, Durchführung einer Aktion und schließlich Sicherstellen, dass die Warnung geschlossen wird.

Dies ist die letzte Lektion im Ereignismanagement Tutorial. In dieser Lektion gehen wir die drei Phasen eines alltäglichen Operator-Workflows durch.

Lektion 1	✓	Übersicht über Events und Warnungen
Lektion 2	✓	Übersicht über die Anwendungsservices
Lektion 3	✓	Ereignismanagement Service Operations-Arbeitsbereich
Lektion 4	○	**Was Operatoren tun**

Ihre Organisation verfügt sicherlich über spezifische Richtlinien und Verfahren, die von den in diesem Thema beschriebenen Phasen abweichen können. Darüber hinaus hat Ihr Administrator möglicherweise die Anwendung Ereignismanagement angepasst, sodass einige dieser Phasen automatisiert sind, und von Ihnen keine Aktion erfordern.

Für die Zwecke dieses Tutorials führen wir Sie durch die einzelnen Phasen und ermöglichen Ihnen, die Aufgaben manuell auszuführen.

Phase 1	Warnungen analysieren und bestätigen	In dieser Phase finden Sie eine Warnung, die bearbeitet werden soll, analysieren die Details und bestätigen die Warnung, damit andere Operatoren wissen, dass es sich um eine gültige Warnung handelt.
Phase 2	Warnungen selektieren	In dieser Phase ergreifen Sie eine Aktion, um das Problem hinter der Warnung zu beheben. In den meisten Fällen werden Sie einen Incident erstellen und jemandem zuweisen, der das zugrunde liegende Problem lösen kann.
Phase 3	Warnungen schließen	In dieser Phase verifizieren Sie, ob die Warnung gelöst wurde, und schließen die Warnung anschließend.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beginnen Sie hier

Lernen Sie zunächst, wie Sie Warnungen analysieren und bestätigen.

Operator-Phase 1: Warnungen analysieren und bestätigen

Als Ereignismanagement Operator sollten Sie zuerst auf Warnungen zugreifen und dann diejenigen suchen, auf die Sie sich konzentrieren möchten. Sie können das Warnungsformular öffnen, um Details zu analysieren, und dann die Warnung bestätigen. So teilen Sie anderen Operatoren mit, dass das Problem hinter der Warnung in irgendeiner Weise behoben werden muss.

Vorbereitungen

Phase 1		**Warnungen analysieren und bestätigen**
Phase 2		Warnungen selektieren
Phase 3		Warnungen schließen

Sie müssen sich mit den Operatorumgebungen Dashboard „Service Operations Workspace“ und Service Operations-Arbeitsbereichauskennen. Überprüfen Sie Ereignismanagement Operator-Umgebung, falls noch nicht geschehen. Dieses Tutorial verwendet das Dashboard „Service Operations Workspace“.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

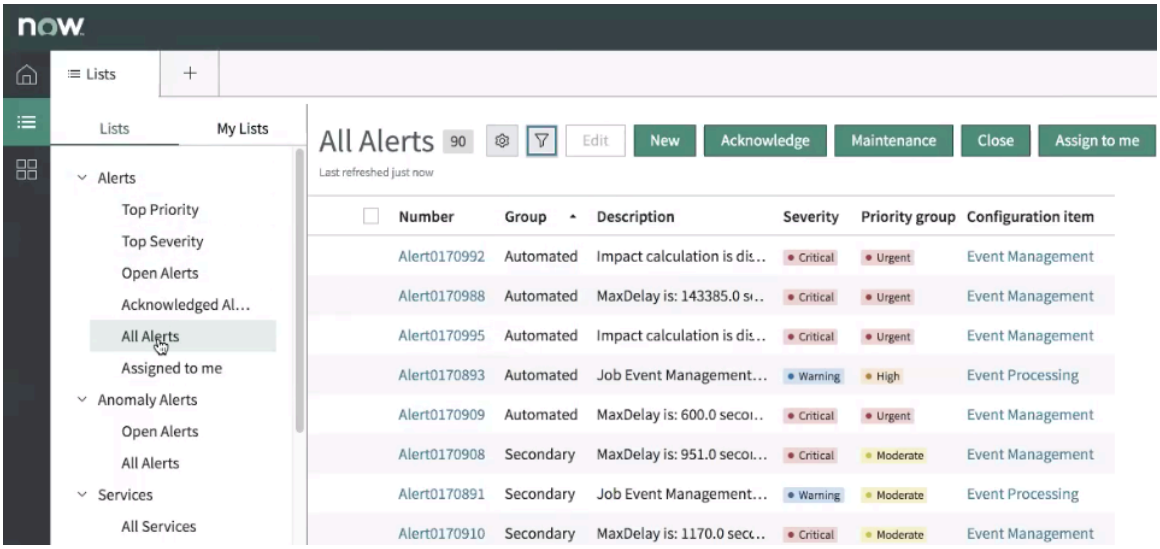
1. Navigieren zu **Ereignismanagement** > **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.

   Klicken Sie in der Liste auf **Warnungen** > **Alle Warnungen**. Standardmäßig werden alle Warnungen nach **Gruppe** sortiert in der Liste angezeigt. Klicken Sie auf eine beliebige Überschrift, um nach diesem Wert zu sortieren. Um die aktuellen Filtereinstellungen anzuzeigen, klicken Sie auf das Filtersymbol

   . Klicken Sie auf **Erweiterte Ansicht**, um die Filtereinstellungen zu ändern.

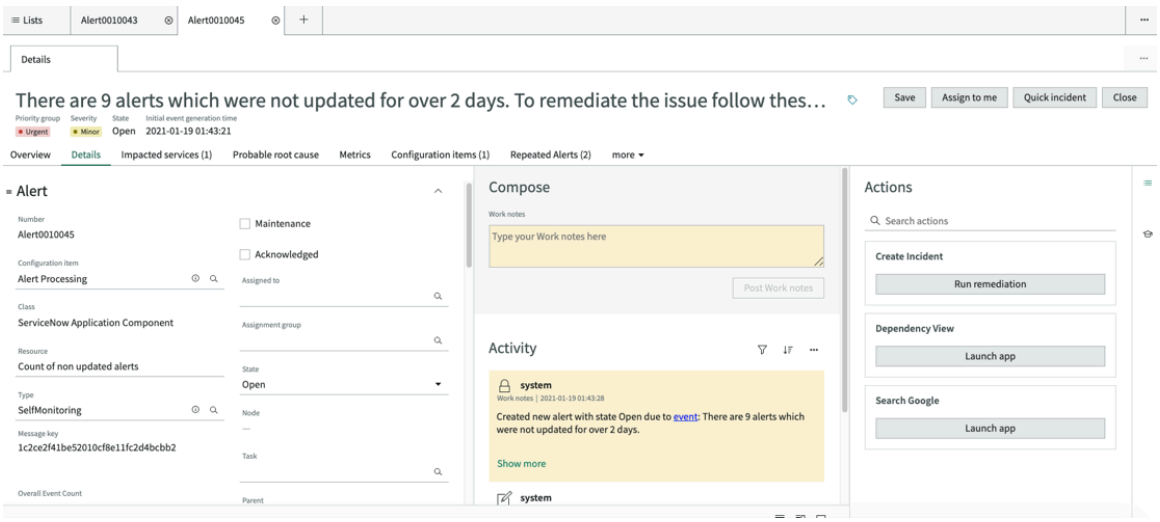
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Suchen Sie die Warnungen, auf die Sie sich konzentrieren möchten, indem Sie auf klicken **Anwendungsservices** > **Services**, oder verwenden Sie eine der Filter- und Sortieroptionen.
3. Klicken Sie auf einen Warnungsnamen, um die Registerkarte **Details** für diese Warnung zu öffnen.

Example
Die wichtigen Felder im Formular und zugehörige Elemente werden nach dem Screenshot beschrieben.



Felder auf der Registerkarte „Warnungsdetails“ für eine Warnung, die einem einzelnen CI zugeordnet ist

Feld	Beschreibung
Nummer	Die automatisch generierte Warnungsnummer, die Sie in der Liste der Warnungen unter Dashboard „Service Operations Workspace“gesehen haben.
Knoten	Der Name für das CI, dem die Warnung zugeordnet ist. Das Event hinter der Warnung ist auf diesem CI aufgetreten. Möglicherweise

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	wird ein Computername, eine IP-Adresse oder eine MAC-Adresse eines Geräts angezeigt.
Ressource	Das Objekt auf dem Knoten, welches das Event verursacht hat. Möglicherweise werden Werte angezeigt, wie der Name einer Festplatte, einer CPU oder eines Prozesses/Services. Bei Bedarf können Sie diesem Feld Informationen hinzufügen.
Konfigurationselement	Das CI in der CMDB, für das diese Warnung gilt Wenn dieses Feld leer ist, während das Feld **Knoten** ausgefüllt ist, und Sie wissen, welches CI der Knoten darstellt, können Sie das CI in dieses Feld eingeben, um die Warnung manuell zuzuordnen. **Hinweis:** Ihr Administrator kann Regeln konfigurieren, die CIs automatisch mit einer Warnung verknüpfen, für gewöhnlich basierend auf den Angaben im Feld **Knoten**. Unter Umständen findet das System aber nicht das richtige CI, an welches die Warnung gebunden werden soll. In diesem Fall müssen Sie möglicherweise manuell ein CI auswählen. Für die Zwecke dieses Tutorials gehen wir davon aus, dass das richtige CI mit der Warnung verknüpft ist. Wenn eine Warnung ein CI enthält, wird bei ihrer Auswahl die Registerkarte **Übersicht** geöffnet.
Aufgabe	Alle vorhandenen Aufgaben, die der Warnung zugeordnet sind, werden in diesem Feld angezeigt, z. B. Incidents, Change-Anforderungen oder Probleme. Wenn Sie eine Warnung zum ersten Mal betrachten, ist dieses Feld leer. Sie können eine Aufgabe zuordnen, wenn Sie die Warnung selektieren. Später in diesem Tutorial werden Sie einen Incident mit einer Warnung verknüpfen und den Incident jemandem zuweisen.
Beschreibung	Eine Beschreibung der Warnung, der von der Software für das Warnungsmonitoring in Ihrer Organisation stammt. Bei Bedarf können Sie Informationen hinzufügen.
Schweregrad	Schweregradwert für die Warnung: ◦ Kritisch: Es ist eine sofortige Aktion erforderlich. Entweder funktioniert die Ressource nicht, oder es drohen kritische Probleme. ◦ Schwerwiegend: Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung wurde beeinträchtigt. ◦ Gering: Es liegt ein partieller, nichtkritischer Verlust der Funktionalität vor, oder die Leistung hat sich verschlechtert. ◦ Warnung: Die Ressource funktioniert zwar noch, bedarf aber der Aufmerksamkeit. ◦ Info: Eine Informationsnachricht. Eine Warnung wird erstellt, die Ressource ist jedoch weiterhin funktionsfähig. ◦ Löschen oder Gelöst: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.

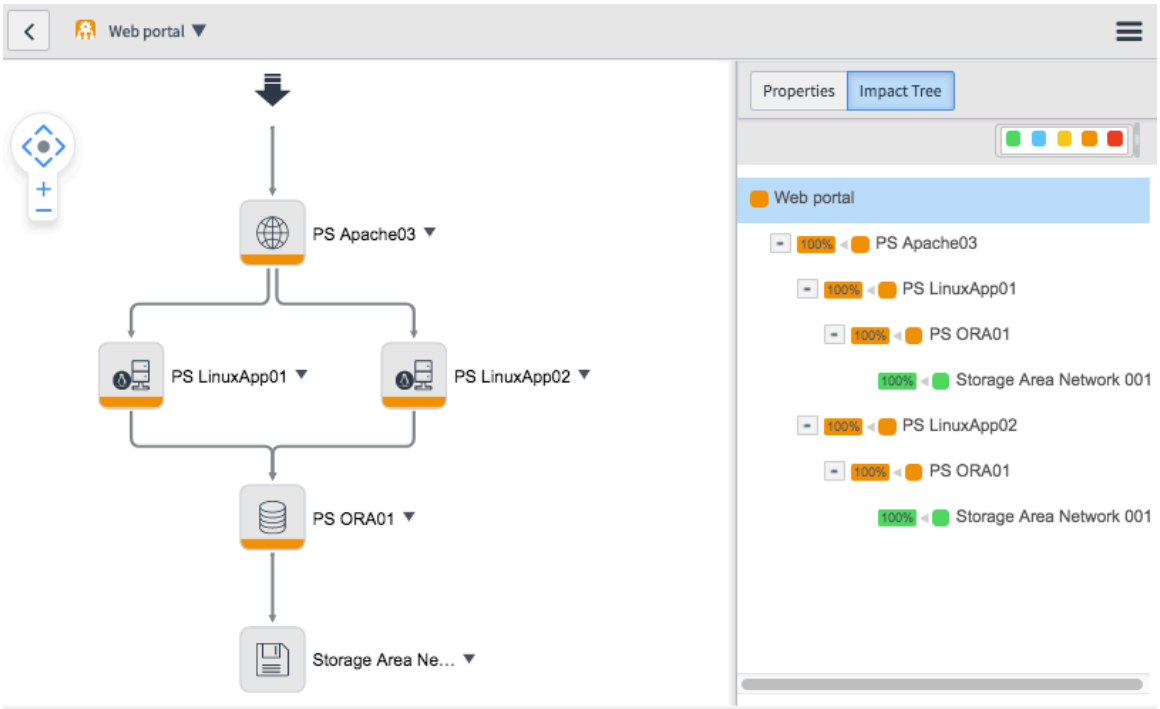
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Der Verarbeitungsstatus, in dem sich die Warnung befindet. Neu generierte Warnungen befinden sich im Status **Offen**. Andere Status sind: ◦ **Erneut öffnen** gibt an, dass eine zuvor geschlossene Warnung erneut geöffnet wurde und Ihre Aufmerksamkeit erfordert. ◦ **Flatternd** gibt an, dass die Warnung häufig identische Events aus der gleichen Quelle erhält. Dadurch werden viele Warnungen erneut geöffnet, nachdem sie geschlossen wurden. ◦ **Geschlossen** gibt an, dass die Warnung geschlossen wurde und keine weitere Aktion erfordert. In der letzten Phase dieses Tutorials werden Sie eine Warnung schließen.
Wartung	Gibt an, dass die Warnung nicht bearbeitet werden muss und in der Liste der Warnungen in Dashboard „Service Operations Workspace“ausgeblendet ist. In diesem Beispiel möchten wir die Warnung nicht in den Status „Wartung“ versetzen.
Bestätigt	Gibt an, dass ein Operator die Gültigkeit der Warnung verifiziert hat und sie derzeit selektiert. In einer späteren Phase in diesem Thema werden Sie eine Warnung bestätigen. Ihr Ereignismanagement Administrator kann Warnungen auch sofort automatisch bestätigen lassen, nachdem sie generiert wurden. In diesem Fall ist das Kontrollkästchen **Bestätigen** im Warnungsformular möglicherweise bereits aktiviert.
Übergeordnet	Zeigt nur für sekundäre Warnungen einen Wert an. Der Wert gibt die Warnungsnummer der übergeordneten Warnung an. Für primäre Warnungen (ohne übergeordnete Warnung) ist das Feld leer.
Wissensartikel	Alle vorhandenen Artikel in der Knowledge Base (KB), die der Warnung zugeordnet sind. Wenn Sie eine Warnung zum ersten Mal öffnen, ist dieses Feld leer. Sie können einen KB-Artikel zuordnen, wenn Sie die Warnung selektieren.

4. Klicken Sie auf die Registerkarte **Betroffene Services**, und klicken Sie dann auf den Servicenamen.
   Bevor Sie die Warnung bestätigen, möchten Sie ggf. mehr über die Services erfahren, die wegen dem Service hinter der Warnung betroffen sind.

   Der Service wird geöffnet und die Registerkarte **Details** wird angezeigt. Klicken Sie auf **Servicezuordnung**, um die Zuordnung der zugehörigen Anwendungsservices anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



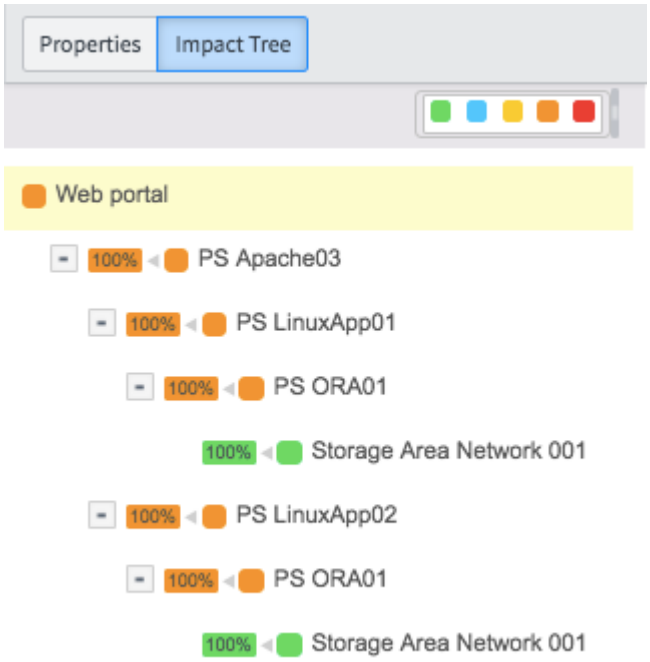
Beachten Sie, dass der Indikator für den Schweregrad „schwerwiegend“ für mehrere CIs in Orange angezeigt wird. Das beginnt mit der Oracle-Datenbank (**PS ORA01**) und wird an alle CIs weitergegeben, die von der Datenbank abhängen. Sie können also davon ausgehen, dass die Warnung mit dem höchsten Schweregrad in der Oracle-Datenbank die Ursache des Problems darstellt.

Das System hat nicht unbedingt separate Warnungen für jedes CI generiert, aber die Möglichkeit besteht. Bei der Selektierung einer Warnung können Sie ermitteln, ob Warnungen über andere CIs unter einer primären Warnung korreliert werden müssen.

5. Klicken Sie auf die Registerkarte **Auswirkungsstruktur** und überprüfen Sie die Auswirkungen auf die CIs.

   Die Prozentsätze neben jedem CI in der Auswirkungsstruktur zeigen die Auswirkung auf die einzelnen CIs an. In diesem Beispiel ist jedes CI zu 100 % von der Warnung betroffen. Das der Warnung zugrunde liegende Problem ist also schwerwiegend genug, um die Funktionalität vom Anwendungsservice zu beeinträchtigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Bestätigen Sie die Warnung.

Wenn Sie eine Warnung bestätigen, wird sie Ihnen nicht zugewiesen, und es wird keine Aufgabe erstellt (z. B. ein Incident oder eine Change-Anforderung). Durch die Bestätigung werden andere Operatoren darüber informiert, dass Sie von dem Problem wissen. Nachdem Sie eine Warnung bestätigt haben, ergreifen Sie während der Selektierungsphase weitere Aktionen.

Option	Bezeichnung
Einzelne Warnungen bestätigen	Mit diesem Prozess können Sie nur die Warnung bestätigen, die Sie gerade anzeigen. **a.** Öffnen Sie das Formular „Warnungsdetails“, wie zuvor beschrieben. **b.** Wählen Sie das Kontrollkästchen **Bestätigt** aus.
Eine oder mehrere Warnungen bestätigen	Mit diesem Prozess können Sie eine Warnung oder mehrere zugehörige Warnungen bestätigen. **a.** Öffnen Sie die Liste der Warnungen, wie zuvor beschrieben. **b.** Wählen Sie alle zu bestätigenden Warnungen aus. **c.** Klicken Sie auf **Bestätigen**.

7. Navigieren Sie zurück, und suchen Sie nach der Warnung, die Sie bestätigt haben. Wie Sie sehen, hat **Bestätigt** den Wert **true**.

Number	Group	Severity ▲	Priority	Source	Description	Node	Configuration item	Maintenance	Task	Acknowledged
Alert0010002		Major	3301	SolarWinds	Database issue	PS ORA01	PS ORA01	false		true

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Gehen Sie zu Operator-Phase 2: Warnungen selektieren.

Operator-Phase 2: Warnungen selektieren

Nachdem Sie eine Warnung analysiert und bestätigt haben, müssen Sie diese selektieren. In der Selektierungsphase verifizieren Sie die Korrelation von Warnungen und ergreifen eine Aktion, um das Problem hinter der Warnung zu beheben. In diesem Thema wird die häufigste Selektierungsaufgabe behandelt: Wie Sie einen Incident aus einer Warnung erstellen.

Vorbereitungen

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	○	**Warnungen selektieren**
Phase 3	○	Warnungen schließen

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Bevor Sie die Warnung bearbeiten, finden Sie heraus, ob andere Warnungen mit der überprüften Warnung verknüpft werden müssen:

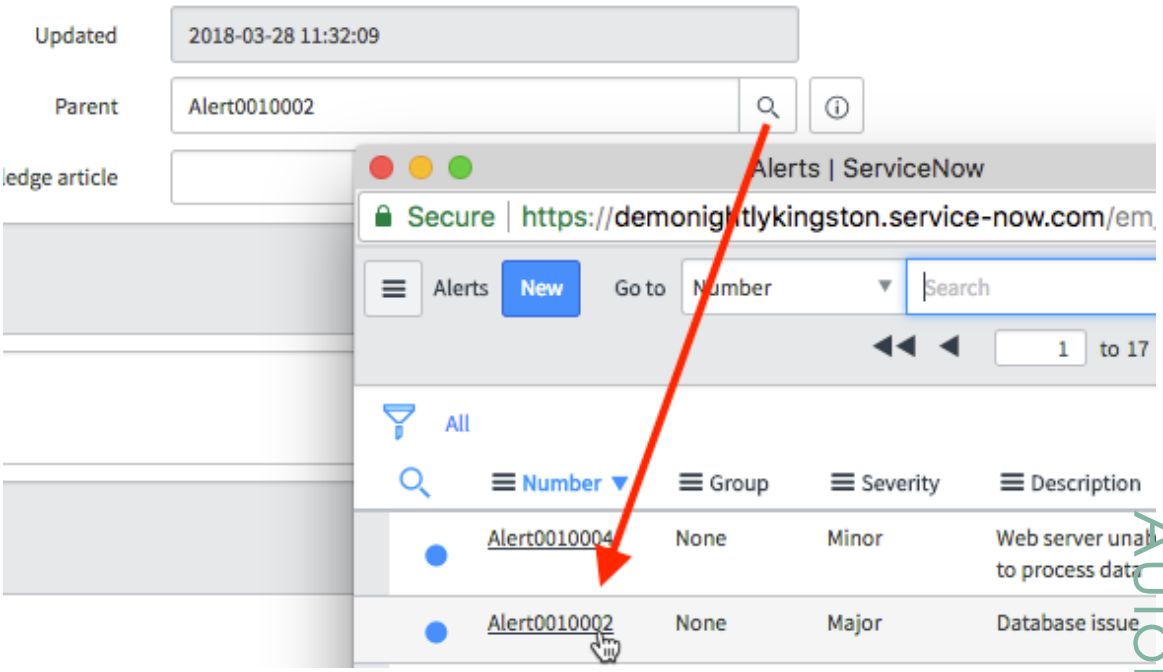
   a. Navigieren zu **Ereignismanagement** > **Service Operations-Arbeitsbereich**.

   b. Klicken Sie auf dieselbe Anwendungsservice Kachel, und überprüfen Sie die Warnungen in der Liste **Warnungen**.

   c. Wenn mehrere Warnungen vorhanden sind, öffnen Sie eine davon. So können Sie bestimmen, ob sie mit der anderen Warnung verknüpft ist, oder ob das zugrunde liegende Problem in beiden Warnungen gleich ist.
   Nehmen wir zum Beispiel an, dass eine Warnung einem Webserver zugeordnet ist, und bereits eine Warnung für das Datenbankproblem vorliegt. Korrelieren Sie in diesem Fall die Webserver-Warnung als sekundäre Warnung mit der Datenbank-Warnung als primäre Warnung.

   d. Öffnen Sie die sekundäre Warnung, klicken Sie auf das Suchsymbol (🔍) im Feld **Übergeordnet**, und wählen Sie dann die primäre Warnung aus.
   Dadurch wird eine Beziehung vom Typ „primär (übergeordnet) / sekundär (untergeordnet)“ zwischen den beiden Warnungen erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Wiederholen Sie diesen Vorgang, um so viele sekundäre Warnungen wie nötig zu korrelieren.

f. Navigieren Sie zurück zu Dashboard „Service Operations Workspace“, um zu verifizieren, dass für die primäre Warnung ein Symbol in der Spalte **Gruppe** angezeigt wird.

Hinweis: Ihr Administrator kann Regeln einrichten, mit denen das System automatisch Warnungen korrelieren kann, sodass Sie dies nicht manuell tun müssen. In diesem Fall wird im Warnungsformular das Feld **Feedback** angezeigt. Wählen Sie **Ja**, wenn das System die Warnung korrekt korreliert hat, andernfalls **Nein**. Derzeit ist die Feedback-Option verfügbar, löst jedoch nach der Protokollierung keine weiteren Aktionen aus.

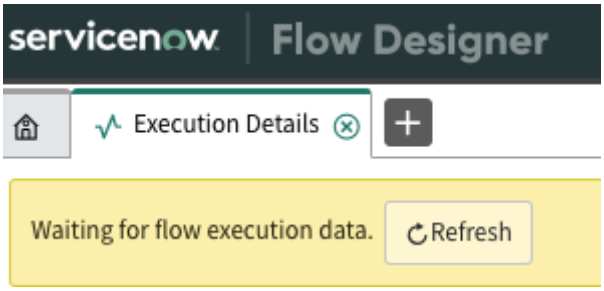
2. Öffnen Sie die primäre Warnung.

3. Klicken Sie im Warnungsformular auf **Aktionen** > **Incident erstellen**.
Wenn Ihre Organisation Security Incident Response verwendet, ist die Schaltfläche stattdessen **Security Incident erstellen**.

Der Flow Designer wird geöffnet.

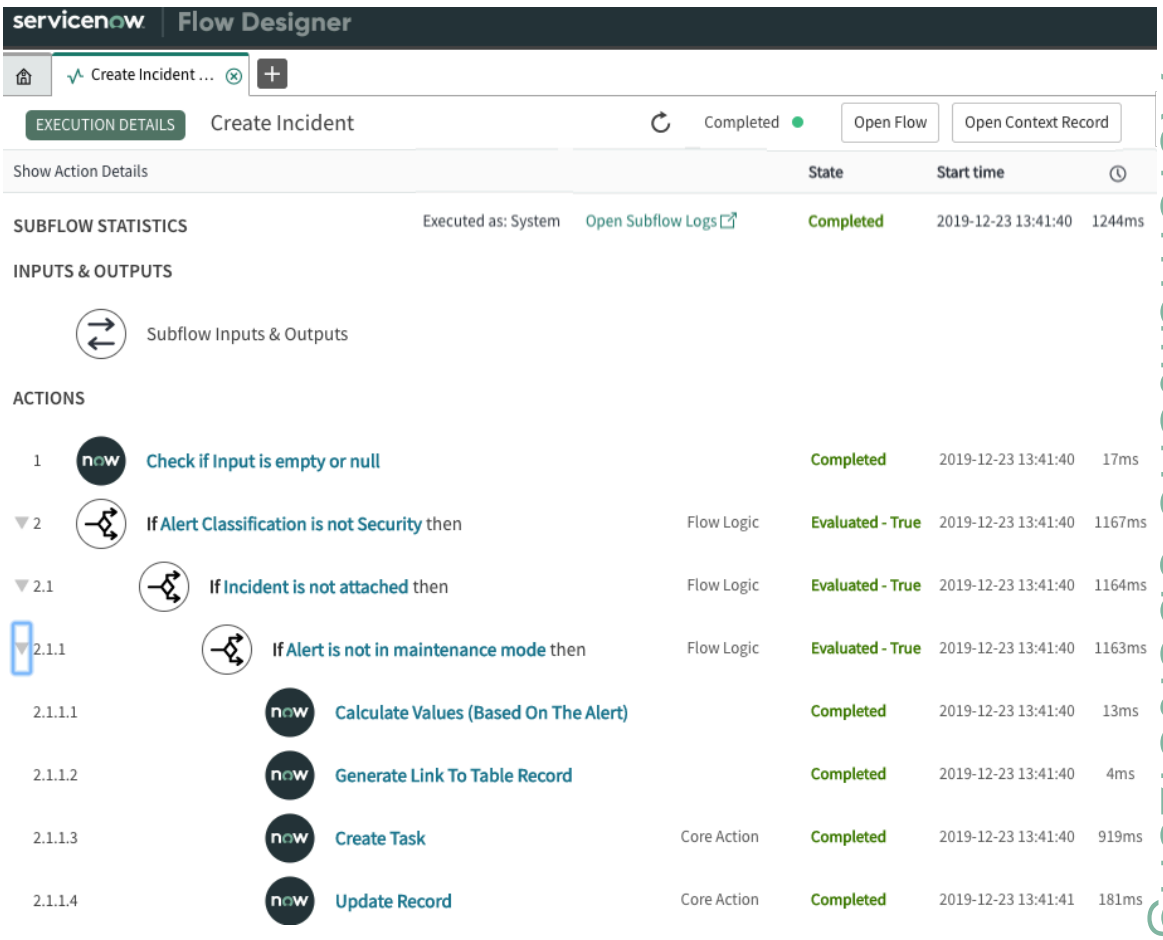
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Klicken Sie auf **Aktualisieren**.

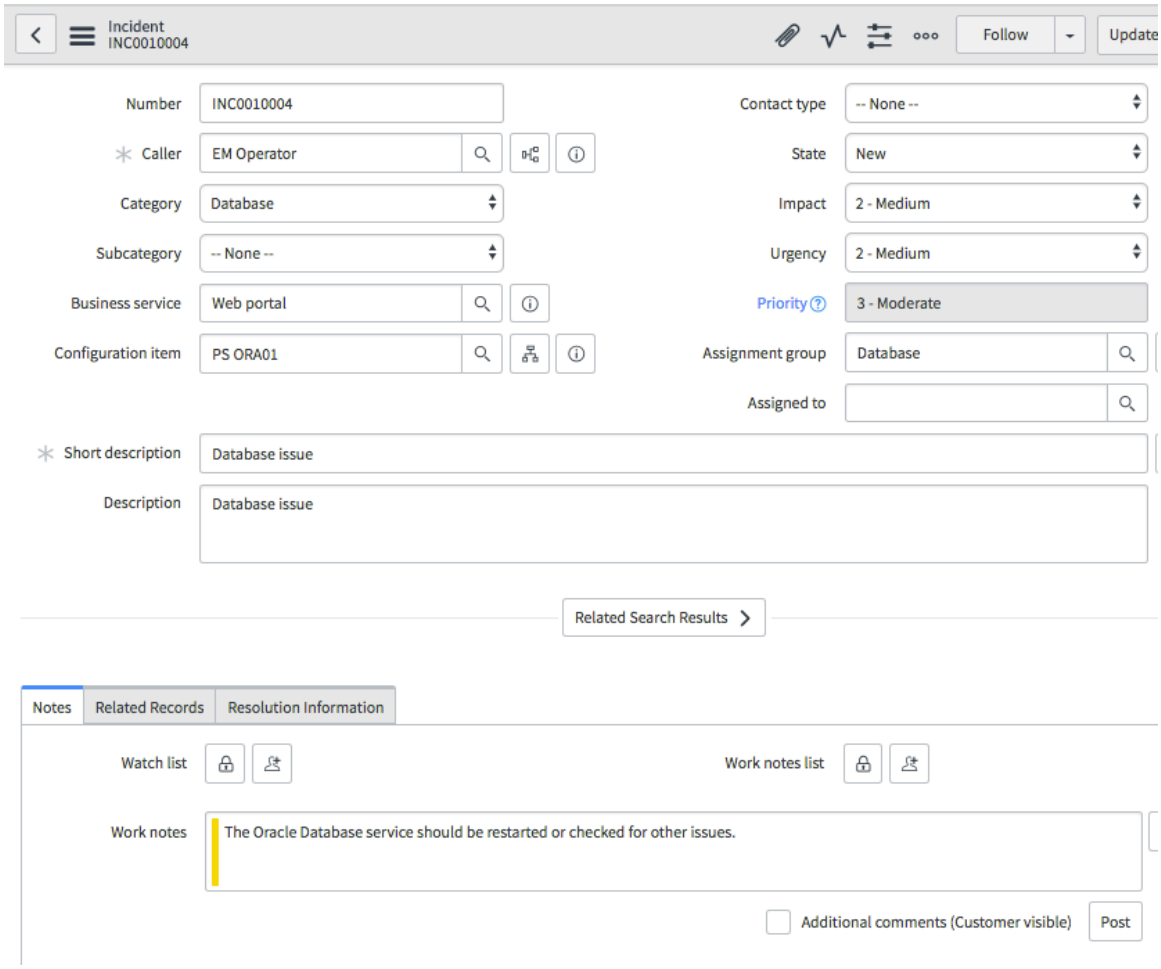
   Die Seite **Ausführungsdetails** wird geöffnet.



5. Klicken Sie auf **Kontextdatensatz öffnen** und füllen Sie das Incident-Formular aus.

Automatische Übersetzung

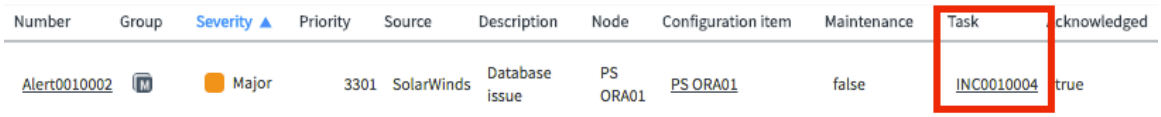
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
Anrufer	Klicken Sie auf das Suchsymbol ( ), und wählen Sie Ihren Namen aus. Der Anrufer ist die Person, die das Problem hinter dem Incident entdeckt hat.
Kategorie und Unterkategorie	Wählen Sie eine Kategorie aus, die diese Warnung am besten beschreibt. In diesem Beispiel ist **Datenbank** die beste Wahl.
Anwendungsservice	Wählen Sie das Anwendungsservice aus, zu dem das CI gehört. In diesem Beispiel ist Anwendungsservice ein **Webportal**.
Konfigurationselement	Wenn es noch nicht ausgefüllt ist, wählen Sie das CI aus. In diesem Beispiel wird die Oracle-Datenbank (**PS ORA01**) automatisch in das Feld eingetragen.
Auswirkung und Dringlichkeit	Wählen Sie die Auswirkungs- und Dringlichkeitsstufen aus, die Sie für angemessen halten.
Zuweisungsgruppe Zugewiesen an	Klicken Sie auf die Suchsymbole ( ) für eines oder beide dieser Felder. Wählen Sie anschließend die Gruppe oder Person aus, die sich dem Problem annehmen soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Klicken Sie auf **Absenden**, um den Incident zu erstellen.
   Die von Ihnen bearbeitete Warnung wird erneut angezeigt. Im Warnungsformular wird der Incident im Feld **Aufgabe** ausgefüllt. Die Incident-Nummer wird auch in der Spalte „Aufgabe“ im Dashboard „Service Operations Workspace“ angezeigt.



Number	Group	Severity ▲	Priority	Source	Description	Node	Configuration item	Maintenance	Task	cknowledged
Alert0010002		Major	3301	SolarWinds	Database issue	PS ORA01	PS ORA01	false	INC0010004	true

Nächste Maßnahme

Es gibt noch andere Aufgaben, die Sie während der Selektierungsphase ausführen:

- Fehlerkorrektur-Workflows für eine Warnung ausführen, wenn Ihr Ereignismanagement Administrator bereits einen Workflow in Ihrer ServiceNow Instanz eingerichtet hat und Ihre Richtlinien das Auslösen aus der Warnung zulassen.
- Webanwendungen aus einer Warnung starten, um eine Website oder ein Tool für die Event-Überwachung aufzurufen und so mehr Informationen zur Warnung zu erhalten.
- Artikel in der Knowledge Base einer Warnung zuordnen, wenn Informationen zur Warnung vorhanden sind, die zur Behebung des zugrunde liegenden Problems beitragen könnten.
- Warnungen in den Status „Wartung“ versetzen, um sie vorübergehend für den Dashboard „Service Operations Workspace“ auszublenden, wenn für die Warnung zu diesem Zeitpunkt keine Aktion erforderlich ist.

Wenn Sie keine weiteren Selektierungsaktionen durchführen müssen, fahren Sie fort mit Phase 3: Warnungen schließen.

Fehlerkorrektur-Workflows für eine Warnung ausführen

Als Ereignismanagement Operator können Sie auch einen Workflow auf Ihrer ServiceNow Instanz ausführen, der Sie bei der Korrektur der Warnung unterstützt. Beispielsweise können Sie einen Workflow ausführen, um automatisch einen Server in Ihrem Netzwerk neu zu starten. Möglicherweise lässt sich so eine Warnung zur CPU-Auslastung lösen.

Vorbereitungen

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	○	**Warnungen selektieren**
Phase 3	○	Warnungen schließen

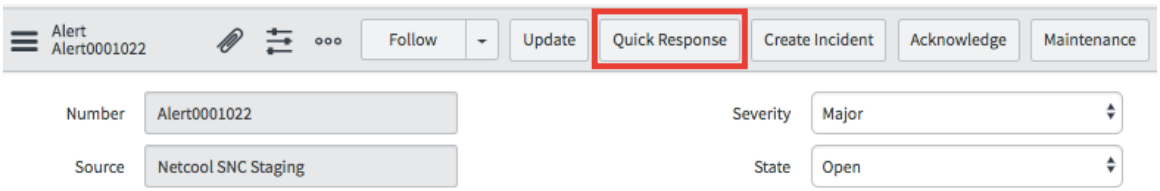
Hinweis: Sie können einen Fehlerkorrektur-Workflow ausführen, sofern Ihr Administrator bereits Workflows für Sie eingerichtet hat. Sicherlich sind Sie mit den Richtlinien Ihrer Organisation zur Selektierung von Warnungen vertraut.

Erforderliche Rolle: evt_mgmt_operator

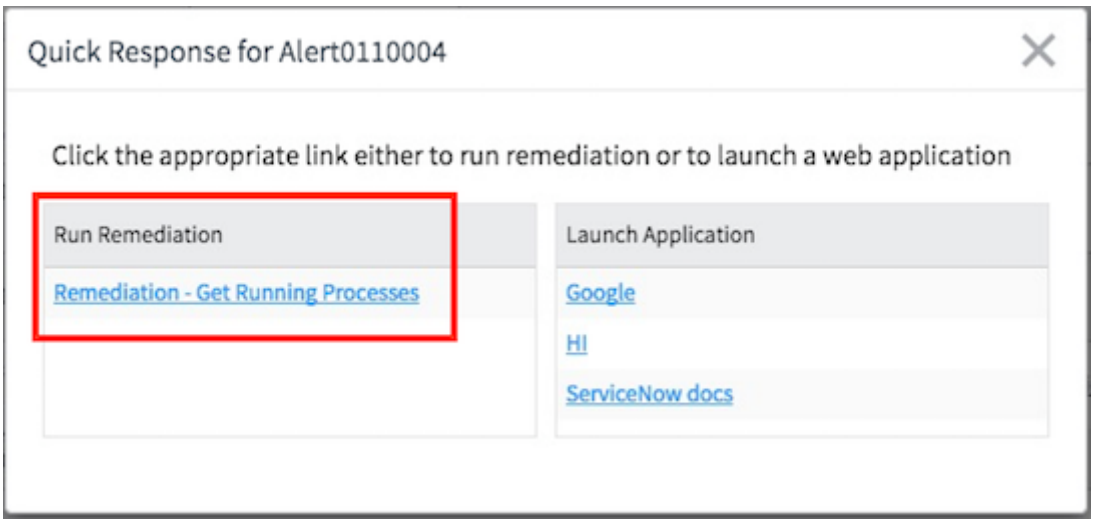
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie in Dashboard „Service Operations Workspace“die Warnung, die Sie in Phase 1: Analysieren bestätigt haben, und bestätigen Sie eine Warnung.
2. Klicken Sie im Warnungsformular auf **Schnelle Antwort**.



3. Klicken Sie im Fenster „Schnelle Antwort“ unter **Fehlerkorrektur ausführen** auf den Namen der Fehlerkorrektur.



Nächste Maßnahme

Es gibt noch andere Aufgaben, die Sie während der Selektierungsphase ausführen können:

- Webanwendungen aus einer Warnung starten, um eine Website oder ein Tool für die Event-Überwachung aufzurufen und so mehr Informationen zur Warnung zu erhalten.
- Warnungen in den Status „Wartung“ versetzen, um sie vorübergehend für den Dashboard „Service Operations Workspace“ auszublenden, wenn für die Warnung zu diesem Zeitpunkt keine Aktion erforderlich ist.
- Artikel in der Knowledge Base einer Warnung zuordnen, wenn Informationen zur Warnung vorhanden sind, die zur Behebung des zugrunde liegenden Problems beitragen könnten.

Wenn Sie keine weiteren Selektierungsaktionen durchführen müssen, fahren Sie fort mit Phase 3: Warnungen schließen.

Webanwendungen aus einer Warnung starten

Als Ereignismanagement Operator können Sie auch Webanwendungen aus einer Warnung starten. Die Webanwendung kann eine Konsole für das von Ihrer Organisation verwendete Tool für die Event-Überwachung oder eine externe Website sein, die zusätzliche Informationen zur Warnung bereitstellt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	○	**Warnungen selektieren**
Phase 3	○	Warnungen schließen

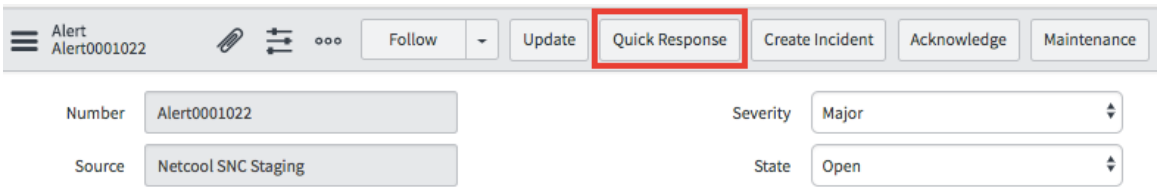
Erforderliche Rolle: evt_mgmt_operator

Sie können eine Webanwendung starten, wenn Ihr Administrator einen Link zur Anwendung eingerichtet hat. Sicherlich sind Sie mit den Richtlinien Ihrer Organisation zur Selektierung von Warnungen vertraut.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

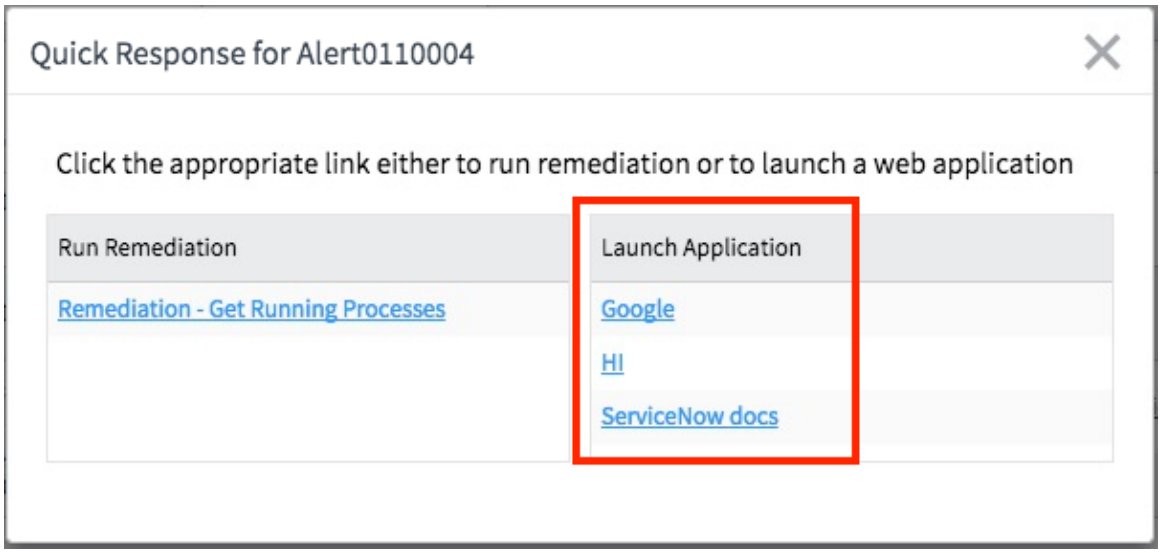
1. Öffnen Sie in Dashboard „Service Operations Workspace“die Warnung, die Sie in Phase 1: Analysieren bestätigt haben, und bestätigen Sie eine Warnung.
2. Klicken Sie im Warnungsformular auf **Schnelle Antwort**.



3. Klicken Sie im Fenster „Schnelle Antwort“ unter **Anwendung starten** auf den Namen der Anwendung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ihr Administrator hat festgelegt, welche Anwendungen in der Liste angezeigt werden sollen.



Nächste Maßnahme

Es gibt noch andere Aufgaben, die Sie während der Selektierungsphase ausführen können:

- Fehlerkorrektur-Workflows für eine Warnung ausführen, wenn Ihr Ereignismanagement Administrator bereits einen Workflow in Ihrer ServiceNow Instanz eingerichtet hat und Ihre Richtlinien das Auslösen aus der Warnung zulassen.
- Warnungen in den Status „Wartung“ versetzen, um sie vorübergehend für den Dashboard „Service Operations Workspace“ auszublenden, wenn für die Warnung zu diesem Zeitpunkt keine Aktion erforderlich ist.
- Artikel in der Knowledge Base einer Warnung zuordnen, wenn Informationen zur Warnung vorhanden sind, die zur Behebung des zugrunde liegenden Problems beitragen könnten.

Wenn Sie keine weiteren Selektierungsaktionen durchführen müssen, fahren Sie fort mit Phase 3: Warnungen schließen.

Artikel in der Knowledge Base einer Warnung zuordnen

Als Ereignismanagement Operator können Sie der Warnung einen Artikel aus der Knowledge Base (KB) zuordnen, um zusätzliche Informationen zur Warnung zu erfassen. Dazu können Verfahren gehören, die jemand befolgen muss, um das zugrunde liegende Problem in Ihrem Netzwerk zu beheben, oder Best Practices, um ein erneutes Auftreten des Problems zu verhindern.

Vorbereitungen

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	○	**Warnungen selektieren**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

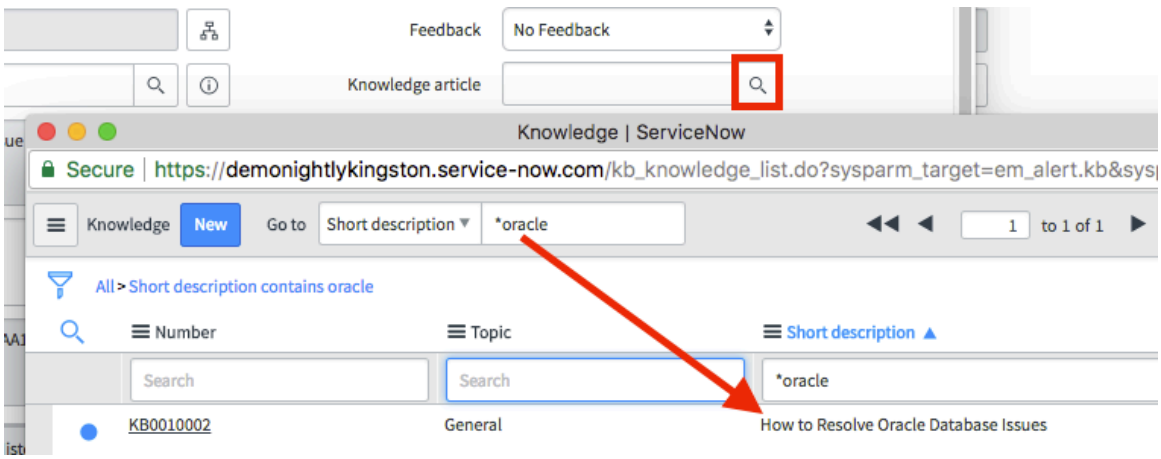
Phase 3 Warnungen schließen

Diese Aufgabe setzt voraus, dass Ihr Unternehmen die Knowledge Base-Anwendung in Ihrer ServiceNow Instanz verwendet.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Öffnen Sie in Dashboard „Service Operations Workspace“die Warnung, die Sie in Phase 1: Analysieren bestätigt haben, und bestätigen Sie eine Warnung.
2. Klicken Sie im Warnungsformular auf das Suchsymbol ( ) neben dem Feld **Wissensartikel**.
3. Filtern Sie die Liste der vorhandenen KB-Artikel, indem Sie zuerst ein Feld auswählen (z. B. **Kurzbeschreibung**) und dann zugehörigen Text in das Suchtextfeld eingeben.
   Mit dem Operator `enthält` (*****) können Sie nach Artikeln suchen, die Stichwörter enthalten. Nehmen wir z. B. an, dass Sie `*oracle` in die Kurzbeschreibung eingegeben haben. Dann werden die KB-Artikel gefiltert, die das Wort `oracle` in der Kurzbeschreibung enthalten.



4. Wenn Sie keine zugehörigen KB-Artikel finden, können Sie auf **Neu** klicken, einen neuen Artikel erstellen und dann auf **Senden** klicken.

   Die KB-Artikelnummer wird im Feld **Wissensartikel** im Warnungsformular angezeigt.

5. Klicken Sie im Warnungsformular auf **Aktualisieren**, um die Informationen zu speichern.

Nächste Maßnahme

Es gibt noch andere Aufgaben, die Sie während der Selektierungsphase ausführen können:

- Fehlerkorrektur-Workflows für eine Warnung ausführen, wenn Ihr Ereignismanagement Administrator bereits einen Workflow in Ihrer ServiceNow Instanz eingerichtet hat und Ihre Richtlinien das Auslösen aus der Warnung zulassen.
- Webanwendungen aus einer Warnung starten, um eine Website oder ein Tool für die Event-Überwachung aufzurufen und so mehr Informationen zur Warnung zu erhalten.
- Warnungen in den Status „Wartung“ versetzen, um sie vorübergehend für den Dashboard „Service Operations Workspace“ auszublenden, wenn für die Warnung zu diesem Zeitpunkt keine Aktion erforderlich ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie keine weiteren Selektierungsaktionen durchführen müssen, fahren Sie fort mit Phase 3: Warnungen schließen.

Warnungen in den Status „Wartung“ versetzen

Als Ereignismanagement Operator können Sie eine Warnung in den Status „Wartung“ versetzen, wenn keine weiteren Aktionen für die Warnung erforderlich sind, Sie diese jedoch weiterhin aktiviert halten möchten. Wenn Sie die Warnung in den Wartungsstatus versetzen, wird sie für Dashboard „Service Operations Workspace“ ausgeblendet, sodass andere Bediener nicht darauf zugreifen müssen. Die Warnung wird jedoch nicht geschlossen.

Vorbereitungen

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	○	**Warnungen selektieren**
Phase 3	○	Warnungen schließen

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Öffnen Sie in Dashboard „Service Operations Workspace“die Warnung, die Sie in Phase 1: Analysieren bestätigt haben, und bestätigen Sie eine Warnung.
2. Wählen Sie das Kontrollkästchen **Wartung** aus und klicken Sie auf **Aktualisieren**, oder klicken Sie oben in der Liste auf die Schaltfläche **Wartung**.
3. Klicken Sie auf **Aktualisieren**.
4. Navigieren zu **Ereignismanagement** > **Operatoren-Arbeitsbereich**.

   Beachten Sie, dass Warnungen im Status „Wartung“ standardmäßig nicht in der Liste angezeigt werden. Der Filter schließt Warnungen aus, bei denen `Wartung` | `=` | `true`.

Nächste Maßnahme

Wenn das Problem, das zu der Warnung geführt hat, später noch weiterer Aufmerksamkeit bedarf, navigieren Sie zu **Ereignismanagement** > **Alle Warnungen**, öffnen Sie die Warnung, deaktivieren Sie das Kontrollkästchen **Wartung**, und klicken Sie auf **Aktualisieren**. Von dort aus können Sie weitere Selektierungsaktionen ausführen.

Es gibt noch andere Aufgaben, die Sie während der Selektierungsphase ausführen können:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fehlerkorrektur-Workflows für eine Warnung ausführen, wenn Ihr Ereignismanagement Administrator bereits einen Workflow in Ihrer ServiceNow Instanz eingerichtet hat und Ihre Richtlinien das Auslösen aus der Warnung zulassen.
- Webanwendungen aus einer Warnung starten, um eine Website oder ein Tool für die Event-Überwachung aufzurufen und so mehr Informationen zur Warnung zu erhalten.
- Artikel in der Knowledge Base einer Warnung zuordnen, wenn Informationen zur Warnung vorhanden sind, die zur Behebung des zugrunde liegenden Problems beitragen könnten.

Wenn Sie keine weiteren Selektierungsaktionen durchführen müssen, fahren Sie fort mit Phase 3: Warnungen schließen.

Operator-Phase 3: Warnungen schließen

Nachdem Sie eine Aktion für eine Warnung ergriffen haben, können Sie mehrere Elemente in der Warnung überprüfen und diese dann schließen.

Vorbereitungen

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Phase 1	✓	Warnungen analysieren und bestätigen
Phase 2	✓	Warnungen selektieren
Phase 3	○	**Warnungen schließen**

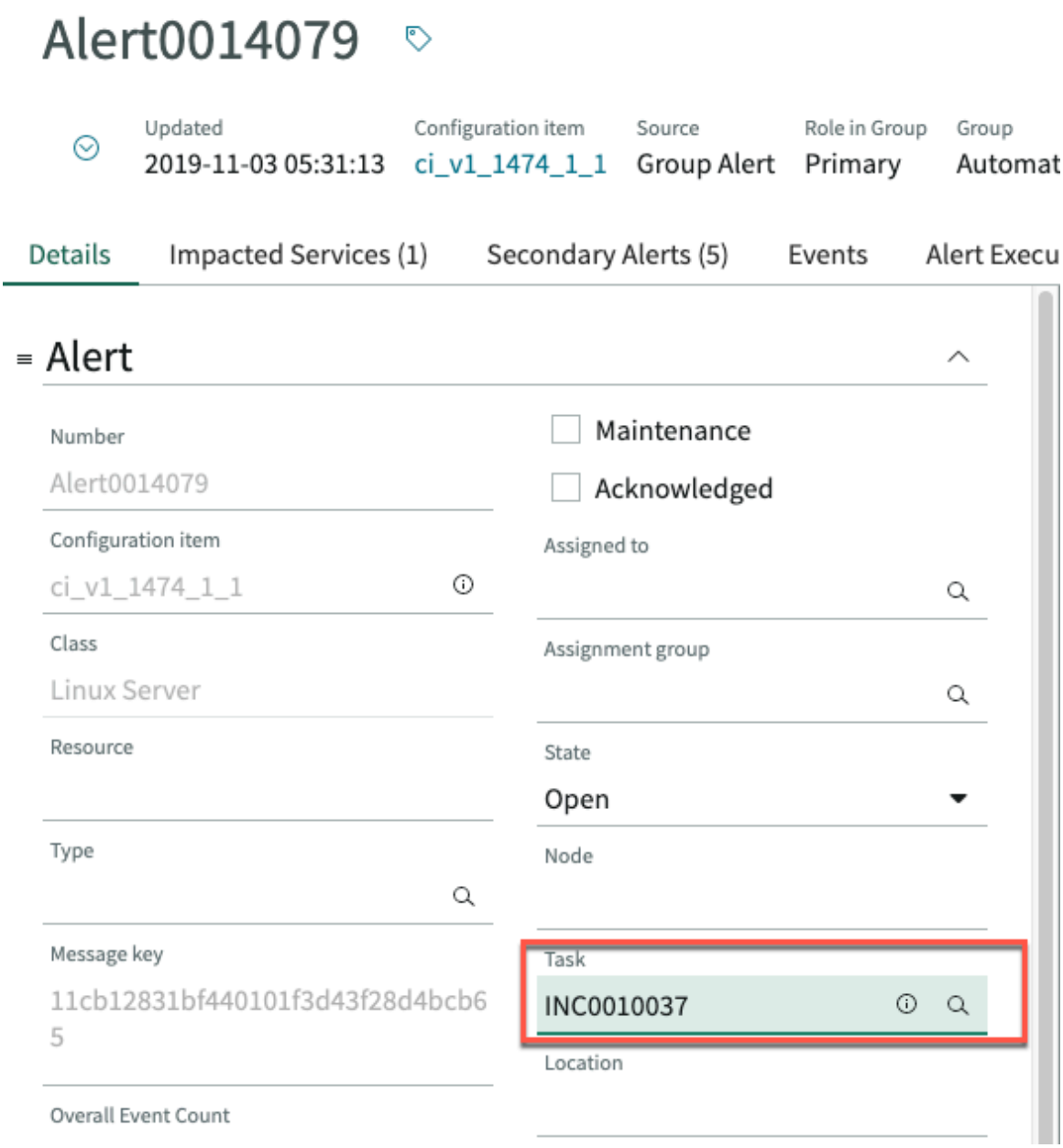
Erforderliche Rolle: evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Arbeitsbereicherfahrung** > **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Suchen Sie die Warnung, die Sie schließen möchten.
   Wird die Warnung nicht in der Liste angezeigt, z. B. weil sie sich im Status „Wartung“ befindet, ändern Sie nach Bedarf die Filteroptionen.
3. Klicken Sie auf die Warnungsnummer, um die Registerkarte „Warnungsdetails“ zu öffnen und wichtige Informationen zur Warnung zu überprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

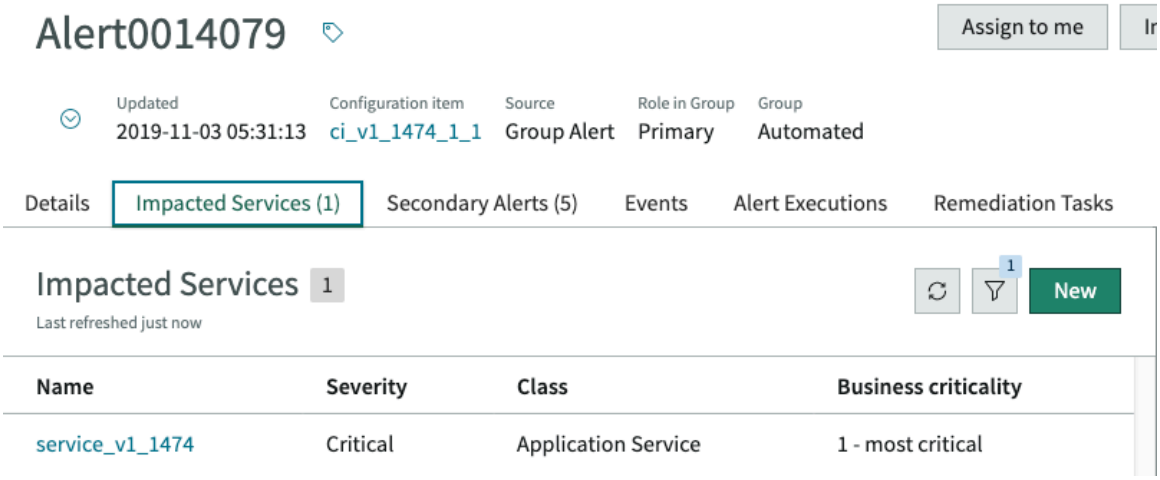


Automatische Übersetzung

4. Überprüfen Sie die Informationen zu Anwendungsservices auf der Registerkarte **Betroffene Services**.

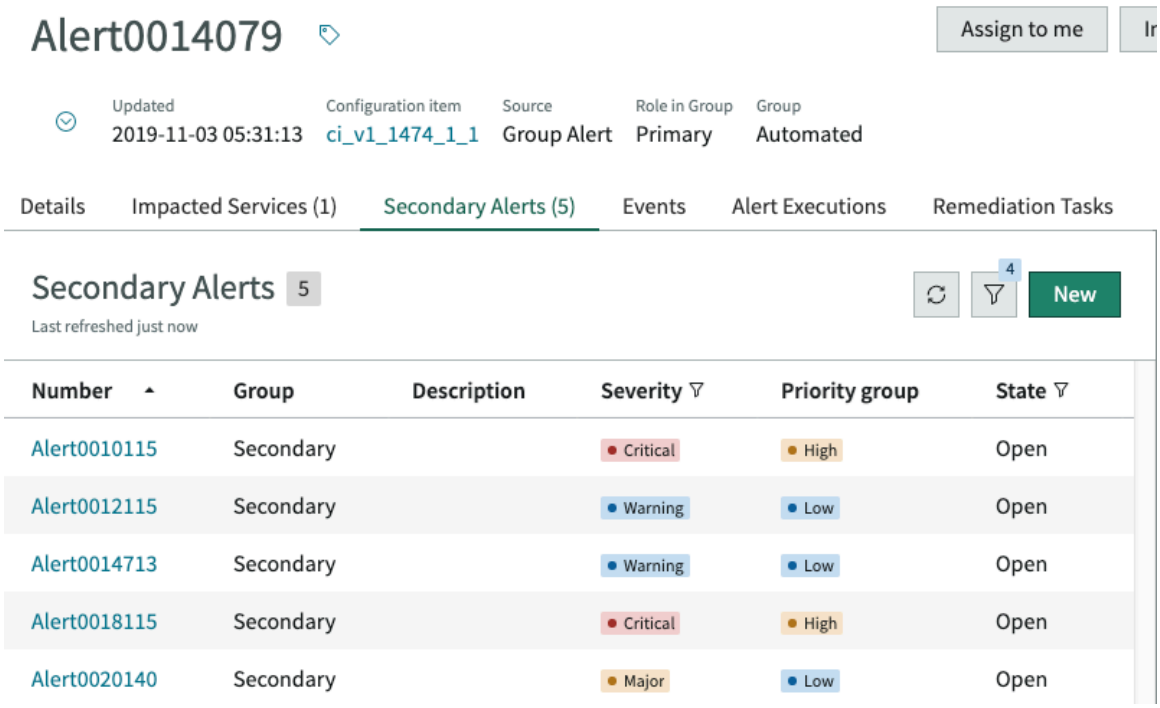
   In diesem Beispiel wird service_1474 Anwendungsservice in der Liste angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie weitere Informationen zu einem Anwendungsservice benötigen und die Servicezuordnung anzeigen möchten, klicken Sie auf den Servicenamen und dann auf **Servicezuordnung**.

5. Sehen Sie sich die zugehörigen Warnungen zu diesem Anwendungsservice an, und ändern Sie bei Bedarf die Korrelation.
   Der Prozess für eine primäre Warnung unterscheidet sich vom Prozess für eine sekundäre Warnung.
   - Bei einer primären Warnung werden alle sekundären Warnungen, die mit der primären Warnung korreliert sind, auf der Registerkarte **Sekundäre Warnungen** angezeigt.



Normalerweise müssen Sie nichts mit den sekundären Warnungen tun, es sei denn, Sie möchten weitere sekundäre Warnungen hinzufügen oder die Korrelation vollständig entfernen.

Hinweis: Wenn Sie eine primäre Warnung schließen, werden die sekundären Warnungen standardmäßig ebenfalls geschlossen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

◦ Bei sekundären Warnungen:

Die Warnungsnummer der primären Warnung wird im Feld **Übergeordnet** angezeigt. Sie müssen nichts mit der übergeordneten Warnung tun, es sei denn, Sie möchten die sekundäre Warnung mit einer anderen primären Warnung neu korrelieren. Sie können auch die Korrelation vollständig entfernen, indem Sie das Feld löschen.

Hinweis: Wenn Sie eine sekundäre Warnung schließen, wird die primäre Warnung standardmäßig nicht geschlossen. Sie müssen daher die primäre Warnung separat schließen.

6. Wenn Sie sicher sind, dass das dem Event zugrunde liegende Problem und die entsprechende Warnung behoben wurden, klicken Sie auf **Schließen**.
Wenn die Warnung Ihrer Meinung nach weitere Aufmerksamkeit erfordert, schließen Sie sie nicht. Versetzen Sie die Warnung stattdessen in den Status „Wartung“, indem Sie das Kontrollkästchen **Wartung** aktivieren.

Nächste Maßnahme

Sie haben das Ereignismanagement Operator-Tutorial abgeschlossen und dabei einen grundlegenden Workflow zum Analysieren, Selektieren und Schließen von Warnungen kennengelernt.

Nachdem Sie eine Warnung geschlossen haben, sind möglicherweise Aktionen für die folgenden Elemente erforderlich:

Warnungen erneut öffnen

Wenn eine Warnung Ihrer Meinung nach weitere Aktionen erfordert, können Sie ihren Status manuell in **Erneut öffnen** ändern. Wenn eine Warnung erneut geöffnet wird, werden zugeordnete Incidents gemäß ihrem Status und den vom Administrator festgelegten Regeln ggf. ebenfalls aktualisiert oder erneut geöffnet.

Hinweis: Jedes Mal, wenn Sie eine Warnung erneut öffnen, müssen Sie die Phasen „Selektierung“ und „Schließen“ erneut durchlaufen.

Warnungen im Status „Fluktuierend“ bearbeiten

In einigen Fällen kann dasselbe Event, das zur soeben geschlossenen Warnung geführt hat, in kurzer Zeit erneut ausgelöst werden, vielleicht sogar mehrmals. In diesem Fall wird der **Status** der soeben geschlossenen Warnung zunächst in **Erneut öffnen** und schließlich je nach vom Administrator konfigurierter Einstellung in **Flatternd** geändert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen dazu, wonach Sie suchen müssen, finden Sie unter Warnungen im Status „Fluktuierend“ bearbeiten.

Eine Zusammenfassung anderer Aufgaben, die Sie vielleicht bei Gelegenheit ausführen müssen, finden Sie unter Erweiterte Aufgaben für Ereignismanagement Operatoren.

Erweiterte Aufgaben für Ereignismanagement Operatoren

Als Ereignismanagement Operator müssen Sie möglicherweise zusätzliche Aufgaben ausführen, die außerhalb Ihres typischen Workflows liegen. Manche Aufgaben müssen Sie ggf. auch nur einmal ausführen.

Erweiterte Aufgabe	Beschreibung
Warnungslistenansichten anpassen	Greifen Sie so schnell wie möglich auf die zu analysierenden Warnungen zu.
Mit fluktuierenden Warnungen arbeiten	Wenn sich eine Warnung im Status „Fluktuierend“ befindet, tritt das zugrunde liegende Problem weiterhin auf. Sie müssen die Warnung erneut selektieren und nach einer anderen Lösung suchen.
Warnungen bearbeiten, während sich CIs im Zustand „Wartung“ befinden	Lernen Sie, Warnungen für ein CI zu behandeln, das sich im Status „Wartung“ befindet, also gerade geändert wird.
Warnungsauswirkungen bei der Selektierung von Warnungen anpassen	Indem Sie die Auswirkungsregeln ändern, können Sie die Berechnung der Warnungsauswirkung und den Schweregrad der Warnung festlegen.

Warnungslistenansichten anpassen

Sie können eine oder mehrere benutzerdefinierte Warnungslistenansichten erstellen, um nur für Sie relevante Informationen anzuzeigen. Beispielsweise können Sie sich nur auf die Warnungen für Anwendungsservices an einem bestimmten Standort oder nur auf die Warnungen für Anwendungsservices mit hoher Relevanz konzentrieren.

Vorbereitungen

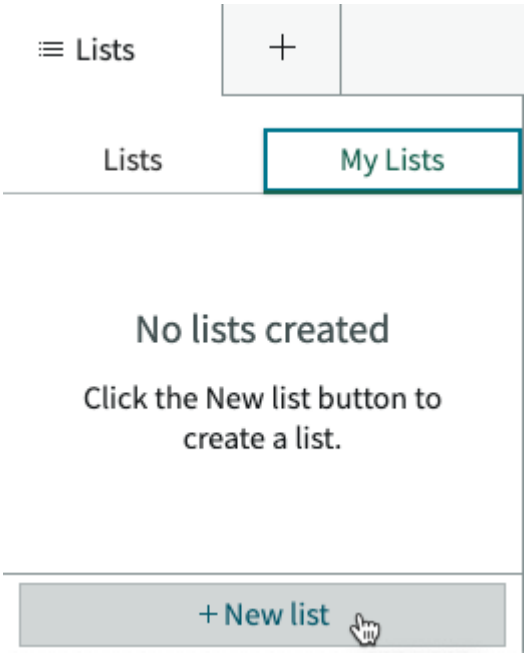
Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Erforderliche Rolle: evt_mgmt_operator

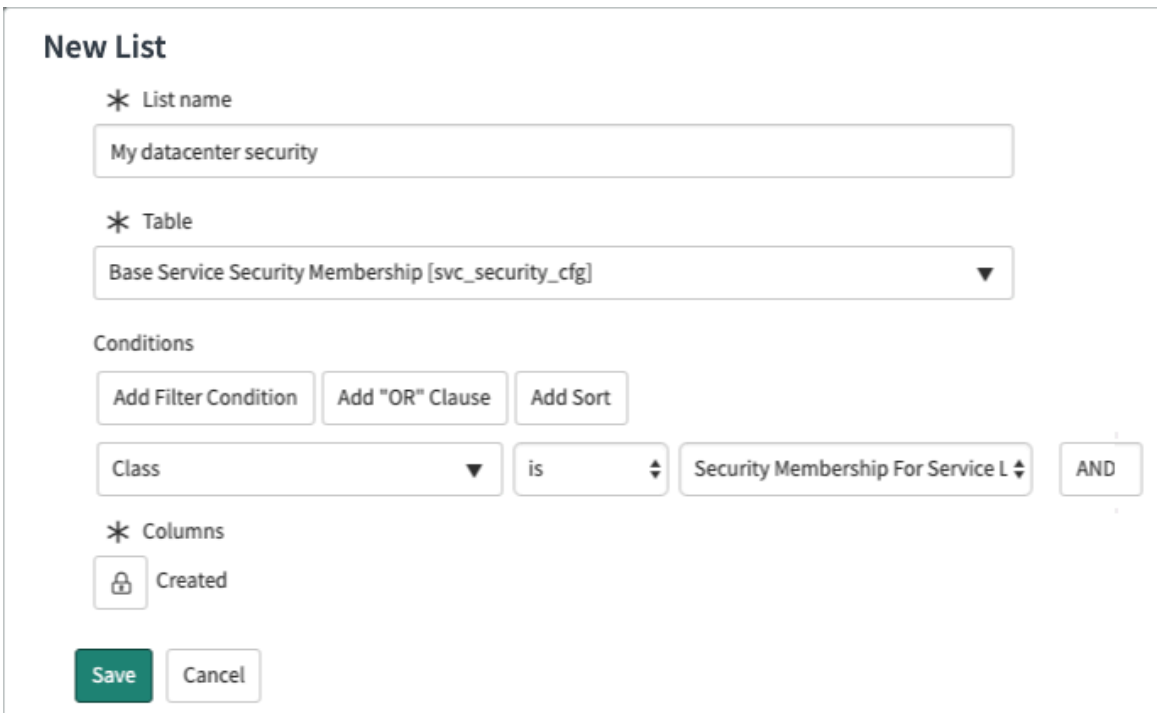
Prozedur

1. Navigieren zu **Ereignismanagement** > **Operatoren-Arbeitsbereich**.
2. Klicken Sie auf der Registerkarte **Listen** auf **Meine Listen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **+ Neue Liste**, füllen Sie das Formular mit Namen und Filterbedingungen aus und klicken Sie dann auf **Speichern**.



Die Liste wird auf der Registerkarte **Meine Listen** angezeigt.

Hinweis: Die Liste gilt nur für Anwendungsservices und nicht für Anwendungsservice -Gruppen. Die Gruppen werden angezeigt, unabhängig davon, ob sie selbst oder dort enthaltene Services dem Filter entsprechen.

Mit fluktuierenden Warnungen arbeiten

Wenn sich eine Warnung im Status „Fluktuierend“ befindet, müssen Sie die Warnung möglicherweise erneut selektieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Erforderliche Rolle: evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Wenn ein Event wiederholt in kurzer Zeit dieselbe Warnung auslöst, wird die Warnung in den Status „Fluktuierend“ versetzt, auch wenn sie zuvor von einem Operator geschlossen wurde. Das Event kann auch zwischen Schweregraden schwanken, z. B. „Info“ und „Kritisch“. Sie müssen die Warnung nun erneut selektieren und Aktionen ergreifen, um ein erneutes Auftreten des Events zu verhindern.

Hinweis: Ihr Ereignismanagement Administrator kann mit verschiedenen Einstellungen festlegen, wann eine Warnung als „Fluktuierend“ markiert wird und welche Aktionen Sie ergreifen können. In diesem Thema behandeln wir ein generisches Beispiel.

Prozedur

1. Warnungen im Status „Fluktuierend“ suchen:
   a. Navigieren zu **Ereignismanagement** > **Operatoren-Arbeitsbereich**.
   b. Ändern Sie die Liste der Warnungen, indem Sie auf das Filtersymbol ( ) klicken und Kriterien angeben, um fluktuierende Warnungen zu finden.
   Klicken Sie auf **Erweiterte Ansicht**, um die Filtereinstellungen zu ändern. Beispielsweise können Sie Folgendes angeben:

   `Status` | `ist` | `Flatternd`.

2. Klicken Sie auf die Warnungsnummer, um die Warnung zu öffnen.
3. Klicken Sie in der Warnung auf die Registerkarte **Flatternd**, und überprüfen Sie diese Informationen:

Feld	Beschreibung
Anzahl der Fluktuationen	Die Häufigkeit, mit der die Warnung seit dem Zeitpunkt im Feld **Startfenster der Fluktuation** zu fluktuieren begonnen hat.
Flattern – Startfenster	Die Zeit, zu der die Fluktuation begann.
Flattern – Zeit des letzten Update	Das letzte Vorkommen der Fluktuation. Dies ist die Verarbeitungszeit der Instanz, nicht die Zeit des Quellsystems.
Flattern – letzter Status	Der Status der Warnung vor dem Übergang in den Status „Fluktuierend“.

4. Entscheiden Sie basierend auf der Fluktuationshäufigkeit, welche Aktion ausgeführt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie haben die folgenden Möglichkeiten, je nach den Standard Operating Procedures Ihrer Organisation und den Einstellungen des Ereignismanagement Administrators:

- Führen Sie einen Fehlerkorrektur-Workflow aus, um z. B. einen Server neu zu starten oder einen Router zurückzusetzen.
- Greifen Sie auf eine Webanwendung zu, z. B. auf die Anwendung für die Event-Überwachungssoftware in Ihrem Netzwerk.
- Ändern Sie einen zugehörigen Incident oder einen KB-Artikel, um zusätzliche Informationen oder Schritte hinzuzufügen.

5. Nachdem Sie das zugrunde liegende Problem sicher behoben haben, schließen Sie die Warnung.

Warnungen bearbeiten, während sich CIs im Zustand „Wartung“ befinden

Wenn eine Warnung für ein CI auftritt, das sich im Wartungsstatus befindet, wird der Warnstatus ebenfalls in „In Wartung“ geändert. Sie sollten den Status dieser Warnungen herausfinden und überwachen. Wenn die Änderungen am CI später abgeschlossen sind, beenden Sie die Selektierung der Warnung und schließen Sie diese.

Vorbereitungen

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Bevor Sie diese Aufgabe abschließen, machen Sie sich mit der grundlegenden Formularkonfiguration einer Instanz vertraut. Möglicherweise müssen Sie Felder und zugehörige Listen zu Formularen hinzufügen.

Im Beispiel in diesem Thema wird davon ausgegangen, dass ein Netzwerkadministrator eine Change-Anforderung geöffnet hat, um einen problematischen Webserver neu zu konfigurieren.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Warnungen im Status „Wartung“ suchen:

   a. Navigieren zu **Ereignismanagement** > **Operatoren-Arbeitsbereich**.

   b. Klicken Sie auf das Filtersymbol ( ), klicken Sie im Feld „Filter“ auf **Erweiterte Ansicht**, und geben Sie Folgendes an:

   `Status | ist | Wartung`.

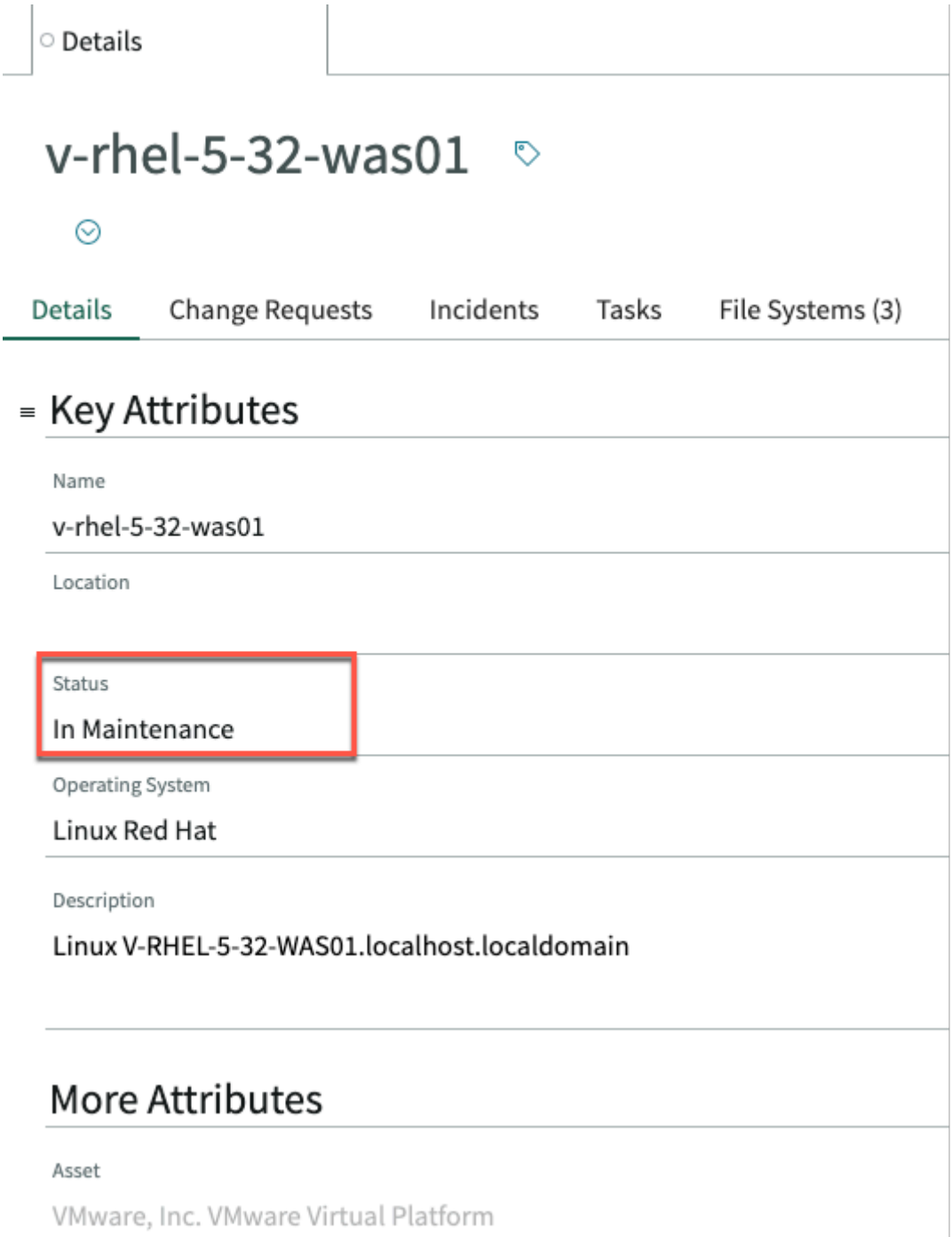
2. Suchen Sie eine Warnung in der Liste, die über einen Wert in der Spalte **Konfigurationselement** verfügt.
   Dies ist das CI, in dem die Warnung aufgetreten ist.
3. Klicken Sie auf den CI-Namen, um das Formular mit Informationen zum CI zu öffnen.

   In diesem Beispiel ist der Status des Webservers **In Wartung** und eine Change-Anforderung wurde geplant, sodass jemand den Server neu konfigurieren kann.

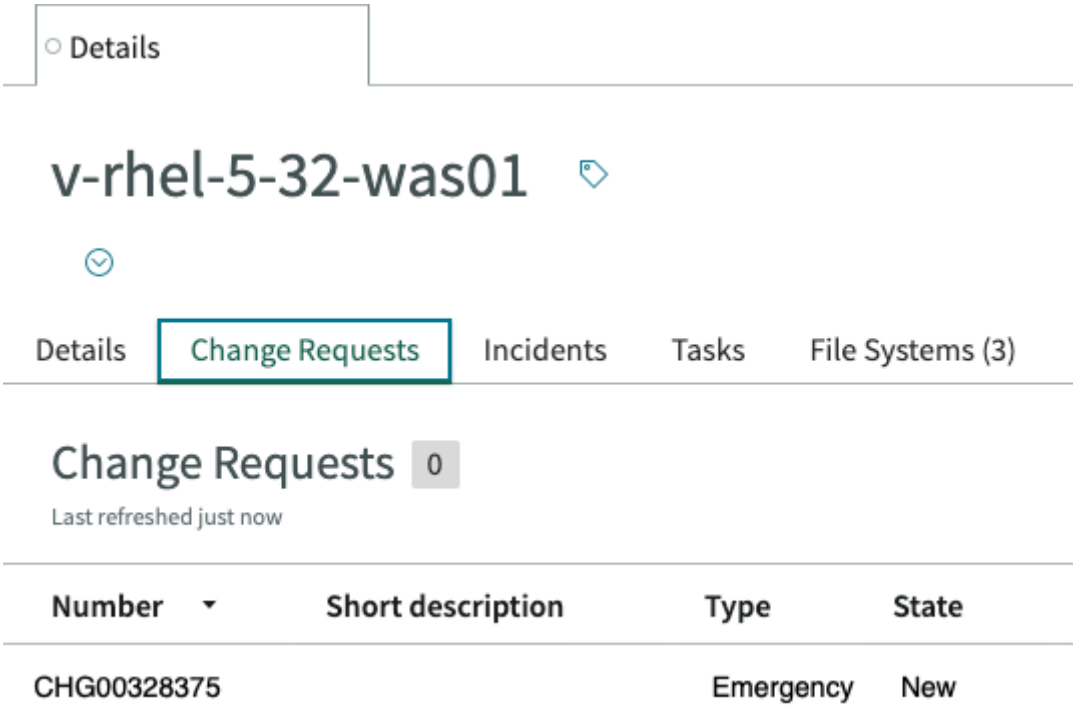
4. Klicken Sie auf den CI-Namen, um das Formular mit Informationen zum CI zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Beispiel hat der Server (auf der Registerkarte **Details**) den Status **In Wartung**. Sie können die geplante Change-Anforderung auf der Registerkarte **Change-Anforderungen** anzeigen (jemand konfiguriert das CI neu).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Zu diesem Zeitpunkt sollten Sie die diesem CI zugeordnete Warnung nicht ändern. Sie können die Change-Anforderung öffnen, um angehängte Zeitpläne anzuzeigen, oder Sie stimmen sich mit Ihrem Team ab, um herauszufinden, wann das CI nicht mehr „In Wartung“ ist.
6. Verifizieren Sie zunächst, dass das Feld **Status** im CI nicht den Wert **In Wartung** hat. Öffnen Sie dann die Warnung erneut, und deaktivieren Sie das Kontrollkästchen **Wartung**.
7. Fahren Sie mit der Selektierung der Warnung fort.

Warnungsauswirkungen bei der Selektierung von Warnungen anpassen

Als Ereignismanagement Operator müssen Sie möglicherweise die Auswirkungen einer Warnung auf einen Anwendungsservice und auf die CIs in einem Service ändern. Tun Sie dies, wenn Sie der Meinung sind, dass die Auswirkung nicht genau mit Ihrer Netzwerkumgebung übereinstimmt. So können andere Operatoren und Administratoren die richtigen Auswirkungsinformationen sehen.

Vorbereitungen

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Erforderliche Rolle: evt_mgmt_operator

Warum und wann dieser Vorgang ausgeführt wird

Bevor Sie Änderungen an Berechnungen der Auswirkung vornehmen, vergewissern Sie sich, dass Sie wissen, wie die Anwendungsservices und CIs tatsächlich funktionieren. Möglicherweise müssen Sie dazu die Netzwerkinfrastruktur testen, oder sich an jemanden wenden, der dies für Sie tun kann.

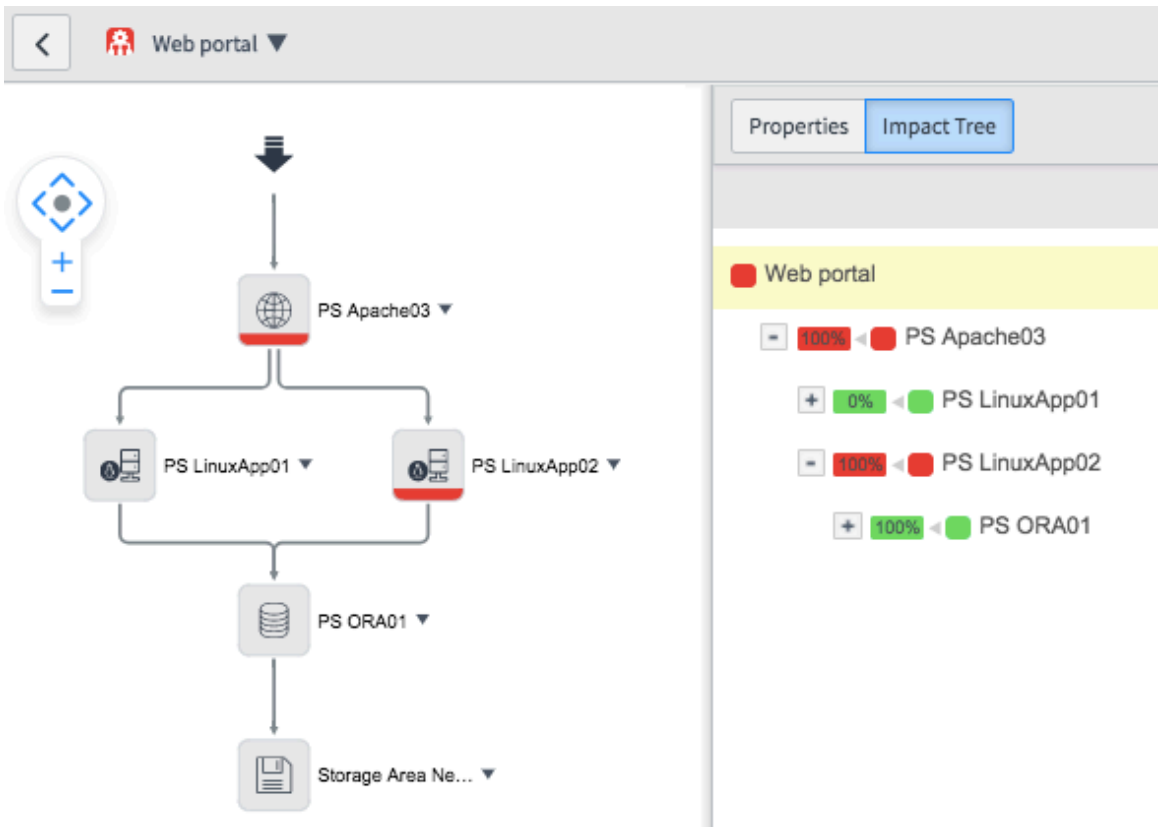
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Ereignismanagement** > **Operatoren-Arbeitsbereich**.
2. Doppelklicken Sie auf den Namen von Anwendungsservice mit den Warnungen, die Sie ändern möchten.
3. Klicken Sie auf der Registerkarte Details auf **Servicezuordnung**.
4. Klicken Sie auf der **Registerkarte Servicezuordnung** auf **Vollständige** Zuordnungsstruktur.
5. Klicken Sie in der Zuordnung auf **Auswirkungsstruktur**.
6. Analysieren Sie den Anwendungsservice, und ermitteln Sie basierend auf Ihren Informationen über die beteiligten CIs, ob die Auswirkungsstruktur die Auswirkung der Warnungen genau widerspiegelt.

   In diesem Beispiel deutet eine kritische Warnung auf ein schwerwiegendes Problem mit einem Linux-Server hin, der Teil von einem Webportal Anwendungsservice ist.



   Beachten Sie, dass die Auswirkung auf das Webportal selbst in roter Farbe dargestellt ist, da es sich um eine kritische Auswirkung handelt – obwohl nur einer der Linux-Server, auf die sich das Portal verlässt, tatsächlich eine kritische Warnung hat. Der andere Linux-Server ist von der Warnung nicht betroffen. Nehmen Sie für dieses Beispiel an, dass die Linux-Server unterschiedliche Rollen für den Webservice ausführen, und dass **PS LinuxApp02** zwar eine kritische Warnung hat, der Server **PS LinuxApp01** Server jedoch alle erforderlichen Services bereitstellen kann, um den Anwendungsservice betriebsbereit zu halten.

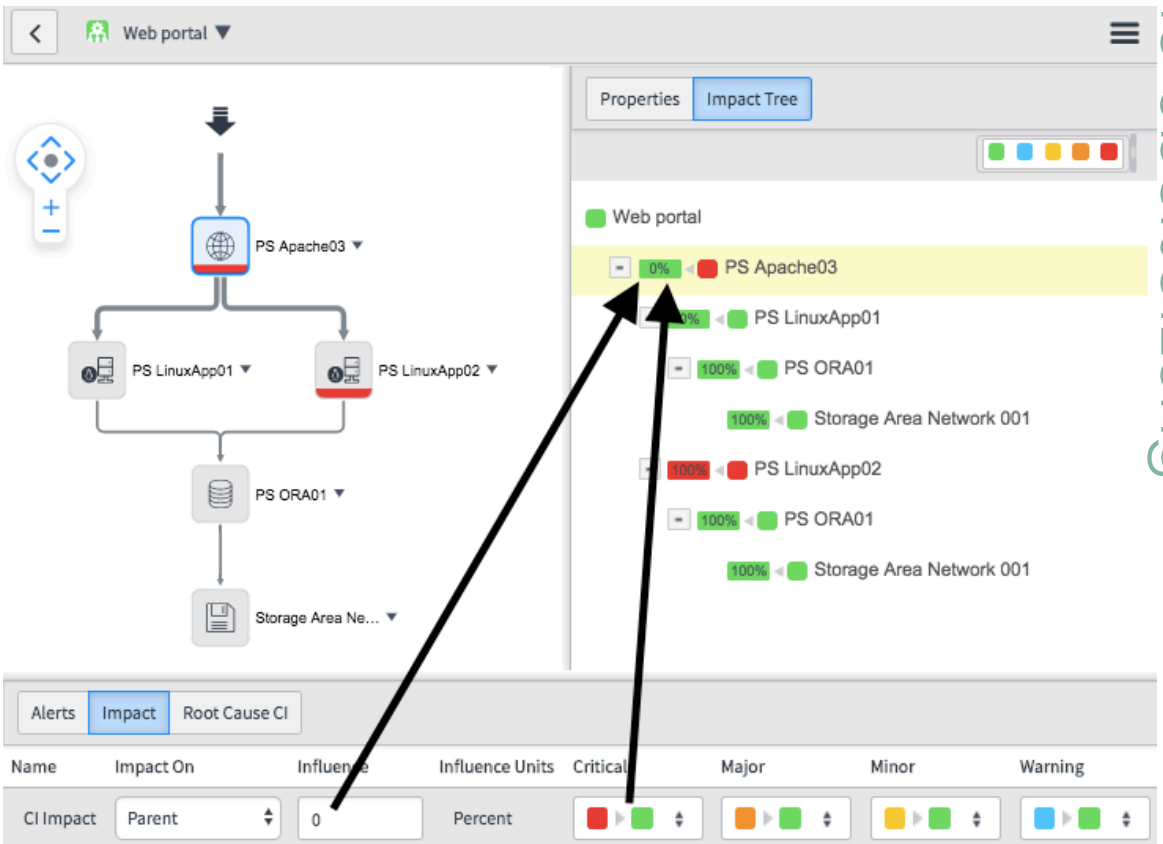
7. Klicken Sie auf das CI **PS Apache03**, und klicken Sie dann auf **Auswirkung**, um die Auswirkungsregeln für das CI anzuzeigen.
   Standardmäßig wird die CI-Auswirkungsregel mit folgenden Informationen angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Die Spalten **Auswirkung auf** und **Einfluss** zeigen an, dass das CI (**PS Apache03**) 100 % der Auswirkung aller untergeordneten CI-Auswirkungen erbt, was in diesem Fall die kritischen Auswirkungen auf den Server **PS LinuxApp02** umfasst. Diese Einstellung ist der Grund, warum der Webserver **PS Apache03** und der Anwendungsservice als Ganzes die Auswirkung zu 100 % erben.
- Die Spalte **Kritisch** zeigt an, dass eine kritische Warnung (rot) als kritische Warnung (rot) geerbt wird.

8. Ändern Sie den Wert **Einfluss** auf `0`, da der Webserver noch betriebsbereit ist. Ändern Sie dann die Spalte **Kritisch**, um anzugeben, dass ein kritischer Auswirkungsstatus (rot) als „Nicht-Auswirkung“ (grün) geerbt werden soll.
9. Warten Sie, bis das Dashboard automatisch aktualisiert wird, oder klicken Sie auf **Ereignismanagement** > **Service Operations-Arbeitsbereich** und doppelklicken Sie auf dieselbe Anwendungsservice, um eine aktualisierte Anwendungsservice -Zuordnung zu erhalten.

   Beachten Sie, dass der Einfluss auf den Apache-Webserver 0 % beträgt und der Auswirkungsstatus grün ist. Beachten Sie auch, dass der kritische Warnungsstatus (rot) unverändert bleibt, obwohl die Auswirkung zu grün geändert wurde.



10. Navigieren Sie zurück zum Dashboard „Service Operations Workspace“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beachten Sie, dass Anwendungsservice jetzt grün ist, was darauf hinweist, dass der gesamte Anwendungsservice betriebsbereit ist. Die kritische Warnung wird weiterhin unten in der Warnungsliste angezeigt und gibt an, dass noch ein Problem besteht, das Sie oder andere Operatoren beheben können.

Nächste Maßnahme

Unter Umständen konfiguriert Ihr Administrator zusätzliche Auswirkungsregeln, die angezeigt werden, wenn Sie in der Anwendungsservice-Zuordnung auf ein CI klicken. Sie können Anpassungen an den **Einflussfeldern** jeder Auswirkungsregel vornehmen, um die genaueste Auswirkungsstruktur zu erhalten.

Ereignismanagement-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Zuordnen und Optimieren von Anwendungsservices mithilfe von Ereignismanagement-Listen und -Formularen.

Mit Ereignismanagement installierte Komponenten

Durch die Aktivierung des Plugins Ereignismanagement (com.glideapp.itom.snac) werden mehrere Rollen, Scheduled Jobs und Tabellen hinzugefügt.

Hinweis: In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Mit Ereignismanagement installierte Rollen

Von der Anwendung Ereignismanagement verwendete Rollen.

Ereignismanagement fügt diese Rollen hinzu.

Rollentitel [Name]	Beschreibung	Enthält Rollen
Ereignismanagement Administrator [evt_mgmt_admin]	Hat Lese- und Schreibzugriff auf alle Ereignismanagement-Funktionen zum Konfigurieren von Ereignismanagement.	• evt_mgmt_user • template_editor_global

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Hinweis: Seien Sie vorsichtig mit der Rolle evt_mgmt_admin, die zur Administratorrolle hochgestuft werden kann. Ein Benutzer mit der Rolle „evt_mgmt_admin“ kann Skripts hinzufügen und ändern, die in einem globalen Bereich ausgeführt werden. Stellen Sie eine ordnungsgemäße Zugriffssteuerung sicher. Mit dieser Rolle kann der Benutzer die folgenden Skripts erstellen und/ oder aktualisieren: • Regeln zur Warnungskorrelation • Warnungsverwaltungsregeln • Wartungsregeln • Erweiterte Skripts • Ereignisfeldzuordnung • Vor- und Nachbindungsskripts	
Ereignismanagement Operator [evt_mgmt_operator]	Neben den evt_mgmt_user-Berechtigungen können auch Vorgänge für Warnungen wie Bestätigen, Schließen, Öffnen von Vorfällen und Ausführen von Korrekturen aktiviert werden.	evt_mgmt_user
Ereignismanagement Benutzer [evt_mgmt_user]	Hat Lesezugriff auf alle Ereignismanagement-Funktionen. Hat die Rolle, um Vorfälle verwalten zu können, die aus Alerts erstellt werden.	itil
Ereignismanagement-Integrator [evt_mgmt_integration]	Hat Zugriff auf die Tabellen Event [em_event] und Registered Nodes [em_registered_nodes], um sie mit externen Ereignisquellen zu integrieren.	

Mit Ereignismanagement installierte regelmäßige Aufgaben

Liste der Scheduled Jobs, die mit Ereignismanagement bereitgestellt werden.

Um die Liste der geplanten Aufgaben zu überprüfen, navigieren Sie zu **Systemzeitplaner** > **Geplante Aufgaben**. Ereignismanagement fügt die folgenden geplanten Aufgaben hinzu.

Geplante Aufgabe	Beschreibung
Ereignismanagement – Connector-Ausführungsjob	Vergleicht die aktuelle Zeit mit der Zeit der letzten Ausführung von aktiven Connector-Instanzen und legt relevante Connectors zur Ausführung fest. Wird alle 10 Sekunden ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
Ereignismanagement – Auswirkungen von abgebrochenen Services behandeln	Löst abgebrochene Services und markiert sie in der Tabelle „Auswirkungsänderungen“ als neu zu erstellende Services, um die Auswirkungsstruktur neu zu erstellen. Wird alle 2 Minuten und 31 Sekunden ausgeführt.
Ereignismanagement – Auswirkungsrechner auslösen	Löst die Auswirkungsberechnung aus. Das Dashboard Ereignismanagement und die Auswirkungsstruktur werden anhand der berechneten Zahlen aktualisiert. Wird alle 6 Sekunden ausgeführt.
Ereignismanagement – Auswirkungstopologie-Verbraucher	Verbraucht Topologieänderungen und markiert die zugehörigen Services in der Tabelle „Auswirkungsänderungen“ als „Neuerstellung erforderlich“, um ihre Auswirkungsstruktur neu zu erstellen. Wird alle 19 Sekunden ausgeführt.
Ereignismanagement – Connectors für abgebrochene Updates	Löst Connector-Instanzen, die abgebrochen werden. Wird alle 2 Minuten ausgeführt.
Ereignismanagement – Warteschlange für Warnungspriorität	Berechnet die Warnungspriorität. Zwei Jobs für Warteschlange für Warnungspriorität sind aktiv und verfügbar und können mit Multi-Thread ausgeführt werden. Wird jede Minute ausgeführt.
Ereignismanagement – Warnungen für automatisches Schließen	Warnungen, die länger als 7 Tage inaktiv sind (Standardzeitraum), werden geschlossen. Ändern Sie den Standardwert mit der Eigenschaft `evt_mgmt.alert_auto_close_interval`. Wird alle 10 Minuten ausgeführt.
Ereignismanagement – Warnungsprioritätsgruppen berechnen	Führt die Prioritätsgruppen aus und berechnet sie: dringend, hoch, mittel und niedrig für die Warnungen gemäß der höchsten und niedrigsten Priorität im System. Wird alle 30 Minuten ausgeführt.
Ereignismanagement – Fluktuierende Warnungen schließen	Schließt fluktuierende Warnungen. Wird alle 5 Minuten ausgeführt.
Ereignismanagement – Schwellenwertwarnung schließen	Schließt Schwellenwertwarnungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
	Wird alle 2 Minuten ausgeführt.
Ereignismanagement – Warnungsverwaltungsregeln evaluieren	Führt Warnungsverwaltungsregeln aus. Wird alle 11 Sekunden ausgeführt.
Ereignismanagement – Auswirkungsstrukturgenerator	Verarbeitet alle Services mit Änderungen aus der Tabelle „em_impact_changes“ und erstellt ihre Auswirkungsstruktur neu. Wird alle 11 Sekunden ausgeführt.
Ereignismanagement – Systemüberwachung einfügen	Auftrag zur Erstellung der **ServiceNow Ereignismanagement-** Anwendungsservices. Wird einmal pro Stunde ausgeführt.
Ereignismanagement – Wartungsrechner	Berechnet die Wartung für CIs. Wird jede Minute ausgeführt.
Ereignismanagement – Knotenanzahl	Berechnet die Lizenznutzung. Wird einmal pro Stunde ausgeführt.
Ereignismanagement – Events verarbeiten	Job, der jedes Bereit-Event ausführt und verarbeitet (Event-Regel anwenden, Zuordnungsregel anwenden und Warnung erstellen oder aktualisieren) Wird alle 5 Sekunden ausgeführt.
Ereignismanagement – Metrikbindung verarbeiten	Verarbeitet Metrikbindungen. Wird alle 5 Sekunden ausgeführt.
Ereignismanagement — Prozessdatensätze in em_extra_data_json	Erstellt Events für Protokollanalyseanomalien. Wird alle 13 Sekunden ausgeführt.
Ereignismanagement – Connector-Prozessor der Warteschlange	Bidirektionale Funktionalität. Verarbeitet alle ausstehenden Warnungen in der Update-Warteschlange und sendet sie an den MID-Server. Standardmäßig wird dieser Prozess aus der Warteschlange in Batches von 1.000 Warnungen ausgeführt. Wird alle 30 Sekunden ausgeführt.
Ereignismanagement – Auswirkung für Gruppen neu berechnen	Dieser Job ist standardmäßig nicht aktiv. Kann bei Bedarf ausgeführt werden, um die Auswirkungen auf Servicegruppen zu korrigieren. Wird bei Bedarf ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
Ereignismanagement – Abgebrochene Events wiederherstellen	Verarbeitet alle Events, die sich in der Warteschlange befinden, und stellt sie zurück auf den Status „Bereit“, um Events vom Anfang an zu verarbeiten. Wird beim Systemstart ausgeführt.
Ereignismanagement – Systemüberwachung aktualisieren	Aktualisiert die Anwendungsservices **von ServiceNow Ereignismanagement**. Wird einmal pro Stunde ausgeführt.
Ereignismanagement – SLA-Konfigurationsergebnis aktualisieren	Synchronisiert die CIs, die dem SLA-Konfigurationsfilter entsprechen, mit der Tabelle Ereignismanagement-SLA [em_ci_severity_task]. Wird alle 10 Minuten ausgeführt.
Ereignismanagement – SLA-Schweregrad aktualisieren	Aktualisiert die Tabelle Ereignismanagement-SLA [em_ci_severity_task] mit dem neuen Schweregrad. Wird einmal pro Stunde ausgeführt.
Ereignismanagement – IT-Service konvertieren	Führen Sie diese Eigenschaft bei Bedarf aus, um manuelle Services in Anwendungsservices zu konvertieren. Wird alle 30 Minuten ausgeführt.
Ereignismanagement – xmlstats erfassen	Erfasst Event-Verarbeitungsstatistiken. Wird einmal pro Minute ausgeführt.
Ereignismanagement – Auswirkungsrechner für Warnungsgruppen und SLA	Berechnet die Auswirkung von Warnungen auf Warnungsgruppen-Services.
4x Ereignismanagement – Auswirkungsrechner für Services	Berechnet die Auswirkung von Warnungen auf Anwendungsservices und erstellt die Auswirkungsstruktur im Dashboard Ereignismanagement. Vier separate Jobs werden ausgeführt, um das System zu entlasten.
Ereignismanagement – Tabelle mit Auffüllungswarnungen	Sucht redundante Datensätze in der Tabelle „em_alert_history“ und bricht sie ab.
Ereignismanagement – Auswirkungsstatustabelle für Auffüllung	Sucht redundante Datensätze in der Tabelle „em_impact_status“ und bricht sie ab.
Ereignismanagement – Auswirkung für Gruppen	Berechnet die Auswirkung von Warnungen auf Servicegruppen.
Ereignismanagement – Tabelle mit Warnungsverlauf bereinigen	Bereinigt die Tabelle mit dem Warnungsverlauf (em_alert_history), indem Datensätze entfernt werden, die älter als 90 Tage sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geplante Aufgabe	Beschreibung
	Sie können die Zeitspanne anpassen, nach der Warnungen entfernt werden, indem Sie *evt_mgmt.impact_calculation.cleanup_age_seconds.e* in der Tabelle sys_properties.list konfigurieren.
Ereignismanagement – Tabelle mit Auswirkungsstatus bereinigen	Bereinigt die Tabelle mit dem Auswirkungsstatus (em_impact_status), indem Datensätze entfernt werden, die älter als 90 Tage sind. Sie können die Zeitspanne anpassen, nach der Warnungen entfernt werden, indem Sie *evt_mgmt.impact_calculation.cleanup_age_seconds.e* in der Tabelle sys_properties.list konfigurieren.

Ereignismanagement fügt die folgenden Scheduled Jobs hinzu, um die Warnungszusammenfassung und RCA zu unterstützen.

Name	Beschreibung
Serviceanalytik löscht alte Beobachtungsdaten – Täglich	Bereinigt die bereitgestellten Daten.
Serviceanalytik bereitet RCA-Learner-Eingabedaten vor – Täglich	Bereitet RCA-Eingabedaten vor. Speichert und prüft MID-Server, um statistische Informationen zu Warnungen zu erfassen
Serviceanalytik-Gruppenwarnungen mithilfe von RCA/ Warnungszusammenfassung	Wendet RCA und Warnungszusammenfassung auf offene Warnungen an und bereitet automatisierte Warnungsgruppen vor.
Serviceanalytik Warnungszusammenfassungs-Learner – Täglich	Lernt Informationen zu vorhandenen Warnungen kennen und gruppiert neue offene Warnungen.
Serviceanalytik-RCA-Konfiguration	Konfiguriert die Ursachenanalyse.
Serviceanalytikprüfung Dateisystembereich auf Analytics MID – Täglich	Überprüft die Datenträgernutzung auf dem dedizierten MID-Server und generiert ein Event, wenn sie den in der Eigenschaft „sa_analytics.rca.mid_max_allowed_space“ festgelegten Schwellenwert überschreitet.
Serviceanalytik sammelt Berichtsdaten – Täglich	Sammelt Daten für den Wertbericht.
Serviceanalytik – Virtuelle Warnungen für Zusammenfassungsgruppen aktualisieren	Aktualisiert die virtuellen Warnungen, die erstellt wurden, um Warnungszusammenfassungsgruppen darzustellen, mit allen Änderungen an Warnungen, die zu dieser Gruppe gehören. Wird jede Minute ausgeführt.
Serviceanalytik Attributausfüllung für historische Warnungen	Füllt Attribute aus, die im Feature-Bezeichner für historische Warnungsdaten mittels Event-Regeln verwendet werden. Wird bei Bedarf ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften zur Personalisierung der Domänentrennung für Ereignismanagement -Connectors

Eigenschaften stellen die Metadaten bereit, um die Domäne zu identifizieren.

Sie können die Werte ändern, wenn Sie andere Tabellen oder Felder für die Domänenidentifizierung verwenden möchten. Stellen Sie jedoch sicher, dass die Tabelle domänengetrennt ist.

Hinweis: Bei der Personalisierung der Domänentrennung für Ereignismanagement-Connectors können alle Eigenschaften auch auf Connector-Ebene überschrieben werden.

Es werden drei Caches für die Personalisierung der Domänentrennung verwaltet (main, user_access, Missing_domain). Sie können einige Systemeigenschaften erstellen, um sie zu steuern.

Standardsystemeigenschaften

Eigenschaft	Beschreibung
evt_mgmt Connector_domain_info_table_name	Die Tabelle, in der Sie Domäneninformationen speichern, um Domain Separation zu personalisieren. • **Typ**: Zeichenfolge • **Standardwert**: core_company
evt_mgmt Connector_domain_info_column_name	Der Feldname in der Tabelle zur Identifizierung der angegebenen Domäne für die Personalisierung von Domain Separation. • **Typ**: Zeichenfolge • **Standardwert**: Name
evt_mgmt Connector_domain_id_column_name	Das Feld, von dem die Domänen-ID für die Personalisierung von Domain Separation abgerufen wird. • **Typ**: Zeichenfolge • **Standardwert**: sys_domain
evt_mgmt Connector_domain_path_column_name	Das Feld, von dem der Domänenpfad für die Personalisierung von Domain Separation abgerufen wird. • **Typ**: Zeichenfolge • **Standardwert**: sys_domain_path

Eigenschaft	Beschreibung
evt_mgmt.connector_custom_domain_sep_cache_expire_in_seconds	Zur Personalisierung Domain Separation wenn Ihr Hauptcac

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	nicht jede Woche ablaufen soll.
evt_mgmt.connector_custom_domain_sep_user_access_on_domain_cache_size	Zur Personalisierung Domain Separation wenn Sie die Größe Benutzerzugriffsca erhöhen möchten.
evt_mgmt.connector_custom_domain_sep_missing_domain_cache_expire_in_seconds	Zur Personalisierung Domain Separation wenn Sie die Ablau für den Cache zum Speichern von Informationen zur fehlenden Domäne erhöhen möchten.
evt_mgmt.connector_custom_domain_sep_cache_size	Zur Personalisierung Domain Separation wenn Sie mehr Hauptcache zum Speichern von Domäneninformati benötigen.

Mit Ereignismanagement installierte Tabellen

Tabellen, die bereitgestellt werden, wenn Ereignismanagement aktiviert ist.

Ereignismanagement fügt diese Tabellen hinzu.

Tabelle	Beschreibung
Warnung [em_alert]	Warnungen, die Ereignismanagement verwaltet.
Warnungskorrelationsregel [em_alert_correlation_rule]	Regeln, die primäre und sekundäre korrelierte Warnungen angeben.
Gruppenwarnungen für Warnungszusammenfassung [em_agg_group_alert]	Speichert Warnungen, die zusammengefassten Warnungsgruppen zugeordnet sind.
Gruppe für Warnungszusammenfassung [em_agg_group]	Beziehungen zwischen zusammengefassten Gruppen und primären Warnungen.
Warnungsverlauf [em_alert_history]	Verlauf von Warnungen. Wird für Auswirkungsberechnungen verwendet.
Warnungsregel [em_alert_rule]	Zuordnungen von Warnungsfeldern zur Incident-Tabelle [Incident].

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Warnvorlage [em_alert_template]	Warnungsvorlagen. Diese Tabelle erweitert die Vorlagentabelle [sys_template].
Ereignismanagement SLA [em_ci_severity_task]	Ereignismanagement-SLA-Aufgaben für CIs und Services.
Connector-Definition [em_connector_definition]	Einstellungen zum Erheben von Events aus externen Event-Quellen.
Anschlussinstanz [em_connector_instance]	Connector-Details für externe Event-Quellen.
MID-Server zu Connector-Instanz [em_connector_instance_to_mid]	Zuordnungen von MID Servers zu Connector-Instanzen
Ereignismanagement-Lizenznutzung [em_unique_nodes]	Wenn Ereignisse von ITOM-Integrität empfangen werden, wird ein Eintrag in dieser Tabelle basierend auf dem in der empfangenen Nachricht angegebenen überwachten Ziel hinzugefügt oder aktualisiert. Der Eintrag ist mit dem entsprechenden CI in der CMDB verknüpft. Wenn kein CI gefunden wird, wird dem Eintrag das Attribut *Type = Unknown* zugewiesen.
Event [em_event]	Events, die von Ereignismanagement empfangen wurden.
Event-Filter [em_event_filter]	Speicher für definierte Event-Filter.
Event-Abgleichregel [em_match_rule]	Aktualisierte Events für die Warnungsverarbeitung. Wird von Event-Regeln verwendet.
Feld zur Ereignisabstimmung [em_match_field]	Zuordnungen von Event-Feldern zu Warnungsfeldern. Einfache Zuordnung. Wird von Event-Regeln verwendet.
Feld zur Ereigniserstellung [em_compose_field]	Zuordnungen von Event-Feldern zu Warnungsfeldern. Zusammengesetzte Zuordnung. Wird von Event-Regeln verwendet.
Event-Zuordnungsregeln [em_mapping_rule]	Aktualisierte Event-Felder für die Warnungsverarbeitung.
Ereignisverarbeitungsstatistiken [em_event_stats]	Statistiken zur Leistung von Ereignismanagement.
Ereignistyp	Event-Typen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[em_event_type]	
Aufgabenvorlage [em_incident_template]	Vorlagen, die definieren, wie neue Aufgaben ausgefüllt werden. Beispielsweise müssen Felder eines Incidents, der aus einer Warnung erstellt wird, ausgefüllt werden. Diese Tabelle erweitert die Vorlagentabelle [sys_template].
Registrierte Knoten [em_registered_nodes]	Registriert Knotendaten.
Schwellenwertregel [em_threshold_rule]	Warnung für Schwellenwertregeln.
Gerätezuordnung verbinden [Em_binding_device_map]	Event-Bindung an Netzwerk- und Speicherpfade.
Prozess für CI-Typ-Zuordnungen [Em_binding_process_map]	Event-Bindung an bestimmte Prozesse.
CI-Fehlerkorrektur [em_ci_remediation]	Regeldefinitionen für Fehlerkorrektur.
Auswirkungsgrafik [em_impact_graph]	Auswirkungsstruktur von CIs, die eine CI-Hierarchie und Auswirkungsregeln für die Auswirkungsberechnung enthalten.
Auswirkungsgrafik-Verläufe [em_impact_graph_history]	Verlauf der Änderungen in der Auswirkungsstruktur.
Auswirkungsregeldefinitionen [em_impact_rule_definition]	Definition der Regeln für die Auswirkungsberechnung.
Auswirkungsregelinstanz [em_impact_rule]	Regeln basierend auf Auswirkungsregeldefinitionen.
Infrastrukturbeziehungen [em_impact_infra_rel_def]	Unter-/übergeordnete Paare oder CI-Typen. CIs, die diesen Definitionen entsprechen, werden den Auswirkungsstrukturen hinzugefügt.
Auswirkungswartungs-CIs [em_impact_maint_ci]	CIs, die sich in der Wartung befinden und daher von der Auswirkungsberechnung ausgeschlossen sind.
Auswirkungsstatus [em_impact_status]	Berechneter Status von CIs und Services, die im Dashboard und in Service Mapping für dynamische CI-Gruppen angezeigt werden sollen.
SLA-Konfiguration	SLA-Konfigurationsdatensätze, die die CIs identifizieren, auf denen SLAs ausgeführt werden können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[em_sla_configuration]	
Serviceanalytik Metriktypregistrierung [sa_metric_registration]	Quellregistrierungsdetails für die Verarbeitung von Rohdaten.
Systemüberwachungsskripts [em_monitor_scripts]	Diese Skripts bestimmen, wie beispielsweise bei Verwendung des Connectors-Überwachungsskripts Überwachungen oder Überprüfungen durchgeführt werden. Sie können ein benutzerdefiniertes Skript zur Überwachung eines Geräts oder einer Entität erstellen. Die mit der Basisinstanz bereitgestellten Skripts sind: • Verzögerung bei der Event-Verarbeitung überprüfen • Connector-Überwachung • Status der Event-Verarbeitung abrufen • MID-Server-Schwellenwertwarnungen
Überwachungskonfiguration [em_monitor_conf]	Verwenden Sie diese Tabelle, um zu konfigurieren, was entsprechend den aufgeführten Skripts überwacht werden soll. Konfigurieren Sie, wie oft jedes Skript ausgeführt werden soll. Wenn ein Skript über einen Schwellenwert verfügt, wird bestimmt, welcher Warnungsschweregrad angezeigt werden soll. Schwellenwerte werden in Minuteneinheiten angegeben und geben die Verzögerungszeit an. Navigieren zu **Ereignismanagement** > **Einstellungen** > **Selbstintegritätskonfiguration** um die Liste der Überwachungskonfigurationen anzuzeigen oder eine neue zu erstellen. Verwenden Sie dieses Skript, um die Überwachung des Rechenzentrums zu testen. Die mit der Basisinstanz bereitgestellten Skripts sind: • Überwachung Connectors im Ruhezustand – Überwachung, um zu überprüfen, ob sich einer der Connectors im Ruhezustand befand und den konfigurierten Schwellenwert [in Minuten] überschritten hat. • Connector-Status – Überwachung zur Nachverfolgung des aktiven Status der Connectors. • Verzögerung bei der Event-Verarbeitung – Überwachung der Dauer [in Minuten] von Events, die im Status „Bereit“ blieben und nicht verarbeitet wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
	• Event-Verarbeitungsjob – Überwachung des Status der Event-Verarbeitungsaufgaben. • MID-Server-Schwellenwertwarnung – Überwacht der Integrität des MID-Server
Event Management-Aufgaben überwachen [em_monitor_jobs_state]	Überwachen Sie Ereignismanagement-Aufgaben, indem Sie dieser Tabelle die entsprechenden Aufgaben hinzufügen. **Hinweis:** Die folgenden Aufgaben werden von dieser Tabelle nicht überwacht: • Ereignismanagement – Events verarbeiten • Ereignismanagement – Auswirkungsstrukturgenerator • Ereignismanagement – Abgebrochene Events wiederherstellen • Event-Verarbeitung
Überwachungsstatus [em_monitor_state]	Verwenden Sie diese Tabelle, um den Schwellenwert für jeden Connector festzulegen. Wenn ein Wert über einem Schwellenwert liegt, wird eine Warnung generiert.
EM-XMLStats-Daten [em_xmlstats_data]	Selbstintegritätsstatistiken und Diagnosedetails für Metrikdaten und Ereignismanagement, die zur Erstellung der XMLStats-Seite verwendet werden.

Ereignismanagement fügt die folgenden Tabellen hinzu, um die Warnungszusammenfassung und RCA zu unterstützen.

Tabelle	Beschreibung
SA-RCA-Status [sa_rca_status]	Informationen (z. B. IDs) für die neuesten Nachrichten, die während der RCA für einen Service an die ECC-Warteschlange gesendet wurden.
SA-RCA-Ausgabe [sa_rca_output]	Ausgabedaten RCA-Learner.
SA-RCA-Gruppe [sa_rca_group]	Automatisierte Warnungsgruppen für die RCA-Abfrage.
Staging des SA-Analysealarms [sa_analytics_alert]	Bereitstellungstabelle für Warnungen, die für Analysen verwendet werden.
SA-RCA-Eingabe [sa_rca_input]	Eingabe von Daten für den RCA-Learner.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
SA-Analysestatus [sa_analytics_status]	Informationen der letzten Ausführung, die für die Warnungszusammenfassung und RCA verwendet werden sollen.
SA-RCA-Gruppenwarnung [sa_rca_group_alert]	Warnungen, die automatisierten Warnungsgruppen zugeordnet sind.
Verknüpfung des SA-RCA-Service-Configuration Items [sa_rca_svc_ci_assoc]	Zuordnungen zwischen CIs und Services.
SA-Warnungszusammenfassung – Erlerntes Muster [sa_agg_pattern]	Erlerntes Muster der Warnungszusammenfassung.
SA-Alarmzusammenfassung – erlernte Musterelemente [sa_agg_pattern_element]	CI-/Metriknamenpaare, die erlernten Mustern zugeordnet sind.
Abfragegruppen-Muster für SA-Warnungszusammenfassung [sa_agg_group_pattern]	Beziehungen zwischen Gruppen, die in Abfragen zur Warnungszusammenfassung erkannt wurden, und Mustern, die im Lernen gefunden wurden.
Abfrage für SA-Warnungszusammenfassung -- bereitgestellte (letzte) Warnungen [sa_agg_group_alert_staging]	Eine Bereitstellungstabelle für Warnungen, die noch keiner zusammengefassten Warnungsgruppe zugeordnet wurden.
SA-Zusammenfassung – Musterattribut [sa_agg_pattern_attribute table]	CI/Warnungsattribute, die zum Auffinden von Mustern für die Warnungszusammenfassung verwendet werden.
SA-Warnungsattribut-Populator-Status [sa_alert_attribute_populator_status table]	Status und Statistiken für das Ausfüllen des Attributjobs.
SA-Warnungszusammenfassung Erlerntes Musterelement Paarweise Gegenseitige Informationen und Gemeinsame Wahrscheinlichkeit [sa_agg_pattern_element_pair]	Paarweise Wahrscheinlichkeiten für Musterelemente.
EM-Agg.-Gruppenvorhersage [em_agg_group_prediction]	Warnungsvorhersagen für Warnungsgruppen.

Event Management Platform Analytics and Reporting-Lösungen

Platform Analytics and Reporting-Lösungen enthalten vorkonfigurierte Dashboards. Diese Dashboards enthalten Visualisierungen handlungsrelevanter Daten, mit denen Sie Ihre Geschäftsprozesse und -praktiken optimieren können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Platform Analytics and Reporting-Lösungen

Platform Analytics Datenvisualisierungen verwenden Performance Analytics Indikatordaten, um Daten im Zeitverlauf anzuzeigen, sodass Sie Ihre Geschäftsprozesse analysieren und Verbesserungsbereiche identifizieren können. Mit Platform Analytics and Reporting-Lösungen können Sie mit einem minimalen Setup den Mehrwert von Performance Analytics für Ihre Anwendung nutzen. Sie können auch jederzeit eigene Objekte erstellen.

Wichtig: Richten Sie Platform Analytics and Reporting-Lösungen in einer Instanz außerhalb der Produktion ein, und testen Sie die Lösung, bevor Sie sie in der Produktion aktivieren.

Um die Lösung für Event Managementzu aktivieren, kann ein Administrator zu navigieren **Performance Analytics** > **Geführtes Setup**. Klicken Sie auf **Erste Schritte**, und scrollen Sie dann zum Abschnitt für Event Management. Das geführte Setup führt Sie durch den gesamten Einrichtungs- und Konfigurationsprozess.

Zugehörige Informationen

Platform Analytics and Reporting-Lösungen

Performance Analytics-Abonnement aktivieren

Performance Analytics-Widgets anpassen

Passen Sie die Darstellung von Widgets beim Anzeigen von Performance Analytics -Visualisierungen an.

Vorbereitungen

Erforderliche Rolle: Benutzer

Prozedur

1. Navigieren zu **Alle** > **Performance Analytics** > **Dashboards**.
2. Wählen Sie auf der Seite **Dashboards** ein Dashboard aus, das angezeigt werden soll.
3. Wählen Sie oben rechts auf der Seite das Freigabesymbol ( ).
4. Wechseln Sie zum oberen Abschnitt des entsprechenden Widgets, und wählen Sie das Symbol Widget bearbeiten ( ).
5. Konfigurieren Sie im Dialogfeld „Widget bearbeiten“ die entsprechenden Optionen. Details finden Sie unter Performance Analytics – Dialogfeld „Widget bearbeiten“.
6. Wählen Sie im Dialogfeld „Widget bearbeiten“ die Option **Fertig** aus.

Nächste Maßnahme

Benutzer mit der Rolle admin können Farben und Schriftarten anpassen.

- Weitere Informationen zum Anpassen von Farben finden Sie unter Performance Analytics-Widgets .
- Um Schriftarten anzupassen, navigieren Sie zu **sys_ux_theme_property.list,** und bearbeiten Sie die entsprechenden Schriftarten.

Lösungen für maschinelles Lernen für Event Management

Erstellen Sie Lösungen für Event Management mit Predictive Intelligence.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lösungsdefinition

Lösungsdefinition für Event Management

Lösungsdefinition	Beschreibung
Ähnlichkeit mit geschlossener Warnung	„Ähnlichkeit geschlossener Warnungen“ ist eine Ähnlichkeitslösungsdefinition, die verwendet wird, um ähnliche Warnungsdatensätze basierend auf diesen Feldern zu empfehlen: Beschreibung, Knoten, Ressource, CI-Typ, Quelle und Metrikname aus der Tabelle „Warnung“ [em_alert]. Die Ergebnisse sind für Benutzer im Formular „Warnung“ und auf der Registerkarte „Ähnliche Warnungen“ in Workspace einsehbar.
Clustering-Lösung für EM-Warnungen	Die EM Alert Clustering-Lösung ist eine Definition der Clustering-Lösung, die in Ereignismanagement verwendet wird. Ermöglicht das Erstellen von Clustering-Modellen, die die Identifizierung gängiger Textmuster in Warnungen ermöglichen, um Warnungsgruppen zu erstellen. Textcluster basieren auf diesen Feldern: Beschreibung, Metrikname, Klasse des Konfigurationselements aus der Tabelle „Warnung“ [em_alert].

Performance Analytics – Dialogfeld „Widget bearbeiten“

Felder im Dialogfeld zum Bearbeiten eines Widgets im Performance Analytics-Dashboard.

Abschnitt	Beschreibung
Echtzeit-Updates anzeigen	Durch die Auswahl werden Aktualisierungen in Echtzeit im Widget angezeigt.
Anzeigen	Aktivieren oder deaktivieren Sie die Kontrollkästchen, um Folgendes im Widget anzuzeigen oder auszublenden: • Rahmen • Kopfzeile • Titel
Titelausrichtung	Wählen Sie die Ausrichtung des Widget-Titels aus: • Left (Links) • Mitte • Mitte
Titelfarbe	Durch die Auswahl wird die Farbe des Widget-Titels konfiguriert.
Farbe der Kopfzeile	Durch die Auswahl wird die Farbe des Widget Headers konfiguriert.
Interaktivität	Wählen Sie aus den angezeigten Optionen aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt	Beschreibung
	• Interaktivem Filter folgen • Anzeigen, wenn Filter gefolgt wird

Formular „Ereignismanagement MID-Webservererweiterung“

Felder im Formular zum Erstellen oder Ändern einer MID-Webservererweiterung.

Formular „MID-Webserver-Kontext“

Feld	Beschreibung
Name	Eindeutiger Name für die Erweiterung zur einfachen Identifizierung
Kurzbeschreibung	Kurze, aussagekräftige Beschreibung der Erweiterung
Status	Dieses Feld wird automatisch mit dem Status der Erweiterung ausgefüllt. Das Feld ist leer, bis die Erweiterung gestartet ist. Nach der Ausgabe eines Befehls an die Erweiterung wird einer der folgenden Werte angezeigt: • Gestartet: Die Erweiterung wird ausgeführt. • Angehalten: Die Erweiterung wird nicht ausgeführt. • Offline: Der MID-Server ist nicht verfügbar. • Fehler: Die Erweiterung ist mit einem Fehler fehlgeschlagen. Die Fehlermeldung wird im Feld **Fehlermeldung** angezeigt. • Warnung: Eine Laufzeitausnahme ist aufgetreten. Die Erweiterung funktioniert weiterhin.
HTTP/HTTPS-Port	Portnummer, die die Erweiterung auf eingehende Anforderungen abhört
Authentifizierungstyp	Die verfügbaren Authentifizierungstypen sind: • **API-Schlüssel** (Standard): Von jedem Client, von dem eine Verbindung mit der Erweiterung hergestellt wird, muss ein API-Schlüssel in den Autorisierungsheader der Anforderung eingegeben werden. Weitere Informationen zum Anzeigen vorhandener API-Schlüssel finden Sie unter API-Schlüsselauthentifizierung für MID-Webserver konfigurieren. • **Schlüsselbasiert** (veraltet und nur aus Gründen der Kompatibilität mit Releases vor Yokohama beibehalten): Der Wert im Feld **Geheimer Key** wird dazu verwendet, ein Authentifizierungstoken zu generieren,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „MID-Webserver-Kontext“ (Fortsetzung)

Feld	Beschreibung
	das im **Autorisierungsheader** eingehender Client-Anforderungen gesendet wird. Details finden Sie unter Schlüsselbasierte MID-Webserverauthentifizierung konfigurieren. • **Standard**: Definieren Sie einen Benutzernamen und ein Passwort in den Feldern **Standardauthentifizierungsbenutzer** und **Benutzerkennwort für Standardauthentifizierung**, die bei Auswahl dieser Option angezeigt werden. • **mTLS**: Eine zertifikatbasierte Authentifizierung, bei der das TLS-Protokoll verwendet wird Details finden Sie unter MID-Webserver und Agent-mTLS-Authentifizierung.
Geheimer Schlüssel	Der Wert, der erzeugt wird, wenn „Schlüsselbasierte Authentifizierung“ als Wert im Feld „Authentifizierungstyp“ ausgewählt ist
Standardauthentifizierungsbenutzer	Benutzername, der bei der Auswahl der Standardauthentifizierung verwendet werden soll
Benutzerkennwort für Standardauthentifizierung	Passwort, das bei der Auswahl der Standardauthentifizierung verwendet werden soll
Sichere Verbindung	Option zur Angabe, dass von der Erweiterung das TLS-Protokoll zum Verschlüsseln eingehender Verbindungen verwendet werden soll. Für die Erweiterung muss auch eine Kombination aus Zertifikat und privatem Schlüssel angegeben werden. Wenn Sie diese Option auswählen, wird das Kontrollkästchen **Einheitlichen MID-Schlüsselspeicher verwenden** angezeigt.
Einheitlichen MID-Schlüsselspeicher verwenden	Option zur Verwendung der Option des einheitlichen MID Server-Schlüsselspeichers für eine sichere Verbindung. Deaktivieren Sie diese Option, um den **Webserver-Schlüsselspeicher** zu verwenden. Details finden Sie unter Sichere MID-Webservererweiterung konfigurieren.
Schlüsselspeicher-Zertifikatalias	Der Aliasname des Schlüsselpaars im ausgewählten Schlüsselspeicher, der von der Erweiterung zum Herstellen einer sicheren Verbindung verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „MID-Webserver-Kontext“ (Fortsetzung)

Feld	Beschreibung
	Lassen Sie dieses Feld leer, um den Standardalias zu verwenden, wenn Sie den einheitlichen MID-Schlüsselspeicher oder den Webserver-Schlüsselspeicher mit einem einzelnen Alias verwenden.
Schlüsselspeicher-Passwort	Das Passwort für den Webserver-Schlüsselspeicher, wenn dieser zum Herstellen einer sicheren Verbindung verwendet wird
Schlüsselpasswort des Schlüsselspeichers	Das Passwort des privaten Schlüsseleintrags, der dem angegebenen Alias des Webserver-Schlüsselspeichers zugeordnet ist. Dieses Feld kann leer gelassen werden, wenn das Passwort mit dem Eintrag im Feld „Schlüsselspeicher-Passwort“ übereinstimmt.
Truststore-Passwort	Das Passwort für den Truststore, der die Zertifikate der Zertifizierungsstelle (Certificate Authority, CA) enthält, die zum Validieren der Signaturen der Client-Zertifikate verwendet werden. Wird angezeigt, wenn **mTLS** als Authentifizierungstyp ausgewählt ist. Lassen Sie dieses Feld leer, wenn die Erweiterung für die Verwendung des cacerts-Truststore der JRE konfiguriert ist, in der der MID-Server ausgeführt wird.
Fehlermeldung	Nachricht, die Fehler beschreibt, die dazu führen, dass Befehle wie „Starten“ oder „Stoppen“ fehlschlagen. Dieses Feld wird nur angezeigt, wenn im Feld „Status“ der Wert „Fehler“ angezeigt wird.
Ausführen auf	Ausführungsort dieser Erweiterung. Die verfügbaren Optionen sind **Spezieller MID Server** oder **Spezieller MID Server-Cluster**.
MID Server	Je nachdem, was Sie im Feld **Ausführen auf** ausgewählt haben, ist dies der Name des festgelegten MID-Servers oder MID-Server-Clusters. • Wenn Sie **Spezifischer MID Server** ausgewählt haben: Name des festgelegten MID-Server • Wenn Sie **Spezifisches MID Server-Cluster** ausgewählt haben: Name des festgelegten MID-Server-Clusters
Ausführung auf	Zeigt den Namen des MID-Servers an, auf dem die Erweiterung ausgeführt wird, auch wenn der MID-Server nicht verfügbar ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „MID-Webserver-Kontext“ (Fortsetzung)

Feld	Beschreibung
	Wenn der Benutzer die Erweiterung stoppt, ist dieses Feld leer.

Ereignismanagement-Formular „Tag-basiertes Warnungs-Clustering-Tag“

Im Formular zum Erstellen oder Ändern eines Tag-basierten Warnungs-Clustering-Tags werden detaillierte Informationen zum Tag angezeigt.

Formular „Tag-basiertes Warnungs-Clustering-Tag“

Feld	Beschreibung
Name	Name des Clustering-Tags. Standardmäßig ist dies eine Beschreibung des konfigurierten Tags (z. B. **Exakte Übereinstimmung mit dem Warnungsfeld „ Metrikname“**). Der Standardname ist erst nach dem Speichern des Tags sichtbar. Tag-Namen müssen eindeutig sein.
Benutzerdefinierter Name	Aktivieren Sie das Kontrollkästchen, um den Wert im Feld **Name** anzupassen.
Domäne	Die Domäne, in der der aktuelle Datensatz erstellt wurde. Schreibgeschützt.
Beschreibung	Geben Sie eine optionale Beschreibung des Tags ein.
Quelle	Wählen Sie die Quelle aus, aus der das abzugleichende Feld ausgewählt werden soll. • **Warnungsfeld** • **Zusätzliche Warnungsinformationen** • **Warnungs-CI** • **Warnungs-CI-Schlüssel** • **Warnungstags** Wenn Sie **Zusätzliche Warnungsinformationen**auswählen, wählen Sie einen **Schlüssel für zusätzliche Informationen** anstelle eines Felds. **„Zusätzliche Warnungsinformationen“** ist ein Feld in der Warnung, das das Schlüssel-Wert-Paar im Jason-Format enthält, und Sie können einen bestimmten Schlüssel verwenden. **Warnungs-CI-Schlüssel**: Erstellen Sie CMDB-Schlüsselwerte, um Warnungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-basiertes Warnungs-Clustering-Tag“ (Fortsetzung)

Feld	Beschreibung
	basierend auf der Tabelle „CMDB-Schlüsselwerte“ [cmdb_key_value] zu gruppieren. Schlüsselwerte bieten eine zusätzliche Methode zur Bestimmung von Gemeinsamkeiten zwischen Warnungs-CIs.
Ausgewähltes Feld	Geben Sie das Feld an, das zwischen Warnungen übereinstimmen muss, damit die Warnungen in eine Gruppe aufgenommen werden. Wird angezeigt, wenn Sie **Alert Field** (Warnungsfeld) oder **Alert CI** (Warnungs-CI) im Feld **Source** (Quelle) auswählen. Wenn Sie im Feld **„Quelle“die Option „Warnungs-CI“** auswählen, müssen Sie einen CMDB-Schlüssel auswählen. Dem CI der Warnung wird ein CMDB-Schlüssel zugewiesen.
Key	Geben Sie den Schlüssel an, der zwischen Warnungen übereinstimmen muss, damit die Warnungen in eine Gruppe aufgenommen werden. Wird angezeigt, wenn Sie im Feld **Quelle„Zusätzliche Warnungsinformationen“** auswählen, oder wird angezeigt, wenn Sie im Feld **QuelleWarnungs-Tags** auswählen. Wenn **„Zusätzliche Warnungsinformationen“** ausgewählt ist, geben Sie im Feld „Zusätzliche Informationen“ den Namen eines der Felder ein. Wenn **Warnungs-Tags** ausgewählt ist, geben Sie den Namen des relevanten Warnungs-Tags ein.
CMDB-Schlüssel	Geben Sie den CMDB-Schlüssel an, der bei Warnungen übereinstimmen muss, die in eine Gruppe aufgenommen werden sollen. Das Feld wird angezeigt, wenn Sie **Alert CI Key** (Warnungs-CI-Schlüssel) im Feld **Quelle** auswählen.
Übereinstimmungsmethode	Wählen Sie die Art der Übereinstimmung aus, die erforderlich ist, damit die Warnungen in eine Gruppe aufgenommen werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-basiertes Warnungs-Clustering-Tag“ (Fortsetzung)

Feld	Beschreibung
	• **Exact** (Genau): Gibt an, dass der Feldwert genau übereinstimmen muss, damit die Warnung in eine Gruppe aufgenommen wird. Sie können beispielsweise ein Alarm-Clustering-Tag konfigurieren, das angibt, dass das Feld **Metrikname** der Warnung genau übereinstimmen muss, um eine Gruppe zu bilden. Wenn man dieses Tag aufruft, sind alle Warnungen mit identischen Werten in dem Feld **Metrikname** in der gleichen Gruppe enthalten. • **Fuzzy** (Ungefähr): Gibt an, dass der Feldwert eine ungefähre Übereinstimmung sein muss (abhängig vom im Feld **Similarity** (Ähnlichkeit) konfigurierten Wert), damit die Warnung in eine Gruppe aufgenommen werden kann. • **Muster**: Gibt an, dass der Feldwert dem Muster im Feld **Muster** folgen muss. Informationen zur korrekten Syntax und zu Verwendungsbeispielen finden Sie unter Musterabgleich .
Ähnlichkeit	Geben Sie den Ähnlichkeitsprozentsatz an, den die Warnungen erfüllen müssen, um in eine Gruppe aufgenommen zu werden. Wenn Sie beispielsweise 50 eingeben, müssen mindestens 50 Prozent des angegebenen Werts in der Warnung angezeigt werden, damit die Warnung in die Gruppe aufgenommen wird. Erscheint nur, wenn **Fuzzy** (Ungefähr) als Wert für **Match Method** (Übereinstimmungsmethode) ausgewählt wurde. Standardwert = 90

Liste der vordefinierten Tags für Warnungs-Clustering

Eine Liste der vordefinierten Tags für Warnungs-Clustering, die mit der Anwendung „Engine für tagbasiertes Alarm-Clustering“ bereitgestellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vordefinierte Tags für Warnungs-Clustering

Name	Quelle	Übereinstimmungsmethode
CI	em_alert.cmdb_ci	Genaue Übereinstimmung
Beschreibung	em_alert.description	Genaue Übereinstimmung
Metrikname	em_alert.metric_name	Genaue Übereinstimmung
Knoten	em_alert.node	Genaue Übereinstimmung
Ressource	em_alert.resource	Genaue Übereinstimmung
Quelle	em_alert.source	Genaue Übereinstimmung
Quellinstanz	em_alert.event_class	Genaue Übereinstimmung
Typ	em_alert.type	Genaue Übereinstimmung
Zuweisungsgruppe	em_alert.assignment_group	Genaue Übereinstimmung
CI-Klasse	cmdb_ci.sys_class_name	Genaue Übereinstimmung
DNS-Domäne	cmdb_ci.dns_domain	Genaue Übereinstimmung
IP-Adresse	cmdb_ci.ip_address	Genaue Übereinstimmung
Standort	cmdb_ci.location	Genaue Übereinstimmung
Umgebung	cmdb_ci.umgebung	Genaue Übereinstimmung
CI-Name	cmdb_ci.name	Genaue Übereinstimmung
Namespace	cmdb_ci.namespace	Genaue Übereinstimmung

Vordefinierte Tags, die aus der Connector-Nutzlast extrahiert werden

Name	Beschreibung	Standardzuordnung aus CMDB
t_ip_address	IP-Adresse	cmdb_ci.ip_address
t_application	Anwendung	-
t_region	Region	-
t_location	Standort	cmdb_ci.location
t_environment	Umgebung	cmdb_ci.umgebung
t_namespace	Namespace	cmdb_ci.namespace

Ereignismanagement-Formular „Tag-basierte Warnungs-Clustering-Definition“

Im Formular zum Erstellen oder Ändern einer Tag-basierten Warnungs-Clustering-Definition werden detaillierte Informationen zur Definition angezeigt.

Formular „Tag-basierte Warnungs-Clustering-Definition“

Feld	Beschreibung
Name	Name der Alarm-Clustering-Definition. Definitionsnamen müssen eindeutig sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-basierte Warnungs-Clustering-Definition“ (Fortsetzung)

Feld	Beschreibung
Aktiv	Wählen Sie die Option, um die Definition zu aktivieren. Diese Option ist standardmäßig ausgewählt.
Reihenfolge	Die Reihenfolge, in der Definitionen für eingehende Warnungen getestet werden. Solche mit niedrigeren Ordnungswerten werden zuerst getestet. Wenn eine Warnung mit einem der Filter der Definitionen übereinstimmt, wird die Suche nach weiteren Definitionen fortgesetzt. Standardwert = 1.000
Domäne	Die Domäne, in der der aktuelle Datensatz erstellt wurde. Schreibgeschützt.
Beschreibung	Geben Sie eine optionale Beschreibung der Alarm-Clustering-Definition ein.
Filter	Legen Sie Bedingungen fest, die eingehende Warnungen erfüllen müssen, um von den Tags der Alarm-Clustering-Definition gemessen zu werden. Wenn die Tags Warnungen entsprechen, die im System vorhanden sind und sich innerhalb des Werts **Clustering timeframe (minutes)** (Clustering-Zeitrahmen (Minuten)) befinden, werden die eingehenden Warnungen mit den vorhandenen Warnungen verbunden, um eine Warnungsgruppe zu bilden. Nachdem Sie den Filter konfiguriert haben, können Sie auf die Schaltfläche **Vorschau** klicken, um anzuzeigen, wie viele vorhandene Warnungen der Bedingung des Filters entsprechen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-basierte Warnungs-Clustering-Definition“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Übereinstimmende Warnungen werden nicht automatisch zusammen in eine Warnungsgruppe aufgenommen. Warnungen werden nur gruppiert, wenn sie über entsprechende Alarm-Clustering-Tags verfügen. • Bei Filterparametern wird standardmäßig zwischen Groß- und Kleinschreibung unterschieden. Um die Unterscheidung zwischen Groß- und Kleinschreibung zu deaktivieren, setzen Sie den *sa_analytics.correlation_case_sensitive* Parameter auf **false**. • Sie können Warnungsfelder auch so konfigurieren, dass sie von der Suche ausgeschlossen werden, indem Sie die Eigenschaft *sn_em_tbac.tag_excluded_alert_fields* verwenden. Standardmäßig werden mit dieser Eigenschaft folgende Elemente ausgeschlossen: ◦ Typ ◦ event_class
Gruppenbeschreibung überschreiben	Standardgruppenbeschreibungen beginnen mit dem Präfix „Gruppe von Warnungen“, gefolgt von der Beschreibung der primären Warnung in der Gruppe. Sie können diese Gruppenbeschreibung überschreiben, indem Sie das Kontrollkästchen **Gruppenbeschreibung überschreiben** aktivieren. Geben Sie dann im Feld **Anwenderdefinierte Beschreibung** eine Beschreibung ein. Diese Beschreibung wird als Beschreibung der Gruppen verwendet, die von dieser Warnungs-Clustering-Definition erstellt werden. **Hinweis:** Sie können das Formular nicht speichern, wenn Sie das Feld „Anwenderdefinierte Beschreibung“ leer oder mit dem Standardtext „Gruppe von Warnungen“ gelassen haben.
Clustering-Zeitrahmen (Minuten)	Die maximale Zeit in Minuten, die zwischen Warnungen für die Warnungsgruppierung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Tag-basierte Warnungs-Clustering-Definition“ (Fortsetzung)

Feld	Beschreibung
	zulässig ist. Zum Beispiel gibt ein Wert von 60 an, dass eine Warnung, die innerhalb von 60 Minuten nach der letzten Warnung generiert wurde, in der Warnungsgruppe enthalten ist. Alle nach dieser Zeit generierten Warnungen werden nicht in die Warnungsgruppe aufgenommen. Standardwert = 60 Erlaubte Werte = 0-1440
M2M-Zuweisung von Definitionen und Tags für tag-basiertes Warnungs-Clustering	Wählen Sie die Alarm-Clustering-Tags aus, die der Alarm-Clustering-Definition zugewiesen werden sollen. Warnungen, die die in den ausgewählten Tags angegebenen Kriterien erfüllen, werden in die Warnungsgruppe aufgenommen. Die verfügbaren Optionen sind die Tags, die auf der Seite **Tag Based Alert Clustering Tags** (Tag-basiertes Alarm-Clustering) erstellt wurden.

Liste der vordefinierten Definitionen für tagbasiertes Warnungs-Clustering

Eine Liste der vordefinierten Definitionen für Warnungs-Clustering, die mit der Anwendung „Engine für tagbasiertes Alarm-Clustering“ bereitgestellt werden.

Vordefinierte Definitionen für Warnungs-Clustering

Name	Beschreibung	Auftrag
Gruppenwarnungen aus derselben Anwendung	Gruppieren Sie alle Warnungen aus derselben Anwendung, die in den letzten 10 Minuten erstellt wurden. In neuen Systemen ist diese Definition standardmäßig aktiviert.	9010
Gruppieren Sie alle Warnungen von derselben IP-Adresse	Alle Warnungen von derselben IP-Adresse gruppieren, die in den letzten 10 Minuten erstellt wurden.	9020
Gruppieren Sie alle Warnungen aus demselben Namespace	Alle Warnungen aus demselben Namespace gruppieren, die in den letzten 10 Minuten erstellt wurden. In neuen Systemen ist diese Definition standardmäßig aktiviert.	9030
Alle Warnungen aus demselben Subnetz gruppieren	Alle Warnungen aus demselben Subnetz gruppieren, die in den letzten 10 Minuten erstellt wurden. In neuen Systemen ist diese Definition standardmäßig aktiviert.	9040
Gruppenwarnungen aus derselben CI-Klasse und demselben Standort	Gruppieren Sie alle Warnungen aus derselben CI-Klasse und demselben Ort, die in den letzten 10 Minuten erstellt wurden.	9050

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vordefinierte Definitionen für Warnungs-Clustering (Fortsetzung)

Name	Beschreibung	Auftrag
Gruppenwarnungen aus derselben Anwendung und Umgebung	Alle Warnungen aus derselben Anwendung und Umgebung gruppieren, die in den letzten 10 Minuten erstellt wurden.	9060
Gruppieren Sie alle Warnungen von einem ähnlichen Knoten	Alle Warnungen von einem ähnlichen Knotennamen gruppieren, die in den letzten 10 Minuten erstellt wurden.	9070
Gruppenwarnungen von desselben Standorts und derselben Zuweisungsgruppe	Gruppieren Sie alle Warnungen vom gleichen Standort und von der gleichen Zuweisungsgruppe, die in den letzten 10 Minuten erstellt wurden.	9080
Gruppenwarnungen aus derselben Region und Metrik	Alle Warnungen aus derselben Region und Metrik gruppieren, die in den letzten 10 Minuten erstellt wurden.	9090
Gruppenwarnungen aus derselben CI-Klasse und Metrik	Alle in den letzten 10 Minuten erstellten Warnungen aus derselben CI-Klasse und Metrik gruppieren.	9100
Gruppenwarnungen von demselben Knoten und derselben Metrik	Alle Warnungen aus demselben Knoten und derselben Metrik gruppieren, die in den letzten 10 Minuten erstellt wurden.	9110
Gruppenwarnungen von derselben Zuweisungsgruppe und Klasse	Gruppieren Sie alle Warnungen aus derselben Zuweisungsgruppe und Klasse, die in den letzten 10 Minuten erstellt wurden.	9120
Gruppenwarnungen von mit gleichem Typ, gleicher Metrik und gleicher Quelle	Gruppieren Sie alle Warnungen aus demselben Typ, derselben Metrik und derselben Quellinstanz, die in den letzten 10 Minuten erstellt wurden.	9130
Gruppenwarnungen von demselben CI	Alle Warnungen aus demselben CI gruppieren, die in den letzten 10 Minuten erstellt wurden. **Wichtig:** Wenn diese Regel aktiv ist, muss die Gruppierung CMDB deaktiviert werden.	9140
Gruppenwarnungen von demselben Knoten	Alle Warnungen vom gleichen Knoten gruppieren, die in den letzten 10 Minuten erstellt wurden. In neuen Systemen ist diese Regel standardmäßig aktiviert.	9150

Mit installierte Domäneneigenschaften Ereignismanagement

Verwenden Sie die mit Ereignismanagement installierten Domäneneigenschaften, um die Metadaten bereitzustellen, die auf die entsprechende Tabelle verweisen, um die Domäne zu identifizieren, damit Sie wissen, in welcher Domäne das Ereignis erstellt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standardmäßige Domänenmetadateneigenschaften

Eigenschaft
evt_mgmt Connector_domain_info_table_name
evt_mgmt Connector_domain_info_column_name
evt_mgmt Connector_domain_id_column_name
evt_mgmt Connector_domain_path_column_name

Metadaten der Connector-Domäne

Überschreiben Sie die mit Ereignismanagement installierten Standardmetadatenwerte des Push-Connectors mit den Werten in der Ereignis-HTTP-Anforderung, einschließlich URL, Header, Anforderungstext (Nutzlast) und Connector-Parameter. Überschreiben Sie die Metadatenwerte der Pull-Connector-Domäne nur mit Connector-Parametern.

Domänenmetadatenparameter

Name	Beschreibung	Überschreibt die Systemeigenschaft
connectorDomainInfoTableName	Name der Tabelle, die die Datensätze mit den Domäneninformationen enthält.	evt_mgmt.connector_domain_info_table_nam • **Typ**: Zeichenfolge • **Standardwert**: core_company
connectorDomainInfoColumnName	Name der Spalte, die einen Wert enthält, der mit dem Domänenbezeichner übereinstimmen muss. Beispielsweise möchten Sie möglicherweise einen Datensatz in der Tabelle „Domäneninformationen“ identifizieren, der einen übereinstimmenden Wert	evt_mgmt.connector_domain_info_column_n • **Typ**: Zeichenfolge • **Standardwert**: Name

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Überschreibt die Systemeigenschaft
	im Feld **„company_name“** enthält.	
connectorDomainIdColumnName	Name der Tabellenspalte, in der die Domänen-ID gespeichert wird.	evt_mgmt.connector_domain_id_column_na • **Typ**: Zeichenfolge • **Standardwert**: sys_domain
connectorDomainPathColumnName	Name der Tabellenspalte, in der der Domänenpfad gespeichert wird.	evt_mgmt.connector_domain_path_column_ • **Typ**: Zeichenfolge • **Standardwert**: sys_domain_path

Präferenzreihenfolge für den Zugriff auf Domänenmetadaten

Sie müssen Domänenmetadaten angeben, um personalisierte Push-Connector-Domänen zu konfigurieren. Die Metadaten in der bevorzugten Zugriffsreihenfolge sind:

1. Push-Connector-Parameter
2. URL-Abfrageparameter
3. HTTP-Header
4. Anforderungstext (Nutzlast)
5. Standardsystemeigenschaften

URL-Abfrageparameter

Push-Connectors weisen die folgende URL-Syntax auf:

- Instanztyp: `https://`<instance-name> .service-now.com/api/sn_em_connector/em/inbound_event?source=<connector-source>
- MID-Server Typ: `http://`<MID_Server_IP> :<MID_Web_Server_Port> /api/mid/em/inbound_event?Transform=<connector-transform-script-name>

Sie können Domänenmetadaten als zusätzliche Abfrageparameter in die Webhook-URL des Push-Connectors ServiceNow aufnehmen. Wenn die Domäneninformationsquelle beispielsweise die Tabelle „sys_user“ ist, könnte die URL „`https://`“lauten.<instance-name> .service-now.com/api/sn_em_connector/em/inbound_event?source=<connector-source> &connectorDomainInfoTableName=sys_user

Anforderungskopfzeilen.

Alle Domänenmetadateneigenschaften können als Teil von HTTP-Anforderungsheadern übergeben werden. Informationen zum Festlegen von Anforderungsheadern finden Sie in der Dokumentation Ihres Drittanbieter-Überwachungstools.

Anforderungstext (Nutzlast)

Sie können Domänenmetadaten aus dem Anforderungstext (JSON-Nutzlast) referenzieren, indem Sie die Metadatenparameter als Schlüssel auf Stammebene in der Nutzlast festlegen. Das folgende Beispiel zeigt, wie die Parameter *connectorDomainInfoTableName* und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

connectorDomainInfoColumnName als Teil des Anforderungstextes übergeben werden können:

```
{
    „source“: „Azure Monitor“,
    „Host“: „127.0.0.1“,
    „company“: „ServiceNow“,
    „connectorDomainInfoTableName“: „sys_user“,
    „connectorDomainInfoColumnName“: „first_name“
    }
```

Hinweis: Informationen zu Connector-Parametern finden Sie unter Personalisieren Sie Domänen für Push-Connector-Ereignisse zur Verwendung bei der Ereigniserstellung.

Dynatrace Formular für die Connector-Instanz

Das Formular für die Dynatrace -Connector-Instanz zeigt die Felder an, die Sie beim Erstellen einer Dynatrace -Connector-Instanz ausfüllen müssen.

Connector-Instanzseite

Feld	Beschreibung
Name	Eindeutiger Name für die Metrik-Connector-Instanz Dynatrace.
Beschreibung	Beschreibung für die Verwendung der Connector-Instanz.
Anschlussdefinition	Die Connector-Definition, die vom Connector verwendet werden soll. Wählen Sie **Dynatrace-Metriken**aus.
Host-IP	Hostname/IP-Adresse des Dynatrace -Servers.
Referenz	Wählen Sie das Suchsymbol und anschließend die vorhandenen API-Schlüssel-Anmeldeinformationen aus. Wenn diese Anmeldeinformationen nicht vorhanden sind, erstellen Sie wie folgt neue Anmeldeinformationen: **1.** Vergewissern Sie sich, dass Sie über ein Zugriffstoken mit Berechtigungen zum Lesen der Metrik (metrics.read) verfügen, das in der Anwenderoberfläche Dynatrace erstellt wurde. **2.** Wählen Sie **Neu** aus, nachdem Sie das Suchsymbol ausgewählt haben. **3.** Wählen Sie **API Key-Anmeldeinformationen**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connector-Instanzseite (Fortsetzung)

Feld	Beschreibung
	4. Geben Sie im Feld **API-Schlüssel** das Zugriffstoken aus der UI Dynatrace ein. 5. Geben Sie im Feld **Name** einen beschreibenden Namen ein, um die Anmeldeinformationen eindeutig zu identifizieren. 6. Füllen Sie alle anderen relevanten Felder aus, und wählen Sie **Absenden**aus.
Metriksammlung	Standardmäßig ausgewählt. Schreibgeschützt.
Zeitplan für Metriksammlung (Sekunden)	Zeitintervall (in Sekunden), in dem der Metrik-Connector Metriken vom Server Dynatrace abruft. Standard: 60.
Aktiv	Wählen Sie diese Option aus, um die Connector-Instanz zu aktivieren.

Dynatrace Wertparameter der Connector-Instanz

Die folgende Tabelle zeigt die Wertparameter der Connector-Instanz Dynatrace, die Sie beim Erstellen einer Connector-Instanz Dynatrace nach Bedarf ausfüllen können.

Wertparameter der Connector-Instanz

Parameter	Beschreibung
debuggen	Legen Sie den Wert auf **„wahr“** fest, um Debug-Protokolle zu aktivieren. Standardwert: false
initialSyncInMins	Anzahl der Minuten vor dem aktuellen Zeitpunkt, zu der die erste Metriksammlung ausgeführt wird. Beispiel: Wenn der Wert 15 ist, ruft der Connector Metriken aus den letzten 15 Minuten ab. Standard: 15
logPayload	Bestimmt, ob die Nutzlast des Rohprotokolls gedruckt werden soll. Legen Sie den Wert nur für Debugging-Zwecke auf **„wahr“** fest, da das Drucken der Rohnutzlast die Protokolle MID-Server schnell füllt. Standardwert: false
maxMetricsProQuery	Maximale Anzahl von Metrik-IDs, die pro API-Aufruf an Dynatraceabgefragt werden sollen. Der Wert darf 32 nicht überschreiten, den von Dynatracezulässigen Höchstwert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wertparameter der Connector-Instanz (Fortsetzung)

Parameter	Beschreibung
	Standard: 32
pageSize	Maximale Anzahl von Datensätzen, die in einer API-Antwort von Dynatracezurückgegeben werden sollen. Standard: 500
port	Portnummer für den Dynatrace -Server, mit dem eine Verbindung hergestellt werden soll. leer
protocol	Protokoll für die Verbindung mit dem Server Dynatrace. Standardwert: https.
DrosselApiCalls	Bestimmt, ob die Drosselung aktiviert ist. Wenn diese Option aktiviert ist (**true**), wird ein Grenzwert für die Anzahl der API-Aufrufe auf Dynatrace pro Minute festgelegt. Standardwert: false
AnforderungProMinute	Die Grenze für die Anzahl der API-Aufrufe auf Dynatrace pro Minute. Nur relevant, wenn *`throttleApiCalls`* = **wahr**. Standardwert: 1000

Formular der Push-Connector-Instanz

Das Formular „Push-Connector-Instanz“ zeigt die Felder an, die Sie beim Erstellen oder Ändern eines Connectors ausfüllen müssen.

Feld	Beschreibung
Name	Ein eindeutiger Name für den Datensatz der Connector-Instanz, z. B. der Name eines Ereignisquellhosts.
Beschreibung	Alle optionalen Informationen, die der Administrator zur Identifizierung dieses Datensatzes verwenden möchte.
Definition des Push-Connectors	Wählen Sie die Definition für das externe System aus, von dem Sie Ereignisse empfangen möchten. Sie können eine beliebige vorhandene Definition auswählen, z. B.:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Thousandeyes • Dynatrace • Catchpoints Eine Liste der im Basissystem verfügbaren Connector-Definitionen finden Sie unter Konfigurieren Sie Ereignismanagement die -Connectors. **Hinweis:** Wenn für den von Ihnen ausgewählten Push-Connector-Typ Konfigurationsparameter verfügbar sind, werden sie unter Konfigurationsparameter für Push-Connector-Instanz angezeigt.
MID-Server	Zeigt die Liste von MID Servers an, für die mindestens ein MID-Server -Ereignis-Listener-Kontext aktiv ist. Der Abschnitt MID-Server wird nur angezeigt, wenn der Definitionstyp MID ausgewählt ist.
URL	Dieses Feld wird nur nach dem Speichern der Details der Connector-Instanz automatisch ausgefüllt. Instanz: Die URL muss in einem externen System mit den Anmeldeinformationen ServiceNow konfiguriert werden, die über die Rolle evt_mgmt_integration verfügen, um die Ereignisse zu empfangen. MID-Push-Connector-Instanz: Die URL muss von einem externen System mit MID-Webservererweiterung konfigurieren -Anmeldeinformationen aus konfiguriert werden, um die Ereignisse zu empfangen. Dieses Feld wird nur angezeigt, nachdem das Formular gespeichert wurde.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um den Empfang von Ereignissen von dieser externen Ereignisquelle zu aktivieren. Dieses Feld wird nur angezeigt, nachdem das Formular gespeichert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular der SCOM-Connector-Instanz

Das Formular SCOM-Connector-Instanz zeigt die Felder an, die Sie beim Erstellen einer SCOM-Connector-Instanz ausfüllen müssen.

Connector-Instanzseite

Feld	Beschreibung
Name	Einzigartiger Name für die SCOM-Connector-Instanz.
Beschreibung	Beschreibung für die Verwendung der Instanz der SCOM-Ereigniserfassung.
Aktiv	Wählen Sie diese Option aus, um die Connector-Instanz zu aktivieren. Wird nur angezeigt, wenn eine bereits erstellte Connector-Instanz ausgewählt wird.
Connector-Definition	Lieferant und Protokoll, die zum Sammeln von Ereignissen aus der externen Quelle verwendet werden. Wählen Sie für einen regulären SCOM-Connector **SCOM**aus. Wählen Sie für eine Connector-Instanz, für die Sie Metriken überwachen möchten, **SCOM-Metriken**aus. Wenn Sie diese Option auswählen, werden die Felder in der Feldertabelle **Connector-Instanz – Metriken** angezeigt.
Zuweisungsgruppe	Wählen Sie die Gruppe aus, der die Connector-Instanz zugewiesen ist. Dies kann beispielsweise eine Gruppe von Administratoren oder eine Supportgruppe sein.
Host-IP	Geben Sie die SCOM-IP-Adresse an. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** als Connector-Definition ausgewählt sind.
Referenz	Wählen Sie die Windows-Anmeldeinformationen aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connector-Instanzseite (Fortsetzung)

Feld	Beschreibung
	Hinweis: Vergewissern Sie sich beim Konfigurieren von Windows-Anmeldeinformationen, wenn diese für bestimmte MID Server gelten, dass die von Ihnen im Anmeldeinformationsdatensatz angegebenen MID Server mit den im Abschnitt **MID Server für Anschlüsse** auf dem Formular „Anschlussinstanz“ angegebenen MID Servern übereinstimmen. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** als Connector-Definition ausgewählt sind.
Zeit der letzten Ausführung der Ereignissammlung	Die letzte Ausführungszeitwert der Ereigniserfassung wird automatisch aktualisiert. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** als Connector-Definition ausgewählt sind.
Status der letzten Ereignissammlung	Die letzte Ausführungszeitstatus der Ereigniserfassung wird automatisch aktualisiert. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** als Connector-Definition ausgewählt sind.
Zeitplan für Ereignissammlung (Sekunden)	Die Häufigkeit in Sekunden, mit der das System nach neuen Ereignissen von SCOM sucht. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** als Connector-Definition ausgewählt sind.
Bidirektional	Wählen Sie diese Option, um die bidirektionale Option aufzurufen. Diese Option ermöglicht sie den bidirektionalen Austausch von Werten mit der externen Event-Quelle. Für SCOM ist eine Standardimplementierung vorhanden. Die Option **Letzter bidirektionaler Status** wird nur angezeigt, wenn diese Option ausgewählt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connector-Instanzseite (Fortsetzung)

Feld	Beschreibung
	Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** als Connector-Definition ausgewählt sind.
Letzter bidirektionaler Status	Das Feld wird automatisch mit einem Wert ausgefüllt. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** als Connector-Definition ausgewählt sind.
Letzte Fehlermeldung	Das Feld der letzten Fehlermeldung wird automatisch aktualisiert. Diese Nachricht ist die letzte Fehlermeldung, die vom Connector empfangen wurde. Wenn der Test-Connector fehlschlägt, wird in diesem Feld eine Fehlermeldung angezeigt. Dieses Feld wird nicht angezeigt, wenn **SCOM-Metriken** als Connector-Definition ausgewählt sind.
MID Server (Abschnitt MID Server für Connectors)	Geben Sie einen oder mehrere MID Servers an, die aktiv und gültig sind. MID Servers werden in der Reihenfolge sortiert, in der ihre Daten im Abschnitt MID-Server für Connectors eingegeben wurden. Die Portanforderung von MID-Server zum SCOM-Server lautet `1433`. Wenn sich der angegebene MID-Server in einem Cluster befindet, kann er nicht ausgewählt werden, und stattdessen wird ein anderer verfügbarer MID-Server ausgewählt. Stellen Sie sicher, dass der angegebene MID Servers mit dem auf der Seite mit den Windows-Anmeldeinformationen angegebenen Wert MID Servers übereinstimmt, da der Connector Windows-Anmeldeinformationen für den Zugriff auf MID Serversverwendet. Wenn kein MID-Server angegeben ist, wird ein verfügbarer MID-Server mit übereinstimmendem IP-Bereich verwendet.

Connector-Instanz – Metrikfelder (angezeigt, wenn Connector-Definition = SCOM-Metriken)

Feld	Beschreibung
Metrikensammlung	Standardmäßig ausgewählt. Schreibgeschützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Connector-Instanz – Metrikfelder (angezeigt, wenn Connector-Definition = SCOM-Metriken) (Fortsetzung)

Feld	Beschreibung
Zeit der letzten Ausführung der Metriksammlung	Die letzte Ausführungszeit der geplanten Aufgabe „Metrikensammlung“. Dieses Feld ist schreibgeschützt.
Letzter Metriksammlungsstatus	Status der Aktivität zur Metrikdaten-Erfassung. Das Feld wird automatisch mit einem Wert ausgefüllt. Dieses Feld ist schreibgeschützt.
Zeitplan für Metriksammlung (Sekunden)	Die Zeit in Sekunden zur Wiederholung der geplanten Aufgabe Metrikdaten Sammlung.
Metrikendatenbank-Host	Die IP-Adresse oder der Hostname des Metrikdatenbank-Hosts.
Verbindung mithilfe einer benannten Instanz	Wenn ausgewählt, wird die Verbindung mit der angegebenen benannten Instanz hergestellt. Andernfalls wird die Verbindung über den angegebenen Port hergestellt.
Metrikendatenbank-Port	Der von der Metrikdatenbank verwendete Port. Die Verbindung wird über JDBC hergestellt. Die Standardportnummer ist 1433. Wenn **Verbindung mithilfe einer benannten Instanz** herstellen ausgewählt ist, wird diese Option nicht angezeigt.
Metrikendatenbank – benannte Instanz	Der Name der Metrikdatenbank-Instanz.
Datenbank-Login mit Windows-Authentifizierung	Führen Sie die Datenbank-Login mit den Anmeldeinformationen des angemeldeten Anwenders durch, der im Service MID-Server definiert ist.
Metrikendatenbank-Anmeldeinformationen	Anmeldeinformationen für die Metrikdatenbank. Verwenden Sie JDBC-Anmeldeinformationen für den lokalen Datenbankbenutzer. Wenn **die Datenbankanmeldung mit Windows-Authentifizierung** ausgewählt ist, wird diese Option nicht angezeigt.

Eigenschaften für die Ereignisweiterleitung

Mit mehreren Systemeigenschaften können Sie einen Ereignis-Weiterleitungsauftrag anpassen.

Hinweis: Um auf die Tabelle „Systemeigenschaften“ [sys_properties] zuzugreifen, geben Sie im Navigationsfilter `sys_properties.list` ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
evt_mgmt.event_sync.sources_to_exclude	Liste der Ereignisquellen, aus denen Ereignisse nicht weitergeleitet werden sollen. Standardmäßig werden alle Ereignisse weitergeleitet. Trennen Sie mehrere Quellen durch Kommas. • **Typ**: Zeichenfolge • **Standardwert**: Leer
evt_mgmt.event_sync.event_fields_to_include	Liste der Ereignisfelder, die beim Senden von Ereignissen an die Zielinstanz neben den erforderlichen Standardfeldern einzubeziehen sind: solution_state, event_class, zusätzliche_Info, Knoten, Ressource, cmdb_ci,severity, time_of_event, message_key, sys_domain, metric_name, ci_type, ci_identifier, Typ, Quelle, Beschreibung , und sys_domain_path. Trennen Sie mehrere Felder durch Kommas. • **Typ**: Zeichenfolge • **Standardwert**: Leer
evt_mgmt.event_sync.event_batch_size	Maximale Anzahl von Ereignissen, die beim Senden an die Zielinstanz gestapelt werden sollen. • **Typ**: Ganzzahl • **Standardwert**: 500
evt_mgmt.event_sync.max_payload_size_in_mb	Maximale Größe der Ereignisnutzlast in MB, die gleichzeitig an die Zielinstanz gesendet wird. • **Typ**: Ganzzahl • **Standardwert**: 5
evt_mgmt.event_sync.max_events_to_sync_per_day	Maximale Anzahl der Ereignisse, die pro Tag von der Instanz weitergeleitet werden können, um die Auswirkungen auf die Leistung auf der Quellinstanz zu minimieren. • **Typ**: Ganzzahl • **Standardwert**: 100000
evt_mgmt.event_sync.log_debug	Aktiviert oder deaktiviert die Debug-Protokollierung für die Ereignis-Weiterleitung. Legen Sie diese Eigenschaft auf „wahr“ fest, um Debugging-Informationen zu protokollieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	• **Typ**: Boolesch • **Standardwert**: Falsch

Teambasierte Integrationseigenschaften

Mit den Systemeigenschaften für die teambasierte Integration können Sie die Zuweisungsgruppenfunktion für vorhandene und neue Kunden für Ereignisregeln und Ereignisfeldzuordnung anpassen.

Systemeigenschaften für die teambasierte Integration

Eigenschaft	Beschreibung
evt_mgmt.alert_auto_assignment_field	Die Eigenschaft bestimmt die automatische W eine geordnete Liste kommagetrennter Felder Der Standardwert dieser Eigenschaft ist cmdb_ IntegrationGroup. Der Wert der Zuweisungsgru Feld **Supportgruppe** (cmdb_ci.support_group) übernommen. Wenn dieses Feld leer ist, wird d IntegrationGroup im Feld **Zuweisungsgruppe** in Instanzen [em_connector_instance] übernomm Bei aktualisierten Instanzen aus früheren Familie leer, um Auswirkungen auf die Produktionsinsta • **Typ**: Zeichenfolge • **Standardwert**: ◦ Leer – für aktualisierte Kunden ◦ cmdb_ci.support_group, IntegrationGroup **Hinweis:** Wenn Sie ein Warnungsfeld in d verwenden, z. B. ein Warnungsfeld im Feld **Informationen“**, ein Warnungs-Tag oder ei muss der Wert des Felds **„Zuweisungsgrupp** sein. Beispiel: `{"Warnungsfeldname":"`<sy sys_user_group record> "}. .
evt_mgmt.enable_group_level_event_rules	Aktiviert die teambasierte Funktionalität zum A Regeln und Event-Feldzuordnungsregeln. Glob Vorrang vor bestimmten teambasierten Regeln • **Typ**: Boolesch • **Standardwert**: ◦ Falsch – für aktualisierte Kunden ◦ Wahr – für Neukunden

Automatische Übersetzung

Formular „Warnungsabfrage“.

Sie können ähnliche Warnungen kombinieren, die bestimmte Kriterien für einen bestimmten Service erfüllen, indem Sie eine Warnungsabfrage erstellen.

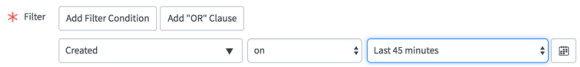
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Warnungsabfrage“.

Feld	Beschreibung
Name	Der Name der Warnungsabfrage.
Business-Relevanz	Die Bedeutung dieser Warnungsabfrage für das Unternehmen. Mit diesem Feld können Notfallwiederherstellungsstrategien für diese Warnungsabfrage ermittelt werden. • 1: sehr kritisch • 2: Kritisch • 3: weniger kritisch • 4: nicht kritisch
Verwendet für	Der Zweck der Warnungsabfrage. Wählen Sie aus: • Produktion (Standard) • Staging • QA • Test • Entwicklung • Demonstration • Schulung • Notfallwiederherstellung
Eigentum von	Partei, die für die Warnungsabfrage verantwortlich ist.
E-Mail	Der E-Mail-Alias für die Warnungsabfrage.
Telefon (geschäftlich)	Die Telefonnummer für das Unternehmen.
Betriebsstatus	Der Status der Warnungsabfrage. • **Funktionsfähig**: Die Warnungsabfrage wird ausgeführt. Die Berechnung der Auswirkung wird nur für Warnungsabfragen im Status „Operativ“ ausgeführt. Wählen Sie diese Option aus, um diesen Service zu verwenden. Wenn Sie vorkonfigurierte Optionen für diese Kategorie angepasst haben, wählen Sie die Option aus, deren Wert auf 1 festgelegt ist. Ereignismanagement berechnet die Auswirkung nur auf die verwendeten Services. Wenn Sie diesen Service jetzt nicht verwenden möchten, wählen Sie eine der folgenden Optionen: • **Nicht funktionsfähig**: Die Warnungsabfrage ist nicht verfügbar, deaktiviert oder ausgefallen. • **Reparatur in Bearbeitung**: Die Warnungsabfrage wird gewartet. • **DR-Standby**: Die Warnungsabfrage ist als Notfallwiederherstellungs-Bereitschaft verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Warnungsabfrage“. (Fortsetzung)

Feld	Beschreibung
	• **Bereit**: Die Warnungsabfrage ist zur Verwendung vorbereitet. • **Deaktiviert**: Die Warnungsabfrage wird der aktiven Verwendung entzogen.
Kommentare	Zusätzliche Hinweise und Informationen.
Servicegruppenmitglieder	Die Servicegruppe, die diesen Service enthält.
Filter	Die Bedingungen für das Senden einer Benachrichtigung an die Warnungsabfrage. Die Bedingungen müssen die Warnungswerte erfüllen. **Hinweis:** • Beziehen Sie bei der Definition eines Warnungsabfragefilters nur Felder ein, die in der Tabelle „Warnungsverläufe“ [em_alert_history] angezeigt werden. Die Berechnung der Auswirkung basiert auf Warnungsverlaufsdaten, und Felder wie „Gesamtanzahl der Ereignisse“, „Priorität“ und „Prioritätsgruppe“ werden nicht in die Tabelle „Warnungsverläufe“ [em_alert_history] kopiert. • Geben Sie keine dynamische Zeitbedingung an. Geben Sie im Filter beispielsweise nicht die Bedingung `Erstellt` der `Letzte 45 Minuten` an, da die Berechnung der Auswirkung durch eine Änderung der Warnung oder Warnungsabfrage ausgelöst wird. Für die dynamische Zeitbedingung hat sich jedoch keine dieser Bedingungen geändert.  • Einige Filter können die Auswirkungsberechnung verlangsamen. Um dieses Problem zu lösen, passen Sie Ihre Warnungsabfrage an, indem Sie einen entsprechenden Index hinzufügen (siehe Indexvorschläge für langsame Abfragen) .

Formular für Warnungskorrelationsregel

Verwalten Sie die Felder, die definieren, wie Warnungen korreliert und gruppiert werden.

Formular für Warnungskorrelationsregel

Feld	Beschreibung
Name	Name der Korrelationsregel.
Auftrag	Die Auswertungspriorität für die Regel. Regeln mit niedrigeren numerischen Werten werden mit höherer Priorität behandelt. Eine Warnung wird für jede Warnungsaktionsregel ausgewertet, bis eine Übereinstimmung gefunden wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Warnungskorrelationsregel (Fortsetzung)

Feld	Beschreibung
	Wenn Sie beispielsweise zwei Warnungskorrelationsregeln mit den Prioritäten 10 bzw. 20 haben, wird die Regel mit der Priorität 10 zuerst ausgewertet. Wenn eine Warnung die Kriterien der Regel mit Priorität 10 erfüllt, werden keine weiteren Regeln überprüft. Wenn dies nicht übereinstimmt, wird die Warnung anhand der Regel mit Priorität 20 ausgewertet.
Aktiv	Option zum Aktivieren oder Deaktivieren der Regel.
Erweitert	Option zum Wechseln in den erweiterten Modus, in dem Sie anwenderdefinierte Skripts verwenden können, um Ihre eigene Logik zu definieren. Die Beispielkorrelationsregel, **Warnungskorrelationsregel SAMPLE**, wird als Referenz sofort einsatzbereit bereitgestellt. Sie können das verfügbare Skript als Leitfaden verwenden. **Hinweis:** Die **Filterbedingung** gibt an, für welche Warnungen die Regel gilt. Stellen Sie sicher, dass dieselbe Bedingung im erweiterten Skript verwendet wird, um Warnungen zu identifizieren, die in die Gruppe aufgenommen werden sollen.
Beschreibung	Eine Beschreibung der Regel.
Primäre Warnung	Die Filterbedingung, welche die primäre (bzw. wichtigste) Warnung in einem Satz zugehöriger Warnungen identifiziert. Dieses Feld erscheint nicht, wenn **Erweitert** ausgewählt ist.
Sekundäre Warnung	Die Filterbedingung, welche die zur primären Warnung zugehörige Warnung von geringerer Bedeutung identifiziert. Dieses Feld erscheint nicht, wenn **Erweitert** ausgewählt ist.
Filter	Die Filterbedingung, welche die Warnung identifiziert, für die das Skript ausgeführt wird. **Filter** ist nur verfügbar, wenn **Erweitert** ausgewählt ist. Bei Filterparametern wird standardmäßig zwischen Groß- und Kleinschreibung unterschieden. Um die Unterscheidung zwischen Groß- und Kleinschreibung zu deaktivieren, setzen Sie den *sa_analytics.correlation_case_sensitive*-Parameter auf **false**.
Beziehungstyp	Geben Sie den Beziehungstyp zwischen der primären und sekundären Warnung an: • **Keine Beziehung**: Die Beziehung wird ignoriert, wenn Sie nach einer Übereinstimmung suchen. • **Gleiches CI oder gleicher Knoten**: Beziehen Sie beide Warnungen auf dasselbe CI. Wenn das CI-Feld leer ist, müssen die Warnungen denselben Knotenwert haben. • **Primär ist übergeordnet**: Verknüpfen Sie die Warnungen, wobei die primäre Warnung das übergeordnete Element in einer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Warnungskorrelationsregel (Fortsetzung)

Feld	Beschreibung
	Übergeordnet/Untergeordnet-Beziehung ist, wie in der Tabelle mit den CI-Beziehungstypen [cmdb_rel_ci] beschrieben. • **Primär ist untergeordnet**: Verknüpfen Sie die Warnungen, wobei die primäre Warnung das untergeordnete Element in einer Beziehung zwischen unter- und übergeordneten Elementen ist, wie in der CI-Beziehungstabelle [cmdb_rel_ci] beschrieben. Dieses Feld wird nicht angezeigt, wenn das Kontrollkästchen **Erweitert** aktiviert ist.
Zeitunterschied in Minuten	Die Zeitspanne in Minuten, in denen das primäre und das sekundäre Event eintreten müssen, damit diese Regel erfüllt wird. Der Standardwert beträgt 60 Minuten. **Hinweis:** Der Wert für diesen Eintrag kann nicht größer sein als 1440 Minuten (ein Tag). Dieses Feld erscheint nicht, wenn **Erweitert** ausgewählt ist.

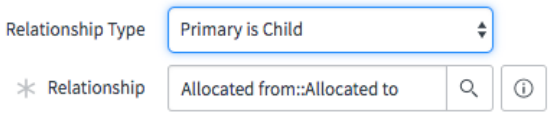
Skript	Ein benutzerdefiniertes Skript, durch dessen Bearbeitung Sie eine JSON-Zeichenfolge zurückgeben können, welche die primären und sekundären Warnungen angibt.
	
	Wählen Sie **Erweitert** aus, um das Skript-Feld anzuzeigen.
	
	`(/* The function needs to return a JSON-{correlationType:[correlatedAlerts]}`
	`for example: if your filter matches the alert, set the alert as the primary alert and set alerts 1, 2 and 3 each as secondary alerts.`
	
	`You can use both multiple primary alerts and multiple secondary alerts.`
	`The correlationType can be PRIMARY or SECONDARY, and the alerts ID must be in an array.`
	`CurrentAlert is the GlideRecord of the currentAlert on which that rule runs.`
	`The system supports only one primary per alert, so:`
	`Do not correlate more than one alert under the PRIMARY array.`
	`Do not correlate alerts that already have a primary under the SECONDARY array.`
	`The system supports open alerts only, so do not correlate alerts that have been closed under either one of the arrays.`
	`*/`
	
	`(function findCorrelatedAlerts(currentAlert){`
	
	`var result = {}; //Insert your code here`
	`result = {'SECONDARY':['alertID1','alertID2','alertID3']};`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Warnungskorrelationsregel (Fortsetzung)

Feld	Beschreibung

	`return JSON.stringify(result);`
	
	`})(currentAlert);`

Beziehung	Beschreibung der CI-Beziehung zwischen den primären und sekundären Elementen, z. B. *Zugeordnet von::Zugeordnet an* oder *Zugeordnet an::Zugeordnet von*. Dieses Feld wird nur angezeigt, wenn entweder **Primäres Element ist übergeordnet** oder **Primäres Element ist untergeordnet** als **Beziehungstyp** ausgewählt ist.  Dieses Feld erscheint nicht, wenn **Erweitert** ausgewählt ist.

Health Log Analytics

Mithilfe der Anwendung ServiceNow® Health Log Analytics können Sie IT-Probleme vermeiden, bevor Benutzer durch sie beeinträchtigt werden. Sie hilft Ihnen, die Ursache eines Problems zu identifizieren, indem Sie zugehörige Protokolle selektieren und die Rohdaten analysieren.

Health Log Analytics sammelt Streaming-Rohdaten in Ihrer Instanz und strukturiert Textdaten in Schlüssel-Wert-Paaren. In den Daten werden aussagekräftige Muster erkannt, und wenn eine Anomalie entdeckt wird, wird ein Event an die Anwendung Ereignismanagement gesendet.

Health Log Analytics ist im verfügbar ServiceNow Store .

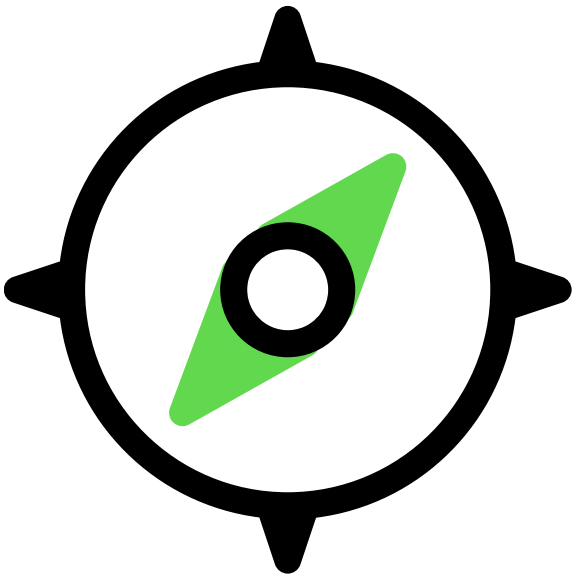
Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

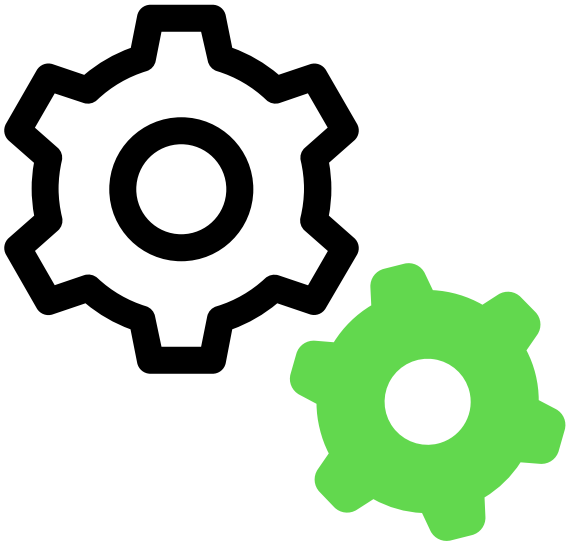
Erste Schritte

Untersuchen



Machen Sie sich mit dem Workflow, der Architektur und den allgemeinen Aufgaben Health Log Analytics von vertraut.

Konfigurieren

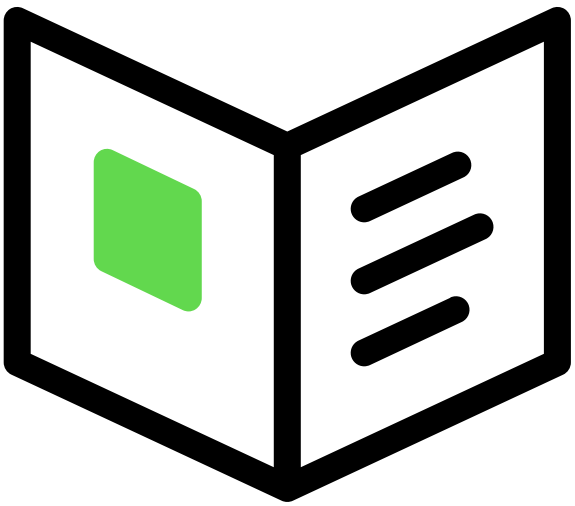


Konfigurieren Sie Setup- und Konfigurationsaufgaben für Health Log Analytics.

Verwenden

Überwachen und beheben Sie Warnungen, die von Health Log Analytics generiert werden.

Referenz



Hier finden Sie Referenzinformationen zu Health Log Analytics.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics Lizenzierung

Bei der für Now Platform® verwendeten Lizenzierungsmethode zahlt Ihre Organisation für die Nutzung von Health Log Analytics, das als separate Lizenz von ITOM-Integritätverfügbar ist. Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung und -Abonnements.

Abhängigkeiten

Eine Liste der Health Log Analytics Plugin-Abhängigkeiten finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Problembehandlung und Hilfe

- Stellen Sie Fragen, und erkunden Sie andere Ressourcen für in ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Health Log Analytics erkunden

Machen Sie sich mit dem Workflow, der Architektur und den allgemeinen Aufgaben Health Log Analytics von vertraut.

Verständnis ServiceNow Health Log Analytics

ServiceNow Health Log Analytics (HLA) prognostiziert IT-Probleme, bevor sie sich auf Ihre Benutzer auswirken.

Health Log Analytics – Übersicht

Health Log Analytics hilft Ihnen, IT-Probleme schneller zu lösen, indem maschinell generierte Protokolldaten in Echtzeit erfasst, analysiert und korreliert werden. Die Anwendung empfängt und verarbeitet Protokolle über MID-Server und sendet Ereignisse an ServiceNow Ereignismanagement. Health Log Analytics erkennt jede Anomalie − Abweichung vom normalen Verhalten −, sobald sie auftritt, und warnt Sie vor möglichen Problemen. Die Anwendung hilft Ihnen, die Ursache eines Problems zu identifizieren, indem Sie es Ihnen ermöglicht, zugehörige Protokolle zu selektieren und die Rohdaten zu analysieren.

Health Log Analytics kann jede Art von maschinell generierten Textprotokolldaten verarbeiten, einschließlich Anwendungs-, Infrastruktur- und Netzwerkprotokolle sowie andere Arten von Textprotokolldaten. Configuration Management Database (CMDB) kann zwar nützlich sein, um hochwertige Events und Warnungen zu generieren, dies ist aber nicht erforderlich.

Hinweis:

- Health Log Analytics unterstützt nur UTF-8-Protokolle. Binärprotokolle werden nicht unterstützt.
- Wenn Sie Protokolle in einer anderen Sprache als Englisch senden, ist möglicherweise eine zusätzliche Konfiguration erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics – Workflow

Health Log Analytics sammelt und verarbeitet automatisch Protokolldaten. Die Daten werden für die Analyse durch die Betreiber strukturiert, und es werden aussagekräftige Warnungen und Vorschläge generiert, die in Ereignismanagement angezeigt werden.

Das Diagramm zeigt den Health Log Analytics-Workflow vom Sammeln der Daten bis zum Senden eines Events oder einer Warnung an Ereignismanagement.

Health Log Analytics-Workflow

Erfassung

Diese Ebene verbindet Ihre Umgebung mit Health Log Analytics. Sie können Ihre Protokolle direkt von Servern und Endpunkten oder aus Protokoll-Repositorys streamen. Das optionale Guided Setup unterstützt Sie beim Erstellen von Dateneingabe-Connectors für die folgenden häufigen Datenquellen:

- Rsyslog
- Beats
- Splunk
- Elasticsearch
- MID-Server
- TCP

Strukturierung

Diese Ebene befasst sich mit der Strukturierung von Protokolldaten und ihrer automatischen Zuordnung zu logischen Silos, die als Komponenten bezeichnet werden. Die Datenstrukturierung kann automatisch oder manuell erfolgen.

Das System strukturiert Protokolldaten automatisch, indem es aus eingehenden Protokollnachrichten die folgenden Eigenschaften extrahiert: Nachricht, Zeitstempel, Host, Schweregrad und externe IDs. Es extrahiert explizite Werte wie „property-name“ und „value is IP“ sowie semantische Werte wie Länge, Anzahl englischer Wörter und Varianz.

Bei der automatischen Zuordnung werden Protokollbeispiele und Metadaten automatisch den entsprechenden Tags zugewiesen. Das System versucht, Protokollzeilen zuzuordnen, indem es die Quelle analysiert, von der die Daten gestreamt werden. Die Zuordnung basiert auf Agent-Hinweisen und allgemeinen Transport-Header-Feldern.

Anreicherung

Auf dieser Ebene geht es um die Identifizierung der variablen Teile einer Protokollnachricht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics-Workflow: Anreicherung

Zudem werden Stichwörter und kontextbezogene Eigenschaften identifiziert. Im Bild sind „WARN“ und „Failed“ die zu verfolgenden Stichwörter. „User“, „source IP“ und „port“ sind die kontextbezogenen Eigenschaften.

Analyse

Auf dieser Ebene wird jede Protokollzeile indiziert. Health Log Analytics extrahiert Eigenschaften aus der inneren Protokollnachricht. Diese tragen zu Modellen von dem Verhalten bei, vom dem das System lernt, es zu erwarten. Anomales Verhalten ist Verhalten, das von diesem erwarteten Verhalten abweicht. Sie können nach einem Event und seinen wichtigsten Eigenschaften für die manuelle Fehlerbehebung suchen.

Maschinelles Lernen (ML) und künstliche Intelligenz (KI)

Health Log Analytics nutzt erweiterte, unüberwachte ML-Algorithmen, um Muster in Protokollen zu erkennen und ihr eindeutiges Datenverhalten zu erlernen. Anschließend werden in Echtzeit dynamische Schwellenwerte basierend auf der Datensignatur festgelegt, um Probleme zu erkennen, wenn sie zum ersten Mal auftreten. Wenn das System eine Abweichung vom typischen Muster erkennt, sendet es ein Event an Ereignismanagement.

Warnung in Ereignismanagement

Health Log Analytics sendet Events an Ereignismanagement. In Ereignismanagement werden Health Log Analytics-Warnungen in der Liste **All alerts** (Alle Warnungen) angezeigt. Diese Liste ermöglicht es Betreibern, Warnungen des Events und den Health Log Analytics-Warntyp an einem einzigen Ort anzuzeigen.

Empfehlungen für weitere Themen

- Health Log Analytics-Architektur
- Wie Health Log Analytics Warnungen generiert

Health Log Analytics-Architektur

Health Log Analytics sammelt Protokolle, die von Endpunkten oder Data Lakes wie Splunk und Elasticsearch in Ihre ServiceNow-Instanz gestreamt werden.

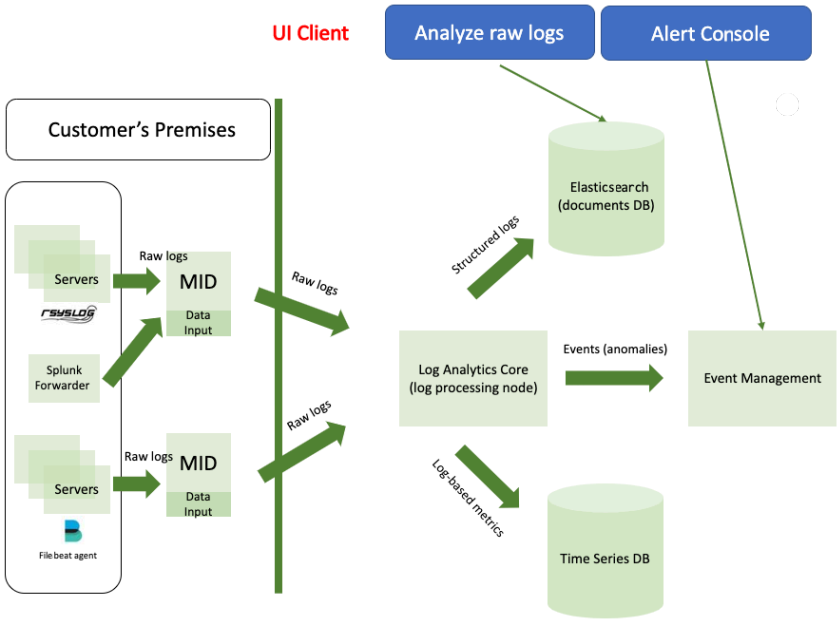
Die Instanz ServiceNow empfängt die Protokolle über die MID-Server- Connector-Instanz. Health Log Analytics identifiziert und selektiert Anomalien in Ihren Protokolldaten mithilfe von nicht überwachten ML-Modellen (maschinelles Lernen). Anschließend werden die Anomalien gruppiert und weitere Algorithmen angewendet, um die Ursache des Problems zu identifizieren.

Die folgende Abbildung zeigt ein Setup mit Rsyslog, Splunk, Filebeatund Elasticsearch.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics-Architektur



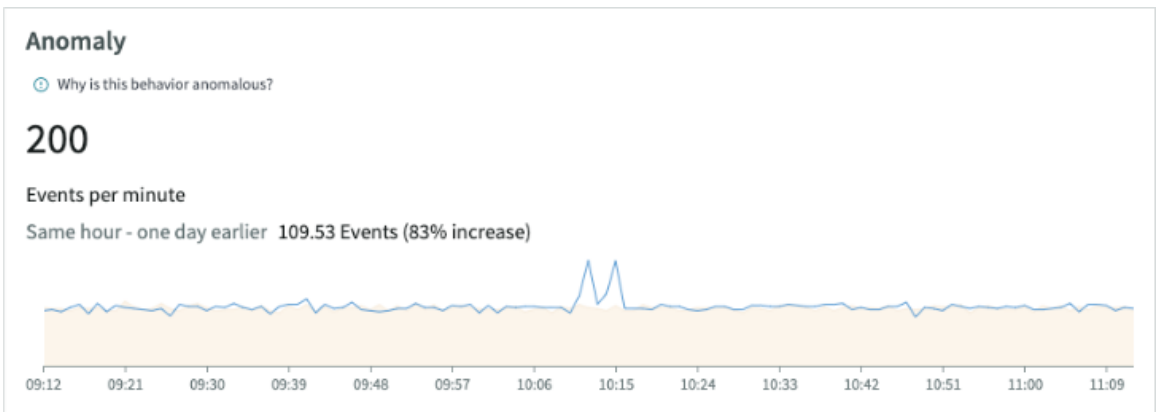
Wie Health Log Analytics Warnungen generiert

Health Log Analytics identifiziert Muster in Ihren Protokolldaten und lernt das Musterverhalten. Wenn die KI-Engine von HLAanomales Verhalten erkennt, sendet sie ein Ereignis an die Anwendung ServiceNow Ereignismanagement. Als -Operator können Sie diese prädikativen Warnungen verwenden, um neu auftretende IT-Probleme zu behandeln, bevor sie sich auf Benutzer auswirken.

Erkennung von Protokollanomalien

Es gibt viele Arten von anomalem (anomalem oder unerwartetem) Verhalten. In diesem Beispiel verfolgt das System die Baselinerate bestimmter Nachrichten (durchschnittliche Anzahl der Events pro Minute). Im Diagramm sind die Werte für den Vortag als hell pfirsichfarben-schattierter Bereich und die Werte für heute als blaue Linie dargestellt. Das Diagramm zeigt eine drastische Abweichung von den erwarteten Baselinewerten ungefähr um 10:10 Uhr. Dieses anomale Verhalten generiert eine Warnung.

Anomales Verhalten



Health Log Analytics verwendet verschiedene Methoden, um Anomalien zu erkennen und Warnungen zu generieren.

Weitere Informationen finden Sie unter Was ist Anomalie-Erkennung?

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsmetriken

Health Log Analytics überwacht mehrere Metriken im Protokollstream, um anomales Verhalten zu erkennen. Jede Metrik ist einer eindeutigen Quelle zugeordnet: der Kombination aus Serviceinstanz und Komponente. Wenn das System ein anomales Muster für eine Metrik identifiziert, generiert es eine Warnung.

Als -Operator können Sie Feedback zu den generierten Warnungen abgeben. Durch Ihr Feedback „lernen“ Health Log Analytics Sie, dass eine bestimmte Warnung für Sie signifikant oder irrelevant ist. Die Anwendung erhöht dann entweder die Priorität der Warnungsmetrik oder schaltet sie stumm, um Rauschen zu reduzieren.

- Eine signifikante Warnung wird eher in eine Log Analytics-Gruppe aufgenommen, wenn sich die zugehörige Metrik anomal verhält. Weitere Informationen finden Sie unter Warnung als signifikant markieren
- Schalten Sie eine Warnung für eine angegebene Quelle stumm, um störende neue Warnungen für unwichtige Probleme zu vermeiden. Wenn eine Metrik stummgeschaltet wird, entfernt Health Log Analytics die aktuelle Warnung und alle anderen Warnungen basierend auf dieser Metrik aus dem Feed. Außerdem werden keine neuen Warnungen aus dieser Metrik mehr generiert. Weitere Informationen finden Sie unter Irrelevante Warnungen stummschalten.
- Wenn sich die Situation ändert, können Sie eine signifikante Metrik auf ihre Standardbedeutung zurücksetzen. Sie können auch eine stummgeschaltete Metrik reaktivieren, damit das System erneut Warnungen generiert. Weitere Informationen finden Sie unter Stummgeschaltete Warnung oder signifikante Warnung wiederherstellen.

Lexikalische Stichwörter

Health Log Analytics durchsucht Ihre Protokolle nach Wörtern, die auf wichtige Probleme hinweisen können. Lexikalische Stichwörter wie „Crash“ oder „Failed“ weisen auf eine Bedingung hin, die der Aufmerksamkeit bedarf.

Das System legt für jedes lexikalische Stichwort einen Schwellenwert fest, der auf den Werten basiert, die es als normales Vorkommensmuster und normale Häufigkeit dieses Stichworts in Ihren Protokollen betrachtet. Beim Scannen Ihrer Protokolle werden alle Vorkommen des Stichworts gefunden. Wenn die Anzahl den Schwellenwert überschreitet, wird eine Warnung generiert. Weitere Informationen finden Sie unter Warnungen generierende lexikalische Stichwörter anzeigen.

Weitere Informationen über die Verwaltung globaler Stichwörter finden Sie unter Lexikalische Stichwörter für Health Log Analytics hinzufügen, bearbeiten oder löschen. Informationen zum Erstellen oder Löschen von Stichwörtern für einen bestimmten Quelltyp finden Sie unter Quelltypfunktionen konfigurieren.

Korrelationen

Protokollkorrelatoren sind Schlüssel oder Werte in Protokolldaten, die Korrelationen zwischen Warnungen erkennen. Beispielsweise könnte ein Protokollkorrelator erkennen, wenn die ID eines bestimmten Netzwerkgeräts gleichzeitig in mehreren Warnungen in verschiedenen Serviceinstanzen vorkommt. Weitere Informationen finden Sie unter Identifizieren von Beziehungen in Protokolldaten mithilfe von Protokollkorrelatoren.

Erweiterte Warnungsfilterung

Fügen Sie erweiterte Protokollwarnungsfilter hinzu, um Warnungen nach von Ihnen angegebenen Bedingungen zu scannen. Die Filter reduzieren das Rauschen, indem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungen verworfen werden, die kein schwerwiegendes Problem anzeigen. Während der Entwicklung eines Filters können Sie den Filter jederzeit testen, aktualisieren, veröffentlichen oder aktivieren. Weitere Informationen finden Sie unter Erweiterte Protokollwarnungsfilter erstellen.

Benutzerdefinierte Warnungsregeln

Definieren Sie eine Log Analytics-Warnungsregel, wenn Sie auf Protokolldaten stoßen, die eine Warnung generieren sollen. Die Warnungsregel generiert eine Warnung für eine angegebene Metrik mit einem von Ihnen angegebenen Schwellenwert und legt die Eigenschaften der generierten Warnung fest. Weitere Informationen finden Sie unter Log Analytics-Warnungsregeln hinzufügen.

Health Log Analytics konfigurieren

Als -Administrator richten Sie Health Log Analytics ein, damit Anwender verwenden können, und führen Administrationsaufgaben aus, um sicherzustellen, dass das System effizient läuft.

Konfiguration – Übersicht

Führen Sie die folgenden Aufgaben aus, um Health Log Analyticserfolgreich einzurichten und zu konfigurieren.

Wichtig: Unabhängig davon, wie Sie Health Log Analyticsimplementieren, müssen Sie zuerst die Systemanforderungen für den MID-Server konfigurieren und sicherstellen, dass die Protokollerfassungsfunktion für MID-Server aktiviert ist.

Informationen zu den Proxy-Anforderungen für MID-Server finden Sie unter MID-Server-Proxy-Vorbedingungen für das Streaming von Protokollen an HLA.

1. Health Log Analytics installieren (HLA).

   Installieren Sie die Anwendung Health Log Analytics.

2. Richten Sie Protokolldateneingaben oder -Connectors für das Streaming von Protokollnachrichten im Rohzustand an Ihre Instanz ServiceNow ein.

   Verwenden Sie eine der folgenden Methoden:

   - Richten Sie Dateneingaben mithilfe des geführten Setups Health Log Analytics ein.

     Das geführte Setup stellt eine Reihe von Aufgaben bereit, mit denen Sie Dateneingaben in Ihrer -Instanz erstellen können. Mit dieser Methode wird sichergestellt, dass Sie über das erforderliche Minimum für den Dateneingabeprozess verfügen.

   - Richten Sie Dateneingaben für Health Log Analytics manuell ein.
   - Integrationen über Integrations Launchpadeinrichten.

     ServiceNow Integrations Launchpad bietet eine einheitliche Schnittstelle für eine bequeme Integration mit Protokolldaten-Connectors, die Protokollnachrichten im Rohzustand an Ihre -Instanz weiterleiten.

   Wenn der Konfigurationsprozess für die Dateneingabe abgeschlossen ist, werden Protokolldaten an Ihre -Instanz gestreamt.

3. Probleme beim Protokoll-Streaming identifizieren und beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identifizieren und beheben Sie Probleme beim Protokoll-Streaming, um sicherzustellen, dass die Dateneingaben, die Sie konfiguriert haben, Daten ordnungsgemäß an Ihre -Instanz streamen.

4. Protokolldaten im Rohzustand vor der Verarbeitung bearbeiten.

   Ändern Sie Protokollnachrichten im Rohzustand, bevor sie in MID-Serververarbeitet werden und daher bevor Health Log Analytics es zuordnet und strukturiert.

5. Protokolldaten im Rohzustand zuordnen.

   Ordnen Sie Protokollrohdaten zu, die in Ihre Instanz gestreamt werden, um zu bestimmen, wie die Daten behandelt werden.

   Health Log Analytics versucht, jede eingehende Protokollzeile automatisch dem richtigen Tag zuzuordnen. Wenn Eigenschaften nicht automatisch erkannt werden, können Sie die Dateneingabequellen manuell zuordnen.

6. Quelltypstruktur verfeinern.

   Feintunen Sie, wie Health Log Analytics Ihre inneren Protokollnachrichten liest und Anomalien erkennt, indem Sie die extrahierten Eigenschaften in der Quelltypstruktur anpassen.

   Mit Health Log Analytics können Sie automatisch klassifizierte Eigenschaften neu klassifizieren und automatisch zugeordnete Bezeichnungen ändern. Diese Anpassungen helfen dem maschinellen Lernen des Systems, Ihre Prioritäten besser zu verstehen.

7. Führen Sie zusätzliche Setup-Aufgaben für die Dateneingabe durch.

   Nachdem Sie das obligatorische Setup und die Konfiguration der Dateneingabe durchgeführt haben, können Sie mit optionalen Setupaufgaben fortfahren.

8. Führen Sie erweiterte Konfigurationsaufgaben für die Dateneingabe durch.

Geführtes Setup zur Implementierung von Health Log Analytics verwenden

Das geführte Setup stellt eine Reihe von Aufgaben bereit, mit denen Sie Health Log Analytics in der Instanz ServiceNow konfigurieren können. Um das geführte Setup für Health Log Analyticszu öffnen, navigieren Sie zu **Alle** > **Geführtes Setup** > **Geführtes Setup für ITOM** > **Health Log Analytics**.

Health Log Analytics installieren (HLA)

Installieren Sie Health Log Analytics, indem Sie die ServiceNow HLA-Installation beim ServiceNow Kundensupport anfordern.

Vorbereitungen

Die minimale Version der Now Platform, die zur Installation von Health Log Analytics benötigt wird, ist Yokohama.

Wichtig: Health Log Analytics verwendet für die interne Kommunikation den Standardbenutzer sn_occ_occultus. Stellen Sie sicher, dass dieser Anwender aktiv ist, und deaktivieren Sie ihn nicht.

Erforderliche Rolle: Administrator

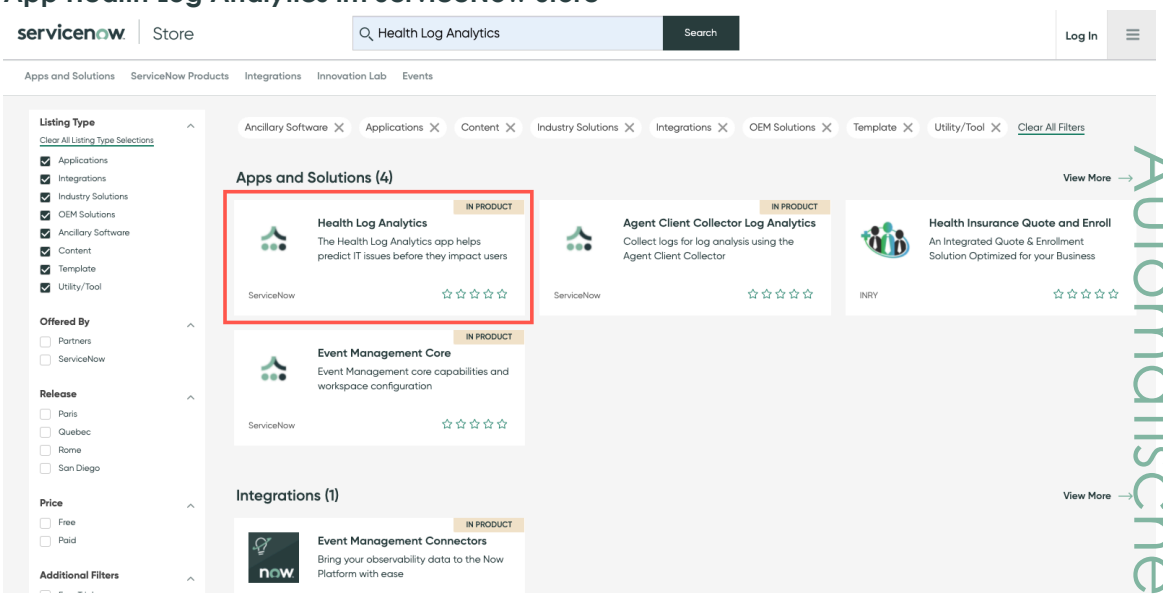
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Vergewissern Sie sich, dass die Anwendung Health Log Analytics und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Um Berechtigungen zu erhalten, wenden Sie sich an Ihren ServiceNow-Lösungsberater.
2. Melden Sie sich für das Produkt ITOM-Integrität an.

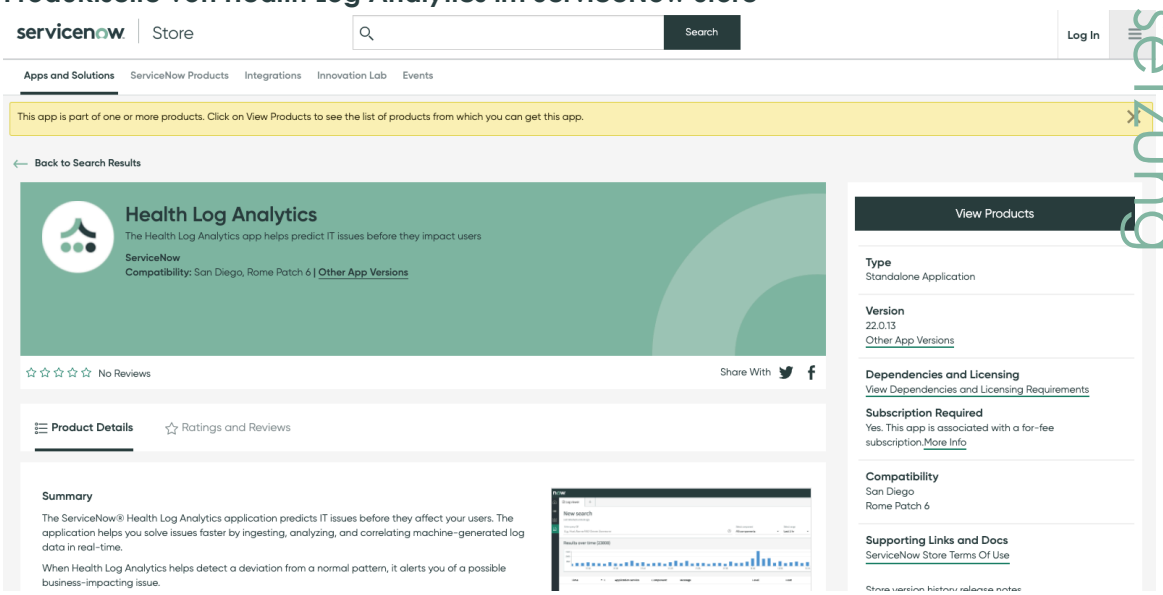
   a. Wechseln Sie zu ServiceNow Store rufen Sie die Website auf, und suchen Sie nach der App Health Log Analytics.

App Health Log Analytics im ServiceNow Store



   b. Wählen Sie Health Log Analytics aus.
   Die Produktseite von Health Log Analytics wird angezeigt.

Produktseite von Health Log Analytics im ServiceNow Store



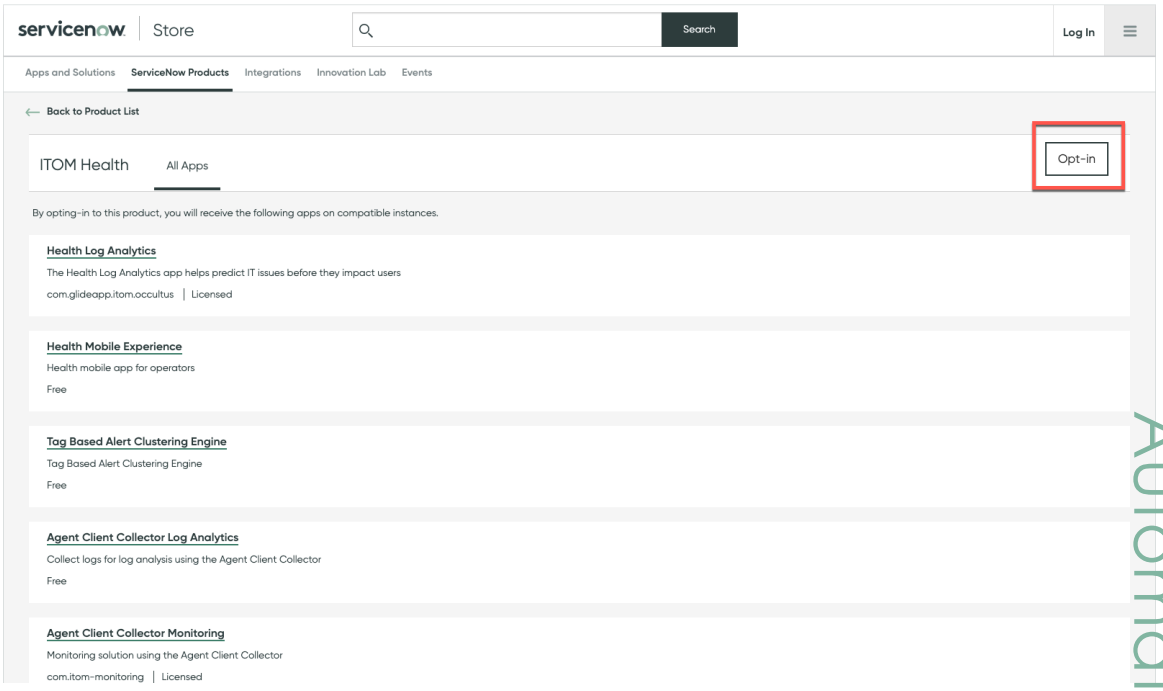
   c. Wählen Sie **Produkte anzeigen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie **Aktivieren**.

Produkt ITOM Health



3. Installieren Sie die Anwendung Health Log Analytics in Ihrer Instanz.

a. Navigieren zu **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.

b. Suchen Sie die Anwendung Health Log Analytics über die Suchleiste.

c. Wählen Sie auf der Kachel Health Log Analytics die Option **Installieren**.
Wenn die Anwendung erfolgreich in der Instanz installiert wurde, wird eine automatische Change-Anforderung (CHG) ausgelöst, um die Bereitstellung für die erforderlichen Endpunkte anzufordern. Der Instanzadministrator erhält die Anforderung und alle relevanten Benachrichtigungen.

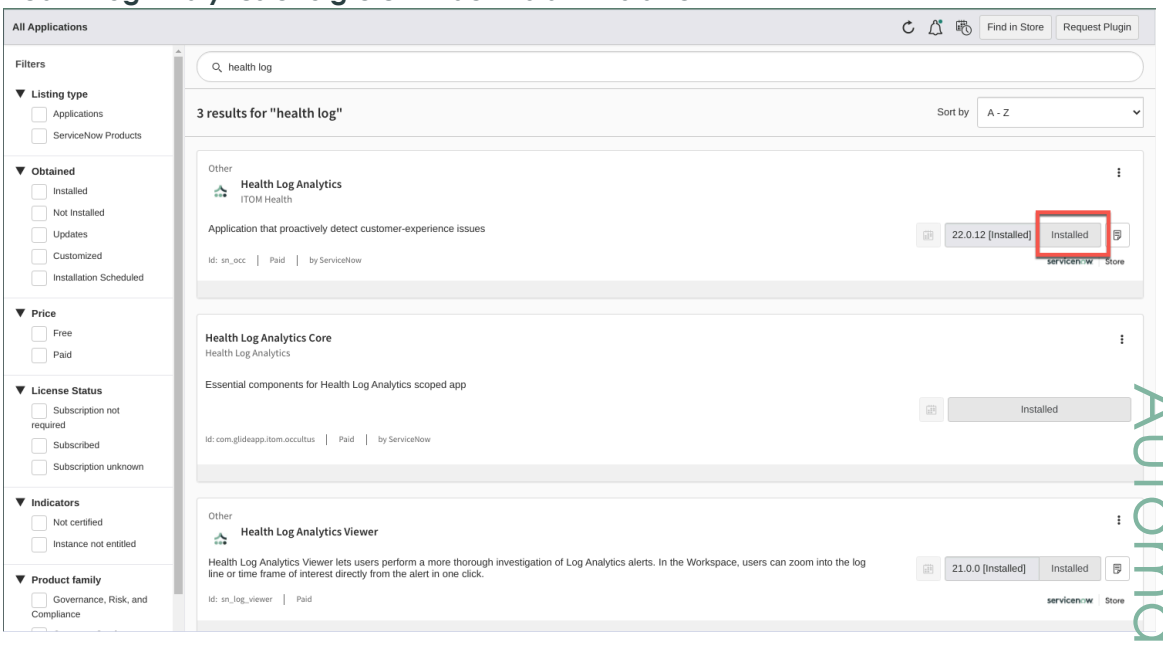
Hinweis: Selbst wenn die Anwendung Health Log Analytics erfolgreich installiert wurde, funktioniert sie erst, nachdem die Endpunkte bereitgestellt wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Stellen Sie sicher, dass die Anwendung und ihre Abhängigkeiten erfolgreich installiert wurden (siehe Abbildung).

Health Log Analytics erfolgreich in der Instanz installiert



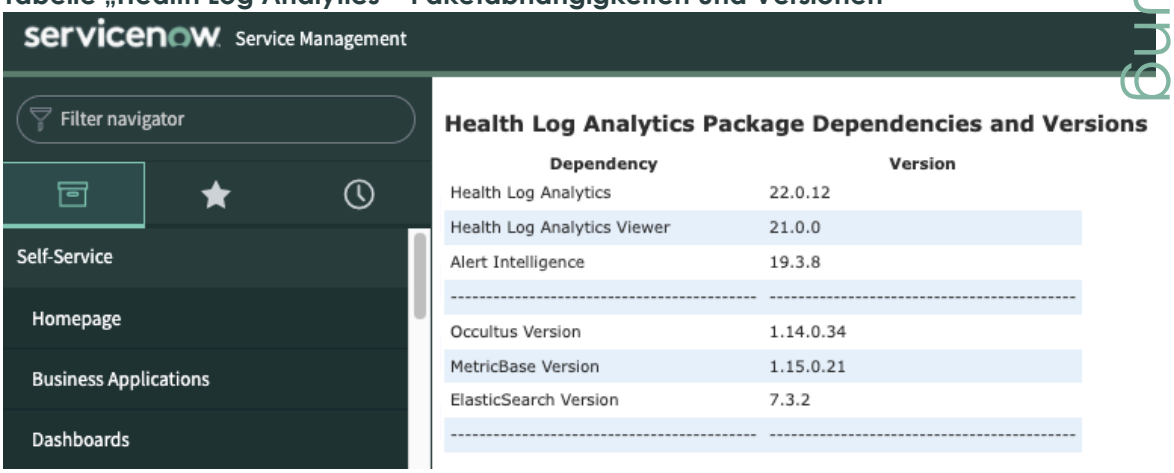
4. Wahlweise: Beobachten Sie den Status des Bereitstellungsprozesses, indem Sie die CHG überprüfen.

> **Hinweis:** Einige Schritte im Bereitstellungsprozess erfordern möglicherweise Ihre explizite Genehmigung. In solchen Fällen wird sich der ServiceNow-Kundensupport mit Ihnen in Verbindung setzen.

5. Stellen Sie nach Abschluss der Bereitstellung sicher, dass die Anwendung Health Log Analytics ausgeführt wird.

a. Geben Sie im Filternavigator `sn_occ_stats.do` ein.
Die Tabelle „Health Log Analytics − Paketabhängigkeiten und Versionen“ wird angezeigt.

Tabelle „Health Log Analytics − Paketabhängigkeiten und Versionen“



Die bereitgestellten Endpunkte werden zusammen mit ihrer Versionsnummer aufgelistet:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Occultus
- MetricBase
- ElasticSearch

Ergebnisse
Die Anwendung Health Log Analytics wird in Ihrer Instanz installiert und bereitgestellt.

Nächste Maßnahme

- Richten Sie den Dateneingabeprozess für Health Log Analytics ein.
- (Optional) Installieren Sie das Plugin „ServiceNow® Agent Client Collector Log Analytics“ (ACC-L).

  Agent Client Collector Log Analytics ermöglicht es Ihnen, Protokolldaten von Linux- und Windows-Hosts mit Agent Client Collector an eine ServiceNow-Instanz zu streamen. Weitere Informationen finden Sie in der Dokumentation zu Agent Client Collector Log Analytics.

Health Log Analytics in Ihrer Instanz von ServiceNow einrichten

Implementieren Sie Health Log Analytics in Ihrer Instanz ServiceNow, indem Sie den Dateneingabeprozess einrichten.

Hinweis: Informationen zur Installation der Anwendung ServiceNow Health Log Analytics finden Sie unter Health Log Analytics installieren (HLA).

Wichtig: Unabhängig davon, wie Sie Health Log Analyticsimplementieren, müssen Sie zuerst die Systemanforderungen für den MID-Server konfigurieren und sicherstellen, dass die Protokollerfassungsfunktion für MID-Server aktiviert ist.

Informationen zu den Proxy-Anforderungen für MID-Server finden Sie unter MID-Server-Proxy-Vorbedingungen für das Streaming von Protokollen an HLA.

Richten Sie den Dateneingabeprozess ein

Sie können Protokolldateneingaben oder -konnektoren für Health Log Analytics auf eine der folgenden Arten konfigurieren:

- Mithilfe des geführten Setups Das geführte Setup stellt eine Reihe von Aufgaben bereit, mit denen Sie Dateneingaben in der Instanz ServiceNow konfigurieren können. Durch die Verwendung des Guided Setups wird sichergestellt, dass Sie über das erforderliche Mindestsetup für den Dateneingabeprozess verfügen. Weitere Informationen finden Sie unter Richten Sie Dateneingaben mithilfe des geführten Setups Health Log Analytics ein.
- Manuell. Weitere Informationen finden Sie unter Richten Sie Dateneingaben für Health Log Analytics manuell ein.
- Aus Ereignismanagement Integrations Launchpad in Service Operations-Arbeitsbereich für ITOM. Mit Integrations Launchpad können Sie schnell und bequem Protokolldaten-Connector-Integrationen einrichten und mit dem Empfang von Protokolldaten beginnen. Weitere Informationen finden Sie unter Integrationen über Integrations Launchpadeinrichten.

  Hinweis: Derzeit sind -Integrationen für die Connectors Elasticsearch, Glide Syslog, TCP und UDP verfügbar.

Zugehörige Informationen

Unterstützte Dateneingaben für Health Log Analytics

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

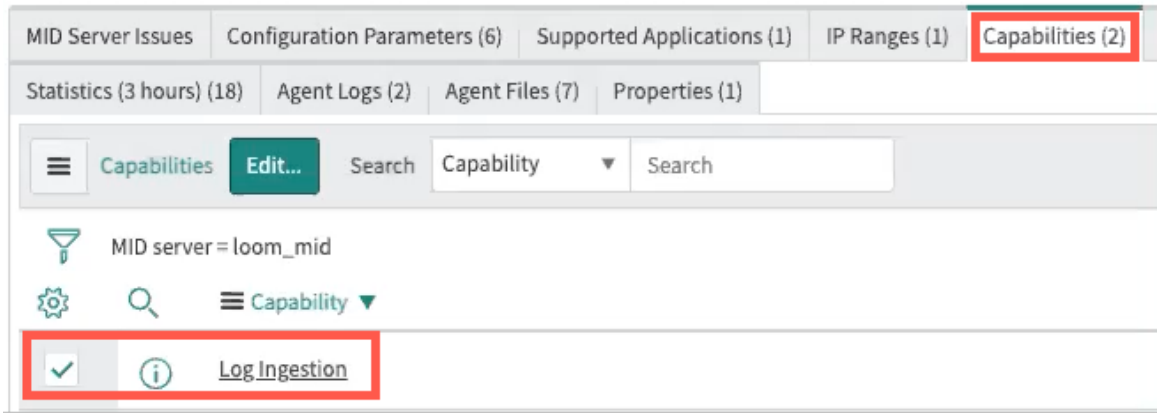
Richten Sie Dateneingaben mithilfe des geführten Setups Health Log Analytics ein

Das Guided Setup von Health Log Analytics bietet eine Reihe von Aufgaben, die Sie beim Erstellen von Dateneingaben für Ihre ServiceNow-Instanz unterstützen. Die Konfiguration der Dateneingabe ist ein wichtiger Schritt beim Einrichten der Anwendung Health Log Analytics. Durch die Verwendung des Guided Setups wird sichergestellt, dass Sie über das erforderliche Mindestsetup für den Dateneingabeprozess verfügen.

Vorbereitungen

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .
- Weitere Informationen zur Übermittlung von Protokollen mit SSL TLS-Verschlüsselung finden Sie im Artikel Streaming Data With Rsyslog & Filebeat Using SSL [KB0866319] (Daten mit Rsyslog & Filebeat über SSL streamen) in der Knowledge Base des Now Support.
- Informationen zu den Proxy-Anforderungen für MID-Server finden Sie unter MID-Server-Proxy-Vorbedingungen für das Streaming von Protokollen an HLA.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Informationen zur Verwendung der Schnittstelle des geführten Setups finden Sie unter Geführtes Setup verwenden .

Prozedur

1. Navigieren zu **Alle** > **Geführtes Setup** > **Geführtes Setup für ITOM** > **Health Log Analytics**.
2. Befolgen Sie die Anweisungen, um eine Dateneingabe auszuwählen und einzurichten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Sobald Sie den Dateneingabe-Connector erstellt haben, fahren Sie mit dem Zuordnen Ihrer Rohprotokolldatenfort.

Zugehörige Informationen

Unterstützte Dateneingaben für Health Log Analytics

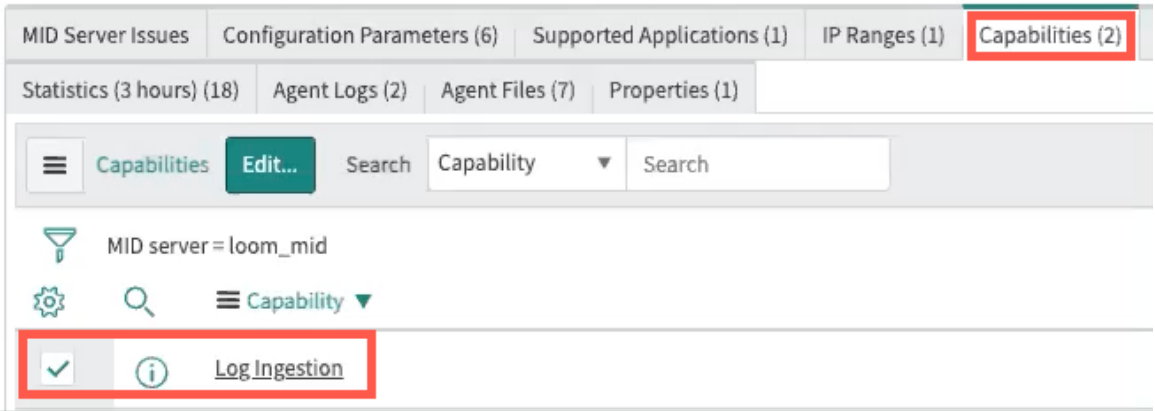
Richten Sie Dateneingaben für Health Log Analytics manuell ein

Richten Sie Ihre Health Log Analytics -Dateneingaben für Health Log Analytics manuell ein. Die Konfiguration der Dateneingabe ist ein wichtiger Schritt beim Einrichten der Anwendung Health Log Analytics.

Vorbereitungen

Hinweis: Erwägen Sie die Verwendung des geführten Setups für die Dateneingabe Health Log Analytics, das sicherstellt, dass Sie über das erforderliche Mindest-Setup für den Dateneingabeprozess verfügen. Weitere Informationen finden Sie unter Richten Sie Dateneingaben mithilfe des geführten Setups Health Log Analytics ein.

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .
- Weitere Informationen zur Übermittlung von Protokollen mit SSL TLS-Verschlüsselung finden Sie im Artikel Streaming Data With Rsyslog & Filebeat Using SSL [KB0866319] (Daten mit Rsyslog & Filebeat über SSL streamen) in der Knowledge Base des Now Support.
- Informationen zu den Proxy-Anforderungen für MID-Server finden Sie unter MID-Server-Proxy-Vorbedingungen für das Streaming von Protokollen an HLA.

Erforderliche Rolle: evt_mgmt_admin. Für die Dateneingabe der Systemprotokolle ServiceNow : admin.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Konfigurieren Sie eine Dateneingabe, indem Sie das entsprechende Verfahren ausführen, das in der Produktdokumentation beschrieben ist.

Dateneingaben

Dateneingabe	Beschreibung
Rsyslog oder Beats	Die Dateneingabe streamt Protokolldaten mit Rsyslog oder Beats in Ihre Instanz.
Splunk	Die Dateneingabe streamt Protokolldaten mit Splunk in Ihre Instanz.
Splunk-Abruf	Die Dateneingabe ruft regelmäßig Protokolldaten aus Splunk mithilfe einer Abfrage ab.
Elasticsearch	Die Dateneingabe ruft Protokolldaten aus Elasticsearch-Indizes in Ihre Instanz ab.
TCP	Die Dateneingabe sendet Rohprotokollmeldungen direkt über ein TCP/SSL-Socket an Ihre Instanz.
UDP	Die Dateneingabe streamt Rohprotokollnachrichten an Ihre Instanz ServiceNow direkt über einen UDP-Socket.
GCP Pub/Sub	Die Dateneingabe empfängt Protokollnachrichten, die in einem Google Cloud Pub/Sub-Thema veröffentlicht werden, und streamt sie an Ihre Instanz ServiceNow.
MID-Server	Die Dateneingabe sammelt MID-Server-Protokolldateien und streamt sie an Ihre Instanz.
Amazon CloudWatch	Die Dateneingabe streamt Protokolldaten aus Amazon CloudWatch an Ihre ServiceNow-Instanz.
Amazon S3	Die Dateneingabe streamt Protokolldaten aus dem Amazon S3-Bucket (Simple Storage Service) an Ihre ServiceNow-Instanz.
Microsoft Azure Log Analytics	Die Dateneingabe streamt Protokolldaten aus Microsoft Azure Log Analytics an Ihre ServiceNow-Instanz.
Microsoft Azure Event Hubs	Die Dateneingabe streamt Events aus Microsoft Azure Event Hubs an Ihre ServiceNow-Instanz.
Apache Kafka	Die Dateneingabe streamt Protokolldaten aus Apache Kafka an Ihre ServiceNow-Instanz.
REST-API	Die Dateneingabe streamt Protokolldaten im JSON-Format an Ihre ServiceNow-Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateneingabe	Beschreibung
ServiceNow-Systemprotokolle	Die Dateneingabe streamt Protokolldaten aus der Systemprotokolltabelle ServiceNow an die KI-Engine Health Log Analytics. **Hinweis:** Im System kann nur eine einzelne Systemprotokoll-Dateneingabe ServiceNow vorhanden sein, und diese Eingabe muss nur von Anwendern mit der Administratorrolle erstellt und konfiguriert werden. Diese Dateneingabe wird nicht für MID-Serverausgeführt.
ServiceNow-Systemprotokolle	Die Dateneingabe streamt Protokolldaten aus der Systemprotokolltabelle ServiceNow an die KI-Engine Health Log Analytics (Occultus).
Cribl	Die Dateneingabe in ermöglicht Health Log Analytics die Verarbeitung von CRBL-Protokollnachrichten, die in Ihre Instanz ServiceNow gestreamt werden.
Edge Delta	Mit der Dateneingabe kann Health Log Analytics Edge-Delta-Protokollnachrichten verarbeiten, die in Ihre Instanz von ServiceNow gestreamt werden.
Vector Agent	Die Dateneingabe ermöglicht es Health Log Analytics, Protokollnachrichten zu verarbeiten, die über einen Vektoragenten in Ihre Instanz ServiceNow gestreamt werden.
Agent Client Collector	Die Dateneingabe streamt Protokollnachrichten mit ServiceNow Agent Client Collector in Ihre ServiceNow-Instanz. Diese Dateneingabe wird für die Verwendung mit der Anwendung Agent Client Collector Log Analytics unterstützt, die im ServiceNow Store verfügbar ist.

Hinweis: Durch Auswahl von **Testverbindung** am Ende des Verfahrens wird sichergestellt, dass Ihre Dateneingabe richtig konfiguriert ist. Sie können eine Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung zwischen MID-Server und dem Daten-Repository hergestellt wurde.

2. Identifizieren und beheben Sie Streaming-Probleme, um sicherzustellen, dass die Dateneingabe Protokolldaten aus allen Quellen an den MID-Server streamt. Weitere Informationen finden Sie unter Probleme beim Protokoll-Streaming identifizieren und beheben.
3. Wahlweise: Bearbeiten Sie Protokollrohdaten, bevor Health Log Analytics sie zuordnet und strukturiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Rohprotokolldaten vor der Verarbeitung bearbeiten.

4. Legen Sie fest, wie Health Log Analytics Protokollrohdaten behandelt, die in Ihre -Instanz gestreamt werden.
   Standardmäßig wird jede eingehende Protokollzeile automatisch dem richtigen Tag zugeordnet. Wenn Eigenschaften nicht automatisch erkannt werden, ordnen Sie die Dateneingabequellen manuell zu, indem Sie eine JavaScript-Funktion definieren. Weitere Informationen finden Sie unter Rohdaten zuordnen.
5. Wahlweise: Optimieren Sie die Quelltypstruktur, um sicherzustellen, dass Health Log Analytics alle Eigenschaften richtig extrahiert und klassifiziert.
   Weitere Informationen finden Sie unter Quelltypstruktur verfeinern.
6. Wahlweise: Führen Sie zusätzliche Setup-Aufgaben für die Dateneingabe durch.
   Weitere Informationen finden Sie unter Weitere Setupaufgaben für Dateneingaben.

Zugehörige Informationen

Unterstützte Dateneingaben für Health Log Analytics

Dateneingaben für Health Log Analytics manuell konfigurieren

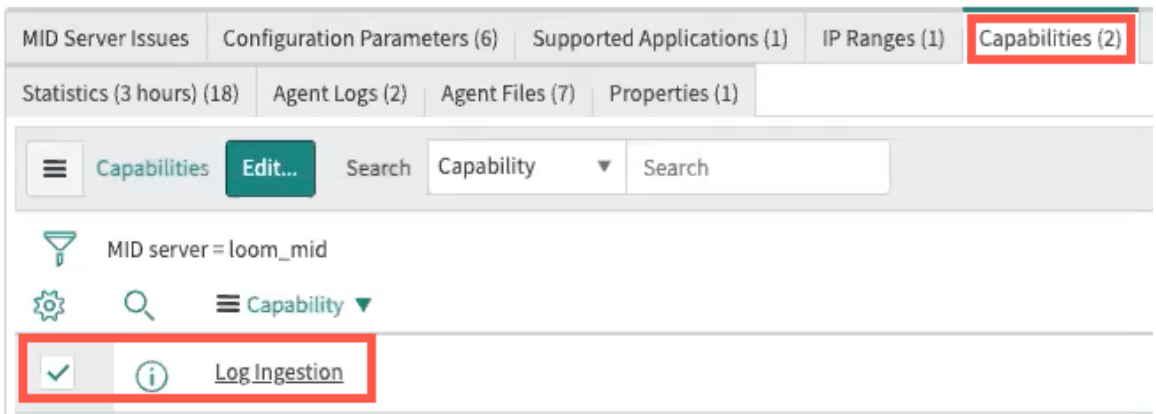
Konfigurieren Sie den Dateneingabeprozess manuell in Health Log Analytics. Die Konfiguration der Dateneingabe ist ein wichtiger Schritt beim Einrichten der Anwendung Health Log Analytics.

Konfigurieren Sie Rsyslog- , Filebeat- oder Winlogbeat-Dateneingaben

Konfigurieren Sie eine Dateneingabe für das Streaming von Protokollnachrichten an Ihre ServiceNow-Instanz mit einem Rsyslog-, Filebeat- oder Winlogbeat-Agent.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

- Weitere Informationen zur Übermittlung von Protokollen mit SSL TLS-Verschlüsselung finden Sie im Artikel Streaming Data With Rsyslog & Filebeat Using SSL [KB0866319] (Daten mit Rsyslog & Filebeat über SSL streamen) in der Knowledge Base des Now Support.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie den zu erstellenden Dateneingabetyp aus den in der Tabelle beschriebenen verfügbaren Dateneingabetypen aus.

   Hinweis: Der ausgewählte Dateneingabetyp ergänzt die passive Dateneingabe (Listener). Weitere Informationen finden Sie unter Unterstützte Dateneingaben.

   Dateneingabetypen

Typ	Beschreibung
Rsyslog	Streamt Protokollmeldungen von UNIX-basierten Servern an die KI-Engine von ServiceNow mit dem Rsyslog-Agent
Linux mit Filebeat	Streamt Systemprotokollnachrichten und lokale Dateien von Linux-Servern mit dem Filebeat-Agent an die Instanz
Windows-Anwendungsprotokolle mit Filebeat	Streamt lokale Dateien von MicrosoftMicrosoft Azure Event Hubs Windows-Geräten mit dem Filebeat-Agent an die ServiceNow-Instanz
Windows-Betriebssystem mit Winlogbeat	Streamt Windows-Event-Protokolle mit dem Winlogbeat-Agent an die ServiceNow-Instanz

4. Füllen Sie das Formular auf der Registerkarte **Erste Schritte** aus.

   Feldbeschreibungen finden Sie unter Rsyslog, Filebeat- oder Winlogbeat-Dateneingabe-Konfigurationsfelder.

   Hinweis: Wenn Sie eine Dateneingabe für Linux mit Filebeat erstellen, können Sie ein Inhaltspaket aus der Dropdown- **Liste Inhaltspaket** auswählen. Das Inhaltspaket enthält Standardquelltypen und Zuordnungsskriptvorlagen, mit denen Sie nicht mehr ohne Vorlage erstellen müssen. Weitere Informationen finden Sie unter Health Log Analytics Inhaltspakete für eine schnellere Amortisierungszeit.

5. Wenn der Agent noch nicht installiert wurde, laden Sie ihn über die Registerkarte **Installation** herunter, und installieren Sie ihn.

   Hinweis: Stellen Sie sicher, dass Sie die neueste Version des Agent ausführen. Frühere Versionen funktionieren, aber mit eingeschränkter Funktionalität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Weisen Sie auf der Registerkarte **Tagging and Bindung** Protokolle einer Serviceinstanz in Configuration Management Database (CMDB) zu, damit der Service die Protokolldaten korrelieren und das System die Ursachenanalyse durchführen kann.

   a. Konfigurieren Sie für jede Quelle den Pfad und die Serviceinstanz für die zu streamenden Protokolle.

      Hinweis: Standardmäßig werden nur die Pflichtfelder **Pfad-** und **Serviceinstanz** angezeigt.

      Feldbeschreibungen finden Sie unter Rsyslog, Filebeat- oder Winlogbeat-Dateneingabe-Konfigurationsfelder.

   b. Wenn Sie mehrzeilige Protokolle mit Filebeat versenden möchten, konfigurieren Sie die Eigenschaften, die steuern, wie Filebeat Nachrichten verarbeitet, die sich über mehrere Textzeilen erstrecken.

Feld	Beschreibung
Match (Übereinstimmung)	Gibt an, wie Filebeat übereinstimmende Zeilen zu einem Event kombiniert
Negieren	Definiert, ob das in den Protokollzeilen identifizierte Muster negiert wird
Regulärer Ausdruck	Gibt den regulären Ausdruck an

      Hinweis: Health Log Analytics unterstützt derzeit keine mehrzeiligen Eigenschaften für Rsyslog.

   c. Wahlweise: Definieren Sie zusätzliche Protokollpfade, damit die Dateneingabe Protokolltypen aus mehreren Pfaden streamen kann.
      Führen Sie für jeden zusätzlichen Protokollpfad die folgenden Schritte aus:

      i. Fügen Sie eine neue Zeile ein.

      ii. Konfigurieren Sie den Protokollpfad.

      iii. Wählen Sie eine Serviceinstanz.

      iv. (Optional) Wählen Sie eine Komponente und einen Quelltyp aus.

      Hinweis: Diese Option ist bei Verwendung von Winlogbeat nicht verfügbar oder erforderlich, da Health Log Analytics die Ereignisprotokolle Windows von streamt.

7. Schließen Sie auf der Registerkarte **Fertigstellen** die Konfiguration für Ihren Dateneingabetyp ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

◦ Rsyslog:

a. Laden Sie die Konfigurationsdatei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis `/etc/rsyslog.d/rsyslog.conf`.

> **Hinweis:** Wenn Sie Health Log Analytics Anwendung, Version 20.0.11 – Juli 2021, verfügbar im ServiceNow Store verwenden, gehen Sie stattdessen wie folgt vor:
>
> **i.** Installieren Sie auf dem Endpunktgerät die Konfigurationsdatei im Verzeichnis `/etc/rsyslog.d/`.
>
> **ii.** Erstellen Sie ein Spool-Verzeichnis, indem Sie den Befehl `sudo mkdir -p/var/spool/rsyslog` ausführen.

b. Validieren Sie die Konfiguration, indem Sie den Befehl `rsyslogd -N1` ausführen und die Ausgabe überprüfen.

c. Starten Sie Rsyslog neu, indem Sie den Befehl `sudo systemctl restart rsyslog` ausführen.

d. Überprüfen Sie die Ausgabe. Wenn die Systemprotokolldatei `/var/log/messages` Fehler enthält, prüfen und beheben Sie die Fehlermeldungen.

◦ Linux mit Filebeat:

a. Laden Sie die Konfigurationsdatei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis `/etc/filebeat/`.

b. Starten Sie den Agent-Service, indem Sie den Befehl `sudo service filebeat start` ausführen.

> **Hinweis:** Die generierte Konfiguration ignoriert Dateien, die zuletzt vor mehr als sechs Stunden geändert wurden. Bei Bedarf können Sie diese Einstellung in der Konfiguration ändern.

c. Starten Sie den Agent-Service neu, indem Sie den entsprechenden Befehl ausführen.

◦ Windows mit Beats (Filebeat oder Winlogbeat):

a. Laden Sie die Konfigurationsdatei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis `C:\Programme\`.

b. Starten Sie den Agent-Service neu, indem Sie den entsprechenden PowerShell-Befehl ausführen.

- Filebeat: `PS > Start-Service filebeat`
- Winlogbeat: `PS > Start-Service winlogbeat`

> **Hinweis:** Die generierte Konfiguration ignoriert Dateien, die zuletzt vor mehr als sechs Stunden geändert wurden. Bei Bedarf können Sie diese Einstellung in der Konfiguration ändern.

c. Starten Sie den Agent-Service neu, indem Sie den entsprechenden Befehl ausführen.

8. Wählen Sie **Speichern**.
Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.

9. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
- Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

  Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

  Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

10. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streaming von Protokolldaten an Ihre ServiceNow -Instanz.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Erweiterte Einstellungen für Rsyslog-, Splunk- oder TCP-Dateneingaben konfigurieren

Erweiterte Einstellungen für Beats-Dateneingaben konfigurieren

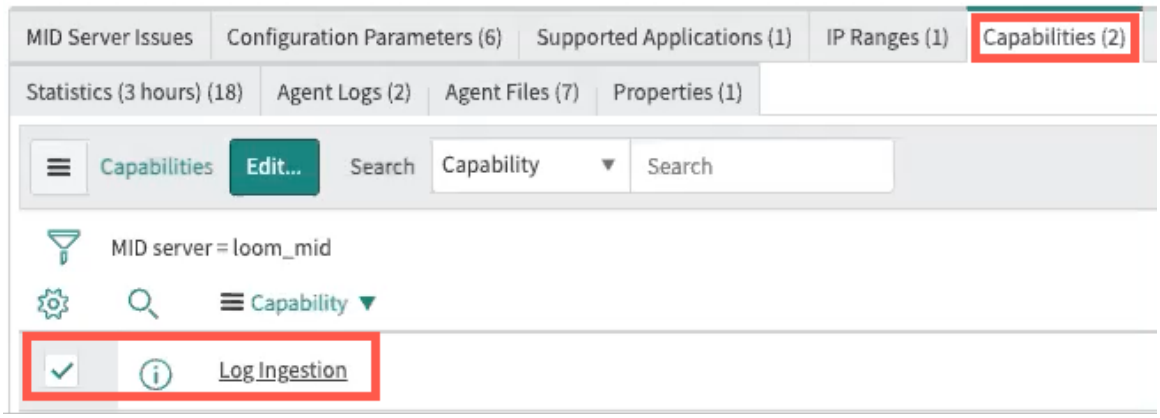
Splunk-Dateneingaben konfigurieren

Konfigurieren Sie eine Dateneingabe für das Streaming von Protokollnachrichten an Ihre ServiceNow-Instanz mit einem Splunk Heavy Forwarder.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .
- Weitere Informationen zur Übermittlung von Protokollen mit SSL TLS-Verschlüsselung finden Sie im Artikel Streaming Data With Rsyslog & Filebeat Using SSL [KB0866319] (Daten mit Rsyslog & Filebeat über SSL streamen) in der Knowledge Base des Now Support.

- Konfigurieren Sie Splunk, um Protokolle mit Syslog an Ihre ServiceNow-Instanz weiterzuleiten.
- Die Konfiguration dieser Dateneingabe setzt das Vorhandensein einer Umgebungsvariablen namens $ SPLUNK_HOME voraus. In Unix-ähnlichen Umgebungen verweist diese Variable normalerweise auf `/opt/splunk`.

Hinweis: In der Umgebung Windows wird dieselbe Verzeichnisstruktur verwendet, jedoch mit umgekehrten Schrägstrichen (\).

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Dieses Setupverfahren dient zum Streamen von Protokollen an Ihre Instanz mit einem Splunk Heavy Forwarder. Wenn Sie keinen Schwerlast-Forwarder verwenden können, können Sie stattdessen einen Universal-Forwarder Splunk verwenden. Weitere Informationen finden Sie im Artikel Splunk Universal Forwarder as a Shipping method [KB0961378] (Splunk Universal Forwarder als Versandmethode) in der Knowledge Base des Now Support.

Ab dem Familienrelease Yokohama können Sie neue Splunk -Dateneingaben verwenden, um Daten im vorverarbeiteten („gebackenen“) Protokollweiterleitungsformat zu erfassen, das Splunk standardmäßig verwendet. Im Kochmodus bettet die Weiterleitung Splunk Konfigurationsdetails wie Host, Quelltyp, Quelle und andere Einstellungen in die Protokolldaten ein. Durch das Erfassen der Daten in HLA in diesem Format wird sichergestellt, dass jede Protokollzeile alle relevanten Kontextinformationen enthält. Wenn Sie die Option für vorgefertigte Daten in HLAverwenden, müssen die Dateien „`props.conf`“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

und „`transforms.conf`“ während der Konfiguration der Dateneingabe für Splunk nicht bearbeitet werden.

Hinweis: Alle Splunk-Konfigurationsdateien befinden sich im Ordner `$SPLUNK_HOME/etc/system/local/`. Wenn eine Konfigurationsdatei, die Sie ändern müssen, nicht vorhanden ist, erstellen Sie sie und speichern Sie sie in diesem Ordner.

Hinweis: Ein ausgefallener MID-Server kann eine Blockade in Ihrer Splunk-Pipeline verursachen. Eine volle Verarbeitungswarteschlange wirkt sich nicht auf die Pipeline aus.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die DateneingabeSplunk für das Streaming von Protokollen über einen Splunk -Heavy Forwarder oder Universal-Forwarderaus.
4. Füllen Sie die Formularfelder auf der Registerkarte **Erste Schritte** aus. Feldbeschreibungen finden Sie unter Splunk Konfigurationsfelder für die Dateneingabe.
5. Fügen Sie auf der Registerkarte **Outputs.conf** der Datei `outputs.conf` die folgenden Absätze hinzu, damit der Versender Protokolldaten über das ausgewählte Transportprotokoll und den ausgewählten Port weiterleitet, und wählen Sie dann **Weiter** aus.

   Hinweis: Wenn Sie bereits Ausgaben konfiguriert haben, führen Sie diese Zeilen mit Ihrer vorhandenen Konfiguration zusammen.

   - Weiterleitung über TCP:

     Hinweis: Verwenden Sie den ersten Absatz nur, wenn Sie noch keinen tcpout-Absatz konfiguriert haben. Der zweite Absatz ist für die Weiterleitung an Health Log Analytics über TCP erforderlich.

     ```
     [tcpout]
     indexAndForward = 1
     defaultGroup = nothing

     [tcpout:health_log_analytics]
     server = ip-172-31-17-121.us-east-2.compute.internal:5000
     sendCookedData = false
     compressed = false
     ```

   - Weiterleitung über UDP:

     Hinweis: Verwenden Sie den ersten Absatz nur, wenn Sie noch keinen syslog-Absatz konfiguriert haben. Der zweite Absatz ist für die Weiterleitung an Health Log Analytics über UDP erforderlich.

     ```
     [syslog]defaultGroup = nothing

     [syslog:health_log_analytics]
     server = ip-172-31-17-121.us-east-2.compute.internal:5000
     ```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Bearbeiten Sie auf der Registerkarte **Props.conf** die Datei `props.conf` und wählen Sie **Weiter** aus.

   Hinweis: Wenn Sie auf der Registerkarte **„Erste Schritte“** die Option **Vorgefertigte Daten verwenden** ausgewählt haben, muss die Datei `props.conf` nicht bearbeitet werden.

   a. Ändern Sie vorhandene Absätze, oder fügen Sie Absätze hinzu, um Quelltypen, Serviceinstanzen und Hosts zur Weiterleitung an Health Log Analyticszu markieren.

      Hinweis: Um optimale Ergebnisse zu erzielen, markieren Sie nur Quelltypen zur Weiterleitung.

      Verwenden Sie beim Hinzufügen von Absätzen folgende Namenformate:

      - Quelltypen: [<source type>]. Beispiel: [syslog]
      - Quellen (nicht empfohlen): [source::<source>]. Beispiel: [source::myApp]
      - Hosts (nicht empfohlen): [host::<host>]. Beispiel: [host::10.9.8.7]

   b. Fügen Sie am Ende jedes Absatzes, den Sie entweder über TCP oder UDP an Health Log Analytics weiterleiten möchten, die folgende Zeile hinzu.

      - Weiterleitung über TCP:

      ```
      TRANSFORMS-cloned_data = clone_for_hla_store_sourcetype,
       clone_for_hla
      ```

      - Weiterleitung über UDP:

      ```
      TRANSFORMS-cloned_data = clone_for_hla_store_sourcetype,
       clone_for_hla_udp
      ```

      Diese Zeile wendet die Transformation CLONE_SOURCETYPE auf die Daten an, um zu verhindern, dass die für die Health Log Analytics-Verarbeitung erforderliche Bearbeitung Ihre vorhandene Datenpipeline beeinträchtigt. Um beispielsweise alle Protokolle vom Quelltyp „syslog“ an Health Log Analytics zu senden, gehen Sie wie folgt vor:

      ```
      [syslog]
                                        #existing configuration goes
       here
                                        TRANSFORMS-cloned_data =
       clone_for_hla_store_sourcetype, clone_for_hla_udp
      ```

   c. Fügen Sie den folgenden Absatz hinzu, um alle relevanten Transformationen anzuwenden, die für die Health Log Analytics-Verarbeitung erforderlich sind:

      Hinweis: Mit Splunk können Sie vertrauliche Daten im geklonten Quelltyp für das ausgewählte Protokoll anonymisieren. Weitere Informationen finden Sie im Abschnitt „Anonymize data“ (Daten anonymisieren) in der Splunk-Dokumentation .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Weiterleitung über TCP:

```
[send_to_hla_tcp]
TRANSFORMS-health_log_analytics =
 health_log_analytics_add_sourcetype,
 health_log_analytics_add_host, health_log_analytics_add_source,
 health_log_analytics_add_syslog5424,
 health_log_analytics_add_index,
 health_log_analytics_add_syslogHost, health_log_analytics_add_time
```

- Weiterleitung über UDP:

```
[send_to_hla_udp]
TRANSFORMS-health_log_analytics =
 health_log_analytics_add_sourcetype,
 health_log_analytics_add_host, health_log_analytics_add_source,
 health_log_analytics_add_syslog5424,
 health_log_analytics_add_index,
 health_log_analytics_add_syslogHost, health_log_analytics_add_time
```

7. Fügen Sie auf der Registerkarte **Transforms.conf** der Datei `transforms.conf` die folgenden Absätze hinzu und wählen Sie anschließend **Weiter** aus.

Hinweis: Wenn Sie auf der Registerkarte **„Erste Schritte“** die Option **Vorgefertigte Daten verwenden** ausgewählt haben, muss die Datei `transforms.conf` nicht bearbeitet werden.

Der dritte Absatz klont die Protokolle zur weiteren Bearbeitung, ohne sich auf die vorhandene Indizierung auszuwirken. Die verbleibenden Absätze fügen die Informationen hinzu, die für die korrekte Verarbeitung von Health Log Analytics erforderlich sind.

Hinweis: Sie können sensible Daten verschleiern, indem Sie hier eine Transformation hinzufügen und dann den Absatz des geklonten Quelltyps in der Datei `props.conf` ändern.

```
[accepted_keys]
#Custom field for preserving sourcetype
hla_sourcetype_preservation=_hla_sourcetype

#Store sourcetype in a custom field, since CLONE_SOURCETYPE overwrites
 it
[clone_for_hla_store_sourcetype]
SOURCE_KEY = MetaData:Sourcetype
REGEX = ^sourcetype::(.+)$
FORMAT = hla_sourcetype::$1
DEST_KEY = _hla_sourcetype

[clone_for_hla]
REGEX=.
DEST_KEY = _TCP_ROUTING
FORMAT = health_log_analytics
CLONE_SOURCETYPE=send_to_hla_tcp

#Only used in case of UDP forwarding
[clone_for_hla_udp]
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
REGEX=.
DEST_KEY = _SYSLOG_ROUTING
FORMAT = health_log_analytics
CLONE_SOURCETYPE=send_to_hla_udp

#Add metadata to the log message, since metadata is lost when
 forwarding externally
[health_log_analytics_add_sourcetype]
SOURCE_KEY = _hla_sourcetype
REGEX = ^hla_sourcetype::(.+)$
FORMAT = sourcetype="$1"] $0
DEST_KEY = _raw

[health_log_analytics_add_host]
SOURCE_KEY = MetaData:Host
REGEX = ^host::(.+)$
FORMAT = host="$1" $0
DEST_KEY = _raw

[health_log_analytics_add_source]
SOURCE_KEY = MetaData:Source
REGEX = ^source::(.+)$
FORMAT = source="$1" $0
DEST_KEY = _raw

[health_log_analytics_add_syslog5424]
REGEX=.
FORMAT = - - [sdid@1234 $0
DEST_KEY = _raw

[health_log_analytics_add_index]
SOURCE_KEY = _MetaData:Index
REGEX = ^(.+)$
FORMAT = $1 $0
DEST_KEY = _raw

[health_log_analytics_add_syslogHost]
SOURCE_KEY = MetaData:Host
REGEX = ^host::(.+)$
FORMAT = $1 $0
DEST_KEY = _raw

[health_log_analytics_add_time]
SOURCE_KEY = _time
REGEX = ^(.+)$
FORMAT = <182>1 $1 $0
DEST_KEY = _raw
```

8. Starten Sie auf der Registerkarte **Finish.conf** Splunk neu, indem Sie den Befehl `$SPLUNK_HOME/bin/splunk restart splunkd` ausführen.
9. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
10. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

    Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
- Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

  Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

  Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

11. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Durch die Dateneingabe wird das Streaming von Protokolldaten an Ihre Instanz ServiceNow mithilfe eines Splunk -Versenders gestartet.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Erweiterte Einstellungen für Rsyslog-, Splunk- oder TCP-Dateneingaben konfigurieren

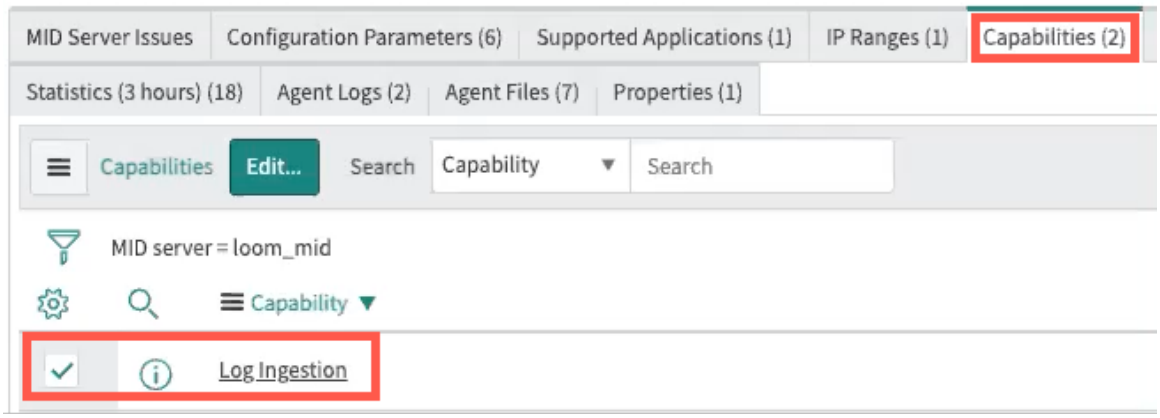
Konfigurieren Sie Abfragedateneingaben für Splunk .

Konfigurieren Sie eine Dateneingabe, die regelmäßig Protokolldaten mithilfe einer Abfrage aus Splunk abruft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .
- Weitere Informationen zur Übermittlung von Protokollen mit SSL TLS-Verschlüsselung finden Sie im Artikel Streaming Data With Rsyslog & Filebeat Using SSL [KB0866319] (Daten mit Rsyslog & Filebeat über SSL streamen) in der Knowledge Base des Now Support.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Eingabe Abrufdaten Splunk aus.
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Splunk Konfigurationsfelder für Abfragedateneingabe.
5. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Füllen Sie die Felder auf den **Registerkarten Transport** und **Erweitert**aus. Feldbeschreibungen finden Sie unter Splunk Konfigurationsfelder für Abfragedateneingabe.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.
   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden. Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

- Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
- Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

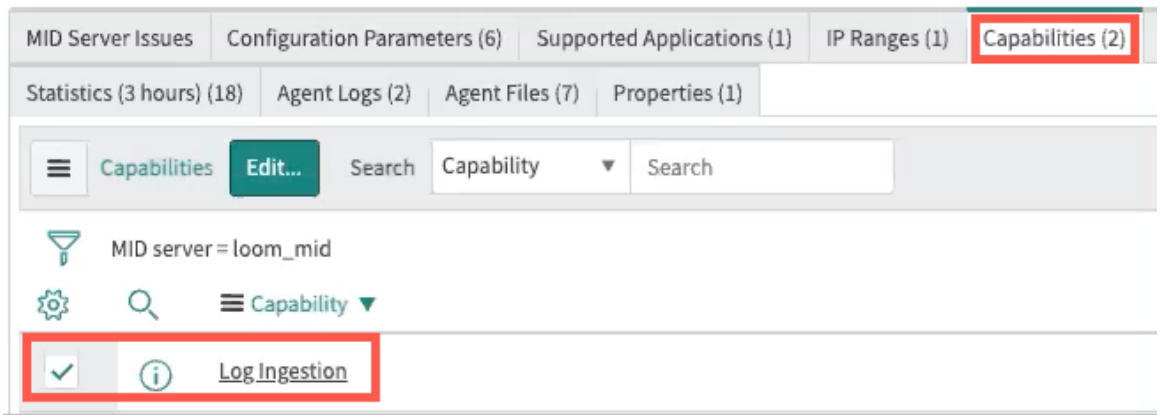
8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Elasticsearch-Dateneingaben konfigurieren

Konfigurieren Sie eine Dateneingabe für das Streaming von Protokollnachrichten von Elasticsearch-Indizes an Ihre ServiceNow-Instanz.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss es sich um eine öffentliche IP-Adresse handeln. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Health Log Analytics unterstützt Elasticsearch Version 5.4 und höher.

Hinweis: Erweiterte Informationen zum Streamen von Protokolldaten aus Indizes Elasticsearch an Ihre -Instanz finden Sie im Artikel Stream-Protokolle mit Elasticsearch-Dateneingabe – Leitfaden für Fortgeschrittene [KB1080162] in der Knowledge Base Now Support.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Elasticsearch-Dateneingabe.
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Wählen Sie **Erweitert** aus, um erweiterte Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Elasticsearch Konfigurationsfelder für die Dateneingabe. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Erweiterte Einstellungen für Elasticsearch-Dateneingaben konfigurieren.
6. Füllen Sie die Felder auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Konfigurationsfelder für die Dateneingabe.
7. Füllen Sie die Formularfelder auf der Registerkarte **Query Settings** (Abfrageeinstellungen) aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Konfigurationsfelder für die Dateneingabe.
8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung**angezeigt. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

     Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

10. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streaming von Protokolldaten aus den Indizes Elasticsearch an Ihre Instanz ServiceNow .

Weitere Informationen zum Streaming von Protokollen mit der Dateneingabe Elasticsearch finden Sie im Artikel Stream-Protokolle mit Elasticsearch-Dateneingabe – Erweiterte Anleitung [KB1080162] in der Knowledge Base Now Support.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Hinweis: Wenn Sie Probleme mit Berechtigungen beim Streaming von Protokolldaten von Elasticsearch haben, lesen Sie den Artikel Granting privileges for data streams from Elasticsearch [KB0967366] (Berechtigungen für Datenströme von Elasticsearch erteilen) in der Now Support-Knowledge Base.

Zugehörige Informationen

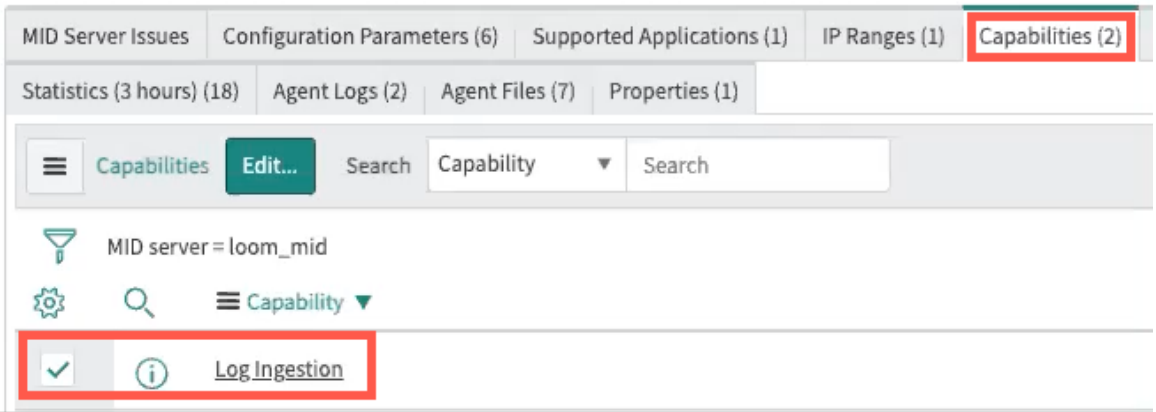
Erweiterte Einstellungen für Elasticsearch-Dateneingaben konfigurieren

Konfigurieren Sie TCP-Dateneingaben

Konfigurieren Sie eine Dateneingabe zum Senden von Protokollmeldungen in Rohform direkt über ein TCP/SSL-Socket an Ihre ServiceNow-Instanz senden.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

- Weitere Informationen zur Übermittlung von Protokollen mit SSL TLS-Verschlüsselung finden Sie im Artikel Streaming Data With Rsyslog & Filebeat Using SSL [KB0866319] (Daten mit Rsyslog & Filebeat über SSL streamen) in der Knowledge Base des Now Support.

Hinweis: Informationen zum Streamen von Daten von Logstash an Ihre -Instanz finden Sie im Artikel Streamingdaten von Logstash an Ihre HLA-Instanz [KB0994735] in der Knowledge Base Now Support.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie den TCP-Dateneingabetyp.

   Hinweis: Der ausgewählte Dateneingabetyp ergänzt die passive Dateneingabe (Listener). Weitere Informationen finden Sie unter Unterstützte Dateneingaben für Health Log Analytics.

4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für TCP-Dateneingabe.
5. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für TCP-Dateneingabe.
   Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Erweiterte Einstellungen für Rsyslog-, Splunk- oder TCP-Dateneingaben konfigurieren.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Senden von Rohprotokollnachrichten an Ihre Instanz ServiceNow direkt über einen TCP/SSL-Socket.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Erweiterte Einstellungen für Rsyslog-, Splunk- oder TCP-Dateneingaben konfigurieren

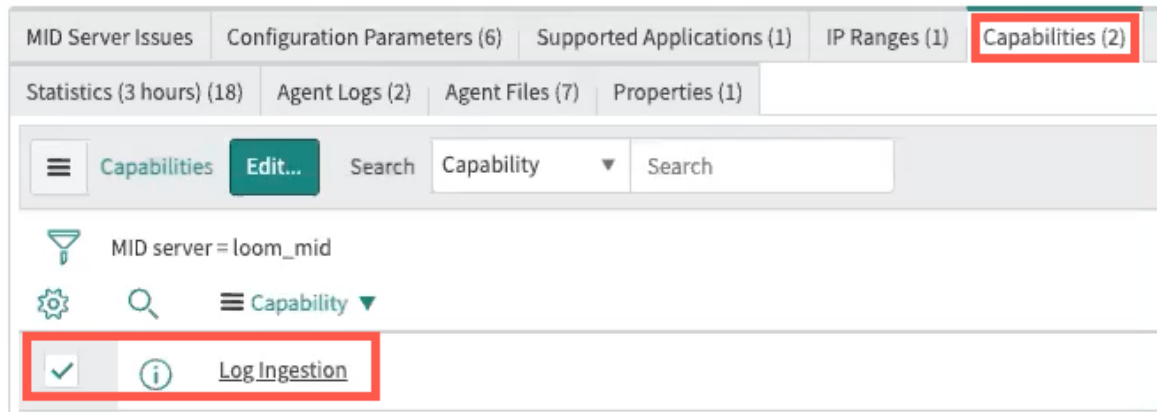
Konfigurieren Sie UDP-Dateneingaben

Konfigurieren Sie eine Dateneingabe zum Senden von Rohprotokollnachrichten an Ihre Instanz ServiceNow direkt über einen UDP-Socket.

Vorbereitungen

Diese Funktion wird in der Anwendung Health Log Analytics, Version 25.0.17 – November 2022 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .
- Weitere Informationen zur Übermittlung von Protokollen mit SSL TLS-Verschlüsselung finden Sie im Artikel Streaming Data With Rsyslog & Filebeat Using SSL [KB0866319] (Daten mit Rsyslog & Filebeat über SSL streamen) in der Knowledge Base des Now Support.

Erforderliche Rolle: evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie den UDP-Dateneingabetyp aus.

   Hinweis: Der ausgewählte Dateneingabetyp ergänzt die passive Dateneingabe (Listener). Weitere Informationen finden Sie unter Unterstützte Dateneingaben für Health Log Analytics.

4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für UDP-Dateneingabe.
5. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für UDP-Dateneingabe.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Senden von Rohprotokollnachrichten an Ihre Instanz ServiceNow direkt über einen UDP-Socket.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

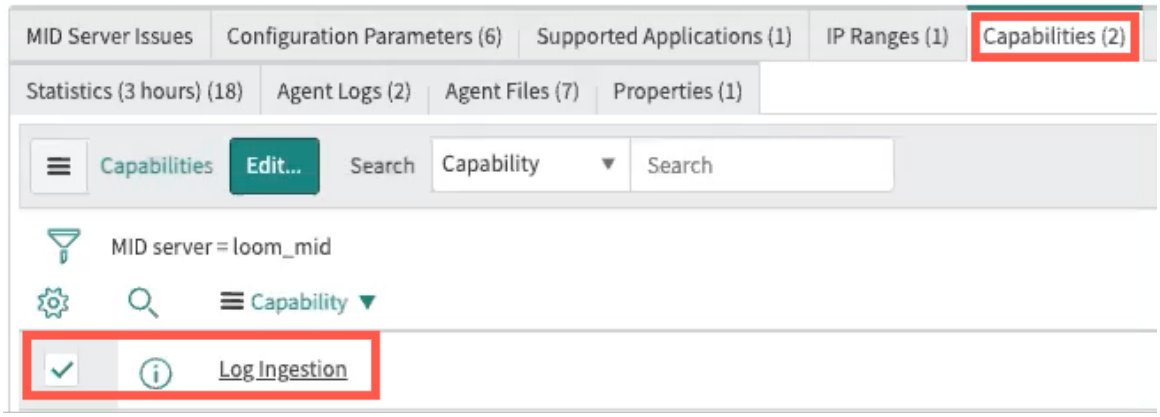
Erweiterte Einstellungen für Rsyslog-, Splunk- oder TCP-Dateneingaben konfigurieren

Konfigurieren Sie GCP PubSub-Dateneingaben

Konfigurieren Sie eine Dateneingabe für den Empfang von Protokollnachrichten, die in einem Google Cloud Pub/Sub-Thema veröffentlicht werden, und deren Streaming an Ihre ServiceNow -Instanz.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .
- Weitere Informationen zur Übermittlung von Protokollen mit SSL TLS-Verschlüsselung finden Sie im Artikel Streaming Data With Rsyslog & Filebeat Using SSL [KB0866319] (Daten mit Rsyslog & Filebeat über SSL streamen) in der Knowledge Base des Now Support.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie den Dateneingabetyp „GCP PubSub“ aus.

   Hinweis: Der ausgewählte Dateneingabetyp ergänzt die passive Dateneingabe (Listener). Weitere Informationen finden Sie unter Unterstützte Dateneingaben für Health Log Analytics.

4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für GCP PubSub-Dateneingabe.
5. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbeschreibungen finden Sie unter Konfigurationsfelder für GCP PubSub-Dateneingabe.

6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe empfängt Protokollnachrichten aus dem Pub/Sub-Thema Google Cloud und streamt sie über ServiceNow an Ihre Instanz MID-Server.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

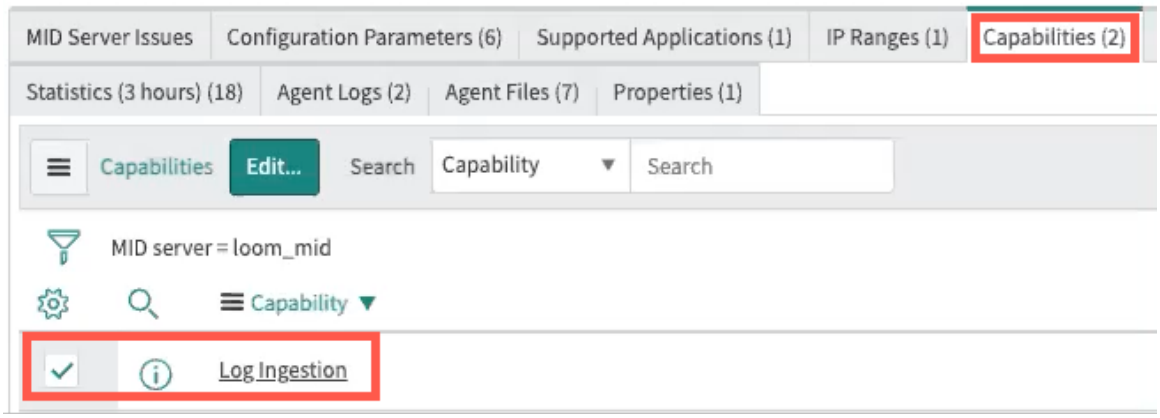
MID-Server-Dateneingaben konfigurieren

Konfigurieren Sie eine Dateneingabe zum Sammeln und Streamen von MID-Server-Protokollnachrichten an Ihre ServiceNow-Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .
- Weitere Informationen zur Übermittlung von Protokollen mit SSL TLS-Verschlüsselung finden Sie im Artikel Streaming Data With Rsyslog & Filebeat Using SSL [KB0866319] (Daten mit Rsyslog & Filebeat über SSL streamen) in der Knowledge Base des Now Support.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren beschreibt, wie Sie eine MID-Server-Dateneingabe auf der Seite „Dateneingaben“ erstellen. Um die MID-Server-Dateneingabe automatisch zu konfigurieren, klicken Sie auf den zugehörigen Link im Formular „MID-Server“.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die MID-Server-Dateneingabe.
4. Geben Sie im Formular eine Beschreibung der Dateneingabe und den Namen des MID-Server an, von dem die Protokolle gestreamt werden.
   Feldbeschreibungen finden Sie unter MID-Server Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Füllen Sie die Felder des Formulars aus. Feldbeschreibungen finden Sie unter MID-Server Konfigurationsfelder für die Dateneingabe. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Erweiterte Einstellungen für MID-Server-Dateneingaben konfigurieren.
6. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Sammeln und Streaming MID-Server von -Protokollnachrichten an Ihre ServiceNow -Instanz.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Amazon CloudWatch-Dateneingaben konfigurieren

Konfigurieren Sie eine Dateneingabe für das Streaming von Protokolldaten aus Amazon CloudWatch an Ihre ServiceNow-Instanz.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss er eine öffentliche IP-Adresse besitzen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Amazon CloudWatch-Dateneingabe.
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Amazon CloudWatch Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Amazon CloudWatch Konfigurationsfelder für die Dateneingabe. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Erweiterte Einstellungen für Amazon CloudWatch-Dateneingaben konfigurieren.
6. Füllen Sie die Felder auf der Registerkarte **Abfrageeinstellungen** aus.
   Feldbeschreibungen finden Sie unter Amazon CloudWatch Konfigurationsfelder für die Dateneingabe.
7. Füllen Sie die Felder auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Amazon CloudWatch Konfigurationsfelder für die Dateneingabe. Diese Felder sind obligatorisch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

10. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe startet das Streaming von Protokolldaten von Amazon CloudWatch an Ihre Instanz ServiceNow .

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Erweiterte Einstellungen für Amazon CloudWatch-Dateneingaben konfigurieren

Amazon S3-Dateneingaben konfigurieren

Konfigurieren Sie eine Dateneingabe für das Streaming von Protokolldaten aus Amazon S3-Buckets (Simple Storage Service) an Ihre ServiceNow-Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss er eine öffentliche IP-Adresse besitzen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Amazon S3-Dateneingabe.
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Amazon S3 Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Amazon S3 Konfigurationsfelder für die Dateneingabe. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Erweiterte Einstellungen für Amazon S3-Dateneingaben konfigurieren.
6. Füllen Sie die Felder auf der Registerkarte **Abfrageeinstellungen** aus.
7. Füllen Sie das Feld auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Amazon S3 Konfigurationsfelder für die Dateneingabe.
8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

10. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe startet das Streaming von Protokolldaten aus Buckets vom Amazon S3 Typ an Ihre Instanz ServiceNow .

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Erweiterte Einstellungen für Amazon S3-Dateneingaben konfigurieren

Microsoft Azure Log Analytics-Dateneingaben konfigurieren

Konfigurieren Sie eine Dateneingabe für das Streaming von Protokolldaten von Microsoft Azure Log Analytics an Ihre Instanz ServiceNow. Die Dateneingabe verweist die KI-Engine von Health Log Analytics an eine Datenquelle in Ihrem Microsoft Azure Log Analytics-Konto.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss er eine öffentliche IP-Adresse besitzen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Microsoft Azure Log Analytics-Dateneingabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Log Analytics Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Microsoft Azure Log Analytics Konfigurationsfelder für die Dateneingabe. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Erweiterte Einstellungen für Microsoft Azure Log Analytics-Dateneingaben konfigurieren.
6. Füllen Sie die Felder auf der Registerkarte **Abfrageeinstellungen** aus.

   Health Log Analytics verwendet die in diesen Feldern festgelegten Werte, um die Abfrage zum Empfangen von Protokolldaten von Microsoft Azure Log Analyticszu generieren.

   Zum Beispiel:

   ```
   {"query": "ContainerLog | where TimeGenerated > %s | take 500",
    "project": ["TimeGenerated", "LogEntry", "LogEntrySource"]}
   ```

   wobei:

   - `ContainerLog`: Der Name der Datenquelle.
   - `TimeGenerated`: Der Name der Ereigniszeiteigenschaft.
   - `500`: Die maximale Anzahl der in jeder Abfrage abgerufenen Zeilen.
   - `["TimeGenerated", "LogEntry", "LogEntrySource"]`: Die Ereigniszeit und die durch Kommas getrennte Liste der zurückzugebenden Spaltennamen.

   Alternativ können Sie eine anwenderdefinierte Abfrage im Feld **Protokollabfrage** konfigurieren. Der Wert, den Sie in diesem Feld festlegen, überschreibt die Werte in allen anderen Feldern auf der Registerkarte **Abfrageeinstellungen** mit Ausnahme des Felds **Von**. Wenn das Feld **Protokollabfrage** leer ist, generiert Health Log Analytics die Abfrage anhand der Werte, die in den anderen Feldern der Registerkarte festgelegt sind.

   Eine Beschreibung der Felder **für Abfrageeinstellungen** finden Sie unter Microsoft Azure Log Analytics Konfigurationsfelder für die Dateneingabe.

7. Füllen Sie die Felder auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Log Analytics Konfigurationsfelder für die Dateneingabe.
8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
- Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

10. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe startet das Streaming von Protokolldaten von Microsoft Azure Log Analytics an Ihre Instanz ServiceNow .

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Erweiterte Einstellungen für Microsoft Azure Log Analytics-Dateneingaben konfigurieren

Microsoft Azure Event Hubs-Dateneingaben konfigurieren

Konfigurieren Sie eine Dateneingabe für das Streaming von Events aus Microsoft Azure Event Hubs an Ihre ServiceNow-Instanz.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss er eine öffentliche IP-Adresse besitzen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Microsoft Azure Event Hubs-Dateneingabe.
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Event Hubs Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Microsoft Azure Event Hubs Konfigurationsfelder für die Dateneingabe. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Erweiterte Einstellungen für Microsoft Azure Event Hubs-Dateneingaben konfigurieren.
6. Füllen Sie die Felder auf der Registerkarte **Abfrageeinstellungen** aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Event Hubs Konfigurationsfelder für die Dateneingabe.
7. Füllen Sie die Felder auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Event Hubs Konfigurationsfelder für die Dateneingabe.
8. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
9. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

10. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe startet das Streaming von Protokolldaten von Microsoft Azure Event Hubs an Ihre Instanz ServiceNow .

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Erweiterte Einstellungen für Microsoft Azure Event Hubs-Dateneingaben konfigurieren

Apache Kafka-Dateneingaben konfigurieren

Konfigurieren Sie eine Dateneingabe für das Streaming von Protokolldaten aus Apache Kafka an Ihre ServiceNow-Instanz.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.

  Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss er eine öffentliche IP-Adresse besitzen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Apache Kafka-Dateneingabe.
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Apache Kafka Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Apache Kafka Konfigurationsfelder für die Dateneingabe. Informationen zur späteren Konfiguration der erweiterten Einstellungen finden Sie unter Erweiterte Einstellungen für Apache Kafka-Dateneingaben konfigurieren.
6. Füllen Sie das Feld auf der Registerkarte **Abfrageeinstellungen** aus.
   Feldbeschreibungen finden Sie unter Apache Kafka Konfigurationsfelder für die Dateneingabe.
7. Füllen Sie die Felder auf der Registerkarte **Übertragung** aus.
   Feldbeschreibungen finden Sie unter Apache Kafka Konfigurationsfelder für die Dateneingabe.
8. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.

9. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

10. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe startet das Streaming von Protokolldaten von Apache Kafka an Ihre Instanz ServiceNow .

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Zugehörige Informationen

Erweiterte Einstellungen für Apache Kafka-Dateneingaben konfigurieren

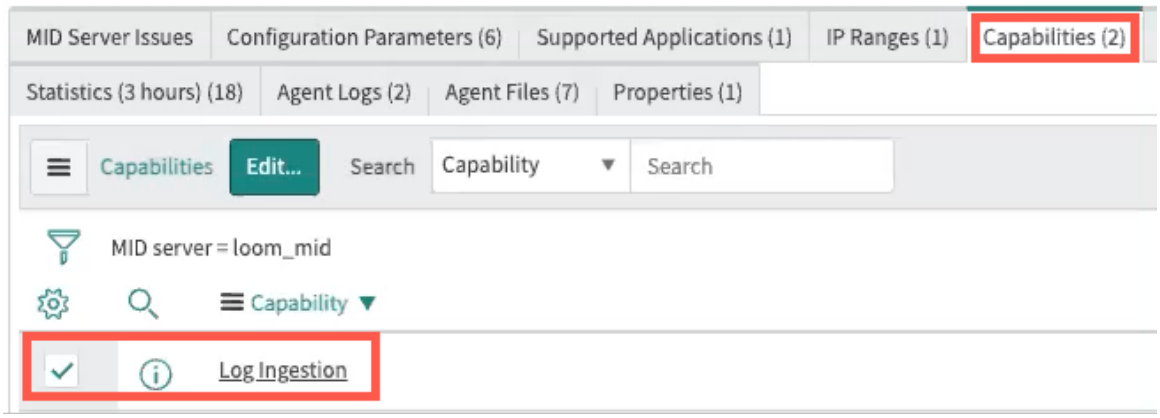
Konfigurieren Sie REST API-Dateneingaben

Konfigurieren Sie eine REST API-Dateneingabe für das Streaming von Protokolldaten an Ihre ServiceNow-Instanz im JSON-Format.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Stellen Sie sicher, dass ein MID-Webserver für MID-Servereingerichtet ist.

  Weitere Informationen finden Sie unter MID-Webservererweiterung konfigurieren.

  Wählen Sie im Formular „MID-Webserver-Kontext“ im Feld **Ausführen für** die Option *Spezifischer MID Server* und nicht die Clusteroption aus. Wählen Sie im Feld **MID-Server** den MID-Server aus, an den die Protokolldaten übertragen werden.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss er eine öffentliche IP-Adresse besitzen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Erweiterung verarbeitet Protokollnachrichten, die von einer externen Protokollquelle an den MID-Server gesendet werden. Der MID-Server verarbeitet die Nachrichten und übergibt sie dann an Ihre Instanz.

Zum Streamen von Protokollnachrichten an den MID-Server muss die URL das Format `http://{MID_SERVER_IP}:{MID_WEB_SERVER_PORT}/api/mid/hla/raw` haben, wobei `/api/mid/hla/raw` der Endpunkt ist.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die REST API-Dateneingabe aus.
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für die REST-API-Dateneingabe.
5. Wählen Sie **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an. Die Dateneingabe beginnt mit dem Streaming von Protokolldaten im JSON-Format an Ihre Instanz ServiceNow.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Konfigurieren Sie ServiceNow Systemprotokolle , um Dateneingaben für abzurufen

Konfigurieren Sie eine Dateneingabe für das Streaming von Protokolldaten aus der Systemprotokolltabelle ServiceNow an die KI-Engine Health Log Analytics (Occultus).

Vorbereitungen

Aktivieren Sie für Versionen vor Yokohama diese Funktion, indem Sie die Anweisungen im Artikel How to enable the HLA Glide Syslog data input for Glide versionälter als Yokohama [KB1651324] in der Knowledge Base Now Support befolgen.

Hinweis: Im System kann nur eine einzelne Dateneingabe für ServiceNow Systemprotokolle Abruf vorhanden sein. Diese Dateneingabe wird nicht auf einem MID-Server ausgeführt.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Dateneingabe ServiceNow Systemprotokolle Abrufen .
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter ServiceNow Systemprotokolle – Dateneingabe-Konfigurationsfelder abrufen.
5. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu und hängt die Konfigurationsdatei an den Dateneingabedatensatz an.

Die Dateneingabe startet das Streaming von ServiceNow Protokolldaten aus der Systemprotokolltabelle an die KI-Engine Health Log Analytics basierend auf den konfigurierten Filtern. Administratoren können Filter festlegen, um die Systemprotokolltabelle abzufragen. Benutzer mit der Rolle evt_mgmt_user können mit Ereignismanagement die Protokolle überwachen und die Warnungen anzeigen, die Health Log Analytics aus ihnen generiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

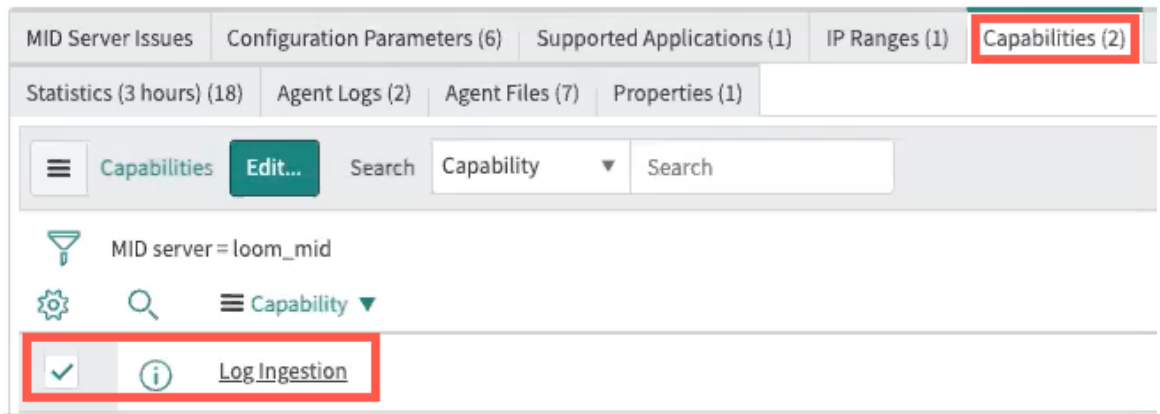
Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Konfigurieren Sie CRBL-Dateneingaben

Konfigurieren Sie eine dedizierte CRBL-Dateneingabe, um Health Log Analytics die Verarbeitung von CRBL-Protokollnachrichten zu ermöglichen, die in Ihre Instanz ServiceNow gestreamt werden.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss es sich um eine öffentliche IP-Adresse handeln. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihre Organisation CRBL zum Filtern und Weiterleiten großer Mengen von Protokolldaten aus verschiedenen Quellen verwendet, unterscheidet sich das Protokollformat, das Health Log Analytics empfängt, von anderen Typen. Die CRBL-Dateneingabe ermöglicht es HLA, Transportheader von inneren Protokollnachrichten in diesem Format zu erkennen und zu trennen und nur die innere Nachricht zur Verarbeitung an die Quelltypstruktur weiterzuleiten.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die CRIB-Dateneingabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Füllen Sie auf der Registerkarte **Erste Schritte** die Formularfelder aus, und wählen Sie **Weiter**aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für die CRBL-Dateneingabe.
5. Füllen Sie auf der **Registerkarte** Konfig die Formularfelder aus, und wählen Sie **Weiter**aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für die CRBL-Dateneingabe.
6. Wählen Sie auf der **Registerkarte** Verarbeiten die gewünschte Route und anschließend **Weiter**aus.

   Weitere Informationen finden Sie unter Konfigurationsfelder für die CRBL-Dateneingabe.

   Hinweis: Informationen zur Behebung von Problemen im Zusammenhang mit diesem Schritt finden Sie unter CRBL – CRBL-Dateneingabe einrichten | Artikel zur Behebung von Problemen bei der Einrichtung und Datenerfassung [KB0558611] in der Now Support-Knowledge Base.

   Die Registerkarte **Fertigstellen** wird geöffnet.
7. Überprüfen Sie in der CRBL-Instanz, ob die Konfiguration der Dateneingabe korrekt ist. Bei Bedarf können Sie die auf der Registerkarte **Fertigstellen** angezeigten CRBL-Befehle verwenden.
8. Wenn die Konfiguration korrekt ist, kehren Sie zur Registerkarte **Fertigstellen** der Dateneingabekonfiguration zurück, und wählen Sie **Veröffentlichen**, um die Dateneingabe zu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Durch die Dateneingabe wird das Streaming von Protokolldaten an Ihre Instanz ServiceNow gestartet.

Informationen zur Behebung von Problemen im Zusammenhang mit der Erfassung von Protokolldaten aus CRBL finden Sie unter CRBL – Einrichten von CRBL-Dateneingabe | Artikel zur Behebung von Problemen bei der Einrichtung und Datenerfassung [KB0558611] in der Now Support-Knowledge Base.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

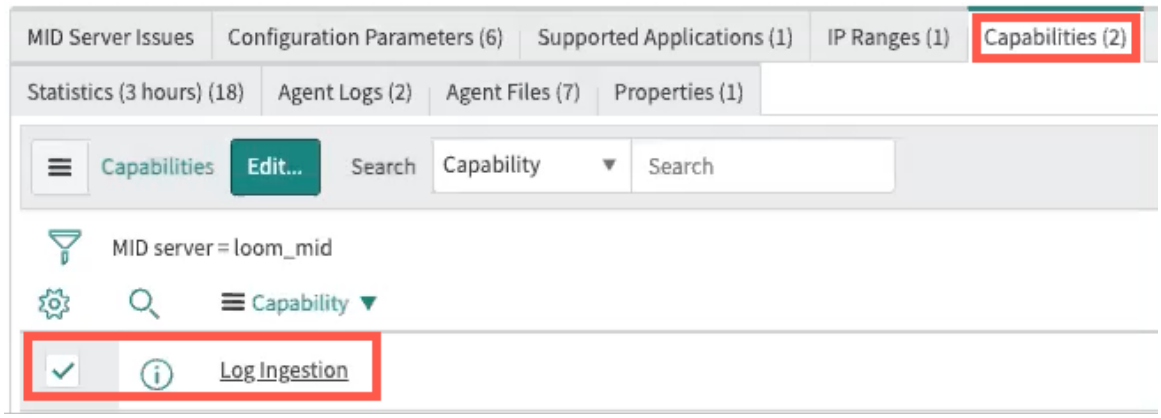
Konfigurieren Sie Edge-Delta-Dateneingaben

Konfigurieren Sie eine Edge-Delta-Dateneingabe, damit Health Log Analytics Edge-Delta-Protokollnachrichten verarbeiten kann, die in Ihre Instanz ServiceNow von gestreamt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss es sich um eine öffentliche IP-Adresse handeln. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihre Organisation Edge-Delta verwendet, um große Mengen von Protokolldaten aus mehreren Quellen zu verarbeiten, bevor sie an HLAgesendet werden, unterscheidet sich das Protokollformat, das HLA empfängt, von anderen Typen. Die Edge-Delta-Dateneingabe ermöglicht es HLA, Transportheader von inneren Protokollnachrichten in diesem Format zu erkennen und zu trennen und nur die innere Nachricht zur Verarbeitung an die Quelltypstruktur weiterzuleiten.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie die Edge-Delta-Dateneingabe aus.
4. Füllen Sie die Felder des Formulars aus.
   Eine detaillierte Beschreibung der Felder finden Sie unter Eingabekonfigurationsfelder für Edge-Delta-Daten.
5. Wählen Sie **Speichern** aus, um Ihre Konfiguration zu speichern.
6. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe zu veröffentlichen.

Ergebnisse

Der Konfigurationsprozess für die Dateneingabe ist abgeschlossen. Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“**hinzu. Durch die Dateneingabe wird das Streaming von Protokolldaten an Ihre Instanz ServiceNow gestartet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

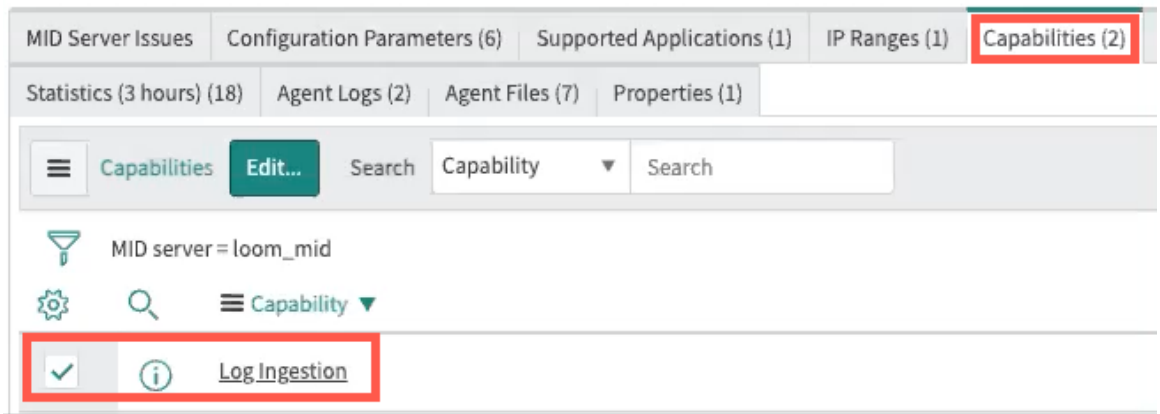
Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Konfigurieren Sie die Dateneingaben des Vektoragenten

Konfigurieren Sie eine Vektoragenten-Dateneingabe, damit Health Log Analytics Protokollnachrichten verarbeiten kann, die über einen Vektoragenten in Ihre Instanz ServiceNow gestreamt werden.

Vorbereitungen

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss es sich um eine öffentliche IP-Adresse handeln. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

- Vergewissern Sie sich, dass Sie eine `vektor.yaml`- Datei auf Ihrem System haben, oder erstellen Sie eine.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Ihre Organisation „Vector by Datadog “ verwendet, um Protokolldaten aus mehreren Quellen zu verarbeiten, bevor sie an HLAgesendet werden, unterscheidet sich das Protokollformat, das HLA empfängt, von anderen Typen. Die Vektoragent-Dateneingabe ermöglicht es HLA, Transportheader von inneren Protokollnachrichten in diesem Format zu erkennen und zu trennen und nur die innere Nachricht zur Verarbeitung an die Quelltypstruktur weiterzuleiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie auf der Seite „Data Inputs“ (Dateneingaben) die Option **Neu** aus.
3. Wählen Sie **Vektor - Stream - Protokolle aus Vektoragent aus**.
4. Füllen Sie auf der Registerkarte **Erste Schritte** das Formular aus, und wählen Sie **Weiter**aus. Eine detaillierte Beschreibung der Felder finden Sie unter Konfigurationsfelder für die Dateneingabe des Vektoragenten.
5. Aktualisieren Sie auf der Registerkarte **„vector.yaml“** den Code nach Bedarf mit den relevanten Werten.
   Sie können beispielsweise die Quellen oder Quelldateien angeben, aus denen die Protokolle gestreamt werden.

   Hinweis: Code, den Sie nicht ändern dürfen, enthält einen kommentierten Hinweis.

   Weitere Informationen finden Sie in der Vektordokumentation .
6. Kopieren Sie den aktualisierten Code, und fügen Sie ihn in die Datei `„vector.yaml“` auf Ihrem System ein.
7. Wählen Sie **Weiter**.
   Auf der Registerkarte **Fertigstellen** wird eine Meldung angezeigt, die bestätigt, dass der Konfigurationsprozess für die Dateneingabe abgeschlossen ist.
8. Starten Sie das Streaming von Protokolldaten, indem Sie „Vector“ mit der Konfigurationsdatei ausführen.
   Führen Sie den folgenden Befehl aus:`vector --config /path/to/your/vector.yaml`, wobei `/path/to/your/` der tatsächliche Pfad zu Ihrer YAML-Datei ist.
9. Wahlweise: Verwenden Sie nach Bedarf die anderen auf der Registerkarte **Fertigstellen** angezeigten Befehle.
10. Wählen Sie **Speichern**, um die Dateneingabe zu speichern.

Ergebnisse

Health Log Analytics fügt den Dateneingabedatensatz der Tabelle **„Dateneingaben“** hinzu. Durch die Dateneingabe wird das Streaming von Protokolldaten an Ihre Instanz ServiceNow gestartet.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

Nächste Maßnahme

Stellen Sie sicher, dass die Dateneingabe aus Streaming-Daten besteht.

Integrationen über Integrations Launchpadeinrichten

Richten Sie Integrationen für Health Log Analytics über Ereignismanagement Integrations Launchpad in Service Operations-Arbeitsbereich für ITOMein.

Integrations-Launchpad

Das Tool Integrations Launchpad bietet eine einheitliche Schnittstelle für eine bequeme Integration mit Protokolldaten-Connectors, die Protokollnachrichten im Rohzustand aus externen Quellen zur Verarbeitung und Analyse in Ihre Instanz ServiceNow einspeisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Integrations Launchpad in Service Operations-Arbeitsbereich für ITOM.

Integrationen für Health Log Analytics

Mit Integrations Launchpad werden die folgenden Integrationen für Health Log Analyticsaktiviert:

Integrationen abrufen

Diese Integrationen rufen Protokolldaten aus externen Datenquellen ab und streamen die Daten über MID-Serveran Ihre -Instanz. Wählen Sie eine Integration in der Tabelle aus, um eine Seite mit dem Setup-Verfahren zu öffnen.

Pull-Connectors

Integration	Beschreibung
Elasticsearch	Streamt Protokolldaten aus -Indizes Elasticsearch an Ihre -Instanz.
ServiceNow-Systemprotokolle	Sendet Protokolldaten aus der Systemprotokolltabelle ServiceNow an die KI-Engine Health Log Analytics. **Hinweis:** Im System kann nur eine einzelne Systemprotokoll-Dateneingabe ServiceNow vorhanden sein, und diese Eingabe muss nur von Anwendern mit der Administratorrolle erstellt und konfiguriert werden. Diese Dateneingabe wird nicht für MID-Serverausgeführt.

Push-Integrationen

Diese Integrationen stellen eine Verbindung zu externen Datenquellen her, die Protokolldaten über MID-Serveran Ihre -Instanz übertragen. Wählen Sie eine Integration in der Tabelle aus, um eine Seite mit dem Setup-Verfahren zu öffnen.

Push-Connectors

Integration	Beschreibung
UDP	Er sendet Protokollnachrichten im Rohzustand direkt über einen UDP-Socket an Ihre Instanz.
TCP	Sendet Protokollnachrichten im Rohzustand direkt über einen TCP/SSL-Socket an Ihre Instanz.

Elasticsearch Integrationenkonfigurieren

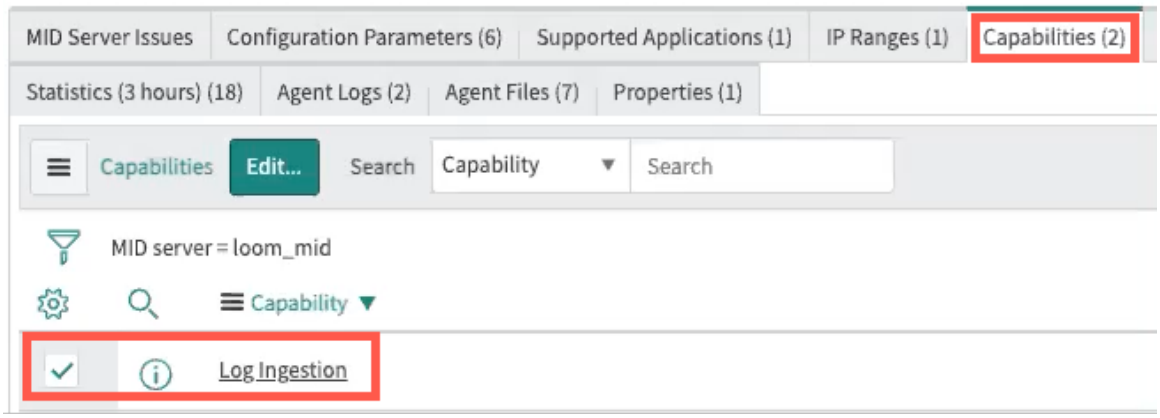
Konfigurieren Sie eine Integration für das nahtlose Streaming von Protokolldaten von Elasticsearch -Indizes an Ihre -Instanz zur Verarbeitung durch Health Log Analytics.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Hinweis: Health Log Analytics unterstützt Elasticsearch Version 5.4 und höher. Erweiterte Informationen zum Streamen von Protokolldaten aus Indizes Elasticsearch an Ihre -Instanz finden Sie im Artikel Stream-Protokolle mit Elasticsearch-Dateneingabe – Leitfaden für Fortgeschrittene [KB1080162] in der Knowledge Base Now Support.

- Stellen Sie sicher, dass die Anwendung Health Log Analytics in Ihrer Instanz installiert und bereitgestellt ist. Weitere Informationen finden Sie unter Health Log Analytics installieren (HLA).
- Stellen Sie sicher, dass eine Serviceinstanz verfügbar ist.
- Stellen Sie sicher, dass die KI-Engine Health Log Analytics aktiv ist und ausgeführt wird.
- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse des MID-Server über Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss es sich um eine öffentliche IP-Adresse handeln. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen `mid.public_ip` mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Geben Sie auf der Registerkarte **Integrationen durchsuchen** im Suchfeld `Elasticsearch` ein.
4. Wählen Sie die Integrationskachel Elasticsearch aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie den Integrationsprozess gestartet haben, ohne alle im Abschnitt Bevor Sie beginnen, zu erfüllen, wird eine Meldung angezeigt. Sie haben die Möglichkeit, die Integration abzubrechen und die fehlenden Anforderungen abzuschließen oder im Entwurfsmodus fortzufahren und sie später zu erfüllen. Beachten Sie, dass Sie eine Integration nur aktivieren können, wenn alle Voraussetzungen erfüllt sind. Konfigurierte und vongespeicherte Integrationen, die nicht aktiviert wurden, sind auf der Registerkarte **Installierte Integrationen** in Integrations Launchpadunter **Warten auf Ihre Aktion**verfügbar.

5. Wählen Sie **Details angeben**aus.
   Die **Details bereitstellen** werden angezeigt. In diesem Bildschirm müssen Sie wichtige Details für die neue Integration angeben, einschließlich MID-Server oder des Clusters, aus dem die Protokollnachrichten abgerufen werden sollen, und der Serviceinstanz, an die die Daten gebunden werden sollen.
6. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Integration Konfigurationsfelder.
7. Wahlweise: Wählen Sie **Erweitert** aus, um erweiterte Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Elasticsearch Integration Konfigurationsfelder.
8. Wählen Sie **Weiter**.
   Der Bildschirm **„Datenabruf festlegen“** wird angezeigt. In diesem Bildschirm müssen Sie angeben, welche Protokolldaten vom Gerät abgerufen werden sollen, welche Extraktionsmethode verwendet wird und wie die Daten an die Instanz gestreamt werden.
9. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Integration Konfigurationsfelder.
10. Wählen Sie **Testen und speichern**aus.
    Das System speichert die neue Integration in der Datenbank und testet den konfigurierten Port. Entweder wird eine Erfolgsmeldung zurückgegeben oder ein Fehler zurückgegeben. Wenn ein Fehler zurückgegeben wird, nehmen Sie Anpassungen an Ihrer Konfiguration gemäß den Vorschlägen auf dem Bildschirm vor, und wählen Sie dann erneut **Testen und speichern** aus. Sobald der Test erfolgreich ist, können Sie die-Integrationaktivieren.
11. Wählen Sie **Aktivieren**.
    Die -Integration wird aktiviert. Die Registerkarte **Übersicht** wird angezeigt.

Ergebnisse

Protokolldaten beginnt das Streaming von an Ihre Instanz ServiceNow. Die Kachel für die -Integration ist auf der Registerkarte **Installierte Integrationen** in Integrations Launchpadverfügbar.

Benutzer mit der Rolle evt_mgmt_user können mit Ereignismanagement die Protokolle überwachen und die Warnungen anzeigen, die Health Log Analytics aus ihnen generiert.

Nächste Maßnahme

Überprüfen Sie den Status des Protokolldaten-Streamings und die Quellen von der Integration auf der Registerkarte **Übersicht**. Nutzen Sie die angezeigten Informationen, um zu verfeinern, wie HLA die Protokolldaten liest, indem Sie die Konfiguration der Integration anpassen. Weitere Informationen finden Sie unter Streamingstatus und Quellen von Protokolldaten von einern Integrationüberprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Auf der Registerkarte **Übersicht** können Sie direkt zu den Seiten „Dateneingabezuordnung“, „Quelltypstrukturen“ und „Protokollquellen“ mit Kontext aus dieser Integration wechseln, indem Sie das Menüsymbol „Ansicht“ (⋮ “) auswählen und die entsprechende Option auswählen. Über das Menü können Sie auch direkt auf den Protokoll-Viewer zugreifen, der die Rohprotokolle anzeigt, die diese Integration erfasst.

Konfigurieren Sie eine ServiceNow Systemprotokollabruf-Integration

Konfigurieren Sie eine-n- - Integration für das Streaming von Protokolldaten aus der Systemprotokolltabelle ServiceNow an die KI-Engine Health Log Analytics.

Vorbereitungen

Hinweis: Diese -Integration wird nicht auf einem MID-Serverausgeführt. Im System kann nur ein einzelner ServiceNow Systemprotokollabruf Integration oder eine einzelne Dateneingabe vorhanden sein.

- Stellen Sie sicher, dass die Anwendung Health Log Analytics in Ihrer Instanz installiert und bereitgestellt ist. Weitere Informationen finden Sie unter Health Log Analytics installieren (HLA).
- Stellen Sie sicher, dass eine Serviceinstanz verfügbar ist.
- Stellen Sie sicher, dass die KI-Engine Health Log Analytics aktiv ist und ausgeführt wird.

Aktivieren Sie für Versionen vor Yokohamadiese -Integration, indem Sie die Anweisungen im Artikel How to enable the HLA Glide Syslog data input for Glideversions veraltet als Yokohama [KB1651324] in der Knowledge Base Now Support befolgen.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Geben Sie auf der Registerkarte **Integrationen durchsuchen** im Suchfeld ServiceNow Systemprotokolle ein.
   Die Kachel ServiceNow Integration für Systemprotokolle wird angezeigt.
4. Wählen Sie die Kachel ServiceNow Integration für Systemprotokolle.

   Hinweis: Wenn Sie den Integrationsprozess gestartet haben, ohne alle im Abschnitt Bevor Sie beginnen, zu erfüllen, wird eine Meldung angezeigt. Sie haben die Möglichkeit, die Integration abzubrechen und die fehlenden Anforderungen abzuschließen oder im Entwurfsmodus fortzufahren und sie später zu erfüllen. Beachten Sie, dass Sie eine konfigurierte Integration nur aktivieren können, wenn alle Voraussetzungen erfüllt sind. Gespeicherte Integrationen, die nicht aktiviert wurden, sind auf der Registerkarte **Installierte Integrationen** in Integrations Launchpadunter **Warten auf Ihre Aktion**verfügbar.

5. Wählen Sie die Registerkarte **Details** angeben aus.
   Auf dieser Registerkarte müssen Sie wichtige Details für die neue Integration angeben, einschließlich des Namens und der Serviceinstanz, an die die Daten gebunden werden.
6. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter ServiceNow Konfigurationsfelder für die Integration des Systemprotokollabrufs.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wählen Sie **Weiter**.
   Die **Registerkarte Datenabrufmethode** festlegen wird angezeigt.
8. Wahlweise: Erstellen Sie die Bedingungen für das Filtern von Protokolldaten aus der Systemprotokolltabelle, bevor sie an die KI-Engine HLA gestreamt werden.
9. Wählen Sie **Speichern** aus, um die Konfiguration zu speichern.
10. Wählen Sie **Aktivieren** aus, um die Integration zu aktivieren.
    Die -Integration wird aktiviert. Die Registerkarte **Übersicht** wird angezeigt.

Ergebnisse

Log Daten starten das Streaming von aus der Systemprotokolltabelle ServiceNow an die KI-Engine Health Log Analytics basierend auf den konfigurierten Filtern.

Benutzer mit der Rolle evt_mgmt_user können mit Ereignismanagement die Protokolle überwachen und die Warnungen anzeigen, die Health Log Analytics aus ihnen generiert.

Nächste Maßnahme

Überprüfen Sie den Protokoll-Streaming-Status der Integration auf der Registerkarte **Übersicht**. Weitere Informationen finden Sie unter Streamingstatus und Quellen von Protokolldaten von einern Integrationüberprüfen.

Hinweis: Da die Systemprotokollintegration ServiceNow nicht auf einem MID-Serverausgeführt wird, werden der Streamingstatus MID-Server und die Tabelle **„Protokoll-Streamingquellen“** für diese Integration nicht angezeigt.

Auf der Registerkarte **Übersicht** können Sie direkt zu den Seiten „Dateneingabezuordnung“, „Quelltypstrukturen“ und „Protokollquellen“ mit Kontext aus dieser Integration wechseln, indem Sie das Menüsymbol „Ansicht“ (⋮ “) auswählen und die entsprechende Option auswählen. Über das Menü können Sie auch direkt auf den Protokoll-Viewer zugreifen, der die Rohprotokolle anzeigt, die diese Integration erfasst.

Konfigurieren Sie UDP-Integrationen

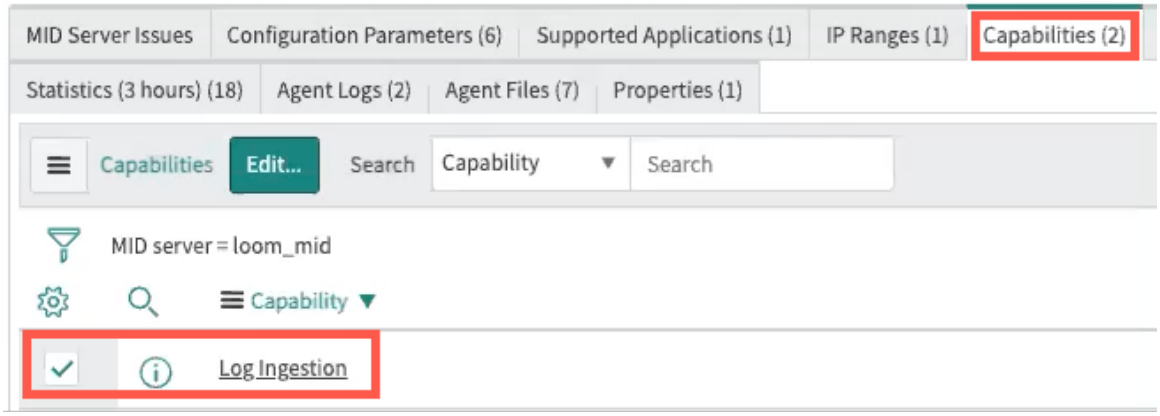
Konfigurieren Sie eine Integration zum Senden von Protokolldaten an Ihre -Instanz ServiceNow direkt über einen UDP-Socket.

Vorbereitungen

- Stellen Sie sicher, dass die Anwendung Health Log Analytics in Ihrer Instanz installiert und bereitgestellt ist. Weitere Informationen finden Sie unter Health Log Analytics installieren (HLA).
- Stellen Sie sicher, dass eine Serviceinstanz verfügbar ist.
- Stellen Sie sicher, dass die KI-Engine Health Log Analytics aktiv ist und ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Geben Sie auf der Registerkarte **Integrationen durchsuchen** im Suchfeld `UDP` ein.
   Die Kachel für die UDP-Integration wird angezeigt.
4. Wählen Sie die Kachel der UDP-Integration aus.

   Hinweis: Wenn Sie den Integrationsprozess gestartet haben, ohne alle im Abschnitt Bevor Sie beginnen, zu erfüllen, wird eine Meldung angezeigt. Sie haben die Möglichkeit, die Integration abzubrechen und die fehlenden Anforderungen abzuschließen oder im Entwurfsmodus fortzufahren und sie später zu erfüllen. Beachten Sie, dass Sie eine konfigurierte Integration nur aktivieren können, wenn alle Voraussetzungen erfüllt sind. Gespeicherte Integrationen, die nicht aktiviert wurden, sind auf der Registerkarte **Installierte Integrationen** in Integrations Launchpadunter **Warten auf Ihre Aktion**verfügbar.

5. Wählen Sie die Registerkarte **Details** angeben aus.
   Das Formular **„Details angeben“** wird angezeigt. In diesem Bildschirm müssen Sie wichtige Details für die neue Integration angeben, einschließlich MID-Server oder des Clusters, aus dem die Protokollnachrichten abgerufen werden, und der Serviceinstanz, an die die Daten gebunden werden.
6. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für die UDP-Integration.
7. Wahlweise: Wählen Sie **Erweitert** aus, um erweiterte Konfigurationsfelder festzulegen.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für die UDP-Integration.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Wählen Sie **Weiter**.
   Der Bildschirm mit den **Setup-Anweisungen** wird angezeigt. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Integration in der Drittanbieterkonsole zu installieren.
9. Wählen Sie **Aktivieren** aus, um die Integration zu aktivieren.
   Die Integration ist aktiviert. Die Registerkarte **Übersicht** wird angezeigt.

Ergebnisse

Protokolldaten werden direkt über einen UDP-Socket an Ihre Instanz ServiceNow gestreamt. Die Kachel für die Integration ist auf der Registerkarte **Installierte Integrationen** in Integrations Launchpadverfügbar.

Benutzer mit der Rolle evt_mgmt_user können mit Ereignismanagement die Protokolle überwachen und die Warnungen anzeigen, die Health Log Analytics aus ihnen generiert.

Nächste Maßnahme

Überprüfen Sie den Status des Protokolldaten-Streamings und die Quellen der Integration auf der Registerkarte **Übersicht**. Nutzen Sie die angezeigten Informationen, um zu verfeinern, wie HLA die Protokolldaten liest, indem Sie Ihre Integrationskonfiguration anpassen. Weitere Informationen finden Sie unter Streamingstatus und Quellen von Protokolldaten von einern Integrationüberprüfen.

Hinweis: Auf der Registerkarte **Übersicht** können Sie direkt zu den Seiten „Dateneingabezuordnung“, „Quelltypstrukturen“ und „Protokollquellen“ mit Kontext aus dieser Integration wechseln, indem Sie das Menüsymbol „Ansicht“ (⋮ “) auswählen und die entsprechende Option auswählen. Über das Menü können Sie auch direkt auf den Protokoll-Viewer zugreifen, der die Rohprotokolle anzeigt, die diese Integration erfasst.

Konfigurieren Sie TCP-Integrationen [.

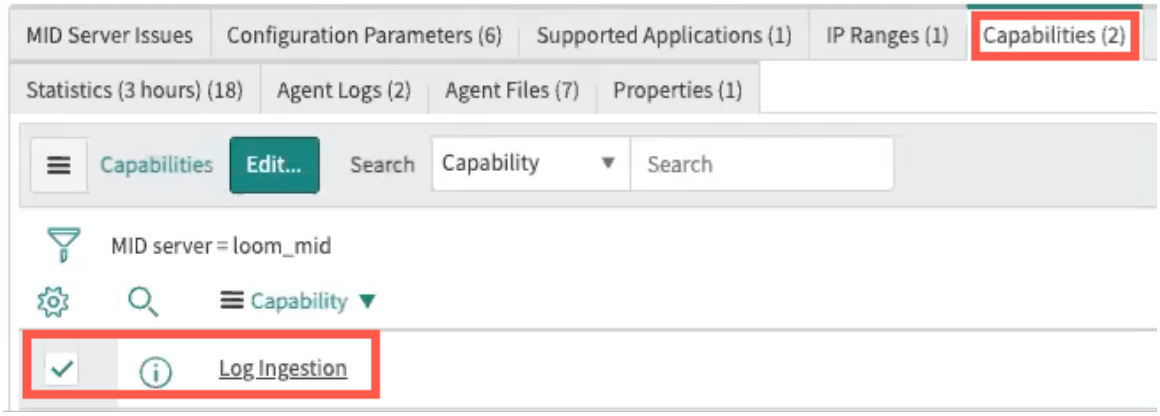
Konfigurieren Sie eine-n- - Integration zum Senden von Protokolldaten an Ihre Instanz ServiceNow direkt über einen TCP/SSL-Socket.

Vorbereitungen

- Stellen Sie sicher, dass die Anwendung Health Log Analytics in Ihrer Instanz installiert und bereitgestellt ist. Weitere Informationen finden Sie unter Health Log Analytics installieren (HLA).
- Stellen Sie sicher, dass eine Serviceinstanz verfügbar ist.
- Stellen Sie sicher, dass die KI-Engine Health Log Analytics aktiv ist und ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass ein MID-Server mit aktivierter Protokollerfassungsfunktion installiert und konfiguriert ist.



Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

- Wenn die IP-Adresse MID-Server durch Network Address Translation (NAT), ein Lastenausgleichsmodul oder ein ähnliches Gerät verfügbar gemacht wird, muss sie über eine öffentliche IP-Adresse verfügen. Fügen Sie in den Eigenschaften des MID-Server eine Eigenschaft mit dem Namen *mid.public_ip* mit der öffentlichen IP-Adresse als Wert hinzu. Weitere Informationen finden Sie unter MID Server-Eigenschaften erstellen .
- Weitere Informationen zur Übermittlung von Protokollen mit SSL TLS-Verschlüsselung finden Sie im Artikel Streaming Data With Rsyslog & Filebeat Using SSL [KB0866319] (Daten mit Rsyslog & Filebeat über SSL streamen) in der Knowledge Base des Now Support.

Hinweis: Informationen zum Streamen von Daten von Logstash an Ihre -Instanz finden Sie im Artikel Streamingdaten von Logstash an Ihre HLA-Instanz [KB0994735] in der Knowledge Base Now Support.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Geben Sie auf der Registerkarte **Integrationen** durchsuchen im Suchfeld `TCP` ein. Die Kachel für die TCP-Integration wird angezeigt.
4. Wählen Sie die Kachel TCP integration (TCP-Integration) aus.

   Hinweis: Wenn Sie den Integrationsprozess gestartet haben, ohne alle im Abschnitt Bevor Sie beginnen, zu erfüllen, wird eine Meldung angezeigt. Sie haben die Möglichkeit, die Integration abzubrechen und die fehlenden Anforderungen abzuschließen oder im Entwurfsmodus fortzufahren und sie später zu erfüllen. Beachten Sie, dass Sie eine konfigurierte Integration nur aktivieren können, wenn alle Voraussetzungen erfüllt sind. Gespeicherte Integrationen, die nicht aktiviert wurden, sind auf der Registerkarte **Installierte Integrationen** in Integrations Launchpadunter **Warten auf Ihre Aktion**verfügbar.

5. Wählen Sie die Registerkarte **Details** angeben aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Formular **„Details angeben“** wird angezeigt. In diesem Bildschirm müssen Sie wichtige Details für die neue Integration angeben, einschließlich MID-Server oder des Clusters, aus dem die Protokollnachrichten abgerufen werden, und der Serviceinstanz, an die die Daten gebunden werden.

6. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Konfigurationsfelder für TCP-Integration.
7. Wählen Sie **Weiter**.
   Der Bildschirm mit den **Setup-Anweisungen** wird angezeigt. Befolgen Sie die Anweisungen auf dem Bildschirm, um die Integration in der Drittanbieterkonsole zu installieren.
8. Wählen Sie **Aktivieren** aus, um die Integration zu aktivieren.
   Die -Integration wird aktiviert. Die Registerkarte **Übersicht** wird angezeigt.

Ergebnisse

Log Daten starten das Streaming von an Ihre Instanz ServiceNow direkt über einen TCP/SSL-Socket. Die Kachel für die -Integration ist auf der Registerkarte **Installierte Integrationen** in Integrations Launchpadverfügbar.

Benutzer mit der Rolle evt_mgmt_user können mit Ereignismanagement die Protokolle überwachen und die Warnungen anzeigen, die Health Log Analytics aus ihnen generiert.

Nächste Maßnahme

Überprüfen Sie den Status des Protokolldaten-Streamings und die Quellen von der Integration auf der Registerkarte **Übersicht**. Nutzen Sie die angezeigten Informationen, um zu verfeinern, wie HLA die Protokolldaten liest, indem Sie die Konfiguration der Integration anpassen. Weitere Informationen finden Sie unter Streamingstatus und Quellen von Protokolldaten von einern Integrationüberprüfen.

Hinweis: Auf der Registerkarte **Übersicht** können Sie direkt zu den Seiten „Dateneingabezuordnung“, „Quelltypstrukturen“ und „Protokollquellen“ mit Kontext aus dieser Integration wechseln, indem Sie das Menüsymbol „Ansicht“ (⋮ “) auswählen und die entsprechende Option auswählen. Über das Menü können Sie auch direkt auf den Protokoll-Viewer zugreifen, der die Rohprotokolle anzeigt, die diese Integration erfasst.

Streamingstatus und Quellen von Protokolldaten von einern Integrationüberprüfen

Überprüfen Sie den Status des Protokolldaten-Streamings und die Quellen von einer aktiven -Integration für Health Log Analytics auf der Registerkarte Übersicht der -Integration. Auf dieser Registerkarte können Sie Streaming-Probleme untersuchen und die Konfiguration der -Integrationverfeinern. Sie können auch direkt von der Registerkarte Übersicht zu den Seiten „Dateneingabezuordnung“, „Quelltypstrukturen“ und „Protokollquellen“ sowie zum Protokoll-Viewer wechseln, mit Kontext aus der Integration.

Vorbereitungen

Bestätigen Sie, dass die -Integration auf Integrations Launchpadaktiviert wurde.Weitere Informationen finden Sie unter Integrationen über Integrations Launchpadeinrichten.

Erforderliche Rolle: evt_mgmt_admin

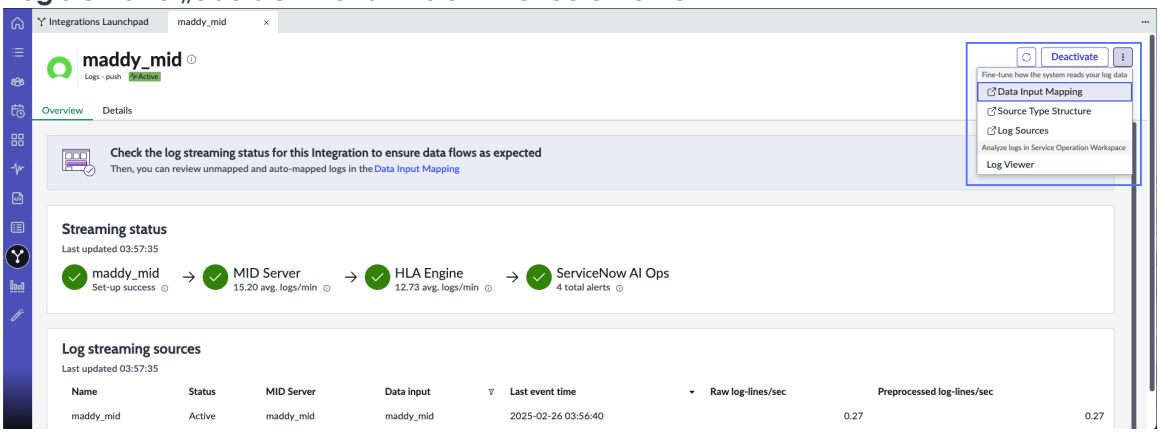
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Suchen Sie auf der Registerkarte **Installierte Integrationen** nach einer aktiven Integration, und öffnen Sie sie.

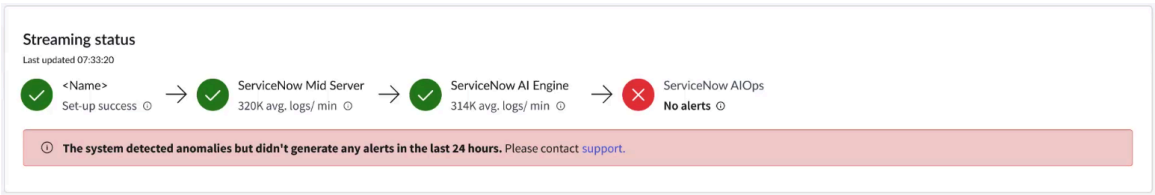
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Registerkarte **Übersicht** wird angezeigt.

Registerkarte „Übersicht“ und Ansicht Menüelemente



Der **Streaming-Status** zeigt die Daten-Streaming-Statistiken der -Integrationzwischen der Protokollquelle und MID-Serversowie MID-Server und der KI-Engine an. Außerdem wird die Gesamtzahl der Warnungen angezeigt, die die KI-Engine in der Tabelle ServiceNow AIOps erstellt hat. Diese Statistiken werden aktualisiert, wenn die Registerkarte **„Übersicht“** geladen wird. Bei einem Streaming-Problem wird eine Fehlermeldung angezeigt. Wenn das Daten-Streaming fehlschlägt, wird die Integration automatisch deaktiviert, und der **Streaming-Status** gibt an, wo der Fehler aufgetreten ist. In einem Banner werden der Fehler und die auszuführenden Schritte erläutert.



Hinweis: Die Integration des ServiceNow -Systemprotokollabrufs wird nicht unter MID-Serverausgeführt. Daher zeigt die Registerkarte **„Übersicht“** für diese Integration den Streaming-Status MID-Server nicht an.

Die Tabelle **„Protokoll-Streaming-Quellen“** zeigt die folgenden Informationen zu den Protokolldatenquellen der -Integrationan.

Protokoll-Streamingquellen

Spalte	Beschreibung
Name	Der Name der Protokolldatenquelle.
Status	Der Streaming-Status: Aktiv oder nicht aktiv.
MID-Server	MID-Server, an den die Protokolldaten gestreamt werden.
Dateneingabe	Die -Integration, die Daten an Ihre -Instanz ServiceNow streamt.
Letztes Ereignis : -Zeit	Datum und Uhrzeit, zu der die Integration das Ereignis latest empfangen hat.
Raw log lines/sec (Protokollzeilen im Rohzutand/Sek.)	Die durchschnittliche Anzahl der Protokollzeilen im Rohzutand, die im letzten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	Ein-Minuten-Intervall pro Sekunde an den MID-Server gestreamt wurden. **Hinweis:** Dieser Wert stellt die Anzahl der Rohprotokollzeilen vor der Vorverarbeitung dar.
Vorverarbeitete Protokollzeilen/Sek	Die durchschnittliche Anzahl vorverarbeiteter Protokollzeilen, die im letzten Minutenintervall pro Sekunde an MID-Server gestreamt wurden. **Hinweis:** Dieser Wert kann sich von der Anzahl der Protokollzeilen im Rohzutand pro Sekunde unterscheiden. Beispielsweise kann der Unterschied darauf zurückzuführen sein, dass während der Vorverarbeitung Protokolle verworfen wurden.

Hinweis: Diese Tabelle ist nicht für die ServiceNow Integration zum Abrufen von Systemprotokollen verfügbar.

4. Untersuchen Sie Probleme beim Daten-Streaming.
5. Wahlweise: Passen Sie die Konfiguration der Integration an, , falls erforderlich. Navigieren Sie zu relevanten Tabellen oder dem Protokoll-Viewer über das Menü Ansicht ( ).

Hinweis: Der Inhalt des Menüs Ansicht ändert sich dynamisch, je nachdem, ob die referenzierten Tabellen Daten enthalten.

Menüoptionen des Menüs anzeigen

Option	Beschreibung
Dateneingabezuordnung	Diese Option öffnet die Seite **„Dateneingabezuordnung“**. Auf dieser Seite können Sie Quellen manuell zuordnen, wenn HLA Eigenschaften nicht automatisch erkannt hat. Weitere Informationen finden Sie unter Protokolldaten im Rohzustand zuordnen.
Quelltypstruktur	Diese Option öffnet die Seite **„Quelltypstruktur“**. In der Quelltypstruktur werden Protokolldaten basierend auf ihrer Herkunft oder ihrem Typ klassifiziert und organisiert. Sie können die Struktur anpassen und verifizieren, dass die KI-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Engine HLA Eigenschaften ordnungsgemäß extrahiert und korrekt klassifiziert. Weitere Informationen finden Sie unter Quelltypstruktur anpassen.
Protokollquellen	Diese Option öffnet die Tabelle **„Protokollquellen“**. Mit dieser Tabelle können Sie überprüfen, ob HLA alle Ihre Protokollquellen erstellt hat. Wenn eine Protokollquelle fehlt, können Sie sie manuell hinzufügen. Weitere Informationen finden Sie unter Protokollquellen überprüfen.
Protokoll-Viewer	Diese Option öffnet den **Protokoll-Viewer**, der die Häufigkeit von Anomalien in den Protokolldaten während eines bestimmten Zeitraums anzeigt. Weitere Informationen finden Sie unter Protokolle für Warnung werden in der Protokollanzeige überprüft.

6. Wenn Sie Streaming-Probleme gelöst und die Konfiguration korrigiert haben, testen und speichern Sie die Integration, und aktivieren Sie sie dann erneut.

   Weitere Informationen finden Sie in der Dokumentation zum Konfigurieren einzelner Integrationen.

Bearbeiten Sie installierte Integrationen

Bearbeiten Sie eine installierte Integration für das Streaming von Protokolldaten an Health Log Analytics im Integrations Launchpad. Sie können beispielsweise zu einer anderen Serviceinstanz wechseln.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Suchen Sie auf der Registerkarte **Installierte Integrationen** nach der Kachel für die Integration, die Sie bearbeiten möchten, und wählen Sie sie aus.
4. Wählen Sie eine Registerkarte aus, die Sie bearbeiten möchten.
5. Wählen Sie **Deaktivieren**, um die Integration zu deaktivieren.

   Hinweis: Sie müssen die Integration deaktivieren, bevor Sie sie bearbeiten können.

6. Wählen Sie **Bearbeiten**.
7. Bearbeiten Sie die Integration gemäß Ihren Anforderungen.
8. Wählen Sie **Testen und speichern**aus.
   Health Log Analytics testet die MID-Server -Konnektivität und gibt entweder eine erfolgreiche Ausführung oder einen Fehler zurück. Wenn ein Fehler zurückgegeben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird, nehmen Sie Anpassungen an Ihrer Konfiguration vor, wie auf dem Bildschirm vorgeschlagen, und wählen Sie dann erneut **Testen und speichern** aus. Wenn der Test erfolgreich ist, können Sie die Integration erneut aktivieren.

9. Wählen Sie **Aktivieren**.

Protokolldaten-Integrationen deaktivieren

Deaktivieren Sie eine Integration für das Streaming von Protokolldaten an Health Log Analytics auf der Seite Integrations Launchpad.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Suchen Sie auf der Registerkarte **Installierte Integrationen** nach der Integrationskachel für die Integration, die Sie deaktivieren möchten, und wählen Sie sie aus.
4. Wählen Sie auf der Registerkarte **Übersichtdie Option Deaktivieren**aus.

Ergebnisse
Die -Integration ist deaktiviert und das Streaming von Protokolldaten an Ihre Instanz ServiceNow beendet sich. Die deaktivierte Integration ist weiterhin unter Integrations Launchpad auf der Registerkarte **Installierte Integrationen** unter **Warten auf Ihre Aktion**verfügbar.

Probleme beim Protokoll-Streaming identifizieren und beheben

Identifizieren und beheben Sie Probleme beim Protokoll-Streaming, um sicherzustellen, dass die Dateneingaben, die Sie für Health Log Analytics konfiguriert haben, Daten ordnungsgemäß an Ihre Instanz ServiceNow von streamen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Streamingquellen**.
   Auf der Seite „Streaming-Quellen“ werden alle Dateneingaben und MID Servers angezeigt, die Protokolle von ihnen empfangen.

Hinweis:

- Wenn in der Konfiguration der erweiterten Dateneingabe die Option **Look up hostnames** (Nach Hostnamen suchen) ausgewählt ist, wird auf der Seite „Streaming Sources“ (Streaming-Quellen) der Hostname von Geräten angezeigt, die einen Rsyslog- oder Filebeat-Absender verwenden. Für Elasticsearch -Indizes wird der Indexname angezeigt.
- „Streaming Sources“ (Streaming-Quellen) ist auch als zugehörige Liste im Dateneingabeformular verfügbar. In der zugehörigen Liste werden nur die Endpunktgeräte angezeigt, die für diese Dateneingabe relevant sind.
- Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Seite „Streaming-Quellen“ eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie einen Dateneingabedatensatz aus, um die Streaming-Daten seiner Quellen anzuzeigen und Streaming-Probleme und ihre mögliche Ursache zu identifizieren. Wenn beispielsweise die letzte aufgezeichnete Event-Zeit für den Endpunktserver einer Dateneingabe gestern war, ist dieser Server möglicherweise ausgefallen oder falsch konfiguriert. Ein Streaming-Problem kann auch dadurch verursacht werden, dass die Dateneingabe-Konfigurationsdatei nicht auf dem Endpunkt installiert ist.

Filter	Beschreibung
Status	Status der Quelle. Ein rotes Aufzählungszeichen zeigt an, dass diese Quelle in der letzten Stunde keine Daten gestreamt hat.
Last event time (Zeit des letzten Events)	Die letzte aufgezeichnete Zeit, zu der auf dem MID-Server ein Event im letzten Ein-Minuten-Intervall eingetroffen ist. Health Log Analytics aktualisiert kontinuierlich die Zeit des letzten Events. Wenn die Zeit des letzten Events nicht aktuell ist, werden keine Daten gestreamt.
Raw log lines/sec (Protokollzeilen im Rohzutand/Sek.)	Die durchschnittliche Anzahl der Protokollzeilen im Rohzutand, die im letzten Ein-Minuten-Intervall pro Sekunde an den MID-Server gestreamt wurden. **Hinweis:** Dieser Wert stellt die Anzahl der Protokollzeilen im Rohzutand vor der Vorverarbeitung dar.
Preprocessed log lines/sec (Vorverarbeitete Protokollzeilen/Sek.)	Die durchschnittliche Anzahl der vorbearbeiteten Protokollzeilen, die im letzten Ein-Minuten-Intervall pro Sekunde an MID-Server gestreamt wurden. **Hinweis:** Dieser Wert kann sich von der Anzahl der Protokollzeilen im Rohzutand pro Sekunde unterscheiden. Beispielsweise kann der Unterschied darauf zurückzuführen sein, dass Protokolle während der Vorverarbeitung gelöscht wurden.

3. Untersuchen und lösen Sie alle Probleme beim Datenstreaming.

Hinweis: Wenn Sie Probleme mit Berechtigungen beim Streaming von Protokolldaten von Elasticsearch haben, lesen Sie den Artikel Granting privileges for data streams from Elasticsearch [KB0967366] (Berechtigungen für Datenströme von Elasticsearch erteilen) in der Now Support-Knowledge Base.

Nächste Maßnahme

Wenn die Protokolle ordnungsgemäß gestreamt werden, fahren Sie mit der Zuordnung Ihrer Protokolldaten im Rohzustand fort.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie können eingehende Protokolldaten im Rohzustand bearbeiten, bevor Health Log Analytics sie verarbeitet. Mit der Vorverarbeitung können Sie beispielsweise Protokollteile verwerfen oder vertrauliche Daten aus Ihren Protokollen entfernen. Diese Aufgabe ist optional.

Protokolldaten im Rohzustand vor der Verarbeitung bearbeiten

Sie können Rohprotokolldaten ändern und Protokollnachrichten löschen oder aufteilen, bevor sie auf dem MID-Server verarbeitet werden, sprich: daher bevor Health Log Analytics sie zuordnet und strukturiert. Sie können beispielsweise verhindern, dass sensible Daten das System erreichen, indem Sie Benutzernamen und Passwörter durch ein Sternchen (*) ersetzen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingabe-Präprozessor**.
2. Öffnen Sie einen Datensatz.

   Hinweis: Wenn das Vorverarbeitungsformular zum ersten Mal angezeigt wird, ruft Health Log Analytics automatisch Protokollbeispiele ab. Rufen Sie in den folgenden Sitzungen neue Beispiele manuell ab, indem Sie **Beispiele neu laden**wählen.

3. Wahlweise: Verhindern Sie, dass Protokollbeispiele angezeigt werden, die aus den Protokolldaten im Rohzustand Ihrer Organisation stammen, indem Sie **Disable raw log samples** (Rohprotokollbeispiele deaktivieren) auswählen.
   Wählen Sie diese Option aus, wenn Sie Ihre Protokolle nicht für Health Log Analytics verfügbar machen möchten.
4. Wahlweise: Schauen Sie sich an, wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
   a. Fügen Sie im Feld **Test manual sample** (Manuelles Beispiel testen) eine Beispielnachricht hinzu.
   b. Wählen Sie **Start**.
   c. Beachten Sie, wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
5. Wählen Sie im Feld **Unformatierte Eingabebeispiele** ein Protokollbeispiel aus, das die Auswirkungen Ihrer neuen JavaScript-Funktion auf Protokollzeilen veranschaulicht, wenn Sie sie testen.
6. Definieren Sie eine JavaScript-Funktion, die Ihre Protokolldaten im Rohzustand ändert, bevor Health Log Analytics sie zuordnet und strukturiert.

   Hinweis:

   (Ausschließlich ACC-Dateneingaben) Wenn Agent Client Collector zu einem anderen MID-Server wechselt, um Failover-Schutz bereitzustellen, muss zu einer anderen ACC-Dateneingabe gewechselt werden. Daher müssen alle ACC-Dateneingaben dieselbe JavaScript-Funktion aufweisen. Von Health Log Analytics wird die neueste veröffentlichte JavaScript-Funktion für alle vorhandenen und zukünftigen ACC-Dateneingaben bereitgestellt. Das vorherige Skript wird dabei ersetzt. Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, verfügbar im ServiceNow Store. Informationen zum Failover-Schutz in Agent Client Collector Log Analytics (ACC-L) finden Sie unter Agent Client Collector Log Analytics.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Ändern Sie in der JavaScript-Konsole entweder die bereitgestellte JavaScript-Standardfunktion, ändern Sie eine vorhandene benutzerdefinierte JavaScript-Funktion, oder definieren Sie eine neue.

Hinweis: Zusätzlich zur JavaScript-Standardfunktion für die Datenvorverarbeitung bietet Health Log Analytics eine JavaScript-Funktionsvorlage mit dem Namen *Scrubbing*. Diese JavaScript-Funktion entfernt personenbezogene Daten wie E-Mail-Adressen, Sozialversicherungsnummern und Passwörter aus den Rohprotokolldaten. Die Vorlage kann als Ausgangspunkt für Ihren benutzerdefinierten Skriptcode dienen. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

Hinweis: (Nur ACC-Dateneingaben) Stellen Sie sicher, dass Ihre JavaScript-Funktion zur Verarbeitung von Daten verwendet werden kann, die von allen ACC-Dateneingaben gestreamt werden.

Die JavaScript-Funktionen zur Vorverarbeitung von Rohprotokolldaten verwenden die folgenden Objekte:

- Signatur: Funktionsprozess (Beispiel, Metadaten)

Objekt	Beschreibung
Beispiel	Das aktuelle Protokollbeispiel
Metadaten	Objekt, das den Event-Stream enthält. Um auf den Event-Stream zuzugreifen, rufen Sie die Funktion `metadata.eventStream` auf. Da der Event-Stream ein Objekt ist, können Sie auf jede seiner Eigenschaften zugreifen, indem Sie die Funktionen `metadata.eventStream.origin` oder `metadata.eventStream.LocalPort` aufrufen. Die Liste der verfügbaren Event-Stream-Eigenschaften ist auf der Registerkarte **Event Stream: access via metadata** (Event-Stream: Zugriff über Metadaten) verfügbar.

- Typ und Struktur der Rückgabe

Hinweis: Die JavaScript-Funktion gibt eine Zuordnung mit zwei Einträgen zurück. Ändern Sie diese Rückgabestruktur nicht.

Objekt	Beschreibung
modifiedInput	Die aktuelle Protokollnachricht, nachdem die JavaScript-Funktion die ursprüngliche Nachricht geändert hat. Falls dies Null ist,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Objekt	Beschreibung
	wird die ursprüngliche Protokollnachricht verwendet.
splitEvents	Array der Protokollnachrichten, nachdem die JavaScript-Funktion die ursprüngliche Nachricht aufgebrochen hat.

- Um eine Protokollnachricht zu verwerfen, rufen Sie `return drop ()` auf.

b. Testen Sie die JavaScript-Funktion, indem Sie **Test** wählen und das Ergebnis in Ihrem Protokollbeispiel in zugehörigen Listen anzeigen.

Registerkarte	Beschreibung
Ergebnis	Ergebnis der Ausführung der JavaScript-Funktion für Ihr Protokollbeispiel
Event-Stream: Zugriff über Metadaten	Schlüssel-Wert-Paare, die die Event Stream-Metadaten darstellen
Failures (Fehler)	Protokollbeispiele, in denen die JavaScript-Funktion nicht erfolgreich ausgeführt werden konnte

Hinweis: Wenn sich Ihre neue JavaScript-Funktion nicht wie erwartet verhält, können Sie zur zuletzt veröffentlichten Funktion zurückkehren, indem Sie auf den zugehörigen Link **JS-Funktion zurücksetzen** klicken.

c. Wahlweise: Nehmen Sie alle erforderlichen Anpassungen vor, und testen Sie die JavaScript-Funktion erneut.

7. Klicken Sie auf **Save template** (Vorlage speichern), um die JavaScript-Funktion zu speichern.
Sie können die JavaScript-Funktion entweder als neue Vorlage speichern oder die aktuell ausgewählte Vorlage überschreiben.

- Um die JavaScript-Funktion als neue Vorlage zu speichern, geben Sie einen neuen Namen in das Feld **Template name** (Vorlagenname) ein.
- Um die aktuell im Feld **JS function templates** (JS-Funktionsvorlagen) ausgewählte Vorlage zu überschreiben, lassen Sie das Feld **Template name** (Vorlagenname) leer.

8. Klicken Sie auf **Publish** (Veröffentlichen), um die JavaScript-Funktion in der Datenbank zu speichern.

Ergebnisse

Wenn die JavaScript-Funktion veröffentlicht wird, verwendet Health Log Analytics sie, um Ihre Protokolldaten im Rohzustand vorzuverarbeiten, bevor sie zugeordnet und strukturiert werden.

Das neue Skript wird automatisch der Liste der JS-Funktionsvorlagen hinzugefügt, aus denen Sie auswählen können. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Nur ACC-Dateneingaben) Health Log Analytics bietet die veröffentlichte JavaScript-Funktion für alle vorhandenen und zukünftigen ACC-Dateneingaben. Die neue JavaScript-Funktion ersetzt das vorherige Skript.

Nächste Maßnahme

Fahren Sie mit der Seite **Data Input Mapping** (Dateneingabezuordnung) fort, indem Sie auf den zugehörigen Link **Go to Mapping** (Zu Zuordnung wechseln) klicken. Ordnen Sie Rohdaten zu, die in Ihre Instanz gestreamt werden, um festzustellen, wie sie durch Health Log Analytics verarbeitet werden.

Automatische Zuordnung und Zuordnung von Protokolldaten

Standardmäßig versucht die KI-Engine von Health Log Analytics, jede eingehende Protokollzeile automatisch den richtigen Tags zuzuordnen. Sie können die Ergebnisse der automatischen Zuordnung manuell ändern, indem Sie eine JavaScript-Funktion definieren.

Automatische Zuordnung eingehender Protokollzeilen

Health Log Analytics Bei der automatischen Zuordnung werden Protokollbeispiele und Metadaten drei Tags zugewiesen: Serviceinstanz, Komponente und Quelltyp. Die Zuweisung der Serviceinstanz basiert auf der Serviceinstanz, die im Setup der Dateneingabe angegeben ist. Die verbleibenden Tags werden automatisch zugewiesen.

In der folgenden Beispielprotokollzeile verwendet Health Log Analytics beispielsweise das Feld „source“, um die Komponente und den Quelltyp zu finden.

```
{"beat":{"version":"6.8","name":"abc3.prd.acme.com","hostname":"abc3.prd.
acme.com"},"@timestamp":"2020-08-27T10:12:24.792Z","prospector":{"type":"
log"},"message":"**** User null is requesting the following
 page http://www.acme.com PROPS:{"subcategory1":"home
 pages","httpStatus":"200","loginLevel":"Anonymous","userAgent":"Mozilla5
.0",
 ("pageUrl":\"http://www.acme.com","host":"abc3.prd.acme.com","@version":
"1","source":"/opt/oracle/weblogic/abc/online_store3/logs/online_store3.o
ut","offset":3951550786}
```

Im Beispiel extrahiert Health Log Analytics die Zeichenfolge „online_store“. Es analysiert die folgenden Felder, wenn sie in der Protokollzeile vorhanden sind: source, path, channel, namespace_name, name, pod_name, source_name und aws_lambda_name. Wenn Daten über Syslog gesendet werden, wird auch das syslog-Tag analysiert.

Extraktion nicht benötigter Daten stoppen

Wenn eine extrahierte Zeichenfolge nicht aussagekräftig genug ist oder redundanten Text oder Informationen enthält, können Sie die Extraktion von verzichtbaren Daten dieser Art stoppen. Weitere Informationen finden Sie unter Extraktion nicht benötigter Protokolldaten stoppen.

Extraktion bestimmter Daten sicherstellen

Sie können sicherstellen, dass Health Log Analytics bestimmte gewünschte Begriffe extrahiert. Weitere Informationen finden Sie unter Extraktion bestimmter Protokolldaten sicherstellen.

Dateneingabequellen zuordnen

Sie können die Ergebnisse der automatischen Zuordnung manuell ändern, indem Sie eine JavaScript-Funktion definieren. Mitder Dateneingabezuordnung können Sie Ihre Protokolldaten nach Serviceinstanz und Verfügbarkeitszone organisieren. Eine einzelne Serviceinstanz kann mehrere Komponenten enthalten, und eine Komponente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

kann Protokolle von vielen verschiedenen Quelltypen empfangen. Ein Serviceinstanz-Komponenten-Paar ist jedoch eindeutig. Quelltypen basieren auf einer bestimmten Protokollstruktur und einem bestimmten Format. Serviceinstanzen und -komponenten sind breiter definiert und werden daher hauptsächlich für die logische Zuordnung verwendet.

Durch Aktivieren **des Testmodus** wird vermieden, dass der Speicher Elasticsearch durch Beispieldaten überlastet wird, die nur zur Perfektionierung der Protokolldatenzuordnung verwendet werden. Wenn sich die Dateneingabe im Testmodus befindet, erstellt Health Log Analytics nicht die Quelltypen, Quellen oder andere Objekte, die im Standard-Flow erstellt werden. Die gestreamten Daten werden in dedizierten temporären Elasticsearch Indizes gespeichert, die als Komponenten in der Protokollanzeige angezeigt werden. Wenn Sie das Skript veröffentlichen und den Testmodus beenden, werden diese temporären Indizes gelöscht, um den Speicherplatzverbrauch zu minimieren.

Wenn Sie eine JavaScript-Funktion definieren, wählen Sie **„Testen“,** um das Ergebnis des Skripts so anzuzeigen, wie es derzeit angegeben ist. Mit dieser Funktionalität können Sie eine Vorschau der erstellten Quelltypen und Quellen anzeigen. Anschließend können Sie das Skript verfeinern, bis das gewünschte Ergebnis erreicht ist. Beispielsweise kann es nützlich sein, die Testergebnisse mehrerer Versionen der JavaScript-Funktion zu vergleichen.

Hinweis: Standardmäßig verarbeitet der Test 100 Protokolldatenmuster. Sie können diese Anzahl in den Systemeigenschaften anpassen. Weitere Informationen finden Sie unter Globale Health Log Analytics-Systemeigenschaften konfigurieren.

Während des Setups der Dateneingabe erstellt das System unter Umständen eine zu hohe Gesamtzahl von Dateneingabequellen. Dies kann beispielsweise auf ein fehlerhaftes Zuordnungsskript zurückzuführen sein. In den Systemeigenschaften können Sie Grenzwerte für die Anzahl der pro Dateneingabe erstellten Quellen konfigurieren:

Systemeigenschaft	Beschreibung	Standard
log_source.sources_warning_limit	Warngrenze für die Anzahl der pro Dateneingabe erstellten Quellen.	500
log_source.sources_critical_limit	Kritische Grenze für die Anzahl der pro Dateneingabe erstellten Quellen.	600

Die Anzahl der Protokollquellen, die eine bestimmte Dateneingabe erstellt hat, wird im Feld **Quellenanzahl** für diese Dateneingabe angezeigt. Wenn die Gesamtanzahl der während der Dateneingabekonfiguration erstellten Quellen die Warngrenze erreicht, sendet das System eine Warnbenachrichtigung per E-Mail. Außerdem wird eine Nachricht auf den Seiten **Dateneingabezuordnung**, **Protokollquellen** und **Dateneingabe** angezeigt. Die Benachrichtigung und die Nachricht enthalten die Gesamtzahl der bisher erstellten Quellen und die drei Dateneingaben, die die meisten Quellen zu dieser Gesamtzahl beigetragen haben. Wenn keine Aktion ausgeführt wird, erstellt das System weiterhin Quellen, bis die Gesamtzahl die kritische Grenze erreicht. In diesem Fall werden das Setup der Dateneingabe und das Streaming aus allen Dateneingaben automatisch beendet. Sie können Dateneingaben nicht manuell erneut starten, bis das Problem gelöst wurde. Um diesen Status zu beheben, folgen Sie den Anweisungen im Artikel How to handle too many sources in data inputs [KB0963067] (Umgang mit zu vielen Quellen in Dateneingaben) in der Knowledge Base des Now Support.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokolldaten binden

Durch das Binden von Protokolldaten an Konfigurationselemente (CIs) in Configuration Management Database (CMDB) können Sie die CMDB nach Endpunkten durchsuchen, die einem Protokoll entsprechen. Wenn Sie eine Dateneingabe konfigurieren, binden Sie Protokolleinträge an eine Serviceinstanz, die an ein CI in der CMDB gebunden ist. Durch die Bindung von Protokolleinträgen, Serviceinstanzen und CIs kann die KI-Engine Health Log Analytics sie zur Verwendung in der Ursachenanalyse (RCA) korrelieren. Weitere Informationen finden Sie unter Konfigurieren Sie Rsyslog- , Filebeat- oder Winlogbeat-Dateneingaben oder Elasticsearch-Dateneingaben konfigurieren.

Protokolldaten im Rohzustand zuordnen

Die Zuordnung von Protokolldaten im Rohzustand, die in Ihre Instanz gestreamt werden, bestimmt, wie die Daten behandelt werden. Health Log Analytics strukturiert Protokolle automatisch, erstellt Metriken zur Erkennung von Anomalien und zeigt Warnungen abhängig vom Tagging Ihrer Daten an.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig versucht Health Log Analytics, jede eingehende Protokollzeile automatisch den richtigen Tags zuzuordnen. Wenn Eigenschaften nicht automatisch erkannt werden, ordnen Sie die Dateneingabequellen manuell zu, indem Sie eine JavaScript-Funktion definieren.

In der JavaScript-Funktion müssen Sie nur die Serviceinstanz (hier als Anwendungsservicebezeichnet)zuordnen. Die Zuordnung der Komponente und des Quelltyps ist optional: Health Log Analytics versucht, ihre Werte automatisch aus den Protokolldaten zu extrahieren. Wenn der Versuch fehlschlägt, werden die Standardwerte zugewiesen. Wenn Sie die Komponente zuordnen, aber nicht den Quelltyp oder umgekehrt, versucht das System, den fehlenden Wert aus den Protokolldaten zu extrahieren. Wenn dies fehlschlägt, wird der Komponentenwert dem Quelltyp zugewiesen (oder umgekehrt, je nachdem, welchen Sie zugeordnet haben). Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

Hinweis:

(Nur ACC-Dateneingaben) Wenn Agent Client Collector zu einem anderen MID-Server wechselt, um Failover-Schutz zu bieten, muss er zu einer anderen ACC-Dateneingabe wechseln. Daher müssen alle ACC-Dateneingaben dieselbe JavaScript-Funktion aufweisen. Von Health Log Analytics wird die neueste veröffentlichte JavaScript-Funktion für alle vorhandenen und zukünftigen ACC-Dateneingaben bereitgestellt. Das vorherige Skript wird dabei ersetzt. Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, verfügbar im ServiceNow Store . Informationen zum Failover-Schutz in Agent Client Collector Log Analytics (ACC-L) finden Sie unter Agent Client Collector Log Analytics.

Hinweis: Sie können Protokolldaten im Rohzustand ändern, bevor Health Log Analytics sie zuordnet und strukturiert. Weitere Informationen finden Sie unter Protokolldaten im Rohzustand vor der Verarbeitung bearbeiten.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Zuordnung** > **Dateneingabezuordnung**.
2. Öffnen Sie einen Datensatz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn das Formular „Dateneingabezuordnung“ angezeigt wird, ruft Health Log Analytics automatisch Protokollbeispiele ab. Rufen Sie in nachfolgenden Sitzungen neue Beispiele ab, indem Sie **Refresh Samples** (Beispiele aktualisieren) auswählen.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Seite „Dateneingabezuordnung“ eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

3. Wahlweise: Um die vollständige Protokollnachricht im Rohzustand weiterzuleiten, deaktivieren Sie die automatische Erkennung der Headereigenschaften für diese Dateneingabe, indem Sie **Disable header detection** (Headererkennung deaktivieren) auswählen.
   Weitere Informationen finden Sie unter Erkennung von Headereigenschaften.
4. Wahlweise: Aktivieren Sie den Testmodus, indem Sie für den **Testmodus** -Wert auf EIN setzen.
   Im Testmodus erstellt Health Log Analytics nicht die Quelltypen, Quellen oder andere Objekte, die im Standard-Flow erstellt werden, um zu vermeiden, dass der Speicher Elasticsearch von durch Beispieldaten überlastet wird. Weitere Informationen finden Sie unter Automatische Zuordnung und Zuordnung von Protokolldaten.
5. Wahlweise: Beachten Sie, wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
   a. Fügen Sie im Feld **Test manual sample** (Manuelles Beispiel testen) eine Beispielnachricht hinzu.
   b. Wählen Sie **Start**.
   c. Beachten Sie, wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
6. Wählen Sie im Feld **Unformatierte Eingabebeispiel** ein Protokollbeispiel aus, das die Auswirkungen Ihrer neuen JavaScript-Funktion auf Protokollzeilen veranschaulicht, wenn Sie sie testen.
7. Definieren Sie eine JavaScript-Funktion, die Ihre Dateneingabequellen der richtigen -Serviceinstanz (hier als Anwendungsservicebezeichnet), Komponente und Quelltyp zuordnet.

   Hinweis: (Nur ACC-Dateneingaben) Stellen Sie sicher, dass Ihre JavaScript-Funktion zur Verarbeitung von Daten verwendet werden kann, die von allen ACC-Dateneingaben gestreamt werden.

   a. Ändern Sie in der JavaScript-Konsole entweder die bereitgestellte JavaScript-Standardfunktion, ändern Sie eine vorhandene benutzerdefinierte JavaScript-Funktion, oder definieren Sie eine neue.

      Hinweis: Neben der JavaScript-Standardfunktion bietet Health Log Analytics JS-Funktionsvorlagen für die Datenzuordnung für Linux-Betriebssystem-Protokolle, die mit syslog gestreamt werden, und Windows-Event-Protokolle, die mit Filebeat gestreamt werden, oder Winlogbeat-Event-Protokolle, die mit Winlogbeat gestreamt werden. Die Vorlagen können als Ausgangspunkt für Ihren benutzerdefinierten Skriptcode dienen. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JavaScript-Funktionsvorlagen

Vorlage	Beschreibung
Mit Syslog gestreamte Linux-Betriebssystemprotokolle	Skript für die Zuordnung von Linux-Protokollen. Ordnet Protokolle der verschiedenen Daemons den richtigen Quelltypen, Komponenten und Serviceinstanzen zu (hier Anwendungsservices). **Hinweis:** Damit diese JavaScript-Funktion ordnungsgemäß funktioniert, müssen Protokolle über einen Syslog-Wrapper verfügen.
Mit Filebeat gestreamtes Windows-Event-Protokoll	Skript für die Zuordnung von Windows-Event-Protokollen, die mit Filebeat gestreamt werden. Ordnet die verschiedenen Windows -Services Quelltypen, Komponenten und -Serviceinstanzen (hier als Anwendungsservicesbezeichnet) zu und gruppiert sie.
Windows – Mit Winlogbeat gestreamte Winlogbeat-Protokolle	Skript für die Zuordnung von Windows-Event-Protokollen, die mit Winlogbeat gestreamt werden. Ordnet die verschiedenen Windows -Services den richtigen Quelltypen, Komponenten und -Serviceinstanzen (hier als Anwendungsservicesbezeichnet)zu.

Die JavaScript-Funktion zur Vorverarbeitung von Rohprotokolldaten verwendet die folgenden Objekte:

- Signatur: Funktionszuordnung (Beispiel, Metadaten)

Objekt	Beschreibung
Beispiel	Das aktuelle Protokollbeispiel nach der Vorverarbeitung
Metadaten	Objekt, das Folgendes enthält: ▪ Event-Stream: Zugriff über: <Metadatenwert>. Beispiel: `metadata.eventStream.origin` ▪ Transform-Header 1: Zugriff über: <Metadatenwert>. Beispiel: `metadata.headers.i1.type` ▪ Transform-Header 2: Zugriff über: <Metadatenwert>. Beispiel: metadata.headers.i2.type

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Objekt	Beschreibung
	▪ type-Transform-Header 3: Zugriff über: <Metadatenwert>. Beispiel: `metadata.headers.i3.type` ▪ Fallback-Zuweisung: Zugriff über: <Metadatenwert>. Beispiel: `metadata.fallBacks.host`

Hinweis: Sie können mehrere Services pro Quelltyp erstellen und zuordnen.

- Typ und Struktur der Rückgabe

Hinweis: Die JavaScript-Funktion gibt eine Zuordnung mit zwei Einträgen zurück. Ändern Sie diese Rückgabestruktur nicht.

Objekt	Beschreibung
applicationService	Der vorhandene Anwendungsservice (d. h. die Serviceinstanz) , dem dieses Muster zugewiesen wird. **Hinweis:** Die Serviceinstanz muss an Anomaliewarnungen im Zusammenhang mit dem Protokoll gebunden sein.
Komponente	Komponente, der dieses Beispiel zugewiesen wird
sourceType	Quelltyp, dem dieses Beispiel zugewiesen wird

- Um eine Protokollnachricht zu verwerfen, rufen Sie `return drop ()` auf.

b. Testen Sie die JavaScript-Funktion, indem Sie auf **Test** klicken.

Durch das Testen der JavaScript-Funktion können Sie das Ergebnis des Skripts im Protokollbeispiel anzeigen. Eine Beschreibung der angezeigten Felder finden Sie unter Ergebnisfelder für JavaScript-Funktionstests.

Hinweis: Wenn sich Ihre neue JavaScript-Funktion nicht wie erwartet verhält, können Sie zur zuletzt veröffentlichten Funktion zurückkehren, indem Sie auf den zugehörigen Link **JS-Funktion zurücksetzen** klicken.

c. Wahlweise: Nehmen Sie alle erforderlichen Anpassungen vor, und testen Sie die JavaScript-Funktion erneut.

d. Wahlweise: Vergleichen Sie die Ergebnisse mehrerer Tests.
Durch den Vergleich der Testergebnisse mehrerer Versionen der JavaScript-Funktion können Sie das Skript verfeinern, bis das gewünschte Ergebnis erreicht ist.

8. Wenn Sie die JavaScript-Funktion abgeschlossen haben, wählen Sie **Vorlage speichern**, um sie zu speichern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die JavaScript-Funktion entweder als neue Vorlage speichern oder die aktuell ausgewählte Vorlage überschreiben.

- Um die JavaScript-Funktion als neue Vorlage zu speichern, geben Sie einen neuen Namen in das Feld **Template name** (Vorlagenname) ein.
- Um die aktuell im Feld **JS function templates** (JS-Funktionsvorlagen) ausgewählte Vorlage zu überschreiben, lassen Sie das Feld **Template name** (Vorlagenname) leer.

9. Klicken Sie auf **Publish** (Veröffentlichen), um die JavaScript-Funktion in der Datenbank zu speichern.

Ergebnisse

Wenn die JavaScript-Funktion veröffentlicht wird, verwendet Health Log Analytics sie zum Zuordnen von Dateneingabequellen.

Das neue Skript wird automatisch der Liste der JS-Funktionsvorlagen hinzugefügt, aus denen Sie auswählen können. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

(Nur ACC-Dateneingaben) Health Log Analytics bietet die veröffentlichte JavaScript-Funktion für alle vorhandenen und zukünftigen ACC-Dateneingaben. Die neue JavaScript-Funktion ersetzt das vorherige Skript.

Nächste Maßnahme

- (Optional) Ändern Sie Rohprotokolldaten, bevor Health Log Analytics sie zuordnet und strukturiert. Wenn Sie diese Aufgabe sofort ausführen möchten, klicken Sie auf den zugehörigen Link **Go to Preprocessor** (Zu Präprozessor wechseln), um zur Seite **Data Input Preprocessor** (Dateneingabe-Präprozessor) zu wechseln.
- (Optional) Feintunen Sie, wie das System Ihre Protokolldaten liest, indem Sie die Quelltypstruktur verfeinern. Mit diesem Schritt können Sie automatisch klassifizierte Eigenschaften neu klassifizieren und automatisch zugeordnete Bezeichnungen ändern.

Zugehörige Informationen

Automatische Zuordnung und Zuordnung von Protokolldaten

Zeigen Sie die Beziehungen zwischen Quelltypen und Protokollquellen an

Erkennung von Headereigenschaften

Extraktion nicht benötigter Protokolldaten stoppen

Extraktion bestimmter Protokolldaten sicherstellen

Zeigen Sie die Beziehungen zwischen Quelltypen und Protokollquellen an

Erkunden Sie die Viele-zu-Viele-Beziehungen zwischen Quelltypen und Protokollquellen in Health Log Analytics, um Ihre Dateneingabezuordnung zu optimieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Health Log Analytics verwendet Quelltypen zum Analysieren von Protokollen und Protokollquellen als Framework für die Erkennung von Anomalien. Jeder Quelltyp stellt Protokolle bereit, die von mehreren Protokollquellen analysiert werden, und jede Protokollquelle empfängt Protokolle, die von mehreren Quelltypen analysiert werden. Durch das Überprüfen der Zuordnungen zwischen Quelltypen und Protokollquellen können Sie Ihre Dateneingabezuordnung verbessern, um Leistung und Ergebnisse zu verbessern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Zuordnung** > **Dateneingabezuordnung**.
2. Stellen Sie sicher, dass Protokolldaten in Ihre -Instanz gestreamt werden, und öffnen Sie dann einen Dateneingabe-Zuordnungsdatensatz.
3. Zeigen Sie die Zuordnungen zwischen den Protokollquellen und den Quelltypen an.
   - Zeigen Sie die Protokollquellen an, die einem Quelltyp zugeordnet sind:
     a. Öffnen Sie die Registerkarte **Quelltypen**, um die generierten Quelltypstrukturen anzuzeigen.
     b. Öffnen Sie einen Quelltyp-Strukturdatensatz.
     c. Wählen Sie einen Quelltyp aus.
     d. Zeigen Sie unter **Quellen**alle Protokollquellen an, die Daten von diesem Quelltyp empfangen.
   - Zeigen Sie die Quelltypen an, die einer Protokollquelle zugeordnet sind:
     a. Öffnen Sie die Registerkarte **Quellen**, um die generierten Protokollquellen anzuzeigen.
     b. Wählen Sie einen Protokollquelldatensatz aus.
     c. Zeigen Sie auf der Registerkarte **Quelltypen** alle Quelltypen an, die Daten in diese Protokollquelle einspeisen.

Hinweis: Die angezeigten Ergebnisse werden einmal pro Tag aktualisiert. Ergebnisse, die älter als 24 Stunden sind, werden automatisch gelöscht.

Erkennung von Headereigenschaften

In Health Log Analyticstrennt die automatische Erkennung von Headereigenschaften den Transportheader von der inneren Protokollnachricht und leitet nur die innere Protokollnachricht an die Quelltypstruktur weiter. Die innere Nachricht enthält die tatsächlichen Protokolldaten ohne Informationen zur Übermittlung.

Die Anwendung Health Log Analytics unterstützt die Erkennung von Headereigenschaften für Fluentd, Beats und Syslog (RFC 3164, RFC 5424).

Ab Version 33.0.27 – August 2024 unterstützt das System auch die Erkennung von Headereigenschaften für Protokolle, die dem OpenTelemetry-Protokolldatenmodell und den semantischen Konventionen entsprechen. Weitere Informationen finden Sie in der Dokumentation zum OpenTelemetry-Protokolldatenmodell .

Erkennung von Headereigenschaften wird deaktiviert

Wenn Sie die Erkennung von Headereigenschaften für eine Dateneingabe deaktivieren, stoppt die KI-Engine von Health Log Analytics das Extrahieren von Eigenschaften aus dem Header. Das Weiterleiten der vollständigen Rohnachricht kann in den folgenden Situationen nützlich sein:

- Die innere Protokollnachricht enthält keine Informationen zum Analysieren, z. B. Zeitstempel und Schweregrad.
- Die Dateneingabe enthält Informationen, die zur Strukturierung verwendet werden können.
- Die Dateneingabe leitet die vollständig analysierten Protokolle weiter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zum Deaktivieren der Erkennung von Headereigenschaften finden Sie unter Protokolldaten im Rohzustand zuordnen.

Extraktion nicht benötigter Protokolldaten stoppen

Wenn eine extrahierte Datenzeichenfolge nicht aussagekräftig genug ist oder redundanten Text oder Informationen enthält, können Sie Health Log Analytics so konfigurieren, dass die Extraktion solcher Daten aus den Protokollen gestoppt wird.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Zuordnung** > **Ausgeschlossene Werte**.
2. Wählen Sie **Neu**.
3. Geben Sie im Feld **Value to exclude** (Auszuschließender Wert) die Zeichenfolge ein, die Health Log Analytics nicht mehr extrahieren soll.
4. Wahlweise: Verfeinern Sie die Festlegung der Werte, die nicht mehr extrahiert werden sollen, indem Sie zusätzliche Optionen auswählen:
   - Starts with (Beginnt mit)
   - Ends with (Endet mit)
   - Enthält
   - Case sensitive (Groß-/Kleinschreibung beachten)
5. Wahlweise: Fügen Sie im Feld **Beschreibung** eine Beschreibung des Werts hinzu.
6. Wählen Sie **Absenden** aus.

Extraktion bestimmter Protokolldaten sicherstellen

Konfigurieren Sie Health Log Analytics so, dass bestimmte Begriffe aus Feldern extrahiert werden und sie bestimmten Komponenten zugeordnet werden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Zuordnung** > **Extrahierte Werte**.
2. Wählen Sie **Neu**.
3. Geben Sie im Feld **Value to extract** (Zu extrahierender Wert) den Begriff ein, den Health Log Analytics aus den Protokollen extrahieren soll.
4. Geben Sie im Feld **Map to component** (Zu Komponente zuordnen) die Komponente ein, der der Wert zugeordnet werden soll.
5. Wählen Sie im Feld **Property** (Eigenschaft) eine Eigenschaft aus der Liste aus.
6. Wahlweise: Verfeinern Sie die Festlegung der Werte, die extrahiert werden sollen, indem Sie zusätzliche Optionen auswählen:
   - Exact match (Genaue Übereinstimmung)
   - Case sensitive (Groß-/Kleinschreibung beachten)
7. Wahlweise: Fügen Sie im Feld **Beschreibung** eine Beschreibung des Werts hinzu.
8. Wählen Sie **Absenden** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Quelltypstruktur anpassen

Mit Health Log Analytics können Sie automatisch klassifizierte Eigenschaften neu klassifizieren und automatisch zugeordnete Bezeichnungen ändern. Durch diese Anpassungen können die ML-Funktionen (maschinelles Lernen) Health Log Analytics Ihre Prioritäten besser verstehen.

Health Log Analytics trennt den Transport-Header automatisch von der inneren Protokollnachricht und sendet die innere Protokollnachricht an die Quelltypstruktur. Eigenschaften werden aus eingehenden Protokollnachrichten extrahiert, und Quelltypfeldern werden automatischBeschriftungen zugeordnet.

Durch die Änderung der Struktur und Klassifizierung des Quelltyps können Sie sicherstellen, dass die KI-Engine von Health Log Analytics alle Eigenschaften ordnungsgemäß extrahiert und entsprechend klassifiziert. Da eine einzelne Dateneingabe mehr als einen Quelltyp enthalten kann, strukturiert das System Protokolldaten nach Quelltyp und nicht nach Dateneingabe.

Betrachten Sie beispielsweise das folgende Protokoll:

```
{
  "TenantId": "abc-01-02-03-04-05050708091011121314",
  "@timestamp": "2020-08-28T08:29:23.967Z",
  "Computer": "john Doe_computer",
  "EventType_s": "LogMessage",
  "Job_s": "johnDoe_cell",
  "IP_s": "1.00.00.00",
  "message": "This is the extracted message. This part of the message
 includes superfluous content and values",
  "MessageType_s": "OUT",
  "Timestamp_d": 1598603359017850000,
  "Type": "my_LogMessage_is",
  "_ResourceId": ""
}
```

Der Beispielcode enthält `„Schlüssel":„Wert"`-Paare. Der Schlüssel ist der Eigenschaftsname, und der Wert ist der Eigenschaftswert.

Der Schlüssel „message" hat den folgenden Wert: `„This is the extracted message. This part of the message includes superfluous content and values"`. Wenn Sie möchten, dass Ihre Protokolle nur den aussagekräftigen Teil dieser Nachricht enthalten, fügen Sie JavaScript-Code hinzu, der das System anweist, nur diesen Teil zu extrahieren.

```
//Added JavaScript to extract only the first sentence in the
 message! if (output['message'] != null){ output['message'] =
 output['message'].slice(0, output['message'].indexOf("\.")); } (edited)
```

Dieselbe Logik können Sie verwenden, um einen Wert neu zu klassifizieren. Wenn beispielsweise der Schlüssel „Computer" nicht signifikant ist, können Sie seinen Wert auf „Ungültig" festlegen.

Weitere Informationen zur Quelltypstruktur finden Sie im Artikel Source Type Structure – Labels & Classifications (Quelltypstruktur – Bezeichnungen und Klassifizierungen) [KB0863562] in der Now Support-Knowledge Base.

Quelltypstruktur verfeinern

Feintunen Sie, wie Health Log Analytics Ihre inneren Protokollnachrichten liest und Anomalien erkennt, indem Sie die extrahierten Eigenschaften in der Quelltypstruktur anpassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingaben** > **Quelltypstruktur**.
2. Öffnen Sie einen Datensatz.

Hinweis:

- Standardmäßig ist **Auto extraction** (Automatische Extraktion) ausgewählt, damit Health Log Analytics den Transport-Header automatisch von der inneren Protokollnachricht trennt.
- Wenn das Formular „Source Type Structure“ (Quelltypstruktur) zum ersten Mal angezeigt wird, ruft Health Log Analytics Protokollbeispiele automatisch ab. Rufen Sie in nachfolgenden Sitzungen die neuesten Beispiele ab, indem Sie **Refresh Samples** (Beispiele aktualisieren) auswählen.

3. Wahlweise: Schauen Sie sich an, wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
   a. Fügen Sie im Feld **Test manual sample** (Manuelles Beispiel testen) eine Beispielnachricht hinzu.
   b. Wählen Sie **Start**.
   c. Beachten Sie auf der Registerkarte **Key/Value Mapping** (Schlüssel-Wert-Zuordnung), wie sich die JavaScript-Funktion auf Protokollzeilen auswirkt.
4. Wählen Sie im Feld **Raw input sample** (Roheingabebeispiel) eine Protokollnachricht aus.

   Health Log Analytics verwendet diese Beispielnachricht, um den kombinierten Effekt der automatischen Extraktion und der JavaScript-Funktion in den Protokollzeilen zu veranschaulichen, wenn Sie Ihre JavaScript-Funktion testen.

   Die folgenden Felder sind schreibgeschützt:

Feld	Beschreibung
Duration (ms) (Dauer (ms))	Verarbeitungszeit aller Beispiele in Millisekunden
Dropped (Verworfen)	Gesamtzahl der in allen Beispielen verworfenen Protokolle
Fehler	Gesamtzahl der in allen Beispielen aufgetretenen Fehler
Zeitstempel-Extraktionsfehler	Anzahl der Zeitstempel-Extraktionsfehler, die in allen Beispielen aufgetreten sind
Severity extraction failures (Schweregrad-Extraktionsfehler)	Gesamtzahl der Schweregrad-Extraktionsfehler, die in allen Beispielen aufgetreten sind
Message extraction failures (Nachrichten-Extraktionsfehler)	Gesamtzahl der Nachrichten-Extraktionsfehler, die in allen Beispielen aufgetreten sind
Lengthy properties (Lange Eigenschaften)	Gesamtzahl der längeren Eigenschaften in allen Beispielen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Lange Eigenschaften sind Eigenschaften mit mehr als 256 Zeichen. **Hinweis:** Da Health Log Analytics solche Eigenschaften nicht extrahiert, werden sie in Elasticsearch nicht als Stichwörter indiziert.

5. Definieren Sie eine JavaScript-Funktion, die automatisch extrahierte Eigenschaften anpasst oder der Quelltypstruktur Eigenschaften hinzufügt.

   a. Ändern Sie in der JavaScript-Konsole entweder die bereitgestellte JavaScript-Standardfunktion, ändern Sie eine vorhandene benutzerdefinierte JavaScript-Funktion, oder definieren Sie eine neue.

      Hinweis: Zusätzlich zur JavaScript-Standardfunktion bietet Health Log Analytics mehrere JS-Funktionsvorlagen zum Verfeinern der Quelltypstruktur. Die Vorlagen können als Ausgangspunkt für Ihren benutzerdefinierten Skriptcode dienen. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

JS-Funktionsvorlagen	Beschreibung
Key_Values mit regulärem Ausdruck extrahieren	Skript, das zum Analysieren von Protokollen in einer Reihe von Schlüssel-Wert-Paaren verwendet wird, indem reguläre Ausdrücke verwendet werden, um bestimmte Muster von regulären Ausdrücken zu identifizieren. Abhängig von den Protokolldaten, die an den Quelltyp gesendet werden, analysiert es entweder die innere Nachricht oder die vollständige Protokollzeile. Sie können sich anschauen, wie die Daten in den Beispielen angezeigt werden, die in die Quelltypstruktur geladen werden. Dieser Prozess ist iterativ. Er wird wiederholt, bis alle Schlüssel-Wert-Paare gefunden wurden.
Key_Values mit split-regex extrahieren	Skript, das zum Analysieren von Protokollen in einer Reihe von Schlüssel-Wert-Paaren verwendet wird, indem reguläre Ausdrücke verwendet werden, um bestimmte Muster von regulären Ausdrücken zu identifizieren. Dieser Prozess erfasst zuerst die Werte in einem LIST-Formular und verwendet dann die Java-Split-Funktion, um Schlüssel-Wert-Paare zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JS-Funktionsvorlagen	Beschreibung
	Je nachdem, wie die Daten in der Roheingabe angezeigt werden, ist diese Funktion möglicherweise effizienter als das `Extrahieren von Key_Values mit regulärem Ausdruck`. Die Roheingabe ist entweder die innere Nachricht, die die Headererkennung weiterleitet, oder das vollständige Rohprotokoll, wenn die Headererkennung deaktiviert ist oder für dieses bestimmte Protokoll nicht funktioniert.
JSON-Analyse - reduzieren	Skript, das zum Extrahieren von JSON-Informationen verwendet wird, die Teil einer anderen Textzeichenfolge aus der Roheingabe sind. Beispielsweise könnten die Informationen eine JSON-Anforderung sein, die als Teil einer längeren inneren Nachricht geschrieben wurde. Innere JSON-Abschnitte sind schwer aufzuteilen. In solchen Fällen kann dieses Skript verwendet werden, um die Schlüssel-Wert-Paare zu „reduzieren“ oder zu analysieren.
Neues Feld aus Roheingabe extrahieren	Skript, das zum Extrahieren eines neuen Felds aus der Roheingabe verwendet wird, indem ein regulärer Ausdruck mit Erfassungsgruppen verwendet wird, um das Muster des neuen Felds zu identifizieren.
XML-Format analysieren	Skript, das zum Extrahieren von Schlüssel-Wert-Paaren aus dem XML verwendet wird, indem das XML-Format mithilfe eines regulären Ausdrucks identifiziert wird. Dieser Prozess ist iterativ. Er wird wiederholt, bis alle Schlüssel-Wert-Paare gefunden wurden.
Numerischen Schweregrad als Textwerte festlegen	Skript, das zum Konvertieren von numerischen Schweregradwerten in entsprechende Textschweregradwerte verwendet wird. **Hinweis:** Damit das System den Schweregrad eines Protokolls richtig identifizieren kann, muss der Schweregrad im Textformat angegeben werden. Es dürfen keine numerischen Schweregradwerte übrig bleiben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JS-Funktionsvorlagen	Beschreibung
Trim-Funktion	Skript, das zum Entfernen der doppelten Anführungszeichen verwendet wird, die die Zeichenfolge von VALUE umgeben. Sie können diese Funktion anpassen, um alle anderen Zeichen zu entfernen, die den Ausgabewert eines Schlüssel-Wert-Paares umgeben.

Die JavaScript-Funktion zum Verfeinern der Quelltypstruktur verwendet die folgenden Objekte:

Signatur: Funktionskonstrukt (Beispiel, Ausgabe)

Objekt	Beschreibung
Beispiel	Aus der Beispielnachricht extrahierte innere Nachricht
Ausgabe	Objekt, das die Schlüssel-Wert-Paarzuordnung enthält

b. Testen Sie die JavaScript-Funktion, indem Sie auf **Test** klicken.

c. Zeigen Sie das Ergebnis der JavaScript-Funktion in den zugehörigen Listen an, und nehmen Sie bei Bedarf Änderungen vor.

- Die Registerkarte **Schlüssel/Wert-Zuordnungen** zeigt die Auswirkungen Ihrer JavaScript-Funktion in Kombination mit der automatischen Extraktion des Systems für Ihr Roheingabebeispiel.

  Gegebenenfalls können Sie Schlüssel ändern.

  - Mit dem Feld **Classification** (Klassifizierung) können Sie die Klassifizierung einer Eigenschaft zurücksetzen. Die verfügbaren Typen lauten:

Typ	Beschreibung	Beispiel
Zähler	Eine Eigenschaft bei dieser Klassifizierung erkennt Anomalien anhand der Häufigkeit, in der die Eigenschaft in jeder Protokollnachricht erscheint. Sie stellt Änderungen in der Menge dieses Werts als Teil der automatischen Ursachenanalyse dar.	Statuscodes, Antwortcodes, Aktionen oder Muster

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Beschreibung	Beispiel
	Hinweis: Als Zähler klassifizierte Eigenschaften verbrauchen Ressourcen.	
Anzeige	Eine Eigenschaft mit dieser Klassifizierung erkennt Anomalien in einem numerischen Wert, der kontinuierlich gemeldet wird. **Hinweis:** Als Anzeige klassifizierte Eigenschaften verbrauchen Ressourcen.	CPU, Arbeitsspeicher oder Antwortzeit
Anzeige ohne Zeit	Eine Eigenschaft mit dieser Klassifizierung erkennt Anomalien in einem numerischen Wert, der nicht kontinuierlich gemeldet wird. Das System meldet eine Anomalie in diesem Wert, egal wann die Anomalie aufgetreten ist. **Hinweis:** Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .	
Automatische Ursachenanalyse (nur ARC)	Eine Eigenschaft mit dieser Klassifizierung meldet die Eigenschaft nicht als eigenständige Anomalie, sondern als Teil der automatischen Ursachenanalyse einer anderen Anomalie.	Benutzername, IP-Adressen, Anwendungskomponenten oder Rechenzentrum
Ungültig	Eine Eigenschaft mit dieser Klassifizierung wird in der automatischen Ursachenanalyse nicht berechnet oder angezeigt.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Beschreibung	Beispiel
	Hinweis: Als ungültig klassifizierte Eigenschaften sparen Ressourcen.	

- Über das Feld **Bezeichnungen, die zugewiesen werden sollen** können Sie eine Eigenschaft für eine Bezeichnung festlegen.

Bezeichnung	Beschreibung
Zeitstempel	Eigenschaft, die den Zeitstempel des Events enthält **Hinweis:** Wenn die automatische Erkennung von Headereigenschaften aktiviert ist und der Quelltyp keinen Zeitstempel hat, extrahiert das System den Zeitstempel aus dem Übertragungsheader. Wenn die Headererkennung deaktiviert ist oder für die relevanten Protokollzeilen in der Dateneingabe nicht funktioniert, müssen alle Protokollzeilen über die richtigen Zeitstempel verfügen.
Schweregrad	Eigenschaft, die den Schweregrad des Protokolls darstellt
Nachricht	Protokollnachricht Das System verwendet diese Eigenschaft, um Textmuster in den Daten zu identifizieren.
Host	Eigenschaft, die den Host darstellt, von dem das Event gesendet wurde **Hinweis:** Wenn die automatische Erkennung von Headereigenschaften aktiviert ist und der Quelltyp keinen Host hat, extrahiert das System den Host aus dem Übertragungsheader. Wenn die Headererkennung deaktiviert ist oder für die relevanten Protokollzeilen in der Dateneingabe nicht funktioniert, müssen alle Protokollzeilen über die einen Host verfügen.
Externe ID	Eigenschaft, die als eindeutiger Bezeichner für diesen Event-Typ dient.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bezeichnung	Beschreibung
	Beispiel: Event-ID im Windows-Event-Protokoll

- Im Feld **Rename key** (Schlüssel umbenennen) können Sie den Schlüssel umbenennen.

- Die Registerkarte **Outcome Key-Value** (Ergebnis-Schlüssel-Wert) zeigt, wie Ihre JavaScript-Funktion die Daten verarbeitet hat.
- Auf der Registerkarte **„Dateneingabezuordnungen“** werden die Dateneingabezuordnungen für den aktuellen Quelltyp angezeigt.
- Die übrigen Registerkarten zeigen Fehler, Nachrichten-Extraktionsfehler, Schweregrad-Extraktionsfehler, Zeitstempel-Extraktionsfehler und lange Eigenschaften an.

Hinweis: Wenn sich Ihre neue JavaScript-Funktion nicht wie erwartet verhält, können Sie zur zuletzt veröffentlichten Funktion zurückkehren, indem Sie auf den zugehörigen Link **JS-Funktion zurücksetzen** klicken.

d. Wahlweise: Nehmen Sie alle erforderlichen Anpassungen vor, und testen Sie die JavaScript-Funktion erneut.

6. Klicken Sie auf **Save template** (Vorlage speichern), um die JavaScript-Funktion zu speichern.
   Sie können die JavaScript-Funktion entweder als neue Vorlage speichern oder die aktuell ausgewählte Vorlage überschreiben.
   - Um die JavaScript-Funktion als neue Vorlage zu speichern, geben Sie einen neuen Namen in das Feld **Template name** (Vorlagenname) ein.
   - Um die aktuell im Feld **JS function templates** (JS-Funktionsvorlagen) ausgewählte Vorlage zu überschreiben, lassen Sie das Feld **Template name** (Vorlagenname) leer.
7. Klicken Sie auf **Publish** (Veröffentlichen), um die JavaScript-Funktion in der Datenbank zu speichern.

Ergebnisse

Wenn die JavaScript-Funktion veröffentlicht wird, verwendet Health Log Analytics sie, um zu optimieren, wie sie Ihre inneren Protokollnachrichten liest und Anomalien erkennt.

Das neue Skript wird automatisch der Liste der JS-Funktionsvorlagen hinzugefügt, aus denen Sie auswählen können. Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

Nächste Maßnahme

Fahren Sie mit den verbleibenden Setup-Aufgaben für Dateneingaben fort: Stellen Sie sicher, dass alle Protokollquellen vorhanden und aktiv sind, und fügen Sie gegebenenfalls Zeitstempelformate hinzu.

Weitere Setupaufgaben für Dateneingaben

Nach der ersten Einrichtung und Konfiguration der Dateneingabe können Sie die übrigen Setupaufgaben für die Dateneingabe ausführen.

Zeitstempelformate hinzufügen

Definieren Sie ein Zeitstempelformat, das nicht in der Liste der definierten Formate angezeigt wird. Health Log Analytics muss Zeitstempel jedes Formats lesen können, das in Ihren Protokolldateien enthalten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Zeitstempelformate**.
2. Um zu bestimmen, ob Ihr Zeitstempelformat mit einem vordefinierten Format im System übereinstimmt, gehen Sie wie folgt vor:
   a. Klicken Sie auf **Find format** (Format suchen).
   b. Geben Sie ein Beispiel für Ihren Zeitstempel ein.
   c. Klicken Sie auf **Find format** (Format suchen).
   Wenn das Beispiel einem vorhandenen Format entspricht, gibt das System seine ID an.
3. Wenn das Zeitstempelbeispiel nicht mit einem vorhandenen Format übereinstimmt, definieren Sie Ihr benutzerdefiniertes Format manuell, und fügen Sie es den verfügbaren Zeitstempelformaten hinzu.
   a. Wählen Sie auf der Seite „Timestamp Formats“ (Zeitstempelformate) die Option **New** (Neu) aus.
   b. Füllen Sie die Felder des Formulars aus.

Formular „Zeitstempelformat“

Feld	Beschreibung
ID	ID des Zeitstempelformats. Dieser Wert ist automatisch ausgewählt.
Format	Gültiges Zeitstempelformat. Beispiel: tt-MMM-jjjj, HH:mm. **Hinweis:** Für die Zeitstempelsyntax verwendet Health Log Analytics die Java 8-API.
Beispiel	Beispiel für das Zeitstempelformat. Beispiel: 03. Mai 2018, 10:20
Beschreibung	Beschreibung des Zeitstempelformats.

4. Wählen Sie **Absenden** aus.

Ergebnisse
Das System validiert das Zeitstempelformat und fügt es der Liste der verfügbaren Zeitstempel hinzu.

Quelltypen manuell hinzufügen

Erstellen Sie einen Quelltyp manuell, bevor Sie eine Dateneingabe konfigurieren, wenn Sie Protokolldaten nicht an den Quelltyp streamen möchten, der während des Zuordnungsprozesses von Health Log Analytics automatisch extrahiert wird, sondern an einen bestimmten Quelltyp.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Quelltypen**.
2. Wählen Sie auf der Registerkarte „Quelltypen“ **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular „Quelltyp“

Feld	Beschreibung
Name	Name des Quelltyps. Der Name muss zwischen 3 und 50 Zeichen lang sein. Zulässige Zeichen sind Buchstaben, numerische Werte, Bindestriche und Unterstriche.
Beispiele	Mindestens ein Beispiel für Roheingaben für diesen Quelltyp. Geben Sie jedes Beispiel in eine neue Zeile ein. **Hinweis:** Dieses Feld muss Daten enthalten.

Die Felder in der folgenden Tabelle sind schreibgeschützt.

Feld	Beschreibung
Manuell erstellt	Option zum Angeben, dass dieser Quelltyp manuell erstellt wurde. Standardwert: true
Auto-extraction enabled (Automatische Extraktion aktiviert)	Standardmäßig ist die automatische Extraktion für diesen Quelltyp deaktiviert.
Lernmodus	Option zur Angabe, dass der Lernmodus für den Quelltyp ausgeführt wird. Die KI-Engine muss das Format der Protokollnachrichten in jedem neuen Protokollstream erlernen. Im Lernmodus erlernt sie das Format von Nachrichten für diesen Quelltyp und extrahiert Eigenschaften basierend auf diesen Informationen.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
5. Wählen Sie **Load examples** (Beispiele laden), um die Roheingabebeispiele für diesen Quelltyp zu laden, die Sie im Feld **Beispiele** angegeben haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn das Laden der Protokollbeispiele erfolgreich abgeschlossen wurde, werden das Feld **Beispiele** und die Schaltflächen **Load examples** (Beispiele laden) nicht mehr im Formular angezeigt.

6. Wahlweise: Überprüfen Sie, wie die KI-Engine die Roheingabebeispiele analysiert hat, indem Sie auf den zugehörigen Link **Go to Source Type Structure** (Gehe zu Quelltypstruktur) klicken, und ändern Sie die extrahierten Eigenschaften gegebenenfalls.
7. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Konfigurieren Sie eine Dateneingabe, und ordnen Sie sie dann dem neuen Quelltyp zu. Weitere Informationen finden Sie unter Richten Sie Dateneingaben für Health Log Analytics manuell ein und Protokolldaten im Rohzustand zuordnen.

Zugehörige Informationen

Quelltypstruktur verfeinern

Quelltypfunktionen konfigurieren

Health Log Analytics extrahiert Quelltypen im Zuordnungsprozess automatisch. Sie können Zeitstempelformate hinzufügen und Stichwörter für einzelne Quelltypen angeben, löschen oder ausschließen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Quelltypen**.
   Die Tabelle „Quelltypen“ enthält alle Quelltypen, die während der Zuordnung von Rohdaten automatisch extrahiert wurden.

Quelltypen

Feld	Beschreibung
Automatische Extraktion aktiviert	Die automatische Extraktion für diesen Quelltyp ist entweder aktiviert oder deaktiviert. Dieser Wert wird im Formular „Source Type Structure“ (Quelltypstruktur) festgelegt. Standardwert: true
Lernmodus	Der Lernmodus für den Quelltyp ist entweder fortlaufend oder abgeschlossen. Die KI-Engine muss das Format der Protokollnachrichten in jedem neuen Protokollstream erlernen. Im Lernmodus erlernt sie das Format von Nachrichten für diesen Quelltyp und extrahiert Eigenschaften basierend auf diesen Informationen.
Stack trace detection enabled (Stack Trace-Erkennung aktiviert)	Die Erkennung der aktiven Stack Frames für diesen Quelltyp ist entweder aktiviert oder deaktiviert. Normalerweise ermöglicht ein Stack Trace die Nachverfolgung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	eines Fehlers in dem Protokoll, aus dem er stammt.

2. Öffnen Sie einen Datensatz.
3. Wahlweise: Fügen Sie ein Zeitstempelformat für diesen Quelltyp hinzu.
   a. Wählen Sie auf der Registerkarte **Source Type Timestamps** (Quelltyp-Zeitstempel) die Option **New** (Neu) aus.
   b. Wählen Sie im Feld **Timestamp format** (Zeitstempelformat) ein Format aus der Liste der verfügbaren Zeitstempelformate aus.
   c. Wählen Sie **Absenden** aus.
4. Wahlweise: Geben Sie ein Stichwort für diesen Quelltyp an.
   a. Wählen Sie auf der Registerkarte **Lexical Keywords** (Lexikalische Stichwörter) **New** (Neu) aus.

      Hinweis: Die Registerkarte **Lexical Keywords** (Lexikalische Stichwörter) enthält sowohl globale als auch angegebene Stichwörter. Durch die Auswahl von **New** (Neu) wird ein angegebenes Stichwort für diesen Quelltyp erstellt.

   b. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für das Stichwort
Regulärer Ausdruck	Der reguläre Ausdruck („Regex"), mit dem Übereinstimmungen definiert werden
Exact match (Genaue Übereinstimmung)	Boolescher Wert. Wenn er auf True gesetzt ist, erwartet Health Log Analytics eine exakte Übereinstimmumg mit dem regulären Ausdruck. Beispiel: „NullPointerException" würde in einer Nachricht nicht mit dem regulären Ausdruck „exception" übereinstimmen. Standardwert: True
Groß-/Kleinschreibung beachten	Boolescher Wert. Wenn diese Option ausgewählt ist, sucht Health Log Analytics nach einer Übereinstimmung des regulären Ausdrucks, bei der die Groß-/Kleinschreibung übereinstimmt. Standardwert: False

   c. Wählen Sie **Absenden** aus.
5. Wahlweise: Löschen Sie ein Stichwort, das für diesen Quelltyp festgelegt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Markieren Sie die Zeile des angegebenen Stichworts, das Sie löschen möchten.

b. Wählen Sie in der Liste **Actions on selected rows** (Aktionen für ausgewählte Zeilen) unten auf der Seite die Option **Exclude keyword** (Stichwort ausschließen) aus.

c. Klicken Sie auf **Continue** (Fortsetzen), um das Stichwort zu löschen.

6. Wahlweise: Schließen Sie ein globales Stichwort für diesen Quelltyp aus.
Wenn Sie ein Stichwort ausschließen, sucht Health Log Analytics in den Protokolldaten dieses Quelltyps nicht mehr danach.

a. Markieren Sie die Zeile des globalen Stichworts, das Sie ausschließen möchten.

b. Wählen Sie in der Liste **Actions on selected rows** (Aktionen für ausgewählte Zeilen) unten auf der Seite die Option **Exclude keyword** (Stichwort ausschließen) aus.

Hinweis: Sie können globale Stichwörter auf der Seite Lexical Keywords (Lexikalische Stichwörter) löschen.

7. Wählen Sie **Aktualisieren**.

Protokollquellen überprüfen

Stellen Sie sicher, dass alle Ihre Protokollquellen vorhanden und aktiv sind, nachdem durch das Tagging Health Log Analytics ein Protokoll einer Serviceinstanz und Komponenten zugewiesen und das Protokoll automatisch einer Quelle zugeordnet wurde.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Protokollquellen**.
Die Tabelle „Log Sources“ (Protokollquellen) enthält Informationen zu den Quellen, die beim Zuordnen der Streaming-Daten erstellt wurden. In der Tabelle werden diese Quellen nach Serviceinstanz geordnet aufgelistet.

Spalte	Beschreibung
Serviceinstanz	Die Serviceinstanz. Serviceinstanzen repräsentieren große oder vollständige Geschäftsprozesse. Eine einzelne Serviceinstanz kann aus mehreren Komponenten bestehen, während verschiedene Serviceinstanzen dieselben Komponenten enthalten können.
Komponente	Die Komponenten, aus denen die Serviceinstanz besteht. Komponenten stellen kleine technische Teile oder Geschäftsprozesse dar. In der Regel stellen sie Konfigurationselemente (CIs) dar. Mehrere Komponenten sind häufig in einer einzigen Serviceinstanzzusammengefasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Status	Status der Protokollquelle: „Active“ oder „Inactive“ (Aktiv oder Inaktiv). Der Status „Active“ gibt an, dass während der letzten Stunde Protokolle aus dieser Quelle in das System gestreamt wurden.
Erstellt	Datum und Uhrzeit der Erstellung dieser Protokollquelle
Last event time (Zeit des letzten Events)	Zeitpunkt, an dem zum letzten Mal Protokolle aus dieser Quelle in das System gestreamt wurden

2. Stellen Sie sicher, dass im System alle Ihre Protokollquellen erstellt wurden.
3. Überprüfen Sie Erstellung, Status und Protokollbeispiele einer bestimmten Quelle im Quelldatensatz.

   Hinweis: Da bei der automatischen Zuordnung Protokolldaten mehreren Quellen zugeordnet werden können, müssen Sie diese Informationen für jede einzelne Quelle überprüfen.

4. Wenn eine Protokollquelle fehlt, fügen Sie sie hinzu.

   a. Navigieren zu **Health Log Analytics** > **Dateneingabe** > **Dateneingabezuordnung**.

   b. Verwenden Sie die JavaScript-Funktion, um ein Protokollbeispiel manuell der richtigen Serviceinstanz, Komponente und dem richtigen Quelltyp zuzuordnen.
   Weitere Informationen finden Sie unter Protokolldaten im Rohzustand zuordnen.

   c. Navigieren Sie zurück zur Seite „Log Sources“ (Protokollquellen), und stellen Sie sicher, dass der Status der neuen Protokollquelle „Active“ lautet.

   Das System erstellt eine Protokollquelle.
5. Stellen Sie sicher, dass der Status aller Protokollquellen „Active“ ist.
   Wenn der Status einer Quelle „Inactive“ ist, doppelklicken Sie darauf, und ändern Sie sie manuell in „Active“.
6. Wählen Sie **Aktualisieren**.

Zugehörige Informationen

Löschen Sie eine Protokollquelle

Extraktion nicht benötigter Protokolldaten stoppen

Extraktion bestimmter Protokolldaten sicherstellen

Überprüfen Sie die aus einem Quelltyp in Health Log Analyticsextrahierten Eigenschaften

Zeigen Sie die Eigenschaften, die aus allen Quelltypen in einer Quelltypstruktur extrahiert wurden, in einer einzigen Tabelle an, um Setup-Probleme zu identifizieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

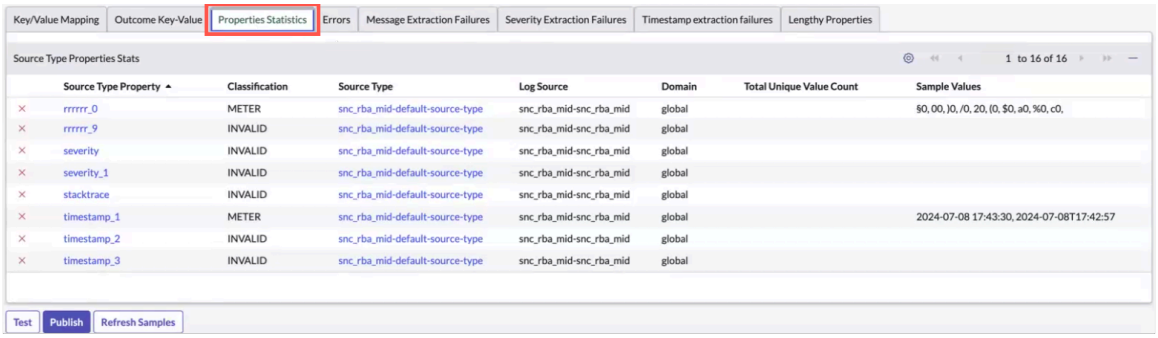
Warum und wann dieser Vorgang ausgeführt wird

Die Statistiktabelle zu Quelltypeigenschaften bietet eine umfassende Übersicht über die Eigenschaften, die aus den Quelltypen extrahiert wurden. Indem Sie die statistische Verteilung der Werte überprüfen, können Sie die Klassifizierung dieser Eigenschaften beurteilen und Ihre Einstellungen bei Bedarf anpassen.

In diesem Abschnitt wird erläutert, wie Sie über die Quelltypstruktur auf die Statistiktabelle der Quelltypeigenschaften zugreifen. Von einem Quelltyp-Datensatz aus können Sie zur Quelltypstruktur navigieren, indem Sie den zugehörigen Link **„Zur Quelltypstruktur wechseln“** auswählen.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Quelltypstrukturen**.
2. Öffnen Sie einen Quelltyp-Strukturdatensatz.
3. Öffnen Sie die Registerkarte Zugehörige Links **zu Eigenschaftenstatistiken**.



Die Statistiktabelle **der Quelltypeigenschaften** zeigt die Eigenschaften aller Quelltypen, die Teil dieser Quelltypstruktur sind.

Statistiken zu Quelltypeigenschaften

Spalte	Beschreibung
Quelltypeigenschaft	Die aus dem Quelltyp extrahierte Eigenschaft.
Klassifizierung	Die Klassifizierung der Eigenschaft. Die verfügbaren Typen sind: METER, GAUGE, ARC und INVALID. **Hinweis:** Eine als INVALID klassifizierte Eigenschaft (die Standardklassifizierung) wird nicht für die Anomalie-Erkennung nachverfolgt oder in der Analyse der aussagekräftigen Eigenschaften angezeigt.
Quelltyp	Der Quelltyp, aus dem die Eigenschaft extrahiert wurde.
Protokollquelle	Die Liste der Protokollquellen, in denen diese Eigenschaft angezeigt wird.
Domäne	Die Domäne, zu der die Protokollquelle gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Gesamtanzahl eindeutiger Werte	Nur für als METER klassifizierte Eigenschaften: Die Gesamtzahl der darin enthaltenen unterschiedlichen Werte. Dieses Feld ist inaktiv, wenn die Eigenschaft als ARC oder GAUGE klassifiziert ist. **Hinweis:** Die Gesamtanzahl der eindeutigen Werte wird einmal pro Tag aktualisiert. Datensätze, die älter als 24 Stunden sind, werden automatisch gelöscht.
Beispielwerte	Nur für Eigenschaften, die als METER klassifiziert sind: Beispiel für eindeutige Werte, die vom System verfolgt werden. Der Standardwert ist 30 Beispiele. Dieses Feld ist inaktiv, wenn die Eigenschaft als ARC oder GAUGE klassifiziert ist.

4. Überprüfen Sie die Eigenschaften, und identifizieren Sie mögliche Klassifizierungsprobleme.
5. Wahlweise: Zeigen Sie Statistiken für einzelne Quelltypeigenschaften an, die als ARC_ONLY oder GAUGE klassifiziert sind.
   a. Öffnen Sie eine Quelltypeigenschaft, die als ARC_ONLY oder GAUGE klassifiziert ist, auf der Registerkarte mit zugehörigen Links **zu Eigenschaftenstatistiken**.
   b. Wählen Sie im Formular **„Quelltypeigenschaft“Quelltypeigenschaften Statistiken**aus.
   Die folgenden Informationen werden in einem Popup-Fenster angezeigt:
   - Für eine ARC-Eigenschaft: Die prozentuale Verteilung der Begriffe basierend auf den verarbeiteten Protokollen. Zum Beispiel der Prozentsatz von „Ungültige Anforderung“ vs. Erfolg.
   - Für eine GAUGE-Eigenschaft: Durchschnitt, Minimum und Standardabweichung vom erwarteten numerischen Wert.
6. Wahlweise: Ändern Sie die Klassifizierungseinstellungen auf der Registerkarte **Schlüssel/ Wert-Zuordnung**.
   Weitere Informationen finden Sie unter Quelltypstruktur verfeinern.

Aus einem Quelltyp in Health Log Analyticsextrahierte Muster überprüfen

Zeigen Sie alle gelernten Muster, die aus einem Quelltyp extrahiert wurden, in einer Quelltypstruktur zusammen mit den Protokollquellen an, in denen diese Muster aufgetreten sind. Die Überprüfung dieser Muster kann wertvolle Einblicke in die Protokollnachrichtenmuster liefern, die Health Log Analytics für jeden Quelltyp und jede Protokollquelle nachverfolgt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Quelltypstrukturen**.
2. Wählen Sie einen Quelltyp in der Spalte **Quelltypname** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie im Formular „Quelltyp“ die zugehörige Liste **Aggregierte Protokollmuster** aus. Die Registerkarte zeigt die folgenden Daten für jedes Muster, das aus diesem Quelltyp extrahiert wurde. Die angezeigten Daten werden stündlich aktualisiert.

Zusammengefasste Protokollmuster

Spalte	Beschreibung
Mustertext	Der Inhalt des aggregierten Musters.
Quellen	Die Quellen, in denen das Muster angezeigt wurde.
Domäne	Die Domäne, zu der das Muster gehört.

Löschen Sie eine Protokollquelle

Löschen Sie eine Protokollquelle mit oder ohne die zugehörigen Protokolldaten in Health Log Analytics.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie eine Protokollquelle löschen, löscht Health Log Analytics automatisch die zugehörigen Protokolldaten. Sie können eine Quelle auch löschen, während Sie die Protokolldaten beibehalten. Die zugehörigen Daten werden dann gemäß der Protokollaufbewahrungsrichtlinie gelöscht. Weitere Informationen finden Sie unter Speicherplatz für die Protokollaufbewahrung in Health Log Analytics.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Protokollquellen**.
2. Öffnen Sie einen Quelldatensatz.
3. Löschen Sie die Protokollquelle auf eine der folgenden Arten:
   - Löschen Sie die Quelle und die zugehörigen Daten, indem Sie **Löschen**wählen.
   - Löschen Sie die Quelle ohne die zugehörigen Daten, indem Sie den zugehörigen Link **Ohne Protokolle löschen** auswählen.

Ändern Sie die Dateneingabekonfigurationen

Ändern Sie die Konfiguration einer Dateneingabe für Health Log Analytics, indem Sie einen neuen Pfad zu einer vorhandenen Dateneingabekonfiguration hinzufügen oder das MID-Server-Ziel und den Port der Dateneingabe ändern.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Öffnen Sie einen Datensatz aus der Tabelle der Dateneingaben.
3. Bearbeiten Sie die Konfiguration der Dateneingabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Name	Name der Dateneingabe
Beschreibung	Beschreibung der Dateneingabe
Port	Port auf dem MID-Server. **Hinweis:** Der Port darf nicht von einem anderen Prozess belegt sein. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet.
MID	Der MID-Server, an den die Protokolle gestreamt werden **Hinweis:** ◦ Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. ◦ Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern.

Einstellungen

Spalte	Beschreibung
Pfad	Der vollständige Pfad, aus dem Protokolle gestreamt werden sollen. Sie können einen Platzhalter verwenden. **Hinweis:** Diese Spalte ist in Windows-Systemen, in denen Winlogbeat verwendet wird, nicht verfügbar.
Service Instanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
Komponente	Gerätetyp oder Stapelebene als Kontext für die Protokolle, die zur Anomalieerkennung und -korrelation verwendet werden. Beispiel: Tomcat. Komponenten stellen normalerweise CIs in der CMDB dar. Mehrere Komponenten sind häufig in einer einzigen Serviceinstanzzusammengefasst.
Quelltyp	Quelltyp, der definiert, wie Health Log Analytics eine bestimmte Anwendung behandelt und die Protokolldaten analysiert. Beispiel: Tomcat Catalina. Jede Dateneingabe kann je nach Vielfalt ihrer Protokollformate mehrere Quelltypen haben. Serviceinstanzen und -komponenten können eine beliebige Anzahl von Quelltypen aufweisen.
Nur zur Verarbeitung mehrzeiliger Nachrichten in Linux-/Windows-Systemen mit Filebeat:	
Match (Übereinstimmung)	Gibt an, wie Filebeat übereinstimmende Zeilen zu einem Event kombiniert, entweder **nach** oder **vor**.
Negieren	Boolescher Wert, der definiert, ob das in den Protokollzeilen identifizierte Muster negiert wird. Der Standardwert ist **false**.
Regulärer Ausdruck	Der entsprechende reguläre Ausdruck

Hinweis: Sie können die Rsyslog-Konfigurationsdatei ändern, damit der Agent zusätzlich zu den Anwendungsprotokollen Systemprotokolle versendet. Weitere Informationen finden Sie im Artikel Shipping system logs using Rsyslog (Übermittlung von Systemprotokollen mit Rsyslog) [KB0954507] in der Knowledge Base des Now Support.

4. Wählen Sie **Aktualisieren**.
5. Erstellen Sie für Dateneingaben, die nur Rsyslog- oder Beats-Agents verwenden, die serverseitige Konfigurationsdatei neu, und installieren Sie sie auf dem Endpunktgerät.
   a. Wählen Sie **Rebuild configuration file** (Konfigurationsdatei neu erstellen) aus.

      Health Log Analytics erstellt die Datei neu und speichert sie im Abschnitt „Manage Attachments“ (Anhänge verwalten). Abhängig vom verwendeten Agent wird die neu erstellte Datei als `rsyslog.yml`, `filebeat.yml` oder `winlogbeat.yml` gespeichert.

      Das System benennt die vorherige Konfigurationsdatei automatisch um, indem ein Suffix mit Datum und Uhrzeit an den Dateinamen angehängt wird. Damit wird angegeben, wann die Datei neu erstellt wurde.

   b. Installieren Sie die neu erstellte Konfigurationsdatei auf dem Endpunkt entsprechend Ihrem Dateneingabetyp.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dateneingabetyp	Aktion
Rsyslog	**i.** Laden Sie die Datei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis `/etc/rsyslog.d/rsyslog.conf`. **ii.** Validieren Sie die Konfiguration, indem Sie den Befehl `rsyslogd -N1` ausführen. **iii.** Überprüfen Sie die Ausgabe. Wenn die Systemprotokolldatei `/var/log/messages` Fehler enthält, prüfen und beheben Sie die Fehlermeldungen. **iv.** Starten Sie Rsyslog neu, indem Sie den Befehl `sudo systemctl restart rsyslog` ausführen.
Linux	**i.** Laden Sie die Datei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis `/etc/filebeat/`. **ii.** Starten Sie den Agent-Service neu, indem Sie den Befehl `sudo service filebeat restart` ausführen. **Hinweis:** Die generierte Konfiguration ignoriert Dateien, die zuletzt vor mehr als sechs Stunden geändert wurden. Bei Bedarf können Sie diese Einstellung in der Konfigurationsdatei ändern.
Windows mit Beats (Filebeat oder Winlogbeat):	**i.** Laden Sie die Datei herunter, und installieren Sie sie auf dem Endpunktgerät im Verzeichnis `C:\Programme\`. **ii.** Starten Sie den Agent-Service neu, indem Sie den entsprechenden PowerShell-Befehl ausführen: ▪ Filebeat: `PS > Restart-Service filebeat` ▪ Winlogbeat: `PS > Restart-Service winlogbeat` **Hinweis:** Die generierte Konfiguration ignoriert Dateien, die zuletzt vor mehr als sechs Stunden geändert wurden. Bei Bedarf können Sie diese Einstellung in der Konfigurationsdatei ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erweiterte Einstellungen für Rsyslog-, Splunk- oder TCP-Dateneingaben konfigurieren

Erweiterte Einstellungen für Beats-Dateneingaben konfigurieren

Konfiguration der erweiterten Dateneingabe

Wenn Sie eine Dateneingabe erfolgreich konfiguriert haben, fügt Health Log Analytics der entsprechenden Tabelle einen Datensatz hinzu und hängt die Konfigurationsdatei an. Für Ihre Dateneingabe können Sie erweiterte Einstellungen konfigurieren. Die Konfiguration von erweiterten Einstellungen ist optional.

Erweiterte Einstellungen für Rsyslog-, Splunk- oder TCP-Dateneingaben konfigurieren

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben, die Rsyslog-, Splunk- oder TCP-Agents verwenden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Weitere Informationen zum Ändern der Einstellungen, die beim Erstellen der Dateneingabe konfiguriert wurden, wie das Hinzufügen eines neuen Pfads oder das Ändern des MID-Server-Ziels oder Ports der Dateneingabe, finden Sie unter Ändern Sie die Dateneingabekonfigurationen.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Öffnen Sie einen Rsyslog-, Splunk- oder TCP-Dateneingabe-Datensatz aus der Dateneingabentabelle.

   Die Dateneingabe-Konfiguration wird angezeigt.

   Hinweis: Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben, wird im Feld **Quellenanzahl** angezeigt. Weitere Informationen zu Dateneingabequellen finden Sie unter Automatische Zuordnung und Zuordnung von Protokolldaten.

   Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

3. Wählen Sie **Erweitert** aus.
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Rsyslog, Filebeat- oder Winlogbeat-Dateneingabe-Konfigurationsfelder.
5. Wahlweise: Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen zu Streaming-Quellen finden Sie unter Probleme beim Protokoll-Streaming identifizieren und beheben.

6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

     Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Erweiterte Einstellungen für Beats-Dateneingaben konfigurieren

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben, die Beats-Agents verwenden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die beim MID-Server eintreffenden Protokolldaten ausführt. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Weitere Informationen zum Ändern der Einstellungen, die beim Erstellen der Dateneingabe konfiguriert wurden, wie das Hinzufügen eines neuen Pfads oder das Ändern des MID-Server-Ziels oder Ports der Dateneingabe, finden Sie unter Ändern Sie die Dateneingabekonfigurationen.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben protokollieren**.
2. Öffnen Sie den Datensatz einer Beats-Dateneingabe aus der Dateneingabentabelle.
   Die Dateneingabe-Konfiguration wird angezeigt.

   Hinweis: Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben, wird im Feld **Quellenanzahl** angezeigt. Weitere Informationen zu Dateneingabequellen finden Sie unter Automatische Zuordnung und Zuordnung von Protokolldaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

3. Wählen Sie **Erweitert** aus.
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Rsyslog, Filebeat- oder Winlogbeat-Dateneingabe-Konfigurationsfelder.
5. Wahlweise: Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Probleme beim Protokoll-Streaming identifizieren und beheben.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

     Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Zugehörige Informationen

Konfigurieren Sie Rsyslog- , Filebeat- oder Winlogbeat-Dateneingaben

Erweiterte Einstellungen für Elasticsearch-Dateneingaben konfigurieren

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten von Elasticsearch-Indizes an Ihre Instanz.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Weitere Informationen zu Streaming-Protokollen mit der Elasticsearch-Dateneingabe finden Sie im Artikel Stream logs using Elasticsearch data input – Advanced Guide [KB1080162] (Protokolle mit Elasticsearch-Dateneingabe streamen - Erweiterte Anleitung) in der Now Support-Knowledge Base.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben protokollieren**.
2. Öffnen Sie den Datensatz einer Elasticsearch-Dateneingabe aus der Dateneingabentabelle.
   Die Dateneingabe-Konfiguration wird angezeigt.

   Hinweis: Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben, wird im Feld **Quellenanzahl** angezeigt. Weitere Informationen zu Dateneingabequellen finden Sie unter Automatische Zuordnung und Zuordnung von Protokolldaten.

   Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Elasticsearch Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Probleme beim Protokoll-Streaming identifizieren und beheben.

   Hinweis: Wenn Sie Probleme mit Berechtigungen beim Streaming von Protokolldaten von Elasticsearch haben, lesen Sie den Artikel Granting privileges for data streams from Elasticsearch [KB0967366] (Berechtigungen für Datenströme von Elasticsearch erteilen) in der Now Support-Knowledge Base.

6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
- Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

  Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

  Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Zugehörige Informationen

Elasticsearch-Dateneingaben konfigurieren

Erweiterte Einstellungen für MID-Server-Dateneingaben konfigurieren

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben, die zum Sammeln und Streamen von MID-Server-Protokollnachrichten verwendet werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben protokollieren**.
2. Öffnen Sie den Datensatz einer MID-Server-Dateneingabe aus der Dateneingabentabelle. Die Dateneingabe-Konfiguration wird angezeigt.

   Hinweis: Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben, wird im Feld **Quellenanzahl** angezeigt. Weitere Informationen zu Dateneingabequellen finden Sie unter Automatische Zuordnung und Zuordnung von Protokolldaten.

   Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

3. Wählen Sie **Erweitert** aus.
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter MID-Server Konfigurationsfelder für die Dateneingabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wahlweise: Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt. Weitere Informationen zu Streaming-Quellen finden Sie unter Probleme beim Protokoll-Streaming identifizieren und beheben.
6. Wählen Sie **Aktualisieren**.

Ergebnisse
Health Log Analytics aktualisiert die Systemparameter.

Zugehörige Informationen

MID-Server-Dateneingaben konfigurieren

Erweiterte Einstellungen für Amazon CloudWatch-Dateneingaben konfigurieren

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten aus Amazon CloudWatch an Ihre Instanz.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Prozedur
1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Öffnen Sie den Datensatz einer Amazon CloudWatch-Dateneingabe aus der Dateneingabentabelle.

   Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Amazon CloudWatch Konfigurationsfelder für die Dateneingabe.

   Das Feld **Zeichencodierung** ist schreibgeschützt. Standardmäßig lautet die für diese Dateneingabe verwendete Zeichenkodierung UTF-8.

5. Wahlweise: Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt. Weitere Informationen zu Streaming-Quellen finden Sie unter Probleme beim Protokoll-Streaming identifizieren und beheben.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

- Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
- Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Zugehörige Informationen

Amazon CloudWatch-Dateneingaben konfigurieren

Erweiterte Einstellungen für Amazon S3-Dateneingaben konfigurieren

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten von Amazon S3-Buckets an Ihre Instanz.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben protokollieren**.
2. Öffnen Sie den Datensatz einer Amazon S3-Dateneingabe aus der Dateneingabentabelle.

Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldbeschreibungen finden Sie unter Amazon S3 Konfigurationsfelder für die Dateneingabe.

5. Wahlweise: Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt. Weitere Informationen zu Streaming-Quellen finden Sie unter Probleme beim Protokoll-Streaming identifizieren und beheben.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Zugehörige Informationen

Amazon S3-Dateneingaben konfigurieren

Erweiterte Einstellungen für Microsoft Azure Log Analytics-Dateneingaben konfigurieren

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten aus Microsoft Azure Log Analytics an Ihre Instanz.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Öffnen Sie den Datensatz einer Microsoft Azure Log Analytics-Dateneingabe aus der Dateneingabentabelle.

   Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Log Analytics Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Probleme beim Protokoll-Streaming identifizieren und beheben.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Zugehörige Informationen

Microsoft Azure Log Analytics-Dateneingaben konfigurieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen für Microsoft Azure Event Hubs-Dateneingaben konfigurieren

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten aus Microsoft Azure Event Hubs an Ihre Instanz.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Öffnen Sie den Datensatz einer Microsoft Azure Event Hubs-Dateneingabe aus der Dateneingabentabelle.

   Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Microsoft Azure Event Hubs Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Probleme beim Protokoll-Streaming identifizieren und beheben.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Zugehörige Informationen

Microsoft Azure Event Hubs-Dateneingaben konfigurieren

Erweiterte Einstellungen für Apache Kafka-Dateneingaben konfigurieren

Konfigurieren Sie erweiterte Einstellungen für Dateneingaben für das Streaming von Protokolldaten aus Apache Kafka an Ihre Instanz.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können Systemparameter zum Lesen von Protokolldaten festlegen, um Aktionen festzulegen, die das System für die Protokolldaten ausführt, die auf dem MID-Server eintreffen. Sie können beispielsweise die zu verwendende Zeitzone festlegen, wenn ein Protokoll keinen Zeitstempel enthält. Wenn keine erweiterten Einstellungen konfiguriert sind, verwendet das System die Standardwerte.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben protokollieren**.
2. Öffnen Sie den Datensatz einer Apache Kafka-Dateneingabe aus der Dateneingabentabelle.

   Hinweis: Wenn die KI-Engine Health Log Analytics ausgefallen ist und das Streaming von Daten beendet wurde, wird oben auf der Konfigurationsseite für die Dateneingabe eine Benachrichtigung angezeigt. Wenden Sie sich in diesem Fall an den Support ServiceNow.

3. Wählen Sie **Advanced** (Erweitert) und dann die Registerkarte **Advanced** (Erweitert).
4. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter Apache Kafka Konfigurationsfelder für die Dateneingabe.
5. Wahlweise: Überprüfen Sie in der zugehörigen Liste „Streamingquellen“, ob diese Dateneingabe Protokolldaten aus allen relevanten Endpunktgeräten streamt.
   Weitere Informationen zu Streaming-Quellen finden Sie unter Probleme beim Protokoll-Streaming identifizieren und beheben.
6. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
7. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Dateneingabe für die Ausführung in einem MID-Server -Cluster konfiguriert ist, versucht das System, alle MID Servers im Cluster mit dem Repository zu verbinden. Der Cluster besteht den Test, wenn mindestens einer seiner MID Servers verbunden wird. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

- Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
- Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

8. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Zugehörige Informationen

Apache Kafka-Dateneingaben konfigurieren

Health Log Analytics Inhaltspakete für eine schnellere Amortisierungszeit

Verkürzen Sie die Onboarding-Zeit für die Anwendung Health Log Analytics durch die Installation von Inhaltspaketen. Die Pakete enthalten Standardquelltypen und Zuordnungsskriptvorlagen, mit denen Sie Zeit sparen, um sie von Grund auf neu erstellen zu können.

Nach der Installation eines Inhaltspakets beginnt Health Log Analytics sofort mit dem Streamen und Analysieren Ihrer Protokolldaten. Die Anwendung erkennt und analysiert die -Daten, generiert relevantere Warnungen und reduziert das Rauschen ab dem Zeitpunkt der Integration. Sie können die Zuordnungskonfiguration später noch bei Bedarf anpassen.

Sie können Inhaltspakete auf zwei verschiedene Arten integrieren:

- Wählen Sie ein Inhaltspaket aus, wenn Sie eine Dateneingabe konfigurieren. Health Log Analytics aktiviert das ausgewählte Paket automatisch und verwendet das zugehörige Zuordnungsskript für die Zuordnung der Dateneingabequellen.
- Aktivieren Sie ein Inhaltspaket, bevor Sie eine Dateneingabe konfigurieren. Wenn Sie die Dateneingabe konfiguriert haben und die Rohprotokolldaten zuordnen, wählen Sie das Zuordnungsskript des Inhaltspakets im Formular **„Dateneingabezuordnung“** aus.

Derzeit ist ein Inhaltspaket zum Streamen von Protokollen von Linux mithilfe von Filebeatverfügbar.

Hinweis: Alle Konfigurationen in Inhaltspaketen sind in der globalen Domäne vorhanden. Wenn Sie Domain Separation verwenden, ist der Inhalt des Inhaltspakets nur für Protokolle in der globalen Domäne verfügbar.

Diese Funktion wird in der Anwendung Health Log Analytics, Version 25.0.17 – November 2022 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhaltspaket in Health Log Analyticsaktivieren

Sie können ein Inhaltspaket aktivieren, bevor Sie eine Dateneingabe konfigurieren.

Vorbereitungen

Eine Übersicht über diese Funktion finden Sie unter Health Log Analytics Inhaltspakete für eine schnellere Amortisierungszeit.

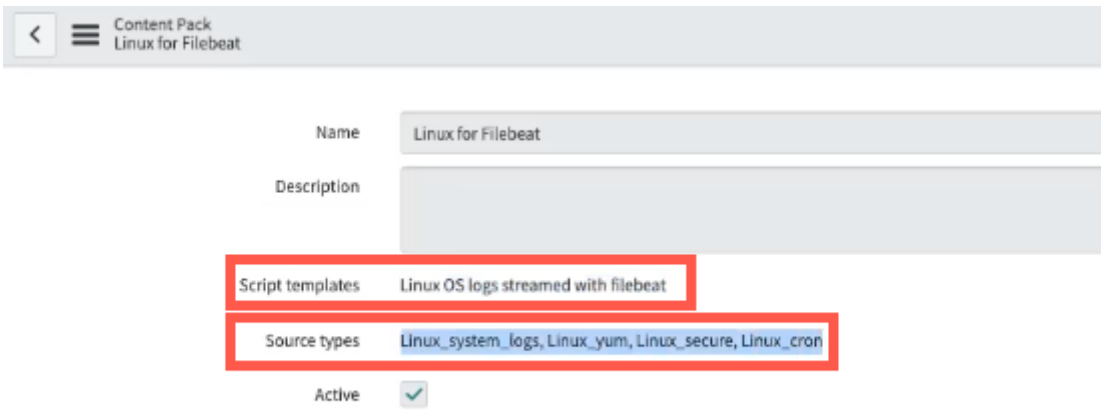
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Inhaltspakete**.
2. Öffnen Sie das entsprechende Inhaltspaket für Ihre Dateneingabe.

   Hinweis: Derzeit ist ein Inhaltspaket zum Streamen von Protokollen von Linux mithilfe von Filebeatverfügbar.

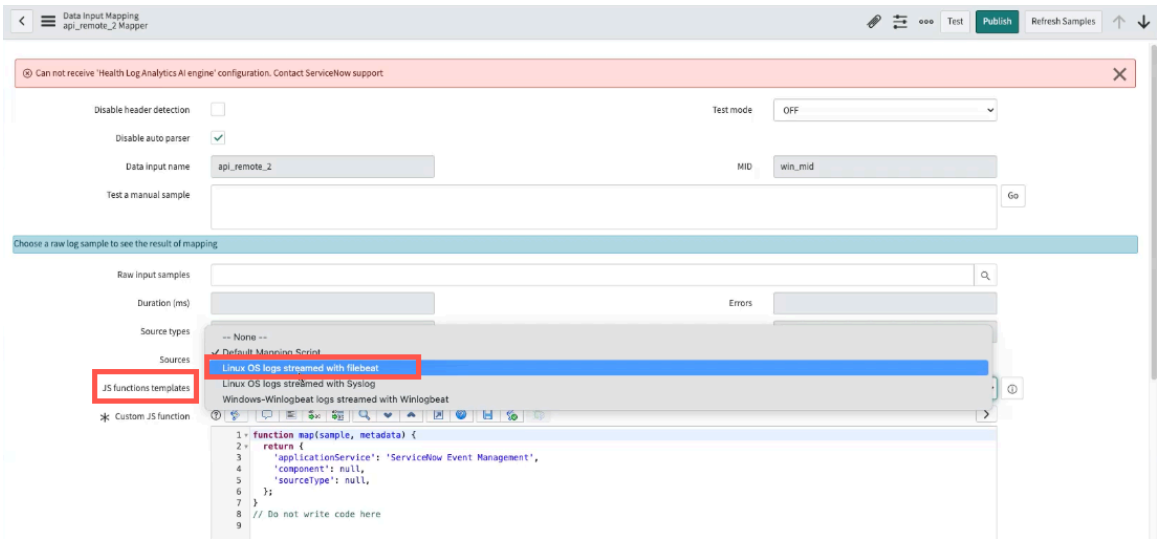
3. Wählen Sie im Formular **„Inhaltspaket“Aktivieren aus**.
   Das Kontrollkästchen **Aktiv** wird aktiviert angezeigt. Das aktivierte Inhaltspaket zeigt die zugehörigen Skriptvorlagen und Quelltypen an.



Hinweis: Die im Inhaltspaket enthaltenen Quelltypen sind möglicherweise bereits in Ihrer Instanz ServiceNow vorhanden. In diesem Fall benennt Health Log Analytics die Inhaltspaket-Quelltypen automatisch um, indem ihrem Namen ein Inhaltspaket-Suffix hinzugefügt wird. Wenn Sie die Quelltypen des Inhaltspakets und ihre Zuordnung verwenden möchten, löschen Sie die ursprünglichen Quelltypen, oder benennen Sie sie um, und entfernen Sie dann das Suffix aus den Quelltypen des Inhaltspakets. Andernfalls verwendet Health Log Analytics die ursprünglichen Quelltypen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Formular **„Dateneingabezuordnung“** wird das Zuordnungsskript als Vorlagenoption für JavaScript-Funktionen aufgeführt.



Nächste Maßnahme

Wenn Sie die Dateneingabe konfiguriert haben und Ihre Rohprotokolldaten zuordnen, können Sie das Zuordnungsskript des Inhaltspakets in der Dropdownliste **JS-Funktionsvorlagen** auswählen.

Dateneingabe in beenden oder neu starten Health Log Analytics

Sie können die Verwendung einer Dateneingabe zum Streamen von Protokollnachrichten an Ihre Instanz ServiceNow beenden. Starten Sie die Dateneingabe neu, wenn das Streaming von Daten fortgesetzt werden soll.

Vorbereitungen

Diese Funktionalität ist nur verfügbar, wenn die Dateneingabekonfiguration veröffentlicht wurde.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben protokollieren**.
2. Öffnen Sie den Datensatz einer Dateneingabe aus der Dateneingabentabelle.
3. Klicken Sie auf **Stop Data Input** (Dateneingabe anhalten).
   Der Name der Schaltfläche ändert sich in **Start Data Input** (Dateneingabe starten).
4. Um die Dateneingabe erneut zu verwenden, klicken Sie auf **Start Data Input** (Dateneingabe starten).

Health Log Analytics -Dateneingabekonfigurationen werden zwischen Instanzen migriert

Exportieren Sie eine Health Log Analytics -Dateneingabe- und Quelltypkonfiguration als Update Set, und importieren Sie sie in eine andere ServiceNow -Instanz. In der Zielumgebung können Sie die migrierte Dateneingabe zum Streaming und Verarbeiten von Protokolldaten verwenden. Diese Funktionalität spart Zeit und reduziert mögliche Fehler, indem Sie vermeiden, dass die Einstellungen in der Zielinstanz erneut konfiguriert werden müssen.

Die migrierte Konfiguration umfasst die Zuordnung und alle anderen relevanten Einstellungen mit Ausnahme der Anmeldeinformationen. Abhängig von der Dateneingabe, die Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

exportieren, müssen Sie möglicherweise die Anmeldeinformationen in der Zielumgebung konfigurieren. Wenn Sie beispielsweise Amazon CloudWatch- oder Amazon S3-Dateneingaben exportieren, müssen Sie Amazon Web Services (AWS)-Anmeldeinformationen konfigurieren.

Diese Funktion wird in der Anwendung Health Log Analytics, Version 25.0.17 – November 2022 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

Hinweis: Wenn Sie die HLA-Konfigurationsmigration mit Now Platform -Versionen vor Release Tokyo verwenden möchten, müssen Sie ein Update Set importieren. Weitere Informationen finden Sie im Artikel HLA Configuration Migration Enablement [KB1274850] in der Knowledge Base Now Support.

Allgemeine Informationen zu Update-Sätzen im Now Platformfinden Sie unter System-Update-Sätze .

Exportieren Sie eine Dateneingabekonfiguration

Exportiert die Konfiguration einer Health Log Analytics -Dateneingabe mit oder ohne die zugehörigen Quelltypen in einen Update-Satz. Anschließend können Sie das Update Set in die Zielumgebung importieren.

Vorbereitungen

Eine Übersicht über diese Funktion finden Sie unter Health Log Analytics -Dateneingabekonfigurationen werden zwischen Instanzen migriert.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Dateneingaben**.
2. Wählen Sie in der Liste „Dateneingaben“ die Dateneingabe aus, die Sie exportieren möchten.
3. Exportieren Sie die Dateneingabe in einen Update-Satz.

   Hinweis: Die exportierte Konfiguration enthält nicht die Serviceinstanz, die für die Dateneingabe konfiguriert ist.

   a. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilendie Option Dateneingabe exportieren aus**.

   b. Führen Sie im Dialogfeld **„Dateneingabe exportieren“** eine der folgenden Aktionen aus:

   - Lassen Sie das Kontrollkästchen aktiviert, um die Quelltypen einzuschließen, die der Dateneingabe im Update Set zugeordnet sind.

     Wenn das Kontrollkästchen aktiviert ist, enthält das Update Set die folgenden Tabellen für den Quelltyp:

     - sn_occ_source_type
     - sn_occ_source_type_structure
     - sn_occ_sources
     - sn_occ_timestamp_formats
     - sn_occ_lexical_keywords
     - sn_occ_log_correlator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- sn_occ_log_source_retention
- sn_occ_quick_replacements
- sn_occ_reconstructors
- sn_occ_replacements

- Deaktivieren Sie das Kontrollkästchen, um die Dateneingabe ohne die zugehörigen Quelltypen zu exportieren. Dies ist beispielsweise der Fall, wenn Sie die Dateneingabekonfiguration wiederverwenden, die Quelltypen jedoch von Grund auf neu konfigurieren möchten.

  Wenn das Feld leer ist, enthält das Update Set die oben aufgeführten Tabellen für den Quelltyp nicht.

  Hinweis: Sie können Quelltypen separat exportieren. Weitere Informationen finden Sie unter Exportieren Sie Quelltypen in einen Update-Satz.

c. Wählen Sie **Fortsetzen**.

Die Dateneingabe wird mit oder ohne Quelltypen in ein Update Set exportiert.

Hinweis: Ein Update Set kann als übergeordnetes Element für mehrere untergeordnete Update Sets fungieren.

4. Wählen Sie **Update Set herunterladen** aus, um das Update Set auf die Instanz herunterzuladen.
Das Update Set wird als XML-Datei heruntergeladen.

Nächste Maßnahme
Importieren Sie das Update Set in die erforderliche Instanz ServiceNow. Weitere Informationen finden Sie unter Importieren Sie eine Dateneingabe in eine Zielinstanz.

Importieren Sie eine Dateneingabe in eine Zielinstanz

Importieren Sie eine Dateneingabekonfiguration Health Log Analytics, die Sie aus einer anderen Instanz als Update Set exportiert haben.

Vorbereitungen
Eine Übersicht über diese Funktion finden Sie unter Health Log Analytics -Dateneingabekonfigurationen werden zwischen Instanzen migriert.

Exportieren Sie die Dateneingabe in ein Update Set, bevor Sie dieses Verfahren durchführen. Weitere Informationen finden Sie unter Exportieren Sie eine Dateneingabekonfiguration.

Erforderliche Rolle: Administrator

Prozedur

1. Importieren Sie in der Zielinstanz das Update Set, das die Dateneingabekonfiguration enthält.

a. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.

b. Wählen Sie unter Zugehörige Links **Update Set aus XML importieren aus**.

c. Wählen Sie **Datei auswählen** aus, und öffnen Sie die XML-Datei des Update-Satzes im Ordner „Downloads“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie **Hochladen** aus.
Das Update Set wird in die Instanz hochgeladen und erscheint in der Liste **der abgerufenen Update Sets** im Status Geladen.

2. Identifizieren und beheben Sie Fehler im Update Set.

a. Öffnen Sie in der Liste **der abgerufenen Update-Sätze** den Update-Satz-Datensatz.

b. Wählen Sie **Vorschau auf Update-Satz-Batch anzeigen,** um Fehler zu erkennen.
Im Dialogfeld **„Batch-Update-Satz-Vorschau“** wird ein Fehler angezeigt. Dies ist das erwartete Verhalten.

c. Schließen Sie das Dialogfeld, und beheben Sie die Fehler in der zugehörigen Liste **„Probleme bei der Update-Satz-Vorschau“**.

Weitere Informationen finden Sie unter Vorschau auf Remote-Update Set anzeigen .

Sie können Fehler, die mit „In [Tabelle] konnte kein Datensatz gefunden werden“ beginnen, für die folgenden Tabellen ignorieren:

- AWS_Credentials
- azure_sas_credentials
- azure_service_principal
- standard_auth_credentials
- cmdb_ci_service_auto – Service Instanz
- ecc_agent: MID
- ecc_agent_cluster: MID-Server-Cluster
- kafka_ssl_credentials
- sn_occ_data_input_preprocess_example
- sn_occ_data_input_preprocess_example_row
- sn_occ_gcp_credentials
- sn_occ_mapper_example
- sn_occ_source_type_examples
- sn_occ_source_type_structure_data

d. Wählen Sie die Fehler aus, die Sie ignoriert haben, und aktivieren Sie dann das Kontrollkästchen **Alle auswählen**.

e. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen... dieOption Remote-Aktualisierung akzeptieren aus**.

f. Wählen Sie in der zugehörigen Liste **Vorschauprobleme für Batch** alle verbleibenden Fehler aus, und akzeptieren Sie das Remote-Update, wie in den vorherigen Schritten beschrieben.

3. Wenn alle Fehler im Update Set behoben wurden, wählen Sie **Commit Update Set Batch (Update-Satz-Batch**festlegen) aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die importierte Dateneingabe wird in der Liste der Dateneingaben angezeigt. Der Import enthält Zuordnungseinstellungen und alle anderen relevanten Konfigurationen.

4. Konfigurieren Sie in der importierten Dateneingabe Folgendes.
   - Der MID-Server, an den die Protokolle gestreamt werden
   - Anmeldeinformationen.

     Hinweis: Ob Sie Anmeldeinformationen konfigurieren müssen, hängt von der Dateneingabe ab, die Sie importiert haben. Beispielsweise müssen Sie Amazon Web Services (AWS)-Anmeldeinformationen für die Dateneingaben Amazon CloudWatch und Amazon S3 konfigurieren.

   - (Optional) Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen.

   Weitere Informationen finden Sie in der Konfigurationsdokumentation für die relevante Dateneingabe: Richten Sie Dateneingaben für Health Log Analytics manuell ein.

Ergebnisse
Sie können die Dateneingabe für das Streaming und die Verarbeitung von Protokolldaten verwenden.

Exportieren Sie Quelltypen in einen Update-Satz

Exportieren Sie Quelltypen in einen Update-Satz, der von der Dateneingabekonfiguration Health Log Analytics getrennt ist. Anschließend können Sie das Update Set in die Zielumgebung importieren.

Vorbereitungen
Eine Übersicht über diese Funktion finden Sie unter Health Log Analytics -Dateneingabekonfigurationen werden zwischen Instanzen migriert.

Erforderliche Rolle: evt_mgmt_admin

Prozedur
1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Quelltypen**.
2. Wählen Sie in der Liste der Quelltypen mindestens einen Quelltyp aus, den Sie exportieren möchten.
3. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilendie Option Exportquelltypen**aus.
   Die Quelltypen werden in ein Update Set exportiert.

   Hinweis: Ein Update Set kann als übergeordnetes Element für mehrere untergeordnete Update Sets fungieren.

4. Wählen Sie **Update Set herunterladen** aus, um das Update Set auf die Instanz herunterzuladen.
   Das Update Set wird als XML-Datei heruntergeladen.

Nächste Maßnahme
Importieren Sie das Update Set in die erforderliche Instanz ServiceNow. Weitere Informationen finden Sie unter Importieren Sie Quelltypen in eine Zielinstanz.

Importieren Sie Quelltypen in eine Zielinstanz

Importieren Sie Quelltypen, die Sie getrennt von der Dateneingabekonfiguration Health Log Analytics exportiert haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Eine Übersicht über diese Funktion finden Sie unter Health Log Analytics -Dateneingabekonfigurationen werden zwischen Instanzen migriert.

Exportieren Sie die Quelltypen in ein Update Set, bevor Sie dieses Verfahren durchführen. Weitere Informationen finden Sie unter Exportieren Sie Quelltypen in einen Update-Satz.

Erforderliche Rolle: Administrator

Prozedur

1. Importieren Sie in der Zielinstanz das Update Set, das die Quelltypen enthält.

   a. Navigieren zu **Alle** > **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.

   b. Wählen Sie unter Zugehörige Links **Update Set aus XML importieren aus**.

   c. Wählen Sie **Datei auswählen** aus, und öffnen Sie die XML-Datei des Update-Satzes im Ordner „Downloads“.

   d. Wählen Sie **Hochladen** aus.
   Das Update Set wird in die Instanz hochgeladen und erscheint in der Liste **der abgerufenen Update Sets** im Status Geladen.

2. Identifizieren und beheben Sie Fehler im Update Set.

   a. Öffnen Sie in der Liste **der abgerufenen Update-Sätze** den Update-Satz-Datensatz.

   b. Wählen Sie **Vorschau auf Update-Satz-Batch anzeigen**, um Fehler im Update Set zu erkennen.
   Im Dialogfeld **„Batch-Update-Satz-Vorschau“** wird ein Fehler angezeigt. Dies ist das erwartete Verhalten.

   c. Schließen Sie das Dialogfeld, und beheben Sie die Fehler in der zugehörigen Liste **„Probleme bei der Update-Satz-Vorschau“**.
   Sie können Fehler, die mit „In [Tabelle] konnte kein Datensatz gefunden werden“ beginnen, für die folgenden Tabellen ignorieren:

   d. Wählen Sie die Fehler aus, die Sie ignoriert haben, und aktivieren Sie dann das Kontrollkästchen **Alle auswählen**.

   e. Wählen Sie im Dropdown-Menü **Aktionen für ausgewählte Zeilen... dieOption Remote-Aktualisierung akzeptieren aus**.

   f. Wählen Sie in der zugehörigen Liste **Vorschauprobleme für Batch** alle verbleibenden Fehler aus, und akzeptieren Sie das Remote-Update, wie in den vorherigen Schritten beschrieben.

3. Wenn alle Fehler im Update Set behoben wurden, wählen Sie **Commit Update Set Batch (Update-Satz-Batch**festlegen) aus.

Ergebnisse

Die importierten Quelltypen werden in der Liste Quelltypen angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überprüfen Sie gRPC und Netzwerkkonnektivität auf der MID-Server

Stellen Sie sicher, dass Health Log Analytics ordnungsgemäß funktioniert, indem Sie Diagnosetests auf MID-Server durchführen, um gRPC und die Netzwerkkonnektivität zu überprüfen.

Vorbereitungen

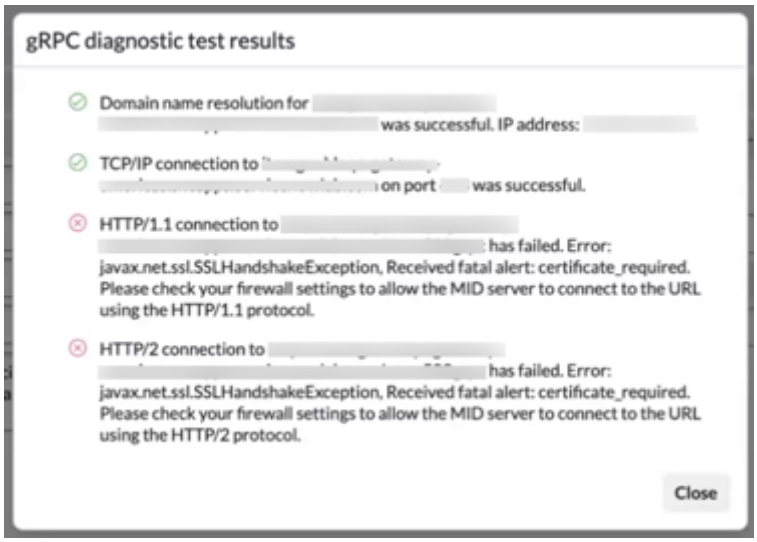
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die Netzwerk- und Sicherheitskonfiguration Ihrer Organisation führt möglicherweise dazu, dass Health Log Analytics nicht ordnungsgemäß funktioniert. Beispielsweise können komplexe Konfigurationen mit Proxy- und Firewall-Einstellungen ausgehende Verbindungen blockieren. Um Betriebsprobleme zu vermeiden, können Sie gRPC und die Netzwerkkonnektivität auf der Seite MID-Servertesten.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Server**.
2. Öffnen Sie den relevanten Datensatz MID-Server.
3. Wählen Sie unter „Zugehörige Links“ **gRPC-Verbindung testen aus**.
   Das System führt gRPC-Konnektivitätstests durch, z. B. Auflösung von Domänennamen, TCP/IP und HTTP-Verbindung. Wenn der Test abgeschlossen ist, werden die Testergebnisse angezeigt. Erfolgreichen Tests geht ein grünes Häkchen voran, fehlgeschlagenen Tests ein rotes x.



4. Beheben Sie die Probleme, die zum Fehlschlagen von Tests geführt haben, indem Sie die Anweisungen auf dem Bildschirm **mit den Ergebnissen des gRPC-Diagnosetests** befolgen.
5. Wählen Sie erneut **GRPC-Verbindung testen** aus, und bestätigen Sie, dass alle Tests erfolgreich abgeschlossen wurden.

Health Log Analytics verwalten

Dieser Abschnitt behandelt Aufgaben im Zusammenhang mit der Verwaltung von Health Log Analytics. Es stellt Systemadministratoren die erforderlichen Informationen bereit, damit Health Log Analytics effizient läuft.

Health Log Analytics-Systemeigenschaften für eine einzelne Protokollquelle konfigurieren

Konfigurieren Sie Systemeigenschaften für eine bestimmte Protokollquelle, wenn Sie die Standardwerte ändern müssen. Normalerweise sollte das nicht erforderlich sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Das Ändern der Health Log Analytics-Systemeigenschaften wirkt sich auf Back-end-Prozesse aus und kann zu unerwarteten Ergebnissen führen. Wenn Sie diese Eigenschaften ändern müssen, sollten Sie daher Ihre Anpassungen dokumentieren. Notieren Sie sich beispielsweise den Wert vor und nach einer Änderung und den Zeitpunkt der Änderung.

Hinweis: Um eine Health Log Analytics -Systemeigenschaft zu ändern, deren Wert **„Neustart erforderlich“** auf **„true“**festgelegt ist, wenden Sie sich an den Support von ServiceNow, um dies für Sie zu ändern.

Eine vollständige Beschreibung aller Health Log Analytics -Systemeigenschaften finden Sie im Artikel HLA-Systemeigenschaften [KB0869842] in der Knowledge Base Now Support.

Prozedur
1. Navigieren zu **Alle** > **Health Log Analytics** > **Dateneingabe** > **Protokollquellen**.
2. Klicken Sie auf der Registerkarte **Source properties** (Quelleigenschaften) mit der rechten Maustaste auf eine Eigenschaft.
3. Wählen Sie im Popup-Menü **Override property value** (Eigenschaftswert überschreiben) aus.
4. Geben Sie im Feld **Value** (Wert) den entsprechenden Wert ein.
5. Wählen Sie **Absenden** aus.

Ergebnisse
Die vorherige Einstellung für die ausgewählte Protokollquelle wird mit dem neuen Wert überschrieben.

Zugehörige Informationen

Globale Health Log Analytics-Systemeigenschaften konfigurieren

Globale Health Log Analytics-Systemeigenschaften konfigurieren

Konfigurieren Sie globale Health Log Analytics -Systemeigenschaften, wenn Sie die Standardwerte ändern müssen, was normalerweise nicht erforderlich sein sollte.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Das Ändern der Health Log Analytics-Systemeigenschaften wirkt sich auf Back-end-Prozesse aus und kann zu unerwarteten Ergebnissen führen. Wenn Sie diese Eigenschaften ändern müssen, sollten Sie daher Ihre Anpassungen dokumentieren. Notieren Sie sich beispielsweise den Wert vor und nach einer Änderung und den Zeitpunkt der Änderung.

Hinweis: Um eine Health Log Analytics -Systemeigenschaft zu ändern, deren Wert **„Neustart erforderlich“** auf **„true“**festgelegt ist, wenden Sie sich an den Support von ServiceNow, um dies für Sie zu ändern.

Eine vollständige Beschreibung aller Health Log Analytics -Systemeigenschaften finden Sie im Artikel HLA-Systemeigenschaften [KB0869842] in der Knowledge Base Now Support.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Health Log Analytics-Verwaltung** > **Systemeigenschaften**.
2. Wählen Sie eine Eigenschaft mit dem Bereich „Source“ (Quelle) aus.
3. Geben Sie im Feld **Value** (Wert) den entsprechenden Wert ein.
4. Wählen Sie **Aktualisieren**.
   Die Einstellung gilt für Protokollquellen, die ab diesem Zeitpunkt erstellt werden.
5. Bestimmen Sie den Anwendungsbereich der neuen Einstellung.
   - Um die Einstellung nur auf Protokollquellen anzuwenden, die ab diesem Zeitpunkt erstellt werden, wählen Sie **Update** (Aktualisieren).
   - Um Werte für diese Eigenschaft in allen vorhandenen Protokollquellen zu überschreiben und die geänderte Einstellung auf alle neuen Protokollquellen anzuwenden, wählen Sie **Override source property** (Quelleigenschaft überschreiben).

Zugehörige Informationen

Health Log Analytics-Systemeigenschaften für eine einzelne Protokollquelle konfigurieren

Health Log Analytics-Systemfunktionen aktivieren oder deaktivieren

Passen Sie die Basiskonfiguration von Health Log Analytics an, indem Sie Systemfunktionen aktivieren oder deaktivieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Health Log Analytics-Verwaltung** > **Funktionen**.
   Standardmäßig zeigt die Tabelle die Systemfunktionen, die Administratoren am häufigsten ändern. Um die vollständige Liste der Funktionen anzuzeigen, verwenden Sie die Filteroptionen.
2. Wählen Sie in der Tabelle einen Funktionsdatensatz aus.
   Der Datensatz enthält die folgenden Informationen:
   - Name der Funktion
   - Beschreibung des Zwecks der Funktion
   - Standardstatus der Funktion
   - Aktueller Status der Funktion
3. Legen Sie den Status einer Systemfunktion auf EIN fest, um die Funktion zu aktivieren, bzw. auf AUS, um sie zu deaktivieren.
4. Wählen Sie **Aktualisieren**.

Warnungsbenachrichtigungen in Slack- oder Microsoft Teams-Kanälen

Von Health Log Analytics werden Benachrichtigungen für neue Anomaliewarnungen in Echtzeit an Slack- oder Microsoft Teams-Kanäle gesendet. Diese integrierte Funktionalität befreit Sie von der kontinuierlichen Überwachung von Protokollen, um Incidents zu vermeiden.

Die Benachrichtigungen enthalten die Nummer der Warnung, die Beschreibung, den Schweregrad, das zugehörige Konfigurationselement, den Status und die Prioritätsgruppe. Sie können die Warnungen filtern, für die Benachrichtigungen an Ihren Kanal gesendet

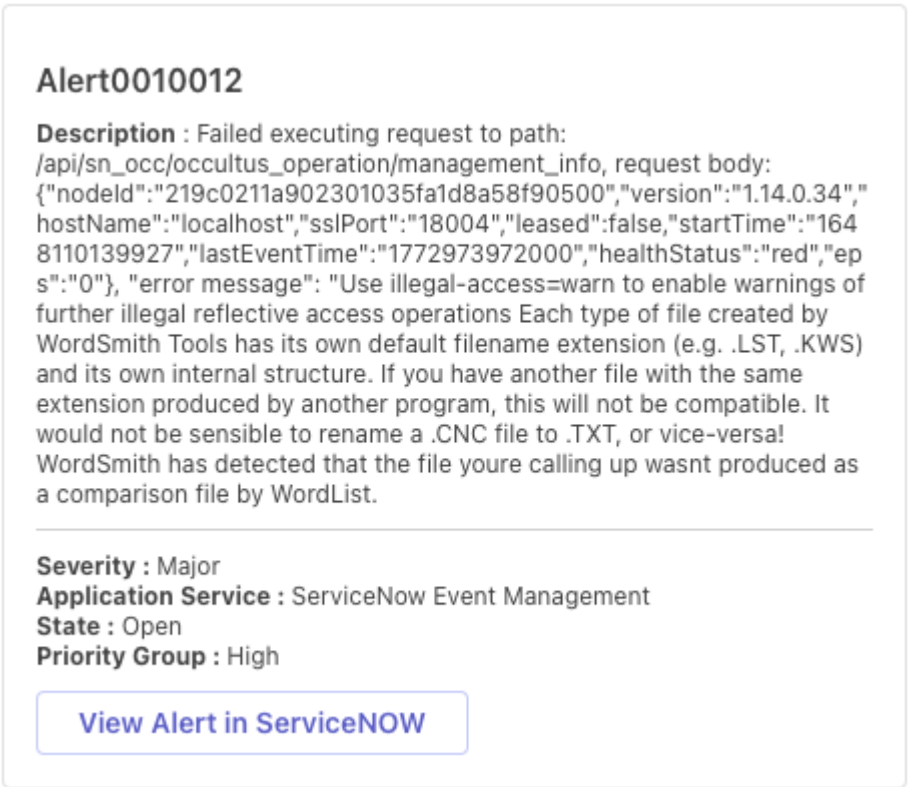
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

werden. Beispielsweise kann es empfehlenswert sein, nur Warnungen mit dem Schweregrad „Schwerwiegend“ oder der Prioritätsgruppe „Hoch“ zu erhalten. Standardmäßig werden bei sekundären Warnungen keine Benachrichtigungen gesendet.

Um die Kanalbenachrichtigung zu unterstützen, muss der Kanal für den Empfang von Health Log Analytics-Benachrichtigungen konfiguriert sein.

Ab Version 33.0.27 von August 2024 verwendet Health Log Analytics die Spoke-Anwendung Microsoft Teams Graph, um Benachrichtigungen über neue Anomaliewarnungen zu senden. Die Anwendung ersetzt das Spoke-Plugin Microsoft Teams, das veraltet ist. Wenn Sie eine HLA-Version vor 33.0.27 verwenden, führen Sie das Setup-Verfahren in Richten Sie Warnungsbenachrichtigungen in Kanälen einaus. Andernfalls siehe Richten Sie Warnungsbenachrichtigungen in einem Microsoft Teams -Kanal ein.

HLA-Warnungsbenachrichtigungen in Microsoft Teams – Beispiel



Richten Sie Warnungsbenachrichtigungen in Kanälen ein

Richten Sie Benachrichtigungen für neue Health Log Analytics -Anomaliewarnungen in einem Kanal Slack oder Microsoft Teams ein.

Vorbereitungen

Ab Version 33.0.27 von August 2024 verwendet Health Log Analytics die Spoke-Anwendung Microsoft Teams Graph zum Senden von Benachrichtigungen für neue Anomaliewarnungen. Die neue Anwendung ersetzt das Spoke-Plugin Microsoft Teams, das veraltet ist. Wenn Sie eine HLA-Version vor 33.0.27 verwenden, führen Sie das folgende Setup-Verfahren aus. Andernfalls siehe Richten Sie Warnungsbenachrichtigungen in einem Microsoft Teams -Kanal ein.

Hinweis: Wenn Sie ein Upgrade von einer früheren Version auf Version 33.0.27 – August 2024 oder höher durchführen, wiederholen Sie das Setup anhand des Verfahrens in Richten Sie Warnungsbenachrichtigungen in einem Microsoft Teams -Kanal ein.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie eine Webhook-URL für einen Kanal in Slack oder Microsoft Teams.

   Von Health Log Analytics wird der Webhook dazu verwendet, im Kanal über die Warnungen zu informieren.

   Führen Sie das entsprechende Verfahren aus:

   - Erstellt eine Webhook-URL für einen Kanal in Slack
   - Webhook-URL für einen Kanal in Microsoft Teams erstellen

2. Ordnen Sie die Webhook-URL für den Kanal der Serviceinstanz zu, die der Warnung zugeordnet ist.

   a. Navigieren zu **Health Log Analytics-Verwaltung** > **Webhook-Benachrichtigung**.

   b. Wählen Sie **Neu**.

   c. Füllen Sie die Felder des Formulars aus.

   Webhook für Warnungsbenachrichtigungen – Formular

Feld	Beschreibung
Webhook	Webhook-URL, die Sie für den Kanal erstellt haben.
Aktiv	Wählen Sie diese Option aus, um den Webhook zu aktivieren.
Konfigurationselement	Die Serviceinstanz, die der Warnung zugeordnet ist. Wenn dieses Feld leer ist, verwendet das System die Standardeigenschaft für den Kanal: default.slack.webhook.url für Slack oder default.teams.webhook.url für Microsoft Teams.

   d. Wählen Sie **Absenden**.

3. Aktivieren Sie die Health Log Analytics-Warnungsverwaltungsregel, um Warnungen an den entsprechenden Kanal zu übermitteln.

   a. Navigieren zu **Ereignismanagement** > **Regeln** > **Warnungsverwaltungsregeln**.

   b. Suchen Sie nach der entsprechenden Regel:

      - Für Slack: HLA-Warnungen an Slack übermitteln.
      - Für Microsoft Teams: HLA-Warnungen an Microsoft Teams übermitteln.

   c. Legen Sie den Wert in der Spalte **Aktiv** für die Regel auf `true` fest.

4. Wahlweise: Filtern Sie die Warnungen, für die Benachrichtigungen an den Kanal gesendet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie in der Tabelle „Warnungsverwaltungsregeln“ die Regel für Ihren Kanal aus.

b. Wählen Sie **Warnungsfilter** aus.

c. Legen Sie im Formular die Bedingungen fest, die erfüllt sein müssen, damit eine Benachrichtigung über die Warnung an den Kanal gesendet wird.

d. Wählen Sie **Aktualisieren**.

Richten Sie Warnungsbenachrichtigungen in einem Microsoft Teams -Kanal ein

Richten Sie Benachrichtigungen für neue Health Log Analytics -Anomaliewarnungen in einem Microsoft Teams -Kanal ein.

Vorbereitungen

Ab Version 33.0.27 von August 2024 verwendet Health Log Analytics die Spoke-Anwendung Microsoft Teams Graph, um Benachrichtigungen über neue Anomaliewarnungen zu senden. Weitere Informationen finden Sie unter Microsoft Teams Graph Spoke . Wenn Sie eine HLA-Version vor 33.0.27 verwenden, lesen Sie das Setup-Verfahren in Richten Sie Warnungsbenachrichtigungen in Kanälen ein.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Installieren Sie die neueste Version der Microsoft Teams Graph-Spoke aus dem ServiceNow Store .
2. Richten Sie die Graph-Spoke Microsoft Teams ein.
   Anweisungen hierzu finden Sie unter: Richten Sie die ein .
3. Aktivieren Sie die Warnungsverwaltungsregel Health Log Analytics für die Übermittlung von Warnungen an den Kanal Microsoft Teams.
   a. Navigieren zu **Ereignismanagement** > **Regeln** > **Warnungsverwaltungsregeln**.
   b. Suchen Sie die entsprechende Regel: HLA-Warnungen an Teams übermitteln.
   c. Legen Sie den Wert in der Spalte **Aktiv** für die Regel auf `true` fest.
4. Ordnen Sie die Serviceinstanz dem Kanal Microsoft Teams zu.

   a. Geben Sie im Navigationsmenü **Alle**`sn_occ_teams_alert_notification_config` ein, und drücken Sie die Eingabetaste.

   b. Wählen Sie **Neu**.

   c. Füllen Sie die Felder des Formulars aus.

   Hinweis:

   - Sie können die Teams-ID und die Kanal-ID aus dem Kanal Microsoft Teams abrufen.
   - Das Feld **Configuration Item** muss der Serviceinstanz entsprechen. Lassen Sie dieses Feld leer, wenn kein CI erforderlich ist. In diesem Fall wird der Datensatz für Warnungen verwendet, wenn kein Datensatz vorhanden ist, der dem CI entspricht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie **Absenden**.

e. Wahlweise: Wiederholen Sie die Schritte 1 bis 4, um weitere Konfigurationen hinzuzufügen.

Speicherplatz für die Protokollaufbewahrung in Health Log Analytics

Das Health Log Analytics-Basissystem bietet normalerweise 1.000 GB Speicherplatz für die Aufbewahrung der Protokollquelle, obwohl die Speicherkapazität je nach Lizenz variieren kann. Die Standardaufbewahrungszeit für Protokolle beträgt drei Tage. Sie können diesen Zeitraum jedoch ändern.

Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, verfügbar im ServiceNow Store . Wenden Sie sich an Ihren ServiceNow Account Manager oder den ServiceNow Support, um sie zu aktivieren.

Wenn der von allen Protokollquellen verwendete Speicherplatz 80 Prozent der Gesamtmenge überschreitet, erhalten Sie eine E-Mail-Benachrichtigung. Sie können den standardmäßigen Schwellenwertprozentsatz ändern, indem Sie die Systemeigenschaft *sn_occ.elastic_storage.utilization_limit.percent* in der Tabelle „ServiceNow-Systemeigenschaften“ ändern. Weitere Informationen finden Sie unter Globale Health Log Analytics-Systemeigenschaften konfigurieren.

Automatische Reduzierung der Protokollaufbewahrungstage

Standardmäßig werden Protokolle drei Tage lang gespeichert. Sie können diesen Zeitraum auf 3, 7, 14 oder 30 Tage anpassen. Weitere Informationen finden Sie unter Aufbewahrungszeitraum für Protokollquellen ändern.

Wenn der von allen Protokollquellen verwendete Speicherplatz 100 Prozent erreicht, wird die Anzahl der pro Quelle zugewiesenen Aufbewahrungstage automatisch um eine Ebene verringert und Sie erhalten eine E-Mail-Benachrichtigung mit den Details. Der automatische Reduzierungsprozess beginnt mit den Quellen, denen die höchste Anzahl von Aufbewahrungstagen zugewiesen wurde. Beispiel: Für eine Quelle mit 30 Aufbewahrungstagen wird die Anzahl auf 14 reduziert. Wenn die Quelle 14 Aufbewahrungstage hat, wird die Anzahl auf 7 reduziert usw.

Sie können den Schwellenwertprozentsatz für die automatische Reduzierung der Protokollaufbewahrungstage ändern, indem Sie die Systemeigenschaft *sn_occ.log_retention.automatic_reduction_utilization_percent* ändern.

Zugehörige Informationen

Aufbewahrungszeitraum für Protokollquellen ändern

Aufbewahrungszeitraum für Protokollquellen ändern

Ändern Sie den Zeitraum, über den Health Log Analytics Protokolle aus einer bestimmten Quelle aufbewahrt. Sie können die Auswirkungen Ihrer beabsichtigten Änderung auf den Speicher berechnen, um eine fundierte Entscheidung zu treffen.

Vorbereitungen

Diese Funktion wird in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und höher, die im ServiceNow Store verfügbar ist, unterstützt. Wenden Sie sich an Ihren ServiceNow Account Manager oder den ServiceNow Support, um sie zu aktivieren.

So zeigen Sie **Protokollquellenaufbewahrungen** im Filternavigator an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Navigieren zu **Alle** > **Systemeigenschaften** > **Alle Eigenschaften**.
2. Geben Sie den Eigenschaftsnamen *sn_occ.activate_log_source_retention* in das Suchfeld ein.
3. Stellen Sie sicher, dass der Eigenschaftswert auf **true**festgelegt ist.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig ist die Aufbewahrungsdauer für Protokolle pro Quelle auf drei Tage festgelegt. Sie können diese Zahl auf 7, 14 oder 30 Tage ändern. Weitere Informationen finden Sie unter Speicherplatz für die Protokollaufbewahrung in Health Log Analytics. Beachten Sie, dass eine längere Protokollaufbewahrung zu einer höheren Speichernutzung führt.

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Aufbewahrungen der Protokollquelle**.
2. Wahlweise: Berechnen Sie, wie sich das Ändern des Aufbewahrungszeitraums für Protokolle aus einer bestimmten Quelle auf den Speicher auswirkt.

   a. Öffnen Sie einen Protokollquelldatensatz.

   b. Wählen Sie im Abschnitt „Zugehörige Links“ die Option **Calculate how retention impacts storage** (Auswirkung der Aufbewahrung auf den Speicher berechnen) aus.

   c. Wählen Sie in der Liste „New retention“ (Neue Aufbewahrung) die vorgeschlagene Anzahl von Aufbewahrungstagen für Protokolle aus dieser Quelle aus.

   d. Wählen Sie **Berechnen** aus.
   Im Feld **Projected storage usage (GB)** (Prognostizierte Speichernutzung (GB)) wird die Speichermenge in GB angezeigt, die die Quelle bei Implementierung der neuen Richtlinie verwenden würde.

   > **Hinweis:** Health Log Analytics basiert die Berechnung der prognostizierten Speichernutzung auf dem Umfang der Protokolldaten, die in der Vergangenheit gestreamt wurden. Die Schätzung kann sich ändern, wenn das Volumen der gestreamten Protokolldaten variiert.

   e. Vergleichen Sie die prognostizierte Nutzung mit der Speichermenge, die für die aktuelle Richtlinie erforderlich ist, die im Feld **Current storage usage (GB)** (Aktuelle Speichernutzung (GB)) angezeigt wird.

   f. Wählen Sie **Abbrechen** aus, um das Dialogfeld zu schließen.

3. Aktualisieren Sie die Protokollaufbewahrungsrichtlinie pro Quelle oder für mehrere Quellen auf einmal.
   - So aktualisieren Sie die Protokollaufbewahrung für eine einzelne Quelle:

     a. Öffnen Sie einen Protokollquelldatensatz.

     b. Wählen Sie aus der Liste „Retention days“ (Aufbewahrungstage) die erforderliche Anzahl von Aufbewahrungstagen für Protokolle aus dieser Quelle aus.

     c. Wählen Sie **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- So aktualisieren Sie die Protokollaufbewahrung für mehrere Quellen:
  a. Wählen Sie mehrere Protokollquelldatensätze aus.
  b. Wählen Sie in der Auswahlliste „Aktionen für ausgewählte Zeilen“ die Option **Update multiple source retentions** (Mehrere Quellenaufbewahrungen aktualisieren) aus.
  c. Wählen Sie aus der Liste „New retention policy“ (Neue Aufbewahrungsrichtlinie) die erforderliche Anzahl von Aufbewahrungstagen für Protokolle aus den ausgewählten Quellen aus.
  d. Wählen Sie **Aktualisieren**.

Die aktualisierte Richtlinie wird in bis zu 15 Minuten wirksam.

4. Wahlweise: Stellen Sie die standardmäßige Protokollaufbewahrungsrichtlinie pro Quelle oder für alle Protokollquellen wieder her.
   - So stellen Sie die Standardrichtlinie für eine einzelne Quelle wieder her:
     a. Öffnen Sie einen Protokollquelldatensatz aus der Tabelle.
     b. Wählen Sie im Abschnitt „Zugehörige Links“ des Datensatzes die Option **Standardwerte wiederherstellen** aus.

     Die Protokollaufbewahrungsrichtlinie für diese Protokollquelle wird auf den Standardwert von drei Tagen zurückgesetzt.
   - So stellen Sie die Standardrichtlinie für alle Quellen wieder her:
     a. Wählen Sie im Abschnitt „Zugehörige Links“ die Option **Standardwerte wiederherstellen** aus.
     b. Wählen Sie im Bestätigungsdialogfeld **Fortsetzen** aus.

     Die Protokollaufbewahrungsrichtlinie für alle Protokollquellen wird auf den Standardwert von drei Tagen zurückgesetzt.

Health Log Analytics wird skaliert, um Protokolle mit einer höheren Rate zu streamen

Streamen Sie Protokolldaten mithilfe der erweiterten ServiceNow -Infrastruktur skalierbar und stabiler an Health Log Analytics.

Die neue ServiceNow -Architektur nutzt Warteschlangentechnologie in IT Operations Management Cloud Services für die Authentifizierung und Protokollerfassung. Die KI-Engine Health Log Analytics wurde verbessert und skaliert dynamisch mit der erhöhten Protokollerfassung durch Ihre Organisation. Health Log Analytics kann so skaliert werden, dass mehr als 50.000 Ereignisse pro Sekunde (EPS) oder mehr als 10.000 Abonnementeinheiten (SUs)unterstützt werden.

Sie können zur erweiterten ServiceNow -Infrastruktur wechseln, indem Sie eine Skalierungsanforderung über den Now Support -Katalog senden. Weitere Informationen finden Sie unter Senden Sie eine HLA-Skalierungsanforderung über den -Katalog Now Support .. Sie können sich auch an Ihren Account Manager ServiceNow wenden, um eine Skalierung anzufordern. Wenn Ihre Skalierungsanforderung genehmigt wird, stellt ServiceNow die Anzahl der Elasticsearch - und HLA AI Engine-Knoten bereit, die zur Unterstützung Ihrer Abonnementeinheiten erforderlich sind.

Senden Sie eine HLA-Skalierungsanforderung über den -Katalog Now Support .

Skalierung von Health Log Analytics anfordern, um Streaming-Protokolle mit einer höheren Rate zu unterstützen.

Vorbereitungen

Erforderliche Rolle: keine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

In diesem Verfahren wird erläutert, wie Sie eine Skalierungsanforderung über den Katalog Now Support übermitteln. Sie können auch Ihren ServiceNow Account Manager kontaktieren, um die Skalierung Health Log Analytics von anzufordern.

Prozedur

1. An Now Support , navigieren Sie zu **Alle** > **Servicekatalog**.
2. Wählen Sie im Dialogfeld „Skala anfordern“ die entsprechende Option aus:
   - Installieren Sie die App Health Log Analytics Prime aus dem ServiceNow Store.

     Wenn die App installiert ist, können die zusätzlichen Services zur Unterstützung Ihrer Anforderung neben dem Ihre Instanz ServiceNow gemeinsam genutzten Ressourcen in anderen Rechenzentren verwenden. Diese Funktion ermöglicht eine bessere Ressourcenzuteilung für die Unterstützung Ihrer aktuellen und zukünftigen Anforderungen.

     Hinweis: Um die App Health Log Analytics Prime zu installieren, müssen Sie die Nutzungsbedingungen akzeptieren.

   - Fordern Sie eine Skala an, ohne die App Health Log Analytics Prime zu installieren.

     Wenn Sie diese Option auswählen, befinden sich die zusätzlichen Ressourcen zur Unterstützung Ihrer Anforderung im selben Rechenzentrum wie Ihre -Instanz. Es kann zu Einschränkungen bei der Kapazität kommen.
3. Füllen Sie die Felder aus.

Skalafelder anfordern

Feld	Beschreibung
Wählen Sie die Instanz aus	Der Name Ihrer ServiceNow -Instanz.
Anzahl der Abonnementeinheiten	Die Anzahl der Abonnementeinheiten Health Log Analytics, die unterstützen müssen.

4. Wählen Sie **Absenden**.
   Ihre Skalierungsanforderung wird übermittelt. Wenn genehmigt wird, benachrichtigt Sie ServiceNow Sie per E-Mail.

CMDB mit in Protokollen gefundenen Hostdaten erweitern

Wenn Health Log Analytics Protokolle streamt, werden Hostdaten aus den Protokollereignissen extrahiert. Wenn Hostdaten erkannt werden, die nicht mit den Informationen in der Configuration Management Database (CMDB) übereinstimmen, erstellt das System einen Configuration Item(CI)-Kandidaten basierend auf den in den Protokollen gefundenen Daten, die Sie überprüfen können.

Nachdem Sie einen CI-Kandidaten überprüft haben, können Sie ihn entweder der CMDB hinzufügen oder als irrelevant ablehnen. Die Tabelle **Log-Based CI Candidates** (Protokollbasierte CI-Kandidaten) listet alle von Health Log Analytics erstellten CI-Kandidaten sortiert nach Systemaktualisierungszeit auf. In der Spalte **Vorgang** wird die vorgeschlagene Aktion für jeden CI-Kandidaten angezeigt. Sie werden automatisch benachrichtigt, wenn neue CI-Kandidaten für Ihre Berücksichtigung in Frage kommen. Weitere Informationen finden Sie unter Protokollbasierte CIs der CMDB hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Beschreibung aller zugehörigen Systemeigenschaften finden Sie im Abschnitt „logsourceinfo (CMDB)“ im Artikel HLA System Properties [KB0869842] (HLA-Systemeigenschaften) in der Now Support-Knowledge Base.

Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, verfügbar im ServiceNow Store. Sie können sie auf der Now Platform mit dem Release Rome Patch 6 (geplant für den 27. Januar 2022) oder höher verwenden.

Protokollbasierte CIs der CMDB hinzufügen

Halten Sie die Configuration Management Database (CMDB) aktuell. Nutzen Sie dazu Hostdaten, die in Ihren Protokollen erkannt wurden, indem Sie protokollbasierte Konfigurationselemente (Configuration Items, CIs) hinzufügen.

Vorbereitungen

Diese Funktion wird in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und höher, die im ServiceNow Store verfügbar ist, unterstützt. Sie können es auf dem Now Platform mit Release Rome Patch 6 (geplante Veröffentlichung am 27. Januar 2022) oder höher verwenden.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Health Log Analytics-Verwaltung** > **Protokollbasierte CI-Kandidaten**.
2. Behandeln Sie einen einzelnen CI-Kandidaten oder mehrere CI-Kandidaten auf einmal.

Option	Prozedur
Maßnahmen für einen einzelnen CI-Kandidaten ergreifen	**a.** Wählen Sie einen CI-Kandidatendatensatz aus und überprüfen Sie die Informationen im Formular. Feldbeschreibungen finden Sie unter Feldbeschreibungen für protokollbasierte CI-Kandidaten. **b.** Fügen Sie der CMDB den CI-Kandidaten hinzu oder löschen Sie ihn. ▪ Wenn der CI-Kandidat geeignet ist, fügen Sie ihn entweder unverändert der CMDB hinzu oder fügen Sie weitere Informationen hinzu, bevor Sie ihn der CMDB hinzufügen. ▪ Um den CI-Kandidaten unverändert der CMDB hinzuzufügen, wählen Sie **Add to CMDB** (Zu CMDB hinzufügen) und dann **Fortsetzen** aus. ▪ Um weitere Informationen hinzuzufügen, wählen Sie **Edit additional CI fields** (Zusätzliche CI-Felder bearbeiten) aus. Geben Sie Daten ein, die nicht aus den Protokollen extrahiert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Prozedur
	wurden, z. B. den Namen des Unternehmens, das dem CI zugeordnet ist, und wählen Sie dann **Absenden** aus. Das CI wird der CMDB hinzugefügt. In der CMDB-Tabelle für den entsprechenden Klassentyp ist die Erkennungsquelle für das neue CI Health Log Analytics. Der CI-Kandidatendatensatz wird automatisch aus der Tabelle mit den protokollbasierten CI-Kandidaten gelöscht. ▪ Wenn der CI-Kandidat irrelevant ist, löschen Sie ihn, indem Sie **Löschen** auswählen.
Maßnahmen für mehrere CI-Kandidaten gleichzeitig ergreifen	**Hinweis:** Mit dieser Option können Sie den ausgewählten CIs keine zusätzlichen Informationen hinzufügen. ◦ Fügen Sie der CMDB mehrere CIs hinzu. **a.** Wählen Sie in der Tabelle der protokollbasierten CI-Kandidaten die CI-Kandidaten aus, die Sie der CMDB hinzufügen möchten. **b.** Wählen Sie in der Liste „Aktionen für ausgewählte Zeilen“ unten auf der Seite **Add to CMDB** (Zu CMDB hinzufügen) aus. Die ausgewählten CIs werden der CMDB hinzugefügt. Die CI-Kandidatendatensätze werden automatisch aus der Tabelle mit den protokollbasierten CI-Kandidaten gelöscht. ◦ Löschen Sie mehrere CI-Kandidaten. **a.** Wählen Sie in der Tabelle der protokollbasierten CI-Kandidaten die CI-Kandidaten aus, die Sie löschen möchten. **b.** Wählen Sie in der Liste „Aktionen für ausgewählte Zeilen“ unten auf der Seite **Löschen**.

Feldbeschreibungen für protokollbasierte CI-Kandidaten

Feldbeschreibungen für die Tabelle „Log-Based CI Candidates“ (Protokollbasierte CI-Kandidaten), das Formular „Log-Based CI Candidate“ (Protokollbasierter CI-Kandidat) und das Formular „Add CI candidate to CMDB“ (CI-Kandidaten der CMDB hinzufügen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Log-based CI candidates“ (Protokollbasierte CI-Kandidaten)

Feld	Beschreibung
Host-Name	Der Hostname, den Health Log Analytics in den Protokolldaten erkannt hat.
CI-Klassentyp	Der in den Protokolldaten erkannte CI-Klassentyp. Der CI-Klassentyp wird durch den Dateneingabetyp bestimmt: • Rsyslogs – CI-Klassentyp: Linux-Server • Linux-Filebeat – CI-Klassentyp: Linux-Server • Windows Filebeat – CI-Klassentyp: Windows Server • Winlogbeat – CI-Klassentyp: Windows-Server
Zeit des letzten Protokolls	(Schreibgeschützt) Das letzte Mal, dass dieser Host in den Protokolldaten gefunden wurde.
Vorgang	(Schreibgeschützt) Vorgeschlagene Aktion: Hinzufügen – Fügt das CI der CMDB hinzu.
Status	(Schreibgeschützt) Der Status des vorgeschlagenen Aktion. • Ausstehend – Es wurde keine Aktion ausgeführt. • Wenn die ausgeführte Aktion fehlgeschlagen ist, enthält dieses Feld eine Fehlermeldung.

Formular „Log-based CI candidate“ (Protokollbasierter CI-Kandidat)

Feld	Beschreibung
CI-Klassentyp	Der in den Protokolldaten erkannte CI-Klassentyp. Der CI-Klassentyp wird durch den Dateneingabetyp bestimmt: • Rsyslogs – CI-Klassentyp: Linux-Server • Linux-Filebeat – CI-Klassentyp: Linux-Server • Windows Filebeat – CI-Klassentyp: Windows Server • Winlogbeat – CI-Klassentyp: Windows-Server
CI-Name	Der Hostname, den Health Log Analytics in den Protokolldaten erkannt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Log-based CI candidate“ (Protokollbasierter CI-Kandidat) (Fortsetzung)

Feld	Beschreibung
Vorgang	(Schreibgeschützt) Vorgeschlagene Aktion: Hinzufügen – Fügt das CI der CMDB hinzu.
Zeit des letzten Protokolls	(Schreibgeschützt) Das letzte Mal, dass dieser Host in den Protokolldaten gefunden wurde.
Status	(Schreibgeschützt) Der Status der vorgeschlagenen Aktion: • Ausstehend – Es wurde keine Aktion ausgeführt. • Wenn die ausgeführte Aktion fehlgeschlagen ist, enthält dieses Feld eine Fehlermeldung.

Formular „Add CI candidate to CMDB“ (CI-Kandidaten der CMDB hinzufügen) (Linux-Server)

Feld	Beschreibung
Name	Name des CI
Asset-Tag	Alphanumerische Informationen zum Nachverfolgen des mit dem CI verknüpften Assets.
Hersteller	Hersteller des Geräts
Asset	(Schreibgeschützt) Das dem CI zugeordnete Asset.
Klasse	Die Asset-Gruppe. Zum Beispiel Linux-Server.
Kommentare	Informationen zum Asset.
Unternehmen	Das dem CI zugeordnete Unternehmen. Dies ist ein Pflichtfeld.
Seriennummer	Seriennummer, die dem CI zugeordnet ist
Modell-ID	Modell-ID des Geräts
Zugewiesen an	Person, die dieses Element verwendet oder die Hauptverantwortung dafür trägt.
Host-Name	Der Hostname des CI.
BS-Domäne	Die BS-Domäne des CI.
Betriebssystem	Auf dem CI ausgeführtes Betriebssystem
BS-Version	Version des auf dem CI ausgeführten Betriebssystems

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Add CI candidate to CMDB“ (CI-Kandidaten der CMDB hinzufügen) (Linux-Server) (Fortsetzung)

Feld	Beschreibung
BS-Service Pack	Das auf dem Betriebssystem installierte Service Pack.
DNS-Domäne	Die DNS-Domäne des CI.
IP-Adresse	IP-Adresse für das CI
Festplattenspeicher (GB)	Die Menge des Speicherplatzes in GB.
Beschreibung	Kurze Textbeschreibung des CI.
RAM (MB)	Die Größe des Arbeitsspeichers auf dem Computer in MB.
CPU-Hersteller	Hersteller der CPU
CPU-Typ	CPU-Typ
CPU-Geschwindigkeit (MHz)	Die Geschwindigkeit der CPU in MHz.
CPU-Anzahl	Die Anzahl der Server-CPUs.
Anzahl CPU-Kerne	Die Anzahl der Kerne pro CPU.
IsVirtual	Option zum Angeben, ob das Gerät in einer VM-Instanz ausgeführt wird.

Starten Sie die Nachbesserung einer Log Analytics -Warnung auf der Registerkarte „Übersicht“.

Beginnen Sie den Nachbesserungsprozess für eine Log Analytics -Warnung auf der Registerkarte **Übersicht** der Warnung. Diese Registerkarte enthält Informationen zur Warnung, die Protokolldaten, die dem anomalen Verhalten zugeordnet sind, die mit der Warnung verknüpften CIs und die von ihr betroffenen Services.

Vorbereitungen

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_user oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in Service Operations-Arbeitsbereich das Listensymbol ( ) aus.
3. Wählen Sie in der Unterliste Warnungen die entsprechende Liste aus, und navigieren Sie zur entsprechenden Warnung oder Gruppe.

   Alle Health Log Analytics-Warnungen weisen in der Spalte **Quelle** den Wert **Log Analytics** auf. Durch den Wert in der Spalte **Gruppe** wird die Art der Log Analytics-Warnung identifiziert. Unter Typs von Health Log Analytics Warnungen finden Sie eine detailliertere Beschreibung der einzelnen Arten von Warnungen oder Gruppen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tipp: Um die Vorschau einer Warnung in der Liste anzuzeigen, klicken Sie auf das zugehörige Info-Symbol (ⓘ).

4. Wählen Sie die Warnungsnummer aus.

   Die Registerkarte **Übersicht** wird angezeigt.

5. Zeigen Sie den Abschnitt der Registerkarte **Übersicht** an, der die Informationen enthält, die Sie benötigen.

   Eine Beschreibung der Abschnitte und Karten finden Sie unter Abschnitte und Karten auf der Registerkarte „Warnungsübersicht“ in Health Log Analytics.

   Hinweis: Da in einigen Abschnitten der Registerkarte **Übersicht** nur ein Teil der Informationen zu sehen ist, enthalten viele Abschnitte einen Link, über den Sie andere oder vollständigere Informationen aufrufen können.

Die Protokolle, die die Anomalie umgeben, werden analysiert

Wenn Health Log Analytics eine Anomalie identifiziert, gibt die Anzeige der die Anomalie umgebenden Protokolle Hinweise auf den Status fehlerhafter Systeme. Mithilfe dieser Informationen können Sie die Ursache einer Warnung eingrenzen.

Bei der Anzeige einer Log Analytics -Warnung werden auf der Registerkarte **Umgebende Protokolle** die Protokollzeilen aufgelistet, die eine Minute vor und eine Sekunde nach dem Auftreten der Anomalie generiert wurden. Die Protokollzeilen beziehen sich auf die Metrik oder das Muster, die bzw. das die Warnung ausgelöst hat. Die Liste wird nach der entsprechenden Komponente gefiltert.

Sie können den Zeitbereich der angezeigten Protokollzeilen ändern, um beispielsweise Protokolle von mehr als einer Minute vor der Anomalie oder von mehr als einer Sekunde danach zu untersuchen.

Hinweis: Protokolle, die die Anomalie umgeben, werden aufbewahrt und sind nach Erstellung der Warnung 30 Tage lang verfügbar. Diese Protokolle werden vom System nicht gelöscht, wenn der globale Aufbewahrungszeitraum der Protokolle abgelaufen ist. Wenn der Aufbewahrungszeitraum abgelaufen ist, sind die umgebenden Protokolle nur auf der Registerkarte **Umgebende Protokolle** und nicht im Protokoll-Viewer verfügbar.

Health Log Analytics ermöglicht Ihnen die grafische Anzeige der anomalen Protokolldaten im Protokoll-Viewer, auf den Sie über Service Operations-Arbeitsbereichzugreifen. Der Protokoll-Viewer zeigt ein Diagramm der Häufigkeit der anomalen Protokollzeilen während einer Minute vor und eine Minute nach der Warnung Log Analytics an und listet die zugehörigen Protokollzeilen auf. Er zeigt automatisch die Abfrage im Zusammenhang mit der Anomalie, der ausgewählten Komponente und dem entsprechenden Zeitfilter an. Weitere Informationen finden Sie unter Protokolle für Warnung werden in der Protokollanzeige überprüft.

Zugehörige Informationen

Protokollzeilen rund um eine Anomalie analysieren

Protokollzeilen rund um eine Anomalie analysieren

Zeigen Sie die Protokollzeilen um eine Anomalie an, um die Ursache einer Log Analytics-Warnung zu identifizieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Protokollzeilen rund um eine Anomalie analysieren.

Protokolle für Warnung werden in der Protokollanzeige überprüft

Auf der Registerkarte **Protokoll-Viewer** können Sie die Protokolle nach einer Warnung nach Zeitstempel oder Zeitbereich durchsuchen und die Anomaliehäufigkeit innerhalb eines bestimmten Zeitraums visualisieren. Durch das Anpassen der angezeigten Daten und das Anpassen von Zeitfiltern können Sie das Framework, in dem die Anomalie aufgetreten ist, besser verstehen und die Ursache schneller finden.

Der Protokoll-Viewer zeigt alle mit der Log Analytics-Warnung verbundenen Daten an. Angezeigt werden die Abfrage, die sich auf die Anomalie, die ausgewählte Komponente und den entsprechenden Zeitfilter bezieht. Sie können die angezeigten Daten personalisieren und den Zeitbereich manuell anpassen, ohne die anderen Einstellungen zu beeinträchtigen. Die angewendeten Filter werden im Bereich **Filter** angezeigt. Sie können Filter nach Bedarf hinzufügen oder entfernen, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Der **Protokoll-Viewer** zeigt ein Diagramm der Häufigkeit anomaler Protokollzeilen während einer Minute vor und eine Minute nach der Warnung Log Analytics an und listet die zugehörigen Protokolldaten auf. Diese Informationen helfen Ihnen, Trends im Vorfeld und nach dem Ereignis zu identifizieren, und bieten Kontext für die Ursachenanalyse.

Während Sie die Protokolle für eine Warnung im **Protokoll-Viewer**analysieren, können Sie die Abfrage ändern, um die Suche zu optimieren, nützliche Suchvorgänge speichern und sie für andere freigeben. Eine Beschreibung der Informationen, die in der **Protokoll-Viewer** -Tabelle angezeigt werden, finden Sie unter Felder der Protokoll-Viewer-Tabelle.

In der **Protokollanzeige**können Sie folgende Aufgaben ausführen:

- Protokolldaten für eine Warnung anzeigen

  Zeigen Sie ein Diagramm der Häufigkeit anomaler Protokollzeilen und der zugehörigen Protokolldaten an.

- Suche nach Protokolldaten definieren, speichern und teilen

  Optimieren Sie die Suchabfrage, um die Ursachen des Problems zu ermitteln, und speichern und teilen Sie nützliche Suchvorgänge.

- Gespeicherte Suche verwenden oder ändern

  Verwenden Sie eine gespeicherte Suche. Als Besitzer einer gespeicherten Suche können Sie die Suchwerte ändern und Ihre Änderungen speichern.

- Im Protokoll-Viewer angezeigte Suchergebnisse filtern

  Wenden Sie Filter an, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

- Protokoll-Viewer-Tabelle anpassen

  Fügen Sie der Tabelle Spalten hinzu, oder entfernen Sie sie, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie in den Protokolldaten eine wichtige Metrik entdecken, können Sie damit eine neue Log Analytics Warnungsregel definieren. Weitere Informationen finden Sie unter Log Analytics-Warnungsregel hinzufügen.

Zugehörige Informationen

Die Protokolle, die die Anomalie umgeben, werden analysiert

Protokolldaten für eine Warnung anzeigen

Zeigen Sie im Protokoll-Viewer ein Diagramm der Häufigkeit anomaler Protokollzeilen und der zugehörigen Protokolldaten an.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Protokolldaten für eine Warnung anzeigen.

Suche nach Protokolldaten definieren, speichern und teilen

Definieren, speichern und teilen Sie Suchen nach Protokolldaten, um die Ursachen von Log Analytics-Warnungen zu ermitteln.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Suche nach Protokolldaten definieren, speichern und teilen.

Gespeicherte Suche verwenden oder ändern

Verwenden Sie eine gespeicherte Suche nach Protokolldaten, um die Ursachen einer Warnung besser zu verstehen. Als Besitzer einer gespeicherten Suche können Sie die Suchwerte ändern und Ihre Änderungen speichern.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wenn Sie nicht der Besitzer der gespeicherten Suche sind, speichern Sie die Suche unter einem anderen Namen. Anschließend können Sie Suchwerte aktualisieren, Ihre Änderungen speichern und die Suche für andere freigeben.

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Gespeicherte Suche verwenden oder ändern.

Im Protokoll-Viewer angezeigte Suchergebnisse filtern

Wenden Sie auf den **Protokoll-Viewer** Filter an, um nur die gewünschten Daten anzuzeigen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_user oder evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Im Protokoll-Viewer angezeigte Suchergebnisse filtern.

Protokoll-Viewer-Tabelle anpassen

Fügen Sie der Tabelle **Protokoll-Viewer** Spalten hinzu, oder entfernen Sie sie, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Protokoll-Viewer-Tabelle anpassen.

Identifizieren von Beziehungen in Protokolldaten mithilfe von Protokollkorrelatoren

Protokollkorrelatoren sind Schlüssel oder Werte in Protokolldaten, die Korrelationen zwischen Warnungen erkennen, um Ihnen zu helfen, zu bestimmen, ob eine Warnung Teil eines größeren Problems ist. Beispielsweise könnte ein Protokollkorrelator erkennen, wenn die Schnittstellen-ID eines bestimmten Netzwerkgeräts gleichzeitig in mehreren Warnungen in verschiedenen Serviceinstanzen vorkommt.

Sie können zugehörige Warnungen in Ihren Protokolldaten mithilfe von Protokollkorrelatoren identifizieren. Das Basissystem enthält mehrere Protokollkorrelatoren, und Sie können anwenderdefinierte Korrelatoren für eine bestimmte Protokollquelle, alle Protokollquellen oder nur Protokollquellen definieren, die nach der Aktivierung des Korrelators erstellt wurden.

Die meisten Protokollzeilen enthalten einen Metadatenteil sowie einen Nachrichtenteil. Einige Protokollzeilen enthalten jedoch nur Nachrichtentext mit darin enthaltenen Metadaten. Mit den beiden Arten von Protokollkorrelatoren, Freitextkorrelatoren und Protokolleigenschaftskorrelatoren, werden die verschiedenen Teile jedes Protokolls analysiert, damit Beziehungen zwischen Protokolldaten aus mehreren Protokollquellen identifiziert werden können.

Freitextkorrelatoren

Freitextkorrelatoren analysieren den Text im Protokollnachrichtenteil von Protokollzeilen, die einer Anomalie zugeordnet sind. Das System verwendet Freitextkorrelatoren, um Korrelationen zwischen Warnungen zu identifizieren. Sie verwenden Freitextkorrelatoren, um einen Begriff hinzuzufügen, der in Protokollnachrichten erwartet wird. Eine gute Wahl ist ein Begriff, der nicht strukturiert ist und andernfalls nicht als Protokolleigenschaft extrahiert würde. Beispiel: „Richtlinien-ID“ oder „Thread-ID“.

In der Regel fügen Sie auch Freitextkorrelatoren für die Namen von Systemen, Anwendungen und Services hinzu, die für Ihre Umgebung eindeutig sind. Da auf einen solchen Wert von mehreren Quellen, Ebenen, Middlewares oder Datenbanken verwiesen werden kann, kann der Freitextkorrelator ein effektiver Tester für korrelierte Warnungen sein. Wenn der Service Ihrer Organisation beispielsweise „TeaTime“ heißt, können Sie „teatime“ als Freitextkorrelator hinzufügen. Der Korrelator identifiziert Warnungen, die im Zusammenhang miteinander stehen, da sie für Ressourcen generiert wurden, die den Service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„TeaTime“ unterstützen, z. B. eine Datenbanksperre oder ein Verbindungsfehler zwischen Komponenten von „TeaTime“.

Protokolleigenschaftskorrelatoren

Protokolleigenschaftskorrelatoren analysieren den Metadatenteil von Protokollzeilen. Beispielsweise kann der Korrelator den Namen einer Serviceinstanz, die Schnittstellen-ID eines Netzwerkgeräts oder die Anforderungs-ID einer Komponente mit Webzugriff analysieren. Ein Protokolleigenschaftskorrelator kann eine Korrelation kennzeichnen, wenn die Schnittstellen-ID eines Netzwerkgeräts gleichzeitig in mehreren Warnungen in verschiedenen Protokollquellen vorkommt. Protokolleigenschaftskorrelatoren sind spezifisch für den Geschäftskontext Ihrer Umgebung.

Sie können den Satz der Protokollquellen angeben, deren Protokolldaten von einem Protokollkorrelator analysiert werden. Die Auswahlmöglichkeiten lauten wie folgt:

- **Nur neue Quellen**: Das System wendet den Protokollkorrelator nur auf Protokollzeilen aus Protokollquellen an, die nach der Aktivierung dieses Protokollkorrelators erstellt wurden.
- **Alle Quellen**: Das System wendet den Protokollkorrelator auf Protokollzeilen aus allen Protokollquellen an.
- **Angegebene Quelle**: Für einen Protokollkorrelator analysiert das System nur Protokollzeilen aus der von Ihnen angegebenen Protokollquelle.

Protokollkorrelatoren hinzufügen, um Beziehungen in Protokollen zu identifizieren

Erkennen Sie zugehörige Warnungen in Protokolldaten, indem Sie Protokollkorrelatoren hinzufügen. Das Basissystem enthält mehrere Protokollkorrelatoren, und Sie können anwenderdefinierte Protokollkorrelatoren definieren.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Informationen zu den Typen und Funktionen von Protokollkorrelatoren finden Sie unter Identifizieren von Beziehungen in Protokolldaten mithilfe von Protokollkorrelatoren.

Prozedur
1. Verwenden Sie eine der folgenden Methoden, um einen Protokollkorrelator hinzuzufügen.

Option	Verfahren
Fügen Sie einen Protokollkorrelator für eine bestimmte Protokollquelle hinzu	**a.** Navigieren zu **Health Log Analytics** > **Anomalie-Erkennung protokollieren** > **Protokollkorrelatoren**. Die Liste der vorhandenen Protokollkorrelatoren wird geöffnet. **b.** Klicken Sie auf den Namen eines Protokollkorrelators. Die Namen werden in der Spalte **Korrelationsindikator** angezeigt. **c.** Klicken Sie auf **Neu**.
Fügen Sie einen Protokollkorrelator hinzu, der entweder für alle Protokollquellen gilt oder nur für die Protokollquellen, die nach der Definition dieses Protokollkorrelators aktiv werden	**a.** Navigieren zu **Health Log Analytics** > **Dateneingabe** > **Protokollquellen**. **b.** Klicken Sie auf den Namen der Protokollquelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Verfahren
	In der zugehörigen Liste „Protokollkorrelatoren“ wird die Liste der vorhandenen Protokollkorrelatoren angezeigt, die Protokolldaten aus der ausgewählten Protokollquelle analysieren. **c.** Klicken Sie auf der Registerkarte **Log correlators** (Protokollkorrelatoren) auf **Neu**.

2. Füllen Sie das Formular „Protokollkorrelator“ aus.
   Feldbeschreibungen finden Sie unter Formularfelder für Protokollkorrelatoren.
3. Aktivieren Sie **Aktiv**, und klicken Sie dann auf **Absenden**.

Quellen aus einem Protokollkorrelator ausschließen

Verhindern Sie, dass das System Protokollzeilen aus einer bestimmten Quelle analysiert, indem Sie diese Quelle aus dem Protokollkorrelator ausschließen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Health Log Analytics** > **Dateneingabe** > **Protokollquellen**.
2. Öffnen Sie die entsprechende Quelle im Formular „Protokollquellen“.
3. Wählen Sie auf der Registerkarte **Protokollkorrelatoren** die Option für den Protokollkorrelator.
4. Wählen Sie in der Liste „Actions on selected items“ (Aktionen für ausgewählte Elemente) die Option **Exclude from this source** (Aus dieser Quelle ausschließen) aus.

Fügt einen KB-Artikel zu einer Warnung hinzu

Fügen Sie Ihren eigenen KB-Artikel (Knowledge Base) einer Warnung hinzu, die von Health Log Analytics generiert wurde. Sie können beispielsweise zusätzliche Informationen angeben, die zur Lösung des zugrunde liegenden Problems beitragen können. Health Log Analytics verwendet Ihr Wissen auch, um ähnliche Warnungen zu verbessern.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: KB-Artikel einer Log Analytics-Warnung hinzufügen.

Mithilfe von Warnungsregeln steuern, wann Health Log Analytics Warnungen generiert

Mit Warnungsregeln können Sie Schwellenwerte und Bedingungen festlegen, die bestimmen, wann Health Log Analytics eine Warnung auslöst. Wenn die Bedingungen einer Warnungsregel erfüllt sind, generiert das System eine Log Analytics -Warnung. Sie können Warnungsregeln hinzufügen, ändern oder löschen, um Log Analytics Warnungen für eine bestimmte Metrik zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In Health Log Analyticskönnen Sie mithilfe von Warnungsregeln angeben, wann Warnungen ausgelöst werden. Durch die Verwendung dieser Regeln stellen Sie sicher, dass bei Erfüllung bestimmter Bedingungen eine Warnung generiert wird. So können Sie neu auftretende Probleme proaktiv überwachen und beheben. Sie können Warnungsregeln erstellen, wenn Sie auf Protokolldaten stoßen, die eine Warnung auslösen sollen, und von Ihnen definierte Warnungsregeln ändern oder löschen.

Sie können die folgenden Aufgaben im Zusammenhang mit Warnungsregeln ausführen:

- Log Analytics-Warnungsregel hinzufügen

  Fügen Sie eine Warnungsregel Log Analytics hinzu, wenn Sie auf Protokolldaten stoßen, die eine Warnung generieren sollten.

- Ändern Sie eine definierte Warnungsregel Log Analytics .

  Bearbeiten Sie eine Log Analytics Warnungsregel, die Sie definiert haben.

- Löschen Sie eine definierte Warnungsregel Log Analytics .

  Löschen Sie eine von Ihnen definierte Warnungsregel Log Analytics, wenn sie nicht mehr benötigt wird.

Log Analytics-Warnungsregeln hinzufügen

Definieren Sie eine Log Analytics-Warnungsregel, wenn Sie auf Protokolldaten stoßen, die eine Warnung generieren sollen. Die Warnungsregel generiert eine Warnung für eine angegebene Metrik mit einem von Ihnen angegebenen Schwellenwert und legt die Eigenschaften der generierten Warnung fest.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Log Analytics-Warnungsregel hinzufügen.

Ändern Sie eine definierte Log Analytics-Warnungsregel

Sie können eine von Ihnen definierte Warnungsregel Log Analytics ändern.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Ändern Sie eine definierte Warnungsregel Log Analytics ..

Löscht eine definierte Log Analytics-Warnungsregel

Löschen Sie eine definierte Log Analytics-Warnungsregel, wenn sie nicht mehr erforderlich ist.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Löschen Sie eine definierte Warnungsregel Log Analytics ..

Einer Warnung eine höhere oder niedrigere Bedeutung zuweisen

Kennzeichnen Sie eine Warnung in Health Log Analytics als bedeutungsvoll oder unbedeutend, oder stellen Sie für die Metrik, die an ihrer Generierung beteiligt war, die normale Wichtigkeit wieder her.

Wenn Sie einer Warnung eine höhere oder niedrigere Bedeutung zuweisen, können Sie die von Health Log Analytics generierten Warnungen priorisieren. Im Folgenden sind einige häufige Anwendungsfälle für die Anpassung der Wichtigkeit einer Warnung aufgeführt:

- Warnungen als aussagekräftig kennzeichnen: Sie können die Wahrscheinlichkeit erhöhen, dass eine signifikante Warnung in eine Gruppe Log Analytics aufgenommen wird, wenn sich die zugehörige Metrik anomal verhält. Dadurch wird sichergestellt, dass wichtige Warnungen die gebührende Aufmerksamkeit erhalten.
- Ablenkende Warnungen stummschalten: Sie können Warnungen für unwesentliche Probleme stummschalten, um das Rauschen zu reduzieren und zu vermeiden, dass Sie von Warnungen für geringfügigere Probleme überhäuft werden. Dadurch können Sie sich auf kritischere Warnungen konzentrieren. Sie können eine Liste der stummgeschalteten Metriken anzeigen, um sicherzustellen, dass Sie über Metriken informiert sind, die keine Warnungen mehr generieren.
- Empfindlichkeit gegenüber bestimmten Anomalien reduzieren: Sie können die Empfindlichkeit der Anomalie-Erkennung gegenüber einer bestimmten Anomalie verringern. Dies kann Ihnen helfen, sich auf schwerwiegendere Anomalien zu konzentrieren.
- Normale Signifikanz wird wiederhergestellt: Wenn Sie zuvor eine Warnung als signifikant markiert oder stummgeschaltet oder die Sensibilität gegenüber bestimmten Anomalien verringert haben, können Sie die zugehörige Metrik wieder auf ihre normale Signifikanz zurücksetzen. Dies ist nützlich, wenn Sie die Warnung nicht mehr besonders behandeln möchten.

Sie können wie folgt vorgehen, um die Wichtigkeit einer Warnung anzupassen oder die Empfindlichkeit gegenüber bestimmten Anomalien zu reduzieren:

- Warnung als signifikant markieren

  Sorgen Sie dafür, dass eine Warnung eher in eine Log Analytics-Gruppe aufgenommen wird, wenn sich die zugeordnete Metrik anomal verhält, indem Sie die Warnung als aussagekräftig kennzeichnen.

- Irrelevante Warnungen stummschalten

  Beseitigen Sie störende neue Warnungen für unwichtige Probleme, indem Sie sie stummschalten. Zeigen Sie die Liste der Metriken an, die stummgeschaltet wurden und keine Warnungen mehr generieren.

- Sensitivität bei ähnlichen Anomalien verringern

  Verringern Sie bei der Health Log Analytics-Anomalie-Erkennung die Sensitivität gegenüber Anomalien wie denjenigen, durch die die aktuelle Log Analytics-Warnung ausgelöst wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Normale Wichtigkeit einer Warnungsmetrik wiederherstellen

  Stellen Sie die normale Signifikanz der Metrik wieder her, die an der Generierung einer Log Analytics-Warnung beteiligt ist.

Ausführliche Informationen zu Warnungsmetriken finden Sie unter Wie Health Log Analytics Warnungen generiert.

Warnung als signifikant markieren

Sorgen Sie dafür, dass eine Warnung eher in eine Log Analytics-Gruppe aufgenommen wird, wenn sich die zugeordnete Metrik anomal verhält, indem Sie die Warnung als aussagekräftig kennzeichnen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Warnung als signifikant markieren.

Irrelevante Warnungen stummschalten

Beseitigen Sie störende neue Warnungen für unwichtige Probleme, indem Sie sie stummschalten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Irrelevante Warnungen stummschalten.

Liste der stummgeschalteten Metriken anzeigen

Zeigen Sie die Liste der Metriken an, die stummgeschaltet wurden, damit sie keine Warnungen mehr generieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

Navigieren zu **Alle** > **Health Log Analytics** > **Anomalie-Erkennung protokollieren** > **Stummgeschaltete Metriken**.

Stummgeschaltete Metriken

Feld	Beschreibung
Serviceinstanz	Serviceinstanz, in der die stummgeschaltete Warnung angezeigt wird, der die Metrik zugeordnet ist.
Komponente	Logische Komponente von Serviceinstanz, die das Event generiert hat. Mehrere CIs

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	können manchmal dieselbe Funktion ausführen.
Mustertext	Text für die Metrik, die der stummgeschalteten Warnung zugeordnet ist.
Metrik	Protokolltext oder -schlüssel, der einen Zähler- oder Anzeigewert in den Daten darstellt. Zum Beispiel Muster, Rohmetriken, Stichwort, Schweregrad, alle Event-Metriken
Erstellt	Datum und Uhrzeit, zu der die Metrik der Liste hinzugefügt wurde.

Zugehörige Informationen

Irrelevante Warnungen stummschalten

Normale Wichtigkeit einer Warnungsmetrik wiederherstellen

Stummgeschaltete Warnung oder signifikante Warnung wiederherstellen

Wenn eine stummgeschaltete oder als signifikant markierte Warnung nicht mehr besonders behandelt werden soll, können Sie die normale Relevanz der Metrik wiederherstellen, die an der Generierung der Warnung beteiligt ist.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Wichtig: Ab dem Vancouver-Release ist der **Operator-Arbeitsbereich** veraltet und wird durch Service Operations-Arbeitsbereichersetzt. Informationen zum neuen Verfahren finden Sie im entsprechenden Thema in der Dokumentation Service Operations-Arbeitsbereich für ITOM: Normale Wichtigkeit einer Warnungsmetrik wiederherstellen.

Beeinflussen der Anomalie-Erkennung mit lexikalischen Stichwörtern

Beeinflussen Sie, wie Health Log Analytics Anomalien findet, indem Sie Stichwörter verwalten, nach denen in Ihren Protokolldaten gesucht wird. Wenn Text in Protokolldaten für eine Quelle mit einem lexikalischen Stichwort übereinstimmt, das einen angegebenen Schwellenwert überschreitet, identifiziert das System eine Anomalie und generiert eine Warnung.

Health Log Analytics durchsucht Ihre Protokolle nach Wörtern, die auf wichtige Probleme hinweisen können. Lexikalische Stichwörter wie „abgestürzt“ oder „fehlgeschlagen“ als Signalbedingungen, die möglicherweise Aufmerksamkeit erfordern. Die Anwendung legt für jedes lexikalische Stichwort einen Schwellenwert basierend auf dem Muster des normalen Vorkommens in den Protokollen fest.

Wenn Health Log Analytics Ihre Protokolle scannt, identifiziert es alle Vorkommen des Stichworts. Wenn die Häufigkeit eines lexikalischen Stichworts in den Protokolldaten für eine Quelle den angegebenen Schwellenwert überschreitet, erkennt das System eine Anomalie und generiert eine Warnung.

Health Log Analytics enthält viele standardmäßige globale Schlüsselwörter. Sie können diese globalen Stichwörter oder Ausdrücke, die für alle Quelltypen gelten, hinzufügen, bearbeiten und löschen.

Hinweis: Informationen zum Hinzufügen eines bestimmten Stichworts, das einem bestimmten Quelltyp zugeordnet ist, finden Sie unter Quelltypfunktionen konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können lexikalische Stichwörter wie folgt verwalten:

- Lexikalische Stichwörter für Health Log Analytics hinzufügen, bearbeiten oder löschen

  Globale Stichwörter oder Ausdrücke hinzufügen, bearbeiten und löschen.

- Warnungen generierende lexikalische Stichwörter anzeigen

  Zeigen Sie die Liste der lexikalischen Stichwörter an, die auf wichtige Probleme in Protokolleinträgen hinweisen können. Standardmäßig werden in der Tabelle nur globale Stichwörter aufgelistet.

Lexikalische Stichwörter für Health Log Analytics hinzufügen, bearbeiten oder löschen

Verwalten Sie die Stichwörter, nach denen Health Log Analytics in Ihren Protokolldaten sucht.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
In den Protokolldaten werden Begriffe wie „Crash“ oder „Failed“ als lexikalische Stichwörter bezeichnet, da sie auf Probleme hinweisen, die der Aufmerksamkeit bedürfen. Wenn Text in Protokolldaten für eine Quelle mit einem lexikalischen Stichwort übereinstimmt, das einen angegebenen Schwellenwert überschreitet, identifiziert das System eine Anomalie und generiert eine Warnung.

Wichtig: Ein lexikalisches Stichwort unterscheidet sich von einem Schlüssel in einem `Schlüssel:Wert`-Paar in einer Protokollzeile. Zum Beispiel ist *`Hostname`* ein Schlüssel, der einen Wert annimmt: den Namen oder die IP-Adresse des Hosts. Im Gegensatz dazu ist ein Stichwort wie *`Failed`* selbst wichtig und nimmt keinen Wert an.

Die Anwendung enthält viele standardmäßige globale Stichwörter. Sie können globale Stichwörter oder Ausdrücke hinzufügen, bearbeiten und löschen. Diese Stichwörter gelten für alle Quelltypen.

Hinweis: Informationen zum Hinzufügen eines bestimmten Stichworts, das einem bestimmten Quelltyp zugeordnet ist, finden Sie unter Quelltypfunktionen konfigurieren.

Prozedur
1. Navigieren zu **Alle** > **Health Log Analytics** > **Anomalie-Erkennung protokollieren** > **Lexikalische Stichwörter**.
   Standardmäßig werden in der Tabelle „Lexikalische Stichwörter“ nur globale Stichwörter aufgelistet.
2. Wahlweise: Fügen Sie ein globales Stichwort hinzu.
   a. Wählen Sie **Neu**.
   b. Füllen Sie die Felder des Formulars aus.

Formular „Lexikalische Stichwörter“

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für das Stichwort

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Regulärer Ausdruck	Regulärer Ausdruck („Regex"), mit dem Übereinstimmungen definiert werden.
Exact match (Genaue Übereinstimmung)	Option, damit Health Log Analytics dem genauen regulären Ausdruck entspricht. Beispiel: „NullPointerException" würde in einer Nachricht nicht mit dem regulären Ausdruck „exception" übereinstimmen. Dieses Feld wird automatisch auf **True** gesetzt.
Groß-/Kleinschreibung beachten	Option, damit Health Log Analytics nach einer Übereinstimmung des regulären Ausdrucks sucht, bei der die Groß-/Kleinschreibung übereinstimmt. Dieses Feld wird automatisch auf **False** gesetzt.
Analyseumfang	Bereich von Quelltypen, in denen Health Log Analytics nach dem Stichwort in den Protokolldaten sucht: Die Auswahlmöglichkeiten lauten wie folgt: ▪ **Alle Quelltypen** ▪ **Angegebener Quelltyp**
Excluded source types (Ausgeschlossene Quelltypen)	Quelltypen, denen das Stichwort nicht zugeordnet ist. Health Log Analytics sucht in den Protokolldaten dieser Quelltypen nicht nach dem Stichwort.

c. Wählen Sie **Absenden** aus.

3. Wahlweise: Bearbeiten Sie ein globales Stichwort.

a. Klicken Sie in der Liste auf das Stichwort, das Sie bearbeiten möchten.

b. Bearbeiten Sie im Formular die relevanten Felder.

c. Wählen Sie **Aktualisieren**.

4. Wahlweise: Löschen Sie eines oder mehrere globale Stichwörter.

a. Markieren Sie die Zeile des angegebenen Stichworts, das Sie löschen möchten.

b. Wählen Sie in der Liste „Aktionen für ausgewählte Zeilen" unten auf der Seite **Löschen**.

c. Wählen Sie **OK** aus.

Zugehörige Informationen

Warnungen generierende lexikalische Stichwörter anzeigen

Warnungen generierende lexikalische Stichwörter anzeigen

Zeigen Sie die Liste der lexikalischen Stichwörter an, die auf wichtige Probleme in Protokolleinträgen hinweisen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

Navigieren zu **Alle** > **Health Log Analytics** > **Anomalie-Erkennung protokollieren** > **Lexikalische Stichwörter**.
Die Tabelle „Lexikalische Stichwörter“ wird angezeigt. Standardmäßig werden in der Tabelle nur globale Stichwörter aufgelistet.

Weitere Informationen über das Hinzufügen, Bearbeiten oder Löschen globaler Stichwörter finden Sie unter Lexikalische Stichwörter für Health Log Analytics hinzufügen, bearbeiten oder löschen.

Informationen zum Hinzufügen eines bestimmten Stichworts, das einem bestimmten Quelltyp zugeordnet ist, finden Sie unter Quelltypfunktionen konfigurieren.

Reduzierung des Rauschens durch Hinzufügen erweiterter Protokollwarnungsfilter

Verwenden Sie erweiterte Protokollwarnungsfilter, um zu bestimmen, ob eine Warnung zugelassen oder verworfen werden soll. Diese Filter reduzieren das Rauschen, indem sie Warnungen verwerfen, die nicht auf ein schwerwiegendes Problem hinweisen.

Sie können erweiterte Protokollwarnungsfilter hinzufügen, um Warnungen für die von Ihnen definierten Bedingungen zu scannen. Sie können beispielsweise einen Filter definieren, der Warnungen aus bestimmten Protokollquellen oder Warnungen für Anomalien verwirft, die den angegebenen Schwellenwert nicht überschreiten.

Einige Beispiele für Aktionen, die mit erweiterten Filtern möglich sind:

- Warnung nur bei Anomalien, die auf mehreren Hosts auftreten.
- Keine Warnung bei Anomalien, die außerhalb der Arbeitszeit auftreten.
- Keine Warnung auslösen, wenn die Anomalie den angegebenen Schwellenwert nicht überschreitet.
- Warnung nur bei Anomalien, die Teil einer Korrelation sind.

Sie können erweiterte Protokollwarnungsfilter wie folgt verwalten:

- Erweiterte Protokollwarnungsfilter erstellen

  Fügen Sie erweiterte Protokollwarnungsfilter hinzu, um Warnungen nach von Ihnen angegebenen Bedingungen zu scannen. Die Filter reduzieren das Rauschen, indem Warnungen verworfen werden, die kein schwerwiegendes Problem anzeigen. Während der Entwicklung eines Filters können Sie den Filter jederzeit testen, aktualisieren, veröffentlichen oder aktivieren.

- Ändern Sie den Filter weiter, indem Sie den Filterdatensatz aus der Filterlisteerneut öffnen. Sie können den Filter dann bearbeiten, testen, veröffentlichen und aktivieren.

Weitere technische Informationen zu Protokollwarnungsfiltern finden Sie im Artikel Erweiterte Protokollwarnungsfilterung [KB0863538] in der Knowledge Base Now Support.

Erweiterte Protokollwarnungsfilter erstellen

Fügen Sie erweiterte Protokollwarnungsfilter hinzu, um Warnungen nach von Ihnen angegebenen Bedingungen zu scannen. Die Filter reduzieren das Rauschen, indem Warnungen verworfen werden, die kein schwerwiegendes Problem anzeigen. Während der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Entwicklung eines Filters können Sie den Filter jederzeit testen, aktualisieren, veröffentlichen oder aktivieren.

Vorbereitungen

Die Funktionen „Disable Alert Rule Engine“ (Warnungsregel-Engine deaktivieren) und „Disable Detection Rule Engine“ (Erkennungsregel-Engine deaktivieren) müssen sich im Status AUS befinden. Sie legen die Werte fest, indem Sie zu navigieren **Health Log Analytics** > **Health Predictive AI Ops Administration** > **Funktionen**.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

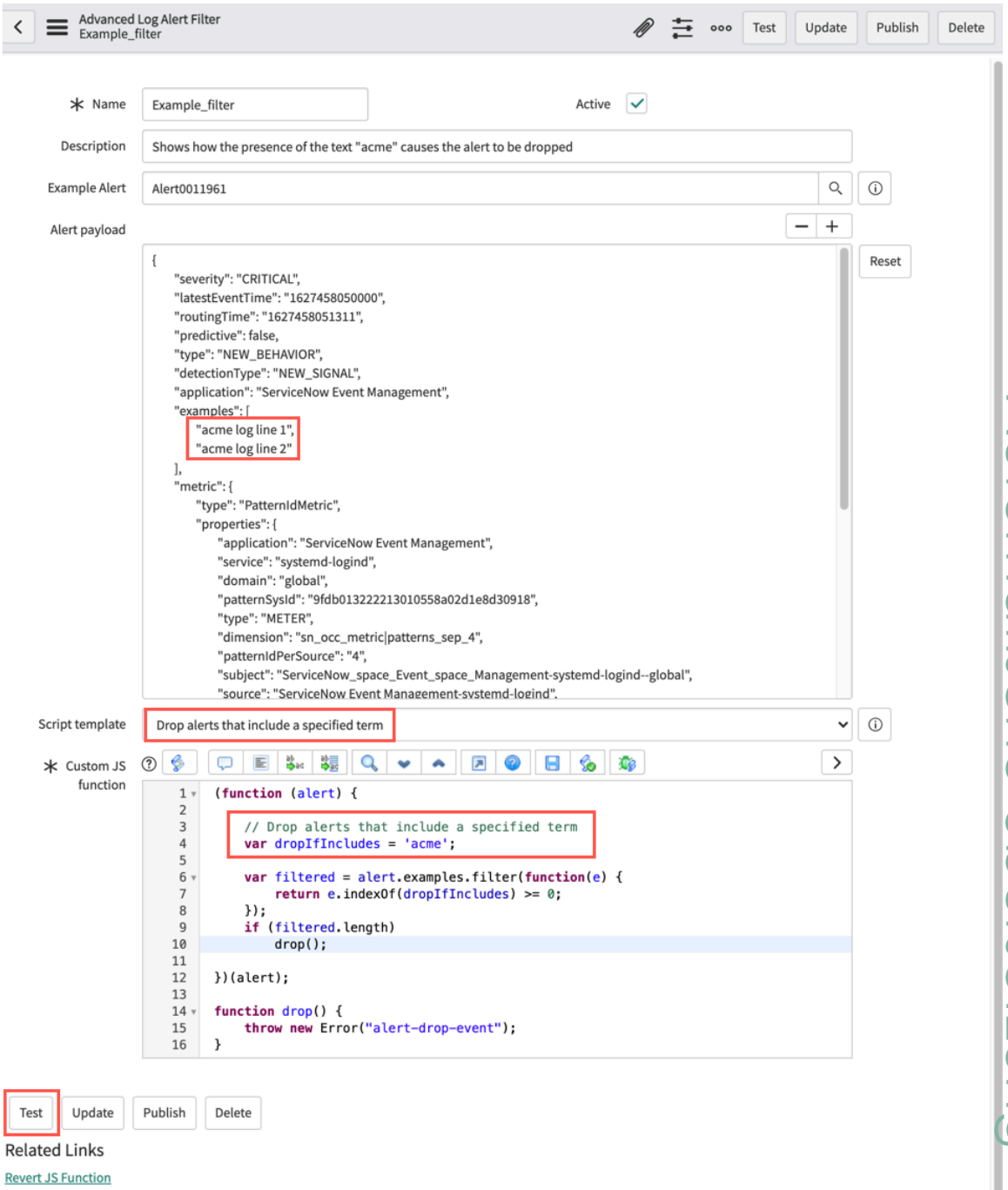
1. Navigieren zu **Health Log Analytics** > **Anomalie-Erkennung protokollieren** > **Erweiterter Protokollwarnungsfilter**.
2. Wählen Sie **Neu**.
3. Geben Sie einen eindeutigen und beschreibenden Namen für den Filter an.
4. Wahlweise: Geben Sie eine Beschreibung für den Betrieb des Filters ein.
5. Wählen Sie im Feld **Skriptvorlage** das Skript aus, das Ihrer beabsichtigten Logik am ehesten entspricht.
   Die Vorlage kann als Ausgangspunkt für Ihren benutzerdefinierten Skriptcode dienen. Nachdem Sie eine Vorlage ausgewählt haben, wird das Textfeld Benutzerdefinierte JS-Funktionen mit der entsprechenden JavaScript-Funktion ausgefüllt. Die JavaScript-Funktion wendet den Filter auf die Nutzlastdaten der Warnung an und lässt die Warnung entweder zu oder fallen. Die Warnungsnutzlast besteht aus dem Text und den Metadaten für die Art der Warnung, die der Filter analysiert.
6. Speichern Sie den Datensatz, indem Sie **Absenden** auswählen.
   Um weiterhin die Filter ändern zu können, müssen Sie den Datensatz aus der Filterliste wieder öffnen. Sie können den Filter dann bearbeiten, testen, veröffentlichen und aktivieren.
7. Bearbeiten Sie den Standardtext der **Warnungsnutzlast**, um die beabsichtigte Logik zu testen.

   Um Ihre Änderungen zu entfernen und das Textfeld „Warnungsnutzlast“ wiederherzustellen, klicken Sie auf **Zurücksetzen**.

   Um es Ihnen leichter zu machen, bietet Health Log Analytics Beispielwarnungen mit vorkonfigurierten Nutzlasten. Wählen Sie eine Beispielwarnung im Feld **Beispielwarnung** aus, um die Nutzlast im Textfeld „Warnungsnutzlast“ anzuzeigen.
8. Wahlweise: Speichern Sie die aktuellen Werte des Filters ohne Tests, indem Sie **Aktualisieren** auswählen.
9. Wenn Ihr Inhalt für die Warnungsnutzlast und Ihre JavaScript-Funktion abgeschlossen sind, wählen Sie **Test**.
   Um den Warnungsvorgang zu simulieren, speichert das System die Filterwerte, wendet den Filter auf den Text der **Warnungsnutzlast** an und zeigt dann eines der folgenden Ergebnisse an:
   - `Warnung wird verworfen.`
   - `Warnung ist zulässig.`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

JavaScript testen, um festzustellen, ob die Warnung zugelassen oder verworfen wird



Hinweis: Wenn sich Ihre neue JavaScript-Funktion nicht wie erwartet verhält, können Sie zur zuletzt veröffentlichten Funktion zurückkehren, indem Sie auf den zugehörigen Link **JS-Funktion zurücksetzen** klicken.

10. Wiederholen Sie den Vorgang zum Aktualisieren der Warnungsnutzlast und zum Testen der JavaScript-Funktion so oft wie erforderlich.
11. Wenn Sie mit dem Filter zufrieden sind, speichern Sie seine Werte, und bestimmen Sie, ob er auf den Protokollstream angewendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um die Werte zu speichern und den Filter auf den Protokollstream anzuwenden, stellen Sie sicher, dass das Kontrollkästchen **Aktiv** aktiviert ist, und wählen Sie **Veröffentlichen**.
- Um den Filter zu speichern, ohne ihn auf den Protokollstream anzuwenden, deaktivieren Sie das Kontrollkästchen **Aktiv** und wählen **Veröffentlichen**.

Hinweis: Wenn Sie einen veröffentlichten Filter bearbeiten, müssen Sie den geänderten Filter veröffentlichen, um ihn auf den Protokollstream anzuwenden.

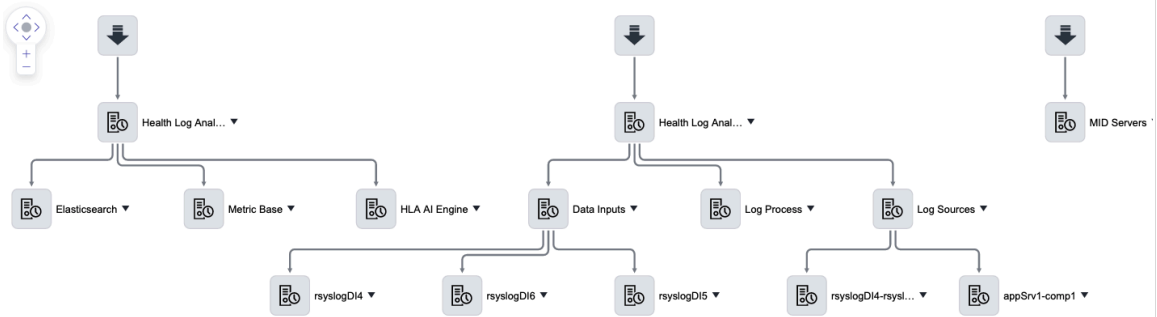
Ergebnisse
Die Werte des aktiven Filters werden gespeichert. Wenn Sie die Option „Aktiv“ wählen, wird der Filter auf den Protokollstream angewendet.

Health Log Analytics-Systemintegritätswarnungen in der Servicezuordnung anzeigen

Die Zuordnung der Serviceinstanz ServiceNow Ereignismanagement enthält ein Modell der Health Log Analytics -Kernkomponenten und der Systemintegritätswarnungen, die sich auf sie auswirken.

Health Log Analytics und die Anwendung Ereignismanagement bilden einen einzigen Service. Durch Anzeigen der Configuration Items (CIs), aus denen Health Log Analytics besteht, und ihrer Beziehungen können Sie visualisieren, wie sich HLA-Systemintegritätsprobleme auf den Service auswirken.

HLA-Komponenten in der Zuordnung der Ereignismanagement-Serviceinstanz



Von Health Log Analytics werden Selbstintegritätsprüfungen dazu verwendet, die Integrität der zugehörigen Komponenten zu überwachen. Wenn ein Systemintegritätsproblem erkannt wird, wird von einer Benachrichtigung eine Warnung ausgelöst. Systemintegritätswarnungen werden auf den betroffenen CIs in der Servicezuordnung angezeigt. Ein farbiger Balken auf einem betroffenen CI zeigt die Kritikalitätsstufe der Warnung an: Ein roter Balken bedeutet eine kritische Warnung, ein orangefarbener Balken eine schwerwiegende Warnung und ein gelber Balken eine Warnung mit Schweregrad „gering“.

Der rote Balken auf diesem CI zeigt beispielsweise eine kritische Warnung an:

Wenn sich die Warnung auf das übergeordnete Objekt auswirkt, weist das übergeordnete Objekt einen Balken derselben Farbe auf. Weitere Informationen finden Sie unter Auswirkung von Warnungen auf CIs in Servicezuordnungen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können in Bezug auf das Problem Detailinformationen zu einer Warnung anzeigen und dann zur Behebung des Problems die in der Benachrichtigung vorgeschlagene Aktion ausführen. Weitere Informationen finden Sie unter Health Log Analytics selbst-Integritätsprüfungen , Benachrichtigungen, und vorgeschlagene Aktionen.

Überwachte Komponenten

Komponente	Was wird überwacht
Health Log Analytics – Core	• Elasticsearch • Metrikbasis • HLA-KI-Engine
Health Log Analytics	• Dateneingaben • Protokollquellen **Hinweis:** Neue Dateneingaben und Protokollquellen werden der Servicezuordnung automatisch hinzugefügt.
Protokollerfassungsprozess	Alle Elemente, die sich auf den Protokollerfassungsprozess auswirken.

Zugehörige Informationen

Health Log Analytics-Systemintegritätsprobleme in der Servicezuordnung identifizieren

Health Log Analytics-Systemintegritätsprobleme in der Servicezuordnung identifizieren

Zeigen Sie Systemintegritätsprobleme Health Log Analytics mit (HLA) in der Zuordnung der Serviceinstanz ServiceNow Ereignismanagement an.

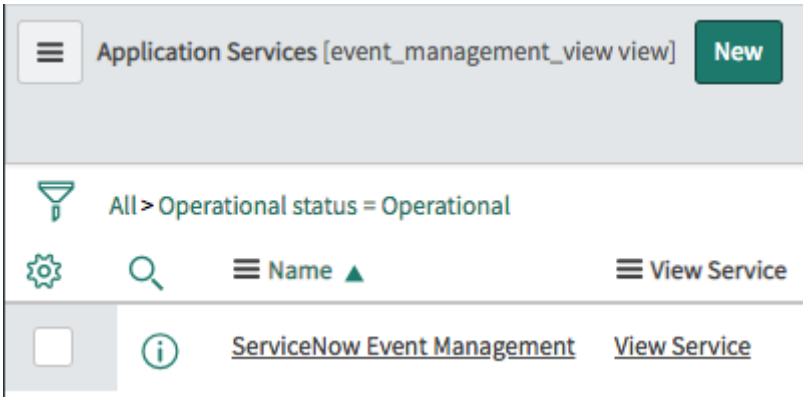
Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Durch Anzeigen der Configuration Items (CIs), aus denen Health Log Analytics besteht, und ihrer Beziehungen können Sie visualisieren, wie sich HLA-Systemintegritätsprobleme auf den Service auswirken. Weitere Informationen finden Sie unter Health Log Analytics-Systemintegritätswarnungen in der Servicezuordnung anzeigen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Services** > **Serviceinstanzen**.
2. Suchen Sie auf der Seite **„Serviceinstanzen“** nach ServiceNow Ereignismanagement, und wählen Sie **Service anzeigen**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Zuordnung der Serviceinstanz Ereignismanagement zeigt die Kernkomponenten Health Log Analytics von und die Systemintegritätswarnungen, die sie betreffen.

3. Identifizieren Sie in der Servicezuordnung Health Log Analytics Systemintegritätsprobleme.
4. Zeigen Sie problembezogene Detailinformationen zu einer Warnung an.

Nächste Maßnahme

Beheben Sie den Gegenstand der Warnung, indem Sie die in der Benachrichtigung vorgeschlagene Aktion ausführen. Weitere Informationen finden Sie unter Health Log Analytics selbst-Integritätsprüfungen , Benachrichtigungen, und vorgeschlagene Aktionen.

Zugehörige Informationen

Health Log Analytics-Systemintegritätsbenachrichtigungen

Zeigen Sie die Einstellungen der Systemfunktionen für Health Log Analytics an

Zeigen Sie die Einstellungen für alle Health Log Analytics -Systemfunktionen an. Mit diesen Funktionen können Sie viele Vorgänge konfigurieren, die sich auf Ihre Arbeit auswirken. Der -Administrator kann Funktionen für Sie aktivieren oder deaktivieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

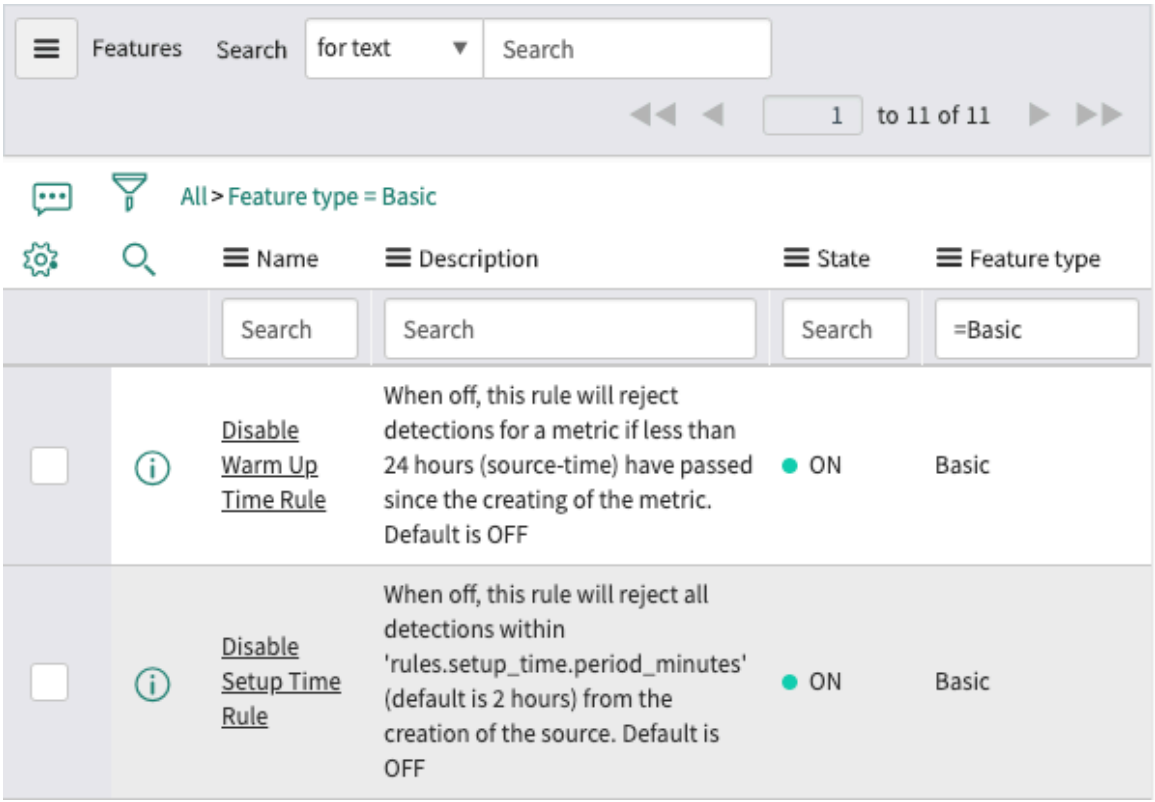
Prozedur

1. Navigieren zu **Alle** > **Health Log Analytics** > **Health Predictive AI Ops Administration** > **Funktionen**.

   Eine vollständige Definition der Funktion wird im Feld **Description** (Beschreibung) angezeigt.

   Standardmäßig zeigt die Tabelle die Systemfunktionen, die Administratoren am häufigsten ändern. Um die vollständige Liste der Funktionen anzuzeigen, verwenden Sie die Filteroptionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Wahlweise: Bitten Sie Ihren Administrator, eine Funktion zu aktivieren oder zu deaktivieren, indem er die Einstellung **Status** aktualisiert.

Analytics und Reporting in Health Log Analytics

Gewinnen Sie wertvolle Einblicke in die Anzahl der vorhergesagten IT-Probleme, bevor Ihre Anwender betroffen waren, und in die Kosten, die Ihre Organisation dadurch gespart hat, indem Sie Analytics und Reporting in Health Log Analyticsverwenden.

Platform Analytics and Reporting-Lösungen für Health Log Analytics

Platform Analytics-Lösungen enthalten vorpaketierte Performance Analytics- und Reporting-Inhalte zur Verwendung mit anderen Now Platform-Produkten. Performance Analytics und Reporting-Lösung bietet wertvolle Einblicke in die Anzahl der IT-Probleme Health Log Analytics, die vorhergesagt wurden, bevor Ihre Benutzer betroffen waren, und in die Höhe der Kosteneinsparungen, die Ihrem Unternehmen durch die Verhinderung kritischer Ausfälle entstanden sind.

Erforderliche Rollen

Dieser Lösung sind die folgenden Rollen und Aufgaben zugeordnet:

- Now Platform-Administrator (admin): Installiert und aktiviert diese Lösung und nimmt alle erforderlichen Änderungen an Systemeigenschaften vor.
- Performance Analytics Administrator (pa_admin): Überprüft die Indikatoren, Aufgliederungen, Widgets und Dashboards. Richtet die Datenerfassung ein und startet sie. Gibt die Dashboards für die entsprechenden Stakeholder frei.

Zugehörige Informationen

Analytics- und Reporting-Lösungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Performance Analytics und Reporting-Lösung für Health Log Analytics aktivieren

Aktivieren Sie die Anwendung ServiceNow Store des Inhaltspakets für Performance Analytics und Reporting-Lösung.

Vorbereitungen

Aktivieren Sie die vollständige Abonnementversion von Performance Analytics auf der Instanz, auf der Sie diese Performance Analytics und Reporting-Lösung aktivieren. Sie können Performance Analytics in einer Instanz außerhalb der Produktion aktivieren, ohne ein Abonnement zu erwerben. Weitere Informationen finden Sie unter Performance Analytics-Abonnement aktivieren .

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle Anwendungen** > **ServiceNow Store**.
2. Suchen Sie nach Health Log Analytics , und vergewissern Sie sich, dass Sie über die erforderlichen gültigen Berechtigungen verfügen.

   Sie benötigen ein HI-Konto und die Berechtigung zum Anfordern von Anwendungen für die betreffenden Instanzen. HI-Konto und Instanz müssen zum selben Unternehmen gehören. Weitere Informationen finden Sie unter Install a ServiceNow Product (ServiceNow-Produkte installieren) im ServiceNow Store.
3. Suchen Sie nach `Health Log Analytics (sn.occ)`.
4. Installieren Sie die Anwendung.

   Wenn Sie diese Anwendung installieren, aktivieren Sie auch das Plugin „Performance Analytics - Premium“ (com.snc.pa.premium).

   Hinweis: Für dieses Plugin wird eine zusätzliche Gebühr fällig.

Performance Analytics und Reporting-Lösung für Health Log Analytics konfigurieren

Führen Sie Diagnosen aus, überprüfen Sie Komponenten, passen Sie sie an, und beginnen Sie mit der Datenerfassung.

Vorbereitungen

Ein Now Platform-Administrator muss die Plugins für Inhaltspakete oder die ServiceNow Store-Anwendung für diese Performance Analytics und Reporting-Lösung installiert haben.

Erforderliche Rolle: pa_admin

Prozedur

1. Führen Sie Diagnosen für alle Datensätze aus.

   Diese Diagnosen können viele Nichtübereinstimmungen zwischen der Konfiguration Ihrer Platform Analytics and Reporting-Lösungen und Ihren Tabellen erfassen. Weitere Informationen finden Sie unter Performance Analytics-Diagnose .
2. Navigieren zu **Alle** > **Performance Analytics** > **Administrationskonsole**.
3. Überprüfen Sie den Namen des mit Performance Analytics und Reporting-Lösunginstallierten Dashboards:
   Health Log Analytics Übersichts- Dashboard
4. Öffnen Sie die Registerkarte **Indikatorquellen**.

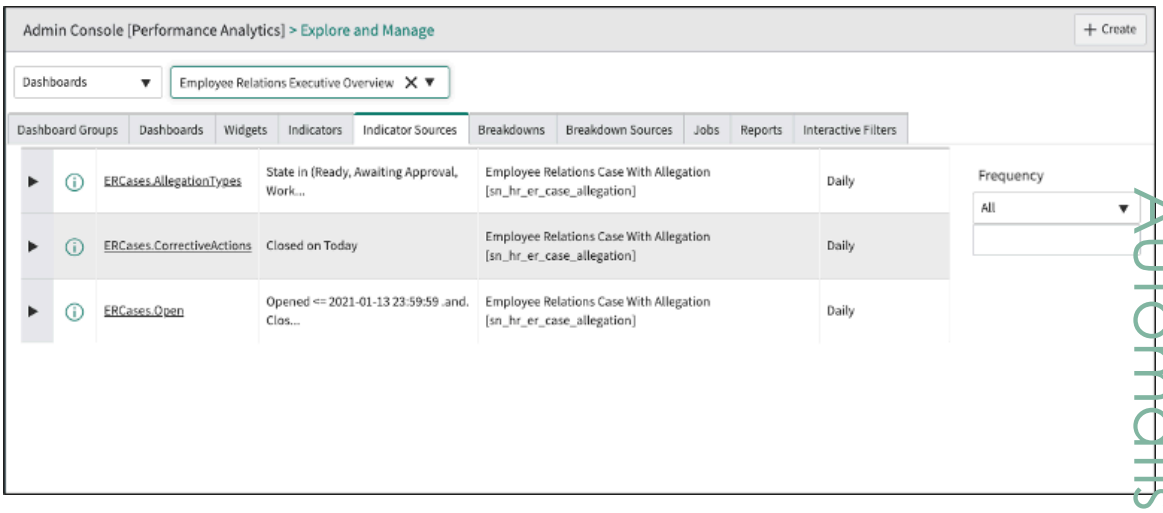
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Für jedes Dashboard, das in dieser Performance Analytics und Reporting-Lösung enthalten ist:

   a. Filtern Sie die Indikatorquellen nach dem Dashboardnamen.

      Example

      Hier werden die Indikatorquellen dargestellt, die im Dashboard für Selfservice-Analysen der Leitungsübersicht für Mitarbeiterbeziehungen gefiltert wurden.



   b. Überprüfen Sie die Faktentabelle, die Bedingungen und die Häufigkeit der Indikatorquellen im Vergleich zur Datenstruktur auf Ihrer eigenen Instanz.

      Wichtig: Achten Sie besonders auf Zeitstempelfelder wie „Gelöst“ oder „Erstellt“, auf die im Feld **Bedingungen** verwiesen wird. Möglicherweise müssen Sie andere Zeitstempelfelder verwenden.

   c. Öffnen Sie bei Bedarf eine Indikatorquelle, und nehmen Sie Korrekturen vor.

   d. Wenn Sie einen Indikatorquelldatensatz bearbeiten, wechseln Sie zur zugehörigen Liste „Indikatoren“, und überprüfen Sie das Feld **Bedingungen** für jeden Indikator.

      Das Ändern der Indikatorquelle kann sich auch auf die zusätzlichen Bedingungen für die einzelnen Indikatoren auswirken.

6. Wenn Sie die Zeitstempelfelder in einer beliebigen Indikatorquelle geändert haben, ändern Sie auch alle zugehörigen Performance Analytics-Skripts.

   Weitere Informationen finden Sie unter Performance Analytics-Skripte aktualisieren .

7. Öffnen Sie die Registerkarte „Aufgliederungsquellen“.
8. Für jedes Dashboard, das in dieser Performance Analytics und Reporting-Lösung enthalten ist:

   a. Filtern Sie die Aufgliederungsquellen nach dem Dashboardnamen.

   b. Überprüfen Sie die unter Aufgliederungsquellen überprüfen beschriebenen Bedingungen der Aufgliederungsquelle.

9. Navigieren zu **Alle** > **Performance Analytics** > **Aufträge**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Richten Sie die Verlaufsaufgabe für Performance Analytics und Reporting-Lösung, *[PA HLA] Historic Data Collection*ein, und führen Sie sie aus.
11. Bearbeiten und aktivieren Sie den geplanten Datensammlungsauftrag für Performance Analytics und Reporting-Lösung, *[PA HLA] Historic Data Collection*.

Dashboard „Health Log Analytics Overview“ (Health Log Analytics - Übersicht)

Im Dashboard „Health Log Analytics Overview“ (Health Log Analytics - Übersicht) wird Performance Analytics verwendet, um einen Trend aus Verlaufsdaten sowie regelmäßige Berichte bereitzustellen.

Ab dem Xanadu-Release ist das Dashboard Health Log Analytics „Übersicht“ veraltet und wurde durch das Dashboard „HLA-Vorgänge“ ersetzt. Das Dashboard „HLA-Vorgänge“ verwendet Performance Analytics, um Ihnen die Überwachung von Protokolldaten, Warnungen und Fehlerrateninformationen in Service Operations-Arbeitsbereich zu ermöglichen und Probleme zu beheben, sobald sie im System auftreten. Weitere Informationen finden Sie unter Dashboard für HLA-Vorgänge.

Health Log Analytics-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Health Log Analytics.

Mit Health Log Analytics installierte Komponenten

Durch Aktivieren der Plugins „Health Log Analytics, „Health Log Analytics Viewer“ und „Health Log Analytics Core“ werden mehrere Komponenten hinzugefügt.

Hinweis: In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Plugins

Plugin	Beschreibung
Health Log Analytics	Health Log Analytics ist eine KI-gestützte Protokollanalyselösung, die IT-Incidents verhindern kann, bevor Benutzer betroffen sind. Sie identifiziert automatisch Ihre Umgebung, protokolliert und prognostiziert IT-Incidents, generiert Warnungen und bietet Expertenvorschläge zur Behebung von Problemen. Health Log Analytics ist eine App aus dem ServiceNow Store. Nach der Installation ist das Modul verfügbar, Sie können sich jedoch dafür entscheiden, es nicht zu nutzen. Abhängigkeit: • Health Log Analytics Zentral • Die ServiceNow® Ereignismanagement Anwendung
Health Log Analytics-Betrachter	Ereignismanagement-Betreiber verwenden das Plugin „Health Log Analytics Viewer“,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Plugin	Beschreibung
	um Protokolle nach Zeitstempel oder Zeitbereich zu durchsuchen. Mit dem Health Log Analytics Viewer können Ereignismanagement-Betreiber nach einem bestimmten Protokolltext suchen und die Häufigkeit der Treffer in einem bestimmten Zeitraum anzeigen. Abhängigkeit: ServiceNow® Ereignismanagement Anwendung.
Health Log Analytics Zentral	Dieses Plugin enthält wichtige Komponenten für Health Log Analytics, z. B. die KI-Engine und Elasticsearch. Health Log Analytics Core ist eine App aus dem ServiceNow Store. Nach der Installation ist das Modul verfügbar, Sie können sich jedoch dafür entscheiden, es nicht zu nutzen. Abhängigkeit: ServiceNow® Ereignismanagement Anwendung.

Rollen

Health Log Analytics verwendet die folgenden Rollen.

Rollentitel [Name]	Beschreibung
Ereignismanagement-Administrator [evt_mgmt_admin]	Hat Lese- und Schreibzugriff auf alle Ereignismanagement-Funktionen zum Konfigurieren von Health Log Analytics.
Ereignismanagement-Betreiber [evt_mgmt_operator]	Hat Lesezugriff auf alle Ereignismanagement-Funktionen. Hat Schreibzugriff auf Warnungen, um den Lebenszyklus der Warnungenen zu verwalten. Verfügt über die itil-Rolle, um Incidents verwalten zu können, die aus Warnungen erstellt wurden. Kann auch Vorgänge für Warnungen wie Bestätigen, Schließen, Öffnen von Vorfällen und Ausführen von Korrekturen aktivieren

Listen

Mit Health Log Analytics werden die folgenden Listen hinzugefügt.

Tabelle [name]	Beschreibung
Erweiterte Protokollwarnungsfilterung [sn_occ_advanced_alert_filtering]	Steuert die Verarbeitung von Warnungsmetriken mit Feedbackoptionen. Ermöglicht die Bereitstellung komplexeren Feedbacks für die KI-Engine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle [name]	Beschreibung
	Ab Version 20.0.11 - Juli 2021 von Anwendung Health Log Analytics, verfügbar im ServiceNow Store , wird diese Erklärung nicht mehr angezeigt.
Erweiterte Protokollwarnungsfilterung [sn_occ_advanced_alert_filter]	Steuert die Verarbeitung von Warnungsmetriken mit Feedbackoptionen. Ermöglicht die Bereitstellung komplexeren Feedbacks für die KI-Engine **Hinweis:** Diese Funktion wird unterstützt in Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, verfügbar im ServiceNow Store .
Dateneingaben [sn_occ_base_data_input_config]	Ermöglicht das Einrichten von Dateneingabe-Connectors zum Streamen von Protokolldaten in die Instanz
Dateneingabezuordnung [sn_occ_event_mapper]	Ermöglicht die Zuordnung von unbearbeiteten Protokolldaten, die in Ihre Instanz gestreamt werden, um zu bestimmen, wie Health Log Analytics sie verarbeitet
Dateneingabe-Präprozessor [sn_occ_data_input_preprocess_screen]	Ermöglicht das Bearbeiten von unbearbeiteten Protokolldaten, bevor das System sie zuordnet und strukturiert
Warnung definieren [sn_occ_custom_alert]	Ermöglicht das Erstellen benutzerdefinierter Warnungen basierend auf einem vordefinierten Regelsatz
Ausgeschlossene Werte [sn_occ_auto_service_normalizer]	Ermöglicht die Konfiguration von Health Log Analytics, um das Extrahieren bestimmter Protokolldaten zu stoppen, die nicht aussagekräftig genug sind oder redundanten Text oder Informationen enthalten
Extrahierte Werte [sn_occ_auto_service_mapper]	Ermöglicht die Konfiguration von Health Log Analytics, um einen bestimmten Begriff aus einem Feld zu extrahieren und einer angegebenen Komponente zuzuordnen
Funktionen [sn_occ_features]	Listet alle Health Log Analytics-Funktionen auf. Die Funktionen können aktiviert und deaktiviert werden.
Lexikalische Stichwörter [sn_occ_lexical_keywords]	Zeigt alle standardmäßigen lexikalischen Stichwörter an, nach denen Health Log Analytics in Protokolldaten sucht
Protokollkorrelator [sn_occ_log_correlator]	Zeigt alle Korrelatoren an, die bestimmen, ob unterschiedliche Warnungen mit derselben Gruppe korreliert werden sollen. Ermöglicht das Hinzufügen von Korrelatoren zu Health Log Analytics
Protokollquellen [sn_occ_sources]	Bietet eine Ansicht aller Dateneingabequellen, wenn die Protokolldaten zugeordnet wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle [name]	Beschreibung
	Ermöglicht die Steuerung von Eigenschaften und Korrelatoren für diese Quellen
Stummgeschaltete Metriken [sn_occ_metric_state]	Zeigt alle stummgeschalteten Warnungsmetriken zusammen mit den stummgeschalteten Komponenten an. Ermöglicht die Reaktivierung der stummgeschalteten Warnungsmetriken
Quelltyp [sn_occ_source_type]	Enthält die Quelltypen, die im Zuordnungsprozess extrahiert wurden
Quelltypstruktur [sn_occ_source_type_structure]	Ermöglicht die Feinabstimmung der Quelltypstruktur. Bietet eine Ansicht aller Quelltypen, wenn die Protokolldaten zugeordnet wurden. Mit Quelltypen wird definiert, wie Health Log Analytics bestimmte Quellen behandelt und wie die Protokolle analysiert werden.
Streaming-Quellen [sn_occ_log_streaming_source_stats]	Ermöglicht die Überwachung aller Entitäten, die Protokolldaten an die Instanz streamen
Systemintegrität – Benachrichtigungen [sn_occ_health_check]	Zeigt alle Systemintegritätsbenachrichtigungen zusammen an und ermöglicht die Aktualisierung ihres Status
Systemeigenschaften [sn_occ_system_settings]	Zeigt Systemeigenschaften an und ermöglicht die Anpassung ihrer Werte
Zeitstempelformate [sn_occ_timestamp_formats]	Zeigt vordefinierte Zeitstempelformate an. Ermöglicht das Definieren und Hinzufügen von Zeitstempelformaten
Zeitzonen [sn_occ_time_zones]	Aktiviert das Löschen von Datensätzen in sn_occ_time_zones für Benutzer mit der Rolle evt_mgmt_admin

Forms

Mit Health Log Analytics werden die folgenden Formulare hinzugefügt.

Tabelle [name]	Beschreibung
Beats-Dateneingabe [sn_occ_data_input_config_filebeat]	Ermöglicht die Konfiguration erweiterter Einstellungen für Beats-Dateneingabe-Connector
Beats Linux (Filebeat) [sn_occ_data_input_connector_filebeat]	Ermöglicht die Konfiguration von Filebeat-Dateneingabe-Connectors
Elasticsearch-Dateneingabe [sn_occ_data_input_config_filebeat]	Ermöglicht die Konfiguration einer Elasticsearch-Dateneingabe
MID-Server-Dateneingabe [sn_occ_data_input_config_midserver]	Ermöglicht die Konfiguration einer MID-Server-Dateneingabe
Rsyslog [sn_occ_data_input_connector_rsyslog]	Ermöglicht die Konfiguration von Rsyslog-Dateneingabe-Connectors
Rsyslog-Dateneingabe [sn_occ_data_input_config_rsyslog]	Ermöglicht die Konfiguration erweiterter Einstellungen für Rsyslog-Dateneingabe-Connector

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle [name]	Beschreibung
TCP-Dateneingabekonfiguration [sn_occ_data_input_config_tcp]	Ermöglicht die Konfiguration erweiterter Einstellungen für TCP-Dateneingabe-Connectors
Windows Beats [sn_occ_data_input_connector_winbeat]	Ermöglicht die Konfiguration von Windows Beats-Dateneingabe-Connectors
WinLog Beats [sn_occ_data_input_connector_winlogbeat]	Ermöglicht die Konfiguration von WinLog Beats-Dateneingabe-Connectors

Unterstützte Dateneingaben für Health Log Analytics

Health Log Analytics (HLA) ermöglicht Ihnen, Ihre Instanz ServiceNow mit verschiedenen Arten von Dateneingaben zu verbinden.

HLA unterstützt die folgenden Dateneingabetypen:

- Passive Dateneingaben (Listener), die darauf warten, dass Protokolldaten an sie übertragen werden. Diese Dateneingaben erfordern, dass ein Netzwerkport auf MID-Servergeöffnet ist:

  Rsyslog, Beats, Splunk, TCP, UDP, MID-Server, GCP PubSubund REST API.

  Die Agent Client Collector-Dateneingabe wird für die Verwendung mit der Anwendung Agent Client Collector Log Analytics unterstützt, die im ServiceNow Store verfügbar ist.

- Aktive Dateneingaben (Puller), bei denen es sich um Connectors handelt, die Daten aus Daten-Repositorys abrufen:

  Elasticsearch, Splunk-Polling, Amazon CloudWatch, Amazon S3, Microsoft Azure Log Analytics, Microsoft Azure Event Hubs, und Apache Kafka.

  Für alle aktiven Dateneingaben unterstützt Health Log Analytics Cluster MID-Server von für den Failover-Schutz. Die aktive Dateneingabe wird auf einem einzelnen MID-Server im Cluster ausgeführt. Wenn MID-Server fehlschlägt, verschiebt das System seine Aufgaben zum nächsten verfügbaren MID-Server im Cluster in einer konfigurierten Reihenfolge.

  Die Dateneingabe Elasticsearch ruft mithilfe von Anmeldeinformationen Daten aus einem Daten-Repository oder einer Datenbank ab. Wenn sich Ihre Daten in Elasticsearch befinden, muss Health Log Analytics über Folgendes verfügen:

  - Berechtigungen zum Abfragen von Elasticsearch

    Eine der folgenden Arten von Anmeldeinformationen:

    - Standardauthentifizierung (Benutzer und Kennwort)
    - AWS, für Elasticsearch unter Amazon AWS Cloud

  - Netzwerkverbindung zum relevanten Elasticsearch-Cluster

  Hinweis: Health Log Analytics muss auf den richtigen Index verweisen, um mit dem Abrufen der Daten zu beginnen.

Native ServiceNow Dateneingaben

Streamingprotokolle von Cloud Observability nach Health Log Analytics

Health Log Analytics kann Protokolldaten verarbeiten, die aus der Anwendung ServiceNow® Cloud Observability, ehemals Lightstep, erfasst werden. HLA richtet automatisch die erforderliche Konfiguration ein, um das Protokoll-Streaming von Cloud Observability als Teil der nativen Integration zu aktivieren. Das Einrichten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

der Verbindung von Cloud Observability zu HLA muss in der Anwendung Cloud Observability erfolgen. In HLA behandeln Sie Protokolldatensätze aus Cloud Observability auf die gleiche Weise wie alle anderen Datensätze für Dateneingabezuordnung und Quelltypstruktur, wie in Automatische Zuordnung und Zuordnung von Protokolldaten und Quelltypstruktur anpassenerläutert. Weitere Informationen zu Cloud Observabilityfinden Sie in der Dokumentation zu Cloud Observability erkunden .

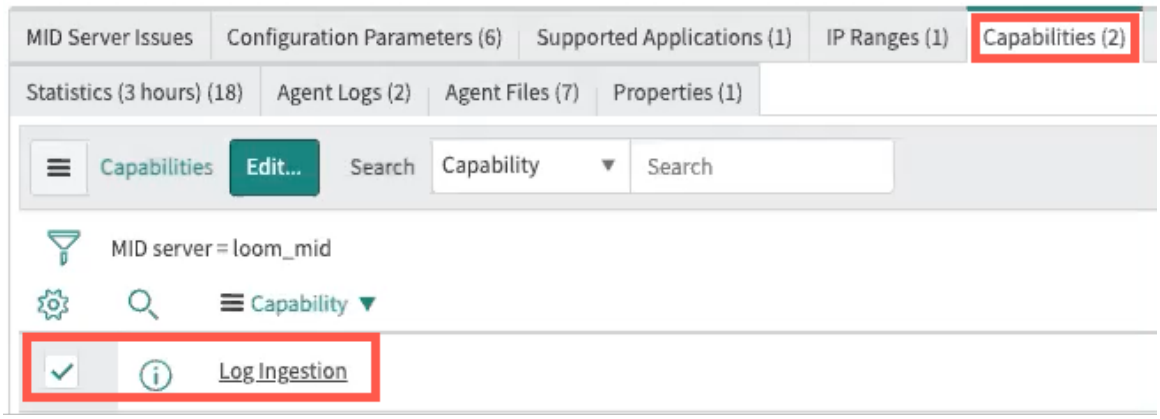
Zugehörige Informationen

Health Log Analytics in Ihrer Instanz von ServiceNow einrichten

MID-Server-Proxy-Vorbedingungen für das Streaming von Protokollen an HLA

Anforderungen für die Verwendung eines MID-Server -Proxy zum Streamen von Protokolldaten an Health Log Analytics.

- Verwenden Sie einen Squid-Proxy MID-Server, um das Streaming von Protokolldaten an Health Log Analyticszu aktivieren. Weitere Informationen finden Sie unter Proxy-Server-Konfiguration für MID Servers, die für Cloud-Discovery und Cloud Provisioning and Governance verwendet werden.
- Installieren und konfigurieren Sie den MID-Server -Proxy mit aktivierter Protokollerfassungsfunktion.



Konfigurieren Sie außerdem die folgenden Eigenschaften:

- mid.proxy.use_proxy = wahr
- mid.proxy.host =<proxy_ip>
- mid.proxy.port =<proxy_port>

Health Log Analytics-Konfigurationspräferenzen

Häufig verwendete Einstellungen für Health Log Analytics-Eigenschaften und allgemeine Konfiguration

MID-Server-Einstellungen

- Die MID-Server-Protokollerfassungsfunktion muss aktiviert sein.

Hinweis: Das Aktivieren von **„Alle Fähigkeiten“** für MID-Server beinhaltet das Aktivieren der Protokollerfassungsfunktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verwenden Sie nach Möglichkeit dedizierte MID Servers für die Protokollerfassung.
- Damit MID Servers mehrere Produkte ausführen können, muss Health Log Analytics für jede MID-Server-Thread-Konfiguration mindestens die JVM-Speichereinstellung (Java Virtual Machine) für das Standardprodukt aufweisen.

Die bevorzugten MID-Server -Einstellungen für Health Log Analytics sind:

- ◦ CPUs: 8
  ◦ RAM: 32 GB
  ◦ Netzwerkbandbreite: Bis zu 10 Gbit/s
  ◦ EBS-Bandbreite: Bis zu 4.750 Mbit/s
  ◦ Maximale Java-Heap-Größe für MID-Server: 8.192 MB

  Mit den obigen Spezifikationen ist der erwartete Durchsatz bei der Protokollerfassung in einer Washington DC-Instanz wie folgt:
  ◦ Bei einer Protokollnachricht von 300 Byte: 20.000
  ◦ Bei einer Protokollnachricht von 1,1 KB: 12.300
  ◦ Für eine Protokollnachricht von 2 KB: 7.970

  Die Mindestanforderungen für das Streaming von Protokollen an Health Log Analytics sind:
  ◦ CPUs: 4
  ◦ RAM: 16 GB
  ◦ Java-Heap-Größe für MID-Server: 8 GB

  Allgemeine Informationen finden Sie unter: Systemanforderungen für MID-Server .

- Um den Durchsatz der Protokollerfassung zu erhöhen, können Sie entweder die ulimit-Einstellung oder die Netzwerkbandbreite erhöhen oder die Größe der gestreamten Protokolle verringern. Die ulimit-Einstellung kann für einen einzelnen MID-Server konfiguriert werden. Die Korrelation zwischen dem ulimit und dem Durchsatz kann jedoch nicht geändert werden.

  In der folgenden Tabelle sind die ulimit-Einstellungen für offene Dateien im Zusammenhang mit dem Netzwerkdurchsatz auf dem MID-Server aufgeführt . Es zeigt die Größe der Protokolle, die vom MID-Server an den Agent gestreamt werden, und die gRPC-Streaming-Rate, die dem Durchsatz entspricht.

Ulimit-Einstellungen im Verhältnis zum Durchsatz

Warteschlangentyp	Protokollzeilengröße	gRPC-Rate
In der Speicherwarteschlange	300 Byte	18,000
In der Speicherwarteschlange	1.1 KB	13,000
In der Speicherwarteschlange	2 KB	10.000
Datenträgerbasierte Warteschlange	300 Byte	11.000

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warteschlangentyp	Protokollzeilengröße	gRPC-Rate
Datenträgerbasierte Warteschlange	1,1 KB	5.000
Datenträgerbasierte Warteschlange	2 KB	3,000

Ab dem Release von August 2024können Sie die Kommunikation MID-Server von mit der ServiceNow-Instanz verbessern, indem Sie den Lightning gRPC-Client verwenden, der die Geschwindigkeit des Protokoll-Streamings auf Health Log Analytics um das bis zu Sechsfache erhöhen kann. Der Lightning gRPC-Client erfordert eine manuelle Konfiguration zum Aktivieren. Weitere Informationen finden Sie im Artikel „Lightning gRPC-Client – Aktivierung der neuen MID gRPC-Streaming-Architektur“ [KB1648419] in der Knowledge Base Now Support.

- Standardmäßig ist die Anzahl der Dateneingaben pro MID-Server auf 10 beschränkt. Sie können diese Einschränkung für einen einzelnen MID-Server oder für alle MID Servers konfigurieren.
- Sowohl im FIPS- als auch im Nicht-FIPS-Modus müssen MID Servers mit Health Log Analytics-Funktionalität in der Java Runtime Environment (JRE) 11 oder höher ausgeführt werden.

Hinweis: Zur Unterstützung von BC-FIPS Version 2.0 erfordert Health Log Analytics ein Upgrade auf Version 34.0.37, Dezember 2024.

Einstellungen für Protokollquellenaufbewahrung

Standardmäßig ist die Protokollaufbewahrung pro Quelle auf drei Tage festgelegt. Diese Einstellung kann nicht geändert werden.

Bei Verwendung der Health Log Analytics Anwendung, Version 22.0.12 – Dezember 2021 und höher, verfügbar im ServiceNow Store können Sie die Protokollaufbewahrungsrichtlinie pro Quelle oder für mehrere Quellen auf einmal ändern. Weitere Informationen finden Sie unter Aufbewahrungszeitraum für Protokollquellen ändern.

Health Log Analytics-Systemintegritätsbenachrichtigungen

Health Log Analytics Systemintegritätsbenachrichtigungen tragen dazu bei, sich über potenziell gefährliche Bedingungen zu informieren. Sie können den Status einer Benachrichtigung manuell anpassen, während das Problem behoben wird.

Von Health Log Analytics werden Selbstintegritätsprüfungen dazu verwendet, die Integrität der zugehörigen Komponenten zu überwachen. Wenn ein Systemintegritätsproblem erkannt wird, wird eine Benachrichtigung erstellt und eine E-Mail an alle Abonnenten gesendet. In der (unter „Health Log Analytics-Verwaltung“ verfügbaren) Liste **Systemintegrität – Benachrichtigungen** werden alle Benachrichtigungen zur HLA-Systemintegrität angezeigt, einschließlich der Benachrichtigungen zu internen Fehlern. Bitten Sie Ihren Administrator, die Benachrichtigungen zur Systemintegrität für Sie zu abonnieren.

Health Log Analytics – Systemintegrität – Benachrichtigungen

Feld	Beschreibung
Name	Header der Benachrichtigung.
Beschreibung	Beschreibung der Benachrichtigung.
Erstellt	Datum, an dem die Benachrichtigung erstellt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics – Systemintegrität – Benachrichtigungen (Fortsetzung)

Feld	Beschreibung
Status	Status der Benachrichtigung. • **Neu**: Die Benachrichtigung wurde neu hinzugefügt. • **Bestätigt**: Der Benachrichtigungsdatensatz wurde gelesen. • **In Bearbeitung**: Das in der Benachrichtigung beschriebene Problem wird aktuell behoben. Passen Sie den Wert manuell an. • **Geschlossen**: Das Problem ist nicht mehr aktiv. Passen Sie den Wert manuell an. **Hinweis:** Das Ändern des Status einer Benachrichtigung wirkt sich nicht auf den Status des darin beschriebenen Problems aus. Eine Benachrichtigung im Status „Geschlossen“ wird weiterhin in der Tabelle angezeigt. Die Benachrichtigung wird nur dann automatisch aus der Tabelle herausgefiltert, wenn das Problem als behoben erkannt wird (d. h. wenn der Status „Fehlerfrei“ auf **True** festgelegt ist).
Fehlerfrei	Feld, das den Status des in der Benachrichtigung genannten Problems angibt. In der Tabelle werden nur Benachrichtigungen angezeigt, bei denen der Statuswert „Fehlerfrei“ auf **False** festgelegt ist. Wenn das Problem als behoben erkannt wird, wird der Wert automatisch in **True** geändert, und die Benachrichtigung wird aus der Tabelle herausgefiltert.

Health Log Analytics selbst-Integritätsprüfungen , Benachrichtigungen, und vorgeschlagene Aktionen

Health Log Analytics bietet Selbstintegritätsprüfungen, Benachrichtigungen und vorgeschlagene Problemlösungsschritte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics-Systemintegritätsbenachrichtigungen

Selbstintegritätsprüfung	Benachrichtigung	Vorgeschlagene Aktion
Maximale Warteschlangengröße der KI-Engine überschritten	The AI engine is running at overcapacity (size=%s, threshold=%s, duration= %s). (Die KI-Engine wird mit Überkapazität ausgeführt.) As a result, the accuracy of anomaly detection might deteriorate. (Dadurch kann sich die Genauigkeit der Anomalie-Erkennung verschlechtern.)	Wenden Sie sich an den Support von ServiceNow.
Hohe Rate nicht klassifizierter Fehler in %s %s	"%s %s has a high rate of unclassified errors and is failing frequently. ("%s %s weist eine hohe Rate nicht klassifizierter Fehler auf und schlägt häufig fehl.)	Wenden Sie sich an den Support von ServiceNow.
Fehler beim Aufrufen der Glide-API	Errors invoking '%s' for %s. (Fehler beim Aufrufen von '%s' für %s.)	Wenden Sie sich an den Support von ServiceNow.
Protokollgrößenbeschränkung wurde überschritten	Log messages from %s: %s are being dropped because the log size limitation was exceeded. (Protokollnachrichten von %s: %s werden verworfen, da die Protokollgrößenbeschränkung überschritten wurde.)	Wenn der Unterschied gering ist, erhöhen Sie die Beschränkung der Protokollgröße, indem Sie die Eigenschaft *mid.data_inputs.max_length_bytes_per_* im Formular „MID-Server-Eigenschaften“ anpassen. Wenn die Protokolle zu lang oder mehrzeilig sind, können Sie auch die Protokollgröße an der Quelle der Protokolle ändern.
Übermäßiges Datenvolumen für Dateneingabe %s.	The data volume for data input %s is too high. (Das Datenvolumen für Dateneingabe %s ist zu hoch.) Log messages are being discarded. (Protokollnachrichten werden verworfen.)	Wenden Sie sich an den Support von ServiceNow.
Protokollnachrichten werden aufgrund einer fehlgeschlagenen automatischen Strukturierung verworfen	Log messages are being dropped because auto-structuring of Source Type %s failed. (Protokollnachrichten werden verworfen, da die automatische Strukturierung von Quelltyp %s fehlgeschlagen ist.)	Finden Sie im Quelltyp heraus, was dazu führen könnte, dass die automatische Strukturierung fehlschlägt. Überprüfen Sie die Fehlerprotokolle, um festzustellen, welche

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics-Systemintegritätsbenachrichtigungen (Fortsetzung)

Selbstintegritätsprüfung	Benachrichtigung	Vorgeschlagene Aktion
		Komponente oder Analyseaktion fehlschlägt.
Übermäßige Anzahl von Skriptfehlern pro Sekunde in %s:%s	The rate of script errors in %s:%s is too high. (Die Rate der Skriptfehler in %s:%s ist zu hoch.)	Überprüfen Sie den JavaScript-Analysefehler in der Quelle, die in der Nachricht angegeben ist: Bildschirm der Dateneingabezuordnung oder Bildschirm der Quelltypstruktur.
Protokollnachrichten, die die zulässige Anzahl von Eigenschaften überschreiten, werden verworfen	The source type %s contains multiple log messages with too many properties. (Der Quelltyp %s enthält mehrere Protokollnachrichten mit zu vielen Eigenschaften.) Such log messages are discarded. (Solche Protokollnachrichten werden verworfen.) Review the Source Type Structure record. (Überprüfen Sie den Datensatz der Quelltypstruktur.)	Überprüfen Sie im entsprechenden Datensatz der Quelltypstruktur die Eigenschaften, die extrahiert werden. Suchen Sie nach Skriptschleifen oder Bedingungen, die dazu führen könnten, dass zu viele Eigenschaften erstellt werden. Vermeiden Sie die Verwendung eines dynamischen Eigenschaftsnamens. Weitere Informationen finden Sie unter Quelltypstruktur verfeinern.
Es werden zu viele Cluster generiert. Die Genauigkeit der Anomalie-Erkennung könnte sich verschlechtern.	Too many clusters are being generated for Source Type %s. (Zu viele Cluster werden für Quelltyp %s generiert.) As a result, the accuracy of anomaly detection might deteriorate. (Dadurch kann sich die Genauigkeit der Anomalie-Erkennung verschlechtern.)	Überprüfen Sie die erstellten Muster, und vergewissern Sie sich, dass die Nachrichtenbezeichnung korrekt zugewiesen wird. Überprüfen Sie im Formular der Quelltypstruktur die Nachrichteneigenschaft.
Quellen werden sehr schnell erstellt	Sources are being created at a very high rate. (Quellen werden sehr schnell erstellt.) Data input %s was stopped automatically. (Dateneingabe %s wurde automatisch angehalten.)	Überprüfen Sie im Formular „Dateneingabezuordnung“ das Zuordnungsskript, und beheben Sie alle JavaScript-Fehler, die dazu führen könnten, dass zu viele Quellen erstellt werden.
Quelltypen werden sehr schnell erstellt	Source Types are being created at a very high rate. (Quelltypen werden sehr schnell erstellt.) Data input %s was stopped automatically.	Überprüfen Sie im Formular „Dateneingabezuordnung“ das Zuordnungsskript, und beheben Sie alle JavaScript-Fehler, die dazu führen könnten, dass zu viele Quelltypen erstellt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics-Systemintegritätsbenachrichtigungen (Fortsetzung)

Selbstintegritätsprüfung	Benachrichtigung	Vorgeschlagene Aktion
	(Dateneingabe %s wurde automatisch angehalten.)	
Metriken werden sehr schnell erstellt	Source Type %s is generating too many metrics. (Quelltyp %s generiert zu viele Metriken.) The properties %s were automatically classified as invalid. (Die Eigenschaften %s wurden automatisch als ungültig klassifiziert.)	Beobachten Sie im Formular der Quelltypstruktur die generierten Metriken. Stellen Sie sicher, dass die Metrikbezeichnung nur den erforderlichen Eigenschaften zugewiesen ist. Ein dynamischer Eigenschaftsname oder eine ungenaue JavaScript-Funktion können dazu führen, dass zu viele Eigenschaften generiert werden.
Die Verarbeitungsdauer von REST-Aufrufen in der KI-Engine ist zu lang	Processing of REST calls in the AI Engine is taking too long. (Die Verarbeitung von REST-Aufrufen in der KI-Engine dauert zu lange.)	Wenden Sie sich an den Support von ServiceNow.
Die Anzahl der verworfenen Protokollnachrichten ist zu hoch	Too many log messages are being discarded from source %s. (Zu viele Protokollnachrichten werden von der Quelle %s verworfen.)	Überprüfen Sie die Einstellungen für die Protokollaufbewahrung. Vergewissern Sie sich, dass der Zeitstempel der Protokollzeilen korrekt ist und keine zukünftige oder vergangene Zeit außerhalb des Aufbewahrungszeitraums darstellt.
Durch automatische Strukturierung wird die KI-Engine verlangsamt	Auto-structuring is slowing down the AI engine. (Durch automatische Strukturierung wird die KI-Engine verlangsamt.)	Wenden Sie sich an den Support von ServiceNow.
Protokollnachrichten werden aufgrund eines Fehlers bei der Zeitstempelanalyse verworfen	Log messages from %s %s are being dropped due to a timestamp parsing failure. (Protokollnachrichten von %s %s werden aufgrund eines Fehlers bei der Zeitstempelanalyse verworfen.) Suchen Sie in den Protokollen für die relevante Serviceinstanz , Instanz und Komponente, nach „Fehler beim Analysieren des Zeitstempels aus Protokollnachricht“, und beheben Sie das Problem.	Suchen Sie im Formular „Dateneingabezuordnung“ nach dem extrahierten Zeitstempel. Wenn dieser fehlt, navigieren Sie vom Formular zur entsprechenden Quelltypstruktur, und öffnen Sie die Registerkarte „Timestamp Parsing Error“ (Fehler bei Zeitstempelanalyse). Auf der Registerkarte wird das Problem angezeigt, das zum Analysefehler geführt hat. Beheben Sie das Problem.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics-Systemintegritätsbenachrichtigungen (Fortsetzung)

Selbstintegritätsprüfung	Benachrichtigung	Vorgeschlagene Aktion
Kein Rückgang des Arbeitsspeicherverbrauchs	Memory consumption hasn't dropped in the last few minutes. (Der Arbeitsspeicherverbrauch ist in den letzten Minuten nicht gesunken.)	Wenden Sie sich an den Support von ServiceNow.
Pingt zur Bestimmung der Verbindungsintegrität die Integritätsendpunkte der Elasticsearch-Cluster	Elasticsearch connectivity issues. (Elasticsearch-Verbindungsprobleme.)	Wenden Sie sich an den Support von ServiceNow.
Verwendet die Clientverbindungsprüfung der Metrikbasis zur Bestimmung der Verbindungsintegrität	Metric base connectivity issues. (Verbindungsprobleme bei Metrikbasis.)	Wenden Sie sich an den Support von ServiceNow.
Verwendet die Prüfung der Glide-Clientverbindung zur Bestimmung der Verbindungsintegrität	Glide connectivity problems. (Glide-Konnektivitätsprobleme.)	Wenden Sie sich an den Support von ServiceNow.
Die Dateneingabe weist den Status „Fehlgeschlagen" auf	The data input %s failed to stream logs. (Das Streamen von Protokollen von Dateneingabe %s ist fehlgeschlagen.)	Überprüfen Sie im Formular „Dateneingabe" die Verbindung zum MID-Server, und überprüfen Sie die Fehlermeldung.

Health Log Analytics Sprachunterstützung

Health Log Analytics bietet Unterstützung für internationale Sprachen. Die Standardsprache ist US-Englisch.

Abdeckung des Sprachsupports

Die derzeit für Health Log Analytics verfügbaren Sprachen sind: US-Englisch, UK-Englisch, Französisch, Deutsch, Italienisch, Japanisch und Spanisch.

Hinweis: Um stichwortbasierte Warnungen für andere Sprachen als Englisch zu erhalten, müssen dem System Stichwörter in der entsprechenden Sprache hinzugefügt werden, bevor Sie das Streaming starten. Wenden Sie sich an den Support ServiceNow von [], um Unterstützung zu erhalten.

Domänentrennung und Health Log Analytics

Domänentrennung wird für Health Log Analytics unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Domain Separation und Health Log Analytics overview

Domänentrennung ist in allen Aspekten der Anwendung Health Log Analytics vorhanden. Benutzer, die zu einer bestimmten Domäne gehören, sehen nur die Daten, die in ihrer eigenen Domäne vorhanden sind.

So funktioniert Domain Separation in Health Log Analytics

Wenn Daten mit einem einzelnen Health Log Analytics-Server domänengetrennt sind, kann jeder Managed Service Provider (MSP) die Protokolldaten nur in seiner eigenen Domäne oder den untergeordneten Domänen darunter sehen. Benutzer können Warnungen anzeigen, die Health Log Analytics nur in ihrer eigenen Domäne generiert. Aktionen zum Korrigieren der Warnungen gelten nur für den Bereich dieser Domäne. Standardmäßig werden alle Benutzer und Datensätze auf die übergeordnete Domäne festgelegt, es sei denn, der Administrator weist sie einer bestimmten Domäne zu.

Das Plugin „Health Log Analytics Domain Separation“ muss installiert sein, bevor Sie Ihre Dateneingaben in der Anwendung Health Log Analytics konfigurieren. Es gibt kein Setup-Verfahren für das Plugin. Installieren Sie das Plugin mit der Anwendung Health Log Analytics Version 21.0.1 - September 2021 und aktivieren Sie es dann. Stellen Sie sicher, dass Sie Ihre Daten logischen Silos zuordnen und Regeln und Entitäten konfigurieren.

Sie definieren die domänengetrennte Umgebung, wenn Sie Ihre Dateneingaben konfigurieren. Benutzer können Dateneingaben verwenden, die nur in ihrer eigenen Domäne verfügbar sind. Health Log Analytics erstellt Warnungen nur für Protokolle, die in diesen Dateneingaben ankommen. Alle relevanten Datensätze und die gesamte Datenverarbeitung im Health Log Analytics-Programmablauf befinden sich in derselben Domäne wie die Dateneingabe. Der Domänenname einer Dateneingabe wird in der Spalte **Domäne** angezeigt, die in den Tabellen Ihrer Instanz angezeigt wird.

Die Verwendung der Domänentrennung in Ihrer Instanz ist für Health Log Analytics transparent. Die Anwendung verwaltet alle Aspekte der Daten, z. B. Systemeinstellungen und benutzerdefinierte Vorgänge, separat. Wenn eine Eigenschaft geändert wird, wirkt sich der neue Wert nur auf neue Quellen in der spezifischen Domäne aus. Systemeigenschaften, die den Server betreffen, gelten für alle Domänen, da alle Domänen den Health Log Analytics-Server verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Health Log Analytics unterstützt bis zu 60 Kilobyte Events pro Sekunde (EPS) über alle Domänen hinweg, ohne die Möglichkeit, eine Servicelevel-Vereinbarung (SLA) für eine bestimmte Domäne bereitzustellen, und ohne Fairness. Wenn eine Domäne eine große Datenmenge streamt, verarbeitet der Health Log Analytics-Server sie. Andere Domänen können daher Latenz, Abbrüche oder andere Probleme erfahren, auch wenn sie eine geringe Anzahl von Protokollen streamen. Auf der MID-Server-Seite werden 10 Kilobyte EPS erwartet.

Anwendungsfälle

- Ein MSP möchte die Anwendung Health Log Analytics mehreren Kunden in einer ähnlichen Umgebung mit einer einzelnen Instanz bereitstellen.
- Eine Organisation mit vielen Mandanten möchte ihre vertraulichen Daten, wie beispielsweise Sicherheitsprotokolle, isolieren.
- Ein Administrator einer Mandantenorganisation möchte eine Dateneingabe nur für seine eigene Domäne definieren.
- Ein Operator in einer Mandantenorganisation möchte Protokolle nur in seiner eigenen Domäne anzeigen.
- Ein Operator in einer Mandantenorganisation möchte Feedback für Warnungen nur in seiner eigenen Domäne bereitstellen.
- Ein MSP-Administrator möchte Protokolldaten aus allen Mandantendomänen seiner Organisation anzeigen.

Zugehörige Informationen

Domänentrennung für Service Provider

Ergebnisfelder für JavaScript-Funktionstests

Beschreibung der Ergebnisfelder des JavaScript-Funktionstests.

Die folgenden Felder sind schreibgeschützt:

Feld	Beschreibung
Duration (ms) (Dauer (ms))	Verarbeitungszeit aller Beispiele in Millisekunden
Quelltypen	Die Anzahl der Quelltypen, die für diese Dateneingabe vorhergesagt oder erstellt wurden.
Quellen	Die Anzahl der Quellen, die für diese Dateneingabe vorhergesagt oder erstellt wurden.
Fehler	Die Anzahl der JavaScript-Fehler, die in allen Beispielen aufgetreten sind.
Nicht zugeordnet	Anzahl der Protokollzeilen, die nicht zugeordnet werden konnten. Diese Protokollzeilen sind Standard-Tags zugeordnet.
Muster	Die Anzahl der Protokollbeispiele, für die der Test ausgeführt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Der Standardwert ist 1.000. **Hinweis:** Sie können die Anzahl der Protokollbeispiele in der Systemeigenschaft „data_input_mapping.max_examples“ auf bis zu 5.000 Beispiele erhöhen. Weitere Informationen finden Sie unter Globale Health Log Analytics-Systemeigenschaften konfigurieren.

Zeigen Sie in den zugehörigen Listen die vorhergesagten oder erstellten Quelltypen und Quellen an.

Liste/Registerkarte	Beschreibung
Zuordnung des Ergebnis-Schlüssel-Werts	Die Ergebnisse der Ausführung der JavaScript-Funktion für die Protokollbeispiele.
Quelltypen (aus Beispielen)	Die vorhergesagten oder erstellten Quelltypen. **Hinweis:** Sie können bereits erstellte Quelltypen öffnen, indem Sie den entsprechenden Link auswählen.
Quellen (aus Beispielen)	Die vorhergesagten oder erstellten Quellen. **Hinweis:** Sie können bereits erstellte Quellen öffnen, indem Sie den entsprechenden Link auswählen.
Testergebnis	Die Protokollbeispiele, die zum Testen Ihrer JavaScript-Funktion verwendet werden, sortiert nach Quellen und Quelltypen. Die Liste **„Testergebnis“** zeigt die Anzahl der Protokollbeispiele für jede Kombination aus Quelle und Quelltyp an. Sie wird aktualisiert, wenn die Protokollbeispiele aktualisiert werden und Sie mit dem Testen Ihres Skripts beginnen. Die Liste ist mit Beispielen in der Tabelle **„Zuordnungsbeispiele“** verknüpft, die das Ergebnis der JavaScript-Funktion für jedes Beispiel anzeigt. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.
Quelltypstrukturen	Die Quelltypstrukturen für diese Dateneingabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste/Registerkarte	Beschreibung
	Durch Überprüfen der Quelltypstrukturen können Sie den Daten-Flow besser verstehen.

Health Log Analytics Schweregradzuordnung

Health Log Analytics (HLA) verwendet allgemeine Schweregradwerte, um Schweregradbezeichnungen in der Quelltypstruktur zu identifizieren.

Die Zuordnungstabelle **für den Protokollschweregrad** veranschaulicht, wie HLA Schweregradwörter aus Rohprotokollen identifiziert (in der linken Spalte angezeigt), sie ihren eigenen Schweregradwerten zuordnet (mittlere Spalte) und sie dann in Warnungen Ereignismanagement (rechte Spalte) darstellt.

Schweregradzuordnung protokollieren

Schweregrad des Rohprotokolls	HLA-Protokollschweregrad	Ereignismanagement **Schweregrad der Warnung**
TRACE	TRACE	Stichwortbasiert
AUSFÜHRLICH	TRACE	Stichwortbasiert
FEIN	TRACE	Stichwortbasiert
FINER	TRACE	Stichwortbasiert
vom Feinsten	TRACE	Stichwortbasiert
DEBUG	DEBUG	Stichwortbasiert
DBG	DEBUG	Stichwortbasiert
KONFIGURATION	DEBUG	Stichwortbasiert
INFORMIERT	INFORMIERT	Stichwortbasiert
HINWEISE	INFORMIERT	Stichwortbasiert
INF	INFORMIERT	Stichwortbasiert
INFO	INFORMIERT	Stichwortbasiert
UNBEKANNT	UNBEKANNT	Stichwortbasiert
HINWEIS	HINWEIS	NIEDRIG
BENACHRICHTIGUNG	HINWEIS	NIEDRIG
WARNUNG	WARNUNG	MITTEL
WARN	WARNUNG	MITTEL
FEHLER	FEHLER	HOCH
ERR	FEHLER	HOCH
KRITISCH	KRITISCH	KRITISCH
KRIT	KRITISCH	KRITISCH
FAT	KRITISCH	KRITISCH
FATAL	KRITISCH	KRITISCH

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schweregradzuordnung protokollieren (Fortsetzung)

Schweregrad des Rohprotokolls	HLA-Protokollschweregrad	Ereignismanagement **Schweregrad der Warnung**
SCHWERWIEGEND	KRITISCH	KRITISCH
WARNUNG	WARNUNG	KRITISCH
NOTFALL	NOTFALL	KRITISCH
EMER	NOTFALL	KRITISCH

Hinweis: Wenn Ihr Rohprotokoll numerische Schweregrade oder nicht erkannte Wörter enthält, ordnen Sie diese Werte der Spalte „HLA-Protokollschweregrad“ zu, indem Sie mit der JS-Funktion in der Quelltypstruktur eine bedingte Anweisung erstellen. Weitere Informationen finden Sie unter Quelltypstruktur anpassen.

Beschreibungen der Konfigurationsfelder für die Dateneingabe

Dieser Abschnitt enthält Beschreibungen der Felder in den Konfigurationsformularen für Dateneingaben Health Log Analytics.

Rsyslog, Filebeat- oder Winlogbeat-Dateneingabe-Konfigurationsfelder

Beschreibung der Felder in den Konfigurationsformularen für Dateneingaben Rsyslog, Filebeat und Winlogbeat.

Basiskonfiguration

Registerkarte „Erste Schritte“

Feld	Beschreibung
Dateneingabename	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
MID-Server	Der MID-Server, an den die Protokolle gestreamt werden **Hinweis:** • Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. Dies ist ein Pflichtfeld.
Port	Port auf dem MID-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
	Wählen Sie einen Port innerhalb des vorgeschlagenen Bereichs aus dem Array aus. Der Port darf nicht von einem anderen Prozess belegt sein. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.
Inhaltspaket	(Linux nur mit Filebeat) Das zu verwendende Inhaltspaket. Inhaltspakete enthalten Standardquelltypen und Zuordnungsskriptvorlagen. Health Log Analytics aktiviert das ausgewählte Paket automatisch und verwendet das zugehörige Zuordnungsskript für die Zuordnung der Dateneingabequellen. Weitere Informationen finden Sie unter Health Log Analytics Inhaltspakete für eine schnellere Amortisierungszeit.

Registerkarte Tagging und Bindung

Feld	Beschreibung
Pfad	Der vollständige Pfad, aus dem Protokolle gestreamt werden sollen. Sie können einen Platzhalter verwenden. Dies ist ein Pflichtfeld.
Service Instanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest.
Komponente	Gerätetyp oder Stapelebene als Kontext für die Protokolle, die zur Anomalieerkennung und -korrelation verwendet werden. Beispiel: Tomcat. Komponenten stellen normalerweise CIs in der CMDB dar. Mehrere Komponenten werden häufig in einer einzigen Serviceinstanz zusammengefasst.
Quelltyp	Quelltyp, der definiert, wie Health Log Analytics eine bestimmte Anwendung behandelt und die Protokolldaten analysiert. Beispiel: Tomcat Catalina.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte Tagging und Bindung (Fortsetzung)

Feld	Beschreibung
	Jede Dateneingabe kann je nach Vielfalt ihrer Protokollformate mehrere Quelltypen haben. Serviceinstanzen und -komponenten können eine beliebige Anzahl von Quelltypen aufweisen.

Erweiterte Konfiguration

Für Rsyslog Dateneingaben:

Formular für erweiterte Rsyslog-Konfiguration

Feld	Beschreibung	Standardwerte
SSL/TLS verwenden	Hiermit geben Sie an, ob SSL/TLS verwendet werden soll.	
Look up hostnames (Nach Hostnamen suchen)	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen.	false
Anzahl der Boss-Threads	Anzahl der Threads, mit denen Verbindungen verwaltet werden	1
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden	4
Lesezeitüberschreitung in Sekunden	Zeitüberschreitung in Sekunden seit dem letzten Lesen. Wenn die Zeitüberschreitung abläuft, schließt das System den Kanal.	30
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für erweiterte Rsyslog-Konfiguration (Fortsetzung)

Feld	Beschreibung	Standardwerte
	werden, wenn der MID-Server ausgelastet ist.	

Für Dateneingaben, die Beats Agents verwenden:

Formular für erweiterte Konfiguration von Beats

Feld	Beschreibung	Standardwert
Client inactivity timeout (sec) (Zeitüberschreitung bei Client-Inaktivität (Sek.))	Die Zeitüberschreitung in Sekunden, nach der ein inaktiver Kanal geschlossen wird	15
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden	4
Default time zone (Standardzeitzone)	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	falsch

Splunk Konfigurationsfelder für die Dateneingabe

Beschreibung der Felder im Formular Splunk zur Konfiguration der Dateneingabe.

Basiskonfiguration

Registerkarte „Erste Schritte“

Feld	Beschreibung
Dateneingabename	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
MID-Server	Der MID-Server, an den die Protokolle gestreamt werden **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. Dies ist ein Pflichtfeld.
Port	Port für den MID-Server. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port auf dem MID-Server öffnet. Dies ist ein Pflichtfeld.
Transportprotokoll	Das Protokoll, das zum Streamen von Protokollnachrichten an Ihre ServiceNow-Instanz verwendet wird. • TCP: Bei Verwendung des TCP-Protokolls (Transmission Control Protocol) erreichen alle Protokolle die Instanz. Die Splunk-Pipeline kann jedoch blockiert werden, wenn der MID-Server inaktiv ist oder die Verbindung unterbrochen wird. TCP ist das Standardtransportprotokoll. • UDP: Bei Verwendung des UDP-Protokolls (User Datagram Protocol) wird die Splunk-Pipeline niemals blockiert. Einige Protokolle werden jedoch möglicherweise gelöscht, bevor sie die Instanz erreichen. Weitere Informationen zum Streamen von Protokolldaten mit dem TCP- oder UDP-Transportprotokoll finden Sie im Artikel Streaming Splunk data using Heavy Forwarder: Select TCP or UDP [KB0998928] (Splunk mit Heavy Forwarder streamen: TCP oder UDP auswählen in der Now Support-Knowledge Base).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
Vorbereitete Daten verwenden	Option zum Erfassen von Protokolldaten von Splunk im vorverarbeiteten Format („gekocht“), das Splunk für die Weiterleitung verwendet. Durch das Erfassen von Daten in HLA in diesem Format wird sichergestellt, dass jede Protokollzeile die relevanten kontextbezogenen Informationen beibehält, die in Splunk eingebettet sind. **Hinweis:** Wenn Sie diese Option auswählen, müssen die Dateien „`props.conf`“ und „`transforms.conf`“ während der Konfiguration der Dateneingabe für Splunk nicht bearbeitet werden.
Zeitzone der Weiterleitung verwenden	Option zum Übergeben von Informationen über die Zeitzone, in der sich der Forwarder befindet. MID-Server verwendet diese Informationen, um die Zeitzone anzupassen, aus der die Protokolle eingehen. Diese Option ist relevant, wenn Splunk universelle Weiterleitungen verwendet werden.
Komprimierung aktivieren	Option zum Senden von Protokollen im komprimierten Format. Durch das Senden von Protokollen in einem komprimierten Format wird die Größe der übertragenen Daten minimiert. Dies ist wichtig, wenn große Mengen von Protokolldaten verarbeitet werden. Diese Option ist relevant, wenn Splunk universelle Weiterleitungen verwendet werden, und kann nur verwendet werden, wenn SSL/TLS aktiviert ist.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwerte
SSL/TLS verwenden	Hiermit geben Sie an, ob SSL/TLS verwendet werden soll.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwerte
	Hinweis: Zum Senden von Protokollen in einem komprimierten Format muss SSL/TLS aktiviert sein.	
Look up hostnames (Nach Hostnamen suchen)	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen.	false
Anzahl der Boss-Threads	Anzahl der Threads, mit denen Verbindungen verwaltet werden	1
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden	4
Lesezeitüberschreitung in Sekunden	Zeitüberschreitung in Sekunden seit dem letzten Lesen. Wenn die Zeitüberschreitung abläuft, schließt das System den Kanal.	30
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	

Splunk Konfigurationsfelder für Abfragedateneingabe

Beschreibung der Felder im Konfigurationsformular Splunk für Abfragedateneingabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basiskonfiguration

Registerkarte „Erste Schritte“

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option, um zu bestimmen, ob ein bestimmtes MID-Server - oder ein MID-Server -Cluster verwendet werden soll. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.
MID	(Nur, wenn das Feld **Ausführen** auf auf Spezifischer MID-Server festgelegt ist.) Der MID-Server, an den die Protokolle gestreamt werden. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur, wenn das Feld **Ausführen** auf auf MID-Server Cluster festgelegt ist.) Der Cluster MID-Server, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen MID-Server im Cluster ausgeführt, bis dieser MID-Server ausfällt. Das System verschiebt dann alle Dateneingabeaufgaben entsprechend der konfigurierten Reihenfolge zu den nächsten verfügbaren MID-Server im Cluster. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: • Health Log Analytics unterstützt nur Failover-Cluster MID-Server. In diesen Clustern sind mehrere MID Servers zum Failover-Schutz in einer Gruppe zusammengefasst. Wenn Sie ein Cluster aus dem Dateneingabeformular auswählen, werden in der Liste der Cluster MID-Server nur Failover-Cluster angezeigt. • Der Cluster MID-Server darf nur MID Servers enthalten, die die Standardauthentifizierung unterstützen. mTLS wird für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden MID-Server im Cluster aktiviert werden. Wenn die Protokollerfassung für den aktiven MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn es mindestens einen MID-Server enthält und weniger als 10 Dateneingaben darauf ausgeführt werden, selbst wenn dieser MID-Server ausgefallen ist. Weitere Informationen zu MID-Server -Clustern finden Sie unter MID-Server-Cluster konfigurieren . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, erstellen Sie eine Serviceinstanz , und fügen Sie ihr CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
Übertragung	Das Protokoll, das zum Streamen von Protokollnachrichten an Ihre ServiceNow-Instanz verwendet wird.
Quellenanzahl	Die Anzahl der Protokollquellen, die von dieser Dateneingabe erstellt wurden
Status	Status der Dateneingabe
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde

Erweiterte Konfiguration

Registerkarte „Transport“

Feld	Beschreibung
Server-URL	Die für den Zugriff auf die REST API Splunk verwendete URL.
Abfrage	Die Abfrage, die Splunk zum Durchsuchen Ihrer Daten verwendet.
Authentifizierungstyp	Der Authentifizierungstyp. • Standardauthentifizierung: Sendet mit jeder HTTP-Anforderung einen Anwendernamen und ein Passwort. Die Standardauthentifizierung ist einfacher als die tokenbasierte Authentifizierung, aber weniger sicher. • Token-Authentifizierung: Der Client erhält ein Token von einem Authentifizierungsserver und verwendet dieses Token zur Authentifizierung bei Splunk.
Splunk Alias für Anmeldeinformationen für Abfragen	Der zu verwendende Anmeldeinformationsalias. Geben Sie einen Splunk -Polling-Alias für Anmeldeinformationen an, indem Sie das Lupensymbol und dann entweder einen vorhandenen Anmeldeinformationsalias aus der Liste **„Aliasse für Verbindungen und Anmeldeinformationen“** auswählen oder **Neu** wählen, um einen neuen Datensatz zu erstellen. Der ausgewählte Alias für Anmeldeinformationen kann Basisauthentifizierungs-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Transport“ (Fortsetzung)

Feld	Beschreibung
	und Tokenauthentifizierungs-Anmeldeinformationen enthalten. Informationen zum Erstellen von Anmeldeinformationsaliasen finden Sie unter Aliasse für Anmeldeinformationen für Discovery .
Von	Datum und Uhrzeit, ab der Splunk die Daten durchsucht.
An	Datum und Uhrzeit, bis zu der Splunk die Daten durchsucht.

Registerkarte „Erweitert“

Feld	Beschreibung
Max. Anzahl von Dokumenten pro Abfrage	Die maximale Anzahl von Dokumenten, die jedes Mal abgerufen werden, wenn Protokolldaten von Splunkabgerufen werden. Standard: 10.000.
Splunk Zeitüberschreitung für Anforderung (Sekunden)	Die maximale Zeit in Sekunden, die für den Datenabruf verwendet werden darf, bevor die Anforderung abläuft.

Elasticsearch Konfigurationsfelder für die Dateneingabe

Beschreibung der Felder im Formular Elasticsearch zur Konfiguration der Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option, um zu bestimmen, ob ein bestimmter MID-Server oder ein MID-Server-Cluster verwendet werden soll. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.
MID	(Nur, wenn das Feld **Ausführen** auf auf Spezifischer MID-Server gesetzt ist) MID-Server, von dem Protokolldaten aus Elasticsearch-Indizes abgerufen werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für den ausgewählten MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur, wenn das Feld **Ausführen** auf auf Spezifischer MID-Server Cluster festgelegt ist) Der Cluster MID-Server, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen MID-Server im Cluster ausgeführt, bis dieser MID-Server ausfällt. Das System verschiebt dann alle Dateneingabeaufgaben gemäß der konfigurierten Reihenfolge zum nächsten verfügbaren MID-Server im Cluster. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Health Log Analytics unterstützt nur Failover-Cluster MID-Server. In diesen Clustern sind mehrere MID Servers zum Failover-Schutz in einer Gruppe zusammengefasst. Wenn Sie ein Cluster aus dem Dateneingabeformular auswählen, werden in der Liste der Cluster MID-Server nur Failover-Cluster angezeigt. • Der Cluster MID-Server darf nur MID Servers enthalten, die die Standardauthentifizierung unterstützen. mTLS wird für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden MID-Server im Cluster aktiviert werden. Wenn die Protokollerfassung für den aktiven MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. • Wenn Elasticsearch die Client- oder CA-Zertifikatauthentifizierung verwendet, müssen alle MID Servers im Cluster über die entsprechenden Zertifikate verfügen. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn es mindestens einen MID-Server enthält und weniger als 10 Dateneingaben darauf ausgeführt werden, selbst wenn dieser MID-Server ausgefallen ist. Weitere Informationen zu MID-Server-Clustern finden Sie unter MID-Server-Cluster konfigurieren . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Diese Dateneingabe verwendet Elastic, um Protokolldaten an Ihre -Instanz zu streamen.
Quellenanzahl	Die Anzahl der Protokollquellen, die von dieser Dateneingabe erstellt wurden
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde

Registerkarte „Transport“

Feld	Beschreibung
Server-URL	URL für den Zugriff auf das Cluster. Dies ist ein Pflichtfeld.
Max. Anzahl von Verbindungen pro Route	Maximale Anzahl der pro Knoten zu öffnenden Verbindungen. Standardwert: 2
Max. Bildlaufsegmente	Die Anzahl der für den relevanten Index in Elasticsearchkonfigurierten Shards. Diese Zahl teilt Elastic mit, wie viele parallele Abfragen in jeder Abfrageanforderung ausgeführt werden sollen.
Proxy-Host	Hostname des HTTP-Proxy, über den Anforderungen gesendet werden.
Proxy-Port	Port des HTTP-Proxy, über den Anforderungen gesendet werden
Authentifizierungsmethode	Die Authentifizierungsmethode, die zum Authentifizieren der in Elasticsearcheingegebenen Daten verwendet wird. Die Optionen sind: Standardauthentifizierung, API-Schlüssel oder Client-Zertifikat. **Hinweis:** Wenn Sie die erforderliche Authentifizierungsmethode auswählen, werden die entsprechenden Felder für Anmeldeinformationen im Formular angezeigt.
Anmeldeinformationen für Standardauthentifizierung	Anwendername und Passwort, die zum Herstellen der Verbindung mit der Suchmaschine Elasticsearch verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Transport“ (Fortsetzung)

Feld	Beschreibung
	Hinweis: Füllen Sie entweder dieses Feld oder das Feld **AWS-Anmeldeinformationen** aus.
AWS-Anmeldeinformationen	AWS-Anmeldeinformationen für die Verbindung mit der von AWS gehosteten Elasticsearch-Such-Engine **Hinweis:** Füllen Sie entweder dieses Feld oder das Feld **Anmeldeinformationen für Standardauthentifizierung** aus.
AWS-Region	AWS-Region, in der das Elasticsearch-Cluster ausgeführt wird
Anmeldeinformationen für API-Keys	Der API-Schlüssel, der zum Herstellen einer Verbindung mit der Suchmaschine Elasticsearch verwendet wird.
Client-Zertifikat	Das Client-Zertifikat, das zum Herstellen einer Verbindung mit der Suchmaschine Elasticsearch verwendet wird.
MID-Zertifikatrichtlinienprüfung verwenden	Option zum Aktivieren der Prüfung der MID-Zertifikatsrichtlinie. Wählen Sie diese Option aus, wenn Sie die Protokolle mit SSL/TLS verschlüsselt senden möchten. Navigieren Sie dann zu **Alle** > **MID-Server** > **MID-Sicherheitsrichtlinie** und fügen Sie die MID-Zertifikatrichtlinienprüfung zur Tabelle hinzu. Weitere Informationen finden Sie unter Richtlinien für MID-Server-Zertifikatprüfung .

Registerkarte „Abfrageeinstellungen“.

Feld	Beschreibung	Beispiel
Von/Bis	Von- und Bis-Datum und Uhrzeit zum Lesen der Daten • Von: Es werden keine Daten gelesen, die älter als dieses Datum sind. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt.	Von: 1970-01-01 15:59:59 Bis: 2300-01-01 15:59:59

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“. (Fortsetzung)

Feld	Beschreibung	Beispiel
	• Bis: Nach diesem Datum werden keine Daten gelesen. Legen Sie für Live-Daten dieses Datum weit in die Zukunft.	
Cross-Cluster-Suche verwenden	Option für die Suche nach Daten in Elasticsearch -Clustern. Wenn dieses Kontrollkästchen aktiviert ist, wird das Feld **Zu durchsuchende Cluster** angezeigt. **Hinweis:** Ihre Einstellungen im Kontrollkästchen **Minimale Rechte verwenden** und im Feld **Verzögerung beim Lesen des aktuellen Zeitstempels (Sekunden)** im Formular **Erweiterte Konfiguration** wirken sich darauf aus, wie Daten in mehreren Clustern erfasst werden.	
Cluster für Suche	Die zu durchsuchenden Elasticsearch -Cluster. Dieses Feld wird nur angezeigt, wenn das Kontrollkästchen **Cross-Cluster-Suche verwenden** aktiviert ist. Führen Sie einen der folgenden Schritte aus: • Lassen Sie dieses Feld leer, oder geben Sie „*“ ein, um alle in Elasticsearchdefinierten Remote-Cluster zu durchsuchen. • Geben Sie die zu durchsuchenden Cluster in einer durch Kommas getrennten Liste an. **Hinweis:** Um auch den lokalen Cluster zu durchsuchen, fügen Sie ein Komma am Anfang oder Ende oder zwei Kommas nacheinander in der Liste hinzu. Beispiel: „east,,west“ oder „,east,west“ oder „*“,	Ost, West, Süd
Indexpräfix	Präfix für die Elasticsearch-Indizes, aus denen gelesen werden soll. Die Dateneingabe wird nur aus Indizes mit diesem Präfix gelesen. Dies ist ein Pflichtfeld.	only-read-these-indices-*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“. (Fortsetzung)

Feld	Beschreibung	Beispiel
Minimale Berechtigungen verwenden	Option zum Lesen von Protokolldaten direkt aus den Indizes Elasticsearch mit dem konfigurierten Präfix. • Wenn diese Option ausgewählt ist, liest die Dateneingabe die Protokolldaten direkt aus den Indizes Elasticsearch mit dem konfigurierten Präfix. Zum Ausführen dieser Aufgabe sind nur Leseberechtigungen erforderlich. **Hinweis:** Wenn dieses Kontrollkästchen aktiviert ist und Sie die Cross-Cluster-Suche verwenden, werden Daten von allen Clustern gleichzeitig gesammelt. • Wenn diese Option gelöscht ist, ruft die Dateneingabe alle Indizes mit dem Präfix ab, filtert sie und liest die Protokolldaten aus den gefilterten Indizes. Das Ausführen dieser Aufgabe erfordert zusätzliche Berechtigungen. **Hinweis:** Wenn Sie diese Checkbox bei Verwendung der Cross-Cluster-Suche deaktiviert lassen, wirkt sich dies darauf aus, wie Daten aus den Clustern gesammelt werden. Weitere Informationen finden Sie im Artikel „Cross-Cluster Search for Elasticsearch Data Inputs in Health Log Analytics“ [KB1556079] in der Knowledge Base Now Support. Weitere Informationen zu Streaming-Protokollen mit der Elasticsearch-Dateneingabe finden Sie im Artikel Stream logs using Elasticsearch data input – Advanced Guide [KB1080162] (Protokolle mit Elasticsearch-Dateneingabe streamen - Erweiterte Anleitung) in der Now Support-Knowledge Base.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“. (Fortsetzung)

Feld	Beschreibung	Beispiel
Zeitstempelfeld des Dokuments	Zeitstempelfeld in Dokumenten, die in den Leseindizes gespeichert sind. Dies ist ein Pflichtfeld.	
Format des Zeitstempelfelds	Format des Zeitstempelfelds in den Dokumenten. Wenn kein Format angegeben ist, wird das Standardformat für die Unix-Epoch-Zeit in Millisekunden verwendet. Zum Beispiel: 1684168407 (15. Mai 2023 16:33:27)	jjjj-MM-tt'T'HH:mm:ss.SSSSSS'Z'
Begriffsfilter	JSON-Zuordnung der zu filternden Begriffe **Hinweis:** Vermeiden Sie die Verwendung von Begriffsabfragen für Textfelder. Wenn das Zielfeld sowohl als Text als auch als Stichwort zugeordnet ist, referenzieren Sie das Stichwort mit feldname.stichwort.	{"severity": ["error", "warning"]}
Max. Anzahl von Dokumenten pro Abfrage	Maximale Anzahl von Dokumenten, die in einer einzelnen Abfrage abgerufen werden	
Sliced-Scrolling-Tiebreaker	Wert, der zum Teilen der Daten verwendet wird. Jeder Teil wird parallel gescrollt. Standard: _id	
Search-after-Tiebreaker	Eindeutiger Wert pro Dokument, der beim Sortieren von Protokolleinträgen nach Zeitstempel als Tiebreaker verwendet werden soll.	
Search-after-API verwenden	Option für das Wechseln zwischen Sliced-Scrolling- und Search-after-APIs. **Hinweis:** Sliced-Scrolling-APIs sind beim Lesen historischer Daten vorzuziehen, während Search-after-APIs besser zum Lesen von Echtzeitdaten geeignet sind.	
Zeitsuffixformat für Index	Format des Zeitsuffix bei Verwendung von zeitbasierten Indexnamen, z. B. [logstash-]JJJJ.MM.TT. Wenn Sie Aliasse verwenden, lassen Sie dieses Feld leer.	uuuu.MM.tt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung
Datenlese-Zeitüberschreitung (Millisekunden)	Dauer in Millisekunden, bevor eine Anforderung an den Elasticsearch-Cluster abläuft
Intervall für Indexerkennung (Sekunden)	Anzahl der Sekunden zwischen intermittierenden MID-Server-Anforderungen an das Elasticsearch-Cluster für neue Indizes, aus denen Daten gelesen werden sollen
Scroll-Kontextzeit (Millisekunden)	Lebensdauer des erstellten Scroll, wenn die Scroll-API zum Lesen von Daten aus Elasticsearch verwendet wird. Weitere Informationen finden Sie in der Elasticsearch Dokumentation zur Scroll API .
Event Processor Worker	Maximale Anzahl von CPU-Kernen, die parallel zur Verarbeitung von aus Elasticsearch abgerufenen Events verwendet werden. Eine höhere Einstellung erhöht den Dateneingabedurchsatz auf Kosten einer höheren CPU-Auslastung.
Größe der Worker-Warteschlange	Maximale Anzahl von Stapeln, die zur Verarbeitung in die Warteschlange gestellt werden. Eine höhere Einstellung erhöht den Durchsatz auf Kosten einer höheren RAM-Auslastung.
Standardzeitzone	Standardzeitzone, wenn Datum und Uhrzeit des Events keine Zeitzoneninformationen enthalten.
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.
Zeichencodierung	Zeichencodierung für diese Dateneingabe
Ruheintervall (Sekunden)	Intervall der Wartzeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Daten zurückgegeben hat
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung
Verzögerung beim Lesen des aktuellen Zeitstempels (Sekunden)	Die Anzahl der Sekunden vor dem aktuellen Zeitpunkt, zu dem verzögerte Daten abgefragt werden sollen. Die konfigurierte Anzahl von Sekunden wird von der aktuellen Zeit für das Lesen des letzten Zeitstempels abgezogen. **Hinweis:** Wenn dieser Wert 0 ist und Daten von mehreren Clustern gleichzeitig gesammelt werden, enthält die Abfrage möglicherweise keine Daten, die in einem der Cluster mit Verzögerung gesendet wurden.

Konfigurationsfelder für TCP-Dateneingabe

Beschreibung der Felder im Konfigurationsformular für die TCP-Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Port	Port für den MID-Server. Wählen Sie einen eindeutigen Port aus dem Array aus. Der Platzhalter zeigt den Bereich der Ports an, aus denen Sie auswählen können. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.
MID	Der MID-Server, an den die Protokolle gestreamt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Senden der Protokolldaten. Rsyslog und Splunk senden Daten mit dem TCP-Protokoll.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
SSL/TLS verwenden	Hiermit geben Sie an, ob SSL/TLS verwendet werden soll.	
Look up hostnames (Nach Hostnamen suchen)	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen.	false
Anzahl der Boss-Threads	Anzahl der Threads, mit denen Verbindungen verwaltet werden	1
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden	4
Lesezeitüberschreitung in Sekunden	Zeitüberschreitung in Sekunden seit dem letzten Lesen. Wenn die Zeitüberschreitung abläuft, schließt das System den Kanal.	30
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	
Trennzeichen für Trennlinien	Das Zeilenumbruchzeichen, das die Rohprotokollzeilen trennt. Teilende Werte müssen durch ein Komma gefolgt von einem Leerzeichen getrennt werden: ", ". Beispiel: „\r, \n, , aufgeteilt hier, #“.	

Konfigurationsfelder für UDP-Dateneingabe

Beschreibung der Felder im Konfigurationsformular für die UDP-Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Port	Port für den MID-Server. Wählen Sie einen eindeutigen Port aus dem Array aus. Der Platzhalter zeigt den Bereich der Ports an, aus denen Sie auswählen können. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.
MID	Der MID-Server, an den die Protokolle gestreamt werden. **Hinweis:** • Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest.

Die Felder in der folgenden Tabelle zeigen schreibgeschützte Informationen.

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Zum Senden der Protokolldaten verwendetes Protokoll: UDP.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Erweiterte Konfiguration

Feld	Beschreibung	Standardwert
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Quotengrenze	Begrenzung der Anzahl der Ereignisse pro Sekunde, die diese Dateneingabe verarbeitet.	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32.766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Option zum Auswählen, dass Protokolle verworfen werden, wenn viele Prozesse in der Warteschlange auf den Zugriff auf den MID-Server warten.	false

Konfigurationsfelder für GCP PubSub-Dateneingabe

Beschreibung der Felder im Konfigurationsformular für die GCP PubSub-Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Port	Port für den MID-Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wählen Sie einen eindeutigen Port aus dem Array aus. Der Platzhalter zeigt den Bereich der Ports an, aus denen Sie auswählen können. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.
Ausführen auf	Option, um zu bestimmen, ob ein bestimmtes MID-Server - oder ein MID-Server -Cluster verwendet werden soll. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.
MID	(Nur, wenn das Feld **Ausführen** auf auf Spezifischer MID-Server gesetzt ist) Der MID-Server, an den die Protokolle gestreamt werden. **Hinweis:** • Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für den ausgewählten MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur, wenn das Feld **Ausführen** auf auf MID-Server Cluster festgelegt ist.) Der Cluster MID-Server, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen MID-Server im Cluster ausgeführt, bis dieser MID-Server ausfällt. Das System verschiebt dann alle Dateneingabeaufgaben entsprechend der konfigurierten Reihenfolge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	zu den nächsten verfügbaren MID-Server im Cluster. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt. **Hinweis:** • Health Log Analytics unterstützt nur Failover-Cluster MID-Server. In diesen Clustern sind mehrere MID Servers zum Failover-Schutz in einer Gruppe zusammengefasst. Wenn Sie ein Cluster aus dem Dateneingabeformular auswählen, werden in der Liste der Cluster MID-Server nur Failover-Cluster angezeigt. • Der Cluster MID-Server darf nur MID Servers enthalten, die die Standardauthentifizierung unterstützen. mTLS wird für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden MID-Server im Cluster aktiviert werden. Wenn die Protokollerfassung für den aktiven MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn es mindestens einen MID-Server enthält und weniger als 10 Dateneingaben darauf ausgeführt werden, selbst wenn dieser MID-Server ausgefallen ist. Weitere Informationen zu MID-Server -Clustern finden Sie unter MID-Server-Cluster konfigurieren . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest.

Die Felder in der folgenden Tabelle zeigen schreibgeschützte Informationen.

Feld	Beschreibung
Übertragung	Zum Senden der Protokolldaten verwendetes Protokoll: PubSub.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Status	Status der Dateneingabe
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde

Registerkarte „Transport“

Feld	Beschreibung
Projekt-ID	Die Projekt-ID des Projekts Google Cloud. Beispiel: my-project-id.
Themenname	Das Google Cloud Pub/Sub-Thema, das Health Log Analyticsabonnieren soll. Beispiel: my_topic.
Alias für GCP-Anmeldeinformationen	Der zu verwendende Anmeldeinformationsalias. Geben Sie einen Alias für GCP-Anmeldeinformationen an, indem Sie das Lupensymbol wählen und dann entweder einen vorhandenen Alias für Anmeldeinformationen aus der Liste **„Aliasse für Verbindungen und Anmeldeinformationen“** auswählen oder **Neu** wählen, um einen neuen Datensatz zu erstellen. Der Standardwert ist sn_occ.HLA_Credential_Alias. Informationen zum Erstellen von Anmeldeinformationsaliasen finden Sie unter Aliasse für Anmeldeinformationen für Discovery .
Aboname	Das -Abonnement Health Log Analytics verwendet zum Empfangen von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Transport“ (Fortsetzung)

Feld	Beschreibung
	Protokolldaten, die im Pub/Sub-Thema Google Cloud veröffentlicht werden. Wenn Sie dieses Feld leer lassen, verwendet Health Log Analytics ServiceNow-Abonnement.

Erweiterte Konfiguration

Registerkarte „Erweitert“

Feld	Beschreibung	Standardwert
Größe des Abonnenten-Thread-Pools	Die Anzahl der gleichzeitigen Threads, die Dateien aus dem Google Cloud Pub/Sub-Thema herunterladen.	1
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32.766
Zeichencodierung	(Schreibgeschützt) Die Zeichencodierung für diese Dateneingabe.	UTF-8
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Quotengrenze	Maximale Anzahl von Events pro Sekunde, die diese Dateneingabe verarbeitet.	-1
Verwerfen, wenn Warteschlange voll ist	Option zum Auswählen, dass Protokolle verworfen werden, wenn viele Prozesse in der Warteschlange auf den Zugriff auf den MID-Server warten.	Leeren

MID-Server Konfigurationsfelder für die Dateneingabe

Beschreibung der Felder im Formular MID-Server zur Konfiguration der Dateneingabe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basiskonfiguration

Feld	Beschreibung
Beschreibung	Beschreibung der Dateneingabe
MID	Der Name des MID-Server, von dem die Protokolle gestreamt werden.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Diese Dateneingabe verwendet MID-Server, um Protokolldaten an Ihre -Instanz zu streamen.
Quellenanzahl	Die Anzahl der Protokollquellen, die von dieser Dateneingabe erstellt wurden
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde

Erweiterte Konfiguration

Feld	Beschreibung	Standardwert
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn das Protokoll keine Zeitzone angibt.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Option zum Verwerfen von Protokollen, wenn der MID-Server ausgelastet ist	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Amazon CloudWatch Konfigurationsfelder für die Dateneingabe

Beschreibung der Felder im Formular Amazon CloudWatch zur Konfiguration der Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option, um zu bestimmen, ob ein bestimmtes MID-Server - oder ein MID-Server -Cluster verwendet werden soll. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.
MID	(Nur, wenn das Feld **Ausführen** auf auf Spezifischer MID-Server gesetzt ist) MID-Server, in den Protokolldaten aus Amazon CloudWatch abgerufen werden. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für den ausgewählten MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur, wenn das Feld **Ausführen** auf auf MID-Server Cluster festgelegt ist.) Der Cluster MID-Server, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen MID-Server im Cluster ausgeführt, bis dieser

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	MID-Server ausfällt. Das System verschiebt dann alle Dateneingabeaufgaben entsprechend der konfigurierten Reihenfolge zu den nächsten verfügbaren MID-Server im Cluster. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt. **Hinweis:** • Health Log Analytics unterstützt nur Failover-Cluster MID-Server. In diesen Clustern sind mehrere MID Servers zum Failover-Schutz in einer Gruppe zusammengefasst. Wenn Sie ein Cluster aus dem Dateneingabeformular auswählen, werden in der Liste der Cluster MID-Server nur Failover-Cluster angezeigt. • Der Cluster MID-Server darf nur MID Servers enthalten, die die Standardauthentifizierung unterstützen. mTLS wird für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden MID-Server im Cluster aktiviert werden. Wenn die Protokollerfassung für den aktiven MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn es mindestens einen MID-Server enthält und weniger als 10 Dateneingaben darauf ausgeführt werden, selbst wenn dieser MID-Server ausgefallen ist. Weitere Informationen zu MID-Server -Clustern finden Sie unter MID-Server-Cluster konfigurieren . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet Amazon CloudWatch zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Registerkarte „Abfrageeinstellungen“.

Feld	Beschreibung	Beispiel
Von	Datum und Uhrzeit für den Beginn des Lesenvorgangs der Daten. Daten, die älter als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt.	Jetzt -1 Woche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“. (Fortsetzung)

Feld	Beschreibung	Beispiel
	Dies ist ein Pflichtfeld.	
Gruppenname(n)	Die zu durchsuchenden Protokollgruppen. Wenn mehrere Protokollgruppen durchsucht werden müssen, geben Sie die Gruppen in einer kommagetrennten Liste an. Um Protokolldaten aus allen Gruppen abzurufen, verwenden Sie ein Sternchen (*) als Platzhalterzeichen. Dies ist ein Pflichtfeld.	hla-cw-loggroup1,hla-cw-loggroup2
Präfix	Namenspräfix für die Amazon CloudWatch-Protokollstreams, aus denen gelesen werden soll. Die Dateneingabe wird nur aus Protokollstreams mit diesem Namenspräfix gelesen. **Hinweis:** Pro Datenelement wird nur ein Protokollstream-Präfix unterstützt. Um mehrere Präfixe nutzen zu können, erstellen Sie mehrere Dateneingaben.	hla-cw
Filtermuster	Muster, nach dem eingehende Events gefiltert werden sollen. Es werden verschiedene Arten von Filtermustern unterstützt. Beispiel: • Ein Muster zum Abrufen von Protokoll-Events, die einen einzelnen Begriff enthalten. • Ein Muster zum Abrufen von Protokoll-Events, die mehrere Begriffe enthalten. • Ein Muster zum Abrufen von Protokoll-Events, die	• Ein Muster zum Abrufen von Protokoll-Events, die den einzelnen Begriff „STATUS_CODE“ enthalten: „STATUS_CODE“ • Ein Muster zum Abrufen von Protokoll-Events, die mehrere Begriffe enthalten, „STATUS_CODE“ und „200“: „STATUS_CODE 200“ • Ein Muster zum Abrufen von Protokoll-Events, die den Begriff „STATUS_CODE“ enthalten und einen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“. (Fortsetzung)

Feld	Beschreibung	Beispiel
	einen Begriff enthalten und einen anderen ausschließen. **Hinweis:** Bei Filtermustern wird zwischen Groß- und Kleinschreibung unterschieden. Weitere Informationen finden Sie unter https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/FilterAndPatternSyntax.html	anderen Begriff („200“) ausschließen: “STATUS_CODE” – “200”

Registerkarte „Transport“

Feld	Beschreibung
AWS-Anmeldeinformationen	Feld, das auf die Liste „AWS-Anmeldeinformationen“ (aws_credentials.list) verweist. Die Liste enthält den AWS-Zugriffsschlüssel und den geheimen Zugriffsschlüssel.
AWS-Region	Die AWS-Region, in der der Amazon CloudWatch-Cluster ausgeführt wird , z. B. us-west-1. Eine Liste der AWS-Regionen finden Sie unter https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-regions . Dies ist ein Pflichtfeld.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
Verbindungstimeout	Anzahl der Millisekunden, die gewartet werden soll, bevor der AWS-Verbindungsversuch abgebrochen wird.	1.000
Batchgröße	Maximale Anzahl der pro Abfrage abgerufenen Protokolle.	2.500

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwert
Socket-Zeitüberschreitung	Anzahl der Millisekunden, die gewartet werden soll, bevor bei einer Datenübertragung über eine hergestellte Verbindung eine Zeitüberschreitung auftritt.	10000
Standardzeitzone	Standardzeitzone, wenn Datum und Uhrzeit des Protokolls keine Zeitzoneninformationen enthalten.	GMT
Anteil der zu verwerfenden Unterstichproben	Anzahl der Protokolle, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Protokolle zu reduzieren.	-1
Anteil der zu empfangenden Unterstichproben	Anzahl der Protokolle, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Protokolle zu reduzieren.	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32766
Ruhezustandsintervall	Intervall der Wartezeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Protokolle zurückgegeben hat.	60
Abfrageintervall	Intervall in Sekunden, das gewartet werden soll, bevor neue Protokolle abgerufen werden.	0
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	falsch

Amazon S3 Konfigurationsfelder für die Dateneingabe

Beschreibung der Felder im Formular Amazon S3 zur Konfiguration der Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option, um zu bestimmen, ob ein bestimmtes MID-Server - oder ein MID-Server -Cluster verwendet werden soll.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.
MID	(Nur, wenn das Feld **Ausführen** auf auf Spezifischer MID-Server gesetzt ist) MID-Server, in den Protokolldaten aus Amazon S3 abgerufen werden. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für den ausgewählten MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur, wenn das Feld **Ausführen** auf auf MID-Server Cluster festgelegt ist.) Der Cluster MID-Server, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen MID-Server im Cluster ausgeführt, bis dieser MID-Server ausfällt. Das System verschiebt dann alle Dateneingabeaufgaben entsprechend der konfigurierten Reihenfolge zu den nächsten verfügbaren MID-Server im Cluster. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Health Log Analytics unterstützt nur Failover-Cluster MID-Server. In diesen Clustern sind mehrere MID Servers zum Failover-Schutz in einer Gruppe zusammengefasst. Wenn Sie ein Cluster aus dem Dateneingabeformular auswählen, werden in der Liste der Cluster MID-Server nur Failover-Cluster angezeigt. • Der Cluster MID-Server darf nur MID Servers enthalten, die die Standardauthentifizierung unterstützen. mTLS wird für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden MID-Server im Cluster aktiviert werden. Wenn die Protokollerfassung für den aktiven MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn es mindestens einen MID-Server enthält und weniger als 10 Dateneingaben darauf ausgeführt werden, selbst wenn dieser MID-Server ausgefallen ist. Weitere Informationen zu MID-Server -Clustern finden Sie unter MID-Server-Cluster konfigurieren . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet Amazon S3 zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe gestoppt wurde oder fehlgeschlagen ist.
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in die Dateneingabe gestreamt wurde.
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Registerkarte „Abfrageeinstellungen“.

Feld	Beschreibung	Beispiel
Von/Bis	Von/Bis-Datum und -Uhrzeit zum Lesen der Daten. • Von: Daten, die älter als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt. • Bis: Daten, die neuer als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. Legen Sie für Live-Daten dieses Datum weit in die Zukunft. Dies ist ein Pflichtfeld.	Von: Jetzt -1 Woche Bis: 2300-01-01 15:59:59

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“. (Fortsetzung)

Feld	Beschreibung	Beispiel
Bucket-Name	Das zu streamende Amazon S3-Bucket Dies ist ein Pflichtfeld.	my-s3-bucket
Präfix	Präfix für die abzurufenden Objekte. Die Dateneingabe ruft nur Objekte ab, die mit diesem Präfix beginnen. Dieses Feld wird normalerweise verwendet, um nur bestimmte Ordner in einem Bucket abzurufen.	/nur/dieses/verzeichnis/
Einbeziehen	Datei oder Objekt, die/das einbezogen werden soll, wenn das System einen Musterabgleich durchführt.	.*bezieh-mich-ein.*
Ausschließen	Datei oder Objekt, die/das ausgeschlossen werden soll, wenn das System einen Musterabgleich durchführt.	.*überspring-mich.*

Registerkarte „Transport“

Feld	Beschreibung
AWS-Anmeldeinformationen	Feld, das auf die Liste „AWS-Anmeldeinformationen“ (aws_credentials.list) verweist. Die Liste enthält den AWS-Zugriffsschlüssel und den geheimen Zugriffsschlüssel.
AWS-Region	AWS-Region, in der sich das Amazon S3-Bucket befindet, z. B. us-west-1. Eine Liste der AWS-Regionen finden Sie unter https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-regions . Dies ist ein Pflichtfeld.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
Anonym	Option zum Erzwingen des Zugriffs auf den Amazon S3-Bucket ohne	Falsch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwert
	Anmeldeinformationen, wobei Standardanmeldeinformationen, falls vorhanden, ignoriert werden.	
Durchlaufen	Option für den Zugriff auf jedes Verzeichnis im Bucket.	Falsch
Objekte sortiert nach dem Zeitpunkt der letzten Änderung	Option zum Abrufen von Objekten, wenn die Objekte im Bucket nach Zeit sortiert sind.	Falsch
Verbindungstimeout	Anzahl der Millisekunden, die gewartet werden soll, bevor der AWS-Verbindungsversuch abgebrochen wird.	100
Threadpool-Größe	Anzahl der gleichzeitigen Threads, die Dateien aus dem Bucket herunterladen.	1
Puffergröße	Größe des Download-Puffers in Byte.	100 MB
Socket-Zeitüberschreitung	Anzahl der Millisekunden, die gewartet werden soll, bevor bei einer Datenübertragung über eine hergestellte Verbindung eine Zeitüberschreitung auftritt.	10000
Max retry for file (Max. Wiederholungsversuche für Datei)	Maximale Anzahl der Wiederholungen der Dateiverarbeitung im Fehlerfall.	10
Standardzeitzone	Standardzeitzone, wenn das Protokoll keine Zeitzoneninformationen enthält.	UTC
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.	-1
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen	-1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwert
	werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.	
Quotengrenze	Maximale Anzahl von Events pro Sekunde, die diese Dateneingabe verarbeitet.	-1
Maximale Länge in Bytes	Maximale Länge von Events in Byte.	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Ruhezustandsintervall	Intervall der Wartezeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Events zurückgegeben hat.	60
Abfrageintervall	Intervall in Sekunden, das gewartet werden soll, bevor neue Events abgerufen werden.	0
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	falsch

Microsoft Azure Log Analytics Konfigurationsfelder für die Dateneingabe

Beschreibung der Felder im Formular Microsoft Azure Log Analytics zur Konfiguration der Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option, um zu bestimmen, ob ein bestimmtes MID-Server - oder ein MID-Server -Cluster verwendet werden soll. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID	(Nur, wenn das Feld **Ausführen** auf auf Spezifischer MID-Server gesetzt ist) MID-Server, von dem die Protokolldaten aus Microsoft Azure Log Analytics abgerufen werden. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für den ausgewählten MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur, wenn das Feld **Ausführen** auf auf MID-Server Cluster festgelegt ist.) Der Cluster MID-Server, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen MID-Server im Cluster ausgeführt, bis dieser MID-Server ausfällt. Das System verschiebt dann alle Dateneingabeaufgaben entsprechend der konfigurierten Reihenfolge zu den nächsten verfügbaren MID-Server im Cluster. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Health Log Analytics unterstützt nur Failover-Cluster MID-Server. In diesen Clustern sind mehrere MID Servers zum Failover-Schutz in einer Gruppe zusammengefasst. Wenn Sie ein Cluster aus dem Dateneingabeformular auswählen, werden in der Liste der Cluster MID-Server nur Failover-Cluster angezeigt. • Der Cluster MID-Server darf nur MID Servers enthalten, die die Standardauthentifizierung unterstützen. mTLS wird für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden MID-Server im Cluster aktiviert werden. Wenn die Protokollerfassung für den aktiven MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn es mindestens einen MID-Server enthält und weniger als 10 Dateneingaben darauf ausgeführt werden, selbst wenn dieser MID-Server ausgefallen ist. Weitere Informationen zu MID-Server -Clustern finden Sie unter MID-Server-Cluster konfigurieren . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet Microsoft Azure Log Analytics zum Streamen von Protokolldaten an Ihre Instanz.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Registerkarte „Abfrageeinstellungen“.

Health Log Analytics verwendet die in diesen Feldern festgelegten Werte, um die Abfrage zum Empfangen von Protokolldaten von **Microsoft Azure Log Analytics**zu generieren. Im Feld **Protokollabfrage** können Sie eine anwenderdefinierte Abfrage konfigurieren

Feld	Beschreibung	Beispiel
Von	Von/Bis-Datum und -Uhrzeit zum Lesen der Daten. Daten, die älter als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt. Dies ist ein Pflichtfeld.	Jetzt -1 Woche
Datenquellenname	Der Name der Tabelle in Microsoft Azure Log Analytics, in der die Dateneingabe die Protokolldaten abruft.	ContainerLog

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“.

Health Log Analytics verwendet die in diesen Feldern festgelegten Werte, um die Abfrage zum Empfangen von Protokolldaten von **Microsoft Azure Log Analytics**zu generieren. Im Feld **Protokollabfrage** können Sie eine anwenderdefinierte Abfrage konfigurieren

(Fortsetzung)

Feld	Beschreibung	Beispiel
	Weitere Informationen finden Sie im Abschnitt „Tabelleninformationen anzeigen“ in der Microsoft Azure-Dokumentation . Dies ist ein Pflichtfeld.	
Name der Eigenschaft für die Ereigniszeit	Das Microsoft Azure Log Analytics-Feld, in dem die Events-Zeit erkannt werden soll. Dies ist ein Pflichtfeld.	TimeGenerated
Max. Anzahl von Dokumenten pro Abfrage	Die höchste Anzahl von Zeilen, die in jeder Abfrage abgerufen werden.	500
Spaltenauswahl	Kommagetrennte Liste der Spaltennamen, die zurückgegeben werden sollen. **Hinweis:** Dieses Feld wird ignoriert, wenn Sie eine benutzerdefinierte Abfrage angeben.	LogEntry, LogEntrySource
Protokollabfrage	Eine anwenderdefinierte Abfrage zum Empfangen von Protokolldaten von Microsoft Azure Log Analytics. Die Einstellungen in diesem Feld überschreiben alle anderen Felder auf der Registerkarte **Abfrageeinstellungen** mit Ausnahme des Felds **Von**. Wenn das Feld **Protokollabfrage** leer ist, generiert Health Log Analytics die Abfrage anhand der in den anderen Feldern festgelegten Werte.	`{ "query":"ContainerLog	where LogEntry contains 'cartservice'	where TimeGenerated > %s	take 500", "workspaces": ["defaultworkspace-3ab145ff-f9cd-433f-8533-d1b1ee24aee6-eus"], "project": ["TimeGenerated",`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“.

Health Log Analytics verwendet die in diesen Feldern festgelegten Werte, um die Abfrage zum Empfangen von Protokolldaten von **Microsoft Azure Log Analytics**zu generieren. Im Feld **Protokollabfrage** können Sie eine anwenderdefinierte Abfrage konfigurieren

(Fortsetzung)

Feld	Beschreibung	Beispiel

	Verwenden Sie für die anwenderdefinierte Abfrage das folgende JSON-Format:
	
	`{"query": "query | wobei TimeGenerated > %s | 500 nehmen"}`
		`"LogEntry",`
		`"LogEntrySource"]`
		`}`

Registerkarte „Transport“

Feld	Beschreibung
Umleitungs-URL	Die Umleitungs-URL der Zugriffsprotokollanwendung. Die URL bezieht sich auf die Autorisierungseigenschaft Microsoft Azure redirect_uri. Weitere Informationen finden Sie im Abschnitt „Autorisierungscode-URL (GET-Anforderung)“ in der Microsoft Azure-Dokumentation . Dies ist ein Pflichtfeld.
Azure-Service-Prinzipal-Anmeldeinformationen	Die Anmeldeinformationen, die für den Zugriff auf Microsoft Azure-Ressourcen verwendet werden. Wählen Sie aus der Dropdown-Liste **Geheimer Clientschlüssel** aus. **Hinweis:** Sie benötigen keine Anmeldeinformationen für Azure Enterprise Agreement (EA). Dies ist ein Pflichtfeld.
Arbeitsbereich-ID	Kunden-ID, die zum Aufrufen der Microsoft Azure Log Analytics-REST API verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
Event Processor Worker	Anzahl der gleichzeitigen Event-Verarbeitungs-Worker, wobei jeder Worker einen Event-Batch verarbeitet.	4
Worker queue size (Größe der Worker-Warteschlange)	Warteschlangengröße der Event-Prozessor-Worker.	5
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.	-1
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.	-1
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Ruhezustandsintervall	Intervall der Wartezeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Events zurückgegeben hat.	60
Abfrageintervall	Intervall in Sekunden, das gewartet werden soll, bevor neue Events abgerufen werden.	0
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	falsch

Microsoft Azure Event Hubs Konfigurationsfelder für die Dateneingabe

Beschreibung der Felder im Formular Microsoft Azure Event Hubs zur Konfiguration der Dateneingabe.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option, um zu bestimmen, ob ein bestimmtes MID-Server - oder ein MID-Server -Cluster verwendet werden soll. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.
MID	(Nur, wenn das Feld **Ausführen** auf auf Spezifischer MID-Server gesetzt ist) MID-Server, in den Protokolldaten aus Microsoft Azure Event Hubs abgerufen werden. **Hinweis:** • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für den ausgewählten MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur, wenn das Feld **Ausführen** auf auf MID-Server Cluster festgelegt ist.) Der Cluster MID-Server, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen MID-Server im Cluster ausgeführt, bis dieser MID-Server ausfällt. Das System verschiebt dann alle Dateneingabeaufgaben entsprechend der konfigurierten Reihenfolge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	zu den nächsten verfügbaren MID-Server im Cluster. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt. **Hinweis:** • Health Log Analytics unterstützt nur Failover-Cluster MID-Server. In diesen Clustern sind mehrere MID Servers zum Failover-Schutz in einer Gruppe zusammengefasst. Wenn Sie ein Cluster aus dem Dateneingabeformular auswählen, werden in der Liste der Cluster MID-Server nur Failover-Cluster angezeigt. • Der Cluster MID-Server darf nur MID Servers enthalten, die die Standardauthentifizierung unterstützen. mTLS wird für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden MID-Server im Cluster aktiviert werden. Wenn die Protokollerfassung für den aktiven MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn es mindestens einen MID-Server enthält und weniger als 10 Dateneingaben darauf ausgeführt werden, selbst wenn dieser MID-Server ausgefallen ist. Weitere Informationen zu MID-Server -Clustern finden Sie unter MID-Server-Cluster konfigurieren . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet Microsoft Azure Event Hubs zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Registerkarte „Abfrageeinstellungen“.

Feld	Beschreibung	Beispiel
Von	Von/Bis-Datum und -Uhrzeit zum Lesen der Daten. Daten, die älter als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt. Dies ist ein Pflichtfeld.	Jetzt -1 Woche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Abfrageeinstellungen“. (Fortsetzung)

Feld	Beschreibung	Beispiel
Max. Batchgröße	Maximale Anzahl von Events, die an einen einzelnen Prozessaufruf übergeben werden.	100

Registerkarte „Transport“

Feld	Beschreibung
Event Hubs-Namespace	Bereichscontainer für den/die Event-Hub(s). Dies ist ein Pflichtfeld.
Event Hub-Name	Der Event-Hub, aus dem Protokolldaten abgerufen werden sollen. Dies ist ein Pflichtfeld.
Event Hub credentials (Event-Hub-Anmeldeinformationen)	Freigegebene Zugriffsberechtigungsrichtlinie zur Authentifizierung beim Event-Hub. Dies ist ein Pflichtfeld.
Consumer Group name (Verbrauchergruppenname)	Zu verwendende Verbrauchergruppe. Dies ist ein Pflichtfeld.

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
Restore point rate (Rate für Wiederherstellungspunkt)	Anzahl der Events, die die Dateneingabe lesen kann, bevor ein Wiederherstellungspunkt gespeichert wird.	100
Processor threads count (Anzahl der Prozessor-Threads)	Gesamtanzahl der Prozessor-Threads.	2
Zeitüberschreitung für Vorgang	Anzahl der Sekunden, die gewartet werden soll, bevor Event-Hub-Vorgänge ablaufen.	120
Leerlauf-Zeitüberschreitung beim Empfang	Anzahl der Sekunden, die gewartet werden soll, bevor Empfangsvorgänge ablaufen.	60
Prefetch count (Anzahl der Vorabrufe)	Anzahl der Events, die vor Event-Hub-Vorgängen vorab empfangen wurden.	500

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwert
Standardzeitzone	Standardzeitzone, wenn das Protokoll keine Zeitzoneninformationen enthält.	GMT
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.	-1
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.	-1
Maximale Länge in Bytes	Maximale Länge von Events in Byte.	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Ruhezustandsintervall	Intervall der Wartezeit in Sekunden, bevor eine weitere Abfrage ausgeführt wird, nachdem eine Abfrage keine Events zurückgegeben hat.	60
Abfrageintervall	Intervall in Sekunden, das gewartet werden soll, bevor neue Events abgerufen werden.	0
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	falsch

Kafka SSL-Anmeldeinformationen – Felder

Beschreibung der Felder im Formular „Kafka SSL-Anmeldeinformationen“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SSL-Sicherheitsprotokoll

Feld	Beschreibung
SSL-Schlüsselspeicher	Der Inhalt einer tatsächlichen Datei server.keystore.jks, codiert als base64-Zeichenfolge.
SSL-Schlüsselspeicher-Typ	Format der SSL-Schlüsselspeicherdatei. Standard: Java KeyStore (JKS).
SSL-Schlüsselspeicher-Passwort	Passwort für den Schlüsselspeicher, identisch mit dem Wert der Eigenschaft ssl.keystore.password in Apache Kafka.
SSL-Schlüsselpasswort	Passwort, identisch mit dem Wert der Eigenschaft ssl.key.password in Apache Kafka.
SSL-Truststore	Inhalt einer tatsächlichen Datei client.truststore.jks, codiert als base64-Zeichenfolge.
SSL-Truststore-Typ	Format der Truststore-Datei. Standard: Java KeyStore (JKS).
SSL-Truststore-Passwort	Passwort für den Truststore, identisch mit dem Wert der Eigenschaft ssl.truststore.password in Apache Kafka.
SSL-Anbieter	Name des für SSL-Verbindungen verwendeten Sicherheitsanbieters.
Verifizierung des Hostnamens deaktivieren	Option zum Deaktivieren der Überprüfung des Hostnamens.
Zusätzliche Kafka-Verbrauchereigenschaften	Durch Semikolon getrennte Zeichenfolge zusätzlicher Kafka-Verbrauchereigenschaften. Beispiel: ssl.protocol=TLSv1.2;ssl.enabled.protocols=TLSv1.2,TLSv1.1

SASL_SSL-Sicherheitsprotokoll

Feld	Beschreibung
SSL-Truststore	Inhalt einer tatsächlichen Datei client.truststore.jks, codiert als base64-Zeichenfolge.
SSL-Truststore-Typ	Format der SSL-Truststore-Datei. Standard: Java KeyStore (JKS).
SSL-Truststore-Passwort	Passwort für den Truststore, identisch mit dem Wert der Eigenschaft ssl.truststore.password in Apache Kafka.
SSL-Anbieter	Name des für SSL-Verbindungen verwendeten Sicherheitsanbieters.
Verifizierung des Hostnamens deaktivieren	Option zum Deaktivieren der Überprüfung des Hostnamens.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SASL_SSL-Sicherheitsprotokoll (Fortsetzung)

Feld	Beschreibung
Benutzername	Der diesen Anmeldeinformationen zugeordnete Benutzername (sofern vorhanden). **Hinweis:** Der angegebene Benutzername wird für die SASL-Authentifizierung mit JAAS verwendet. Die folgende JAAS-Konfiguration wird an den Kafka-Server übergeben: `org.apache.kafka.common.security.plain.PlainLo required username=<user_name> password=<password>`.
Passwort	Das mit diesen Anmeldeinformationen verknüpfte Passwort. **Hinweis:** • Das angegebene Passwort wird für die SASL-Authentifizierung mit JAAS verwendet. Die folgende JAAS-Konfiguration wird an den Kafka-Server übergeben: `org.apache.kafka.common.security.plain.Plain required username=<user_name> password=<password>`. • Das von Ihnen angegebene Passwort ist unsichtbar. Es wird in verschlüsselter Form in der Datenbank gespeichert.
Zusätzliche Kafka-Verbrauchereigenschaften	Durch Semikolon getrennte Zeichenfolge zusätzlicher Kafka-Verbrauchereigenschaften. Beispiel: ssl.protocol=TLSv1.2;ssl.enabled.protocols=TLSv1.2,TLSv1.1

SASL_PLAINTEXT-Sicherheitsprotokoll

Benutzername	Der diesen Anmeldeinformationen zugeordnete Benutzername (sofern vorhanden). **Hinweis:** Der angegebene Benutzername wird für die SASL-Authentifizierung mit JAAS verwendet. Die folgende JAAS-Konfiguration wird an den Kafka-Server übergeben: `org.apache.kafka.common.security.plain.PlainLo required username=<user_name> password=<password>`.
Passwort	Das mit diesen Anmeldeinformationen verknüpfte Passwort.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SASL_PLAINTEXT-Sicherheitsprotokoll (Fortsetzung)

	Hinweis: • Das angegebene Passwort wird für die SASL-Authentifizierung mit JAAS verwendet. Die folgende JAAS-Konfiguration wird an den Kafka-Server übergeben: `org.apache.kafka.common.security.plain.PlainLoginModule required username=<user_name> password=<password>`. • Das von Ihnen angegebene Passwort ist unsichtbar. Es wird in verschlüsselter Form in der Datenbank gespeichert.
Zusätzliche Kafka-Verbrauchereigenschaften	Durch Semikolon getrennte Zeichenfolge zusätzlicher Kafka-Verbrauchereigenschaften. Beispiel: ssl.protocol=TLSv1.2;ssl.enabled.protocols=TLSv1.2,TLSv1.1

Apache Kafka Konfigurationsfelder für die Dateneingabe

Beschreibung der Felder im Formular Apache Kafka zur Konfiguration der Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Ausführen auf	Option, um zu bestimmen, ob ein bestimmtes MID-Server - oder ein MID-Server -Cluster verwendet werden soll. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.
MID	(Nur, wenn das Feld **Ausführen** auf auf Spezifischer MID-Server gesetzt ist) MID-Server, in den Protokolldaten aus Apache Kafka abgerufen werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern. • Wenn die Protokollerfassung für den ausgewählten MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur, wenn das Feld **Ausführen** auf auf MID-Server Cluster festgelegt ist.) Der Cluster MID-Server, in den die Protokolldaten abgerufen werden. Die Dateneingabe wird für einen einzelnen MID-Server im Cluster ausgeführt, bis dieser MID-Server ausfällt. Das System verschiebt dann alle Dateneingabeaufgaben entsprechend der konfigurierten Reihenfolge zu den nächsten verfügbaren MID-Server im Cluster. Diese Funktion wird in der Anwendung Health Log Analytics, Version 26.0.17 – Februar 2023 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Health Log Analytics unterstützt nur Failover-Cluster MID-Server. In diesen Clustern sind mehrere MID Servers zum Failover-Schutz in einer Gruppe zusammengefasst. Wenn Sie ein Cluster aus dem Dateneingabeformular auswählen, werden in der Liste der Cluster MID-Server nur Failover-Cluster angezeigt. • Der Cluster MID-Server darf nur MID Servers enthalten, die die Standardauthentifizierung unterstützen. mTLS wird für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden MID-Server im Cluster aktiviert werden. Wenn die Protokollerfassung für den aktiven MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn es mindestens einen MID-Server enthält und weniger als 10 Dateneingaben darauf ausgeführt werden, selbst wenn dieser MID-Server ausgefallen ist. Weitere Informationen zu MID-Server -Clustern finden Sie unter MID-Server-Cluster konfigurieren . Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet Apache Kafka zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Registerkarte „Abfrageeinstellungen“.

Feld	Beschreibung	Beispiel
Von	Von/Bis-Datum und -Uhrzeit zum Lesen der Daten. Daten, die älter als dieses Datum und diese Uhrzeit sind, werden nicht gelesen. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt. Dies ist ein Pflichtfeld.	Jetzt -1 Woche

Registerkarte „Transport“

Feld	Beschreibung	Beispiel
Kafka-Knotennamen	Kommagetrennte Liste im Format HOST:PORT,HOST:PORT. Die Liste muss nicht alle Server des Apache Kafka-Clusters enthalten.	123.4.5.6:9092,123.3.4.5:9093

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Transport“ (Fortsetzung)

Feld	Beschreibung	Beispiel
Themen	Kommagetrennte Liste von Themen, die die Dateneingabe abonnieren muss. Dies ist ein Pflichtfeld.	ErstesThema,ZweitesThema,DrittesThema
Kafka-Anmeldeinformationen	Verweis auf die Apache Kafka-Anmeldeinformationen. Sie können das Formular „Kafka SSL-Anmeldeinformationen“ anzeigen, indem Sie das Informationssymbol (ⓘ) und dann **Datensatz öffnen** auswählen. Im Formular können Sie das Sicherheitsprotokoll für die Authentifizierung mit Apache Kafka aus den folgenden Optionen auswählen: • **SSL**: SSL-Kanal. • **SASL_SSL**: SASL-authentifizierter SSL-Kanal. • **SASL_PLAINTEXT**: SASL-authentifizierter, nicht verschlüsselter Kanal. Eine Beschreibung der Felder im Formular „Kafka SSL-Anmeldeinformationen“ finden Sie unter Kafka SSL-Anmeldeinformationen – Felder.	Keine
Gruppen-ID	Name der Apache Kafka-Verbrauchergruppe.	Protokolle

Erweiterte Konfiguration

Formular „Erweiterte Konfiguration“

Feld	Beschreibung	Standardwert
Zeitüberschreitung	Zeit in Millisekunden, die beim Abruf gewartet wird, wenn in den Themen keine Daten verfügbar sind.	500

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Erweiterte Konfiguration“ (Fortsetzung)

Feld	Beschreibung	Standardwert
Zeitüberschreitung bei Knotenerkennung	Zeit in Millisekunden vor dem Ablaufen der Knotenerkennung.	30
Standardzeitzone	Standardzeitzone, wenn das Protokoll keine Zeitzoneninformationen enthält.	GMT
Anteil der zu verwerfenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen eines verworfen wird. Diese Einstellung wird verwendet, um die Anzahl der abgerufenen Events zu reduzieren.	-1
Anteil der zu empfangenden Unterstichproben	Anzahl der Events, die als Stapel ausgeführt werden sollen und von denen alle bis auf eines verworfen werden. Diese Einstellung wird verwendet, um die Anzahl der empfangenen Events zu reduzieren.	-1
Maximale Länge in Bytes	Maximale Länge von Events in Byte.	32766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.	falsch

Konfigurationsfelder für die REST-API-Dateneingabe

Beschreibung der Felder im Konfigurationsformular für die REST-API-Dateneingabe.

Basiskonfiguration

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
MID-Webserver	MID-Server, an den die Protokolldaten abgerufen werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: • Sie können nur MID Servers auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. Wenn Sie den MID-Server auswählen, werden die Felder **MID** und **Port** automatisch gefüllt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID-Server-Eigenschaften ändern. Dies ist ein Pflichtfeld.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest. Dies ist ein Pflichtfeld.

Die folgenden Felder zeigen schreibgeschützte Informationen:

Feld	Beschreibung
Status	Status der Dateneingabe
Übertragung	Protokoll zum Streamen der Protokolldaten. Die Dateneingabe verwendet REST zum Streamen von Protokolldaten an Ihre Instanz.
Quellenanzahl	Die Anzahl der Protokollquellen, die diese Dateneingabe erstellt haben.
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde

ServiceNow Systemprotokolle – Dateneingabe-Konfigurationsfelder abrufen

Beschreibung der Felder im Konfigurationsformular zum Abrufen der Dateneingabe für Systemprotokolle ServiceNow.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow Systemprotokolle – Dateneingabeformularfelder abrufen

Feld	Beschreibung
Name	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Der Standardwert ist „ServiceNow Glide Sys Log“. Dies ist ein Pflichtfeld. **Hinweis:** Health Log Analytics enthält den Quelltyp „glide_sys_log“ für den Protokolldatenverkehr von der Glide Sys Log-Serviceinstanz ServiceNow.
Von	Ausgangsdatum und -uhrzeit zum Lesen der Daten. Die Dateneingabe liest keine Daten, die älter als dieses Datum und diese Uhrzeit sind. Dies ist ein Pflichtfeld.
Status	Status der Dateneingabe
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Syslog-Tabellenfilter	Die Kriterien, die zum Filtern von Protokolldaten aus der Systemprotokolltabelle verwendet werden, bevor sie an die KI-Engine gestreamt werden.

Konfigurationsfelder für die CRBL-Dateneingabe

Beschreibung der Felder im Konfigurationsformular für die CRBL-Dateneingabe.

Erste Schritte

Feld	Beschreibung
Dateneingabename	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
MID-Server	MID-Server, an den die CRBL-Protokolle gestreamt werden. Dies ist ein Pflichtfeld.
Port	Port auf dem MID-Server. Wählen Sie einen Port innerhalb des vorgeschlagenen Bereichs aus dem Array aus. Der Port darf nicht von einem anderen Prozess belegt sein. Stellen Sie sicher, dass

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte (Fortsetzung)

Feld	Beschreibung
	das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.

Konfiguration

Feld	Beschreibung
URL der Cribl-Instanz	Die URL der CRBL-Instanz. HLA verwendet diese URL, um die Verbindung mit der CRBL-Instanz herzustellen.
Cribl-API-Token	Das Kribl-API-Token HLA verwendet, um sich bei Kribl zu authentifizieren und API-Aufrufe zu tätigen.

Prozess

Feld	Beschreibung
Cribl-Route	Die CRBL-Route. Wählen Sie eine Route aus der Dropdown-Liste aus, um Protokolldaten an ein bestimmtes Ziel zu leiten.
Cribl-Ziel	Das erstellte CRIB-Ziel. Das CRBL-Ziel zeigt auf den Host und Port MID-Server, die in der Dateneingabe konfiguriert sind. Dieses Feld ist schreibgeschützt.

Eingabekonfigurationsfelder für Edge-Delta-Daten

Beschreibung der Felder im Formular für die Konfiguration der Edge-Delta-Dateneingabe.

Formular für die Konfiguration der Delta-Dateneingabe für Edge

Feld	Beschreibung
Dateneingabename	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
Übertragung	Das Edge-Delta-Ziel, das für das Streaming von Protokollnachrichten an die Instanz ServiceNow verwendet wird. Die Optionen sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für die Konfiguration der Delta-Dateneingabe für Edge (Fortsetzung)

Feld	Beschreibung
	• TCP – Wird häufig für die Verarbeitung großer Mengen von Protokolldaten verwendet. Wenn Sie TCP auswählen, müssen Sie MID-Server und den Port angeben. Wenn Sie die TCP-Transportoption auswählen, erstellen Sie ein TCP-Ziel in Edge-Delta, um Protokolldaten aus einer beliebigen Quelle an die Instanz zu senden. Verwenden Sie dazu denselben MID-Server -Host und Port, den Sie für die Edge-Delta-Dateneingabe konfiguriert haben. **Hinweis:** Für TCP wird TLS/SSL nicht unterstützt. • HTTP: Wird häufig zum Senden kleinerer Protokolle über RESTful APIs, HTTP oder HTTPS für die sichere Übertragung verwendet. **Hinweis:** Für das HTTP-Protokoll wird die Authentifizierung verwendet. Wenn Sie HTTP auswählen, müssen Sie den MID-Webserver angeben, der auf dem MID-Serverausgeführt wird. Das System füllt dann die Felder MID-Server und Port automatisch basierend auf dem angegebenen MID-Webserver aus. Je nach MID-Webserverkonfiguration können Sie Protokolle entweder mit HTTP oder HTTPPS senden. Verwenden Sie HTTP, wenn das Kontrollkästchen **„Sichere Verbindung“** im Formular „MID-Webservererweiterung“ deaktiviert ist. Wenn ausgewählt, HTTPS verwenden. Weitere Informationen finden Sie unter Formular „Ereignismanagement MID-Webservererweiterung“. Wenn der **Authentifizierungstyp** im Formular der MID-Webservererweiterung Standard ist, geben Sie im Autorisierungsheader Details zur Standardauthentifizierung an. Wenn der **Authentifizierungstyp** „API-Schlüssel“ ist, geben Sie den Schlüssel als „Key Api_Key“ an. Wenn Sie die HTTP-Transportoption auswählen, erstellen Sie ein HTTP-Ziel in Edge Delta, und geben Sie die Endpunkt-URL im folgenden Format ein: http://{MID_SERVER_IP}:{MID_WEB_SERVER_PORT}/api/mid/hla/raw. Erstellen Sie unter Erweiterte Einstellungen zwei Header, die an die HTTP-Anforderung angehängt werden sollen: ◦ Ein Autorisierungsheader mit dem MID-Webserver-API-Schlüsselwert oder Standardanmeldeinformationen als konfigurierter MID-Webserver. ◦ Ein Inhaltstyp-Header, der mit dem Wert application/json benannt ist.
MID-Webserver	Der MID-Webserver, an den die Protokolldaten gestreamt werden.
MID-Server	MID-Server, an den die Edge-Delta-Protokolle gestreamt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für die Konfiguration der Delta-Dateneingabe für Edge (Fortsetzung)

Feld	Beschreibung
	Dies ist ein Pflichtfeld. Wenn Sie HTTP im Feld **„Transport“** ausgewählt haben, wird dieses Feld automatisch basierend auf dem ausgewählten MID-Webserver ausgefüllt.
Port	Der Port auf MID-Server, der zum Abhören von Protokollen verwendet wird. Wählen Sie einen Port innerhalb des vorgeschlagenen Bereichs aus dem Array aus. Beim TCP-Transport darf der Port nicht von einem anderen Prozess belegt sein. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld. Wenn Sie HTTP im Feld **„Transport“** ausgewählt haben, wird dieses Feld automatisch basierend auf dem ausgewählten MID-Webserver ausgefüllt.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. Die Auswahl der Serviceinstanz ermöglicht es HLA, CIs und Serviceinstanzen in der CMDB für die Ursachenanalyse zu korrelieren. **Hinweis:** Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest.

Konfigurationsfelder für die Dateneingabe des Vektoragenten

Beschreibung der Felder im Konfigurationsformular für die Dateneingabe des Vektoragenten.

Registerkarte „Erste Schritte“

Feld	Beschreibung
Dateneingabename	Name der neuen Dateneingabe. Dies ist ein Pflichtfeld.
Beschreibung	Beschreibung der Dateneingabe
MID-Server	MID-Server, an den die Vektoragentenprotokolle gestreamt werden. Dies ist ein Pflichtfeld. **Hinweis:** Wenn MID-Server ausfällt oder die Verbindung unterbrochen wird, wird die Vektor-Pipeline möglicherweise blockiert.
Port	Der Port auf MID-Server, der zum Abhören von Protokollen verwendet wird. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Erste Schritte“ (Fortsetzung)

Feld	Beschreibung
	Wählen Sie einen Port im Bereich von 6000 bis 6200 aus.
Übertragung	Das Protokoll, das zum Streamen von Protokollnachrichten an Ihre ServiceNow-Instanz verwendet wird. Derzeit ist nur TCP verfügbar.
Status	Status der Dateneingabe

Beschreibungen der Integrationskonfigurationsfelder

Dieser Abschnitt enthält Beschreibungen der Felder in den Integrationskonfigurationsformularen für Health Log Analytics.

Elasticsearch Integration Konfigurationsfelder

Beschreibung der Felder in den Konfigurationsformularen der Elasticsearch -Integration für Health Log Analytics.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den eingegebenen Namen angepasst.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der -Integration, um sie zu identifizieren.
Ausführen auf	Option, um zu bestimmen, ob ein bestimmtes MID-Server - oder ein MID-Server -Cluster verwendet werden soll.
MID-Server	(Nur, wenn das Feld **Ausführen** auf auf Spezifisch MID-Serverfestgelegt ist) Der MID-Server, an den Protokolldaten aus den Indizes Elasticsearch abgerufen werden. Dies ist ein Pflichtfeld.
MID-Server-Cluster	(Nur, wenn das Feld **Ausführen** auf auf MID-Server Cluster festgelegt ist) Der Cluster MID-Server, in den die Protokolldaten abgerufen werden. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	Wenn Sie ein Cluster auswählen, werden die MID Servers im ausgewählten Cluster und deren Status angezeigt. Die -Integration wird für einen einzelnen MID-Server im Cluster ausgeführt, bis dieser MID-Server fehlschlägt. Das System verschiebt dann alle Integrationsaufgaben gemäß der konfigurierten Reihenfolge zu den nächsten verfügbaren MID-Server im Cluster. **Hinweis:** • Health Log Analytics unterstützt nur Failover-Cluster MID-Server. In diesen Clustern sind mehrere MID Servers zum Failover-Schutz in einer Gruppe zusammengefasst. Wenn Sie im Formular Integration ein Cluster auswählen, werden in der Liste der MID-Server -Cluster nur Failover-Cluster angezeigt. • Der Cluster MID-Server darf nur MID Servers enthalten, die die Standardauthentifizierung unterstützen. mTLS wird für die Protokollerfassung nicht unterstützt. • Die Protokollerfassung muss für jeden MID-Server im Cluster aktiviert werden. Wenn die Protokollerfassung für den aktiven MID-Servernicht aktiviert ist, wird sie von Health Log Analytics automatisch aktiviert. • Wenn Elasticsearch die Client- oder CA-Zertifikatauthentifizierung verwendet, müssen alle MID Servers im Cluster über die entsprechenden Zertifikate verfügen. • Die standardmäßige maximale Anzahl von Integrationens, die Protokolle an ein einzelnes MID-Server streamen, beträgt 10. Ein Cluster besteht die Kapazitätsvalidierung, wenn es mindestens einen MID-Server enthält und weniger als 10 Integrationendarauf ausgeführt werden, auch wenn MID-Server ausgefallen ist.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben (Fortsetzung)

Feld	Beschreibung
	Hinweis: Wenn keine relevante Serviceinstanz vorhanden ist, Erstellen Sie eine für Service und fügen Sie CIs hinzu. Legen Sie den Status der neuen Serviceinstanz auf „Funktionsfähig“ fest.

Datenabrufmethode

Feld	Beschreibung
Server-URL	Die für den Zugriff auf den Cluster verwendete URL. Dies ist ein Pflichtfeld.
Authentifizierungsmethode	Die Authentifizierungsmethode, die zum Authentifizieren der -Integration in Elasticsearchverwendet wird. Standard ist keine. Wenn Sie die Authentifizierungsmethode auswählen, werden die entsprechenden Felder für Anmeldeinformationen im Formular angezeigt. **Hinweis:** Als Administrator können Sie eine Authentifizierungsmethode erstellen, indem Sie zu navigieren **Alle** > **Health Log Analytics** > **Authentifizierungsmethoden** und wählen Sie **Neu**.
Indexpräfix	Präfix vor die Namen von der Elasticsearch Indizes , aus denen Sie Daten lesen möchten. Die -Integration liest nur Daten aus Indizes , die mit dem -tene-konfigurierten -Präfix übereinstimmen. Beispiel: network-logs-* stimmt mit Indizes wie network-logs-2024.01.01 überein. Diese Einstellung stellt sicher, dass HLA nur Daten aus den relevanten Indizes erfasst. Dies ist ein Pflichtfeld.
Zeitstempelfeld des Dokuments	Zeitstempelfeld in Dokumenten, die in den Leseindizes gespeichert sind. Dies ist ein Pflichtfeld.
Begriffsfilter	JSON-Zuordnung der zu filternden Begriffe

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenabrufmethode (Fortsetzung)

Feld	Beschreibung
	Hinweis: Vermeiden Sie die Verwendung von Begriffsabfragen für Textfelder. Wenn das Zielfeld sowohl als Text als auch als Stichwort zugeordnet ist, referenzieren Sie das Stichwort mit feldname.stichwort.

Erweiterte Einstellungen

Feld	Beschreibung
Max. Anzahl von Verbindungen pro Route	Die maximale Anzahl von Verbindungen, die pro Knoten geöffnet werden sollen
Max. Bildlaufsegmente	Die Anzahl der für den relevanten Index in Elasticsearchkonfigurierten Shards. Diese Zahl teilt Elastic mit, wie viele parallele Abfragen in jeder Abfrageanforderung ausgeführt werden sollen.
Proxy-Host	Hostname des HTTP-Proxy, über den Anforderungen gesendet werden.
Proxy-Port	Port des HTTP-Proxy, über den Anforderungen gesendet werden
MID-Zertifikatrichtlinienprüfung verwenden	Option zum Aktivieren der Prüfung der MID-Zertifikatsrichtlinie. Wählen Sie diese Option aus, wenn Sie die Protokolle mit SSL/TLS verschlüsselt senden möchten. Navigieren Sie dann zu **Alle** > **MID-Server** > **MID-Sicherheitsrichtlinie** und fügen Sie die MID-Zertifikatrichtlinienprüfung zur Tabelle hinzu. Weitere Informationen finden Sie unter Richtlinien für MID-Server-Zertifikatprüfung .
Cross-Cluster-Suche verwenden	Option für die Suche nach Daten in Elasticsearch -Clustern. Wenn dieses Kontrollkästchen aktiviert ist, wird das Feld **Zu durchsuchende Cluster** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
	Hinweis: Ihre Einstellungen im Kontrollkästchen **Minimale Rechte verwenden** und im Feld **Verzögerung beim Lesen des aktuellen Zeitstempels (Sekunden)** im Formular **Erweiterte Konfiguration** wirken sich darauf aus, wie Daten in mehreren Clustern erfasst werden.
Minimale Berechtigungen verwenden	Option zum Lesen von Protokolldaten direkt aus den Indizes Elasticsearch mit dem konfigurierten Präfix. • Wenn ausgewählt, liest die -Integration die Protokolldaten direkt aus den Elasticsearch -Indizes mit dem konfigurierten Präfix. Zum Ausführen dieser Aufgabe sind nur Leseberechtigungen erforderlich. **Hinweis:** Wenn dieses Kontrollkästchen aktiviert ist und Sie die Cross-Cluster-Suche verwenden, werden Daten von allen Clustern gleichzeitig gesammelt. • Wenn diese Option gelöscht ist, ruft die -Integration alle Indizes mit dem Präfix ab, filtert sie und liest die Protokolldaten aus den gefilterten Indizes. Das Ausführen dieser Aufgabe erfordert zusätzliche Berechtigungen. **Hinweis:** Wenn Sie diese Checkbox bei Verwendung der Cross-Cluster-Suche deaktiviert lassen, wirkt sich dies darauf aus, wie Daten aus den Clustern gesammelt werden. Weitere Informationen finden Sie im Artikel „Cross-Cluster Search for Elasticsearch Data Inputs in Health Log Analytics“ [KB1556079] in der Knowledge Base Now Support. Weitere Informationen zum Streaming von Protokollen mithilfe der Elasticsearch -Integrationfinden Sie im Artikel Stream Logs with Elasticsearch data input - Advanced Guide [KB1080162] (Protokolle mit Elasticsearch-Dateneingabe streamen – Erweiterte Anleitung) in der Knowledge Base Now Support.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
Von	Startdatum zum Lesen der Daten. Daten, die älter als dieses Datum sind, werden nicht gelesen. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie diesen Wert auf ein vergangenes Datum festlegen, muss das System möglicherweise große Datenmengen lesen, was zu einer Überlastung führt.
Format des Zeitstempelfelds	Format des Zeitstempelfelds in den Dokumenten. Wenn kein Format angegeben ist, wird das Standardformat für die Unix-Epoch-Zeit in Millisekunden verwendet. Beispiel: 1684168407 (15. Mai 2023 16:33:27)
Begriffsfilter	JSON-Zuordnung der zu filternden Begriffe **Hinweis:** Vermeiden Sie die Verwendung von Begriffsabfragen für Textfelder. Wenn das Zielfeld sowohl als Text als auch als Stichwort zugeordnet ist, referenzieren Sie das Stichwort mit feldname.stichwort. Beispiel: {"severity":["error", "warning"]}
Tiebreaker für segmentierten Bildlauf	Wert, der zum Teilen der Daten verwendet wird. Jeder Teil wird parallel gescrollt. Standard: _id
Tiebreaker für nicht zunächst auf Suche beschränkt	Eindeutiger Wert pro Dokument, der beim Sortieren von Protokolleinträgen nach Zeitstempel als Tiebreaker verwendet werden soll.
Max. Anzahl von Dokumenten pro Abfrage	Maximale Anzahl von Dokumenten, die in einer einzelnen Abfrage abgerufen werden
Proxy-Port	Port des HTTP-Proxy, über den Anforderungen gesendet werden

ServiceNow Konfigurationsfelder für die Integration des Systemprotokollabrufs

Beschreibung der Felder im Konfigurationsformular für die Integration des Systemprotokollabrufs für ServiceNowHealth Log Analytics.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details angeben

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den eingegebenen Namen angepasst.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld. Die Standardserviceinstanz für diese Integration ist ServiceNow Systemprotokolle.

Konfigurationsfelder für TCP-Integration

Beschreibung der Felder in den Konfigurationsformularen der TCP-Integration für Health Log Analytics.

Registerkarte „Details angeben“.

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den eingegebenen Namen angepasst.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.
Port	Port für den MID-Server. Wählen Sie einen eindeutigen Port aus dem Array aus. Der Platzhalter zeigt den Bereich der Ports an, aus denen Sie auswählen können. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den ausgewählten Port öffnet. Dies ist ein Pflichtfeld.
MID-Server	Der MID-Server, an den die Protokolle gestreamt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Details angeben“. (Fortsetzung)

Feld	Beschreibung
	• Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.

Erweiterte Einstellungen

Feld	Beschreibung
SSL/TLS verwenden	Hiermit geben Sie an, ob SSL/TLS verwendet werden soll.
Hostnamen suchen	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen.
Anzahl der Boss-Threads	Anzahl der Threads, mit denen Verbindungen verwaltet werden
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden
Lesezeitüberschreitung in Sekunden	Zeitüberschreitung in Sekunden seit dem letzten Lesen. Wenn die Zeitüberschreitung abläuft, schließt das System den Kanal.
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte
Zeichencodierung	Zeichencodierung für diese Dateneingabe
Verwerfen, wenn Warteschlange voll ist	Hiermit legen Sie fest, dass Protokolle verworfen werden, wenn der MID-Server ausgelastet ist.
Trennzeichen für Trennlinien	Das Zeilenumbruchzeichen, das die Rohprotokollzeilen trennt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Einstellungen (Fortsetzung)

Feld	Beschreibung
	Teilende Werte müssen durch ein Komma gefolgt von einem Leerzeichen getrennt werden: ", ". Beispiel: „\r, \n, , aufgeteilt hier, #“.

Konfigurationsfelder für die UDP-Integration

Beschreibung der Felder in den Konfigurationsformularen der UDP-Integration für Health Log Analytics.

Registerkarte „Details angeben“.

Feld	Beschreibung
Integrationsname	Eindeutiger Name dieser Integration. Dies ist ein Pflichtfeld. **Hinweis:** Wenn Sie dieses Feld ausfüllen, wird der im Formular angezeigte generische Name automatisch an den eingegebenen Namen angepasst.
Beschreibung	Option zum Hinzufügen einer kurzen Beschreibung der Integration, um sie zu identifizieren.
MID-Server	Der MID-Server, an den die Protokolle gestreamt werden. **Hinweis:** • Sie können nur MID Servers mit Protokollerfassungsfunktion auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, sind nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID Server-Eigenschaften ändern.
Serviceinstanz	Die Serviceinstanz, an die die Protokolldaten gebunden werden sollen. Dies ist ein Pflichtfeld.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweitert

Feld	Beschreibung
Standardzeitzone	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist. Der Standardwert ist GMT.
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events Der Standardwert ist -1.
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events Der Standardwert ist -1.
Quotengrenze	Begrenzung der Anzahl der Ereignisse pro Sekunde, die diese Dateneingabe verarbeitet. Der Standardwert ist -1.
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte Der Standardwert ist 32.766.
Zeichencodierung	Zeichencodierung für diese Dateneingabe Der Standardwert ist UTF-8.
Verwerfen, wenn Warteschlange voll ist	Option zum Auswählen, dass Protokolle verworfen werden, wenn viele Prozesse in der Warteschlange auf den Zugriff auf den MID-Server warten.

Abschnitte und Karten auf der Registerkarte „Warnungsübersicht“ in Health Log Analytics

Die Registerkarte **Übersicht** hilft Ihnen, komponentenbasierte Warnungen, Log Analytics -Warnungen und Log Analytics -Warnungsgruppen zu verstehen.

Informationen auf der Registerkarte „Übersicht“ für eine komponentenbasierte Warnung

Die Registerkarte **„Warnungsübersicht“** in Health Log Analytics erleichtert das Verständnis von Komponentenbasierte Warnungen.

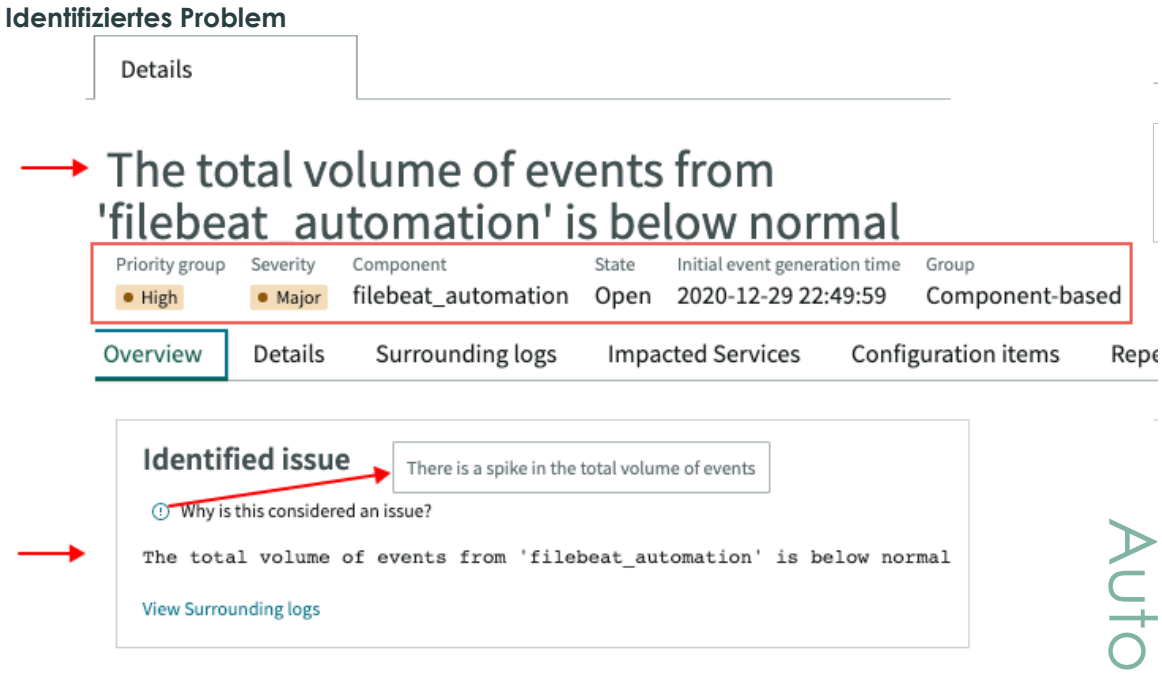
Abschnitte auf der Registerkarte „Übersicht“ für eine komponentenbasierte Warnung

Eine detaillierte Beschreibung von Komponentenbasierte Warnungen finden Sie unter Typs von Health Log Analytics Warnungen.

Identifiziertes Problem

Das „identifizierte Problem“ hat zur Warnung geführt. Das Problem wird im Titel der Warnung und auf einer Karte auf der Registerkarte angezeigt. Informationen zur Warnung werden im Banner angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Klicken Sie auf das Informationssymbol (ⓘ), um zu sehen, wie das Problem identifiziert wurde.
- Klicken Sie auf **Umgebende Protokolle anzeigen**, um die Protokollzeilen anzuzeigen, die von einer Minute vor bis eine Minute nach der Warnung generiert wurden. Weitere Informationen finden Sie unter Protokollzeilen rund um eine Anomalie analysieren.

Configuration Items

Um Einzelheiten zu den CIs anzuzeigen, die der Warnung zugeordnet sind, klicken Sie auf die Registerkarte **Configuration Items** oder auf **View more** (Mehr anzeigen) im Abschnitt „Configuration Items“. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Betroffene Services

Um detaillierte Informationen zu den Services anzuzeigen, die von den Warnungen betroffen sind, klicken Sie auf die Registerkarte **Betroffene Services**. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Anomaly (Anomalie)

Die Karte „Anomaly“ (Anomalie) stellt die anomale Aktivität dar, die zur Warnung geführt hat.

- Die blaue Linie zeigt die aktuelle anomale Aktivität an.
- In einigen Diagrammen zeigt der hell schattierte Bereich das erwartete Verhalten (erlernte Baseline) an.

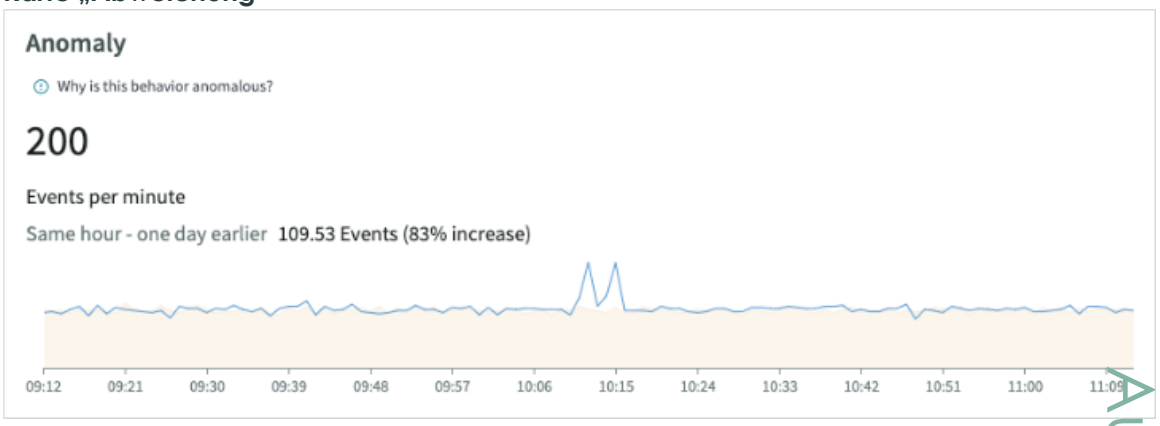
  Ein pfirsichfarbener Bereich stellt die Baselinewerte für die gleiche Stunde einen Tag früher dar. Ein rosa schattierter Bereich zeigt die Werte für den gleichen Zeitraum in der vorherigen Woche an.

- Klicken Sie auf das Informationssymbol, um zu sehen, wie die Anomalie erkannt wurde: ⓘ .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

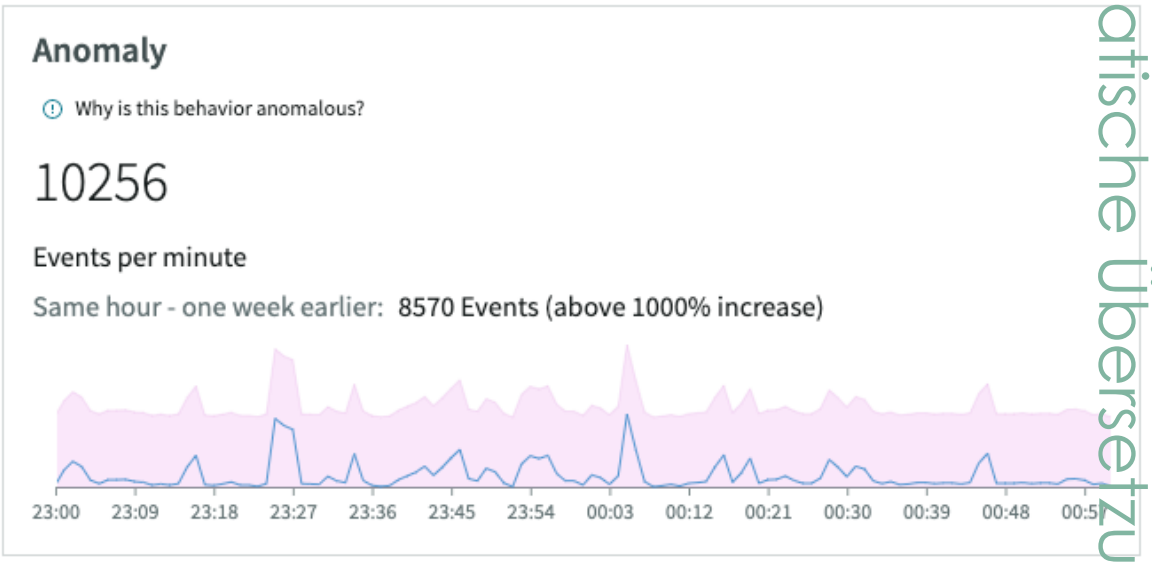
In diesem Beispiel zeigt der pfirsichfarben schattierte Bereich die Daten des vorherigen Tags zur gleichen Stunde. Die Spitze im Metrikwert (Events pro Minute) ist deutlich sichtbar.

Karte „Abweichung“



Der rosa schattierte Bereich in diesem Beispiel zeigt die Baselinewerte für die gleiche Stunde in der vorherigen Woche an.

Anomaliekarte mit Baselinewerten eine Woche früher



Weitere Informationen zu den Arten von Anomalien, die auftreten können, finden Sie unter Arten von anomalem Verhalten.

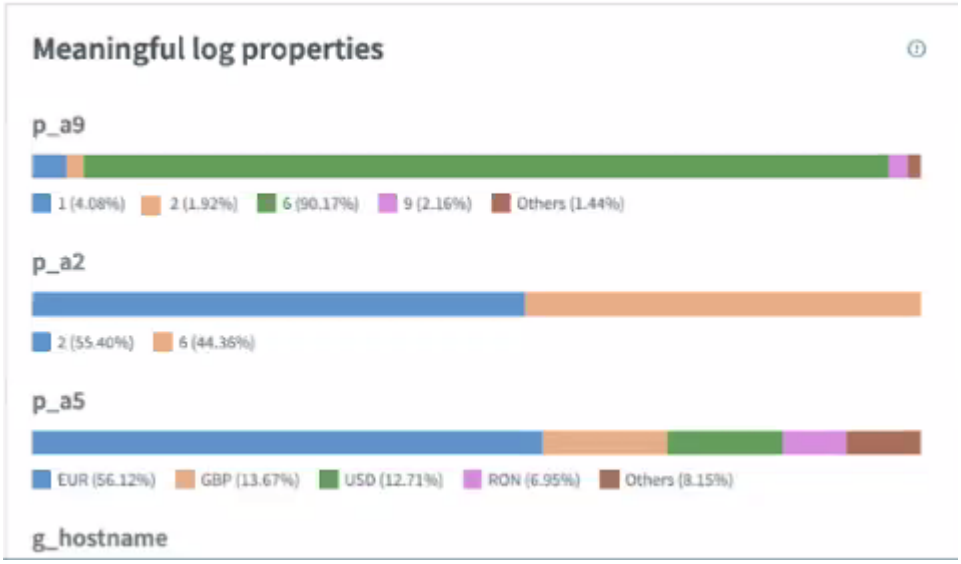
Aussagekräftige Protokolleigenschaften

Auf der Karte Aussagekräftige Protokolleigenschaften zeigt jedes Balkendiagramm die Verteilung der Werte für eine einzelne Protokolleigenschaft, die zur Anomalie beigetragen hat. Jeder Eigenschaftswert ist einer Farbe zugeordnet. Die Länge eines Farbbalkens entspricht dem Prozentsatz, der den Eigenschaftswert im Vergleich zu allen anderen Werten für die Eigenschaft darstellt. Für die Eigenschaft *p_a5* im Beispiel wurde der Wert *EUR* in 56,12 % der Protokollzeilen gefunden, *GBP* in 13,67 % usw.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

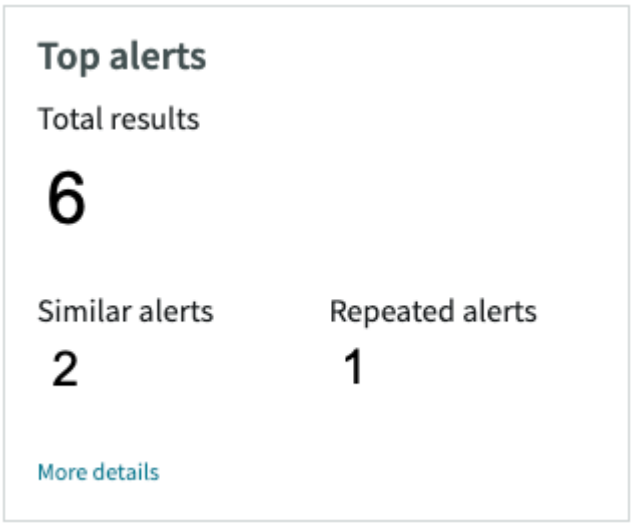
Aussagekräftige Protokolleigenschaften



Häufigste Warnungen

Die Karte „Häufigste Warnungen“ zeigt Zusammenfassungen der Daten aus den Registerkarten **Ähnliche Warnungen** und **Wiederholte Warnungen**. Das Gesamtergebnis ist die Summe der beiden Werte. Klicken Sie auf **Weitere Details**, um die Registerkarte **Alert Insight – Ähnliche Warnungen** zu öffnen. Details finden Sie unter Informationen auf der Registerkarte „Alert Insight – Ähnliche Warnungen“.

Häufigste Warnungen



Häufigste Incidents

Die Karte „Häufigste Incidents“ zeigt Zusammenfassungen der Daten aus den Registerkarten **Incidents für CI** und **Incidents bei zugehörigen CIs**. Das Gesamtergebnis ist die Summe der beiden Werte. Klicken Sie auf **Weitere Details**, um die Registerkarte **Incidents für CI** zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Häufigste Incidents

Informationen auf der Registerkarte „Übersicht“ für eine Log Analytics-Gruppe

Die Registerkarte **„Warnungsübersicht“**in Health Log Analytics erleichtert das Verständnis von Log Analytics-Gruppen.

Abschnitte auf der Registerkarte „Übersicht“ für Log Analytics-Gruppen

Eine detaillierte Beschreibung von Log Analytics-Gruppen finden Sie unter Typs von Health Log Analytics Warnungen.

Korrelationsbanner

Während der ersten Analyse werden Warnungen bewertet. Jede Korrelation in Protokolldaten einer Warnung mit einer anderen Warnung trägt zur Punktzahl einer Warnung bei. Je höher die Punktzahl, desto wahrscheinlicher ist es, dass die Warnung als Log Analytics-Warnung in eine Log Analytics-Warnung aufgenommen wird.

Die folgenden Arten von Daten werden berücksichtigt, wenn untersucht wird, ob Warnungen miteinander in Beziehung stehen:

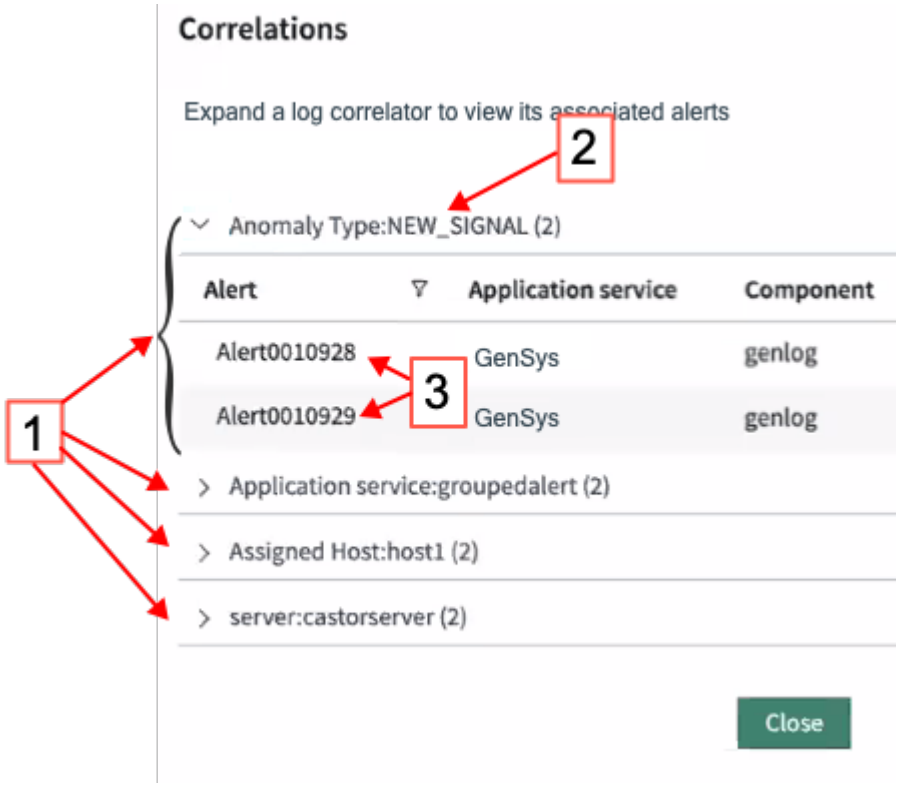
- Zeit: Alle Events traten innerhalb eines konfigurierten Zeitintervalls auf.
- Metadaten: Die Warnungen haben übereinstimmende Werte in Protokollzeile-Metadaten. Beispielsweise beziehen sich alle Warnungen auf denselben Host.
- Nachrichtentext: Der Nachrichtentext in den Protokolldaten ist zwischen Warnungen ähnlich oder identisch.
- Trend: Die Warnungen zeigen eine ähnliche Tendenz bei Werten oder Raten. Beispielsweise steigt ein bestimmter Metrikwert in allen Warnungen an.

Klicken Sie auf den Link **Weitere Informationen** im Banner Korrelationen, um die Liste der Korrelationen anzuzeigen, die die Log Analytics-Warnungen in Beziehung setzen.

Korrelationsbanner

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelationen



1. Liste der Korrelationen: Die erste Korrelation in der Liste wird erweitert, um die einzelnen Log Analytics-Warnungen anzuzeigen, die korrelieren, und Protokollkorrelator, die die Warnungen gemeinsam nutzen. Die Zahl in Klammern ist die Anzahl der Warnungen in der Korrelation.
2. Ein einzelner Protokollkorrelator: Der Bezeichner für eine Gruppe korrelierter Log Analytics-Warnungen. Die Warnungen werden nach den Protokollzeilendaten oder Metadaten gruppiert, die den Warnungen gemeinsam sind (z. B. IP-Adresse, Hostname oder Anwendername). Die Zahl in Klammern ist die Anzahl der miteinander in Beziehung stehenden Warnungen.
3. Log Analytics-Warnungen, die korreliert sind.

Warnungen in Gruppe

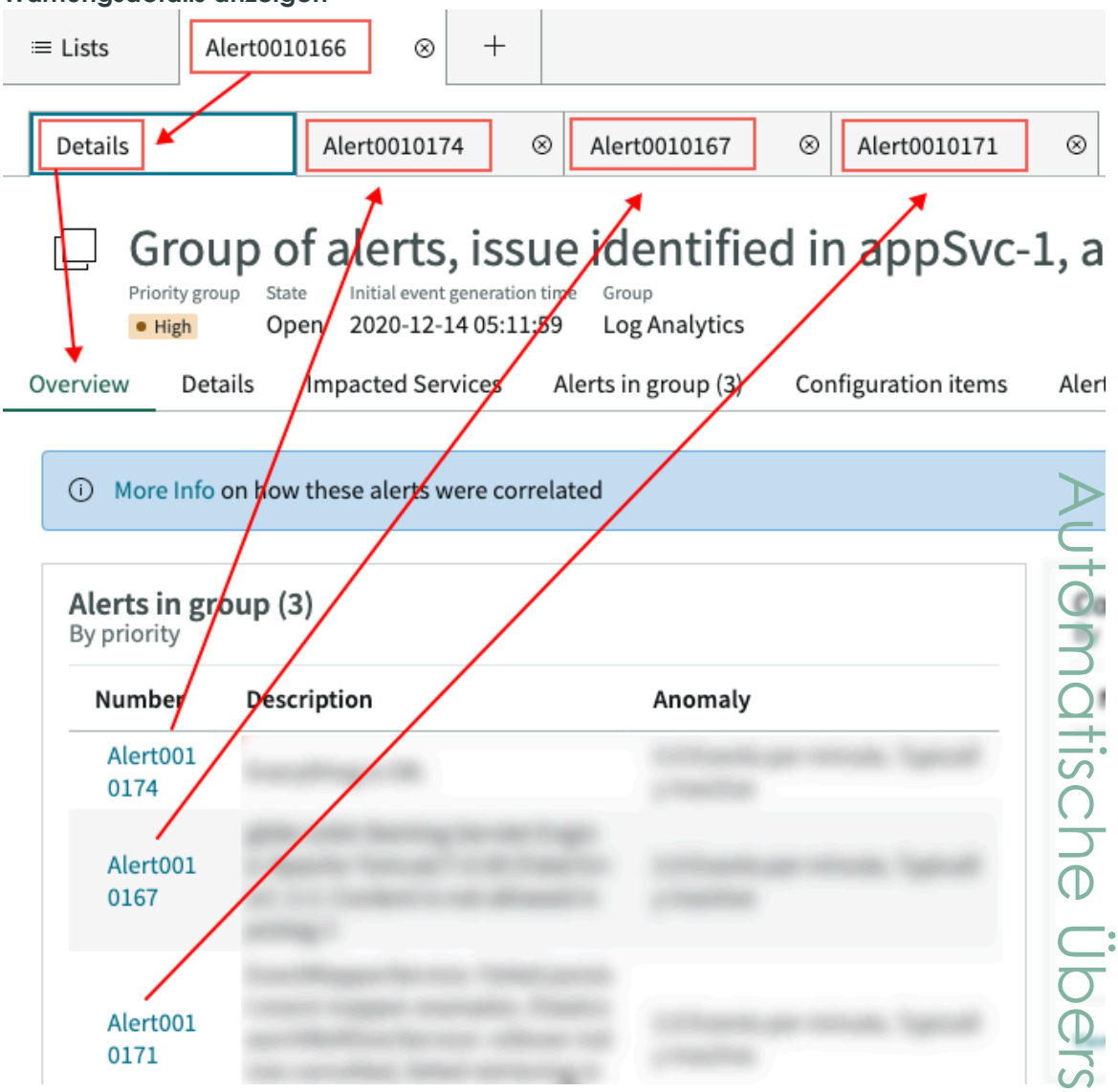
Bei einer Log Analytics-Warnung (im Beispiel Alert0010166) werden im Abschnitt „Warnungen in Gruppe“ die Log Analytics-Warnungen angezeigt, die unter der Log Analytics-Warnung gruppiert sind.

Klicken Sie auf eine Log Analytics-Warnung, um die zugehörigen Details anzuzeigen. Um die vollständige Liste der Log Analytics-Warnungen anzuzeigen, klicken Sie auf **Weitere anzeigen**, oder klicken Sie auf die Registerkarte **Warnungen in Gruppe**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsdetails anzeigen



Configuration Items

Um detailliertere Informationen zu den Konfigurationselementen (CIs) anzuzeigen, die der Warnung zugeordnet sind, klicken Sie auf die Registerkarte **Konfigurationselemente** oder auf **Mehr anzeigen** im Abschnitt „Konfigurationselemente“. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Betroffene Services

Um detaillierte Informationen zu den Services anzuzeigen, die von den Warnungen betroffen sind, klicken Sie auf die Registerkarte **Betroffene Services**. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Log Analytics-Warnungen auf der Registerkarte Warnungen in Gruppe

In der Tabelle werden die Log Analytics-Warnungen in einer Log Analytics-Gruppe auf der Registerkarte **Warnungen in Gruppe** beschrieben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Alerts in group“ (Warnungen in Gruppe)

Spalte	Beschreibung
Nummer	Die Nummer der Warnung, die in der Liste der Warnungen unter Dashboard des Operator-Arbeitsbereichsangezeigt wird. Um detaillierte Informationen für eine Warnung auf der Registerkarte **Details** anzuzeigen, klicken Sie auf die Warnungsnummer. Dieses Feld wird automatisch festgelegt.
Gruppe	Typ der Gruppe, zu der die Warnung gehört: eine eigenständige Log Analytics-Warnung oder eine Komponentenbasierte Warnung.
Beschreibung	Anomales Muster oder anomale Metrik, die die Generierung der Warnung verursacht haben.
Schweregrad	Schweregradwert für die Warnung. Verfügbare Werte: • **Kritisch**: Es ist eine sofortige Aktion erforderlich. Entweder funktioniert die Ressource nicht, oder es drohen kritische Probleme. • **Schwerwiegend**: Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung hat sich verschlechtert. • **Gering**: Die Leistung hat sich verschlechtert, oder es liegt ein partieller, nichtkritischer Verlust der Funktionalität vor. • **Warnung**: Die Ressource funktioniert zwar noch, bedarf aber der Aufmerksamkeit. • **Info**: Eine Informationsnachricht. Eine Warnung wird erstellt, die Ressource ist jedoch weiterhin funktionsfähig. • **Löschen oder Gelöst**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
Prioritätsgruppe	Prioritätsgruppe, die die Reihenfolge angibt, in der Warnungen gelöst werden sollen. Die Auswahlmöglichkeiten lauten wie folgt: • **Dringend** • **Hoch** • **Mittel** • **Niedrig**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Alerts in group“ (Warnungen in Gruppe) (Fortsetzung)

Spalte	Beschreibung
	Der Wert der Prioritätsgruppe ist wichtiger als der Schweregrad allein. Beispielsweise sollte eine Warnung mit hoher Priorität und niedrigem Schweregrad vor einer Warnung mit niedriger Priorität und hohem Schweregrad behandelt werden. Informationen zur Berechnung der Priorität finden Sie unter Warnungspriorität.
Status	Verarbeitungsstatus der Warnung. Neu generierte Warnungen befinden sich im Status **Offen**. Andere Status lauten wie folgt: • **Erneut öffnen**: Eine zuvor geschlossene Warnung wurde erneut geöffnet und erfordert Ihre Aufmerksamkeit. • **Flatternd**: Die Warnung erhält identische Events, die mit hoher Häufigkeit aus derselben Quelle eintreffen. Dieser Status kann dazu führen, dass eine Warnung aus dem Status „Geschlossen“ erneut geöffnet wird, was zu einer Anhäufung von Changes mit den Status „Offen“ und „Geschlossen“ führt. • **Geschlossen**: Die Warnung wurde geschlossen und erfordert keine weitere Aktion. Sie schließen eine Warnung, wenn sie behoben wurde.
Konfigurationselement	CI in der CMDB. Das CI wird von der Warnung angewendet.
Knoten	Knotenfeld, das in der Protokollnachricht empfangen wurde. Das in der Protokollnachricht beschriebene Event ist auf diesem Knoten aufgetreten. Oft ist der Knoten der Name des CI, das der Warnung zugeordnet ist. Zum Beispiel ein Computername, eine IP-Adresse, ein FQDN oder eine MAC-Adresse.
Quelle	Alle Health Log Analytics Warnungen weisen den Wert **Log Analytics** in der Spalte **Quelle** auf, um anzugeben, dass die App Health Log Analytics die Warnung generiert hat.
Metrikname	Name der Metrik, deren anomales Verhalten zu der Warnung geführt hat. Zum Beispiel `I/O request` für den Fall, dass die E/A-Anforderung länger als 15.000 ms dauerte.
Aktualisiert	Zeitpunkt der letzten Aktualisierung der Informationen oder des Status der Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen auf der Registerkarte „Übersicht“ für eine Log Analytics-Warnung

Die Registerkarte **„Warnungsübersicht“** in Health Log Analytics erleichtert das Verständnis von Log Analytics-Warnungen.

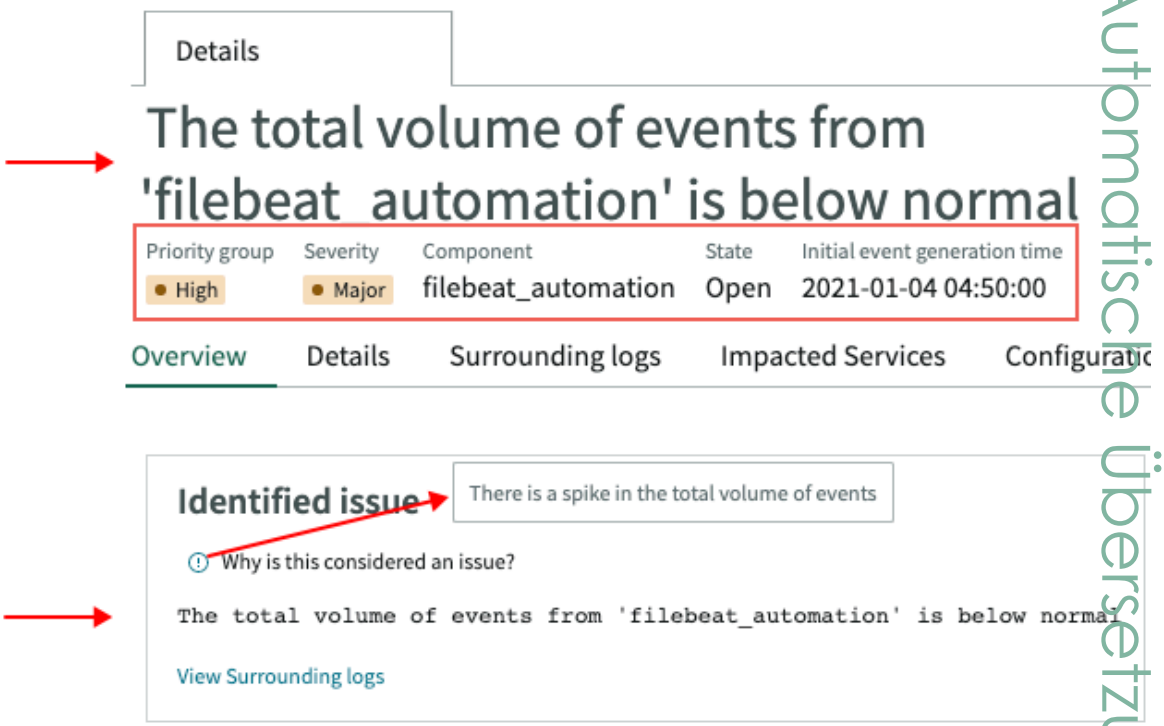
Abschnitte und Karten auf der Registerkarte „Übersicht“ für Log Analytics-Warnungen

Eine detaillierte Beschreibung von Log Analytics-Warnungen finden Sie unter Typs von Health Log Analytics Warnungen.

Identifiziertes Problem

Das „identifizierte Problem“ hat zur Warnung geführt. Das Problem wird im Titel der Warnung und auf einer Karte auf der Registerkarte angezeigt. Informationen zur Warnung werden im Banner angezeigt.

Identifiziertes Problem



- Klicken Sie auf das Informationssymbol (ⓘ), um zu sehen, wie das Problem identifiziert wurde.
- Klicken Sie auf **Umgebende Protokolle anzeigen**, um die Protokollzeilen anzuzeigen, die von einer Minute vor bis eine Minute nach der Warnung generiert wurden. Weitere Informationen finden Sie unter Protokollzeilen rund um eine Anomalie analysieren.

Configuration Items

Um Einzelheiten zu dem CI anzuzeigen, das der Warnung zugeordnet sind, klicken Sie auf die Registerkarte **Configuration Items** oder auf **View more** (Mehr anzeigen) im Abschnitt „Configuration Items“. Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Betroffene Services

Um detaillierte Informationen zu den Services anzuzeigen, die von den Warnungen betroffen sind, klicken Sie auf die Registerkarte **Betroffene Services**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Operator-Phase 1: Warnungen analysieren und bestätigen.

Anomaly (Anomalie)

Die Karte „Anomaly“ (Anomalie) stellt die anomale Aktivität dar, die zur Warnung geführt hat.

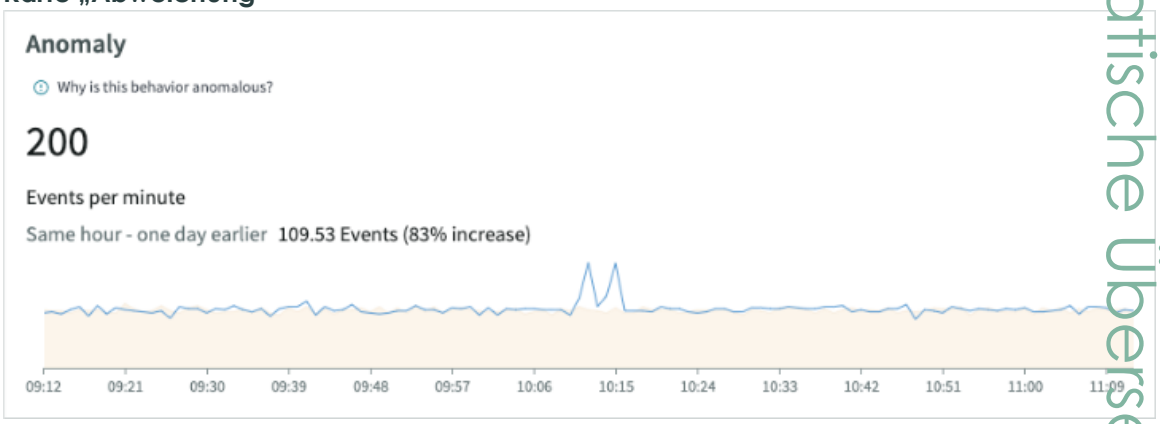
- Die blaue Linie zeigt die aktuelle anomale Aktivität an.
- In einigen Diagrammen zeigt der hell schattierte Bereich das erwartete Verhalten (erlernte Baseline) an.

  Ein pfirsichfarbener Bereich stellt die Baselinewerte für die gleiche Stunde einen Tag früher dar. Ein rosa schattierter Bereich zeigt die Werte für den gleichen Zeitraum in der vorherigen Woche an.

- Klicken Sie auf das Informationssymbol, um zu sehen, wie die Anomalie erkannt wurde: ⓘ.

In diesem Beispiel zeigt der pfirsichfarben schattierte Bereich die Daten des vorherigen Tags zur gleichen Stunde. Die Spitze im Metrikwert (Events pro Minute) ist deutlich sichtbar.

Karte „Abweichung“

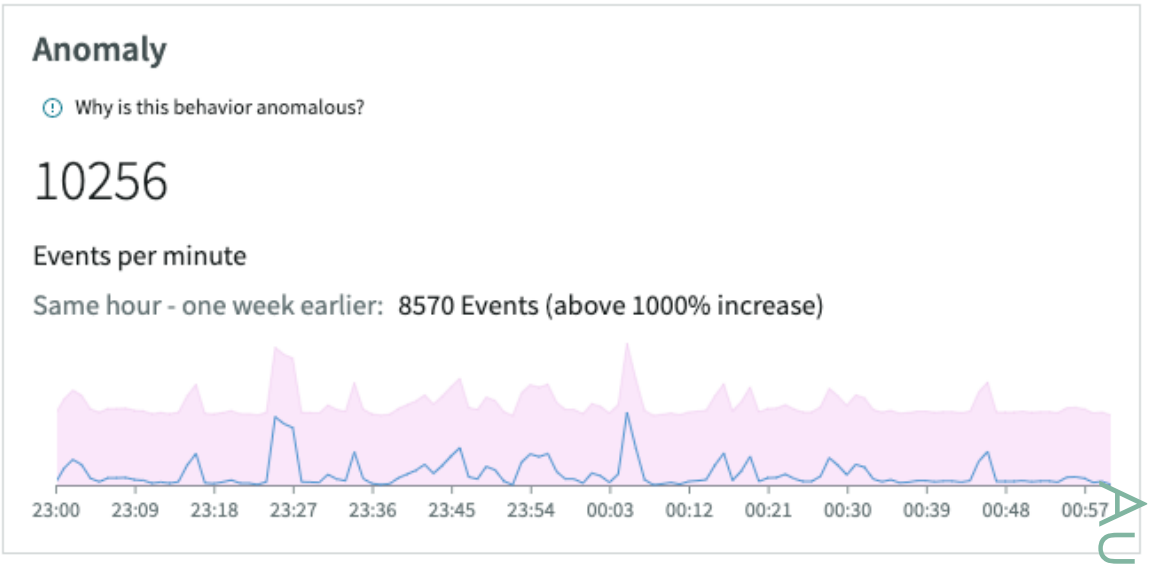


Der rosa schattierte Bereich in diesem Beispiel zeigt die Baselinewerte für die gleiche Stunde in der vorherigen Woche an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anomaliekarte mit Baselinewerten eine Woche früher

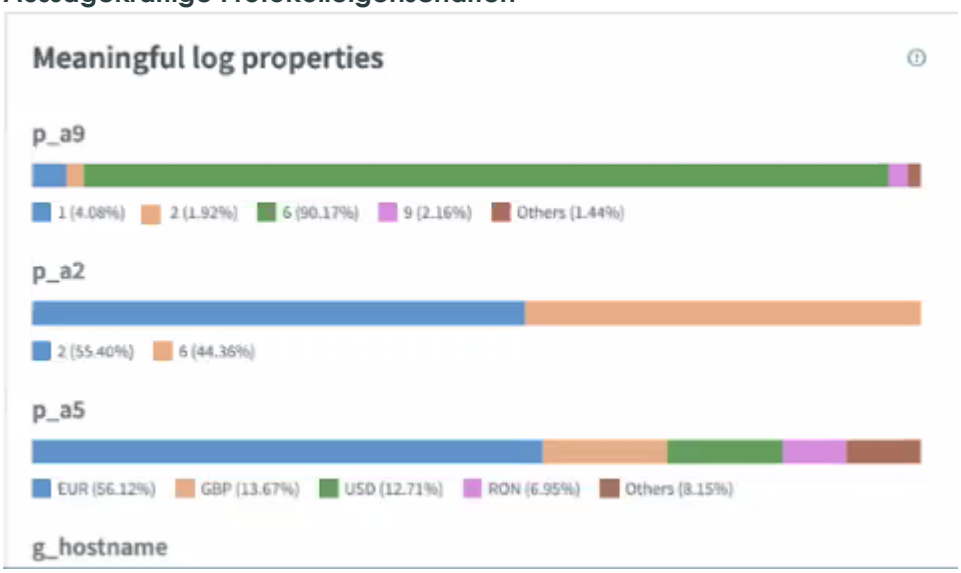


Weitere Informationen zu den Arten von Anomalien, die auftreten können, finden Sie unter Arten von anomalem Verhalten.

Aussagekräftige Protokolleigenschaften

Auf der Karte Aussagekräftige Protokolleigenschaften zeigt jedes Balkendiagramm die Verteilung der Werte für eine einzelne Protokolleigenschaft, die zur Anomalie beigetragen hat. Jeder Eigenschaftswert ist einer Farbe zugeordnet. Die Länge eines Farbbalkens entspricht dem Prozentsatz, der den Eigenschaftswert im Vergleich zu allen anderen Werten für die Eigenschaft darstellt. Für die Eigenschaft *p_a5* im Beispiel wurde der Wert *EUR* in 56,12 % der Protokollzeilen gefunden, *GBP* in 13,67 % usw.

Aussagekräftige Protokolleigenschaften



Häufigste Warnungen

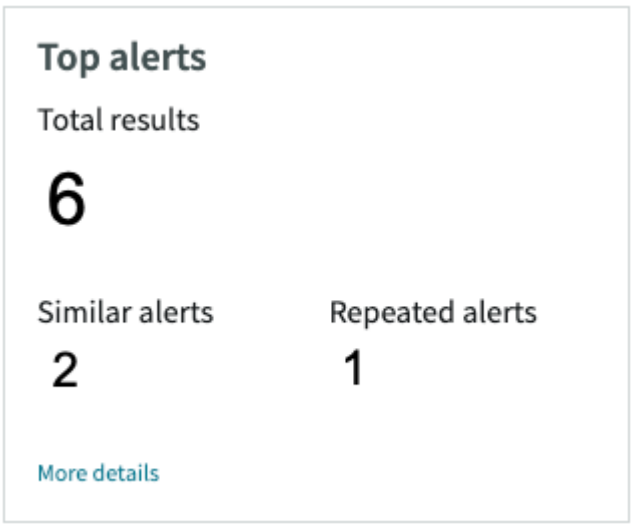
Die Karte „Häufigste Warnungen“ zeigt Zusammenfassungen der Daten aus den Registerkarten **Ähnliche Warnungen** und **Wiederholte Warnungen**. Das Gesamtergebnis ist die Summe der beiden Werte. Klicken Sie auf **Weitere Details**, um die Registerkarte **Alert Insight – Ähnliche Warnungen** zu öffnen. Details

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

finden Sie unter Informationen auf der Registerkarte „Alert Insight – Ähnliche Warnungen“.

Häufigste Warnungen



Häufigste Incidents

Die Karte „Häufigste Incidents“ zeigt Zusammenfassungen der Daten aus den Registerkarten **Incidents für CI** und **Incidents bei zugehörigen CIs**. Das Gesamtergebnis ist die Summe der beiden Werte. Klicken Sie auf **Weitere Details**, um die Registerkarte **Incidents für CI** zu öffnen.

Häufigste Incidents

Typs von Health Log Analytics Warnungen

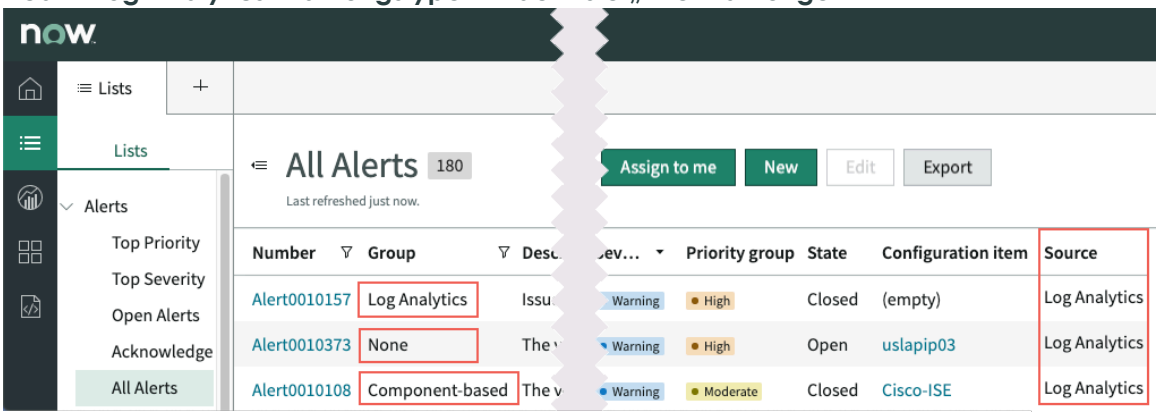
Health Log Analytics generiert mehrere Typen von Warnungen.

In einer Liste von Warnungen weisen alle von Health Log Analytics generierten Warnungen in der Spalte **Source** (Quelle) den Wert **Log Analytics** (Protokollanalytik) auf. Der Wert in der Spalte **Group** (Gruppe) identifiziert wie folgt die Art der Warnung:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Health Log Analytics-Warnungstypen in der Liste „Alle Warnungen“



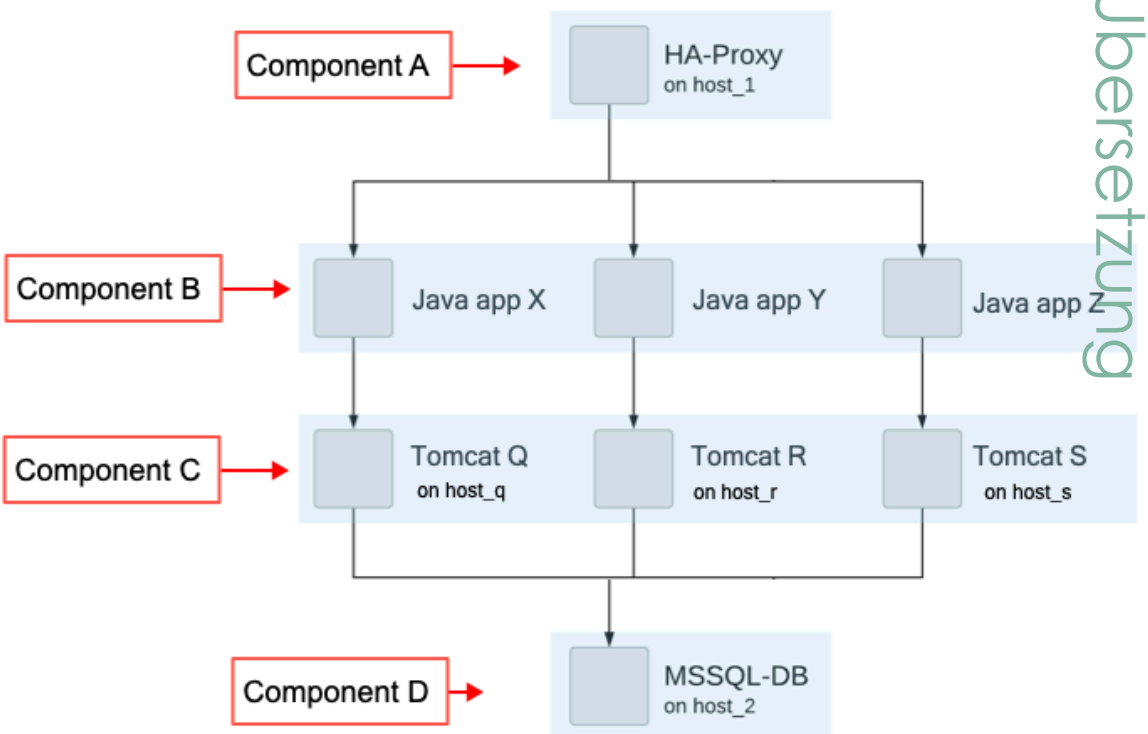
Komponentenbasierte Warnung (Alert0010108 im Beispiel)

Komponentenbasierte Warnungen betreffen mehr als ein Configuration Item (CI). Eine Komponente ist eine logische Komponente einer Serviceinstanz, die die Warnung verursacht hat. Eine Komponente kann mehrere CIs umfassen, die dieselbe Funktion ausführen, z. B. mehrere redundante Hosts.

Wichtig: Jede Komponentenbasierte Warnung ist das übergeordnete Element einer Reihe von schreibgeschützten Warnungen. Sie arbeiten nicht direkt mit schreibgeschützten Warnungen. Sie arbeiten nur an der übergeordneten Komponentenbasierte Warnung.

In dieser Beispielserviceinstanz bilden die identischen Java-Apps X, Y und Z eine einzige Komponente: Komponente B. Die Tomcat-Server Q, R und S und ihre Hosts bilden eine andere Komponente: Komponente C.

Beispielserviceinstanz



Log Analytics-Warnung (Alert0010373 im Beispiel)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Log Analytics-Warnung identifiziert eine Anomalie, die ein einzelnes CI betrifft. Eine Log Analytics-Warnung weist in der Spalte **Group** (Gruppe) den Wert **None** (Keine) auf. Die Anomalie, die zur Warnung führt, kann eine unerwartete Anzahl von Protokolleinträgen oder ein unerwarteter Wert einer Metrik sein.

Log Analytics-Gruppe (Alert0010157 im Beispiel)

Wenn das System mehrere Log Analytics-Warnungen identifiziert, die miteinander in wichtiger Beziehung stehen, werden sie in einem Log Analytics-Gruppegruppiert. Eine Log Analytics-Gruppe kann bis zu vier Warnungen gruppieren. Das System generiert eine Log Analytics-Gruppe, wenn die Log Analytics-Warnungen eine oder mehrere der folgenden Beziehungen gemeinsam haben:

- Zeit: Alle Events traten innerhalb eines konfigurierten Zeitintervalls auf.
- Metadaten: Die Warnungen haben übereinstimmende Werte in Protokollzeile-Metadaten. Beispielsweise beziehen sich alle Warnungen auf denselben Host.
- Nachrichtentext: Der Nachrichtentext in den Protokolldaten ist zwischen Warnungen ähnlich oder identisch.
- Trend: Die Warnungen zeigen eine ähnliche Tendenz bei Werten oder Raten. Beispielsweise steigt ein bestimmter Metrikwert in allen Warnungen an.

Hinweis: Sie können eine Warnung als signifikant markieren. Eine signifikante Warnung ist eher in einem Log Analytics-Gruppe enthalten, wenn sich die zugeordnete Metrik anomal verhält. Weitere Informationen finden Sie unter Warnung als signifikant markieren.

Arten von anomalem Verhalten

Anomales Verhalten in einem CI oder einem Service kann auf ein wichtiges Problem hinweisen. Zum Beispiel kann eine Spitze in der Häufigkeit oder Anzahl von Nachrichten eines bestimmten Typs auf ein Problem hinweisen.

Anomalien interpretieren

Das System überwacht den Protokollstream, um Muster-, Metrik- und Anzeigebaselines über verschiedene Zeiträume zu lernen und auf diese Weise Modelle des erwarteten Verhaltens zu erzeugen. Zeiträume können stündlich, täglich, wöchentlich oder unbegrenzt sein. Verhalten, das von den erlernten Modellen abweicht, wird als anomales Verhalten betrachtet.

Typen der Protokolleigenschaft

Muster

Ein Muster ist ein Wert oder eine Rate, die sich wiederholt − in Text, Zeit oder Beziehungen.

Zähler

Eine Zählereigenschaft ist ein numerischer Wert oder Textwert. Beispiele: Statuscode, Antwortcode, Aktion oder Muster.

Anzeige

Eine Anzeigeneigenschaft besitzt einen numerischen Wert, der kontinuierlich gemeldet wird. Anzeigeneigenschaften stellen Vorgänge dar, die Ressourcen verbrauchen. Beispiele: CPU-Auslastung, Speicherauslastung oder Antwortzeit

Wie Anomalien im Service Operations-Arbeitsbereichangezeigt werden

Die Karte „Anomaly“ (Anomalie) stellt die anomale Aktivität dar, die zur Warnung geführt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

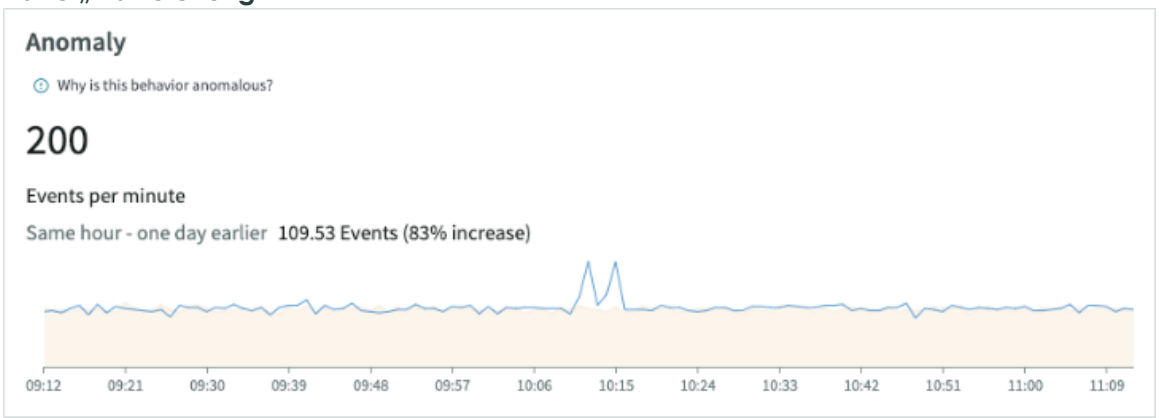
- Die blaue Linie zeigt die aktuelle anomale Aktivität an.
- In einigen Diagrammen zeigt der hell schattierte Bereich das erwartete Verhalten (erlernte Baseline) an.

  Ein pfirsichfarbener Bereich stellt die Baselinewerte für die gleiche Stunde einen Tag früher dar. Ein rosa schattierter Bereich zeigt die Werte für den gleichen Zeitraum in der vorherigen Woche an.

- Klicken Sie auf das Informationssymbol, um zu sehen, wie die Anomalie erkannt wurde: ⓘ.

In diesem Beispiel zeigt der pfirsichfarben schattierte Bereich die Daten des vorherigen Tags zur gleichen Stunde. Die Spitze im Metrikwert (Events pro Minute) ist deutlich sichtbar.

Karte „Abweichung“



Arten von Anomalien

Einige der Anomaliearten

Verhalten	Beschreibung
Neues Verhalten	Bisher unbekanntes Muster. Für den Warnungstyp „Neues Verhalten“ wird kein Diagramm angezeigt.
Signal inaktiv/Wird nicht mehr angezeigt	Alle Muster- oder Protokolldaten aus einer Quelle wurden angehalten. Kein Signal für mindestens fünf Minuten.
Signal aktiv/Wird wieder angezeigt	Muster- oder Protokolldaten aus einer „toten“ Quelle werden erneut angezeigt. Bei einer Baseline von einer Stunde ist ein Muster „inaktiv“, wenn es weniger als einmal pro Minute erscheint.
Anomalie über oder unter Durchschnitt	Aktivität, die vom erwarteten Baselineverhalten für Muster-, Zähler- oder Messmetriken abweicht (z. B. Stichwort- oder Schweregradmetriken).
Anstieg oder Sinken einer Baselinereferenz	Eine Erhöhung/Verringerung des Werts oder der Quantität einer Protokolleigenschaft im Vergleich zur Baseline von einer Stunde oder einer Woche.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einige der Anomaliearten (Fortsetzung)

Verhalten	Beschreibung
Korrelation von Schweregrad- und Stichwortwarnungen	Quantitaver Anstieg eines Schweregrads oder Stichworts

Umgebende Protokollregisterkartenfelder

In diesem Abschnitt werden die Informationen beschrieben, die auf der Registerkarte **„Umgebende Protokolle“** angezeigt werden.

Registerkarte „Umgebende Protokolle“

Spalte	Beschreibung
Uhrzeit	Zeitstempel der Protokollzeile im Format, das die Quelle verwendet. Wenn kein Wert angezeigt wird, überprüfen Sie die Quelltypstruktur der Rohdaten.
Anwendungsservice	Serviceinstanz, in der die Metrik gefunden wurde.
Komponente	Logische Komponente von Serviceinstanz, die das Event generiert hat. Mehrere CIs können manchmal dieselbe Funktion ausführen.
Nachricht	Interne Nachricht aus Protokollzeile in Rohform, die den Text der vom System generierten Protokollnachricht über die Art des Vorkommens enthält.
Ebene	Typ des Events. Die verfügbaren Werte sind in der Reihenfolge ihrer Bedeutung: • **Notfall** • **Warnung** • **Kritisch** • **Fehler** • **Warnung** • **Hinweis** • **Informativ** • **Debuggen**
Host	Hostbezeichner aus der Protokollzeile, bestehend aus dem Hostnamen oder der IP-Adresse des Endpunkts.
Protokollnachricht	Die Rohprotokollnachricht ohne Header.

Felder der Protokoll-Viewer-Tabelle

In diesem Abschnitt werden die Informationen beschrieben, die in der **Protokoll-Viewer** -Tabelle angezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder der Protokoll-Viewer-Tabelle

Spalte	Beschreibung
Zeit	Zeitstempel der Protokollzeile im Format, das die Quelle verwendet. Wenn kein Wert angezeigt wird, überprüfen Sie die Quelltypstruktur der Rohdaten.
Serviceinstanz	Serviceinstanz, in der die Metrik gefunden wurde.
Komponente	Logische Komponente von Serviceinstanz, die das Event generiert hat. Mehrere CIs können manchmal dieselbe Funktion ausführen.
Nachricht	Interne Nachricht aus Protokollzeile in Rohform, die den Text der vom System generierten Protokollnachricht über die Art des Vorkommens enthält.
Ebene	Typ des Events. Die verfügbaren Werte sind in der Reihenfolge ihrer Bedeutung: • **Notfall** • **Warnung** • **Kritisch** • **Fehler** • **Warnung** • **Hinweis** • **Informativ** • **Debuggen**
Host	Hostbezeichner aus der Protokollzeile, bestehend aus dem Hostnamen oder der IP-Adresse des Endpunkts.
Protokollnachricht	Die Rohprotokollnachricht ohne Header.

Hinweis: Standardmäßig wird die Spalte „Rohnachricht“ in der Protokoll-Viewer-Tabelle nicht angezeigt. Sie können diese Spalte anzeigen, indem Sie sie im Bereich **Filter** auswählen. Weitere Informationen finden Sie unter Protokoll-Viewer-Tabelle anpassen.

Formularfelder für Protokollkorrelatoren

In diesem Abschnitt werden die Felder im Formular „Protokollkorrelatoren“ beschrieben.

Formular „Protokollkorrelatoren“.

Feld	Beschreibung
Typ	Typ des Protokollkorrelators. Es gibt folgende Optionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Protokollkorrelatoren“. (Fortsetzung)

Feld	Beschreibung
	• **Freitextkorrelator**: Der Protokollkorrelator analysiert den Text in der Protokollnachricht. • **Protokoll-Schlüssel-Korrelator**: Der Protokollkorrelator analysiert Protokollmetadaten. Zum Beispiel der Name einer Serviceinstanz in Ihrer Infrastruktur. Protokolleigenschaftskorrelatoren sind spezifisch für den Geschäftskontext Ihrer Umgebung. Weitere Informationen finden Sie unter Identifizieren von Beziehungen in Protokolldaten mithilfe von Protokollkorrelatoren.
Freitextbegriff oder Bezeichner	Text, den der Protokollkorrelator beim Analysieren von Protokollzeilen isoliert. Die Bezeichnung für dieses Feld lautet **Freitextbegriff** für Freitext-Protokollkorrelatoren und **Bezeichner** für Protokolleigenschaftskorrelatoren. **Hinweis:** Der Wert dieses Felds kann der Text für beide Arten von Protokollkorrelatoren sein. Daher lautet die Bezeichnung für diese Spalte in der resultierenden Liste der Protokollkorrelatoren **Korrelationsindikator**.
Aktiv	Option zum Anwenden des Protokollkorrelators. Wenn Sie dieses Feld auswählen, wendet das System den Protokollkorrelator auf den Protokollstream an.
Analyseumfang	Satz von Quellen, deren Protokolldaten von diesem Protokollkorrelator analysiert werden. Die Auswahlmöglichkeiten lauten wie folgt: • **Alle Quellen**: Der Protokollkorrelator wird auf Protokollzeilen aus allen Quellen im Datenstrom angewendet. • **Nur neue Quellen**: Der Protokollkorrelator wird auf Protokollzeilen aus allen Quellen angewendet, die nach der Aktivierung dieses Protokollkorrelators erstellt wurden. • **Angegebene Quelle**: Der Protokollkorrelator wird nur auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Protokollkorrelatoren“. (Fortsetzung)

Feld	Beschreibung
	die Protokollzeilen aus der Quelle angewendet, die Sie in diesem Formular angeben.
Ausgeschlossene Quellen	Quellen, die vom Protokollkorrelator ausgeschlossen sind. Das System analysiert keine Protokollzeilen aus Quellen, die in diesem Feld aufgeführt sind. **Hinweis:** Dieses Feld gilt nur, wenn das Feld **Analyseumfang** auf **Alle Quellen** oder **Nur neue Quellen** gesetzt ist. Informationen zum Ausschließen einer Quelle aus einem Protokollkorrelator finden Sie unter Quellen aus einem Protokollkorrelator ausschließen.
Quelle	Quelle des Protokollkorrelators. Der Protokollkorrelator analysiert die Daten dieser Protokollquelle. Dieses Feld wird nur angezeigt, wenn Sie den Protokollkorrelator aus dem Formular „Protokollquellen“ hinzufügen. Das Feld wird automatisch auf die Protokollquelle festgelegt, an der Sie arbeiten.

Informationen auf der Registerkarte „Alert Insight – Ähnliche Warnungen“

Zeigen Sie die Liste der Warnungen an, die auf der Registerkarte **Alert Insight – Ähnliche Warnungen** von der Alert Insight-Funktion bereitgestellt werden. Die Alert Insight-Funktion generiert die Informationen, die Sie bei der Lösung der Warnung unterstützen.

Registerkarte „Alert Insight – Ähnliche Warnungen“

Die Registerkarte enthält Informationen über andere Warnungen, die in den letzten 30 Tagen generiert wurden und die denselben CI-Typ, dieselbe Quelle, dieselbe Ressource, denselben Metriknamen usw. aufweisen.

Service Operations-Arbeitsbereich bietet eine kontextbezogene Warnungsselektierung basierend auf Daten von IT Service Management (ITSM), z. B. aus Incidents, Change-Anforderungen und Problemen. Die Funktion Alert Insight hilft Ihnen, die Ursache zu ermitteln, und empfiehlt eine Lösung. Mit dem intelligenten Start im Kontext können Sie eine der folgenden Aktionen ausführen:

- Anwendung starten
- Browser mit einer angegebenen URL öffnen
- Fehlerkorrektur durchführen (basierend auf Orchestrierung)
- Subflow starten (Workflow basierend auf Flow Designer)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

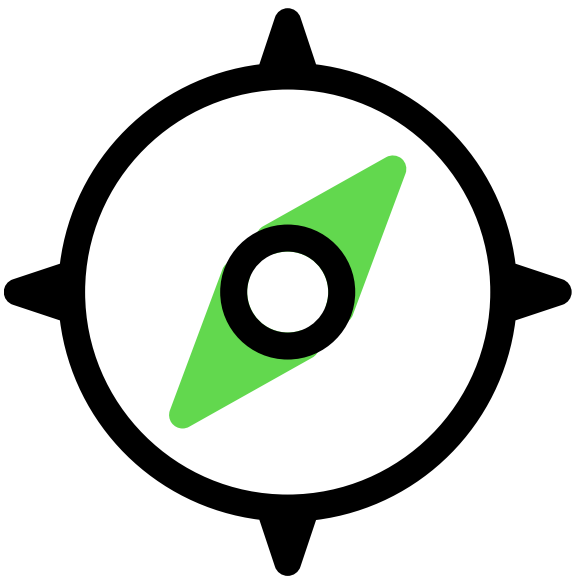
Service Reliability Management

Service Reliability Management (SRM) unterstützt Ihre Organisation bei der Bearbeitung von Warnungen und Incidents bei Reaktion, Zusammenarbeit, Nachverfolgung und Selbstkorrektur. SRM ist verfügbar, wenn Sie Abonnements für ITSM Professional und ITOM Operator Professional haben.

Übersicht von Service Reliability Management

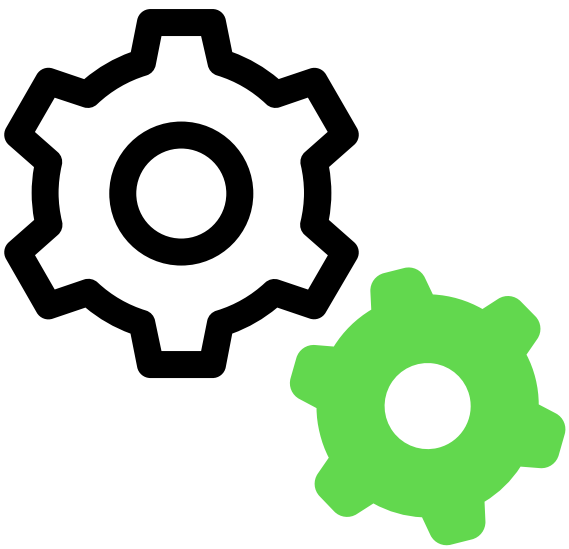
Erste Schritte

Untersuchen



Erfahren Sie mehr über die Konzepte und Funktionen SRM von .

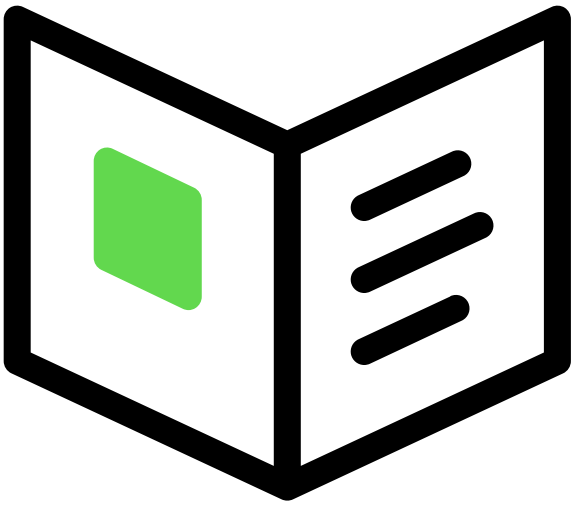
Konfigurieren



Installieren und konfigurieren Sie den SRM.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden	Referenz
	
Arbeiten Sie mit Services, Teams und Zuverlässigkeitsaufgaben in SRM.	Rufen Sie Details zu SRM -Komponenten ab, z. B. Felder, Tabellen und Eigenschaften.

Installieren Sie aus dem Store

Installieren Sie SRM von ServiceNow Store. Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Hinweis: Bestätigen Sie bei der Installation aus dem Store zunächst, dass Sie über alle erforderlichen Abhängigkeiten verfügen, indem Sie die Registerkarte Abhängigkeiten auswählen. Weitere Informationen finden Sie unter Installieren Sie die Anwendung Service Reliability Management aus dem Admin Center oder ServiceNow Store.

Problembehandlung und Hilfe

- Besuchen Sie unsere Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Service Reliability Management erkunden

Service Reliability Management (SRM) bietet Teams eine geführte Selfservice-Experience zur Verwaltung der Serviceintegrität. Die Experience wird mit der Anwendung Service Operations Workspace erstellt und kombiniert ITOM- und ITSM-Funktionen in einem einzigen Workflow.

SRM – Übersicht

Optimieren Sie die Serviceintegrität mit Site Reliability Engineering-Methoden (SRE). SRM ist ein einzelner Betriebsarbeitsbereich, mit dem Teams die Zuverlässigkeit digitaler Services mit SRE verbessern können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Mit Rufbereitschaftseskalationen können Sie rechtzeitig auf Probleme reagieren.
- Reduzieren Sie die Setup-Probleme mit geführtem Self-Service, um verteilte Teams mit getrennten Daten, ermöglichtem Zugriff und minimaler Governance von der zentralen IT einarbeiten zu lassen.

Wenn SRM installiert ist, werden auch mehrere Plugins und Anwendungen aktiviert. Weitere Informationen finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Integrität.

SRM – Anwender

Anwender

Anwender	Beschreibung	Enthält Rollen
Administrator	Ein ServiceNow-Administrator ist für Verwaltung, Entwicklung, Betrieb, Schulung und Wartung der ServiceNow Platform verantwortlich. Verantwortlich für die Installation und kann die Service Operations-Arbeitsbereich Admin Center-Konfiguration von SRM durchführen.	Alle
-Administrator [srm_admin] **Hinweis:** Diese Rolle unterscheidet sich von der Administratorrolle ServiceNow.	SRM-Administratoren können Kontoeinstellungen, Konfigurationen und Benutzer verwalten. Administratoren können folgende Aktionen ausführen: • Alle SRM-Konfigurationen erstellen, bearbeiten oder löschen und darauf zugreifen. • Integrationen hinzufügen oder verwalten. • Erstellen Sie Integrationen mit APM-Tools (Application Performance Monitoring) für Anwendungen. • Zuverlässigkeitsmetriken einrichten und verwalten. • Fehlerbudgetrichtlinien einrichten und verwalten.	• Manager • Beantworter
-Manager [srm_manager]	Manager überwachen ein Team von SREs. Manager weisen dem Rufbereitschaftszeitplan des Teams SREs zu, überwachen ihre Leistung und erstellen Verfahren zur Behandlung von Incidents und zur Entwicklung von Lösungen. -Manager fördern die Resilienz über alle Systeme und DevOps-Workflows hinweg.	Beantworter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender (Fortsetzung)

Anwender	Beschreibung	Enthält Rollen
	Manager können im Kontext ihrer Teams folgende Aktionen ausführen: • Teams, Rufbereitschaftszeitpläne und Services definieren und einrichten. • Benutzer wie Beantworter und Manager für die Teams hinzufügen und löschen, denen sie angehören. • Integrationen hinzufügen oder verwalten. • Erstellen Sie Integrationen mit APM-Tools (Application Performance Monitoring) für Anwendungen. • Zuverlässigkeitsmetriken einrichten und verwalten. • Fehlerbudgetrichtlinien einrichten und verwalten.	
Beantworter [srm_responder]	Ein Service Reliability Engineer (SRE), der SRM zur Ausführung alltäglicher Aufgaben verwendet. Beantworter sind die Personen, die Rufbereitschaft haben und Incidents diagnostizieren und beheben. Beantworter können nur auf Konfigurationen zugreifen, denen sie angehören. Sie können nur auf die Warnungen oder Incidents zugreifen, für die sie Berechtigungen haben. SREs können im Kontext ihrer Teams folgende Aktionen ausführen: • Services, Teams und Integrationen einrichten. • Bestätigen Sie die Rufbereitschaftszeitpläne. • Verwalten Sie Incident- und Warnungsdatensätze. • Die von ihnen erstellten Teams aktualisieren. • Weitere Beantworter hinzufügen • Erstellen Sie Integrationen mit APM-Tools (Application Performance Monitoring) für Anwendungen.	Erbt 17 Rollen, darunter die folgenden: • cmdb_read • sn_sow.sow_user • sn_sow_srm.srm_responder • workspace_user • slo_operator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender (Fortsetzung)

Anwender	Beschreibung	Enthält Rollen
	• Zuverlässigkeitsmetriken einrichten und verwalten. • Fehlerbudgetaktionen einrichten und verwalten.	

Weitere Informationen finden Sie unter SRM Rollen und Zuständigkeiten.

SRM – Workflow

1. Produktteams in IT oder Branchen liefern kontinuierlich neue technische und Anwendungsservices. Beispiel: Neues Kundenabrechnungsportal.

2. Zusammen mit SLO-Managementkönnen Teams Services registrieren und Servicelevel-Ziele (SLOs) definieren, die ihnen beim Erreichen von Geschäftsergebnissen helfen. Beispiel: 95 % monatliche Verfügbarkeit für das Abrechnungsportal.

3. Überwachungsintegrationen werden von den -Teams eingerichtet, um die Echtzeitintegrität dieser Services zu erfassen. Beispiel: Cloud Observability.

4. Die Überwachung erstellt Servicelevel-Indikatoren (SLIs), die sich auf Warnungen auswirken, wenn Services unterdurchschnittlich abschneiden. Automatisierungsgruppen und -bereicherungen Beispiel: Die Latenz des Abrechnungsportals überschreitet 7 s.

5. Wenn die Warnungen auf einen Ausfall oder eine Verschlechterung hinweisen, die sich auf den Kunden auswirkt, werden Incidents erstellt, und die entsprechenden Teamressourcen werden durch Rufbereitschaftsbenachrichtigungen benachrichtigt. Beispiel: Ein SRE-Team für Abrechnungen wird telefonisch über ein Latenzproblem im Abrechnungsportal benachrichtigt.

6. Nachdem Teams gemeinsam Incidents diagnostizieren und beheben, identifizieren sie Aktionselemente zur Verbesserung der Resilienz des Systems. Beispiel: Das Abrechnungsteam beschließt, zusätzliche Webserverkapazität hinzuzufügen.

7. Das Management überprüft kontinuierlich die SLO-Leistung, hilft, Changes zu verhindern, wenn das Fehlerbudget ausgeschöpft ist, und priorisiert Verbesserungsinitiativen für unterdurchschnittliche Services.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SRM – Vorteile

Vorteil	Funktion	Anwender
Teambasierte Experience	Mit SRM-Teams arbeiten	SRM-Administratoren, Manager und Beantworter
Serviceregistrierung	Mit SRM-Services arbeiten	SRM-Administratoren, Manager und Beantworter
Vorgefertigte Integrationen	Mit SRM-Integrationen arbeiten	SRM-Administratoren, Manager und Beantworter
Zum Messen der Serviceintegrität	Mit Zuverlässigkeitsmetriken arbeiten	SRM-Administratoren, Manager und Beantworter
Bereitschaftsabdeckung	Eigene SRM-Rufbereitschaftspläne erstellen	SRM-Administratoren, Manager und Beantworter
Korrigieren Sie Warnungen und Incidents mit hohem Schweregrad	Mit SRM-Zuverlässigkeitsaufgaben arbeiten	SRM-Administratoren, Manager und Beantworter

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von SRM finden Sie unter:

- Service Reliability Management konfigurieren
- Service Reliability Management verwenden
- Service Reliability Management – Referenz

Erste Schritte mit Service Reliability Management

Service Reliability Management (SRM) beschleunigt Ihren Weg zur Anzeige der Serviceintegrität im Kontext von Servicelevel-Zielen und Lösung von Incidents. Die Anwendung unterstützt IT-Betriebs- und DevOps-Teams dabei, ihr Versprechen von Agilität, Leistung und Betriebszeit einzuhalten.

Machen Sie sich mit SRM vertraut, um die verschiedenen Abschnitte der Anwenderoberfläche SRM zu verstehen.

Weitere Informationen zu Rollen finden Sie unter SRM Rollen und Zuständigkeiten.

Grundlegende SRM-Aufgaben

Schritt	Beschreibung	Referenz
Richten Sie Teams und Services ein	Setupleitfäden für die Seiten Homepage, Servicesund Teams zeigen, wie Sie ein Team oder einen Service zu SRM hinzufügen.	SRM-Teams hinzufügen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritt	Beschreibung	Referenz
Besuchen Sie, und erfahren Sie mehr über Ihre Homepage	Auf der Homepage finden Sie die Dinge, die für Sie am wichtigsten sind. Zum Beispiel die Services mit kritischen Warnungen und Incidents sowie Arbeiten, die Ihnen und Ihrem Team zugewiesen sind.	Homepage von SRM
Erfahren Sie, wie Sie navigieren SRM	Machen Sie sich mit den verschiedenen Abschnitten und Elementen der SRM -Schnittstelle vertraut. Die Abschnitte und Elemente werden in der gesamten Dokumentation verwendet.	Anwenderoberfläche von SRM

SRM hilft Ihnen, wenn Sie Teams, Services und Integrationen erstellen und verwalten müssen.

SRM-Aufgaben

Schritt	Beschreibung	Siehe
Anwendungen oder technische Services in SRM verwalten	Definieren Sie die grundlegenden Aufgaben und Parameter, die den Service ausmachen und angeben, wie das Serviceverhalten aussehen soll.	Services zu SRM hinzufügen
SRM-Team einrichten	Richten Sie ein Team ein. Teams sind für die Probleme verantwortlich, die in ihren zugehörigen Services auftreten.	SRM-Teams hinzufügen
Richten Sie Rufbereitschaftszeitpläne und Eskalationsrichtlinien ein	Erstellen Sie einen Rufbereitschaftszeitplan für Ihr Team, um sicherzustellen, dass es für die Lösung von Problemen verfügbar ist. Sie können eine Eskalationsrichtlinie einrichten, um sicherzustellen, dass mindestens ein Teammitglied an der Reaktion auf Incidents beteiligt ist.	Eigene SRM-Rufbereitschaftspläne erstellen
Servicebeziehungen konfigurieren	Verwenden Sie eine Zuordnungs-Canvas, um Services hinzuzufügen, zu konfigurieren und anzuordnen. Sie können untergeordnete Services hinzufügen, die von übergeordneten Services abhängig sind.	Auswirkung des untergeordneten Services auf den übergeordneten Service anzeigen
Services mit Überwachungstools von Drittanbietern integrieren	Richten Sie eine Drittanbieterintegration wie Datadog oder ServiceNow Cloud Observabilitymit SRM ein, damit Warnungen für Ihre Teams in SRMverfügbar sind.	Integrationen zu SRM hinzufügen
SLOs, SLIs und Fehlerbudgets für Services festlegen	Legen Sie mit Zielen fest, wie gut Ihr Service laufen soll. Geben Sie außerdem an, wie lange ein	Servicelevel-Zielmanagement

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SRM-Aufgaben (Fortsetzung)

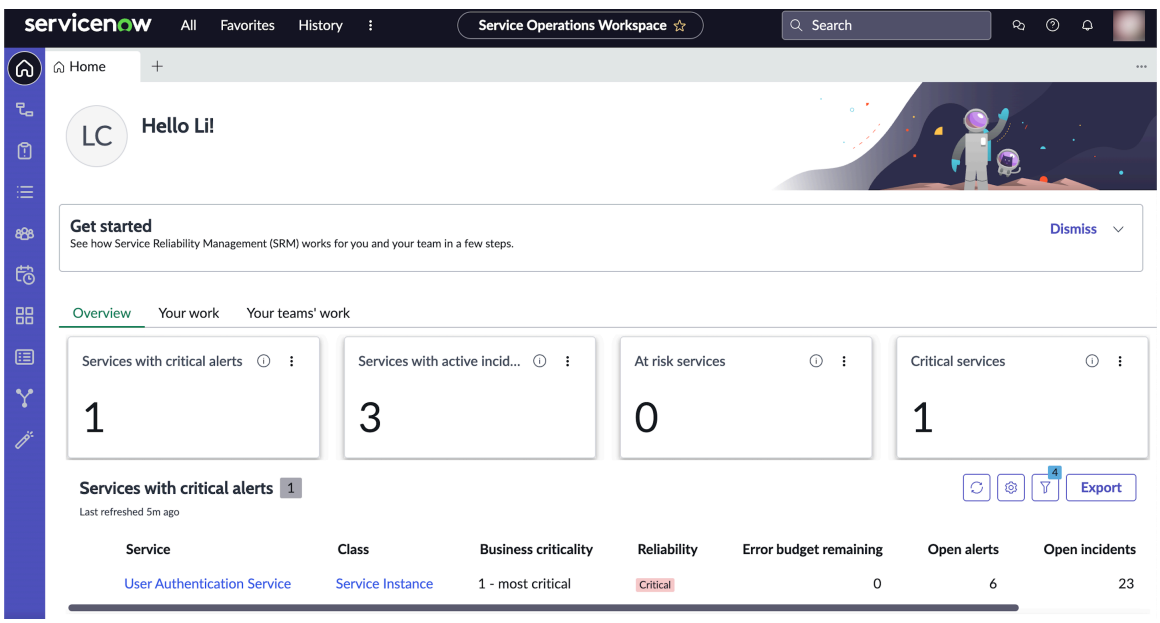
Schritt	Beschreibung	Siehe
	technisches System höchstens ausfallen darf, ohne dass dies vertragliche Konsequenzen hat.	
Warnungsautomatisierungen einrichten **Hinweis:** Diese Funktionalität ist nur verfügbar, wenn Sie die Anwendung Warnungsautomatisierungen installiert haben.	Mit Warnungsautomatisierungen können Sie Warnungsbedingungen definieren. Richten Sie für jedes APM-Tool Warnungsregeln ein, um die Bedingungen zu definieren, unter denen das APM-Tool Benachrichtigungen an SRM senden soll.	Die Anwendung Warnungsautomatisierungen ist über ServiceNow Storeverfügbar.

Homepage von SRM

Die Homepage Service Reliability Management (SRM) bietet relevante Informationen über Ihre Arbeit, Services, Zeitpläne, Wartungserinnerungen und Teams. Zeigen Sie die Homepage an, indem Sie zu navigieren **Service Reliability Management**.

Service Reliability Management Abschnitte der Homepage

Wählen Sie im Arbeitsbereich **Homepage** ( ), um die Homepage anzuzeigen.



Wenn Sie Rufbereitschaft haben, wird Ihr Zeitplan aufgelistet.

Abschnitte der Homepage

Erste Schritte	Enthält Setup-Aufgaben für Teams und Services und deren Fortschritt. Weitere Informationen zum Abschließen des Setups finden Sie unter Services zu SRM hinzufügen und SRM-Servicedetails bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitte der Homepage (Fortsetzung)

	Hinweis: Sie können jeden Abschnitt überspringen und später zurückkehren. Der Fortschritt wird anhand der von Ihnen durchgeführten Aktionen in Prozent angegeben. Solange ein Schritt unvollständig bleibt, sind die Kacheln verfügbar. Sie können sie jederzeit minimieren, indem Sie das Nach oben-Symbol wählen. Verwenden Sie **Verwerfen**, um es von Ihrer Seite zu entfernen. Die Prüflistenstatus lauten wie folgt: • **Keine**: Es wurde keine Aktion ausgeführt. • **Fertig**: Alle erforderlichen Felder wurden hinzugefügt. • **Ausstehend**: Einige Felder oder Genehmigungen müssen noch hinzugefügt oder gewährt werden.
Übersicht	Enthält eine Übersicht über alle Servicewarnungen, Incidents, gefährdeten und kritischen Services. **Services mit kritischen Warnungen** ist die Standardlistenansicht. Wählen Sie eine Karte aus, um die Listenansicht für diesen Bereich anzuzeigen.
Ihre Arbeit	Enthält Ihnen zugewiesene Incidents und Warnungen. Wählen Sie eine Karte aus, um die Listenansicht für diesen Bereich anzuzeigen.
Die Arbeit Ihres Teams	Enthält Incidents und Warnungen, die Ihrem Team zugewiesen sind. Wählen Sie eine Karte aus, um die Listenansicht für diesen Bereich anzuzeigen.

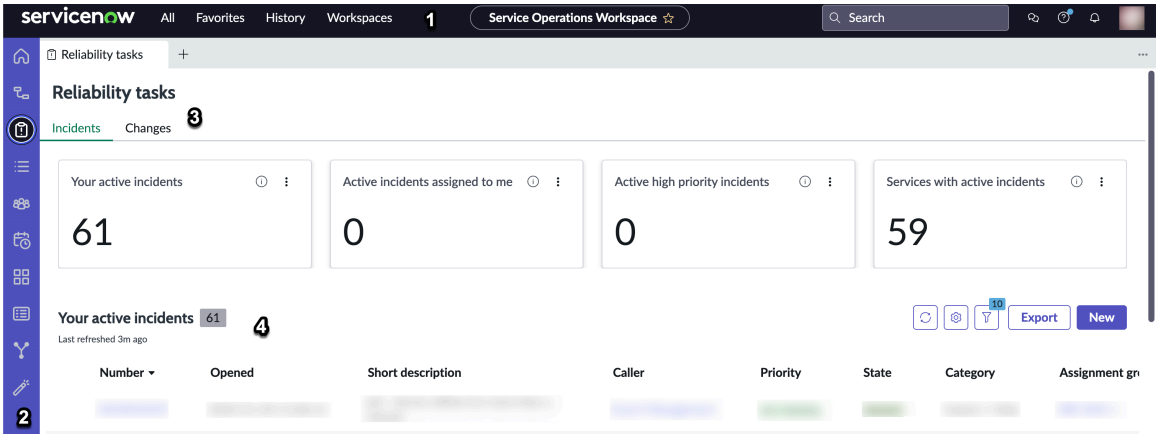
Anwenderoberfläche von SRM

Die verschiedenen Komponenten der Schnittstelle Service Reliability Management (SRM) bieten einfachen Zugriff auf verschiedene Funktionen. Die angezeigten Features und Funktionen hängen von Ihrer Rolle und Ihren Berechtigungen ab.

Die Schnittstelle SRM verfügt über die folgenden verschiedenen Abschnitte:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitte der Schnittstelle



Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken. Abhängig von Ihrer Rolle werden in der primären Navigation möglicherweise andere Symbole angezeigt.

Wenn die SOW-Homepage angezeigt wird, wählen Sie ein SRM-Symbol, um SRM-spezifische Informationen anzuzeigen.

Abschnitte	Beschreibung
1: Header	Ein Homepage für das Logo Ihrer Organisation und Dienstprogramme auf Systemebene, das überall in der Anwenderoberfläche vorhanden ist. • Alle • Favoriten • Verlauf • Arbeitsbereiche • Aktueller Arbeitsbereich • Suchen • Sidebar-Diskussionen • Hilfe • Benachrichtigungen • Profilsymbol: Stellt Ihr Profil dar
2: Primäre Navigation	Einfacher Zugriff auf bestimmte Seiten in SRM. Die primäre Navigation verwendet Symbole, einschließlich Symbolen für Services, Zuverlässigkeitsaufgaben, Teamsund Zeitpläne. Verwenden Sie Tooltips, um sie zu identifizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitte	Beschreibung
	Hinweis: Das Warnungsautomatisierungs-Symbol ist nur verfügbar, wenn Sie die Anwendung Warnungsautomatisierung aus dem ServiceNow Storeinstalliert haben.
3: Inhaltsheader	Registerkarten, Karten oder Schaltflächen, mit denen Aufgaben auf Produktebene ausgeführt werden können. Die Elemente im Inhaltsheader unterscheiden sich von einer Seite zur anderen.
4: Inhaltsbereich	Canvas oder der Hauptbereich, in dem Sie Informationen sammeln, Metriken lesen und Aufgaben ausführen können. **Hinweis:** Wenn Sie den Seitenbereich in Formularen standardmäßig minimieren möchten, navigieren Sie zu **Einstellungen** > **Arbeitsbereich** und deaktivieren Sie die Option **Sidebar anzeigen**. Mit dieser Aktion wird im gesamten Service Operations-Arbeitsbereichdeaktiviert, nicht nur in SRM.

Suche, Filter, Listen, Formulare und Leitfäden

Übersicht über die zusätzlichen Elemente auf der Anwenderoberfläche Service Reliability Management (SRM), mit denen Sie Elemente suchen, verfügbare Formulare und Listen anzeigen und Setup-Prozesse befolgen können.

Tabellenlistenansicht

Zeigen Sie Services und Incidents als Liste an.

- Suchen Sie mithilfe des Headertextfelds.
- Sortieren Sie Elemente mithilfe der Listenspalten.
- Filtern Sie Listenergebnisse mithilfe der Listenspalten.

Hinweis: Zeigen Sie die aktiven Filter über das Filtersymbol im Header der Listenansicht an.

Jede Ansicht enthält eigene spezifische Elemente. Weitere Informationen finden Sie auf diesen Seiten.

Formularansicht

Wenn Sie einen der Tabellendatensätze aus der Listenansicht öffnen, werden die Details des Datensatzes als Formular angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jede Ansicht enthält eigene spezifische Elemente. Weitere Informationen finden Sie auf diesen Seiten.

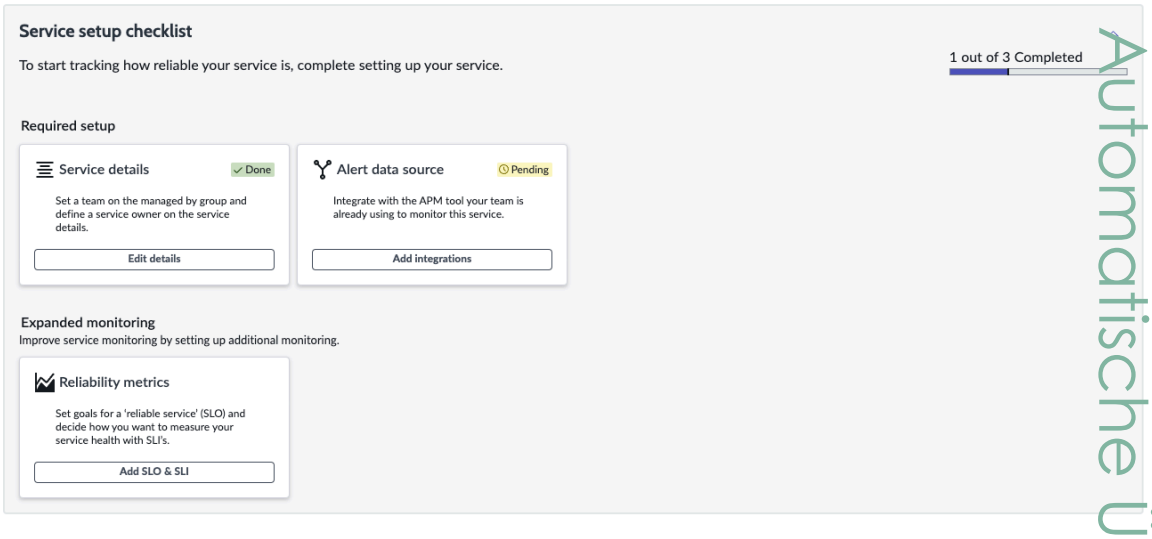
Hinweis: Ausgegraute Felder können nicht geändert werden.

Der Bereich Anhänge ist häufig standardmäßig sichtbar. Um ihn auszublenden, wählen Sie das Anhangsymbol .

Setup-Prüflisten

Verwenden Sie die Setup-Prüflisten, um den Prozess zu visualisieren, den Sie durchlaufen, um Ihre Ziele zu erreichen. Jeder Schritt wird hervorgehoben, wenn Sie ihn abschließen.

Prüflistenbeispiel für Service-Setup



Automatische Übersetzung

Listeninformationen in eine Datei exportieren

Sie können Live-Informationen in eine Datei in Service Reliability Management (SRM) exportieren.

Vorbereitungen

Hinweis: Die Massenauswahl hat keine Auswirkungen auf Exporte. Der Export enthält alle Datensätze, die den aktuellen Filterkriterien entsprechen. Die Auswahl, die Sie in der Listenansicht treffen, berücksichtigt es nicht.

Erforderliche Rolle: srm_admin, srm_manager oder srm_responder

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie die Listenansicht in einem beliebigen Zielseitenabschnitt in SRM über die **Exportieren-Schaltfläche** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Legen Sie die zu verwendenden Filter fest, und wählen Sie sie aus dem Menü „Filter“ oder dem Menü „Weitere Aktionen“ in den Listenspalten.

Hinweis:

Die Schaltfläche „Exportieren“ ist nur verfügbar, wenn in der Listenansicht Datensätze vorhanden sind.

Der Export enthält alle Listendaten, die Ihren gefilterten/gruppierten Listen entsprechen.

4. Wählen Sie **Exportieren**.
Treffen Sie im Popup-Fenster folgende Auswahl:
   - Dateityp:
     - Excel
     - CSV
     - JSON
     - PDF
   - Liefertyp:
     - Herunterladen
     - E-Mail: Geben Sie eine E-Mail-Adresse an.

Für **E-Mail**: Sobald der Export abgeschlossen ist, wird oben im Bildschirm eine Erfolgsmeldung mit Ihrer E-Mail-Adresse angezeigt. Das ist nützlich für größere Dateien, da der Export je nach Größe der Datei einige Zeit dauern kann. Das E-Mail-Programm wird im Hintergrund ausgeführt, sodass Sie während des Wartens etwas anderes tun können.

Beim **Herunterladen**: Der Export wird im Popup-Fenster gestartet, und die Datei wird in Ihrem Download-Verzeichnis angezeigt. Je nach Größe der Datei kann dies einige Zeit dauern. Sie können sie in jeder Anwendung öffnen, die das Dateiformat unterstützt.

SRM-Tags manuell erstellen

Fügen Sie Tags hinzu, um Daten zu klassifizieren und zu kategorisieren und ihnen Kontext hinzuzufügen. Service Reliability Management (SRM) importiert Tags und hängt sie an Services, Warnungen und Incidents an. Sie können Tags auch manuell erstellen.

Vorbereitungen

Erforderliche Rolle: srm_admin, srm_manager oder srm_responder

Warum und wann dieser Vorgang ausgeführt wird

Es gibt zwei Möglichkeiten, wie Tags in das System gelangen und an eine Warnung oder einen Incident angehängt werden. Die erste ist automatisiert, die andere hingegen manuell.

- Importiert aus einer Drittanbieterintegration wie Datadog.
- Über das Tag-Symbol im Header eines Service, einer Warnung oder eines incident.
- Hinzugefügt mithilfe der Aktion **Modify field values (Feldwerte ändern)** in einer Automatisierungsregel.

Diese Aufgabe beschreibt, wie Sie in SRMTags zu Services und Incidents hinzufügen. Informationen zum Verwalten von Warnungen finden Sie unter Warnungen in Service Operations-Arbeitsbereich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation **Services** oder **Zuverlässigkeitsaufgaben**aus.
3. Öffnen Sie einen Service oder Incident.
4. Wählen Sie im Header das **Tag** -Symbol , um Tags hinzuzufügen.
5. Geben Sie Ihr Tag in das Popup-Fenster ein.
   Ihr Tag wird gespeichert und unter dem Feld „Tag hinzufügen“ neben allen vorhandenen Tags angezeigt.
6. Wählen Sie eine beliebige Stelle im Formular aus, um das Popup-Fenster zu schließen.

Hinweis:

Tags werden auch unter der Beschreibung in der Incident-Listenansicht angezeigt.

SRM Incidents

Auf der Registerkarte Incidents können Sie Incidents nachverfolgen und gemeinsam daran arbeiten, damit Sie und Ihre Teams Probleme effizient lösen können.

Die Registerkarte Incidents wird auf der Seite Service Reliability Management (SRM) Zuverlässigkeitsaufgaben angezeigt. Der obere Header enthält Beschreibungsinformationen, Tags, Prioritätsinformationen, Status, Service und Zuweisungsgruppe.

Hinweis: Tags werden aus Drittanbieterintegrationen importiert und an Warnungen angehängt. Sie können jedoch auch Tags erstellen, um Daten zu kategorisieren und die Systemlogik über das Tag-Symbol zu steuern. Weitere Informationen zum Erstellen und Anzeigen von Tags finden Sie unter SRM-Tags manuell erstellen.

Wenn Sie einen Incident auswählen, gelangen Sie zu einer Übersicht. Dieser Abschnitt enthält drei Inhaltsbereiche: Zusammenfassung, Aktivitätund Empfohlene Aktionen.

Hinweis: Wenn ein bearbeitbares Feld aktualisiert wird, werden Benachrichtigungen basierend auf den Benachrichtigungseinstellungen des Anwenders gesendet.

Die Impact-Zusammenfassung enthält die folgenden Informationen:

Betroffene CIs

Feld	Beschreibung
Konfigurationselement	Name des Konfigurationselements, das diesem Incident zugeordnet ist, und der zugehörige Link.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betroffene Services

Feld	Beschreibung
Konfigurationselement	Name des Konfigurationselements, das diesem Incident zugeordnet ist, und der zugehörige Link.
Verwaltet von	Für den Incident verantwortliches Team.
Eigentum von	Incident-Besitzer.
Genehmigungsgruppe	Team, das für Genehmigungen verantwortlich ist.
Standort	Geografischer Standort des Incident, falls definiert.
Betriebsstatus	Status des Incident.
Manuell hinzugefügt.	Gibt an, ob dieser Incident manuell hinzugefügt wurde oder das Ergebnis einer Fehlerbudgetrichtlinie ist.

Details

Enthält Incident-Details und zugehörige Warnungen

Feld	Beschreibung
Kurzbeschreibung	Eine kurze Beschreibung des Incident.
Beschreibung	Detaillierte Beschreibung des Incident.
Nummer	Bezeichner des Incident.
Auswirkung	Die Auswirkung ist ein Messwert für den Effekt, den ein Incident auf Geschäftsprozesse hat. Die Auswahlmöglichkeiten lauten wie folgt: • 1 - Hoch • 2 – Mittel • 3 - Niedrig
Zuweisungsgruppe	Team, das dem Incident zugewiesen ist.
Priorität	Die Priorität beruht auf der **Auswirkung** und der **Dringlichkeit**. Sie bestimmt, wie schnell der Incident behandelt werden sollte. Die Auswahlmöglichkeiten lauten wie folgt: • Hohe Auswirkung = Kritische Priorität • Mittlere Auswirkung = Hohe Priorität • Niedrige Auswirkung = Moderat **Hinweis:** Beachten Sie dazu die Regeln für priorisierte Datensuchen unten.
Kategorie	Kategorie des Incident. Die Auswahlmöglichkeiten lauten wie folgt: • Anfrage/Hilfe • Software

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details

Enthält Incident-Details und zugehörige Warnungen

(Fortsetzung)

Feld	Beschreibung
	• Hardware • Netzwerk • Datenbank
Dringlichkeit	Die Dringlichkeit ist ein Messwert dafür, wie lange die Lösung hinausgeschoben werden kann, bis ein Incident maßgebliche Geschäftsauswirkungen hat.
Service	Betroffener Service, der dem Incident zugeordnet ist. Sie können dieses Feld über ein Listenmenü bearbeiten. **Hinweis:** Wenn Sie einen Service festlegen und dieser Service über ein zugewiesenes Team verfügt, wird das diesem Service zugewiesene Team dem Incident automatisch zugewiesen.
Schweregrad	Importierter Schweregrad für den Incident. Werte P1–P5.
Konfigurationselement	Asset, das dem Incident zugeordnet ist.
Zugewiesen an	Einzelperson, die für die Lösung des Incident verantwortlich ist.
Status	Status des Incident. Der Status ändert sich und verfolgt Incidents durch mehrere Lösungsphasen. Die Auswahlmöglichkeiten lauten wie folgt: • Neu • In Bearbeitung • Warten • Gelöst • Abgebrochen
Beobachtungsliste	Einzelpersonen, die an dem Incident interessiert sind. Sie erhalten Benachrichtigungen entsprechend ihren Einstellungen.
Lösungscode	Code, der der Lösung zugeordnet ist. Die Auswahlmöglichkeiten lauten wie folgt: • Keine (Standard) • Duplikat • Known Error • Keine Lösung bereitgestellt • Von Anrufer gelöst • Gelöst durch Change • Gelöst durch Problem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details

Enthält Incident-Details und zugehörige Warnungen

(Fortsetzung)

Feld	Beschreibung
	• Gelöst durch Anforderung • Lösung bereitgestellt
Lösungsnotizen	Detaillierte Informationen zur Lösung. Lösungshinweise werden in der Zeitleiste **Aktivität** veröffentlicht.

Hinweis: Die Priorität wird anhand der folgenden Beispielregeln für die Datensuche berechnet:

Regeln für Datensuche mit Priorität

Auswirkung	Dringlichkeit	Priorität
1 – Hoch	1 – Hoch	1 - Kritisch
1 – Hoch	2 – Mittel	2 – Hoch
1 – Hoch	3 – Niedrig	3 – Mittel
2 – Mittel	1 – Hoch	2 – Hoch
2 – Mittel	2 – Mittel	3 – Mittel
2 – Mittel	3 – Niedrig	4 – Niedrig
3 – Niedrig	1 – Hoch	3 – Mittel
3 – Niedrig	2 – Mittel	4 – Niedrig
3 – Niedrig	3 – Niedrig	5 - In Planung

Durch das Löschen eines Service werden dessen Integrationen, Warnungen, Incidents und Automatisierungen entfernt. Das Löschen eines Service kann nicht wiederhergestellt werden. Erwägen Sie daher, stattdessen den Service zu deaktivieren.

Die Registerkarte Zugehörige Datensätze enthält alle Warnungen, die diesem Incident zugeordnet sind.

Hinweis: Alle Feldwerte werden aus den zugehörigen Datensätzen importiert und können nicht in SRMbearbeitet werden.

Untergeordnete Incidents

Feld	Beschreibung
Nummer	Bezeichner des zugehörigen Incidents.
Kurzbeschreibung	Kurze Beschreibung des zugehörigen Incidents.
Priorität	Priorität des zugehörigen Incidents.
Status	Status des zugehörigen Incidents.
Zugewiesen an	Teammitglied, das dem zugehörigen Incident zugewiesen ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Untergeordnete Incidents (Fortsetzung)

Feld	Beschreibung
Zuweisungsgruppe	Team, das dem zugehörigen Incident zugewiesen ist.
Service	Service, der dem zugehörigen Incident zugeordnet ist.

Warnungen

Feld	Beschreibung
Nummer	Bezeichner der zugehörigen Warnung.
Schweregrad	Schweregrad der zugehörigen Warnung.
Kurzbeschreibung	Kurze Beschreibung der zugehörigen Warnung.
Bestätigt	Gibt an, ob die zugehörige Warnung bestätigt wurde oder nicht.
Zugewiesen an	Teammitglied, das der zugehörigen Warnung zugewiesen ist.
Konfigurationselement	Asset, das der zugehörigen Warnung zugeordnet ist.
Übergeordnet	Primäre Warnung, die der zugehörigen Warnung zugeordnet ist.

Letzte wirkungsvolle Changes

Feld	Beschreibung
Nummer	Bezeichner für die zugehörigen Changes, die diesem Incident zugeordnet sind.
Kurzbeschreibung	Kurze Beschreibung der zugehörigen Changes, die diesem Incident zugeordnet sind.
Typ	Typ der letzten Changes, die diesem Incident zugeordnet sind.
Status	Status der letzten Changes, die diesem Incident zugeordnet sind.
Geplantes Startdatum	Datum und Uhrzeit, bis zu dem die mit diesem Incident verknüpften Changes gelten.
Geplantes Enddatum	Datum und Uhrzeit, bis zu dem die mit diesem Incident verknüpften Changes gelten.
Zugewiesen an	Teammitglied, das für die Change-Anforderung im Zusammenhang mit diesem Incident verantwortlich ist.

Change-Anforderungen

Feld	Beschreibung
Kurzbeschreibung	Kurze Beschreibung der Change-Anforderung, die diesem Incident zugeordnet ist.
Typ	Typ der Change-Anforderung, die diesem Incident zugeordnet ist.
Status	Status der Change-Anforderung, die diesem Incident zugeordnet ist.
Geplantes Startdatum	Datum und Uhrzeit des Beginns der Arbeiten für die Change-Anforderung, die diesem Incident zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Change-Anforderungen (Fortsetzung)

Feld	Beschreibung
Geplantes Enddatum	Datum und Uhrzeit der Beendigung der Arbeiten für diese Change-Anforderung, die diesem Incident zugeordnet ist.
Zugewiesen an	Teammitglied, das für die Change-Anforderung im Zusammenhang mit diesem Incident verantwortlich ist.

Registerkarte „Postmortem“

Über den Postmortem-Besitzer:

- Wenn in der Liste der Beantworter des Zusammenarbeitsbereichs bereits ein Schreiber ausgewählt wurde, wird er automatisch zum Besitzer.
- Wenn mehr als ein Schreiber vorhanden ist, wird der zuerst zugewiesene ausgewählt. Andernfalls können Sie einen Besitzer aus dem Listenmenü auswählen.
- Wenn ein neuer Schreiber hinzugefügt oder eine vorhandene Benutzerpersona zum Schreiber gemacht wird, wird dieser Benutzer zum Besitzer.
- Wenn Sie einen Besitzer manuell entfernen, wird nicht automatisch ein neuer Besitzer ausgewählt.

Verwenden Sie die Drag-and-Drop-Funktion, um Postmortem-Abschnitte zu bearbeiten. Sie können Abschnitte aus PDFs ausschließen, Abschnitte löschen oder Abschnitte neu anordnen.

Um neue Abschnitte hinzuzufügen, wählen Sie das **Hinzufügen** -Symbol .
Bereich **Verfassen**

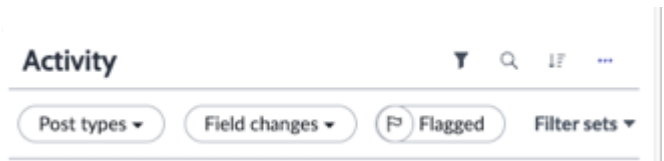
Arbeitsnotizen werden der Aktivitätszeitleiste automatisch hinzugefügt. Sichtbar für Beantworter und höhere Rollen. Fügen Sie Kommentare mithilfe des Textfelds **Verfassen** hinzu.

Kommentare werden der Aktivitätszeitleiste automatisch hinzugefügt. Für alle in SRM sichtbar.

Bereich **Aktivität**

Strom, der alle Systemaktivitäten und Lösungshinweise enthält. Sie können alle Posts mithilfe der Headersymbole filtern, sortieren, erweitern oder reduzieren.

Hinweis: Die Filteroption beinhaltet **Beitragstypen**, **Feldänderungen** und **Filtersätze**. Alle Auswahlmöglichkeiten sind standardmäßig ausgewählt. Es sind entweder alle oder keine Einträge gekennzeichnet.



Bereich **Aktionen**

Hinweis:

Die Bereiche **Benachrichtigungen**, **Agent Assist**, **Experten in Rufbereitschaft**und **E-Mail-Vorlagen** werden derzeit in SRMnicht unterstützt.

Abschnitt **Anhänge**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Öffnen Sie den Abschnitt **„Anhänge** “ mit dem Symbol „Anhang“ .

Im Bereich **Anhänge** können Sie zunächst Ihre lokale Festplatte nach Dateien **Durchsuchen**.

Sobald Sie Anhänge hinzugefügt haben, haben Sie folgende Möglichkeiten:

- Suchen Sie anhand des Namens oder der Erweiterung nach einem Anhang.

  Hinweis: Für eine Suche müssen mindestens zwei Anhänge vorhanden sein.

- Laden Sie über das Symbol ( ) einen neuen Anhang hoch.
- Über das Symbol „Weitere Aktionen“ (“) können Sie Anhänge herunterladen, entfernen oder umbenennen.

Abschnitt **Vorlage**

Öffnen Sie den Bereich **Vorlage** mit dem Vorlagensymbol .

Hinweis: Vorhandene Vorlagen werden angezeigt, das Erstellen von Vorlagen ist jedoch in SRMnicht möglich.

Bereich **Zusammenarbeit**

Zeigt die verfügbaren Zoom-Meetings, Microsoft Teams oder Slack-Kanäle zum Starten oder Beitreten an.

So starten Sie ein Zoom-Meeting oder nehmen daran teil:

Hinweis: Die Zoom-Integration und die erkannten IDs müssen in Ihrer Instanz aktiv sein. Wenn der Startkanal nicht verfügbar ist, wenden Sie sich an Ihren Administrator.

1. Wählen Sie **Start Zoom** (Zoom starten) aus.
   - Ein Besprechungs-Popup wird angezeigt.
   - Fügen Sie Teilnehmer hinzu.
   - Wählen Sie **Besprechung erstellen** aus.
   - Das Meeting wird erstellt, Einladungen werden gesendet und Sie nehmen am Meeting teil.

     Hinweis: Alle beim Starten eines Meetings gefundenen Probleme werden in einer Bannernachricht angezeigt.

2. Wählen Sie **Meeting beitreten** aus.
   - **Melden** Sie sich bei Ihrem Zoom-Konto an.
   - Damit treten Sie dem Zoom-Meeting bei.

1. Wählen Sie **Start Channel** (Kanal starten) aus.
   - Melden Sie sich bei Ihrem Microsoft Teams-Konto an.
   - Wählen Sie **Erstellen** aus. Sie werden zur Microsoft Teams-Anwendung weitergeleitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zurück in der Spalte „Zusammenarbeit“ wird die Schaltfläche **Kanal beitreten** aktiviert.

  Hinweis: Alle beim Beitritt zu einem Kanal gefundenen Probleme werden in einer Bannernachricht angezeigt.

2. Wählen Sie im Bereich „Zusammenarbeit“ in SRM die Option **Kanal beitreten** aus.
3. Melden Sie sich bei Ihrem Microsoft Teams-Konto an.

   Sie treten dem Kanal in Microsoft Teams bei.

Starten Sie einen Slack-Kanal oder nehmen Sie daran teil:

Hinweis: Die Slack-Integration und die erkannten IDs müssen in Ihrer Instanz aktiv sein. Wenn der Startkanal nicht verfügbar ist, wenden Sie sich an Ihren Administrator.

1. Wählen Sie **Start Slack** (Slack starten) aus.

   - Fügen Sie im Popup-Fenster „Create a Slack channel“ (Slack-Kanal erstellen) Teilnehmer hinzu.
   - Wählen Sie **Erstellen** aus. Sie werden zur Slack-Anwendung weitergeleitet.
   - Zurück in der Spalte „Zusammenarbeit“ wird die Schaltfläche **Join Slack** (Slack beitreten) aktiviert.

     Hinweis: Alle beim Starten eines Kanals gefundenen Probleme werden in einer Bannernachricht angezeigt.

2. Wählen Sie im Slack-Anwendungsfenster **Kanal beitreten** aus.
3. Melden Sie sich bei Ihrem Slack-Konto an.

   Sie treten dem Slack-Kanal bei.

Setup von Service Operations-Arbeitsbereich (SOW) für Service Reliability Management

Installieren und konfigurieren Sie Service Reliability Management im Service Operations-Arbeitsbereich Admin Center, damit SRM-Administratoren, -Manager und -Beantworter effizient für Servicezuverlässigkeit sorgen können.

Sie können Installieren Sie die Anwendung Service Reliability Management aus dem Admin Center oder ServiceNow Store über das Service Operations-Arbeitsbereich Admin Center.

Hinweis: Die App Datenvisualisierungen v24.1.8 ist ebenfalls erforderlich. Informationen zum Installieren der App finden Sie unter Datenvisualisierungen im ServiceNow Store.

Nach der Installation wird durch die Konfiguration von SRM im Service Operations-Arbeitsbereich Admin Center der SRM-Arbeitsbereich mit Optionen und Aktionen eingerichtet.

Mit den Service Reliability Management-Menüs im Service Operations-Arbeitsbereich Admin Center haben Sie folgende Möglichkeiten:

- Administratoren zu Service Reliability Management zuweisen.
- Importieren Sie Services zur Verwendung in Service Reliability Management.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Genehmigungsprozess zur Aufnahme von Services in Service Reliability Management hinzufügen.
- Genehmigungsprozess zur Aufnahme von Teams in SRM hinzufügen
- Greifen Sie auf das Anforderungskatalogelement für Benutzer zu, und veröffentlichen Sie es.
- Fehlerbudgetaktionen bei Verletzung eines SRM-SLO konfigurieren.

Warnungsautomatisierungen sind Bedingungsauslöser, die auf Basis des Inhalts einer Warnung automatisch Antwortreaktionen ausführen. Diese Funktionalität ist für SRM auf Anforderung in der Anwendung Warnungsautomatisierungen im ServiceNow Store verfügbar.

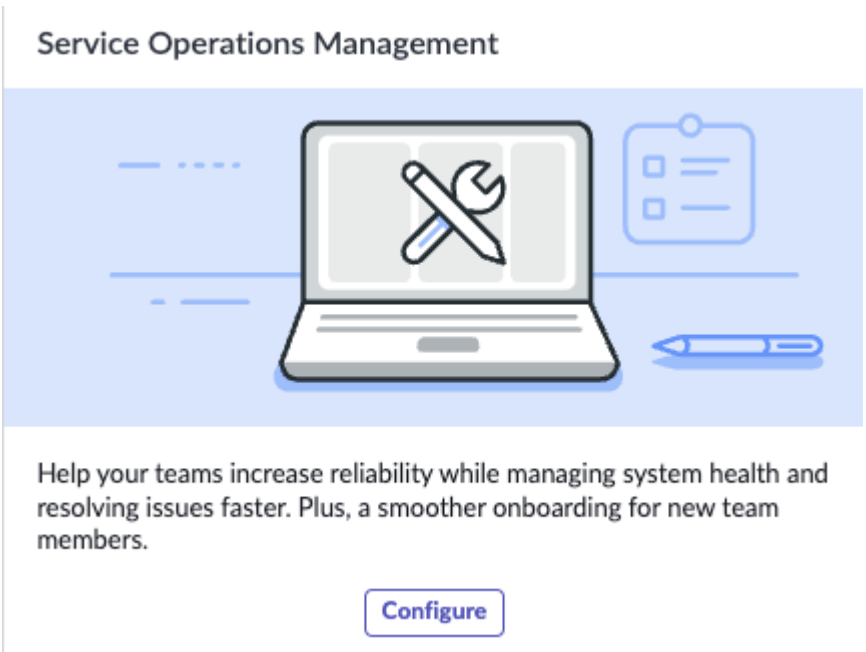
Service Reliability Management konfigurieren

Die Konfiguration von Service Reliability Management umfasst die Installation von ServiceNow Store oder aus dem Admin Center. Sie können Administratoren zuweisen und Services und Teams importieren.

Konfigurationsprüfliste

Geführtes Setup zur Implementierung von SRM verwenden

Das geführte Setup stellt eine Reihe von Aufgaben bereit, mit denen Sie SRM in Ihrer -Instanz konfigurieren können. Um das geführte Setup für SRMzu öffnen, navigieren Sie zu **Alle** > *Service Operations-Arbeitsbereich* > **Übersicht** und wählen Sie **Konfigurieren**aus.



Installieren Sie die Anwendung Service Reliability Management aus dem Admin Center oder ServiceNow Store

Installieren Sie die Anwendung SRM aus dem Admin Center oder ServiceNow Store.

Vorbereitungen

Erforderliche Abonnements: ITSM Professional und ITOM Operator Professional.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Store-App Datenvisualisierungen v24.1.8 ist ebenfalls erforderlich. Informationen zum Installieren der App finden Sie unter Datenvisualisierungen im ServiceNow Store.

Installieren Sie zum Erstellen und Verwalten von Warnungsautomatisierungen die Anwendung Warnungsautomatisierung, die Sie anfordern können unter ServiceNow Store.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

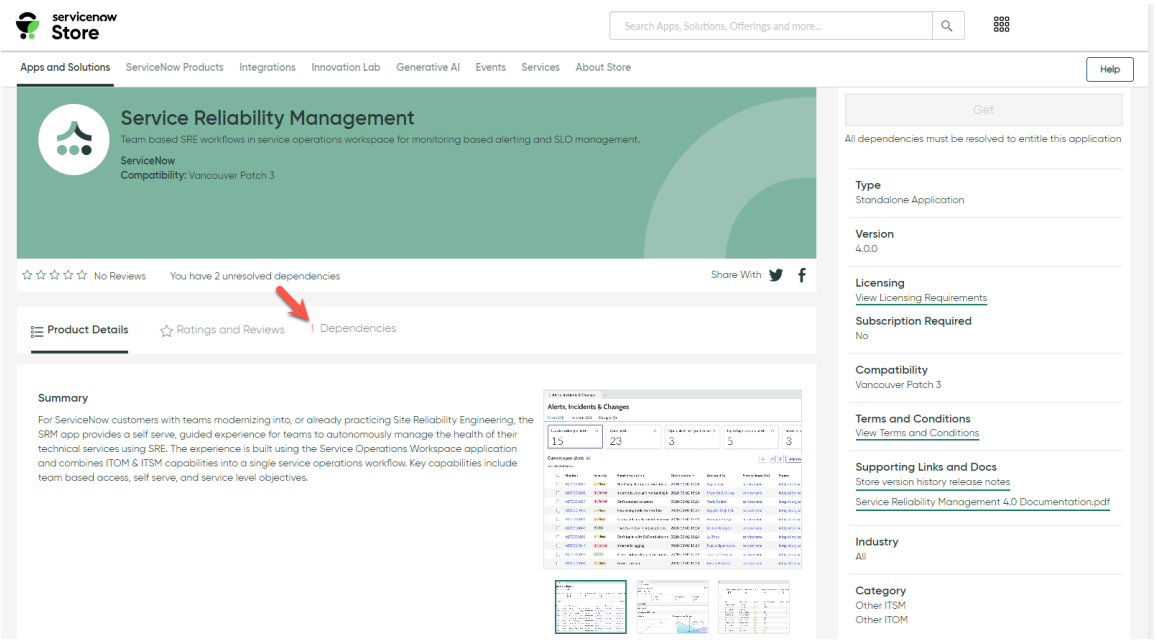
Mit SRM werden Rollen und Demodaten installiert. Die Demodaten enthalten Vorlagen, die die Implementierung beschleunigen und Benutzern helfen, SRM schnell zu verstehen und zu verwenden.

Prozedur

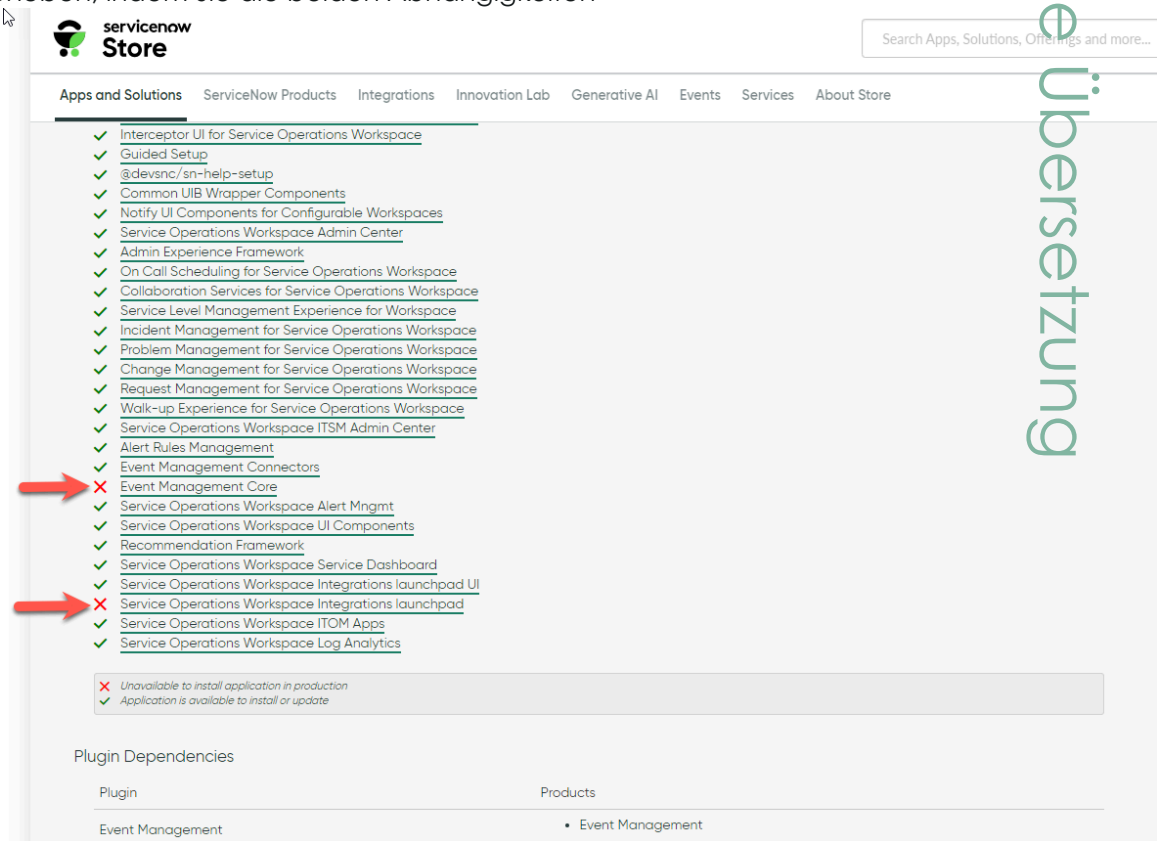
1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Übersicht**.
2. Wählen Sie auf der Karte **Service Betrieb Management**,**Installieren**aus.
3. Wählen Sie im Popup-Fenster **Installation starten**.
   Sie gelangen zum Portal des ServiceNow Store.
4. Führen Sie alle erforderlichen Schritte durch.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Abhängigkeiten in der Liste des App-Stores rot angezeigt werden, wählen Sie die Zeile aus, um die abhängige App zu öffnen und zu installieren. Wenn Sie bereits über die abhängige App verfügen und sie weiterhin in Rot angezeigt wird, können Sie sie nach Bedarf abrufen oder erneut aktivieren.



Das Beispiel zeigt, dass wir zwei ungelöste Abhängigkeiten haben. Bevor Sie die App installieren, müssen Sie dieses Problem beheben, indem Sie die beiden Abhängigkeiten



auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für die gängigen Anwendungsfälle veranschaulichen. Demodaten werden geladen, wenn Sie die Anwendung zum ersten Mal in einer Entwicklungs- oder Testinstanz installieren.

Nach der Installation kann die Karte **„Service Operations Management“** zum Konfigurieren von SRMverwendet werden.

Administratoren zu Service Reliability Management zuweisen

Fügen Sie Personen aus Ihrer Instanz ServiceNow hinzu, um (Ihren Servicebetrieb zu verwalten.

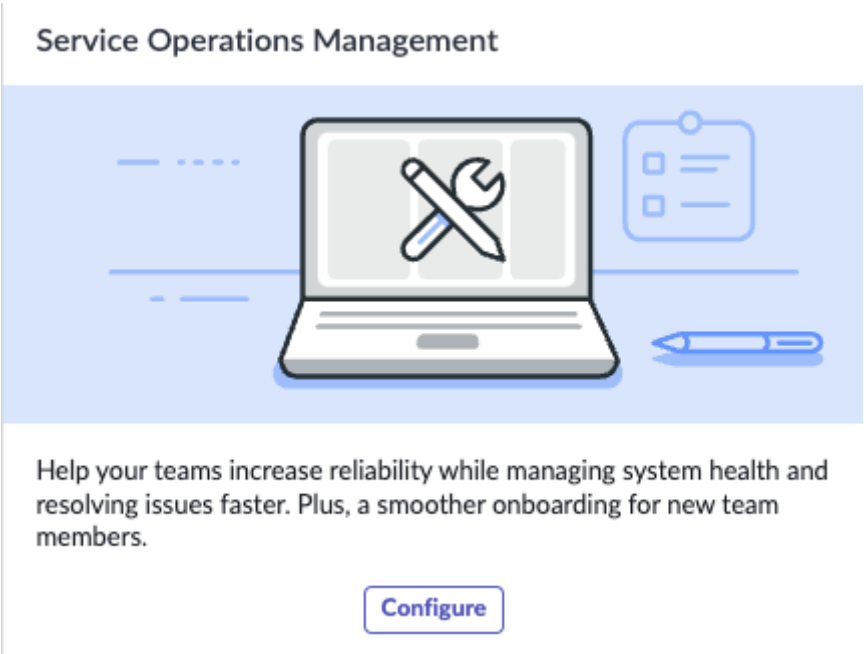
Vorbereitungen

Der -Administrator SRM kann neue Teams erstellen und einrichten sowie Daten für alle Service Reliability Management -Teams von] anzeigen und ändern.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Übersicht**.
2. Im **Servicebetriebsmanagement** Wählen Sie auf der Kachel **Konfigurieren**aus.



Sie gelangen zu **Service Operations Management**

3. Navigieren zu **Zuweisen und aktivieren** > **Administratorrollen zuweisen**.
4. Geben Sie Anwendernamen in das Feld ein.
5. Wählen Sie **Speichern**.

Importieren Sie Services zur Verwendung in Service Reliability Management

Filtern und importieren Sie Services auf der Plattform von ServiceNow, um sie in der Anwendung SRM zu verwalten.

Vorbereitungen

Erforderliche Rolle: Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Konfigurationen**.
2. Navigieren zu **Servicebetriebsmanagement** > **Zuweisen und importieren** > **Importieren Sie Services**.

   Nur Services, die noch nicht in SRM importiert wurden, sind sichtbar.

   Die Listenansicht „Services“ unten enthält bereits angewendete Standardfilter für Services, die in SRM importiert werden können. Sie können nicht bearbeitet werden.

   Hinweis:

   Filter für dieselben Felder werden als UND ausgewertet, Filter für verschiedene Felder werden als ODER ausgewertet. Wenn Sie beispielsweise nach **Business-Relevanz** filtern und **Status** den Wert **Offen** aufweist, wird der Filter **Business-Relevanz**als „1 - sehr kritisch“ ODER „2 - etwas kritisch“ ODER „3 - weniger kritisch“ ODER „4 - nicht kritisch“ UND **Status Offen** ausgewertet.

   Wenn Sie Ihre Listenansichtsfilter ändern, werden Ihre Einstellungen automatisch gespeichert. Wenn Sie an einen anderen Ort navigieren, sind sie bei der Rückkehr weiterhin festgelegt.

3. Auf der Registerkarte **Filtern und auswählen**:
   a. Verwenden Sie **Standardfilter anzeigen**, um die Filter im Popup-Fenster anzuzeigen.
   b. Verwenden Sie den Bedingungsgenerator, um der Listenansicht neue Filter hinzuzufügen. Die Listenansicht wird mit allen Filtern aktualisiert.
4. Verwenden Sie die Kontrollkästchen in der Listenansicht, um die zu importierenden Services auszuwählen.
5. Wählen Sie **Vorschau**.
   Sie wechseln zur Registerkarte **Services für Import**.
6. Überprüfen Sie die Services, und wählen Sie **Importieren**.
   Wenn Sie Ihre Meinung ändern und zur Registerkarte **Filtern und auswählen** zurückkehren, können Sie die ausgewählten Services weiterhin importieren oder den Vorgang ohne Import beenden.
   Die importierten Services sind in SRM verfügbar.
7. Verwenden Sie den Link **Importierte Services anzeigen**, der jetzt im angezeigt wird **Zuweisen und importieren** > **Importieren Sie Services** Bildschirm, um alle in SRMverfügbaren Services anzuzeigen.

Aktivieren Sie Teams und Services in Service Reliability Management

Aktivieren Sie Teams und Services auf der Plattform von ServiceNow, um sie in der Anwendung SRM zu verwalten.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Konfigurationen**.
2. Im **Servicebetriebsmanagement** Wählen Sie auf der Kachel **Konfigurieren**aus.
   Sie gelangen zu **Servicebetriebsmanagement**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Navigieren zu **Zuweisen und aktivieren** > **Teams und Services aktivieren**.
4. Wählen Sie **Teams und Services aktivieren**aus.
   Über die Option **Teams aktivieren** können Sie Teams importieren oder hinzufügen. Die Ansicht „Zuweisungsgruppen“ unten enthält Teams, die in SRM importiert werden können.
5. Verwenden Sie im Editor-Bereich den Bedingungsgenerator, um der Listenansicht neue Filter hinzuzufügen.

   Hinweis:

   Filter für dieselben Felder werden als UND ausgewertet, Filter für verschiedene Felder werden als ODER ausgewertet. Wenn Sie beispielsweise nach **Business-Relevanz** filtern und **Status** den Wert **Offen** aufweist, wird der Filter **Business-Relevanz**als „1 - sehr kritisch“ ODER „2 - etwas kritisch“ ODER „3 - weniger kritisch“ ODER „4 - nicht kritisch“ UND **Status Offen** ausgewertet.

   Wenn Sie Ihre Listenansichtsfilter ändern, werden Ihre Einstellungen automatisch gespeichert. Wenn Sie an einen anderen Ort navigieren, sind sie bei der Rückkehr weiterhin festgelegt.

   Die Listenansicht wird mit allen Filtern aktualisiert.
6. Wählen Sie unter Zuweisungsgruppen die Teams aus, die Sie hinzufügen möchten, und wählen Sie **Aktivieren**aus.
   Sie gelangen zur Option **Services aktivieren**, um Services hinzuzufügen.
7. Wählen Sie in der Liste **Serviceklasse auswählen** einen Service aus.
   Die folgenden sechs Services sind verfügbar:
   - Anwendungsservices
   - Zugeordnete Anwendungsservices
   - Berechnete Anwendungsservices
   - Dynamic CI-Gruppe
   - Technische Services
   - Tag-basierte Services

   Die Ansicht „Ausgewählte Services“ unten enthält Services, die in SRM importiert werden können.
8. Verwenden Sie im Editor-Bereich den Bedingungsgenerator, um der Listenansicht neue Services hinzuzufügen.

   Hinweis:

   Filter für dieselben Felder werden als UND ausgewertet, Filter für verschiedene Felder werden als ODER ausgewertet. Wenn Sie beispielsweise nach **Business-Relevanz** filtern und **Status** den Wert **Offen** aufweist, wird der Filter **Business-Relevanz**als „1 - sehr kritisch“ ODER „2 - etwas kritisch“ ODER „3 - weniger kritisch“ ODER „4 - nicht kritisch“ UND **Status Offen** ausgewertet.

   Wenn Sie Ihre Listenansichtsfilter ändern, werden Ihre Einstellungen automatisch gespeichert. Wenn Sie an einen anderen Ort navigieren, sind sie bei der Rückkehr weiterhin festgelegt.

   Die Listenansicht wird mit allen Filtern aktualisiert.
9. Wählen Sie aus den ausgewählten Services die Services aus, die Sie hinzufügen möchten, und wählen Sie **Aktivieren**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Popup-Fenster **„Services aktivieren“** wird geöffnet.

10. Wählen Sie in der Dropdown-Liste **Supportgruppe** die Supportgruppe aus, die für die Services verantwortlich sein soll, und wählen Sie **Bestätigen**aus.

Ergebnisse

Auf der Seite **Teams und Services aktivieren** werden die folgenden Optionen angezeigt:

- Vorhandene Teams
- Vorhandene Services

Sie können die Optionen auswählen, um die Teams oder Services anzuzeigen.

Genehmigungsprozess zur Aufnahme von Services in Service Reliability Management hinzufügen

Fügen Sie Ihren -Services aus Governance-Gründen einen Genehmigungsprozess hinzu.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Konfigurationen**.
2. Wählen Sie unter **Governance und Autonomie** die Option **Service-Governance** aus.
3. Je nach Einstellungen Ihrer Organisation können Sie einen Genehmigungsprozess hinzufügen, wenn SRM-Administratoren, Manager oder Beantworter die Erstellung eines Service in SRM oder die Zuordnung eines vorhandenen Service mit SRM anfordern.
4. Wählen Sie einen oder beide Prozesse aus, indem Sie das entsprechende Kontrollkästchen aktivieren.

   Genehmigungsanforderungstypen:

   - Beim Erstellen eines neuen Service in SRMist eine Genehmigung erforderlich:

     Erfordert die Genehmigung, wenn ein neuer Service für SRM erstellt wird, und weist die Genehmigung dem für neue Services verantwortlichen Team zu.

   - Genehmigung beim Zuordnen eines vorhandenen CMDB-Service in SRM erforderlich:

     Erfordert die Genehmigung, um SRM einen vorhandenen Service hinzuzufügen, und weist die Genehmigung dem Team zu, das für vorhandene Services verantwortlich ist.

5. Geben Sie das Team ein, das für Genehmigungen verantwortlich ist, oder wählen Sie es aus.
6. Wählen Sie **Speichern**.
   Diese Aktion initiiert den Genehmigungsprozess und weist die Genehmigung dem Team zu, das für die Genehmigung des neuen Service verantwortlich ist.

   Hinweis: Für Genehmigungen sind zwei Schritte auszuführen. Zuerst wird die Anforderung genehmigt, was im Anforderungsdatensatz im Feld **Phase** angezeigt wird. Anschließend bleibt die Anforderung **im Status Ausstehend**, bis das Anforderungselement im **Anforderungsdatensatz** genehmigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Genehmigungsprozess zur Aufnahme von Teams in SRM hinzufügen

Fügen Sie Ihren Service Reliability Management-Teams aus Governance-Gründen einen Genehmigungsprozess hinzu.

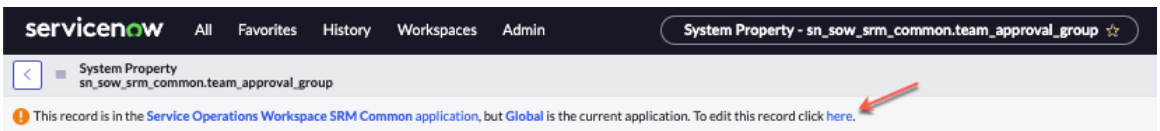
Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Konfigurationen**.
2. Wählen Sie unter **Governance und Autonomie** die Option **Team-Governance** aus.
3. Je nach Einstellungen Ihrer Organisation können Sie einen Genehmigungsprozess hinzufügen, wenn SRM-Administratoren, Manager oder Beantworter die Erstellung eines Teams in SRM anfordern.
4. Wählen Sie den Link **Wert mit sys_id aktualisieren**.
5. Wählen Sie im neuen Fenster den Link, um den Datensatz zu bearbeiten.

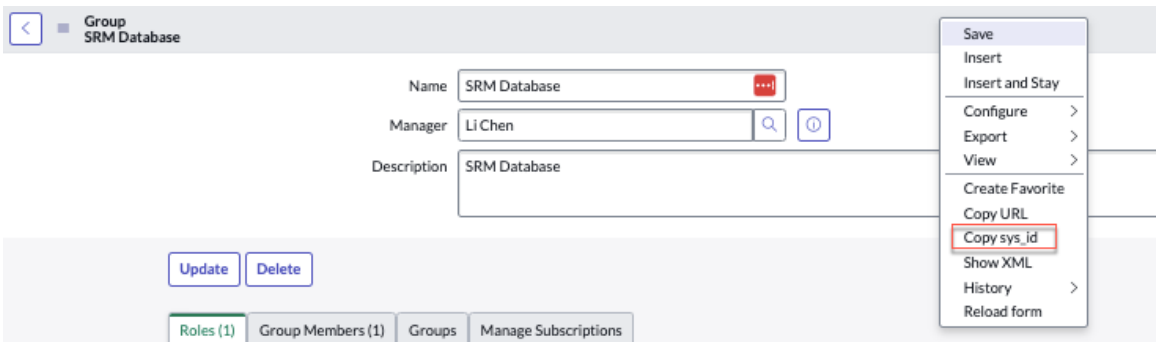


6. Ersetzen Sie die Systemeigenschaft **Wert** durch die `sys_id` des Zuweisungsteams.

   a. Navigieren Sie zum Gruppendatensatz für das gewünschte Team.

   b. Datensatz öffnen

   c. Klicken Sie mit der rechten Maustaste auf den Header (oder verwenden Sie das Tastenkürzel), und wählen Sie **sys_id kopieren**aus.



   d. Kehren Sie zum Systemeigenschaft-Datensatz zurück, und fügen Sie die **sys_id** in das Feld „Wert“ ein.

   e. Fügen Sie der Erfüllung des Elements „SRM – Genehmigung zur Teamerstellung erforderlich“ den entsprechenden Flow hinzu.

   f. Wählen Sie **Aktualisieren aus.**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Aktion initiiert den Genehmigungsprozess und weist die Genehmigung dem Team zu, das für die Genehmigung neuer Teams verantwortlich ist.

Hinweis: Für Genehmigungen sind zwei Schritte auszuführen. Zuerst wird die Anforderung genehmigt, was im Anforderungsdatensatz im Feld **Phase** angezeigt wird. Anschließend bleibt die Anforderung **im Status Ausstehend**, bis das Anforderungselement im **Anforderungsdatensatz** genehmigt wird.

Importieren Sie Teams in Service Reliability Management

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Konfigurationen**.
2. Navigieren zu **Servicebetriebsmanagement** > **Zuweisen und importieren** > **Importieren Sie Teams**.
   Die Teams-Listenansicht unten enthält bereits angewendete Standardfilter, für die Teams in SRM importiert werden können. Sie können nicht bearbeitet werden.

   Hinweis:

   Filter für dieselben Felder werden als UND ausgewertet, Filter für verschiedene Felder werden als ODER ausgewertet. Wenn Sie beispielsweise nach **Business-Relevanz** filtern und **Status** den Wert **Offen** aufweist, wird der Filter **Business-Relevanz**als „1 - sehr kritisch“ ODER „2 - etwas kritisch“ ODER „3 - weniger kritisch“ ODER „4 - nicht kritisch“ UND **Status Offen** ausgewertet.

   Wenn Sie Ihre Listenansichtsfilter ändern, werden Ihre Einstellungen automatisch gespeichert. Wenn Sie an einen anderen Ort navigieren, sind sie bei der Rückkehr weiterhin festgelegt.

   Standardfilter sind:

   - **[Typ] [!=] [c419b12deb412110...]**
   - **[Typ] [ist] [leer]**
   - **[Aktiv] [ist] [true]**
3. Auf der Registerkarte „Filtern und auswählen“:
   a. Verwenden Sie **Standardfilter anzeigen**, um die Filter im Popup-Fenster anzuzeigen.
   b. Verwenden Sie den Bedingungsgenerator, um der Listenansicht neue Filter hinzuzufügen. Die Listenansicht wird mit allen Filtern aktualisiert.
4. Verwenden Sie das Kontrollkästchen in der Listenansicht, um die zu importierenden Teams auszuwählen.
5. Wählen Sie **Vorschau**.
   Wechseln Sie zur Registerkarte **Teams für Import**.
6. Überprüfen Sie die Teams, und wählen Sie **Importieren** aus.
   Wenn Sie Ihre Meinung ändern und zur Registerkarte **Filtern und auswählen** zurückkehren, können Sie die ausgewählten Teams weiterhin importieren oder den Vorgang ohne Import beenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die importierten Teams sind in SRM verfügbar.

7. Verwenden Sie den Link **Importierte Teams anzeigen**, der jetzt im angezeigt wird **Zuweisen und importieren** > **Importieren Sie Teams** Bildschirm, um alle in SRMverfügbaren Teams anzuzeigen.

Team-Anforderungsformulare bearbeiten und für Service Reliability Management veröffentlichen

Bearbeiten Sie ein Team-Anforderungsformular, um Teamanforderungen an die Präferenzen Ihrer Organisation anzupassen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Konfigurationen**.
2. Wählen Sie unter **Governance und Autonomie** die Option **Team-Governance** aus.
3. Wählen Sie den Link **Anforderungsformular für Katalogelemente**.
4. Bearbeiten Sie das Formular, und befolgen Sie die Kataloganweisungen zum Veröffentlichen.
   Ausführliche Informationen zum Bearbeiten eines Katalogelements finden Sie unter Erstellen Sie ein Katalogelement mithilfe einer Vorlage . Folgen Sie den dortigen Verfahren.

   Hinweis: Denken Sie daran, **Übermitteln** zu wählen. Solange Sie das Element nicht übermitteln, befindet es sich im Status **Entwurf** und ist im Katalog nicht verfügbar.

Fehlerbudgetaktionen bei Verletzung eines SRM-SLO konfigurieren

Konfigurieren Sie die Aktionen, die das Team auswählen kann, wenn das Fehlerbudget eines Servicelevel-Ziels (Service Level Objective, SLO) verletzt wird.

Vorbereitungen
Erforderliche Rolle: admin

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Konfigurationen**.
2. Wählen Sie unter **Governance und Autonomie** die Option **Fehlerbudgets** aus.

   Hinweis: Das Ausführen einer dieser Aktionen erfordert fortgeschrittene ServiceNow-Kenntnisse.

   Ausführlichere Informationen zum Bearbeiten von Workflows oder zum Erstellen von anwenderdefinierten Workflows finden Sie unter Flow Designer .

3. Wählen Sie **Incidents konfigurieren**, um den Subflow für Fehlerbudgetaktionen zu bearbeiten.
4. Wählen Sie **E-Mails konfigurieren**, um die Aktionen festzulegen, die das Team auswählen kann, wenn das Fehlerbudget eines Servicelevel-Ziels (Service Level Objective, SLO) verletzt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Change-Anforderungen zur Genehmigung von SRM-Teams genehmigen

Genehmigen Sie eine Change-Anforderung, wenn der Change von jemandem in der Genehmiger-Rolle überprüft und genehmigt wurde.

Vorbereitungen

In dieser Ansicht sind nur offene Change-Anforderungen verfügbar.

Erforderliche Rolle: admin oder SRM-Genehmigungsteam

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte **Changes**.
4. Öffnen Sie einen Change Request.
5. Wenn Sie der vorgesehene Besitzer des Service oder Teams sind, wählen Sie **Mir zuweisen**. Andernfalls weisen Sie den Service oder das Team dem vorgesehenen Besitzer in der Listenansicht oder dem Datensatz zu.
6. Wählen Sie aus, um den Datensatz zu öffnen.
7. Wählen Sie im Feld **Status** die Liste aus, und wählen Sie **Genehmigt**aus.
8. Wählen Sie **Speichern**.
   Der Status der Change-Anforderung wird von **Bewerten** in **Genehmigt** geändert.

   Nach der Genehmigung wird der neue Service oder das neue Team erstellt und dem SRM-Team hinzugefügt. Als Besitzer wird die Person festgelegt, die im Feld „Zugewiesen an“ angezeigt wird. „Verwaltet nach Gruppe“ ist auf das SRM-Team festgelegt, das zum Beauftragten gehört.

Konfigurieren Sie Twilio für das Senden von Benachrichtigungen in SRM

Stellen Sie eine Verbindung zwischen Ihrer Instanz SRM und Ihrem Twilio-Account her, damit Ihre Teams Benachrichtigungen empfangen können.

Vorbereitungen

Bevor Sie beginnen, benötigen Sie eine SID und ein Authentifizierungstoken für ein aktives Twilio-Konto.

Hinweis: Die Ausführung dieser Aktion erfordert fortgeschrittene ServiceNow-Kenntnisse.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

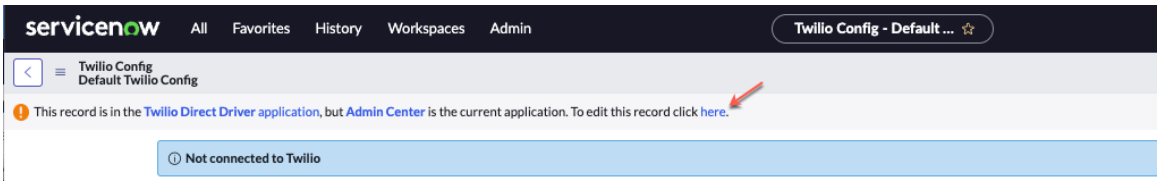
Sie können anpassen, was von Twilio gesendet wird, indem Sie den Rufbereitschafts-Workflow im System bearbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Konfigurationen**.
2. Wählen Sie **Service Reliability Management aus.**
3. Wählen Sie unter **Integrationendie Option Twilio API Key**aus.
4. Wählen Sie **Twilio-Konfiguration**aus.
5. Wählen Sie im neuen Fenster den Link **hier**, um den Datensatz zu bearbeiten.



6. Geben Sie den Wert **für die Account-SID** ein.
7. Wahlweise: Geben Sie einen Wert **für den Gültigkeitszeitraum** ein.
8. Wählen Sie **Verbinden**, um den Schlüssel zu aktivieren, oder **Speichern aus**, um Ihre Änderungen ohne Aktivierung zu speichern.

Installieren Sie die Anwendung Regeln für Warnungsautomatisierung

Installieren Sie die Anwendung **Regeln für Warnungsautomatisierung** und alle unterstützenden Anwendungen.

Vorbereitungen

Erforderliche Rolle: Administrator

Erforderliche Abonnements: ITSM Professional- oder ITOM Operator Professional-Abonnements.

Warum und wann dieser Vorgang ausgeführt wird

Bevor Sie Verwaltungsregeln erstellen, müssen Sie die Anwendung Service Reliability Management installieren und konfigurieren, die im ServiceNow Storeverfügbar ist.

Prozedur

1. Wählen Sie den Link, der Ihnen in der E-Mail bereitgestellt wurde, um auf ServiceNow Store zuzugreifen und die Anwendung auf Ihre Instanz SRM herunterzuladen.
2. Navigieren Sie in Ihrer Now Platform-Instanz zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**
3. Suchen Sie die Anwendung **Regeln für Warnungsautomatisierung**, und wählen Sie **Installieren**, um sie zu aktivieren.
   Warnungsautomatisierungsregeln können in Service Reliability Managementverwendet werden.

Service Reliability Management verwenden

SRM Mit können Sie Services registrieren, die Serviceintegrität überwachen, auf Serviceverschlechterungen mit Rufbereitschaftsschichten und Eskalationsrichtlinien und -auslösern reagieren und verteilte Teams mit minimaler Governance durch die zentrale IT einarbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Grundlegende Aufgaben in SRM

Mit SRM-Services arbeiten

Ein Service stellt ein funktionales Ergebnis dar, z. B. Networking, Zahlungen oder HR-Services, für das ein Team verantwortlich ist. Um dieses Ergebnis zu liefern, kann ein Service eine oder mehrere technische Komponenten enthalten, z. B. einen Benutzerauthentifizierungsservice oder eine gemeinsam genutzte Infrastruktur wie eine Datenbank.

SRM arbeitet mit Integrationen, um Warnungen zu priorisieren und an die richtigen Beantworter weiterzuleiten und die Eskalation nachzuverfolgen, bis die Warnung bestätigt wird und Sie wissen, dass jemand reagiert. Wenn Sie einen Service in SRM erstellen oder hinzufügen, muss er einem Service in Ihrer SRM-Infrastruktur entsprechen.

Hinweis:

Möglicherweise benötigen Sie mehrere Toolintegrationen, um die einzelnen technischen Services zu überwachen und Events von diesen Tools zu erhalten. Fügen Sie SRM mit dem Services eine Integration hinzu. Weitere Informationen finden Sie unter Mit SRM-Integrationen arbeiten.

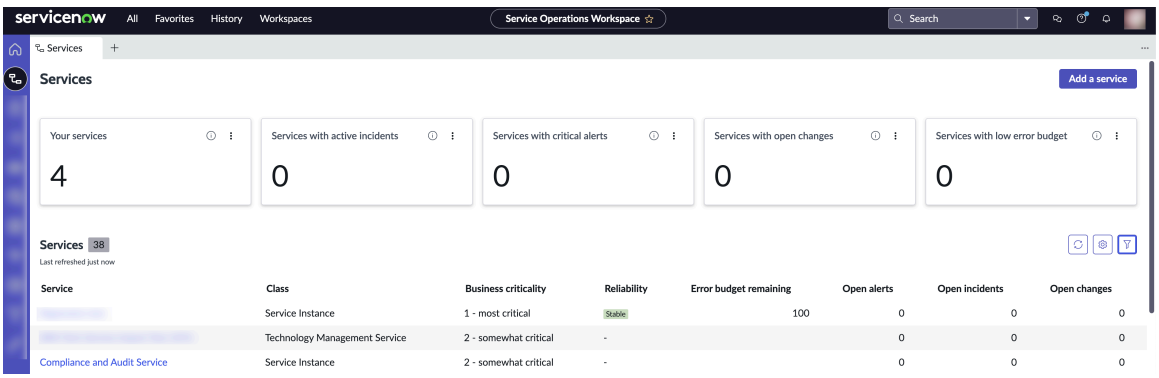
Darüber hinaus können Sie Zuverlässigkeitsmetriken für den Service erstellen. Siehe Mit Zuverlässigkeitsmetriken arbeiten

Die Bindung eines Teams und von Richtlinien an diesen Service erleichtert die Aufteilung von Verantwortlichkeiten und die Nachverfolgung technischer Ergebnisse. Es erleichtert auch die Automatisierung von Antwortroutinen und die Fokussierung darauf, wen Sie wann benachrichtigen.

Der Status eines bestehenden Service wird vererbt. Der Status eines erstellten Service in SRM lautet **Keine**.

Services

Zielseite von Services



Die Karten auf der Zielseite „Services“ zeigen Metriken für Folgendes an:

- **Your Services (Ihre Services)** Anzahl aller Services, für die Sie oder Ihr Team die Zuverlässigkeit verwalten und überwachen.
- **Services mit aktiven Incidents**: Services mit einem oder mehreren offenen Incidents, zuerst sortiert nach Business-Relevanz, die kritischsten ganz oben; dann sortiert nach Anzahl der aktiven Incidents, höchste Anzahl oben; und schließlich sortiert nach % des verbleibenden Fehlerbudgets, niedrigstes oben.
- **Services mit kritischen Warnungen**: Services mit offenen Warnungen, zuerst sortiert nach Business-Relevanz, die kritischsten ganz oben; dann sortiert nach Anzahl der Warnungen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

höchste Anzahl oben; und schließlich sortiert nach % des verbleibenden Fehlerbudgets, niedrigstes oben.

- **Services mit offenen Changes**: Alle Services, die Ihr Team verwaltet und überwacht.
- **Services mit niedrigem Fehlerbudget**: Services mit einem verbleibenden Fehlerbudget von weniger als 25 %.

  Das Fehlerbudget wird das SLO-Volumen dargestellt, das Sie über einen bestimmten Zeitraum ausgeben können. Es kann verwendet werden, um die Release-Geschwindigkeit zu verwalten.

Hinweis: Um die Kartenwerte sowie die Listen, die sie darstellen, zu aktualisieren, verwenden Sie die Browser-Aktualisierung Schaltfläche „ .

Die Listenansicht hängt von der ausgewählten Servicekarte ab.

Hinweis: **Your Services (Ihre Services)** ist die Standardauswahl für die Zielseite.

Jede Spalte in der Liste kann gruppiert oder gefiltert werden.

Jede Liste kann bearbeitet, sortiert oder exportiert werden.

Ausführlichere Informationen zu einzelnen Servicedetails finden Sie unter Formular „Servicedetails“ bearbeiten.

Metrikdefinitionen der Services-Listenansicht

Abschnitt **Servicelevel-Ziele**

- **Service**: Name des Service.
- **Klasse**: „Anwendung“ oder „Technischer Service“.
- **Business-Relevanz**: Wie wichtig dieser Service für die Geschäftstätigkeit ist.

  Die Auswahlmöglichkeiten lauten wie folgt:
  - 1 − Am kritischsten (Standardeinstellung)
  - 2 – Kritisch
  - 3 – weniger kritisch
  - 4 – Nicht kritisch
- **Offene Warnungen**: Anzahl der offenen Warnungen, die dem Service zugewiesen sind.
- **Offene Incidents**: Anzahl der offenen Incidents, die dem Service zugewiesen sind.
- **Verbleibendes Fehlerbudget**: Prozentsatz des für den Service verbleibenden Fehlerbudgets.

Services zu SRM hinzufügen

Fügen Sie Service Reliability Management (SRM) eine Anwendung oder einen technischen Service hinzu, um Ihre Teams bei der Verwaltung der Serviceintegrität zu unterstützen.

Vorbereitungen

Wenn Sie SRMeinen vorhandenen technischen Service hinzufügen, stellen Sie sicher, dass dieser keine Supportgruppe hat. Sie weisen die Supportgruppe zu, indem Sie den Service zu SRMhinzufügen.

Erforderliche Rolle: srm_admin, srm_manager oder srm_responder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Fügen Sie SRM einen Service hinzu, um Teams Zugriff auf seine Incidents und Warnungen zu gewähren. Sie können entweder einen Service erstellen oder einen vorhandenen importieren. SRM unterstützt Anwendungsservices und technische Services.

Wenn Sie SRMeinen technischen Service hinzufügen, fügen Sie auch seine technischen Serviceangebote hinzu. TSOs sind spezifische Komponenten innerhalb eines übergeordneten technischen Service. Beispielsweise ist die Spam-Filterung ein TSO innerhalb des technischen E-Mail-Services. In SRMkönnen Sie einen übergeordneten technischen Service und seine TSOs verschiedenen Teams zuweisen.

Hinweis: Wenn Sie einen vorhandenen technischen Service importieren, übernehmen die zugehörigen TSOs nicht die Supportgruppe. TSOs behalten entweder ihre vorhandene Supportgruppe, oder, wenn sie keine haben, müssen Sie sie vor dem Einrichten von SRM Servicelevel-Zielen (SLOs) zuweisen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Verwenden Sie eine der folgenden Methoden, um das Formular Tell us about the service (Erzählen Sie uns von dem Service) zu öffnen, und wählen Sie die Felder aus, oder füllen Sie sie aus.
   - Wählen Sie auf Ihrer **Homepage** im Abschnitt „Erste Schritte“ die Option **Add a service (Service hinzufügen)**aus.
   - Wählen Sie auf der Seite „Services“ ( ) **Add a service (Service hinzufügen**) aus.
3. Fügen Sie einen Service hinzu, oder registrieren Sie einen vorhandenen Service.

Option	Schritte
Einen Service hinzufügen	**a.** Wählen Sie im Feld **Neu oder vorhanden-** die Option **Neuen Service in Service Reliability Management erstellen aus**. **b.** Füllen Sie die Felder des Formulars aus. Weitere Informationen zu den Feldbeschreibungen finden Sie unter Formular „Service hinzufügen“.. **c.** Wählen Sie **Weiter**.
Registrieren Sie einen vorhandenen Service	**a.** Wählen Sie im Feld **Neu oder vorhanden-** die Option **Vorhandene CMDB-Services zu Service Reliability Management zuordnen**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Schritte
	b. Wählen Sie einen oder mehrere Services aus. **c.** Wählen Sie **Weiter**.

4. Füllen Sie im Schritt Team zuweisen die Felder aus.
   - Wählen Sie im Feld **Serviceverantwortlicher** den Benutzer aus, der die Services besitzen soll.
   - Wählen Sie im Feld **Supportgruppe** ein Team aus, das die Services überwachen soll.

     Um die Services einem neuen Team zuzuweisen, wählen Sie **Neues Team erstellen aus**.

     Weitere Informationen finden Sie unter SRM-Teams hinzufügen.
5. Wählen Sie **Service(s) hinzufügen**aus.

Ergebnisse
Wenn Genehmigungen nicht aktiviert sind, wird Ihr Service in der Serviceliste angezeigt.

Wenn Genehmigungen aktiviert sind, wird Ihre Serviceanfrage zur Genehmigung gesendet. Nachdem der Service genehmigt wurde, wird er in der Servicesliste angezeigt.

Hinweis: Wenn Sie einen technischen Service hinzugefügt haben, werden dessen TSOs auf der Registerkarte Angebote auf der Seite des übergeordneten technischen Service angezeigt. TSOs werden auch in der Servicesliste angezeigt. Um ein TSO ohne zugewiesene Supportgruppe anzuzeigen, entfernen Sie alle Filter aus der Serviceliste.

Nächste Maßnahme
Sie können Ihren Service so einrichten, dass mit der Nachverfolgung seiner Zuverlässigkeit begonnen wird.

Wenn ein TSO keine Supportgruppe hat, weisen Sie ihn einer Supportgruppe zu, bevor Sie SLOs einrichten. Informationen zum Zuweisen von Supportgruppen finden Sie unter SRM-Servicedetails bearbeiten.

Mit SRM-Integrationen arbeiten

Mittels Integrationen in SRM können Benutzer Warnungen und Incidents mit Tools für Überwachung und Zusammenarbeit effizient verwalten. SRM-Integrationen werden nur in Services hinzugefügt oder erstellt.

SRM wird bestmöglich mit den Tools integriert, die Sie benötigen, um effizient zusammenzuarbeiten und Incidents effizient zu lösen.

Hinweis: Wenn Sie in ITOM Rollen im Zusammenhang mit Integrationen haben, wird im linken Navigationsbereich ein Symbol für Integrationen angezeigt. Diese für keine Erstellungen durch, stellen keine Verbindung mit SRM her und können nicht davon verwendet werden.

Verfügbare SRM-Integrationen

Integrationen sind Teil von Services in SRM. SRM verwendet Integrationen, um alle Metriken und Protokolle aus Ihrer Infrastruktur zusammenzuführen und Einblicke in das einheitliche System als Ganzes zu erhalten. Sie können Teile einzeln anzeigen und auch, wie sich einzelne Teile auf das Ganze auswirken.

Beginnen Sie mit der Überwachung Ihrer Projekte so früh wie möglich im Entwicklungsprozess.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Folgende Integrationen sind standardmäßig zum Hinzufügen zu SRM verfügbar:

- Anwenderdefinierter Connector (Webhook)
- Amazon Web Services
- Catchpoint
- Datadog
- Dynatrace Monitor
- Google Cloud Platform
- Grafana
- Honeycomb
- Instana
- ServiceNow Cloud Observability
- Logic Monitor
- Microsoft Azure
- New Relic
- Oracle Cloud
- Prometheus
- Scout APM
- Sentry
- Sumologic
- ThousandEyes
- Generische Ereignisinstanz transformieren

Integrationen zu SRM hinzufügen

Fügen Sie eine Integration hinzu, um Events und SLO/SLI für Ihren Service zu überwachen.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **Services** ( ).
3. Wählen Sie einen Service aus.
4. Wählen Sie die Registerkarte **Integrationen**.
5. Wählen Sie die Schaltfläche **Integration hinzufügen aus**.
6. Fügen Sie eine verfügbare Integration oder eine neue Integration hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

So fügen Sie eine verfügbare Integration hinzu:

a. Wählen Sie das Caret-Symbol aus, um die Liste zu erweitern.

b. Wählen Sie eine Integration aus.

So fügen Sie eine neue Integration hinzu:

a. Verwenden Sie die Suchleiste, oder wählen Sie eine neue Integration aus der Liste aus.

b. Füllen Sie im Integrationsfenster unter **Details bereitstellen** die entsprechenden Felder im Formular aus.

Eine Integration hinzufügen

Feld	Beschreibung
Integrationsname	Name der Integration.
Beschreibung	Beschreiben Sie die Integration. Geben Sie an, wofür sie verwendet wird.
Quelle	Automatisch ausgefüllt. (Wenn leer, laden Sie die Seite neu.)
Service	Wird automatisch mit dem Service ausgefüllt, dem diese Integration zugeordnet ist.
Wie möchten Sie Ereignisse verbinden?	Direkt mit der Instanz. (Standard)
Service-Beschreibung	Beschreibung des Gesamtservice, die anderen hilft, den Zweck des Service und andere relevante Informationen zu verstehen.

c. Wählen Sie **Weiter aus, und speichern Sie**.
Die Integration befindet sich im Status **Entwurf**.

Befolgen Sie die Anweisungen im Bereich **Drittanbieter-Connector einrichten**.

Hinweis: Diese Anweisungen gelten jeweils spezifisch für einen Lieferanten. Wir stellen die zu verwendende URL bereit.

d. Sobald Sie die Anweisungen des Drittanbieters abgeschlossen haben und Sie benachrichtigt werden, dass er aktiv ist, wählen Sie die Schaltfläche **Aktivieren** aus.

e. Wählen Sie **Fortsetzen**.

Hinweis: Ihre Integration ist aktiv, Sie benötigen jedoch weiterhin den Account eines Servicebenutzers zur Authentifizierung. Dieser Account benötigt die Rolle `evt_mgmt_integration`, damit die Drittanbieteranwendung Events pushen kann. Wenden Sie sich an Ihren Administrator, und bitten Sie ihn um die entsprechende Angabe.

Die Integration ist **Aktiv** und in Ihrer Instanz verfügbar.

Integrationen deaktivieren

Wenn Sie eine Integration vorübergehend deaktivieren möchten, versetzen Sie sie in einen inaktiven Status. Wenn Sie Integrationen deaktivieren, werden die über diese Integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

empfangenen Warnungen nicht mehr verarbeitet. Sie können eine Integration deaktivieren, wenn Sie ein System in den Wartungsmodus versetzen möchten und während dieser Zeit keine unnötigen Warnungen erhalten möchten.

Vorbereitungen
Erforderliche Rolle: Beantworter, Manager oder Administrator

Warum und wann dieser Vorgang ausgeführt wird
Beantworter und Manager können Integrationen deaktivieren, die sie erstellt haben oder die von ihrem Team erstellt wurden. Ein Administrator kann jede Integration in SRM deaktivieren.

Prozedur
1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie auf der Seite **„Services“** ( ) einen Service aus.
3. Wählen Sie die Registerkarte **Integrationen**.

Option	Schritte
Über die Registerkarte „Integrationen“	**a.** Wählen Sie für jede aktive Integration, die Sie deaktivieren möchten, das Symbol „Weitere Aktionen“ . **b.** Wählen Sie **Deaktivieren**.
Über den Integrationsdatensatz	**a.** Wählen Sie die Integration aus, um den Datensatz zu öffnen. **b.** Wählen Sie **Deaktivieren**.

Hinweis: Sie können eine inaktive Integration aktivieren und wieder verfügbar machen, indem Sie über das Symbol „Weitere Aktionen“ **die Option Aktivieren** wählen. Wenn jedoch der Service, der der deaktivierten Integration zugeordnet ist, deaktiviert wurde, können Sie die Integration nicht erneut aktivieren.

Fügen Sie einer Integration in mehrere Services hinzu, oder entfernen Sie sie SRM

Fügen Sie einer Integration mehrere Services gleichzeitig hinzu, um Ereignisse von diesen Services an einem zentralen Ort zu überwachen. Sie können auch einen oder mehrere Services aus der Integration entfernen, wenn Sie sie nicht mehr nachverfolgen müssen.

Vorbereitungen
Erforderliche Rolle: srm_responder, srm_manager und srm_admin

Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie das Integrations-Launchpad-Symbol ( ).
3. Wählen Sie eine Integration aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie die Registerkarte **Zugehörige Services**.
5. Mehrere Services hinzufügen oder entfernen.

Option	Schritte
Services hinzufügen	**a.** Wählen Sie **Service hinzufügen**. **b.** Suchen und wählen Sie im Popup-Fenster Services hinzufügen einen oder mehrere Services, die Sie der Integration hinzufügen möchten. **c.** Wählen Sie **Hinzufügen**.
Entfernen Sie Services	**a.** Aktivieren Sie die Checkbox neben jedem Service, den Sie entfernen möchten. **b.** Wählen Sie **Service entfernen aus**.

Nächste Maßnahme
Stellen Sie beim Hinzufügen von Services sicher, dass die Konfigurationen für den Webhook ordnungsgemäß vorgenommen wurden, damit die eingehenden Ereignisse mit dem richtigen Service verbunden werden. Weitere Informationen finden Sie unter KB-Artikel (KB-Permalink hinzufügen!).

SRM-Servicedetails bearbeiten

Bearbeiten Sie einen vorhandenen Service, für den Ihr Team verantwortlich ist. Geben Sie für jeden Service, für den Sie in SRM Support leisten, allgemeine Informationen über den Service und das SRM-Team an, das ihn unterstützt.

Vorbereitungen
Erforderliche Rolle: srm_admin, srm_manager oder srm_responder

Prozedur
1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **Services** ( ).
3. Wählen Sie in Ihrer Serviceliste den Service aus, den Sie bearbeiten oder aktualisieren möchten.
   Um ein technisches Serviceangebot (TSO) ohne zugewiesene Supportgruppe anzuzeigen und auszuwählen, entfernen Sie alle Filter aus der Serviceliste.
4. Wählen Sie auf der Übersichtsseite die Registerkarte **Details**.
5. Füllen Sie die Felder aus, oder bearbeiten Sie sie.
   Weitere Informationen zu den Feldbeschreibungen finden Sie unter Formular „Servicedetails“ bearbeiten.
6. Um die aktualisierten Servicedetails nach der Bearbeitung zu speichern, wählen Sie **Speichern**aus.

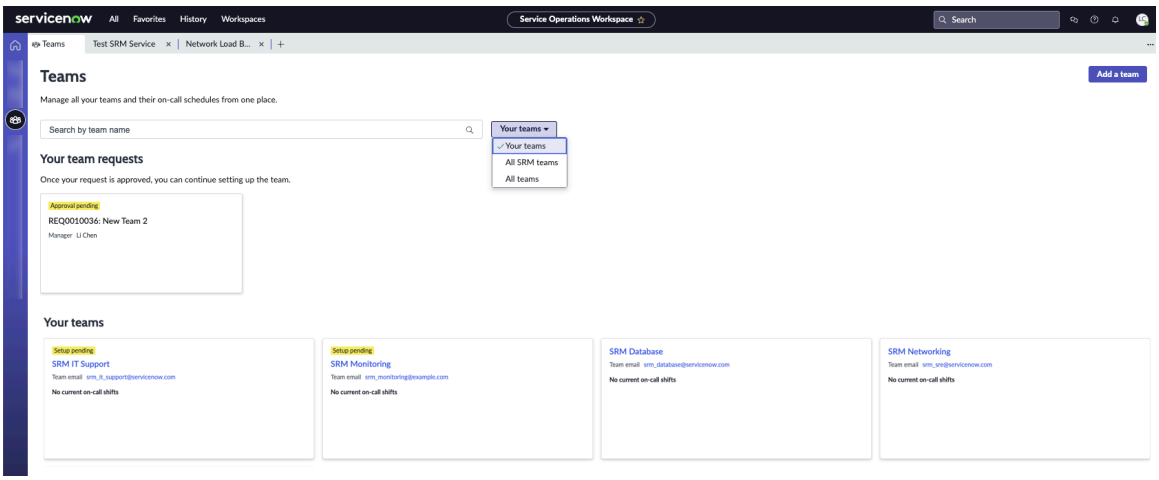
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit SRM-Teams arbeiten

Verwalten Sie Zeitpläne, und definieren Sie Eskalationsrichtlinien für Ihr Team. Auf diese Weise sieht Ihr Team, wer Rufbereitschaft hat und verantwortlich ist, und kann darauf vertrauen, dass kritische Warnungen oder Incidents rechtzeitig bestätigt werden.

Auf der Teams-Zielseite können Sie Ihre Teams und Teamanforderungen anzeigen und verwalten.

Teams-Zielseite



Suchen Sie anhand des Teamnamens unter allen Teams, denen Sie angehören, in allen SRM -Teams oder in allen Teams in Ihrer Organisation.

Ihre Auswahl bestimmt die Karten, die Ihnen auf der Teams-Zielseite angezeigt werden.

Die Auswahlmöglichkeiten lauten wie folgt:

- **Ihre Teams** (Standard)
- **Alle SRM-Teams**: Sämtliche Teams in SRM.

  Hinweis: Ihre Fähigkeit, für jedes Team Aktionen auszuführen, hängt von den Berechtigungen für das Team ab.

- **Alle Teams**: Alle Teams, auf die Sie in Ihrer Organisation Zugriff haben.

  Hinweis: Ihre Fähigkeit, für jedes Team Aktionen auszuführen, hängt von den Berechtigungen für das Team ab.

Der Abschnitt Ihr Teamanforderungen enthält Teamkarten für ausstehende Anforderungen, falls vorhanden.

Der Abschnitt „Ihre Teams“ enthält Karten mit Informationen zu einem bestimmten Team, z. B. Status des Teams, Name des Teams, Manager, E-Mail-Adresse des Teams, Name und Dauer der aktuellen Schicht und primärer Beantworter. Weitere Informationen finden Sie unter Details Ihres SRM-Teams verwalten.

SRM-Teams hinzufügen

Fordern Sie die Erstellung eines Teams an, um mit der Überwachung Ihrer Services zu beginnen. Teams sind für die Probleme zuständig, die im Zusammenhang mit den zugehörigen Services auftreten.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Der ServiceNow-Systemadministrator kann Teams in Ihrem Arbeitsbereich mit einem anderen Prozess einrichten. Weitere Informationen finden Sie unter Importieren Sie Services zur Verwendung in Service Reliability Management.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie **Teams** ( ) und Add **a team (Team hinzufügen**).
3. Erstellen Sie ein neues Team, oder fügen Sie ein vorhandenes hinzu.

Option	Schritte
Fügen Sie ein neues Team hinzu	**a.** Wählen Sie im Feld **Neu oder vorhanden** die Option **Ich erstelle ein neues Team aus**. **b.** Füllen Sie die Felder des Formulars aus. Weitere Informationen zu den Feldbeschreibungen finden Sie unter Formular zum Erstellen eines Teams. **c.** Wählen Sie **Team hinzufügen**.
Registrieren Sie ein vorhandenes Team	**a.** Wählen Sie im Feld **Neu oder vorhanden** die Option **Ich möchte einer Gruppe Zugriff auf die SRM-App gewähren aus**. **b.** Wählen Sie in der Liste **Team** auswählen ein vorhandenes Team aus. **c.** Wählen Sie **Team hinzufügen**.

Ergebnisse

Wenn die Anforderung genehmigt wird, wird das Team erstellt. Ihr Team wird auf der Teams-Zielseite unter **Ihre Teams**angezeigt.

Nächste Maßnahme

- Details Ihres SRM-Teams verwalten
- Richten Sie Eskalationsrichtlinien für Ihr Team in ein SRM
- Eigene SRM-Rufbereitschaftspläne erstellen
- Teammitglieder zu SRM hinzufügen
- Services verwalten oder Ihrem SRM-Team hinzufügen

Details Ihres SRM-Teams verwalten

Fügen Sie Ihrem Team Mitglieder, Beschreibungen und Kontaktinformationen hinzu, oder bearbeiten Sie diese.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das **Teams** -Symbol ( ).
3. Wählen Sie die Teamkarte aus, deren Details Sie aktualisieren möchten.
4. Aktualisieren Sie im Formular auf der Registerkarte **Details** die Details nach Bedarf.

Feld	Beschreibung
Name	Eindeutiger Name des Teams
Manager	Person, die das Team verwaltet.
Gruppen-E-Mail	E-Mail-Kontakt, dem alle Teammitglieder zugeordnet sind.
Beschreibung	Beschreibung des Teams, die anderen helfen soll, Verantwortlichkeiten, Zweck oder Standort des Teams zu verstehen.

5. Wählen Sie **Speichern**.

Teammitglieder zu SRM hinzufügen

Fügen Sie Ihrem Team nach Bedarf neue Teammitglieder hinzu, um zu planen, zu verwalten, Probleme zu lösen und die Effizienz des Geschäftsbetriebs zu steigern.

Vorbereitungen
Erforderliche Rolle: Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das **Teams** -Symbol ( ).
3. Wählen Sie die zu öffnende Teamkarte aus.
4. Wählen Sie die Registerkarte **Teammitglieder**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie **Hinzufügen**.
6. Wählen Sie im Popup-Fenster aus dem Listenmenü Mitglieder aus, die hinzugefügt werden sollen.

   Hinweis: Die Mitgliederdetails werden aus Benutzerdatensätzen importiert und können nicht bearbeitet werden.

7. Wählen Sie **Hinzufügen**.

Services verwalten oder Ihrem SRM-Team hinzufügen

Fügen Sie einem Incident einen Service hinzu, um die Datenmenge für den Incident zu erhöhen.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das **Teams** -Symbol ( ).
3. Wählen Sie eine Teamkarte aus, um ein beliebiges Team zu öffnen, das Sie anzeigen oder dem Sie einen Service hinzufügen möchten.
4. Wählen Sie auf der Teamseite die Registerkarte **Verwaltete Services**.
   Sie können die Liste der Services exportieren. Weitere Informationen finden Sie unter Listeninformationen in eine Datei exportieren.
5. Wahlweise: Fügen Sie Ihrem Team einen Service hinzu, indem Sie **Hinzufügen**wählen.
6. Fügen Sie einen neuen Service hinzu, oder registrieren Sie einen vorhandenen Service.

Option	Schritte
Fügen Sie einen neuen Service hinzu	**a.** Wählen Sie im Feld **Neu oder vorhanden-die Option Neuen Service in Service Reliability Management erstellen aus**. **b.** Füllen Sie die Felder des Formulars aus. Weitere Informationen zu den Feldbeschreibungen finden Sie unter Formular „Service hinzufügen“.. **c.** Wählen Sie **Weiter**.
Registrieren Sie einen vorhandenen Service	**a.** Wählen Sie im Feld **Neu oder vorhanden-die Option Vorhandene CMDB-Services zu Service Reliability Management zuord-nen**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Schritte
	b. Wählen Sie einen oder mehrere Services aus. **c.** Wählen Sie **Weiter**.

7. Füllen Sie im Schritt Team zuweisen die Felder aus.
   - Wählen Sie im Feld **Serviceverantwortlicher** den Benutzer aus, der für die Services verantwortlich sein soll.
   - Wählen Sie im Feld **Supportgruppe** ein Team aus, das die Services überwachen soll.

   Der Servicedatensatz wurde hinzugefügt.
8. Beenden Sie die Einrichtung Ihres Services, oder führen Sie diesen Schritt später aus.

Option	Schritte
Beenden Sie die Einrichtung Ihres Services	**a.** Wählen Sie **Setup fortsetzen aus**. **b.** Wählen Sie **Integrationen hinzufügen**, und verbinden Sie Ihren Service mit einer Datenquelle, um Ereignisse zu überwachen. **c.** Wählen Sie **SLO und SLI hinzufügen** aus, erstellen Sie ein Servicelevel-Ziel und messen Sie Ihre Serviceintegrität mit einem Servicelevel-Indikator.
Später erledigen	Wählen Sie **Später erledigen**aus.

Informationen zu den Service- und Abschlussschritten für das Setup finden Sie unter SRM-Servicedetails bearbeiten und Formular „Servicedetails“ bearbeiten.

Eigene SRM-Rufbereitschaftspläne erstellen

Richten Sie einen Rufbereitschaftszeitplan für Ihr Team ein, damit ein Teammitglied verfügbar ist, das schnell auf Incidents und kritische Warnungen reagieren kann. In Rufbereitschaftszeitplänen wird festgelegt, wer zu einem bestimmten Zeitpunkt Rufbereitschaft hat bzw. verfügbar ist.

Vorbereitungen

Erforderliche Rolle: Manager, Beantworter, Administrator

Warum und wann dieser Vorgang ausgeführt wird

Mit Schichten können Sie in SRM für Ihr in Schichten arbeitendes Personal variable Zeiträume definieren. Erstellen Sie Schichten für bestimmte Tage und Zeiten, zu denen Sie eine Abdeckung benötigen, und weisen Sie sie den Teammitgliedern zu.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Verwenden Sie eine der folgenden Methoden, um ein Team auszuwählen:
   - Wählen Sie auf der Seite „Teams“ ( ) eine Teamkarte aus.
   - Wählen Sie auf der Seite **Zeitpläne** ( ) die Registerkarte **Rufbereitschaftszeitpläne**. Diese Ansicht zeigt Ihr ausgewähltes Team. Um nach einem anderen Team zu suchen, geben Sie den Teamnamen in die Suchleiste ein.
3. Zeigen Sie den Teamkalender an.
4. Richten Sie Ihren Schichtzeitplan ein, indem Sie **Create shift (Schicht erstellen)**wählen.
5. Wählen Sie im Dialogfeld „Neu erstellen“ entweder **Neu erstellen** oder **Vorlage verwenden aus**.
   Ihr Systemadministrator kann vordefinierte Schichtvorlagen erstellen, die Sie zum Erstellen Ihrer Schichten verwenden können.
6. Füllen Sie die Felder im Formular „Create a shift“ (Schicht erstellen) aus.
   Weitere Informationen zu den Feldbeschreibungen finden Sie unter Erstellen Sie ein Schichtformular in Service Reliability Management.
7. Wählen Sie **Create shift (Schicht erstellen)**.

Teameinstellungen für Rufbereitschaft in SRM festlegen

Legen Sie Rufbereitschaftseinstellungen für Teammitglieder fest, um die Effizienz Ihres Geschäftsbetriebs zu steigern.

Vorbereitungen
Erforderliche Rolle: Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das **Teams** -Symbol ( ).
3. Wählen Sie die zu öffnende Teamkarte aus.
4. Wählen Sie die Schaltfläche **Teameinstellungen für Rufbereitschaft**.
5. Füllen Sie die Felder des Formulars aus.

Feld	Beschreibung
Schichtmanager in Rufbereitschaft	Teammanager für die Rufbereitschafts-schicht.
PTO-Anforderungen	Von Teammitgliedern gestellte bezahlte Ab-wesenheit (bezahlter Urlaub) Die Auswahl-möglichkeiten lauten wie folgt: ◦ Systemstandard (nicht zulässig) ◦ Mit Genehmigung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Ohne Genehmigung ◦ Nicht zulässig
Erster Wochentag	Erster Tag Ihrer Arbeitswoche. **Hinweis:** Diese Option ist nur für Washington DC und spätere Releases verfügbar.
Überschneidung von Schichtzeitplänen zulassen	Option, um zuzulassen, dass sich Zeitpläne überschneiden
Eskalationsregel bei Schichtüberschneidung	Die Auswahlmöglichkeiten lauten wie folgt: ◦ Systemstandard (An alle Schichten eskalieren) ◦ An ausgehende Schicht eskalieren ◦ An eingehende Schicht eskalieren ◦ An alle Schichten eskalieren

6. Wählen Sie **Speichern**.

Richten Sie Eskalationsrichtlinien für Ihr Team in ein SRM

Richten Sie eine Eskalationsrichtlinie für Ihr Team ein, um sicherzustellen, dass Warnungen oder Incidents vom entsprechenden Teammitglied rechtzeitig gelöst werden.

Vorbereitungen

Bevor Sie eine Eskalationsrichtlinie erstellen, müssen Sie eine Rufbereitschaftsschicht für Ihr Team erstellen.

Hinweis: Nur der Beantworter, der das Team erstellt hat, und der Manager des Teams können Eskalationsrichtlinien für das einrichten.

Erforderliche Rolle: Beantworter, Manager oder Administrator

Warum und wann dieser Vorgang ausgeführt wird

Eine Eskalationsrichtlinie ist ein Satz von Richtlinien, der beschreibt, wie und wann Incidents auf höhere Autoritätsebenen übertragen werden sollten. Sie definiert klare Verfahren und Verantwortlichkeiten für die Eskalation, damit Beantworter Probleme umgehend beheben können. Sie definiert die Reihenfolge, in der Benachrichtigungen eskaliert werden sollen, wenn eine Warnung oder ein Incident nicht innerhalb einer bestimmten Zeitspanne bestätigt oder gelöst wird. Wenn niemand antwortet, basiert die Eskalation auf Ihren definierten Richtlinien, bis jemand antwortet. Nachdem ein Teammitglied geantwortet hat, wird die Eskalation gemäß der Eskalationsrichtlinie beendet, und es werden keine weiteren Benachrichtigungen gesendet.

Hinweis: Der Eskalations-Workflow wird nur ausgelöst, wenn eine aktive Schicht vorhanden ist.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das **Teams** -Symbol ( ).
3. Wählen Sie die Registerkarte **Eskalationsauslöser und -richtlinien**.
4. Wählen Sie im linken Bereich von **Eskalationsrichtlinien** die Option **Richtlinie erstellen**.
5. Füllen Sie die Felder im Formular „Eskalationsrichtlinie“ aus.
   Weitere Informationen finden Sie unter Richten Sie das Formular für Eskalationsrichtlinien in ein SRM
6. Wahlweise: Wählen Sie **Eskalationsschritt hinzufügen** aus, um die zusätzlichen Schritte für die Eskalation und den Eskalationspfad zu definieren.
   Weitere Informationen zum Formular „Eskalationsschritt hinzufügen“ finden Sie unter Richten Sie das Formular für Eskalationsrichtlinien in ein SRM.
7. Wählen Sie **Änderungen speichern**.
8. Wahlweise: Fügen Sie dem Team eine weitere Eskalationsrichtlinie für eine andere Kategorie von Warnungen oder Incidents hinzu, indem Sie **Richtlinie hinzufügen**wählen.

Eskalationsauslöser in SRM

Lösen Sie eine Eskalationsrichtlinie für das zugehörige Team aus.

Vorbereitungen

Erforderliche Rolle: Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*.
   Sie gelangen zur Homepage SRM – Homepage.

Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das **Teams** -Symbol ( ).
3. Wählen Sie die Registerkarte **Eskalationsauslöser und -richtlinien**.
4. Wählen Sie im linken Bereich unter **Eskalationsauslöser** die Option **Creat trigger (Auslöser erstellen)** aus.
5. Füllen Sie die Felder im Formular „Eskalationsauslöser“ aus.

Formular „Eskalationsauslöser“

Feld	Beschreibung
Name des Eskalationsauslösers	Name des Auslösers.
Aktiv	Option zum Aktivieren oder Deaktivieren des Auslösers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Auftrag	Reihenfolge der Ausführung. Wenn in einem Team mehrere Eskalationsauslöser vorhanden sind, wird zuerst der mit der niedrigeren Auftragsnummer geprüft.
Bedingungen	Bedingungen für den Auslöser. Wählen Sie eine Tabelle und einen Bedingungssatz aus. Wenn die Bedingungen erfüllt sind, werden Eskalationsauslöser für Schichten im SRM-Team ausgelöst.

6. Wählen Sie **Änderungen speichern**.

Hinweis: Wenn ein neuer oder aktualisierter Datensatz für ein Team mit einem Eskalationsauslöser erstellt wird, der der Bedingung des Datensatzes entspricht (z. B. Priorität 1), sollte der Eskalationsauslöser aktiviert werden, und die Eskalationsrichtlinie des Teams sollte wirksam werden. Diese Funktionalität ist jedoch nicht verfügbar.

Sie können auch Unterstützung für Eskalationsauslöser hinzufügen, die bei Bedarf für Warnungen (anstelle von Incidents) ausgeführt werden. Sie können bis zu 5.000 Ereignisse oder 250 Warnungen pro Sekunde hinzufügen. Um die Unterstützung für Rufbereitschaft für Warnungen hinzuzufügen, führen Sie entweder XML für die Auslösertabelle trigger_rule_table_cfg aus, oder erstellen Sie den Datensatz manuell auf der Seite Konfiguration der Auslöserregeltabelle.

Mit SRM-Zuverlässigkeitsaufgaben arbeiten

Warnungen, Incidents und Change-Anforderungen sind Zuverlässigkeitsaufgaben. SRM hilft Ihnen, Ihre Warnungen von der Erstellung bis zur Lösung während des gesamten Antwortlebenszyklus bei der Verwaltung Ihrer Warnungen zu unterstützen.

Der Bereich Zuverlässigkeitsaufgaben ( ) enthält mehrere Registerkarten:

- **Incidents** werden manuell oder basierend auf Servicelevel-Zielen (Service Level Objectives, SLOs) und Servicelevel-Indikatoren (SLIs) erstellt. Weitere Informationen zu Incidents finden Sie unter In SRM mit Incidents arbeiten. Weitere Informationen zu SLO-, SLI- und Fehlerbudgetaktionen finden Sie unter Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien.
- **Changes** können innerhalb von SRMerstellt werden. Weitere Informationen finden Sie unter Change-Aufgabe in SRM manuell erstellen.

Der Bereich Express-Liste ( ) bietet eine fokussierte Ansicht von Warnungen, mit der Sie Integritätsprobleme effizient überwachen, bewerten und lösen können. Sie können Warnungen über die Serviceseiten von SRM oder mithilfe von -Integrationen erstellen. Weitere Informationen zu Warnungen finden Sie unter Express-Liste in Service Operations-Arbeitsbereich für ITOM und SRM-Warnungen manuell erstellen.

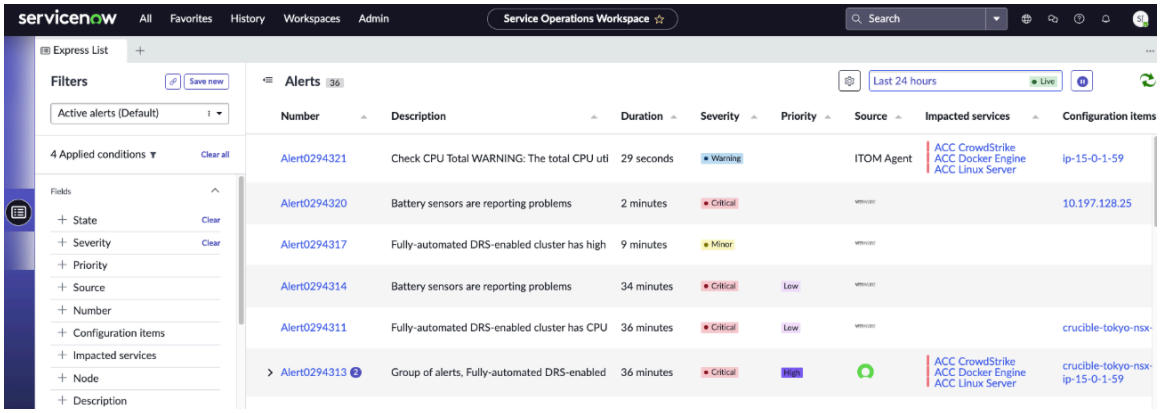
Beantworter und höhere Rollen werden basierend auf ihren Benachrichtigungseinstellungen über Aktualisierungen von Zuverlässigkeitsaufgaben benachrichtigt.

Arbeiten mit Warnungen in SRM

Überwachen, bewerten und beheben Sie Integritätsprobleme in der Express-Liste.

Die Ereignismanagement-Express-Liste bietet eine anpassbare, sortierbare Ansicht für den Zugriff auf und die Verwaltung von Warnungen. Verwenden Sie die Express-Listenfunktion, um Warnungen zu priorisieren, ihre Auswirkungen zu verstehen und Probleme schneller zu lösen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Als Benutzer vom Typ Service Reliability Management (SRM) verfügen Sie automatisch über die Rolle evt_team_operator, mit der Sie auf die Express-Listenfunktion zugreifen können ( ). Weitere Informationen zu dieser Rolle finden Sie unter Von verwendete Rollen Express-Liste.

Rufen Sie Folgendes auf, um mit Warnungen in der Express-Listenfunktion zu arbeiten:

- Bestätigen Sie angezeigte Warnungen in Express-Liste
- Weisen Sie Warnungen in zu Express-Liste
- Schließen Sie eine Warnung in Express-Liste
- Erstellen Sie einen Incident aus einer Warnung in Express-Liste
- Eingehende Warnungen überwachen
- Warnungen in den Status „Bestätigt“ versetzen
- Warnungen in den Status „Wartung“ versetzen

In SRMerstellen Integrationen Warnungen, oder Sie erstellen Warnungen manuell. Unter dem folgenden Link erfahren Sie, wie Sie auf der Seite **„Services“** eine -Warnung erstellen:

SRM-Warnungen manuell erstellen

Erstellen Sie eine Warnung zu Testzwecken oder wenn Sie der Meinung sind, dass ein Problem ein Risiko darstellt.

Vorbereitungen

Erforderliche Rolle: srm_admin, srm_manager oder srm_responder

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie im Navigationsbereich **Services**aus.
3. Wählen Sie den Service aus, für den Sie eine Warnung auslösen möchten.
4. Wählen Sie die Registerkarte **Zugehörige Warnungen**.
5. Wählen Sie **Trigger alert (Warnung** auslösen), und füllen Sie das Formular **Trigger an alert (Warnung** auslösen) aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um eine Warnung auszulösen, müssen Sie zuerst ein Ereignis erstellen, das verarbeitet wird. Nur **Service** ist erforderlich.

Eine Warnung auslösen

Feld	Beschreibung
Service	Wählen Sie einen Service für das Ereignis aus.
Quelle	Manuell.
Knoten	Geben Sie den Namen des Knotens (z. B. FQDN, IP-Adresse oder MAC-Adresse) ein, der dem Ereignis zugeordnet ist.
Typ	Geben Sie den Typ des Ereignisses ein.
Ressource	Geben Sie eine Knotenressource (Prozess oder Service) ein, die dem Ereignis zugeordnet ist.
Metrikname	Geben Sie den Namen der Metrik ein, die dem Ereignis zugeordnet ist.
Quellinstanz	Geben Sie eine Datenquelle für das Ereignis ein.
Nachrichtenschlüssel	Geben Sie einen Bezeichner für mehrere Ereignisse ein, die sich auf dasselbe Ereignis beziehen.
Schweregrad	Wählen Sie die erwarteten Auswirkungen dieses Ereignisses aus. Die Auswahlmöglichkeiten lauten wie folgt: ◦ Kritisch: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. ◦ Schwerwiegend: Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung wurde beeinträchtigt. ◦ Geringfügig (Standard): Ein partieller, nicht kritischer Verlust der Funktionalität oder eine Leistungsverschlechterung ist aufgetreten. ◦ Warnung: Aufmerksamkeit ist erforderlich, obwohl die Ressource noch funktionsfähig ist. ◦ OK: Die Ressource ist weiterhin funktionsfähig.
Zeit des Ereignisses	Wählen Sie das Datum und die Uhrzeit des Auftretens des Ereignisses im Quellsystem aus.
Beschreibung	Geben Sie Informationen ein, die das Ereignis beschreiben.
Zusätzliche Informationen	Fügen Sie weitere Informationen hinzu, die für das Ereignis relevant sind.
Verarbeitungsnotizen	Geben Sie relevante Verarbeitungsinformationen ein.

6. Wählen Sie **Auslöser**.
   Service Reliability Management (SRM) erstellt ein Ereignis, um die Warnung zu generieren. Aktualisieren Sie den Bildschirm, um die Ergebnisse der Event-Verarbeitung anzuzeigen.

   Die Express-Liste zeigt Ihre Warnung automatisch an. Wenn diese Option aktiviert ist, löst SRM die entsprechenden Automatisierungen und Workflows für die Rufbereitschaftseskalation aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Erwägen Sie, zu Testzwecken oder für die Teamzusammenarbeit die folgenden optionalen Anpassungen an Ihrer Warnung vorzunehmen:

- Bestätigen Sie die Warnung, oder weisen Sie sie jemandem in Ihrem Team zu.
- Fügen Sie im Bereich **Verfassen** Kommentare oder Arbeitsnotizen hinzu.
- Fügen Sie über das Anhangsymbol einen Anhang im Zusammenhang mit der Warnung hinzu.

In SRM mit Incidents arbeiten

Planen Sie Serviceunterbrechungen im Voraus, und lassen Sie SRM Benachrichtigungen senden und Status erstellen, wenn Incidents auftreten. Ablenkungen werden minimiert, und der Fokus der Teams liegt stärker auf der Behebung von Problemen.

Sie können Incidents in SRM manuell erstellen oder eine Fehlerbudgetaktion dazu erstellen. Weitere Informationen finden Sie unter SRM-Incidents manuell erstellen und Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien.

- Manuelle Erstellung aus einer Warnung.
- Manuelle Erstellung über die Incident-Ansicht.
- Automatisch aus Warnungsautomatisierungen, wenn die gleichnamige App installiert ist.

Das Feld **Zugewiesen an** für einen Incident legt fest, wer benachrichtigt werden soll. Wenn ein Team als Beantworter ausgewählt ist, werden Teamautomatisierungen überprüft, um zu bestimmen, welcher Zeitplan für die Benachrichtigungen verwendet werden soll.

Hinweis:

Das Feld **Zugewiesen an** wird gelöscht, wenn das Feld **Assigned-team (Zugewiesenes Team)** oder **Service** eines Incident aktualisiert wird. Eskalationsrichtlinien für neu zugewiesene Teams werden ausgeführt. Das Feld bleibt leer, bis ein Benutzer des neuen Teams eine Eskalationsbenachrichtigung bestätigt.

Wenn der Service geändert wird und dem neuen Service kein Team zugewiesen ist, finden keine Änderungen statt.

Durch das Löschen eines Service werden dessen Integrationen, Warnungen, Incidents und Automatisierungen entfernt. Das Löschen eines Service kann nicht wiederhergestellt werden. Erwägen Sie daher, stattdessen den Service zu deaktivieren.

Beantworter und höhere Rollen werden basierend auf ihren Benachrichtigungseinstellungen über Aktualisierungen von Incidents benachrichtigt. Wenn Sie die Aktualisierung vorgenommen haben, werden Sie nicht benachrichtigt.

Sie können Incidents lösen, indem Sie bestimmte Incidents auswählen oder mit einer Mehrfachauswahl arbeiten. Beachten Sie dazu SRM-Incidents lösen, SRM-Incidents schließen oder SRM-Incidents abbrechen.

Hinweis:

Incidents mit dem Status **Gelöst** werden nach 3 Tagen automatisch geschlossen.

Weitere Informationen zu den Bereichen und Feldern, die in einem Incident verfügbar sind, finden Sie unter SRM Incidents.

Listeninformationen in eine Datei exportieren in der Listenansicht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Reagieren Sie auf einen Incident wie folgt:

- Markieren Sie einen Incident.
- Priorität eines SRM-Incident aktualisieren.
- Legen Sie den Incident-Status fest.
- SRM-Incidents kopieren.
- Services zu einem SRM-Incident hinzufügen.
- SRM Incidents.
- SRM-Incidents lösen.
- SRM-Incidents abbrechen.
- SRM-Incidents schließen.
- SRM-Incidents erneut öffnen.

SRM-Incidents manuell erstellen

Erstellen Sie einen Incident, wenn ein Problem Ihrer Meinung nach ein erhebliches Risiko darstellt und so bald wie möglich behoben werden muss.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte Incidents aus.
4. Wählen Sie **Neu**.
5. Füllen Sie die entsprechenden Felder im Formular „Neuen Incident erstellen“ aus.

   Nur das Feld **Kurzbeschreibung** ist erforderlich.

Incident-Feldzuordnung

Feld	Beschreibung
Kurzbeschreibung	Fügen Sie eine kurze Beschreibung des Incident hinzu.
Beschreibung	Fügen Sie eine detaillierte Beschreibung des Incident hinzu.
Nummer	Bezeichner, der dem Incident zugewiesen ist.
Auswirkung	Die Auswahl ist ein Maß für die Auswirkung des Incident. Die Auswirkung wirkt sich auf die **Priorität** aus. Die Auswahlmöglichkeiten lauten wie folgt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ 1 - Hoch ◦ 2 – Mittel ◦ 3 - Niedrig
Zuweisungsgruppe	Wählen Sie durch Eingabe oder Suche ein Team aus, das an dem Incident arbeiten soll.
Priorität	Wird automatisch basierend auf **Auswirkung** und **Dringlichkeit** festgelegt. Gibt an, wie schnell der Incident behandelt werden soll. Beachten Sie dazu die Tabelle **Regeln für Datensuche mit Priorität** unten. Werte sind: ◦ 3 - Mittel ◦ 4 – Niedrig ◦ 5 - In Planung
Kategorie	Wählen Sie eine Kategorie für den Incident aus. Die Auswahlmöglichkeiten lauten wie folgt: ◦ – Keine Angabe – ◦ Anforderung/Hilfe (Standard) ◦ Software ◦ Hardware ◦ Netzwerk ◦ Datenbank
Dringlichkeit	Wählen Sie einen Maß dafür, wie lange die Lösung hinausgeschoben werden kann, bis ein Incident erhebliche Geschäftsauswirkungen hat. Die Dringlichkeit wirkt sich auf die **Priorität** aus.
Service	Wählen Sie einen Service aus, der dem Incident zugeordnet ist.
Schweregrad	Wählen Sie durch Eingabe oder Suche einen Schweregrad aus, der dem Incident zugeordnet werden soll. Die Auswahlmöglichkeiten lauten wie folgt: ◦ 1 - Hoch ◦ 2 – Mittel ◦ 3 - Niedrig
Konfigurationselement	Wählen Sie durch Eingabe oder Suche ein Asset aus, das dem Incident zugeordnet werden soll.
Zugewiesen an	Weisen Sie durch Eingabe oder Suche ein Teammitglied zu, das an dem Incident arbeiten soll.
Status	Wählen Sie einen Status für den Incident aus. Die Auswahlmöglichkeiten lauten wie folgt: ◦ Neu (Standard) ◦ In Bearbeitung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Angehalten ◦ Gelöst ◦ Abgebrochen Weitere Informationen finden Sie unter Status von SRM-Incidents.
Beobachtungsliste	Wählen Sie durch Eingabe oder Suche Einzelpersonen aus, die an dem Incident arbeiten sollen.
Lösungscode	Wählen Sie (falls vorhanden) einen Lösungscode aus. Die Auswahlmöglichkeiten lauten wie folgt: ◦ Keine (Standard) ◦ Duplikat ◦ Known Error ◦ Keine Lösung bereitgestellt ◦ Von Anrufer gelöst ◦ Gelöst durch Change ◦ Gelöst durch Problem ◦ Gelöst durch Anforderung ◦ Lösung bereitgestellt
Lösungsnotizen	Geben Sie alle relevanten Lösungsinformationen ein.

Hinweis: Die Priorität wird anhand der folgenden Beispielregeln für die Datensuche berechnet:

Regeln für Datensuche mit Priorität

Auswirkung	Dringlichkeit	Priorität
1 – Hoch	1 – Hoch	1 - Kritisch
1 – Hoch	2 – Mittel	2 – Hoch
1 – Hoch	3 – Niedrig	3 – Mittel
2 – Mittel	1 – Hoch	2 – Hoch
2 – Mittel	2 – Mittel	3 – Mittel
2 – Mittel	3 – Niedrig	4 – Niedrig
3 – Niedrig	1 – Hoch	3 – Mittel
3 – Niedrig	2 – Mittel	4 – Niedrig
3 – Niedrig	3 – Niedrig	5 - In Planung

6. Wählen Sie **Speichern**.
   Der Incident wird erstellt, und das Formular für einen neuen Incident wird angezeigt.

7. Fügen Sie im Bereich **Aktionen** mithilfe des Symbols „ **Anhänge** “ einen Anhang hinzu, der sich auf den Incident bezieht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Erstellen Sie mit dem Vorlagensymbol eine Incident-Vorlage.
9. Starten Sie im Bereich **Zusammenarbeit** ein Zoom-Meeting, Microsoft Teams oder einen Slack-Kanal, oder nehmen Sie daran teil..
10. Wählen Sie **Speichern**.
    Der Incident wird in Kommentaren, Arbeitsnotizen und Incident-Aktivitäten angezeigt, die im **Aktivitätenstrom** erfasst werden. Weitere Informationen zu Incident-Feldern finden Sie unter SRM Incidents.

SRM-Incidents neu zuweisen

Weisen Sie einen Incident einem Beantworter neu zu, wenn die Incident-Aufgaben von einem bestimmten Teammitglied bearbeitet werden sollen.

Vorbereitungen

Diese Aktion ist verfügbar, wenn das Feld **Zugewiesen an** im Incident ausgefüllt ist.

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte **Incidents** aus.
4. Sie haben zwei Möglichkeiten.

Option	Bezeichnung
Option	Beschreibung
In der Incident-Listenansicht	Doppelklicken Sie auf das Feld **Zugewiesen an** für den Incident, und ersetzen Sie das Teammitglied über das Listenmenü.
Auf der Registerkarte **Details** des Incident-Formulars	Löschen Sie den Namen im Feld **Zugewiesen an**, und weisen Sie ihn neu zu. Wählen Sie **Speichern**.

Der Incident ist jetzt dem neuen Beantworter zugewiesen, dem eine E-Mail-Benachrichtigung zugesendet wird. Der Beauftragte wird in der Listenansicht und im Formular angezeigt.

Priorität eines SRM-Incident aktualisieren

Wenn die Priorität eines Incident geändert werden soll, können Sie sie manuell auf die neue Relevanz aktualisieren.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte **Incidents** aus.
4. Wählen Sie in der Ansicht „Incident-Liste“ im Listenmenü einen Wert für **Priorität** aus.
   - 1 – Kritisch
   - 2 – Hoch
   - 3 – Mittel
   - 4 – Niedrig
   - 5 – Planung (Standard)
5. Wählen Sie **OK**.
   Die neue Priorität wird in der Incident-Listenansicht, im Incident-Header und im Formularfeld angezeigt.

Services zu einem SRM-Incident hinzufügen

Fügen Sie einem Incident einen Service hinzu, um die Datenmenge für den Incident zu erhöhen.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Sie haben zwei Möglichkeiten.

Option	Beschreibung
In der Incident-Listenansicht	Doppelklicken Sie auf das Feld **Service** für den Incident, und ersetzen Sie das Teammitglied mithilfe der Suche. Wählen Sie **OK**.
Im Incident-Formular	Wählen Sie einen neuen Wert für **Service** aus dem Listenmenü aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Beschreibung
	Wählen Sie **Speichern**.

Informationen zur Werteauswahl finden Sie unter SRM Incidents.
Der neue Service wird in der Incident-Listenansicht und im Incident-Formular angezeigt.

SRM-Incidents Lösungscodes und -hinweise hinzufügen

Fügen Sie einem Incident einen Lösungscode und -hinweise hinzu, wenn Sie den Incident gelöst haben.

Vorbereitungen
Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Öffnen Sie den Incident.
4. Wählen Sie im Bereich **Details** des Incident einen **Lösungscode** aus dem Listenmenü aus.
5. Geben Sie Text in das Textfeld **Lösungshinweise** ein.
   Die Lösungshinweise werden im Zeitleistenbereich **Aktivität** angezeigt.
6. Wählen Sie **Speichern**.

SRM-Incidents kopieren

Kopieren Sie einen Incident, wenn Sie ein ähnliches Problem haben.

Vorbereitungen
Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Öffnen Sie den Incident, den Sie kopieren möchten.
4. Wählen Sie im Listenmenü unter der Schaltfläche „Weitere Optionen“ die Option **Incident kopieren** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Listenmenü für das Feld **Anrufer** ein Teammitglied aus.
   Nachdem der Incident kopiert wurde, wird die Zeitleiste **Aktivität** des neuen Incident mit dem ursprünglichen Incident als Arbeitsnotiz aktualisiert.

SRM-Incidents lösen

Lösen Sie einen Incident, wenn dieser überprüft werden muss oder wenn Sie der Meinung sind, dass er bereits bearbeitet wurde, aber noch nicht so weit ist, dass er geschlossen werden könnte.

Vorbereitungen
Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte **Incidents** aus.
4. Sie haben zwei Möglichkeiten.

Option	Schritte
In der Incident-Listenansicht	**a.** Doppelklicken Sie auf das Feld **Status** für den Incident (oder verwenden Sie das Tastaturkürzel), und wählen Sie etwas im Listenmenü aus. **b.** Wählen Sie **OK**.
Im Incident-Formular	**a.** Wählen Sie im Listenmenü einen neuen Wert für das Feld **Status** aus. **b.** Wählen Sie **Speichern**.

Informationen zur Werteauswahl finden Sie unter SRM Incidents.
Der neue Status wird in der Incident-Listenansicht sowie im Incident-Formular und im Formular-Header angezeigt.

Ergebnisse
Gelöste Incidents verbleiben in der Incidents-Listenansicht. Überprüfen Sie Ihre Filter, wenn sie nicht angezeigt werden.

Hinweis:

Wenn Sie einen Incident lösen, bleiben die zugehörigen Warnungen geöffnet, bis Sie den Incident schließen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SRM-Incidents abbrechen

Schließen Sie einen Incident, wenn Sie der Meinung sind, dass es sich nicht um ein Problem handelt oder wenn er bereits behandelt wurde.

Vorbereitungen
Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Öffnen Sie den Incident, den Sie abbrechen möchten.
4. Sie haben zwei Möglichkeiten.

Option	Schritte
In der Incident-Listenansicht	**a.** Doppelklicken Sie auf das Feld **Status** für den Incident (oder verwenden Sie das Tastaturkürzel), und wählen Sie etwas im Listenmenü aus. **b.** Wählen Sie **OK**.
Im Incident-Formular	**a.** Wählen Sie im Listenmenü einen neuen Wert für das Feld **Status** aus. **b.** Wählen Sie **Speichern**.

Informationen zur Werteauswahl finden Sie unter SRM Incidents.
Der neue Status wird in der Incident-Listenansicht sowie im Incident-Formular und im Formular-Header angezeigt.

Ergebnisse
Abgebrochene Incidents verbleiben in der Incidents-Listenansicht. Überprüfen Sie Ihre Filter, wenn sie nicht angezeigt werden.

Hinweis:

Wenn Sie einen Incident abbrechen, werden die zugehörigen Warnungen geschlossen.

SRM-Incidents schließen

Schließen Sie einen Incident, wenn Sie der Meinung sind, dass es sich nicht um ein Problem handelt oder wenn er bereits behandelt wurde.

Vorbereitungen
Erforderliche Rolle: Beantworter, Manager oder Administrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Sie haben zwei Möglichkeiten.

Option	Schritte
In der Incident-Listenansicht	**a.** Doppelklicken Sie auf das Feld **Status** für den Incident (oder verwenden Sie das Tastaturkürzel), und wählen Sie etwas im Listenmenü aus. **b.** Wählen Sie **OK**.
Im Incident-Formular	**a.** Wählen Sie im Listenmenü einen neuen Wert für das Feld **Status** aus. **b.** Wählen Sie **Speichern**.

Informationen zur Werteauswahl finden Sie unter SRM Incidents.
Der neue Status wird in der Incident-Listenansicht sowie im Incident-Formular und im Formular-Header angezeigt.

Ergebnisse

Geschlossene Incidents verbleiben in der Incidents-Listenansicht. Überprüfen Sie Ihre Filter, wenn sie nicht angezeigt werden.

Hinweis:

Wenn Sie einen Incident schließen, werden die zugehörigen Warnungen geschlossen.

SRM-Incidents erneut öffnen

Öffnen Sie einen geschlossenen Incident erneut, wenn Sie denken, dass das Problem noch nicht gelöst wurde.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wählen Sie in der primären Navigation das Symbol **für Zuverlässigkeitsaufgaben** ( ).
3. Suchen und öffnen Sie den Incident, den Sie erneut öffnen möchten.
   Überprüfen Sie Ihre Filter, wenn sie nicht angezeigt werden.
4. Sie haben zwei Möglichkeiten.

Option	Schritte
In der Incident-Listenansicht	**a.** Doppelklicken Sie auf das Feld **Status** für den Incident (oder verwenden Sie das Tastaturkürzel), und wählen Sie etwas im Listenmenü aus. **b.** Wählen Sie **OK**.
Im Incident-Formular	**a.** Wählen Sie im Listenmenü einen neuen Wert für das Feld **Status** aus. **b.** Wählen Sie **Speichern**.

Informationen zur Werteauswahl finden Sie unter SRM Incidents.
Der neue Status wird in der Incident-Listenansicht sowie im Incident-Formular und im Formular-Header angezeigt.

Change-Aufgabe in SRM manuell erstellen

Erstellen Sie eine Change-Aufgabe, um einen kontrollierten Prozess zum Ändern genehmigter und unterstützter Aktionen für SRM zu implementieren.

Vorbereitungen

Allgemeine Informationen zu Change-Anforderungen finden Sie unter Arbeiten mit Change-Management .

Erforderliche Rolle: Beantworter, Manager oder Administrator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie **Zuverlässigkeitsaufgaben** ( ).
3. Wählen Sie die Registerkarte **Changes**.
4. Wählen Sie im Header der Liste **Changes** die Option **Neu**.
5. Suchen Sie im Fenster **Einen Change auswählen** nach einem Change-Datensatz, oder wählen Sie eine SOW-Karte zur Change-Erstellung aus, um den Typ der Change-Anforderung auszuwählen.
6. Wählen Sie **Weiter**.
7. Füllen Sie auf der Registerkarte Details des Formulars die Felder in den Formularen **Change-Anforderung**, **Auswirkung**, **Zuweisung**, **Planung**, **Zeitplan**, **Notizen**und **Abschlussinformationen** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Erstellen Sie Change-Anforderungsformulare.

8. Wahlweise: Wählen Sie **Mir zuweisen**.
9. Wählen Sie **Speichern**.

   Die Change-Anforderung wird erstellt, und für die Anforderung wird die Registerkarte **Zugehörige Datensätze** angezeigt.

10. Wahlweise: Sie können die folgenden Schritte im **Status**-Workflow ausführen.

    (Optional) Wenn für die Change-Anforderung eine Genehmigung erforderlich ist, wird die Schaltfläche **Genehmigung anfordern** angezeigt. Wählen Sie **Genehmigung anfordern**. Der **Status** wechselt zu **Bewerten**. Anweisungen zum Genehmigen von Change-Anforderungen finden Sie unter Change-Anforderungen zur Genehmigung von SRM-Teams genehmigen.

    Wenn die Change-Anforderung vorab genehmigt wurde oder keine Genehmigung erforderlich ist, können Sie den **Status** in **Geplant**ändern.

    Nach der Genehmigung und Planung können Sie **Implementieren** wählen, um die Change-Anforderung in die Tat umzusetzen.

    Sobald die Change-Anforderung implementiert wurde, prüfen Sie die Details, und wählen Sie „Überprüfen“. Die Change-Anforderung wechselt in den Status **Überprüfen**.

    Hinweis: Alle offenen Change-Aufgaben werden auf **Abgebrochen** gesetzt.

    Weitere Informationen zum **Status** von Change-Anforderungen finden Sie unter Status von SRM-Change-Anforderungen.

Arbeiten mit Warnungsautomatisierungen für SRM .

Warnungsautomatisierungen enthalten bedingte Auslöser für die Gruppierung und Verwaltung von Warnungen, die basierend auf dem Inhalt der Warnung automatisch Antwortaktionen ausführen.

In SRM wird eine Warnung erstellt, wenn das Überwachungstool eines Drittanbieters ein Event registriert. Das System analysiert eingehende Warnungen einmal pro Minute und führt entsprechend Automatisierungen aus.

Hinweis: Bevor Sie Warnungsautomatisierungen erstellen, müssen Sie die Anwendung Service Reliability Management installieren und konfigurieren, die unter ServiceNow Storeverfügbar ist. Weitere Informationen finden Sie unter Service Reliability Management.

Gruppierungsautomatisierungen

Verwenden Sie Automatisierungen für die Warnungsgruppierung, um ähnliche Warnungen zu gruppieren und das Rauschen in Ihrer Warteschlange zu reduzieren. Gruppierungsautomatisierungen sind Routing, das Ihnen hilft, nach bestimmten Bedingungen zu kategorisieren. Jede Automatisierung kombiniert eine Reihe von Filtern und Methoden basierend auf Feldern oder Bedingungsübereinstimmungen.

Hinweis: Alle Gruppierungen erfolgen, bevor Verwaltungsautomatisierungen ausgeführt werden.

Systemautomatisierungen für die automatische Gruppenerstellung können enthalten sein, wenn Ihr System bereitgestellt wird. Sie sind standardmäßig aktiv.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie die Gruppierungsautomatisierungen an, indem Sie von Ihrer **Homepage** zum Modul **Warnungsautomatisierungen** navigieren. Wählen Sie im linken Bereich **Gruppierung** aus.

Erstellen Sie Gruppierungsautomatisierungen basierend auf beliebigen Kriterien, die in den Feld- oder Bedingungsfeldern verfügbar sind.

Hinweis: Bevor Sie Gruppierungsautomatisierungen erstellen, sollten Teams, Zeitpläne und Integrationen eingerichtet sein.

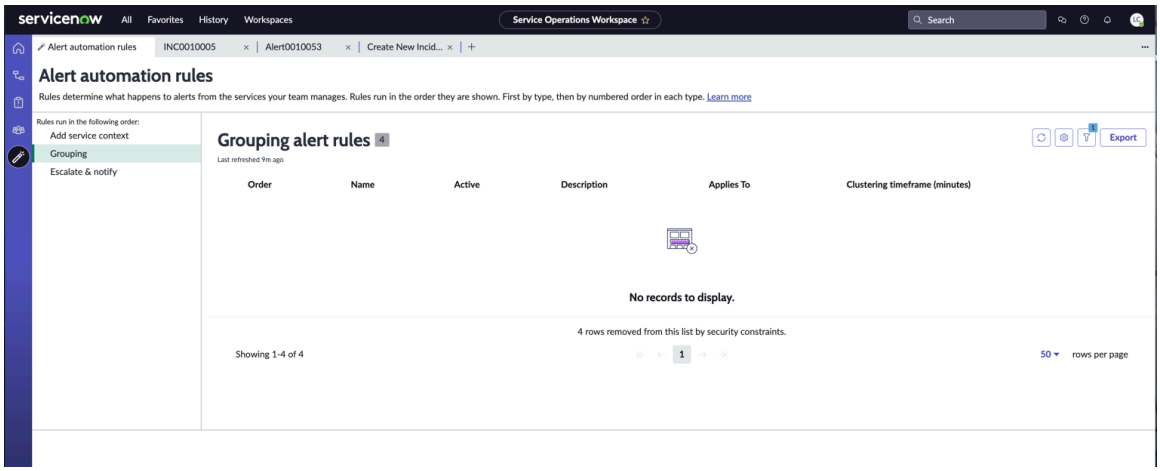
Automatisierungen werden nur einmal für eine Warnung ausgeführt. Je nachdem, wann die Warnung oder Automatisierung im System erfasst wurde, geschehen unterschiedliche Dinge.

- Wenn eine Warnung erstellt wird und Automatisierung 1 die einzige Automatisierung ist, wird sie für diese Warnung nur einmal ausgeführt.
- Wenn Sie die Automatisierungen 2 und 3 hinzufügen, nachdem diese Warnung erstellt wurde, werden sie erst nach Aktualisierung der Warnung ausgeführt. Diese Automatisierungen wurden nie für die Warnung ausgeführt.
- Wenn Sie die Warnung schließen und erneut öffnen, werden alle drei Automatisierungen dafür ausgeführt.

Wenn Sie eine vorhandene Automatisierung ändern, von der eine vorhandene Warnung erfasst worden wäre, ist dem nicht der Fall. Die von Ihnen geänderten Kriterien oder Aktionen werden erst dann berücksichtigt, wenn die vorhandene Warnung geschlossen und erneut geöffnet wird. Dann werden alle geänderten Automatisierungsaktionen durchgeführt.

Gruppierungsautomatisierungen werden in der gewählten Reihenfolge ausgeführt, von der niedrigsten zur höchsten.

Hinweis: Administratoren können jede SRM-Automatisierung aktualisieren, neu anordnen oder löschen. Beantworter und Manager können nur ihre eigenen Automatisierungen oder die ihres Teams aktualisieren und neu anordnen. Nur Administratoren [admin] können globale Automatisierungen löschen.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Die Reihenfolge ist wichtig für die Gruppierung von Automatisierungen, da die Automatisierungen niedrigerer Reihenfolge zuerst ausgeführt werden. Dies kann sich darauf auswirken, ob die Bedingungen von Automatisierungen höherer Ordnung erfüllt sind oder verarbeitet werden. Automatisierungen niedrigerer Ordnung können Feldwerte anpassen oder sogar die Verarbeitung stoppen.

Keine der Filter oder Sortierfunktionen für die Listenansicht ändert die Reihenfolge, in der die Automatisierungen ausgeführt werden.

Die Listenansicht**der Gruppierungsautomatisierungen** enthält Informationen für:

- **Reihenfolge** stellt die Reihenfolge dar, in der die Automatisierungen ausgeführt werden.
- **Name** stellt den Namen und die Beschreibung der Gruppenregel dar.
- **Aktiv** gibt an, ob die Automatisierung ausgeführt wird oder nicht.
- **Beschreibung** beschreibt die Gruppenautomatisierung.
- **Gilt für** die Person, die von dieser Regel betroffen ist. Gibt an, ob die Auswirkung **global** oder auf ein Team ist.
- **Der Clustering-Zeitrahmen (Minuten)** gibt an, wie lange diese Automatisierung nach einer initiierenden Warnung weiter ausgeführt und Warnungen gruppiert werden soll.

Die Ausführungsreihenfolge der Warnungsgruppierung lautet wie folgt:

- Gruppierungsregeln werden ausgeführt
- Manuell erstellte Gruppen werden aktualisiert
- Automatisierte Gruppierungsausführungen

Warnungen werden unter der primären Warnung gruppiert. Die älteste Warnung mit dem höchsten Schweregrad wird zur primären Warnung. Die restlichen werden zu zugehörigen Warnungen. Die Gruppierungsaktivität wird in **den Arbeitsnotizen aufgezeichnet.**.

Hinweis: Administratoren, Manager und Beantworter können nur ihre eigenen Automatisierungen oder die ihres Teams aktivieren oder deaktivieren.

Systemadministratoren [admin] können jede Automatisierung, einschließlich globaler Automatisierungen, aktivieren oder deaktivieren.

Durch das Löschen eines Service werden dessen Integrationen, Warnungen, Incidents und Automatisierungen entfernt. Das Löschen eines Service kann nicht wiederhergestellt werden. Erwägen Sie daher, stattdessen den Service zu deaktivieren.

Eine gruppierte, zugehörige Warnung enthält ein Feld **Gruppiert nach**. Dieses Feld gibt an, wie die zugehörige Warnung gruppiert wurde.

Automatisierungen der Warnungsverwaltung

Verwenden Sie Warnungsverwaltungsautomatisierungen, um Warnungen zuzuweisen und darauf zu reagieren. Sie werden ausgeführt, nachdem alle Gruppierungen stattgefunden haben. Verwaltungsautomatisierungen sind Routing, mit dem Sie Ihre Antwort an bestimmte Bedingungen anpassen können. Jede Automatisierung kombiniert eine Reihe von Filtern und ein Ergebnis. In der Regel wird festgelegt, wer zugewiesen ist, die Priorität festgelegt oder E-Mails, Slack -Kanäle oder Zoom -Meetings erstellt.

Hinweis: Verwaltungsautomatisierungen werden nicht für Incidents ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie die Verwaltungsregeln an, indem Sie von Ihrer **Homepage** zum Modul **Warnungsautomatisierungen** navigieren. Wählen Sie im linken Bereich **Eskalieren und benachrichtigen**.

Erstellen Sie Regeln basierend auf den Kriterien, die in den Bedingungsfilterfeldern verfügbar sind.

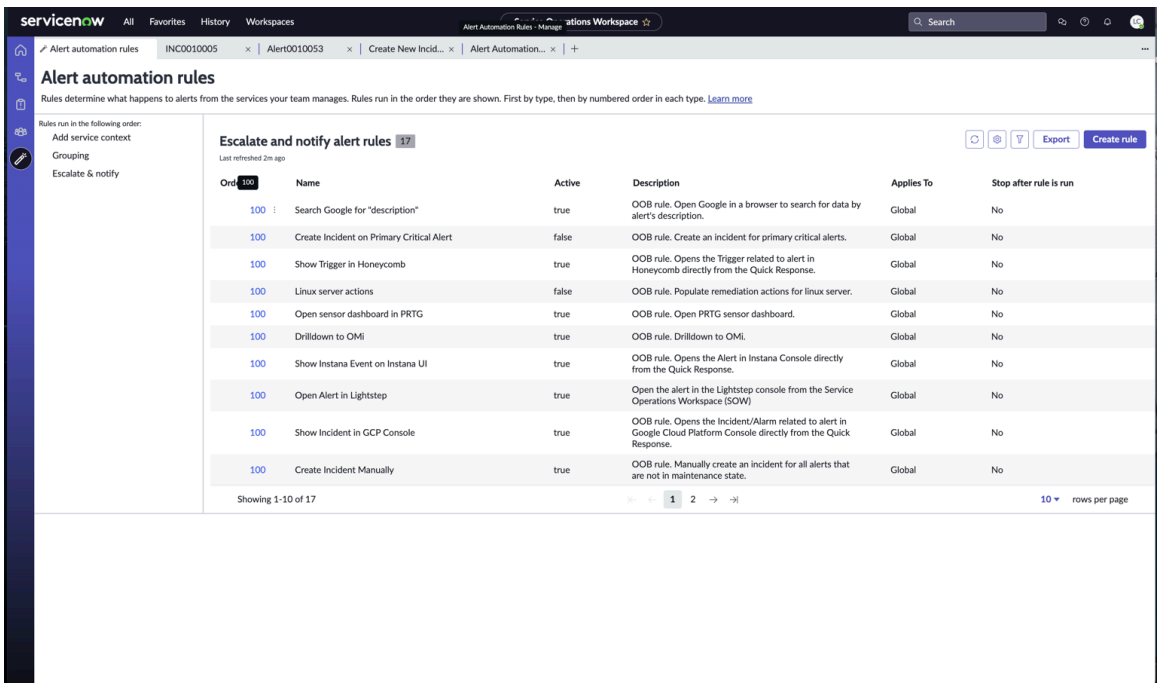
Hinweis: Vor der Erstellung von Verwaltungsautomatisierungen müssen Teams, Zeitpläne und Integrationen SRM von eingerichtet sein.

Automatisierungen werden nur einmal für eine Warnung ausgeführt. Je nachdem, wann die Warnung oder Automatisierung im System erfasst wurde, geschehen unterschiedliche Dinge.

- Wenn eine Warnung erstellt wird und Automatisierung 1 die einzige Automatisierung ist, wird sie für diese Warnung nur einmal ausgeführt.
- Wenn Sie die Automatisierungen 2 und 3 hinzufügen, nachdem diese Warnung erstellt wurde, werden sie erst nach Aktualisierung der Warnung ausgeführt. Diese Automatisierungen wurden nie für die Warnung ausgeführt.
- Wenn Sie die Warnung schließen und erneut öffnen, werden alle drei Automatisierungen dafür ausgeführt.

Wenn Sie eine vorhandene Automatisierung ändern, von der eine vorhandene Warnung erfasst worden wäre, ist dem nicht der Fall. Die von Ihnen geänderten Kriterien oder Aktionen werden erst dann berücksichtigt, wenn die vorhandene Warnung geschlossen und erneut geöffnet wird. Dann werden alle geänderten Automatisierungsaktionen durchgeführt.

Verwaltungsautomatisierungen werden in der gewählten Reihenfolge ausgeführt, von der niedrigsten zur höchsten.



Hinweis: Keine der Filter oder Sortierfunktionen für die Listenansicht ändert die Reihenfolge, in der die Automatisierungen ausgeführt werden.

Das Feld **Reihenfolge** gibt die Reihenfolge an, in der die Automatisierungen ausgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

Die Reihenfolge ist wichtig für Verwaltungsautomatisierungen, da die Automatisierungen niedrigerer Reihenfolge zuerst ausgeführt werden. Dies kann sich darauf auswirken, ob die Bedingungen von Automatisierungen höherer Ordnung erfüllt sind oder verarbeitet werden. Automatisierungen niedrigerer Ordnung können Feldwerte anpassen oder sogar die Verarbeitung stoppen.

Sie können Teamautomatisierungen nicht so neu anordnen, dass sie vor globalen Automatisierungen ausgeführt werden. Wenn eine globale Automatisierung erfüllt ist, wird die gesamte Verarbeitung von Automatisierungen angehalten, sofern die globale Automatisierung entsprechend festgelegt ist.

Die Listenansicht**der Eskalations- und Benachrichtigungsautomatisierungen** enthält Informationen für:

- **Reihenfolge** stellt die Reihenfolge dar, in der die Automatisierungen ausgeführt werden.
- **Name** stellt den Namen und die Beschreibung der Gruppenregel dar.
- **Aktiv** gibt an, ob die Automatisierung ausgeführt wird oder nicht.
- **Beschreibung** beschreibt die Gruppenautomatisierung.
- **Gilt für** die Person, die von dieser Regel betroffen ist. Gibt an, ob die Auswirkung **global** oder auf ein Team ist.
- **Mit „Anhalten nach Automatisierung“** wird festgelegt, ob die Verarbeitung nach dem Ausführen dieser Regel angehalten wird.

Die Aktivität „Verwaltungsregel“ wird in **Arbeitsnotizen**aufgezeichnet.

Hinweis: Manager und Beantworter können nur ihre eigenen Regeln oder die ihres Teams aktivieren, deaktivieren oder löschen.

Administratoren und Systemadministratoren [admin] können jede SRM -Regel aktivieren, deaktivieren und löschen. Nur Systemadministratoren [admin] können globale Automatisierungen aktivieren, deaktivieren oder löschen, und zwar nur in der klassischen Anwenderoberfläche.

Wenn ein Team gelöscht wird, werden seine Automatisierungsregeln entfernt. Dies ist keine wiederherstellbare Aktion. Erwägen Sie daher, das Team zu deaktivieren.

Service Reliability Management – Referenz

Referenzthemen enthalten zusätzliche Informationen zur Verwendung von Service Reliability Management.

SRM Rollen und Zuständigkeiten

Mit Rollen können Sie Benutzern Zugriff auf verschiedene Teile der SRM-Konsole gewähren. Rollen bestimmen die Aktionen, die Benutzer in Service Reliability Managementausführen können.

SRM besitzt die folgenden vordefinierten Rollen:

Hinweis: Die SRM-Experience wurde so optimiert, dass nur die SRM-Rollen vorhanden sind. Zusätzliche Rollen könnten die UI verändern und unbeabsichtigte Folgen haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenliste

Rolle	Aufgaben
SRM-Administrator [srm_admin]	• Aktualisiert einen Service, der von einem beliebigen SRM-Team verwaltet wird • Weisen Sie neue Incidents zu • Incidents erstellen und bearbeiten • Erstellen und bearbeiten Sie Changes • Erstellen Sie Teams • Aktualisieren Sie ein beliebiges SRM-Team • Rufbereitschaftsschichten erstellen und bearbeiten • Rufbereitschaftsschichten löschen • Eskalationsrichtlinien und -auslöser erstellen und bearbeiten • Löschen Sie Eskalationsrichtlinien und -auslöser • Anforderung zur Abdeckung des Zeitplans • Abwesenheit einreichen • Ereignis erstellen
SRM-Manager [srm_manager]	• Aktualisieren Sie einen von Ihrem SRM-Team verwalteten Service • Weisen Sie neue Incidents zu • Incidents erstellen und bearbeiten • Erstellen und bearbeiten Sie Changes • Erstellen Sie Teams • Aktualisieren Sie von Ihnen verwaltete SRM-Teams • Rufbereitschaftsschichten erstellen und bearbeiten • Rufbereitschaftsschichten löschen • Eskalationsrichtlinien und -auslöser erstellen und bearbeiten • Löschen Sie Eskalationsrichtlinien und -auslöser • Anforderung zur Abdeckung des Zeitplans • Abwesenheit einreichen • Ereignis erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollenliste (Fortsetzung)

Rolle	Aufgaben
SRM-Responder [srm_responder]	• Aktualisieren Sie einen Service, wenn Sie sich in der Supportgruppe befinden, die an den Service gebunden ist • Weisen Sie neue Incidents zu • Incidents erstellen und bearbeiten • Erstellen und bearbeiten Sie Changes • Erstellen Sie Teams • Rufbereitschaftsschichten anzeigen • Zeigen Sie Eskalationsrichtlinien und -auslöser an • Kontakteinstellungen bearbeiten • Anforderung zur Abdeckung des Zeitplans • Abwesenheit einreichen • Ereignis erstellen
Administrator [admin]	• Aktualisieren Sie einen von Ihrem SRM-Team verwalteten Service • Löschen Sie Services • Weisen Sie neue Incidents zu • Incidents erstellen und bearbeiten • Erstellen und bearbeiten Sie Changes • Löschen Sie Incidents • Erstellen Sie Teams • Aktualisieren Sie von Ihnen verwaltete SRM-Teams • Rufbereitschaftsschichten löschen • Kontakteinstellungen überschreiben • Warnung manuell erstellen • Löschen Sie Warnungen • Abwesenheit einreichen

Formular zum Erstellen eines Teams

Fordern Sie die Erstellung eines Teams an, um mit der Überwachung Ihrer Services zu beginnen.

Erstellen Sie ein Teamformular

Weitere Informationen finden Sie unter SRM-Teams hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Teamname	Name des Teams.
Teammanager	Manager für das Team.
Team-E-Mail	E-Mail-Kontakt für das Team.
Teammitglieder	Mitglieder für Ihr Team.
Tags	Begriffe, die Ihr Team beschreiben oder sich darauf beziehen.
Kurze Beschreibung der Teamverantwortlichkeiten	Beschreibung Ihres Teams. Beispielsweise die Teamverantwortlichkeiten oder der geografische Standort.

Erstellen Sie ein Schichtformular in Service Reliability Management

Richten Sie für Ihr Team einen Rufbereitschaftszeitplan ein, um sicherzustellen, dass immer die richtige Person verfügbar ist, um schnell auf Incidents und kritische Warnungen zu reagieren.

Erstellen Sie ein Schichtformular

Weitere Informationen finden Sie unter Eigene SRM-Rufbereitschaftspläne erstellen.

Create new shift (Neue Schicht erstellen)

Feld	Beschreibung
Schichtname	Name der Schicht.
All day shift (Ganztägige Schicht)	Wenn diese Option ausgewählt ist, ist die Schicht ganztägig.
Schichtbeginn	Datum und Uhrzeit des Schichtbeginns.
Schichtende	Datum und Uhrzeit des Schichtendes.
Wiederholen	Wiederholung der Schicht. Die Auswahlmöglichkeiten lauten wie folgt: • Nie • Täglich • Wöchentlich
Jede/n/s	Gibt an, wie häufig die Wiederholung erfolgt. Die Anzeige hängt vom ausgewählten Zeitrahmen ab.
Weitere Optionen	Weitere Optionen zum Anpassen Ihres Zeitplans.
Zeitzone	Zeitzone des Anwenders.
Feiertagskalender	Für Feiertage zu verwendender Zeitplan.
Wiederholen bis	Datum und Uhrzeit für das Ende der Wiederholung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schicht mit Schichtvorlage erstellen

Feld	Beschreibung
Schichtname	Name der Schicht.
Template/Schedule (Vorlage/Zeitplan)	Vorhandene Vorlagen für Schichten. Die Auswahlmöglichkeiten lauten wie folgt: • 24 x 7 • Außerhalb Bürozeit (Arbeitstag 8:00 bis 17:00) • Außerhalb Bürozeit (Arbeitstag 9:00 bis 17:00) • Arbeitstag 8:00 bis 17:00 • Arbeitstag 9:00 bis 17:00

Formular „Service hinzufügen“.

Erstellen Sie einen Service, oder fügen Sie Ihrer Instanz einen Service hinzu, damit Warnungen und Incidents zu diesem Service für Ihre Teams in SRMverfügbar sind.

Fügen Sie ein Serviceformular hinzu

Weitere Informationen finden Sie unter Services zu SRM hinzufügen.

Einen Service hinzufügen

Feld	Beschreibung
Servicetyp	• Anwendungsservice: Ein Service, der aus einem oder mehreren Konfigurationselementen besteht, die eine Teilmenge der Aufgaben ausführen, die zusammen eine Funktion auf Geschäftsebene ausführen. Beispiele: Kostenberechnungs-App oder Datenbankserver. • Technischer Service: Ein Service, der aus Produkten wie Service-Mapping und Discovery besteht. Sie stellen die Technologie dar, die Ihr Unternehmen verkauft oder verbraucht.
Servicename	Eindeutiger und aussagekräftiger Name für den Service.
Business-Relevanz	Gibt an, wie wichtig etwas für das Unternehmen ist. Die Auswahlmöglichkeiten lauten wie folgt: • 1 – Am kritischsten (Standardeinstellung) • 2 – Kritisch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einen Service hinzufügen (Fortsetzung)

Feld	Beschreibung
	• 3 – weniger kritisch • 4 – Nicht kritisch
Betriebsstatus	Status des Service. Die Auswahlmöglichkeiten lauten wie folgt: • Operativ • Nicht funktionsfähig • Reparatur in Bearbeitung • DR-Standby • Bereit • Deaktiviert • Pipeline • Katalog
Service-Beschreibung	Beschreibung des Gesamtservice, die anderen dabei hilft, den Zweck des Service und andere relevante Informationen zu verstehen.

Formular „Servicedetails“ bearbeiten

Bearbeiten Sie einen vorhandenen Service, für den Ihr Team verantwortlich ist.

Formular „Servicedetails“.

Weitere Informationen finden Sie unter SRM-Servicedetails bearbeiten.

Feld	Beschreibung
Name	Name des Service
Support-Gruppe	SRM-Team, das den Service verwaltet.
Business-Relevanz	Gibt an, wie wichtig dieser Service für das Geschäft ist. Die Auswahlmöglichkeiten lauten wie folgt: • 1 – Am kritischsten (Standardeinstellung) • 2 – Kritisch • 3 – weniger kritisch • 4 – Nicht kritisch
Eigentum von	Serviceverantwortlicher. Darf nicht Teil eines SRM-Teams sein.
Betriebsstatus	Status für die Fähigkeit des Service, operative Funktionen auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Die Auswahlmöglichkeiten lauten wie folgt: • Operativ • Nicht funktionsfähig • Reparatur in Bearbeitung • DR-Standby • Bereit • Deaktiviert • Pipeline • Katalog
Entscheidungsträger	Produkteigentümer oder Serviceverbraucher, die die Zielverfügbarkeit eines Service bestimmen.
Umgebung	Die Auswahlmöglichkeiten lauten wie folgt: • Keine • Entwicklung • Produktion • Test
Verwaltet von Gruppe	Teammanager, der für den Service verantwortlich ist. Verwenden Sie zum Hinzufügen die Suche und zum Bearbeiten einen Texteditor.
Gruppe ändern	Team, das für Changes verantwortlich ist. Verwenden Sie zum Hinzufügen die Suche und zum Bearbeiten einen Texteditor.
Status	Status des Service.
Lebenszyklusphase	Die Auswahlmöglichkeiten lauten wie folgt: • Bereitstellen • Design • Ende der Lebensdauer • Ideation • Funktionsfähig
Phase	Phase des Service. Die Auswahlmöglichkeiten lauten wie folgt: • Keine • Pipeline • Katalog • Deaktiviert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Standort	Adresse, unter der sich der Service befindet. Verwenden Sie zum Hinzufügen die Suche und zum Bearbeiten einen Texteditor.
Verwendet für	Zweck des Service. Die Auswahlmöglichkeiten lauten wie folgt: • Produktion (Standard) • Staging • QA • Test • Entwicklung • Demonstration • Schulung • Notfallwiederherstellung
Kurzbeschreibung	Zusätzliche Informationen zum Service.
Support by (Support durch)	SRM-Team, das den Service verwaltet. Verwenden Sie zum Hinzufügen die Suche und zum Bearbeiten einen Texteditor.

Richten Sie das Formular für Eskalationsrichtlinien in ein SRM

Eskalationsrichtlinien legen die Reihenfolge und die Bedingungen fest, unter denen Mitglieder oder Geräte Benachrichtigungen erhalten.

Formular „Eskalationsrichtlinie“.

Feld	Beschreibung
Name	Name der Eskalationsrichtlinie.
Aktiv in Schicht	Team, das die Benachrichtigungen für seine Schicht erhält..
Von Grund auf neu erstellen	Option zum Erstellen einer eigenen Richtlinie.
Aus Vorlage erstellen	Option zum Erstellen einer Richtlinie mithilfe einer von Ihrem Administrator erstellten Vorlage.
Beschreibung	Text zur Beschreibung der Richtlinie.
Aktiv	Option zum Aktivieren oder Deaktivieren der Richtlinie.
Als Standard verwenden	Option, um dieses Team als Standard zu verwenden
Auftrag	Reihenfolge der Ausführung. Dies ist die Hierarchie oder Befehlskette. Wenn mehrere Eskalationsrichtlinien mit denselben Bedingungen für ein Team vorhanden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	sind, wird die Eskalationsrichtlinie mit der niedrigeren Reihenfolgenummer zuerst ausgeführt.
Bedingungen	Bedingungen für die Richtlinie. Die Tabelle und die Bedingungen, die die Eskalationsrichtlinie definieren Diese Bedingungen werden überprüft, nachdem die Eskalation durch einen Eskalationsauslöser gestartet wurde. Wenn die Bedingungen erfüllt sind, wird die Richtlinie ausgeführt.
Eskalationsschritte	Hinzuzufügende Eskalationsschritte. Weitere Informationen zu den Feldern finden Sie im Formular „Eskalationsschritte“.
Eskalationsbenachrichtigungen	Benachrichtigungsbedingungen für die Richtlinie. **Hinweis:** Wenn das Überschreiben der Benutzereinstellungen aktiviert ist, überschreibt Ihre Eskalationsrichtlinie alle Richtlinien, die die Service Desk-Mitarbeiter in Rufbereitschaft für ihre eigenen Benachrichtigungseinstellungen festgelegt haben. Wenn das Überschreiben der Anwendereinstellungen deaktiviert ist, haben die Benachrichtigungseinstellungen der Service Desk-Mitarbeiter in Rufbereitschaft Vorrang vor dieser Eskalationsrichtlinie.
Benachrichtigungsschritt hinzufügen	Zusätzlich hinzuzufügende Benachrichtigungsschritte. Sie können E-Mail, Anruf oder SMS auswählen. Sie können beliebig viele Versuche hinzufügen.

Formular „Eskalationsschritte“.

Eskalationsschritt hinzufügen

Feld	Beschreibung
Name des Eskalationsschritts	Name des Eskalationsschrittes.
Auftrag	Reihenfolge der Ausführung. Dies ist die Hierarchie oder Befehlskette.
Beantworter-Ebene	Für die Reaktion auf den Incident erforderliche Autorität oder Fachwissen.
Unter Mitgliedern abwechseln	Option zur Benachrichtigung aller Mitglieder nacheinander, bis eines von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eskalationsschritt hinzufügen (Fortsetzung)

Feld	Beschreibung
	ihnen den Incident bestätigt oder bis alle benachrichtigt wurden.
Zusätzliche Zielgruppe	Bestimmte Benutzer, Teams, Gruppen oder Geräte, die Sie benachrichtigen möchten.
Zeit bis zum nächsten Schritt nach der letzten Benachrichtigung	Die maximale Zeit, die vergeht, bevor das Problem zum nächsten Schritt eskaliert wird. Beispiel: Wenn ein Beantworter das Problem nicht innerhalb von 30 Minuten nach der Benachrichtigung lösen kann, wird das Problem an den -Manager eskaliert.

Domänentrennung und SRM

Service Reliability Management (SRM) unterstützt Domain Separation.

Support-Stufe: Basis*

Die Supportstufe ist „Basis“, weist jedoch einige Ausnahmen oder besondere Bedingungen auf.

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers (SP) übertragen werden.
- Die Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen verwenden die Domäne alle zur Produktionslaufzeit.
- Der Besitzer der Instanz muss in der Lage sein, die Anwendung so einzurichten, dass sie mandantenübergreifend funktioniert.

Beispiel-Anwendungsfall: Wenn ein SP den Chat verwendet, um auf die Nachricht eines Mandanten zu antworten, muss der Client die Antwort des SP sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Übersicht über Domain Separation

- Domänentrennung ist in allen Metadatentabellen in der Anwendung vorhanden. Auch Tabellen auf der Ebene der Instanz verfügen explizit über Domänentrennung. Andere interne Tabellen, z. B. die interne Teamanforderungstabelle, sind implizit domänengetrennt, da sie auf domänengetrennte Datensätze verweisen.
- Systemeigenschaften sind hingegen nicht domänengetrennt, was Auswirkungen auf die Funktionen des Teammanagements hat. Die Eigenschaften werden von mehreren Domänen gemeinsam verwendet und auf Instanzebene festgelegt. Ein domänenspezifisches Setup für diese Eigenschaften wird nicht unterstützt.
- Wenn eine andere Anwendung genutzt wird (z. B. Ereignismanagement-Connectors), hängt die Fähigkeit zur Domänentrennung von den Domänentrennungsfunktionen dieser Anwendung ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

So funktioniert die Domänentrennung in der Service Reliability Management Anwendung

Die spezifischen Bedingungen, die oben durch die Support-Stufe Basic* angegeben werden, beziehen sich auf Teammanagement:

- Neue Teams werden über ein Katalogelement erstellt, das von einem IntegrationHub-Flow unterstützt wird, der vom Service Operations-Arbeitsbereich-Administrator eingerichtet wird. Sie können das über das Serviceportal initiieren. Ein SRM-Administrator, -Manager oder -Beantworter kann das über den SRM-Arbeitsbereich tun. Anweisungen finden Sie in der SRM-Dokumentation.
- Subflows und Aktionen von IntegrationHub steuern die Verwaltung von SRM-Teams.
- Für jede Instanz kann nur ein Katalogelement und ein Flow eingerichtet werden. Der Kunde ist für die Einrichtung von Teameigenschaften zur Unterstützung der Domänentrennung als Anpassung der vorhandenen Flows verantwortlich.
- Die anfordernde Person eines Teamkatalogelements ist der Domäne zugeordnet und als Teil des Anforderungselements verfügbar. Daher kann die anfordernde Person gegebenenfalls das Team in einer bestimmten Domäne oder im Katalogelement erstellen und erweitern, um die Domäne auf andere Weise zu erfassen. In beiden Fällen muss der Service Operations-Arbeitsbereich Änderungen an den Flows und Aktionen von IntegrationHub vornehmen, um dies zu unterstützen.

Weitere Informationen finden Sie unter Domain Separation und Bereitschaftsplanung .

Zugehörige Informationen

Domänentrennung für Service Provider

Erstellen Sie Change-Anforderungsformulare

Füllen Sie die Felder in den Formularen aus, um eine Change-Aufgabe für die Implementierung eines kontrollierten Prozesses zum Ändern genehmigter und unterstützter Aktionen für SRMzu erstellen.

Change-Anforderungs-Formular

Erstellen Sie einen neuen Change Request. Weitere Informationen finden Sie unter Change-Aufgabe in SRM manuell erstellen.

Feld	Beschreibung
Kurzbeschreibung	Kurze Beschreibung der Change-Anforderung.
Beschreibung	Beschreibung basierend auf der Kurzbeschreibung.
Nummer	Bezeichner der Change-Anforderung.
Kategorie	Kategorie der Change-Anforderung. Die Auswahlmöglichkeiten lauten wie folgt: • Hardware • Software • Service • Systemsoftware

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	• Anwendungssoftware • Netzwerk • Telekommunikation • Dokumentation • Sonstige (Standard)
Modell	Für die Change-Anforderung zu verwendendes Modell. Standard (Standard)
Risiko	Risiko, das das Problem darstellt. Die Auswahlmöglichkeiten lauten wie folgt: • Hoch • Mittel (Standard) • Niedrig
Typ	Typ der Change-Anforderung. Standard (Standard) Schreibgeschützt.
Auswirkung	Auswirkung des Problems. Die Auswahlmöglichkeiten lauten wie folgt: • 1 - Hoch • 2 - Mittel • 3 - Niedrig (Standard)
Status	Status der Change-Anforderung. Die Auswahlmöglichkeiten lauten wie folgt: • Neu (Standard) • Bewerten Wenn eine Genehmigung erforderlich ist, sind keine weiteren Status verfügbar. • Geplant • Implementieren • Abgebrochen
Arbeitsnotizenliste	Teammitglieder, die Benachrichtigungen erhalten, wenn Arbeitsnotizen hinzugefügt werden. **Hinweis:** Ein Administrator muss bereits eine E-Mail-Benachrichtigung für die Arbeitsnotizenliste erstellt haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Arbeitsnotizen	Zusätzliche Informationen im Zusammenhang mit dieser Anforderung.

Informationen zu Auswirkung, Zuweisung, Planung, Zeitplan, Notizen und Abschluss

Feld	Beschreibung
Konfigurationselement	Asset, das von dem Problem betroffen ist.
Service	Service, der von dem Problem betroffen ist.
Serviceangebot	Serviceangebot, das von dem Problem betroffen ist.
Zuweisungsgruppe	Team, das der Change-Anforderung zugewiesen ist.
Zugewiesen an	Benutzer, dem die Change-Anforderung zugewiesen ist.
Begründung	Begründung für die Change-Anforderung.
Implementierungsplan	Importierter Text.
Risiko- und Auswirkungsanalyse	Analyse der Risiken und Auswirkungen des Problems.
Rückfallplan	Importierter Text.
Testplan	Importierter Text.
Geplantes Startdatum	Erwartetes Datum für den Beginn des Change.
Geplantes Enddatum	Erwartetes Datum für den Abschluss des Change.
Tatsächliches Startdatum	Datum, an dem die Implementierung des Change begonnen hat.
Tatsächliches Enddatum	Datum, an dem die Implementierung des Change beendet wurde.
Konfliktstatus	Nicht ausgeführt. Schreibgeschützt.
Letzte Konfliktanalyse	In Abhängigkeit vom Konfliktstatus. Abgebrochen
Beobachtungsliste	Interessierte Benutzer.
Arbeitsnotizenliste	Teammitglieder, die Benachrichtigungen erhalten, wenn Arbeitsnotizen hinzugefügt werden. **Hinweis:** Ein Administrator muss bereits eine E-Mail-Benachrichtigung für die Arbeitsnotizenliste erstellt haben.
Zusätzliche Kommentare	Zusätzliche Hinweise für die Anforderung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Arbeitsnotizen	Zusätzliche Hinweise zur Arbeit, die für die Anforderung ausgeführt wird.
Abschlusscode	Code für die Change-Anforderung. Die Auswahlmöglichkeiten lauten wie folgt: • Keine (Standard) • Erfolgreich • Erfolgreich mit Problemen • Nicht erfolgreich
Abschlussnotizen	Hinweise zum Abschluss der Change-Anforderung.

Status von SRM-Incidents

Incidents können verschiedene Status aufweisen, je nachdem, wie auf sie reagiert wird.

In SRM wird ein Incident erstellt, wenn das Überwachungstool eines Drittanbieters ein Event registriert. Incidents können manuell erstellt oder zugewiesen werden. Bearbeiten Sie Aktionen aus dem Incident-Formular über die Status-Schaltfläche im Formular. Verwenden Sie die Schaltfläche **Speichern** im Formular, um die vorgenommenen Änderungen beizubehalten. Änderungen an den Incidents in der Listenansicht werden automatisch gespeichert.

Incident-Status

Status	Beschreibung
Neu	Status oder Incident-Erstellung. Der Incident wurde protokolliert, aber noch nicht bearbeitet.
In Bearbeitung	Der Incident wird zur Bearbeitung zugewiesen.
Angehalten	Die Verantwortung für den Incident wurde vorübergehend zu einer anderen Entität verschoben, um weitere Informationen, Indizien oder eine Lösung bereitzustellen.
Gelöst	Für den Incident wurde eine zufriedenstellende Lösung bereitgestellt, um sicherzustellen, dass er nicht erneut auftritt.
Geschlossen	Der Incident wird geschlossen, wenn bestätigt wird, dass der Incident zufriedenstellend gelöst wurde.
Abgebrochen	Der Incident wurde überprüft, aber es wurde festgestellt, dass es sich um einen doppelten Incident, einen unnötigen Incident oder überhaupt keinen Incident handelt. So öffnen Sie einen Incident erneut. Wählen Sie **Neu**.

Status von SRM-Warnungen

Warnungen können verschiedene Status aufweisen, je nachdem, wie auf sie reagiert wird.

In SRM wird eine Warnung erstellt, wenn das Überwachungstool eines Drittanbieters ein Event registriert. Warnungen werden manuell zugewiesen. Eine Warnung kann einen von vier Status aufweisen. Sie können Aktionen entweder in der Warnungsliste oder im Warnungsformular bearbeiten. Verwenden Sie die Schaltfläche **Speichern** im Formular, um die vorgenommenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Änderungen beizubehalten. Änderungen an Warnungen in der Listenansicht werden automatisch gespeichert.

Hinweis: Sie können Warnungen in jedem Status bestätigen und zuweisen.

Warnungsaktionen

Status	Beschreibung
Offen	Status bei Erstellung der Warnung. In diesem Status können Sie Folgendes bestätigen und festlegen: Flatternd Fluktuieren tritt auf, wenn von der Eventquelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden. Weitere Informationen zu fluktuierenden Events finden Sie unter Fluktuierende Warnungen konfigurieren. Geschlossen Schließt die Warnung.
Erneut öffnen	In diesem Status können Sie Folgendes bestätigen und festlegen: Offen Legt die Warnung auf den Status **Offen** fest. Flatternd Fluktuieren tritt auf, wenn von der Eventquelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden. Geschlossen Schließt die Warnung.
Flatternd	Fluktuieren tritt auf, wenn von der Eventquelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden. Über diesen Status können Sie Folgendes festlegen: Offen Legt die Warnung auf den Status **Offen** fest. Erneut öffnen Öffnet die Warnung erneut. Geschlossen Schließt die Warnung.
Geschlossen	Über diesen Status können Sie Folgendes festlegen: Offen Legt die Warnung auf den Status **Offen** fest. Erneut öffnen Öffnet die Warnung erneut. Flatternd Fluktuieren tritt auf, wenn von der Eventquelle auch nach dem Schließen der zugehörigen Warnung weiterhin Events generiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Status von SRM-Change-Anforderungen

Incidents können verschiedene Status aufweisen, je nachdem, wie auf sie reagiert wird.

Change-Anforderungen können in SRM manuell erstellt werden. Bearbeiten Sie Aktionen im Formular für Change-Anforderungen über das Statusfeld im Formular oder die Schaltflächen im Datensatz für die Change-Anforderung. Verwenden Sie die Schaltfläche **Speichern** im Formular, um die vorgenommenen Änderungen beizubehalten. Änderungen an Change-Anforderungen in der Listenansicht werden automatisch gespeichert.

Change-Anforderung – Status

Status	Beschreibung
Neu	Status bei Erstellung der Change-Anforderung. Die Anforderung wurde protokolliert, aber noch nicht bearbeitet.
Bewerten	Die Genehmigung der Change-Anforderung wird bearbeitet.
Geplant	Eine Change-Anforderung zur Bearbeitung geplant.
Implementieren	Die Change-Anforderung wird umgesetzt.
Überprüfen	Die Change-Anforderung wechselt in den Status **Überprüfen**. **Hinweis:** Alle offenen Change-Aufgaben werden auf **Abgebrochen** gesetzt.
Geschlossen	Die Change-Anforderung wird geschlossen.
Abgebrochen	Die Change-Anforderung wurde selektiert, aber es wurde festgestellt, dass es sich um ein Duplikat handelt oder sie unnötig ist. **Hinweis:** Sie können eine abgebrochene Change-Anforderung nicht erneut öffnen.

CMDB-Serviceklassen

Service Reliability Management unterstützt normalerweise mehrere CMDB-Serviceklassen (Configuration Management Database).

Arten von CMDB-Serviceklassen, die Service Reliability Management unterstützen:

- Serviceinstanzen (cmdb_ci_service_auto)
- Technische Services (cmdb_ci_service_technical)
- Abfragebasierte Services (cmdb_ci_query_based_service)
- Zugeordnete Anwendungsservices (cmdb_ci_service_discovered)
- Berechnete Anwendungsservices (cmdb_ci_calculated)
- Tag-basierte Anwendungsservices (cmdb_ci_service_by_tags)

Servicelevel-Zielmanagement

Servicelevel-Zielmanagement (SLO-Management) hilft Ihrem Unternehmen, vereinbarte Servicequalitätsstandards zu definieren, nachzuverfolgen und zu erfüllen. Es arbeitet mit Servicelevel-Vereinbarungen (Service Level Agreements, SLAs) zusammen, um sicherzustellen, dass die Servicebereitstellung den Kundenerwartungen entspricht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über die Funktionsweise von SLO-Management.

- SLAs legen die Erwartungen fest

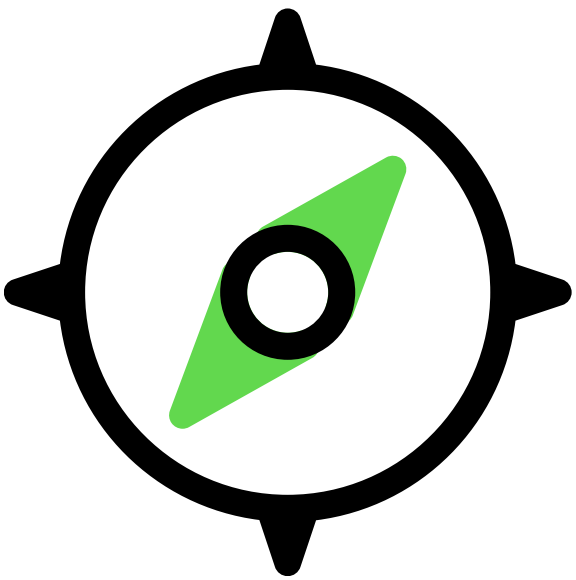
  SLAs sind formelle Vereinbarungen, die das Serviceniveau beschreiben, das ein Kunde erwarten kann. Dies kann Dinge wie Antwortzeiten, Lösungszeiten und Betriebszeitziele umfassen.

- SLOs definieren, wie Erwartungen erfüllt werden

  SLOs sind spezifische, messbare Ziele, die eine Organisation festlegt, um die SLAs zu erreichen. Sie übersetzen die allgemeinen Ziele des SLA in umsetzbare Metriken.

- ServiceNow SLO-Management hilft beim Verwalten von SLOs. Sie bietet folgende Funktionen:
  - Definieren Sie SLOs basierend auf verschiedenen Metriken.
  - Überwachen Sie die SLO-Leistung in Echtzeit.
  - Generieren Sie Warnungen, wenn die Gefahr einer Verletzung von SLOs besteht.
  - Verfolgen Sie Verlaufsdaten, um Trends zu erkennen und Prozesse zu verbessern.

Erste Schritte

Untersuchen	Verwenden
	
Erfahren Sie mehr über die Konzepte und Funktionen Servicelevel-Zielmanagement von .	Servicelevel-Zielmanagement verwenden

Problembehandlung und Hilfe

- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicelevel-Zielmanagement erkunden

Servicelevel-Zielmanagement (SLO-Management) ist ein entscheidender Aspekt von IT Service Management, der sicherstellt, dass IT-Services die Kundenerwartungen erfüllen.

SLO-Management – Übersicht

SLO-Management ist ein Framework, um klare Erwartungen zu formulieren und die Leistung von IT-Services zu messen. Es hilft Unternehmen, eine konsistente Servicebereitstellung sicherzustellen und Bereiche mit Verbesserungspotenzial zu identifizieren. SLOs definieren den Zielservicelevel für einen bestimmten Service, z. B. Lösung von Incidents oder Erfüllung von Serviceanfragen. Effektives SLO-Management beinhaltet das Setzen realistischer Ziele, die Überwachung der Leistung und die kontinuierliche Verbesserung von Services, um die Kundenbedürfnisse zu erfüllen.

SLO-Management Anwender

Anwender

Anwender	Beschreibung	Enthält Rollen
Administrator	Ein ServiceNow-Administrator ist für Verwaltung, Entwicklung, Betrieb, Schulung und Wartung der ServiceNow Platform verantwortlich. Verantwortlich für die Installation und kann die Service Operations-Arbeitsbereich Admin Center-Konfiguration von SRM durchführen.	Alle
-Administrator [srm_admin] **Hinweis:** Nicht die ServiceNow-Rolle *admin*	SRM-Administratoren können Accounteinstellungen, Konfigurationen und Benutzer verwalten. Administratoren können folgende Aktionen ausführen: • Alle SRM-Konfigurationen erstellen, bearbeiten oder löschen und darauf zugreifen. • Integrationen hinzufügen oder verwalten. • Integrationen mit APM-Tools (Application Performance Monitoring) erstellen • Zuverlässigkeitsindikatoren einrichten und verwalten. • Fehlerbudgetrichtlinien einrichten und verwalten.	• Manager • Beantworter
-Manager [srm_manager]	Manager überwachen ein Team von SREs. Manager weisen dem Rufbereitschaftszeitplan des Teams	Beantworter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender (Fortsetzung)

Anwender	Beschreibung	Enthält Rollen
	SREs zu, überwachen ihre Leistung, erstellen Verfahren zur Behandlung von Incidents und entwickeln Lösungen. Manager stellen über alle Systeme und DevOps-Workflows hinweg Resilienz sicher. Manager können im Kontext ihrer Teams folgende Aktionen ausführen: • Teams, Rufbereitschaftszeitpläne und Services definieren und einrichten. • Benutzer wie Beantworter und Manager für die Teams hinzufügen und löschen, denen sie angehören. • Integrationen hinzufügen oder verwalten. • Integrationen mit APM-Tools (Application Performance Monitoring) erstellen • Zuverlässigkeitsindikatoren einrichten und verwalten. • Fehlerbudgetrichtlinien einrichten und verwalten.	
Beantworter [srm_responder]	Ein Service Reliability Engineer (SRE), der SRM zur Ausführung alltäglicher Aufgaben verwendet. Beantworter sind die Personen, die Rufbereitschaft haben und Incidents diagnostizieren und beheben. Beantworter können nur auf Konfigurationen zugreifen, denen sie angehören. Sie können nur auf die Warnungen oder Incidents zugreifen, für die sie Berechtigungen haben. SREs können im Kontext ihrer Teams folgende Aktionen ausführen:	Erbt 17 Rollen, darunter die folgenden: • cmdb_read • sn_sow.sow_user • sn_sow_srm.srm_responder • workspace_user • slo_operator

Hinweis: Benutzer des SLO-Plugins ohne SRM sollten sicherstellen, dass ihren Teammitgliedern die erforderlichen Lesezugriff für Warnungen und cmdb_ci gewährt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SLO-Management – Workflow

1. SLOs definieren – Identifizieren Sie kritische Services und definieren Sie SLOs basierend auf Kundenerwartungen und Geschäftsanforderungen.
2. SLIs einrichten – Entwicklung von Servicelevel-Indikatoren (SLIs) zur Messung der SLO-Leistung.
3. Überwachen und analysieren – Verfolgen Sie SLI-Daten und analysieren Sie die Leistung anhand von SLO-Zielen.
4. Lücken identifizieren und verbessern – Ermitteln Sie Bereiche, in denen SLOs nicht erfüllt werden, und implementieren Sie Changes, um die Serviceleistung zu verbessern.
5. Überprüfen und verfeinern – Überprüfen Sie die SLO-Leistung regelmäßig, und verfeinern Sie SLOs nach Bedarf.

SLO-Management – Vorteile

- Verbesserte Servicequalität – SLOs stellen sicher, dass IT-Services die Kundenerwartungen erfüllen, was zu höherer Zufriedenheit und Treue führt.
- Höhere Transparenz – Eindeutige SLOs sorgen für ein gemeinsames Verständnis der Serviceerwartungen zwischen IT und Kunden.
- Bessere Ressourcenzuteilung – SLOs helfen bei der Priorisierung von Ressourcen und der Fokussierung auf Bereiche, die verbessert werden müssen.
- Verbesserte Zusammenarbeit – SLO-Management fördert die Zusammenarbeit zwischen IT-Teams und Kunden, um gemeinsame Ziele zu erreichen.
- Datengesteuerte Entscheidungsfindung: SLO-Leistungsdaten dienen als Grundlage für Entscheidungen und fördern die kontinuierliche Serviceverbesserung.

Servicelevel-Zielmanagement verwenden

SLO-Management stellt sicher, dass IT-Services die Kundenerwartungen erfüllen, verbessert Servicequalität und Transparenz und ermöglicht eine datengesteuerte Entscheidungsfindung.

Mit Zuverlässigkeitsmetriken arbeiten

Verwenden Sie die Zuverlässigkeitsmetriken SRM, um Servicelevel-Indikatoren (SLI), Servicelevel-Ziele (SLO) und Fehlerbudgetrichtlinien zu definieren, Ihre Serviceintegrität nachzuverfolgen und die erforderlichen Maßnahmen zu ergreifen.

Allgemeiner Workflow

1. SRM nutzt Integrationen für die Signalzusammenfassung.
2. Für den Service in SRM werden Zuverlässigkeitsindikatoren mit SLIs und SLOs erstellt.
3. Wenn für einen Service eine qualifizierte Warnung generiert wird, werden für die Zuverlässigkeitsindikatoren in SRM kumulative Werte für Verstoß und Fehlerbudget aktualisiert.
4. Für den Service wird eine Fehlerbudgetrichtlinie erstellt, mit der Aktionen wie das Erstellen eines Incident oder das Senden einer E-Mail ausgelöst werden, um Serviceprobleme zu beheben. Fehlerbudgets sind durch die Kategorie eingeschränkt.

Die wichtigsten Funktionen der Metriken von SRM sind:

- SLI-Signalzusammenfassung
- Erstellen Sie auf Dauer und Anzahl basierende Servicelevel-Ziele.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Fehlerbudgets berechnen (EB)
- Fehlerbudgetrichtlinien
- Visualisierung von Fehlerbudgets

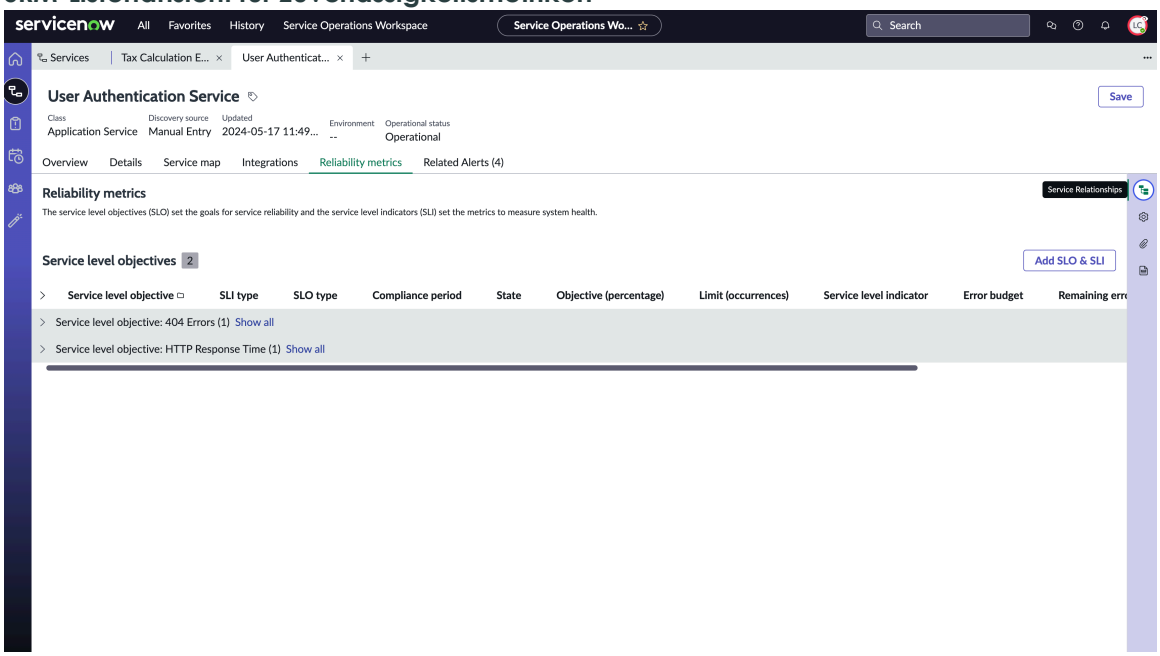
Navigieren Sie zu **Services** > **Übersicht** Registerkarte, um alle zugehörigen kritischen Daten für die Metriken „Zuverlässigkeit“ und „Fehlerbudget“ anzuzeigen. Weitere Informationen finden Sie unter Mit SRM-Services arbeiten.

Hinweis: Punktzahlen sind nur sichtbar, wenn SLIs, SLOs und Fehlerbudgets erstellt wurden und diese betroffen sind. Ausführliche Informationen finden Sie unter Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien.

Registerkarte „Zuverlässigkeitsmetriken“

Navigieren Sie zu **Services** > **Zuverlässigkeitsmetriken** Zeigen Sie auf der Registerkarte die Servicelevel-Ziele (Service Level Objectives, SLO) für einen Service an.

SRM-Listenansicht für Zuverlässigkeitsmetriken



Hinweis: Durch das Aktualisieren des SLO wird der Status geändert. Dies führt auch dazu, dass dieser SLO-Datensatz stillgelegt und eine Kopie für genaue Überwachungszwecke erstellt wird.

Zuverlässigkeitsmetriken

Servicelevel-Ziele zeigen die folgenden Details an:

- **Servicelevel-Ziel**: Name des SLO. Das SLO ist ein Zielwert oder das Ziel, das Ihr Team erreichen muss, um Ihre Servicelevel-Vereinbarung (Service Level Agreement, SLA) zu erfüllen.
- **SLI-Typ**: Die tatsächlichen Zahlen zur Leistung Ihres Services.

  Die SLI-Typen sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verfügbarkeit: Prozentsatz der Zeit, während der Ihr Service verfügbar ist. Wird auch als Betriebszeit bezeichnet. Verfügbarkeit ist die grundlegende Metrik für Zuverlässigkeit. (Standard).
- Fehler: Misst die Häufigkeit Ihrer Servicefehler.
- Latenz: Zeit, die für die Bearbeitung einer Anforderung benötigt wird. Die tatsächlich verstrichene Zeit.
- Sättigung: Misst die „Auslastung“ des Systems, wobei die am stärksten eingeschränkten Ressourcen hervorgehoben werden.

- **Compliance-Zeitraum**:

  Die für den SLO festgelegte Dauer.

  - **Monat**: Als Dauer wird der aktuelle Monat betrachtet. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer vom 1. Januar bis zum 31. Januar angenommen.
  - **Rollend, 7 Tage**: Für die Dauer werden 7 Tage ab dem aktuellen Datum angenommen.
  - **Rollend, 30 Tage**: Für die Dauer werden 30 Tage ab dem aktuellen Datum angenommen. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer ab dem 25. Dezember berücksichtigt.
  - **Rollend, 90 Tage**: Für die Dauer werden 90 Tage ab dem aktuellen Datum angenommen. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer ab dem 25. Oktober berücksichtigt.

- **Status**:

  Status des SLO. Die Auswahlmöglichkeiten lauten wie folgt:

  - Entwurf: Der SLO wird in Ihrer Instanz noch nicht ausgeführt. Sie können neue SLIs hinzufügen oder vorhandene SLIs aktualisieren, und Sie können den SLO löschen.
  - Wird ausgeführt: Der SLO ist in Ihrer Instanz aktiv. Sie können den SLO bearbeiten, stilllegen oder löschen.

    Hinweis: Wenn Sie einen SLO im Ausführungsstatus bearbeiten, wird er deaktiviert und eine neue Kopie wird erstellt.

  - Deaktiviert: Der SLO wird in Ihrer Instanz nicht mehr ausgeführt. Sie können ihn reaktivieren.

- **Ziel (%)**: Prozentsatz der gewünschten SLI-Leistung.
- **Grenzwertvorkommen**: Anzahl der aufgetretenen Überschreitungen des Grenzwerts. (Verwendet von Anzahl SLO-Typen.)
- **Servicelevel-Indikator**: Tatsächliche Zahlen zur Leistung Ihres Services. Messbare Fakten, die anzeigen, ob Sie die Erwartungen der Kunden erfüllen.
- **Fehlerbudget**: Gibt an, wie viel Fehlerbudget Sie ausgeben können. Beim Erstellen eines SLO wird das Fehlerbudget basierend auf den Angaben für Compliance-Zeitraum und Ziel (%) berechnet.
- **Verbleibendes Fehlerbudget**: Gibt an, wie viel Fehlerbudget verbleibt.
- **Verbleibende aufgetretene Verstöße**: Anzahl der verbleibenden Verstöße, bevor der Grenzwert erreicht wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Datensätze für den Verlauf des Servicelevel-Ziels [sn_sow_srm_slo_history] und der Servicelevel-Indikator-Metrik [sn_sow_srm_sli_metric] werden nach einem Jahr archiviert und fünf Jahre danach gelöscht. Es wird erwartet, dass dies zu einer höheren Leistung bei gleicher Dauer der Datenspeicherung führt. Für archivierte Tabellen werden keine Abfragen ausgeführt.

Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien

Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien, die Ihnen und Ihrem Team helfen, Ihre Serviceintegrität nachzuverfolgen und bei Bedarf die erforderlichen Maßnahmen zu ergreifen.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Für einen SLI können Sie nur ein SLO einrichten.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

   Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **Services** ( ).
3. Öffnen Sie auf der Seite **„Services“** den Service, für den Sie SLO und SLI erstellen möchten.
4. Wählen Sie die Registerkarte **Zuverlässigkeitsmetriken**.
5. Wählen Sie **SLO/SLI hinzufügen**.

   Das Servicelevel-Ziel ist das Ziel, das Ihr Team erreichen muss, um die Servicelevel-Vereinbarung (Service Level Agreement, SLA) zu erfüllen. Es ist Ihr Ziel.

   Die Registerkarte Zuverlässigkeitsmetrik einrichten wird geöffnet.
6. Füllen Sie im Formular Servicelevel-Ziel (SLO) die entsprechenden Felder aus.
   Weitere Informationen finden Sie unter Formular „SLO erstellen“..

   Hinweis: Sie definieren einen Zeitraum für Compliance und ein Ziel für die Zuverlässigkeit des Service.

7. Wählen Sie im Formular Servicelevel-Indikatoren (SLI) **SLI hinzufügen**, und füllen Sie die entsprechenden Felder aus.
   Weitere Informationen finden Sie unter Formular „SLI erstellen“..

   Hinweis: Ein SLI ist ein quantitatives Maß für einen Aspekt des bereitgestellten Servicelevels. Diese Metriken werden verwendet, um SLO-Ziele zu definieren. Mindestens ein SLI ist erforderlich.

8. Wahlweise: Wählen Sie im Formular Fehlerbudget-Richtlinien **die Option Schwellenwert hinzufügen** aus, und füllen Sie die entsprechenden Felder aus.
   Weitere Informationen finden Sie unter Formular „Fehlerbudget-Richtlinien erstellen“..

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Fehlerbudget ist die Anzahl der SLO, die Sie über einen bestimmten Zeitraum ausgeben können. SRM zielt darauf ab, den Verbrauch des Fehlerbudgets zu minimieren, um die Zuverlässigkeit zu maximieren.

Hinweis: Wenn Sie jetzt keine Fehlerbudgetrichtlinie hinzufügen, ist **das Ziel (Prozentsatz)**, das Aktionen auslöst, von rein informativer Natur. Wenn Sie eine erstellen, haben Sie einige Korrekturoptionen.

Sie können später eine Fehlerbudgetrichtlinie hinzufügen, indem Sie das SLO öffnen und die Registerkarte **Fehlerbudget-Richtlinien** auswählen.

Hinweis: Der Header im Bereich **Fehlerbudget-Richtlinien** wird abhängig davon aktualisiert, ob Sie **Dauer** oder eine der Einstellungen für **Anzahl** für Ihr SLO ausgewählt haben.

9. Überprüfen Sie Ihre SLO-, SLI- und Fehlerbudget-Richtlinien.
10. Wählen Sie **Aktivieren**.
    Weitere Informationen zur endgültigen SLO-Seite finden Sie unter Bearbeiten Sie eine Zuverlässigkeitsmetrik.

Bearbeiten Sie eine Zuverlässigkeitsmetrik

Aktualisieren Sie eine Zuverlässigkeitsmetrik, damit sie relevant und an den Zielen Ihres Teams ausgerichtet bleibt.

Vorbereitungen

Erforderliche Rolle: srm_admin, srm_manager oder srm_responder

Das Aktualisieren von Zuverlässigkeitsmetriken wie Service Level Objectives (SLOs) oder Service Level Indicators (SLIs) während aktiver Messzeiträume kann zu Inkonsistenzen in den Diagrammen führen.

Warum und wann dieser Vorgang ausgeführt wird

Service Reliability Management (SRM) folgt bestimmten Namenskonventionen, um Sie bei der Verwaltung des Verlaufs der Zuverlässigkeitsmetriken zu unterstützen. Wenn Sie eine Zuverlässigkeitsmetrik bearbeiten, führt SRM Folgendes aus:

- Legt das vorhandene SLO still.
- Erstellt eine Kopie des SLO mit Ihren Bearbeitungen im Entwurfsstatus. Sie können entweder:
  - Speichern Sie die Kopie als Entwurf.
  - Aktivieren Sie die Kopie.
- Hängt dem Namen der Kopie eine Zahl an, z. B. Betriebszeit (2) oder Betriebszeit (3).
- Zeigt alle SLO-Versionen auf der Registerkarte **Zuverlässigkeitsmetriken** an.

Hinweis: Auf der Registerkarte **Zuverlässigkeitsmetriken** haben SLO-Header zwei Zahlen, z. B. HTTP-Antwortzeit (2) (3). Die erste Zahl ist die Version. Der zweite ist die Anzahl der SLIs, die dem SLO zugeordnet sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *Service Operations-Arbeitsbereich*.
   Sie gelangen zur Homepage SRM – Homepage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Führen Sie diese Schritte aus, um auf die Registerkarte **Zuverlässigkeitsmetriken** zuzugreifen:
   a. Wählen Sie das Seitensymbol **Services** ( ).
   b. Wählen Sie den Service aus, der die Zuverlässigkeitsmetrik verwendet, die Sie bearbeiten möchten.
   c. Wählen Sie die Registerkarte **Zuverlässigkeitsmetriken**.
3. Um eine Zuverlässigkeitsmetrik zu bearbeiten, wählen Sie die entsprechende Zuverlässigkeitsmetrik aus, und wählen Sie **Bearbeiten** und **Bearbeitung fortsetzen aus**.
4. Um Ihre Änderungen zu speichern und zu implementieren, wählen Sie **Aktivieren**aus. Die bearbeitete Zuverlässigkeitsmetrik wird auf der Registerkarte **Zuverlässigkeitsmetriken** angezeigt. SRM legt den Status auf „Wird ausgeführt“ fest und enthält eine Versionsnummer im Namen, z. B. Uptime (3).

Nächste Maßnahme
Die Verwaltung von SLOs erfordert laufende Updates, um sicherzustellen, dass sie Ihre Zuverlässigkeitsziele widerspiegeln. Sie können vorhandene SLOs bearbeiten oder stilllegen und bei Bedarf stillgelegte SLOs erneut aktivieren.

Hinweis: Wenn Sie ein stillgelegtes SLO reaktivieren, erstellt und aktiviert SRM eine neue Kopie davon. Beispiel: Wenn zwei Versionen eines SLO vorhanden sind, Betriebszeit (1) und Betriebszeit (2), und Sie Betriebszeit (1) reaktivieren, belässt SRM den Status im Status „Stillgelegt“ und erstellt eine aktive Version mit dem Namen „Betriebszeit“ (3).

Aktivieren Sie SLO-basierte Change-Genehmigungsentscheidungen

Aktivieren Sie Change-Genehmigungsentscheidungen für Servicelevel-Ziele (SLO), um Change-Anforderungen basierend auf der SLO-Leistung zu bewerten.

Vorbereitungen
Überprüfen Sie die Richtlinien für Change-Genehmigungen und ihre Terminologie, einschließlich Richtlinieneingaben, Entscheidungen und Genehmigungsdefinitionen. Weitere Informationen finden Sie unter Richtlinien für Change-Genehmigungen .

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Aktivieren Sie die Entscheidungen der Richtlinie zur Änderung des Servicelevel-Ziels, um die SLO-Leistung in Ihren Change-Management-Prozess zu integrieren. Die Richtlinie ist standardmäßig aktiv, ihre Entscheidungen sind jedoch inaktiv.

Wenn Sie die Entscheidungen der Richtlinie aktivieren, wertet die Richtlinie SLOs als Eingaben aus und implementiert Folgendes:

- Genehmigung des Gruppenmanagers erforderlich, wenn diese Bedingungen zutreffen:
  - Das niedrigste SLO-Fehlerbudget beträgt weniger als 25 %.
  - Der höchste SLO-Durchsatz ist größer als 1 %.
- Change-Anforderungen automatisch genehmigen, wenn diese Bedingungen zutreffen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das niedrigste SLO-Fehlerbudget ist größer als 25 %.
- Der höchste SLO-Durchsatz beträgt weniger als 1 %.

Prozedur

1. Navigieren zu **Alle** > **Wechseln** > **Change-Richtlinie** > **Richtlinien für Change-Genehmigungen**.
2. Wählen Sie die **Richtlinie Servicelevel-Ziel Change**aus.
3. Legen Sie auf der Registerkarte **„Entscheidungen** " für diese Entscheidungen **Aktiv** auf wahr fest:
   - **Budget < 25 % und Durchsatz > 1**
   - **Budget > 25 % und Durchsatz < 1**
4. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.
   Die Entscheidungen sind aktiv und Teil Ihres Change-Management-Prozesses.

Nächste Maßnahme

Verwenden Sie eine Test-Change-Anforderung, um zu überprüfen, ob Change-Anforderungen entweder automatisch genehmigt oder wie erwartet an einen Manager weitergeleitet werden.

Sie können auch die Richtlinie zur Änderung des Servicelevel-Ziels (einschließlich Name und Bedingungen) nach Bedarf anpassen.

Verwenden Sie für erweiterte Setups Flow Designer, um die SLOs und Services anzupassen, die als Richtlinieneingaben enthalten sind:

Wichtig: Durch das Anpassen des Flows wird verhindert, dass er zukünftige Release-Updates erhält. Dieses Verhalten ist beabsichtigt, um ein Überschreiben Ihrer Anpassungen zu vermeiden.

1. Navigieren zu **Prozessautomatisierung** > **Flow Designer**.
2. Wählen Sie in der Liste der Flows **Change – SLO – Autorisieren** und dann **SLO – Get worst performing SLOs (SLOs mit schlechtester Leistung**abrufen) aus.
3. Passen Sie den Abschnitt **„Aktionseingaben"** an.
4. Wählen Sie **Fertig**, um Ihre Änderungen zu implementieren.

Referenz zur Verwaltung von Servicelevel-Zielen

Referenzthemen enthalten zusätzliche Informationen zu Servicelevel-Zielmanagement.

Zeigen Sie SRM Zuverlässigkeitsmetriken an

Zeigen Sie ein Servicelevel-Ziel (SLO) und einen Servicelevel-Indikator (SLI) an, für das Sie oder Ihr Team verantwortlich sind.

Vorbereitungen

Erforderliche Rolle: Beantworter, Manager oder Administrator

Hinweis: Administratoren können jedes SRM-SLO anzeigen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > *`Service Operations-Arbeitsbereich`*.
   Sie gelangen zur Homepage SRM – Homepage.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie andere SOW-Anwendungen (Service Operations Workspace) verwenden, wird möglicherweise die SOW-Homepage anstelle der SRM-Homepage angezeigt. Die SOW-Homepage enthält SRM-Warnungen und -Incidents in ihren Metriken.

2. Wählen Sie in der primären Navigation das Symbol **Services** ( ).
3. Wählen Sie die Registerkarte **Zuverlässigkeitsmetriken**.
4. Öffnen Sie ein **Servicelevel-Ziel**.
5. Zeigen Sie den SLO-Header an.

   Der oberste Header enthält Serviceinformationen für:

   - **SLI-Typ**:

     Typ des SLI, auf dessen Grundlage die Servicelevel-Metriken (SLM) berechnet werden. Die folgenden SLI-Typen sind verfügbar:

     - **Verfügbarkeit**: Prozentsatz der Zeit, während der Ihr Service verfügbar ist. (Standard)
     - **Fehler**: Messung, wie häufig ein Servicefehler auftritt.
     - **Latenz**: Zeit, die für die Bearbeitung einer Anfrage benötigt wird. Die tatsächlich verstrichene Zeit.
     - **Sättigung**: Messung des Systemanteils, wobei die am stärksten eingeschränkten Ressourcen hervorgehoben werden.

     .

   - **SLO-Typ**:

     Typ des SLO basierend auf der von Ihnen ausgewählten Metrik. Die folgenden SLO-Typen sind verfügbar:

     - **Dauer**: Zeit, die der Service ohne Verstoß ausgeführt wird. Dies ist der einzige verfügbare Wert.

       Die Metriken für **Dauer** lauten wie folgt:

       - **Ziel (Prozentsatz)**: Prozentsatz der gewünschten SLI-Leistung.
       - **Fehlerbudget**: Zeigt das verbleibende Fehlerbudget in Tagen und Zeit an.

     - **Anzahl**: Häufigkeit des Auftretens in einem vorgegebenen Konformitätszeitraum.

       Die Metriken für **Anzahl** lauten wie folgt:

       - **Grenze (Vorkommen)**: Anzahl der Vorkommen, nach denen ein Verstoß aufgetreten ist.
       - **Verbleibende aufgetretene Verstöße**: Anzahl der verbleibenden Vorkommen.

   - **Status**:

     Status des SLO. Die Auswahlmöglichkeiten lauten wie folgt:

     - Entwurf: Der SLO wird in Ihrer Instanz noch nicht ausgeführt. Sie können neue SLIs hinzufügen oder vorhandene SLIs aktualisieren, und Sie können den SLO löschen.
     - Wird ausgeführt: Der SLO ist in Ihrer Instanz aktiv. Sie können den SLO bearbeiten, stilllegen oder löschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie einen SLO im Ausführungsstatus bearbeiten, wird er deaktiviert und eine neue Kopie wird erstellt.

- Deaktiviert: Der SLO wird in Ihrer Instanz nicht mehr ausgeführt. Sie können ihn reaktivieren.

◦ **Service**: Service, der dem SLO zugeordnet ist.

◦ **Zuverlässigkeit**: Gibt an, wie zuverlässig der Service ist.

- **Stabil**: Für alle SLOs in diesem Service sind noch mehr als 25 % des Fehlerbudgets verfügbar.
- **Gefährdet**: Alle SLOs in diesem Service verfügen noch über EB, und mindestens ein SLO in diesem Service weist weniger als 25 % des verbleibenden Fehlerbudgets auf.
- **Kritisch**: Für alle SLOs in diesem Service ist das Fehlerbudget aufgebraucht.

Über den Header können Sie das SLO **löschen**, **stilllegen** oder **bearbeiten**.

Wenn Sie ein SLO löschen, werden auch alle zugehörigen SLIs gelöscht.

Wenn Sie ein SLO stilllegen, ändert sich der Status. Auf der Seite „SLO“ oder später auf der Registerkarte **Zuverlässigkeitsmetriken** können Sie es **erneut aktivieren**.

Hinweis: Wenn Sie ein SLO bearbeiten, ändert es den Status, zieht den SLO-Datensatz zurück und öffnet eine neue Kopie zur Bearbeitung. Weitere Informationen finden Sie unter Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien. Sie können das ursprüngliche SLO reaktivieren, indem Sie zur Registerkarte **Zuverlässigkeitsmetriken** zurückkehren.

6. Zeigen Sie die Registerkarte **Übersicht** an, und wählen Sie einen Verlaufszeitraum aus dem Listenmenü aus.
   Die aufgelisteten Zeiträume werden ab dem Datum, an dem das SLO erstellt wurde, bis zur Gegenwart in den ausgewählten Inkrementen dargestellt.
7. Zeigen Sie die **Zusammenfassung**-Metrikkarten für das SLO an.
   Die Metriken zeigen aggregierte oder durchschnittliche Werte an, abhängig vom Typ der ausgewählten SLIs und der ausgewählten Fehlerrichtlinien-Schwellenwerte. Ausführliche Informationen finden Sie unter Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien.
8. Zeigen Sie den Abschnitt **Servicelevel-Indikatoren** an.

   In diesem Abschnitt werden Ihre Indikatoren nach Namen aufgelistet.
9. Zeigen Sie den Abschnitt **Servicelevel-Ziel (SLO) – Verlauf** an.
   In Abhängigkeit von Ihrem **SLO-Typ** wird in diesem Abschnitt Folgendes in Balkendiagrammberichten angezeigt:

   Für **Dauer**:

   ◦ Genutztes Fehlerbudget

   ◦ Verbleibendes Fehlerbudget

   ◦ Durchsatz

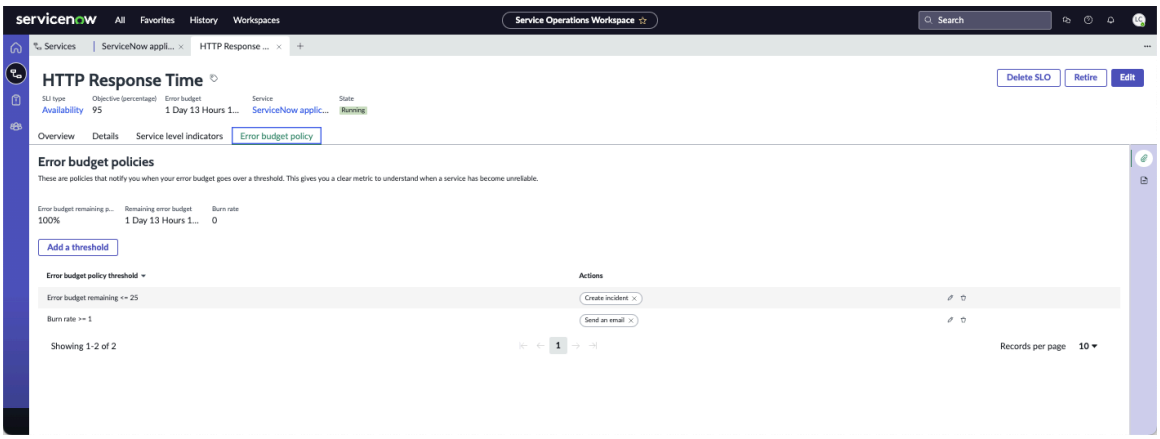
   Für **Anzahl**, **Nach Zeiträumen zählen** oder **Nach Auftreten zählen**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Kumulative aufgetretene Verstöße
- Durchsatz
- Warnungen, Incidents und Changes, die sich auf diesen Service auswirken

Wenn Sie in einem der Analytics-Liniendiagrammberichte auswählen, werden die Werte an diesem Tag angezeigt.

10. Rufen Sie die Registerkarte **Details** auf.
    Die Felder auf dieser Registerkarte werden automatisch gefüllt und können nicht bearbeitet werden. Ausführliche Informationen zu den Feldern finden Sie unter Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien.
11. Zeigen Sie die Registerkarte **Servicelevel-Indikatoren** an.
    Auf dieser Registerkarte werden die SLIs aufgelistet, die diesem SLO zugeordnet sind.
12. Zeigen Sie die Registerkarte **Fehlerbudget-Richtlinie** an.
    Auf dieser Registerkarte können Sie weitere Schwellenwerte hinzufügen und vorhandene bearbeiten oder löschen.



Formular „SLO erstellen“.

Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien, damit Sie und Ihr Team Ihre Serviceintegrität nachverfolgen und bei Bedarf die erforderlichen Maßnahmen ergreifen können.

Formular „Servicelevel-Ziel“

Richten Sie Ihre Servicelevel-Ziele ein. Weitere Informationen finden Sie unter Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien.

Formular „Servicelevel-Ziel“

Feld	Beschreibung
Name	Name des SLO.
SLI-Typ	Typ des SLI, auf dessen Grundlage die Servicelevel-Metriken (SLM) berechnet werden. Die folgenden SLI-Typen sind verfügbar:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Servicelevel-Ziel“ (Fortsetzung)

Feld	Beschreibung
	• **Verfügbarkeit**: Prozentsatz der Zeit, während der Ihr Service verfügbar ist. (Standard) • **Fehler**: Messung, wie häufig ein Servicefehler auftritt. • **Latenz**: Zeit, die für die Bearbeitung einer Anfrage benötigt wird. Die tatsächlich verstrichene Zeit. • **Sättigung**: Messung des Systemanteils, wobei die am stärksten eingeschränkten Ressourcen hervorgehoben werden.
Wie möchten Sie dieses Ziel messen?	Sie können dieses Ziel wie folgt messen: • **Dauer**: Zeit, die der Service ohne Verstoß ausgeführt wird. Dies ist der einzige verfügbare Wert. • **Anzahl**: Die Anzahl der Zeiträume oder Vorkommen in einem bestimmten Compliance-Zeitraum.

Measuring by Duration (Messung nach Dauer)

Feld	Beschreibung
Ziel (%)	Der Prozentsatz der gewünschten Verfügbarkeit (Betriebszeit) des Service über einen bestimmten Zeitraum. Bei der Messung nach Dauer bedeutet ein Zielprozentsatz von „fünf Neunen“ (die sog. Five-Nines-Verfügbarkeit von 99,999 %), dass der Service 26 Sekunden pro Monat oder etwa 5 Minuten und 35 Sekunden pro Jahr nicht verfügbar war. Dies wird verwendet, um Ihr Fehlerbudget zu berechnen.
Compliance-Zeitraum	Zeitraum, für den die Metriken berechnet werden. Verfügbare Optionen: • **Monat**: Als Dauer wird der aktuelle Monat betrachtet. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer vom 1. Januar bis zum 31. Januar angenommen. • **Rollend, 7 Tage**: Für die Dauer werden 7 Tage ab dem aktuellen Datum angenommen. • **Rollend, 30 Tage**: Für die Dauer werden 30 Tage ab dem aktuellen Datum angenommen. Wenn das aktuelle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Measuring by Duration (Messung nach Dauer) (Fortsetzung)

Feld	Beschreibung
	Datum beispielsweise der 26. Januar ist, wird die Dauer ab dem 25. Dezember berücksichtigt. • **Rollend, 90 Tage**: Für die Dauer werden 90 Tage ab dem aktuellen Datum angenommen. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer ab dem 25. Oktober berücksichtigt.
Fehlerbudget	Automatisch ausgefüllt. Das maximale Fehlerniveau (Ausfallzeit), das über einen bestimmten Zeitraum zulässig ist. Ein Prozentsatz der gesamten Serviceverfügbarkeit. Sobald Sie Ihr Ziel in % festgelegt haben, wird Ihr Fehlerbudget automatisch mit der folgenden Formel berechnet: 1 – (gewünschte) Verfügbarkeit. Das Fehlerbudget eines Service wird in Tagen, Stunden, Minuten und Sekunden für eine gewünschte Verfügbarkeit von 99,99 % (Vier Neunen) des Jahres berechnet durch: **1.** Berechnung der Gesamtzeit in Sekunden in einem Jahr: 31536000 Sekunden. **2.** Das Fehlerbudget wird als 1 – (gewünschte) Verfügbarkeit bestimmt: 1 – 0,9999 = 0,0001. **3.** Konvertieren des Fehlerbudgets in Zeiteinheiten. Wenn das Fehlerbudget beispielsweise 0,0001 beträgt: • Fehlerbudget in Sekunden = 0,0001 * 31.536.000 Sekunden = 3.153,6 Sekunden. • Fehlerbudget in Minuten = 3.153,6 Sekunden / 60 = 52,56 Minuten. • Fehlerbudget in Stunden = 52,56/60 = 0,875 Stunden. • Fehlerbudget in Tagen = 52,56 Minuten / (24 * 60) ≈ 0,0364 Tage. **Hinweis:** Ihr Fehlerbudget wird nur dann in Einheiten von Tagen, Stunden, Minuten und Sekunden angezeigt, wenn Sie Ihr SLO nach Dauer messen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Messung nach Anzahl

SLO-Typ	„Nach Zeiträumen zählen oder „Nach Auftreten zählen“
Limit occurrences (Limit Vorkommen)	Die Anzahl der Vorkommen, nach denen ein Verstoß auftritt. Grenzwertvorkommen wirken wie ein Fehlerbudget.
Compliance-Zeitraum	Zeitraum, für den die Metriken berechnet werden. Verfügbare Optionen: • **Monat**: Als Dauer wird der aktuelle Monat betrachtet. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer vom 1. Januar bis zum 31. Januar angenommen. • **Rollend, 7 Tage**: Für die Dauer werden 7 Tage ab dem aktuellen Datum angenommen. • **Rollend, 30 Tage**: Für die Dauer werden 30 Tage ab dem aktuellen Datum angenommen. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer ab dem 25. Dezember berücksichtigt. • **Rollend, 90 Tage**: Für die Dauer werden 90 Tage ab dem aktuellen Datum angenommen. Wenn das aktuelle Datum beispielsweise der 26. Januar ist, wird die Dauer ab dem 25. Oktober berücksichtigt.

Hinweis: Die **Zuweisungsgruppe** wird automatisch gefüllt.

Formular „SLI erstellen“.

Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien, damit Sie und Ihr Team Ihre Serviceintegrität nachverfolgen und bei Bedarf die erforderlichen Maßnahmen ergreifen können.

Formular „Servicelevel-Indikatoren“.

Richten Sie Ihre Servicelevel-Indikatoren ein. Weitere Informationen finden Sie unter Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien.

Formular „Servicelevel-Indikator“

Feld	Beschreibung
SLI-Name	Name des SLI.
Datenquelle für SLIs	Automatisch ausgefüllt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Servicelevel-Indikator“ (Fortsetzung)

Feld	Beschreibung
	Standardmäßig ist dies die Datenquelle für Warnungen, die zur Berechnung des Fehlerbudgets für diesen Service verwendet werden.
Bedingungen festlegen Bedingungen zur Auswahl des relevanten SLI aus den verfügbaren Warnungsdatenquellen.	
Neuer Bedingungssatz	Um neue Bedingungen hinzuzufügen.

Formular „Fehlerbudget-Richtlinien erstellen“.

Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien, damit Sie und Ihr Team Ihre Serviceintegrität nachverfolgen und bei Bedarf die erforderlichen Maßnahmen ergreifen können.

Formular „Fehlerbudget-Richtlinien“.

Richten Sie das Formular für Fehlerbudget-Richtlinien ein. Weitere Informationen finden Sie unter Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien.

Formular „Fehlerbudget-Richtlinien“.

Feld	Beschreibung
Schwellenwert für	• **Durchsatz (Anzahl)**: Prozentsatzrate, mit der ein Fehlerbudget verbraucht wird. • **Verbleibendes Fehlerbudget (%)**: Prozentsatz des verbleibenden Fehlerbudgets für den angegebenen Zeitraum. **Hinweis:** Die Werte **Durchsatz** und **Verbleibendes Fehlerbudget** unterstützen bis zu vier Dezimalstellen und runden dann auf. Für eine Richtlinie können Sie mehrere Schwellenwerte hinzufügen. Sie können jedoch keine doppelten Schwellenwerte hinzufügen. Wenn Sie versuchen, doppelte Schwellenwerte hinzuzufügen, wird eine Fehlermeldung angezeigt.
Schwellenwert	• Für **Durchsatz**: Der ideale Durchsatz liegt bei 1 oder darunter, da dies darauf hinweist, dass das Fehlerbudget mit der erwarteten Geschwindigkeit verbraucht wird. Der Schwellenwert wird überschritten,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

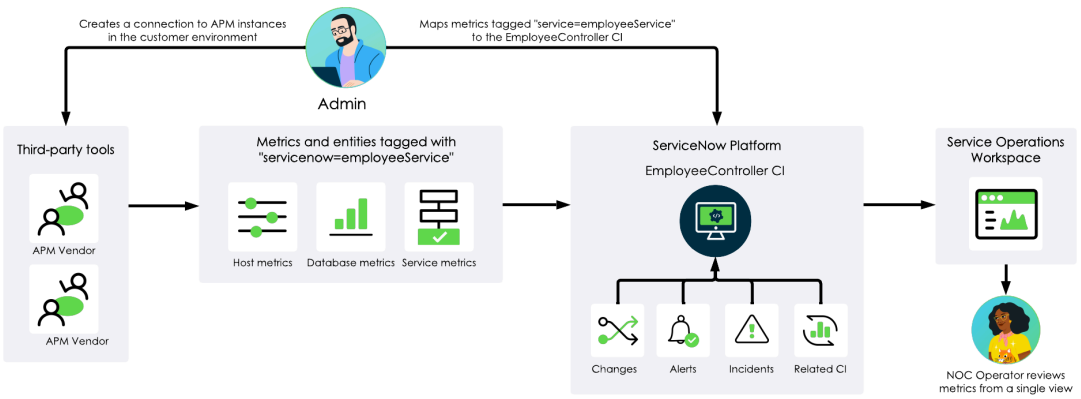
Formular „Fehlerbudget-Richtlinien“. (Fortsetzung)

Feld	Beschreibung
	wenn der Durchsatz größer oder gleich dem angegebenen Wert ist. • Für **Verbleibendes Fehlerbudget**: Der Schwellenwert wird überschritten, wenn der verbleibende Prozentsatz kleiner oder gleich dem angegebenen ist.
Wenn der Schwellenwert überschritten wird, dann	Aktion, die Sie ausführen möchten, wenn ein Verstoß auftritt. • Incident erstellen • E-Mail senden

Service-Beobachtbarkeit

Die Anwendung ServiceNow® Service-Beobachtbarkeit ermöglicht Anwendern das Selektieren und Verwalten von Incidents in einem komplexen und verteilten System. Anwendungs- und Plattform-Telemetrieeinblicke aus mehreren Observability-Tools werden in einem zentralen Workflow kombiniert.

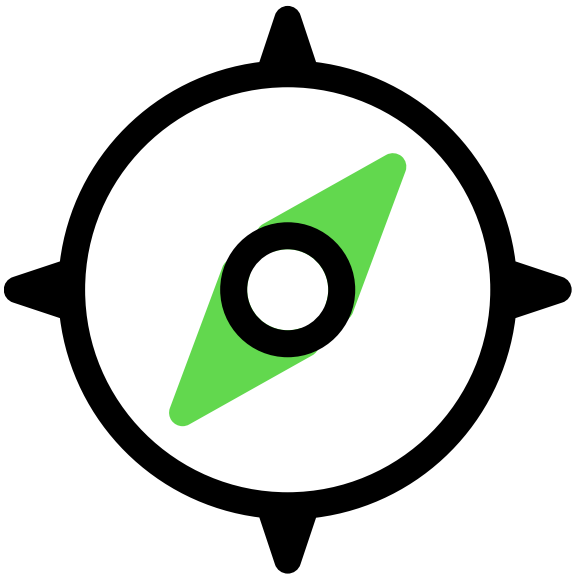
Übersicht über Service Observability



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

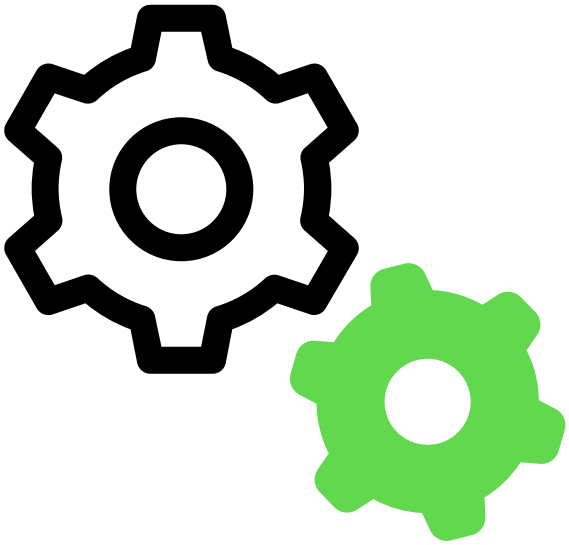
Erste Schritte

Untersuchen



Erfahren Sie, wie Service-Beobachtbarkeit unterschiedliche Daten zusammenführt, um Bediener bei der Suche nach Problemen in Ihrem System zu unterstützen

Konfigurieren

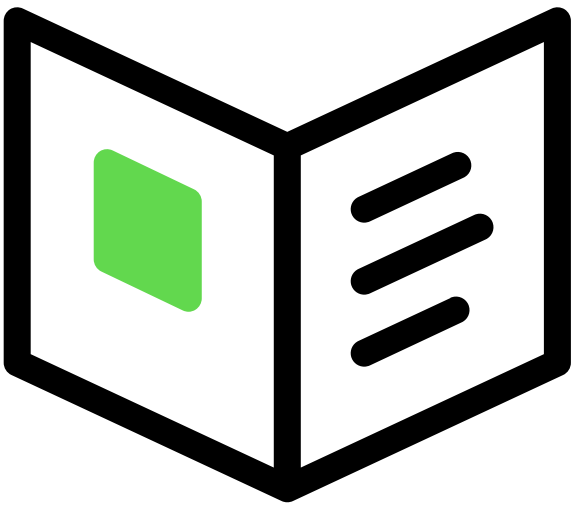


Erfahren Sie, wie Sie installieren und konfigurieren Service-Beobachtbarkeit

Überwachen und untersuchen

Erfahren Sie, wie Sie die Quelle von Problemen finden und den Zustand von Services und den zugehörigen Infrastrukturentitäten anzeigen können

Referenz



Hier finden Sie Referenzinformationen zu Service-Beobachtbarkeit

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hilfreiche Ressourcen

Einige ServiceNow -Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

ServiceNow Community

ServiceNow Community

Customer Success Center

Customer Success Center

Entwickler

developer.servicenow.com

Impact

http://impact.servicenow.com

ServiceNow University

ServiceNow University

NowCreate

Now Create

Partner

https://www.servicenow.com/partners.html

ServiceNow

http://www.servicenow.com

ServiceNow Store

ServiceNow Store

Unterstützung

- https://support.servicenow.com/now
- Known Error-Portal

Service-Beobachtbarkeit erkunden

Service-Beobachtbarkeit unterstützt Betriebsteams bei der Selektierung und Verwaltung von Incidents in einem komplexen und verteilten Produktionssystem. Es kombiniert Telemetriedaten aus externen APM-Systemen (Application Performance Monitoring) mit zugehörigen Daten in Configuration Management Database (CMDB). Beide werden in einem einzigen Workflow in Service Operations-Arbeitsbereich (SOW) angezeigt.

Service-Beobachtbarkeit – Übersicht

Service-Beobachtbarkeit zeigt Integritätsmetriken in SOW an, die sich auf einen bestimmten Service beziehen. Metriken können aus einem externen APM-System erfasst und neben Metriken für zugehörige Configuration Items im CMDBangezeigt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Service-Beobachtbarkeit unterstützt die folgenden APM-Anbieter:

- Dynatrace
- New Relic

Service-Beobachtbarkeit unterstützt die folgenden Datenbanken:

- MySQL
- PostgreSQL

Nachdem Sie eine APM-Instanz mit Service-Beobachtbarkeitverbunden haben, ordnen Sie die in CMDB registrierten Services den APM-Metriken zu, indem Sie vorhandene Tags in den APM-Daten verwenden.

Mit dieser Datenzuordnung kann Service-Beobachtbarkeit Metriken von APM-Entitäten, die Ihrem Service zugeordnet sind, z. B. einem Host oder einer Datenbank, zusammen mit Informationen aus zugehörigen CIs an einem Ort anzeigen. Um die Integrität des Service zu verstehen, verwenden Operatoren die APM-Metriken, zugehörige CI-Informationen und hilfreiche Kontextinformationen wie aktuelle Incidents und Warnungen im Zusammenhang mit dem Service.

Angenommen, Sie verwenden Dynatrace, um Ihren `Checkout-` Service zu überwachen, und Metriken aus Ihrer Datenbank und Ihrem Host verwenden das Tag `checkout-service`, um Anforderungen zu kennzeichnen, die von diesem Service stammen. Durch Zuordnung des `Checkout` -Service-CI zu den APM-Daten, die mit dem `Checkout-Service-Tag`markiert sind, ruft Service-Beobachtbarkeit Metriken für die Datenbanken und Hosts sowie die CIs ab, die sich auf den Service beziehen, und zeigt sie dann zusammen an. Operatoren können Probleme bei Entitäten im Zusammenhang mit dem Service lokalisieren und den Risikominderungsprozess eingrenzen, ohne den SOWverlassen zu müssen.

Service-Beobachtbarkeit Anwender

Anwender

Anwender	Beschreibung
Systemadministrator	Systemadministratoren konfigurieren Benutzer und Teams, registrieren zu überwachende Services, verbinden Service-Beobachtbarkeit mit APMs und ordnen diese Services dann den Daten zu. Sie können die Daten auch im anzeigen SOW
Administrator	Service-Beobachtbarkeit -Administratoren können einzelne zu überwachende Services registrieren. Sie können auch die Daten im SOWanzeigen.
Betreiber/ Betriebsleiter	-Operatoren verwenden Service-Beobachtbarkeit für die Selektierung von Incidents im SOW. Sie können grundlegende Integritätsmetriken für einen Service zusammen mit zugehörigen Incidents, Warnungen und Changes anzeigen. Ausführliche Informationen erhalten sie, indem sie zur Registerkarte **Erkennbarkeit** navigieren, um zusätzliche Servicemetriken zusammen mit Metriken zugehöriger Entitäten wie einem Host oder einer Datenbank anzuzeigen.

Service-Beobachtbarkeit – Workflow

Administratoren konfigurieren Service-Beobachtbarkeit, indem sie Services registrieren, APM-Metriken verbinden und die Services dann diesen Daten zuordnen. Mit Service-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beobachtbarkeit können Operatoren ermitteln, ob eine andere zugehörige Entität Probleme verursacht, die durch die Leistung des Service zu Tage getreten sind.

Als Systemadministrator:

1. Bestimmen Sie die von Service-Beobachtbarkeit zu überwachenden Services basierend auf der Geschäftskritikalität, und registrieren Sie diese Services dann.
2. Verbinden Sie vorhandene APM-Instanzen mit Service-Beobachtbarkeit.
3. Ordnen Sie registrierte Services APM-Metrikdaten basierend auf APM-basierten Tags zu, die für diese Daten verwendet werden.

Als Operator oder Manager:

1. Erkennen Sie ein Problem mit einem Service während der Arbeit in SOW, z. B. anhand einer Warnung, des Service-Dashboards oder Express-Liste, und navigieren Sie dann zur Seite „Servicedetails“.
2. Zeigen Sie allgemeine Integritätsmetriken für den Service zusammen mit zugehörigen Incidents, Warnungen und Changes an. Wenn eine der Metriken fehlerhaft erscheint, navigieren Sie zur Registerkarte Erkennbarkeit.
3. Zeigen Sie detailliertere Servicemetriken sowie Informationen von zugehörigen Entitäten an, um die Untersuchung der Ursache zu starten. Wenn Sie feststellen, dass das Problem weiter unten im Stapel des Systems liegt, identifizieren Sie den Besitz für diese Entität, um die Korrektur zu starten.

Service-Beobachtbarkeit – Vorteile

Vorteil	Funktion	Anwender
Zentralisieren Sie kritische Signale und überbrücken Sie Workflows, um Agilität und Zuverlässigkeit zu erhöhen: • Verbinden Sie Daten aus externen APMs • Ordnen Sie diese Daten den -Services CMDB zu • Zeigen Sie kombinierte Daten in an SOW	• Verbinden Sie eine Observability-Datenquelle • Zuordnungen von Erkennbarkeitsdaten erstellen und verwalten .	Administratoren
Steigern Sie die Effizienz und verkürzen Sie die durchschnittliche Zeit bis zur Lösung (Mean Time to Resolution, MTTR), indem Sie kombinierte Metriken von Entitäten anzeigen, die einem Service zugeordnet sind, um den Blast-Radius und die Verantwortlichkeit für einen Incident zu bestimmen.	Zeigen Sie Serviceintegritätsmetriken an	Operatoren
Zeigen Sie an einem Ort zugehörige Änderungen am System und Warnungen an, die einem Service zugeordnet sind.	Zeigen Sie die allgemeine Serviceintegrität an.	Operatoren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Service-Beobachtbarkeit finden Sie unter:

- Service-Beobachtbarkeit konfigurieren
- Zeigen Sie die allgemeine Serviceintegrität an
- Zeigen Sie Serviceintegritätsmetriken an
- Service-Beobachtbarkeit – Referenz

Service-Beobachtbarkeit konfigurieren

Nach der Installation von Service-Beobachtbarkeitmüssen Sie Services registrieren, externe APM-Instanzen (Application Performance Management) verbinden und diese APM-Daten diesen Services zuordnen.

Konfiguration – Übersicht

Service-Beobachtbarkeit installieren

Wenn Sie über die Systemadministratorrolle verfügen, können Sie die Anwendung Service-Beobachtbarkeit (`sn_sow_svcobs`) installieren. Die Anwendung installiert die zugehörigen ServiceNow® Store -Anwendungen und Plugins, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfung des folgenden Elements: Service-Beobachtbarkeit Anwendungsliste in ServiceNow Store, um Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Releasekompatibilität zu erhalten.

Erforderliche Rolle: Systemadministrator [admin]

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Service-Beobachtbarkeit installiert:

- Plugins
- Store-Anwendungen
- Rollen
- Tabellen

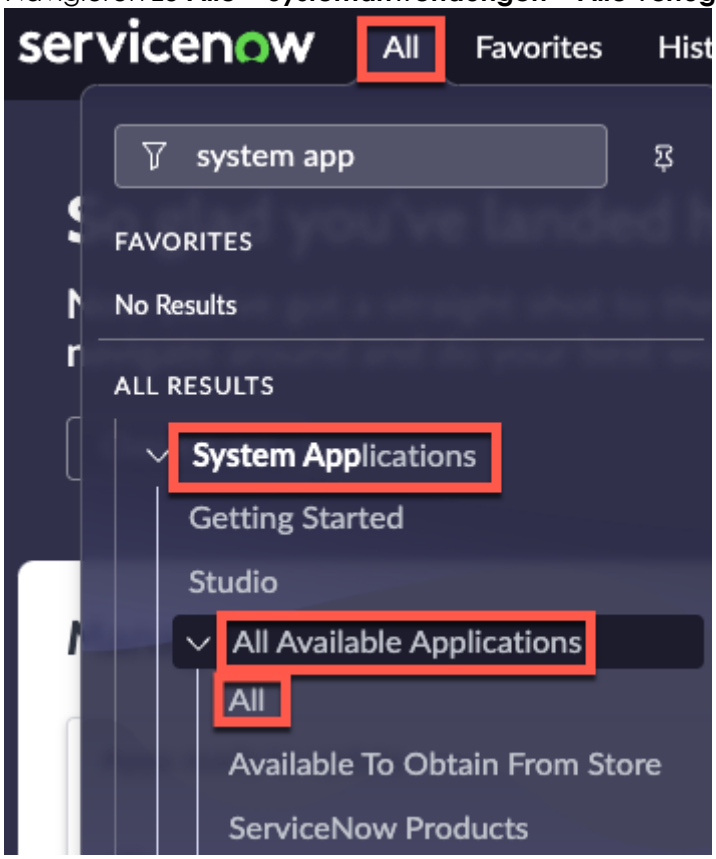
Weitere Informationen finden Sie unter Mit Service-Beobachtbarkeit installierte Komponenten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Service-Beobachtbarkeit (`sn_sow_svcobs`).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Teams und Services aktivieren

Weisen Sie Service-Beobachtbarkeit vorhandene Teams zu, damit sie die von Configuration Management Database (CMDB) zurückgegebenen Daten auf diesen Seiten anzeigen können. Aktivieren Sie die Services in CMDB zur Verwendung in Service-Beobachtbarkeit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Benutzer, die einer Gruppe zugewiesen sind, die die aktivierten Services verwaltet.
- Services, die Sie in Service-Beobachtbarkeit überwachen möchten, müssen in CMDBkonfiguriert sein.

Erforderliche Rolle: Systemadministrator [admin]

Warum und wann dieser Vorgang ausgeführt wird

Teams werden sowohl in Service Reliability Management als auch in Service-Beobachtbarkeit verwendet, um vorhandenen Rollen und Gruppen die Möglichkeit zu geben, CMDB -Daten auf den Registerkarten **„Übersicht“** und **„Erkennbarkeit“** anzuzeigen.

Die Services, die Sie in Service-Beobachtbarkeit überwachen möchten, müssen aktiviert sein. Durch die Aktivierung können Sie diesem Service Daten aus einer APM-Instanz (Application Performance Management) zuordnen und dann die zugehörigen Daten dieses Service auf den Registerkarten **Übersicht** und **Erkennbarkeit** anzeigen.

Hinweis: Teams und Services, die für Service-Beobachtbarkeit aktiviert wurden, werden auch für Service Reliability Management (SRM) aktiviert. Service-Beobachtbarkeit -Administratoren können einen einzelnen Service erstellen. Weitere Informationen finden Sie unter Services zu SRM hinzufügen. Wenn Administratoren Service-Beobachtbarkeit von einen einzelnen Service erstellen, wird er automatisch für Service-Beobachtbarkeit und SRMaktiviert. Weitere Informationen finden Sie unter Service Reliability Management.

Prozedur

1. Navigieren zu **Alle** > **Service Operations-Arbeitsbereich** > **Konfigurationen** und wählen Sie die Karte **Service Operations Management**.
2. Navigieren zu **Servicebetriebsmanagement** > **Zuweisen und aktivieren** > **Teams und Services aktivieren**.
3. Wählen Sie **Teams und Services aktivieren**.
4. Wählen Sie die Zuweisungsgruppen aus, die Sie als Teams in Service-Beobachtbarkeit möchten, und wählen Sie dann **Aktivieren**aus.
   Es werden nur Teams angezeigt, die noch nicht zugewiesen wurden.
5. Wählen Sie im Modal **Bestätigen**aus.
6. Wählen Sie im Dropdown-Menü Serviceklasse den Servicetyp CMDB aus.
7. Wählen Sie in der Liste der Services aus, welche Services für Service-Beobachtbarkeit aktiviert werden sollen, und wählen Sie **Aktivieren**aus.
8. Wählen Sie im Modal ein Support-Team für die Services aus, und wählen Sie **Bestätigen**aus.
   Sie haben jetzt Services, die in überwacht werden können Service-Beobachtbarkeit

Nächste Maßnahme

1. Verbinden Sie eine Observability-Datenquelle
2. Zuordnungen von Erkennbarkeitsdaten erstellen und verwalten

Verbinden Sie eine Observability-Datenquelle

Verbinden Sie Service-Beobachtbarkeit mit einer externen APM-Instanz (Application Performance Management). Service-Beobachtbarkeit zeigt Metriken in Service Operations-Arbeitsbereich (SOW) aus dieser APM-Instanz an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Für Dynatrace-Verbindungen muss der von Ihnen verwendete API-Schlüssel über Berechtigungen `zum Lesen von Entitäten` und `zum Lesen des` Metrikbereichs verfügen.

Erforderliche Rolle: Systemadministrator [admin]

Warum und wann dieser Vorgang ausgeführt wird
Service-Beobachtbarkeit akzeptiert Daten von New Relic und Dynatrace. Der erste Schritt zur Erfassung dieser Daten besteht darin, eine Verbindung zur APM-Instanz herzustellen.

Prozedur
1. Navigieren zu **Alle** > **Service Operations-Arbeitsbereich** > **Konfigurationen** und wählen Sie die Karte **Service Operations Management**.
2. Navigieren zu **Service Observability Management** > **Verwalten Sie Erkennbarkeitsdaten** > **Datenquellen**.
3. Wählen Sie entweder **New Relic** oder **Dynatrace**aus.
4. Verwenden Sie eine vorhandene HTTP- oder HTTPS-Verbindung und vorhandene API-Schlüssel-Anmeldeinformationen, oder erstellen Sie eine.
5. Füllen Sie die Felder des Formulars „Verbindung hinzufügen“ aus.
   Eine Beschreibung der Feldwerte finden Sie unter Formular „Verbindung hinzufügen“..
6. Wählen Sie **Speichern**.

Ergebnisse
In der Liste der Erkennbarkeitsdatenquellen wird eine neue Verbindung angezeigt. Sie verwenden diese Verbindung, wenn Sie eine Datenzuordnung erstellen.

Nächste Maßnahme
Ordnen Sie Ihre Verbindung den Services zu, die Sie in Service-Beobachtbarkeitüberwachen möchten. Weitere Informationen finden Sie unter Zuordnungen von Erkennbarkeitsdaten erstellen und verwalten.

Zuordnungen von Erkennbarkeitsdaten erstellen und verwalten

Ordnen Sie Ihre Services den Daten einer verbundenen externen APM-Instanz (Application Performance Management) zu, und zeigen Sie sie in Diagrammen für den Service und die zugehörigen Entitäten an.

Vorbereitungen
- Aktivieren Sie die Services, die Daten aus einer externen APM-Instanz enthalten. Anweisungen zum Aktivieren der Services finden Sie unter Teams und Services aktivieren.
- Verbinden Sie eine Observability-Datenquelle

Erforderliche Rolle: Systemadministrator [admin]

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie die Configuration Items (CIs) eines Service bestimmten Tag-Schlüssel/Wert-Paaren in den APM-Metrikmetadaten zuordnen, kann Service-Beobachtbarkeit Metriken mit diesen Tags im Kontext dieses Service und der zugehörigen CIs anzeigen. Diese Metriken sind nach den folgenden Entitätstypen gruppiert:

- Anwendungsmetriken: Metriken, die den Anwendungsservices zugeordnet sind
- Metriken berechnen: Metriken, die den Hosts der Anwendung zugeordnet sind

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Datenbanken: Metriken, die den von der Anwendung verwendeten Datenbanken zugeordnet sind

  Hinweis: Service-Beobachtbarkeit unterstützt die folgenden Datenbanken:

  - MySQL
  - PostgreSQL

Angenommen, Sie haben Metriken aus New Relic, die zur Überwachung von Services, Datenbanken und Hosts verwendet werden. Für diese Metriken haben Sie das Tag `service_name`verwendet. Angenommen, Sie haben auch das `Checkout-Service-` CI aktiviert und dann das `Checkout-` Service-CI dem APM-Metadaten-Schlüssel/Wert-Paar `service_name = checkout`zugeordnet. Service-Beobachtbarkeit zeigt alle Datenbank- und Hostmetriken, die mit `„service_name = checkout“` im Kontext des `Checkout` -Service-CI gekennzeichnet sind, zusammen mit zugehörigen CIs.

Wenn einige Ihrer Metriken in anderen Entitäten einen anderen Schlüsselnamen oder einen anderen Schlüsselwert verwenden, können Sie Ausnahmen erstellen. Wenn Ihre Hostmetriken beispielsweise `„service“` anstelle von `„service_name“`verwenden, können Sie eine Ausnahme erstellen, um diese Metriken einzubeziehen.

Jeder Entitätstyp verfügt über ein eigenes Dashboard, und jede Metrik und jedes zugehörige CI verfügt über ein eigenes Diagramm.

Prozedur

1. Navigieren zu **Alle** > **Service Operations-Arbeitsbereich** > **Konfigurationen** und wählen Sie die Karte **Service Operations Management**.
2. Navigieren zu **Service Observability Management** > **Observability verwalten** > **Datenzuordnungen** und wählen Sie **Zuordnung erstellen aus**.
3. Füllen Sie die Felder im Formular „Erkennbarkeitsdatenzuordnung“ aus. Eine Beschreibung der Feldwerte finden Sie unter Zuordnungsformular für Erkennbarkeitsdaten.
4. Wählen Sie **Zuordnung speichern**.
5. Wahlweise: Wenn einige Ihrer Entitäten andere Schlüsselnamen oder -werte verwenden, erstellen Sie Ausnahmen von der Standardrichtlinie, indem Sie diese auf der Karte Ausnahmen konfigurieren.

Ergebnisse

Auf der Registerkarte **Erkennbarkeit** der Seite Servicedetails werden Dashboards und Diagramme für die im Mapping gefundenen Entitäten angezeigt.

Überwachen Sie Services, und untersuchen Sie Probleme

Anwender verwenden Service-Beobachtbarkeit, um die Integrität ihrer Services zu überwachen und Incidents zu selektieren und zu verwalten, indem sie Leistungsmetriken aus externen APM-Systemen (Application Performance Management) im Kontext eines Anwendungsservice und der zugehörigen CIs anzeigen.

Übersicht über die Verwendung von Service-Beobachtbarkeit

Service-Beobachtbarkeit kann Metriken aus einer APM-Instanz im Kontext eines Service anzeigen. Neben Metriken für den Service und Informationen zu zugehörigen CIs kann Service-Beobachtbarkeit auf mit dem Service verbundene Entitäten wie Host oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenbank ableiten und deren Metriken anzeigen. Diese Funktionalität ermöglicht dem Bediener eine ganzheitlichere Ansicht der möglichen Auswirkungen auf die Leistung.

Auf der Registerkarte **Übersicht** auf der Seite Servicedetails werden allgemeine Leistungsmetriken für den Service und andere kontextbezogene Informationen wie offene Warnungen oder Incidents, die sich auf den Service auswirken, angezeigt. Auf der Registerkarte **Erkennbarkeit** werden detailliertere Metriken aus APM für den Service zusammen mit Metriken für abgeleitete Entitäten angezeigt, die durch während des Setups konfigurierte Datenzuordnungen gefunden werden. Außerdem werden Informationen zu CIs angezeigt, die sich auf diese abgeleiteten Entitäten beziehen. Anstatt zu einem externen Tool wechseln zu müssen, kann ein -Operator diese externen Metriken im Kontext von Service Operations-Arbeitsbereich (SOW) anzeigen.

- Zeigen Sie die allgemeine Serviceintegrität an

  Zeigen Sie auf der Registerkarte **Übersicht** der Seite Servicedetails in SOWdie allgemeine Serviceintegrität und zugehörige Informationen wie Warnungen und Changes an.

- Zeigen Sie Serviceintegritätsmetriken an

  Zeigen Sie auf der Registerkarte **Erkennbarkeit** detailliertere Servicemetriken sowie Metriken von zugehörigen, von APM überwachten Entitäten wie Datenbanken und Hosts an.

Zeigen Sie die allgemeine Serviceintegrität an

Zeigen Sie mit der Registerkarte **Übersicht** auf der Seite Servicedetails in SOWdie allgemeine Serviceintegrität und zugehörige Ereignisse wie Warnungen und Changes an.

Vorbereitungen

- Ein Service muss aktiviert werden. Weitere Informationen finden Sie unter Teams und Services aktivieren.
- Eine Datenzuordnung muss konfiguriert sein. Weitere Informationen finden Sie unter Zuordnungen von Erkennbarkeitsdaten erstellen und verwalten.

Erforderliche Rolle: Operator [snc_sow_svcobs.manager]

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie beispielsweise durch eine Warnung benachrichtigt wurden, dass bei einem Service Leistungsprobleme auftreten, können Sie Ihre Untersuchung auf der Registerkarte **Übersicht** auf der Seite Servicedetails beginnen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
   Auf die Seite „Servicedetails“ können Sie über die folgenden Seiten im SOWzugreifen:
   - **Servicesliste** : Wählen Sie einen Service aus der Liste aus.
   - **Service-Dashboard**: Wählen Sie im Dashboard einen Service und dann **Servicedetails**aus.
   - **Liste**: Navigieren Sie zu **Anwendungsservices** > **Services** und wählen Sie einen Service aus.
   - **Express-** Listenwarnung: Wählen Sie einen Service in der Spalte **Betroffene Services** aus.

   Die Seite Servicedetails wird geöffnet, und die Registerkarte Übersicht wird angezeigt.

   Trouble?
   Wenn in Diagrammen Fehlermeldungen angezeigt werden, lesen Sie unter Fehlerstatus des Diagrammsnach.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Verwenden Sie die Diagramme im Abschnitt „Übersicht“, um zu ermitteln, wo möglicherweise Leistungsprobleme auftreten.
   Im Abschnitt „Übersicht“ werden die Basismetriken für Rate, Fehler und Dauer (RED) zusammen mit Metriken für wichtige Transaktionen angezeigt, die im Service gefunden wurden. Bewegen Sie den Mauszeiger über eine Metrik, um weitere Details anzuzeigen.

   Hinweis: Wenn mehrere Services mit demselben Namen gefunden wurden, wählen Sie im Dropdown-Menü **Alle Services** einen einzelnen Service aus.

3. Ändern Sie den Zeitraum mithilfe der Dropdown-Liste **Zeitbereich**.
4. Verwenden Sie die anderen Diagramme auf der Seite, um zugehörige Informationen zum Service anzuzeigen, z. B. aktuelle Changes, offene Incidents und Trends für Incidents und Warnungen.
   Diese Diagramme helfen zu erklären, ob wiederkehrende Incidents oder Warnungen durch Leistungsprobleme im Service verursacht werden können. Ausführliche Informationen zur Verwendung dieser Seite finden Sie unter Registerkarte „Übersicht“ für Service-Beobachtbarkeit.

Nächste Maßnahme

Um detailliertere Metriken und Metriken für zugehörige Entitäten anzuzeigen, wählen Sie die Registerkarte **Observability (Erkennbarkeit)**. Weitere Informationen finden Sie unter Zeigen Sie Serviceintegritätsmetriken an.

Zeigen Sie Serviceintegritätsmetriken an

Zeigen Sie detaillierte Metriken für einen Service sowie Informationen und Metriken von zugehörigen Entitäten wie Datenbanken und Hosts auf der Registerkarte **Erkennbarkeit** in SOWan.

Warum und wann dieser Vorgang ausgeführt wird

Auf der Registerkarte **Erkennbarkeit** auf der Seite Servicedetails werden Metriken für zugehörige Entitäten angezeigt, die aus externen APM-Instanzen (Application Performance Management) abgeleitet wurden. So können Sie zugehörige Metriken anzeigen, ohne die Plattform ServiceNow verlassen zu müssen.

Die Metriken werden nach den folgenden Entitätstypen gruppiert:

- Anwendungsmetriken: Metriken, die den Anwendungsservices zugeordnet sind
- Computermetriken: Metriken, die den Hosts des Service zugeordnet sind
- Datenbanken: Metriken, die den vom Service verwendeten Datenbanken zugeordnet sind

Angenommen, Sie haben Metriken aus New Relic, die zur Überwachung von Services, Datenbanken und Hosts verwendet werden. Angenommen, Sie haben auch ein Problem mit dem `Checkout` -Service und möchten Leistungsinformationen und Metriken zu diesem Service anzeigen. Service-Beobachtbarkeit kann Ihnen die Service-, Datenbank- und Hostmetriken im Zusammenhang mit diesem Service anzeigen, die von New Relicstammen, zusammen mit zugehörigen CI-Informationen von der Plattform ServiceNow. Jeder Entitätstyp verfügt über ein eigenes Dashboard, und jede Metrik und zugehörige CI-Informationen verfügen über ein eigenes Diagramm.

Vorbereitungen

- Ein Service muss aktiviert werden. Weitere Informationen finden Sie unter Teams und Services aktivieren.
- Eine Datenzuordnung muss konfiguriert sein. Weitere Informationen finden Sie unter Zuordnungen von Erkennbarkeitsdaten erstellen und verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: Operator [snc_sow_svcobs.manager]

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
   Auf die Seite „Servicedetails“ können Sie über die folgenden Seiten im SOWzugreifen:
   - **Servicesliste** : Wählen Sie einen Service aus der Liste aus.
   - **Service-Dashboard**: Wählen Sie im Dashboard einen Service und dann **Servicedetails**aus.
   - **Liste**: Navigieren Sie zu **Anwendungsservices** > **Services** und wählen Sie einen Service aus.
   - **Express-** Listenwarnung: Wählen Sie einen Service in der Spalte **Betroffene Services** aus.

   Die Seite Servicedetails wird geöffnet, und die Registerkarte Übersicht wird angezeigt.

   Trouble?
   Wenn in Diagrammen Fehlermeldungen angezeigt werden, lesen Sie unter Fehlerstatus des Diagrammsnach.
2. Wählen Sie die Registerkarte **Observability (Erkennbarkeit)**.
   Auf der Registerkarte **Erkennbarkeit** werden die zugehörigen Metriken und CI-Informationen angezeigt, die für den Service verfügbar sind. Verwenden Sie den Navigationsbereich, um die Entitäts-Dashboards anzuzeigen.

   Hinweis: Wenn für eine Entität keine Navigationsoptionen angezeigt werden, wurden die Metriken für diese Entität nicht erkannt oder zugeordnet.
3. Wählen Sie eine Entität aus, um das zugehörige Dashboard anzuzeigen.
   Mit den Diagrammen können Sie:
   - Zeigen Sie Metriken für eine einzelne Entität an, indem Sie die Dropdown-Liste **Alle [Entitätstyp]** und dann eine Entität auswählen.

     Hinweis: Wenn mehr als eine Entität Metriken zurückgegeben hat, zeigen Diagramme mehrere Zeilen mit einer Zeile für jede Entität an.
   - Zeigen Sie Metriken aus einem anderen Zeitraum an, indem Sie in der Dropdown-Liste **Zeitbereich** einen Zeitraum auswählen. Der Standardzeitraum ist die letzte Stunde.
   - Aktualisieren Sie die Diagramme mit dem aktuellen Zeitraum der letzten Stunde, indem Sie die Schaltfläche **Aktualisieren** wählen.
   - Bewegen Sie den Mauszeiger über einen Punkt, um detaillierte Informationen anzuzeigen.

   Ausführliche Informationen zu dieser Seite finden Sie unter Registerkarte „Erkennbarkeit“ für Service-Beobachtbarkeit.

Service-Beobachtbarkeit – Referenz

Referenzthemen enthalten zusätzliche Informationen zur Verwaltung und Verwendung von Service-Beobachtbarkeit.

Mit Service-Beobachtbarkeit installierte Komponenten

Bei der Aktivierung des Service-Beobachtbarkeit-Plugins werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Benutzerrollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
Operator/Betriebsmanager [snc_sow_svcobs.manager]	Selektiert Incidents im SOW. Zeigt grundlegende Integritätsmetriken für einen Service und detailliertere Servicemetriken von zugehörigen Entitäten an.	• sn_sow_srm.srm_responder • connection_admin • evt_mgmt_connector_instance_write
Service-Beobachtbarkeit -Administrator [sn_sow_svcobs.admin]	Erstellt und aktiviert einzelne Services.	• sn_sow_srm.srm_admin • connection_admin • evt_mgmt_connector_instance_write

Installierte Store-Anwendungen

Folgendes wird installiert, wenn Sie Service-Beobachtbarkeitinstallieren.

Store-Anwendung [Plugin]	Beschreibung
Service-Beobachtbarkeit-Benutzeroberfläche sn_service_obs_ui]	Die Registerkarten „Übersicht“ und „Erkennbarkeit“ auf der Seite „Servicedetails“ von SOW.
Service Reliability Management	Service Reliability Management und Service-Beobachtbarkeit zeigen gemeinsam Serviceleistungsmetriken an, um einen ganzheitlichen Überblick über die Serviceintegrität zu geben.

Installierte Tabellen

Tabelle	Beschreibung
Dashboard-Fragmente [sn_sow_svcobs_dashboard_fragments]	Enthält die Definitionen von Dashboards im JSON-Format.
Konfigurationszuordnung für die Service-zu-Daten-Zuordnung [sn_sow_svcobs_svc_to_config_map]	Ordnet Datenzuordnungskonfigurationen mithilfe der Tabelle „CMDB-Gruppe enthält Konfigurationselement“ [cmdb_group_contains_ci] einem registrierten Service zu.
Konfigurationen für Datenzuordnungen	Definiert eine Datenzuordnungskonfiguration für einen Service.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
sn_sow_svcobs_mapping_config]	
Konfigurationsregeln für die Datenzuordnung [sn_sow_svcobs_mapping_config_rules]	Definiert eine einzelne Tag-basierte Zuordnungsregel.
Observability-Datenquelle [sn_sow_svcobs_data_source]	Definiert eine APM-Lieferantendatenquelle einer Drittpartei (ein `http_connections`), die zum Abrufen von Telemetriedaten für Services verwendet werden kann.
Datensätze der Service Observability-Entität [sn_sow_svcobs_entity_records]	Zeichnet Konfigurationselemente und unbekannte überwachte Objekte für Entitäten auf, die in Dashboards angezeigt werden.

Service-Beobachtbarkeit und Domain Separation

Service-Beobachtbarkeit unterstützt keine Domänentrennung. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Kein Support

- Das Feld „Domäne“ kann in Datentabellen vorhanden sein, es ist jedoch keine Geschäftslogik zum Verwalten der Daten vorhanden.
- Diese Ebene wird nicht als domänengetrennt betrachtet.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Formular „Verbindung hinzufügen“.

Feldbeschreibungen für das Formular „Verbindung hinzufügen“ beim Herstellen einer Verbindung mit einer Observability-Datenquelle. Fügen Sie eine Datenverbindung für Service-Beobachtbarkeit hinzu, um Daten von New Relic oder Dynatracezu erfassen. Sie können eine Verbindung und einen API-Schlüssel erstellen oder vorhandene verwenden.

Erstellen Sie eine Verbindung

Feld	Beschreibung
Name	Eindeutiger Name für die Verbindung. Der Name wird in der Tabelle „Erkennbarkeits-Datenquelle“ [sn_sow_svcobs_data_source] verwendet.
Verbindungs-URL	URL für die Verbindung. Diese URL wird der Tabelle mit den HTTP(s)-Verbindungen [http_connection] hinzugefügt.
Anwendername	Anwendername für die Verbindung. Wenn Sie einen vorhandenen API-Schlüssel verwenden, vergewissern Sie sich, dass es sich um den Namen handelt, der in der Tabelle „API-Schlüssel-Anmeldeinformationen“ [api_key_credentials] eingegeben wurde. Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Sie eine Verbindung erstellen, wird dieser Name in die entsprechende Tabelle eingegeben.

Erstellen Sie API Key-Anmeldeinformationen

Feld	Beschreibung
API-Schlüssel	API-Schlüssel für diese Verbindung. Dieser Schlüssel erstellt einen Eintrag in der Tabelle der API-Schlüssel-Anmeldeinformationen [api_key_credentials].

Verwenden Sie eine vorhandene Verbindung

Feld	Beschreibung
Verwenden Sie eine vorhandene HTTP(s)-Verbindung	Option zum Suchen nach einer vorhandenen Verbindung. Wählen Sie das Feld **HTTP-Verbindung** aus, um alle Ihre gültigen Verbindungen anzuzeigen.

Verwenden Sie einen vorhandenen API-Schlüssel

Feld	Beschreibung
Verwenden Sie vorhandene API-Schlüssel-Anmeldeinformationen	Option zur Suche nach vorhandenen API-Schlüssel-Anmeldeinformationen. Wählen Sie das Feld **API-Schlüssel** aus, um alle Ihre gültigen Anmeldeinformationen anzuzeigen.

Zuordnungsformular für Erkennbarkeitsdaten

Feldbeschreibungen für das Formular „Erkennbarkeitsdatenzuordnung“. Verwenden Sie dieses Formular, um aktivierte Services in Service-Beobachtbarkeit Metriken aus Ihrer APM-Instanz (Application Performance Monitoring) zuzuordnen. Jeder Service kann nur einmal zugeordnet werden, kann jedoch Ausnahmen enthalten, um alle zugehörigen Entitäten einzubeziehen.

Feld	Beschreibung
Zuordnungsname	Name für die Zuordnung. Der Name sollte beschreibend sein, damit Anwender verstehen, woher die Daten stammen.
Services	Für diese Zuordnung zu verwendender Service. Jeder Service kann nur einmal zugeordnet werden, und die Services müssen aktiviert sein, um zugeordnet zu werden. Informationen zum Aktivieren eines Service finden Sie unter Teams und Services aktivieren.
Standard	
Suchen Sie nach Metriken aus dieser Quelle	Vorhandene Datenverbindung zur Verwendung für Metriken. Informationen zum Hinzufügen einer Verbindung finden Sie unter Verbinden Sie eine Observability-Datenquelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
wobei der Quell-Tag-Schlüssel	Tag-Schlüssel, den Sie dem aktivierten Service zuordnen möchten. Wenn Sie mehr als ein Tag verwenden, um einen Service darzustellen, können Sie eine Ausnahme erstellen. Beispielsweise verwenden die meisten Tags `service_name`, mit Ausnahme von Datenbankmetriken, die `service`verwenden.
Quell-Tag-Wert	Wert, der den Servicenamen darstellt. Werte können Zeichenfolgen oder eine Variable sein, die Felder im CI für den Service darstellt. Sie können Variablen in Ihren APM-Daten als Wert verwenden, um mehrere Entitäten gleichzeitig zuzuordnen. Wenn in Ihren APM-Daten beispielsweise die Variable `$service_name` verwendet wird und Sie diesen Wert als **Quell-Tag-Wert**eingeben, werden alle Services zugeordnet, die diesen Wert verwenden.
Ausnahmen	
Für Entitätstyp	Entität, die einen anderen Schlüssel oder Wert als den Standardwert verwendet.
Suchen Sie nach Metriken aus dieser Quelle	Vorhandene Datenverbindung zur Verwendung für Metriken. Informationen zum Hinzufügen einer Verbindung finden Sie unter Verbinden Sie eine Observability-Datenquelle.
wobei der Quell-Tag-Schlüssel	Tag-Schlüssel, den Sie dem aktivierten Service für diese Entität zuordnen möchten.
Quell-Tag-Wert	Wert, der den Servicenamen darstellt. Werte können Zeichenfolgen oder eine Variable sein, die Felder im CI für den Service darstellt.

Registerkarte „Übersicht“ für Service-Beobachtbarkeit

Informationen, die auf der Registerkarte **Übersicht** der Seite Servicedetails in SOWangezeigt werden.

Datensatzheader

Der Header enthält grundlegende Informationen über den Service.

Bezeichnung	Beschreibung	Datenquelle
Klasse	CMDB Servicetyp für den Service.	CMDB
Discovery-Quelle	Discovery-Methode, die zum Eingeben des Service in CMDBverwendet wird.	CMDB
Aktualisiert	Zeitstempel, der angibt, wann die Servicekonfiguration zuletzt aktualisiert wurde.	CMDB
Betriebsstatus	Status des Service.	CMDB

Abschnitt „KPIs“.

Im Abschnitt „KPIs“ werden grundlegende Leistungsmetriken für den Service angezeigt.

Diagrammname	Beschreibung	Datenquelle
Kurs	Aggregierte Rate der Transaktionen über den Service.	APM-Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammname	Beschreibung	Datenquelle
Fehler %	Prozentsatz der Transaktionen, die einen Fehler aufweisen.	APM-Instanz
Latenz	Aggregierte Dauer von Transaktionen über den Service in Millisekunden.	APM-Instanz

Transaktionsdiagramme

Die Transaktionsdiagramme zeigen Metriken für bestimmte Schlüsseltransaktionen im Service an. Die Schlüsseltransaktionen hängen von Ihrer APM-Konfiguration ab.

Diagrammname	Beschreibung	Datenquelle
Kurs	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion durch den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	APM-Instanz
Fehler %	Jede Zeile stellt den Prozentsatz der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	APM-Instanz
Latenz	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion für den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	APM-Instanz

Abschnitt mit kontextbezogenen Informationen

In der Tabelle „Letzte Changes“ werden die am System vorgenommenen Änderungen angezeigt, die sich auf den Service auswirken können. Diese Daten stammen aus den zugehörigen Configuration Items in CMDB.

Abschnitt „Statusindikatoren“.

Im Abschnitt Statusindikatoren werden Diagramme für zugehörige CIs angezeigt, die sich möglicherweise auf den Service auswirken.

Diagrammname	Beschreibung	Datenquelle
SLO-Fehlerbudget	Informationen zu Ihrem aktuellen Fehlerbudget für diesen Service, wie in Service Reliability Management (SRM) konfiguriert. Weitere Informationen zu Fehlerbudgets finden Sie unter Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien.	CMDB
Betroffene Systeme	Services oder Serviceangebote, die in einer Beziehung mit dem ausgewählten Service stehen.	CMDB
Offene Incidents der letzten 30 Tage	Tägliches Auftreten offener Incidents, die diesen Service im letzten Monat betroffen haben.	CMDB
Offene Warnungen der letzten 30 Tage	Tägliches Vorkommen von Warnungen, die diesen Service im letzten Monat betroffen haben.	CMDB

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammname	Beschreibung	Datenquelle
Aktuelle offene Incidents	Liste der aktiven Incidents, die sich auf diesen Service auswirken.	CMDB
Aktuelle offene Warnungen	Liste der aktiven Warnungen, die sich auf diesen Service auswirken.	CMDB

Registerkarte „Erkennbarkeit“ für Service-Beobachtbarkeit

Informationen, die auf der Registerkarte **„Erkennbarkeit“** der Seite „Servicedetails“ in SOWangezeigt werden.

Anwendung > Service-Dashboard

Dieses Dashboard zeigt Leistungsmetriken für den ausgewählten Service an.

Grundlegende Metriken

Diagramm	Beschreibung	Datenquelle
Kurs	Aggregierte Rate der Transaktionen über den Service.	APM-Instanz
Fehler %	Prozentsatz der Transaktionen, die einen Fehler aufweisen.	APM-Instanz
Latenz	Aggregierte Dauer von Transaktionen über den Service in Millisekunden.	APM-Instanz
Client-Fehlerrate	Fehlerrate, die bei den Serviceclients aufgetreten ist.	APM-Instanz
Client-Durchsatz	Rate der Client-Anforderungen für diesen Service.	APM-Instanz
Client-Antwortzeit	Antwortzeit für Client-Anforderungen für diesen Service in Millisekunden.	APM-Instanz
DB-Verbindungen insgesamt	Anzahl der Datenbanken, zu denen dieser Client Verbindungen hat.	APM-Instanz
DB-Verbindungsfehler	Anzahl der Fehler, die der Client beim Versuch, auf Datenbanken zuzugreifen, empfangen hat.	APM-Instanz
Für Datenbankaufrufe aufgewendete Zeit	Dauer von Anforderungen an Datenbanken in Millisekunden.	APM-Instanz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Transaktionen

Diagramm	Beschreibung	Datenquelle
Kurs	Jede Zeile stellt den Durchsatz einer Schlüsseltransaktion durch den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	APM-Instanz
Fehler %	Jede Zeile stellt den Prozentsatz der Fehler für eine Schlüsseltransaktion im Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	APM-Instanz
Latenz	Jede Zeile stellt die Antwortzeit für eine Schlüsseltransaktion für den Service dar. Bewegen Sie den Mauszeiger über einen Punkt, um die verschiedenen Transaktionsnamen anzuzeigen.	APM-Instanz

Compute > Host-Dashboard

Dieses Dashboard zeigt Metriken für Hosts an, die mit dem Service zusammenhängen.

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozent der verbrauchten Rechenleistung des Hosts.	APM-Instanz
Arbeitsspeicherauslastung	Prozentsatz des Arbeitsspeichers, den der Host verwendet.	APM-Instanz
Festplattenauslastung	Verwendeter Speicherplatz in Prozent.	APM-Instanz
Alle aktiven Hosts	Informationen für alle Hosts, die der Service aktiv verwendet. Wählen Sie einen Host-Link, um detailliertere Informationen anzuzeigen.	CMDB

Datenbanken > MySQL

Dieses Dashboard zeigt Metriken für MySQL-Datenbanken an, die sich auf den -Service beziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagramm	Beschreibung	Datenquelle
CPU-Auslastung	Prozent der verbrauchten Rechenleistung der Datenbank.	APM-Instanz
Arbeitsspeicherauslastung	Prozentsatz des Arbeitsspeichers, den die Datenbank verwendet.	APM-Instanz
Verfügbarkeit	Prozentsatz der Zeit, in der die Datenbank verfügbar ist.	APM-Instanz
Verbindungen	Anzahl der Verbindungen zur Datenbank.	APM-Instanz
Langsame Abfragen	Anzahl der Datenbankabfragen, die von APM als langsam kategorisiert wurden.	APM-Instanz
Alle MySQL-Instanzen	Informationen für alle Datenbanken, die der Service aktiv verwendet. Wählen Sie einen Datenbanklink aus, um detailliertere Informationen anzuzeigen.	CMDB

Datenbanken > PostgreSQL

Dieses Dashboard zeigt Metriken für PostgreSQL-Datenbanken an, die sich auf den Service beziehen.

Diagramm	Beschreibung	Datenquelle
Geplante Prüfpunkte	Durchschnittliche Anzahl der geplanten Prüfpunkte, die tatsächlich durchgeführt wurden.	APM-Instanz
Für Prüfpunkt geschriebene Puffer	Durchschnittliche Anzahl der während Prüfpunkten geschriebenen Puffer.	APM-Instanz
Vom Hintergrund-Writer geschriebene Puffer	Durchschnittliche Anzahl der vom Hintergrund-Writer geschriebenen Puffer.	APM-Instanz
Zugeteilte Puffer	Durchschnittliche Anzahl der zugewiesenen Puffer.	APM-Instanz
Prüfpunkt-Schreibzeit	Zeit in Millisekunden, die zum Schreiben von Dateien auf den Datenträger aufgewendet wurde.	APM-Instanz
Alle PostgreSQL-Instanzen	Informationen aller Datenbanken, die der Service aktiv verwendet. Wählen Sie einen Datenbanklink aus, um detailliertere Informationen anzuzeigen.	CMDB

Fehlerstatus des Diagramms

Lernen Sie die verschiedenen Fehlerstatus kennen, die in den Diagrammen in Service-Beobachtbarkeit angezeigt werden können, und erfahren Sie, wie Sie sie beheben können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fehlermeldung	Beheben
Richten Sie die Erkennbarkeitsdatenzuordnung dieses Services ein	Die Observability-Zuordnung wurde für den Service nicht von einem Administrator konfiguriert. Weitere Informationen finden Sie unter Zuordnungen von Erkennbarkeitsdaten erstellen und verwalten.
Datenzuordnung ist nicht konfiguriert	Die Observability-Zuordnung wurde für den Service nicht von einem Administrator konfiguriert. Weitere Informationen finden Sie unter Zuordnungen von Erkennbarkeitsdaten erstellen und verwalten.
Authentifizierung fehlgeschlagen	Service-Beobachtbarkeit kann keine Verbindung zur Datenquelle herstellen. Weitere Informationen finden Sie unter Verbinden Sie eine Observability-Datenquelle.
Keine Ergebnisse gefunden	Für das Diagramm wurden keine Metriken gefunden.
Ein Fehler ist aufgetreten.	Die Verbindung mit der Datenquelle war erfolgreich, die APM-Instanz (Application Performance Management) hat jedoch nicht geantwortet. Dieser Fehler kann auf eine Verbindungszeitüberschreitung auf der APM-Seite zurückzuführen sein.
Keine betroffenen Systeme gefunden (Diagramm der betroffenen Systeme auf der Seite „Übersicht“)	Nur Services, die Sie in Ihrer Servicezuordnung finden, können angezeigt werden. Aktualisieren Sie Ihre Servicezuordnung so, dass sie alle Services enthält, die im Diagramm enthalten sein sollen. Weitere Informationen finden Sie unter Service-Mapping.
Ziele einrichten (SLO-Fehlerbudget-Diagramm auf der Übersichtsseite)	SLOs wurden nicht für Service Reliability Managementkonfiguriert. Weitere Informationen finden Sie unter Erstellen Sie SLO-, SLI- und Fehlerbudgetrichtlinien.

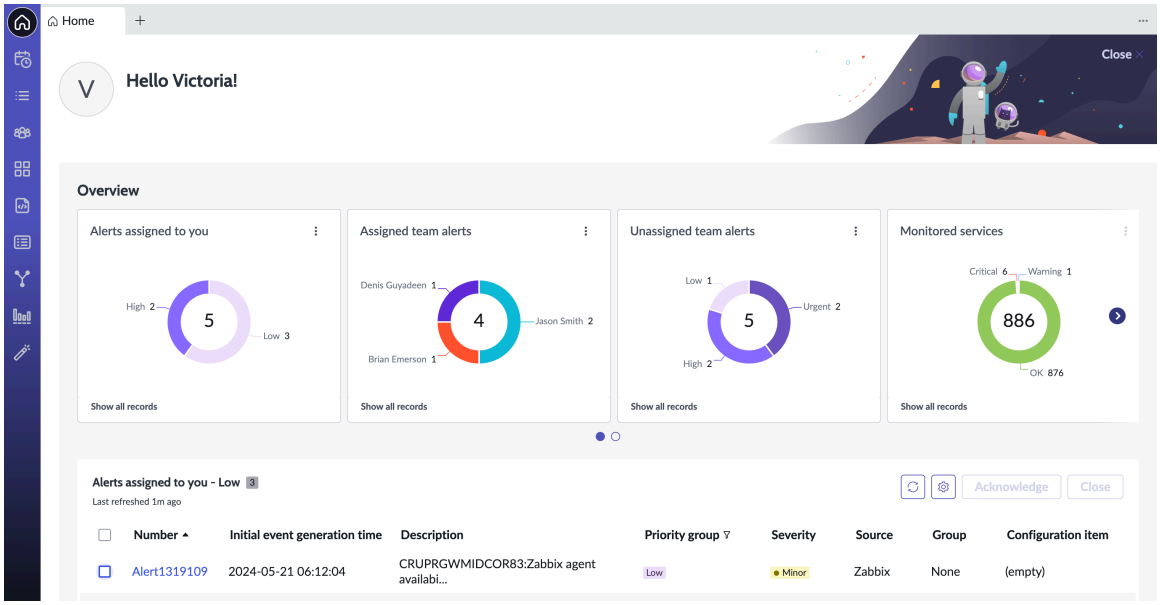
Service Operations-Arbeitsbereich für ITOM

ServiceNow® Service Operations-Arbeitsbereich (SOW) ist ein konfigurierbarer Arbeitsbereich zur Optimierung von IT Operations Management (ITOM) Workflows, der eine einheitliche Experience für mehrere IT-Betriebsprozesse bietet. Es ist konfigurierbar und anwenderfreundlich. Es fasst verschiedene Aufgaben in einer einzigen Oberfläche zusammen und ermöglicht so nahtlose Navigation und einfachen Zugriff auf Tools und Informationen.

Durch die Zentralisierung von Workflows verbessert sich die Zusammenarbeit, ermöglicht ein effizientes Aufgabenmanagement und bietet Echtzeiteinblicke durch verschiedene Metriken. Es ist hochgradig anpassbar und ermöglicht es Ihnen, den Arbeitsbereich an Ihre spezifischen Anforderungen anzupassen, um Produktivität und Workflow-Effizienz zu optimieren. Mit seinen umfassenden Funktionen, einschließlich Automatisierungs- und Zusammenarbeits-Tools, ermöglicht Service Operations-Arbeitsbereich Anwendern, effektiver in verschiedenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflows zu arbeiten und die Produktivität unternehmensweit zu steigern. Die Lösung ist entsprechend den sich ändernden Geschäftsanforderungen skalierbar und gewährleistet einen kontinuierlichen Support für IT-Umgebungen jeder Größe. Sie bietet hervorragende Services und verbessert die operative Qualität.



Informationen zu Abonnements für ITOM Service Operations-Arbeitsbereichfinden Sie im Abonnement von ITOM-Integrität unter Abonnement für ITOM Health.

Beim Einrichten von Service Operations-Arbeitsbereichist es wichtig, IT Operations Management (ITOM) für die Verwaltung von Warnungen und IT Service Management (ITSM) für die Lösung von Incidents und die Bereitstellung von Services zu konfigurieren. Dieses integrierte Setup gewährleistet den Zugriff auf alle Funktionen und erleichtert die umfassende Verwaltung des IT-Betriebs und der Servicequalität.

Informationen zu den Funktionen ITSM finden Sie unter Service Operations-Arbeitsbereich for ITSM .

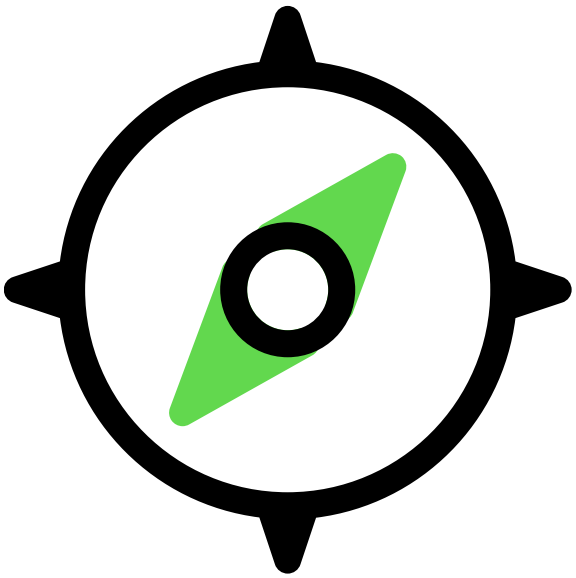
Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

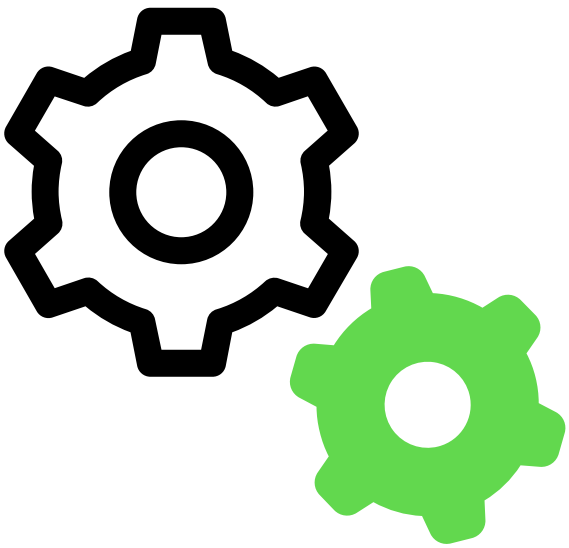
Erste Schritte

Untersuchen



Erfahren Sie mehr über die Konzepte und Funktionen Service Operations-Arbeitsbereich von [].

Konfigurieren



Konfigurieren Sie Umgebung, Tools und Benutzerzugriff

Verwenden

Erfahren Sie, wie Service Desk-Mitarbeiter verwenden können Service Operations-Arbeitsbereich

Referenz

Rufen Sie Details zu Service Operations-Arbeitsbereich -Komponenten wie Rollen und abhängigen Anwendungen ab

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Problembehandlung und Hilfe

Kontakt Kundenservice und Support

Service Operations-Arbeitsbereich für ITOM erkunden

Erfahren Sie, wie Service Operations-Arbeitsbereich für ITOM den gesamten Lebenszyklus von Warnungen optimiert, einschließlich Generieren, Benachrichtigung, Gruppieren, Analyse, Untersuchung, Lösung und Abschluss.

Übersicht über Service Operations-Arbeitsbereich

Service Operations-Arbeitsbereich für ITOM bietet leistungsstarke AIOps-Experience -Fähigkeiten, und zwar die Dashboards Express-Liste, Integrations Launchpad, Warnungsautomatisierungund AIOps, die jeweils einen eindeutigen Wert bieten.

Express-Liste

Express-Liste verbessert das Warnungsmanagement durch Bereitstellung einer konsolidierten Plattform für effiziente Selektierung, Ursachenanalyse (RCA) und Behebung von Warnungen. Mit Echtzeitaktualisierungen, dynamischen Filtern und einem intuitiven Vorschaubereich können Anwender ihre Warnungs-Workflows mühelos verwalten und sofort Maßnahmen ergreifen – mit beispielloser Geschwindigkeit und Geschwindigkeit.

Integrations-Launchpad

Integrations Launchpad bietet eine Schnittstelle zu nahtlosen Verbindungen mit verschiedenen externen Tools und Services und vereinfacht so das Onboarding neuer Datenquellen. Dadurch wird der Integrationsprozess optimiert, sodass Benutzer ihr vorhandenes ITOM -Ökosystem innerhalb der ServiceNow -Plattform mühelos nutzen können. Das Integrations-Launchpad verbessert den Datenaustausch und die plattformübergreifende Zusammenarbeit und steigert dadurch die Effizienz und Produktivität.

Warnungsautomatisierung

Die Warnungsautomatisierung bietet wichtige Unterstützung bei der Bewältigung komplexer IT-Infrastrukturen und steigender Datenmengen. Die manuelle Warnungsverarbeitung ist fehleranfällig und ineffizient, was den Bedarf an automatisierten Systemen unterstreicht. Durch das Ignorieren irrelevanter oder falsch positiver Warnungen durch die Automatisierung des Ignorierens von Warnungen und durch die Verwendung von Warnungsanreicherung, Gruppierung und Reaktion optimieren diese Systeme die Reaktion auf Warnungen, reduzieren menschliches Versagen und stellen konsistente und rechtzeitige Maßnahmen sicher.

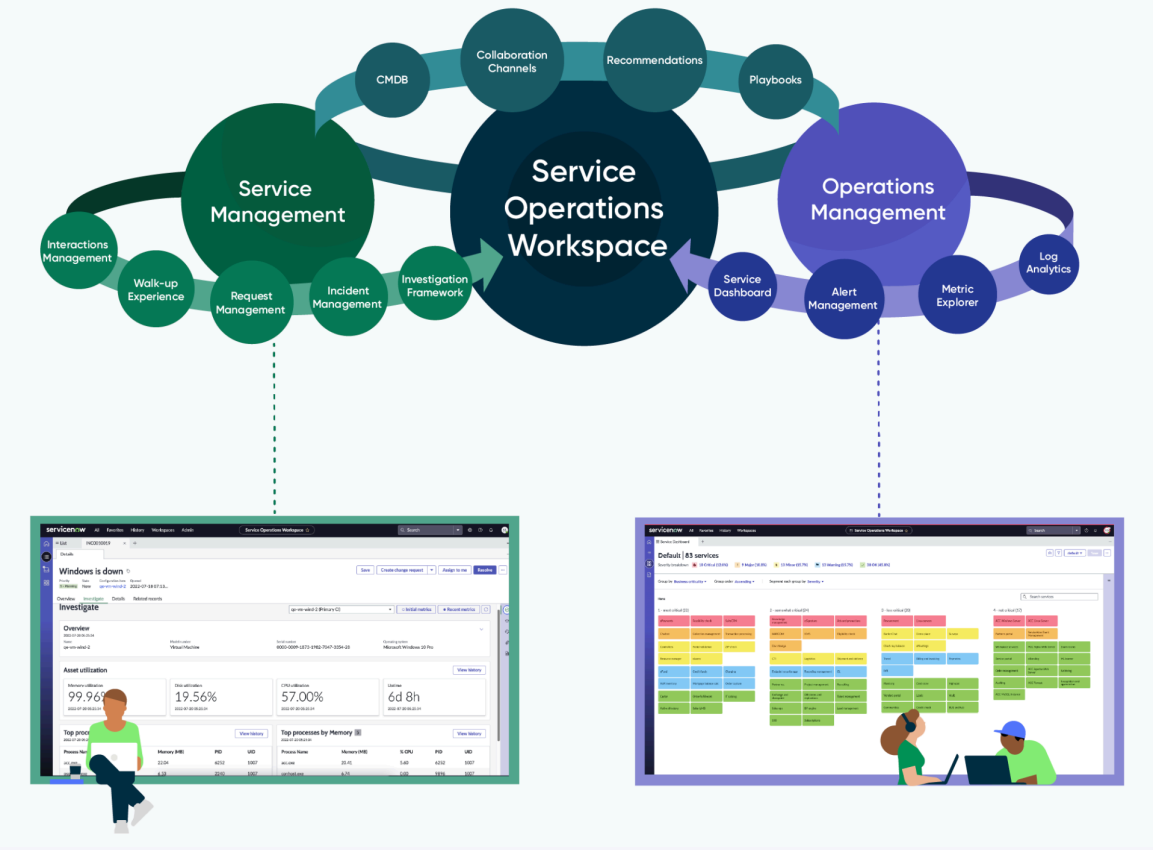
AIOps – Dashboards

AIOps-Dashboards bieten umfassende Visualisierungen kritischer Betriebsdaten und Einblicke. Benutzer können Leistungskennzahlen (Key Performance Indicators, KPIs) überwachen, die Serviceintegrität nachverfolgen und wertvolle Kontextinformationen zur gesamten IT-Umgebung abrufen. Diese anpassbaren Dashboards bieten Anwendern umsetzbare Einblicke, erleichtern die datengesteuerte Entscheidungsfindung und stellen proaktive Antworten auf potenzielle Probleme sicher.

Beim Einrichten von Service Operations-Arbeitsbereichist es wichtig, IT Operations Management (ITOM) für die Verwaltung von Warnungen und IT Service Management (ITSM) für die Lösung von Incidents und die Bereitstellung von Services zu konfigurieren. Dieses integrierte Setup gewährleistet den Zugriff auf alle Funktionen und erleichtert die umfassende Verwaltung des IT-Betriebs und der Servicequalität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weitere Informationen finden Sie unter Service Operations-Arbeitsbereich für ITSM erkunden .



Benutzer-Experience in Service Operations-Arbeitsbereich

1. Tagesbeginn: Der Operator prüft zunächst eine Übersicht über Warnungen und Metriken im Service Operations-Arbeitsbereich, um die Arbeit zu priorisieren.
2. Warnungspriorisierung: Der Operator priorisiert Warnungen basierend auf SLAs, Prioritätsstufe und Dringlichkeit.
3. Warnungsuntersuchung: Der -Operator untersucht Warnungen detailliert und nutzt dabei Verlaufsdaten und Trends.
4. Auf Warnungsinformationen zugreifen: Der Operator greift über die Warnungsdatensatzseite auf alle zugehörigen Informationen zu, um eine umfassende Ansicht zu erhalten.
5. Warnungen lösen: Mithilfe von maßgeschneiderten Empfehlungen löst der Operator Warnungen effizient.
6. Beratung durch Fachexperten (SME): Bei komplexen Aufgaben oder Aufgaben mit hoher Priorität wendet sich der Bediener an KMUs oder verwendet automatisierte Tools.
7. Zusammenarbeit: Der Operator arbeitet direkt von der Warnung aus mit Teammitgliedern und Stakeholdern zusammen, tauscht Einblicke aus und koordiniert Antworten.
8. Change-Anforderungen oder Wartung initiieren: Um zukünftige Vorkommnisse zu verhindern, initiiert der Operator Change-Anforderungen oder Wartungsaktivitäten, behebt die Ursachen und implementiert langfristige Lösungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender

Rollentitel [Name]	Beschreibung
Administrator [evt_mgmt_admin]	Konfiguriert Eigenschaften und Regeln für Ereignismanagement und richtet sie ein.
Betreiber [evt_mgmt_operator]	Verwaltet Warnungen, einschließlich Schließen und Bestätigen von Warnungen.
Anwender [evt_mgmt_user]	Verwaltet den Lebenszyklus von Warnungen, einschließlich der Durchführung grundlegender Vorgänge wie Anzeigen und Bestätigen von Warnungen.

Vorteile

Vereinheitlichen Sie die Experience für mehrere Workflows

Konsolidieren Sie verschiedene IT-Betriebs-Workflows in einer einzigen, intuitiven Oberfläche, um ein nahtloses Aufgabenmanagement in verschiedenen Bereichen des IT-Betriebs zu ermöglichen, die Effizienz zu steigern und die Komplexität zu reduzieren.

Stellen Sie automatisierte Empfehlungen bereit

Verbessern Sie die Effizienz und Entscheidungsfindung mit automatisierten Empfehlungen, die auf Bedieneraktionen zugeschnitten sind.

Stellen Sie Echtzeiteinblicke bereit

Stellen Sie Echtzeit-Analyse- und Berichterstellungsfunktionen für jeden integrierten Workflow bereit, die eine fundierte Entscheidungsfindung und eine proaktive Problemlösung ermöglichen, indem Sie wichtige Leistungsmetriken überwachen und den Betriebsstatus in Echtzeit verfolgen.

Zielgerichtete Experience

Bieten Sie dynamische und minimale Inhalte basierend auf der aktuellen Aufgabe an, wobei die nächste Aufgabe mit minimalen Klicks zugänglich ist. Ermöglichen Sie den Zugriff auf zugehörige Warnungen, um schnellere Antwortzeiten zu ermöglichen.

Passen Sie die Konfigurierbarkeit an

Ermöglichen Sie Organisationen, den Arbeitsbereich an bestimmte Anforderungen und Präferenzen anzupassen und die Produktivität zu optimieren, indem relevante Daten und Tools für jeden Workflow angezeigt werden.

Steigern Sie die Produktivität

Ermöglichen Sie Anwendern, effizienter in mehreren Workflows zu arbeiten, indem Sie Routineaufgaben automatisieren, Zugriff auf relevante Informationen gewähren und die Zusammenarbeit erleichtern, wodurch die Produktivität unternehmensweit gesteigert wird.

Nahtlos skalieren

Berücksichtigen Sie Änderungen in Bezug auf Arbeitsauslastung, Anforderungen und betriebliche Komplexität für alle integrierten Workflows, um unabhängig von der Organisationsgröße eine kontinuierliche Unterstützung für sich entwickelnde IT-Umgebungen sicherzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Liste der Arbeitsbereiche

Service Operations-Arbeitsbereich für die Anwenderoberfläche ITOM .

Erkunden Sie die Anwenderoberfläche, um zu verstehen, wie ein -Operator Aufgaben priorisieren und Lösungen anbieten kann.

Zugriff Service Operations-Arbeitsbereich

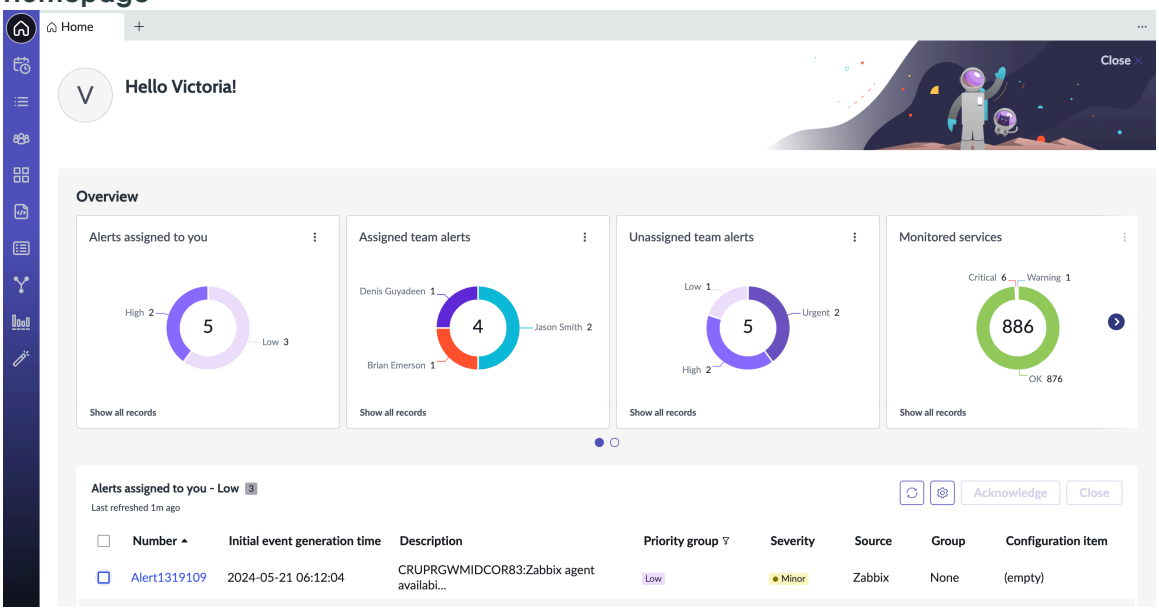
Öffnen Sie den Arbeitsbereich, indem Sie zu navigieren **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.

Homepage

Um auf Informationen auf der Homepage zuzugreifen, wählen Sie das Homepage-Symbol ( ).

Die Homepage von bietet Betreibern einen umfassenden Überblick über die aktuelle Betriebslandschaft. Der Abschnitt Übersicht enthält wichtige Einblicke, einschließlich dem Operator zugewiesener Warnungen, teambasierter Warnungen, nicht zugewiesener Teamwarnungen, überwachter Services und offener Warnungen. Dieser Abschnitt Ihnen zugewiesene Warnungen enthält spezifische Details zu Warnungen, die auf ihre Zuständigkeiten zugeschnitten sind. Zu den Informationen gehören die Warnungsnummer, die Generierungszeit des ersten Ereignisses, die Beschreibung, die Prioritätsgruppe, der Schweregrad, die Quelle, die Gruppe, das Configuration Item, der Status, der Knoten, der Metrikname und der Zeitstempel der letzten Aktualisierung. Beide Abschnitte optimieren den Betrieb, indem sie den Bedienern einen genauen Überblick und personalisierte Einblicke in Warnungen bieten, die für ihre Zuständigkeiten relevant sind. Dies erleichtern die schnelle Priorisierung und die proaktive Lösung kritischer Probleme.

Homepage



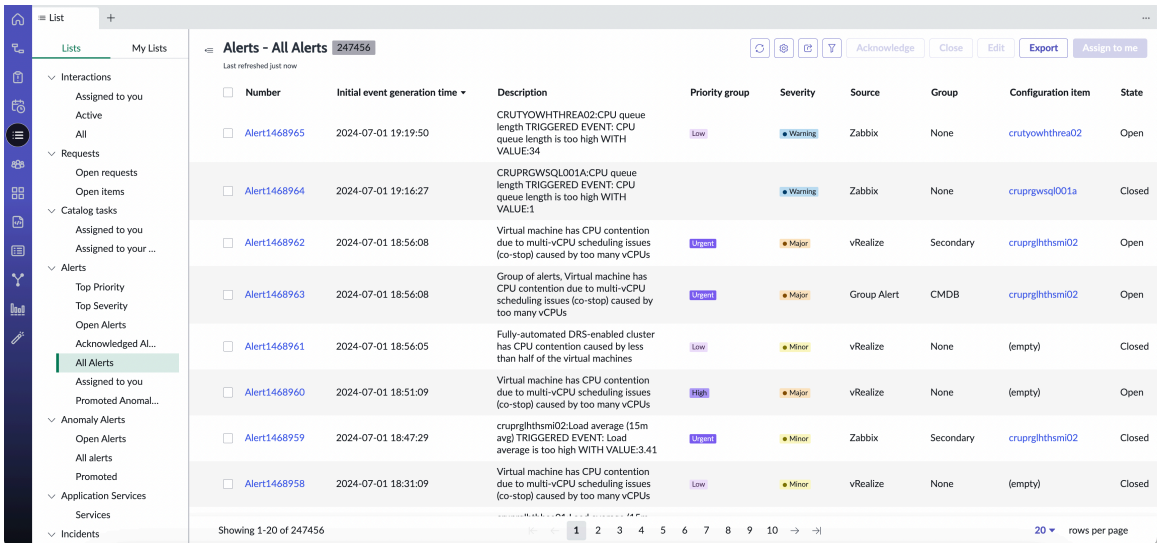
Listen-Seite

Um auf Informationen zu Warnungen in der Liste zuzugreifen, wählen Sie das Listensymbol ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Auf der Registerkarte **Listen** werden vordefinierte Listen angezeigt, während Benutzer auf der Registerkarte **Meine Listen** ihre eigenen Listen für die personalisierte Aufgabenverwaltung erstellen und anpassen können. Ausführliche Anweisungen zum Erstellen einer Liste finden Sie unter Liste in Service Operations-Arbeitsbereich für ITOMerstellen.

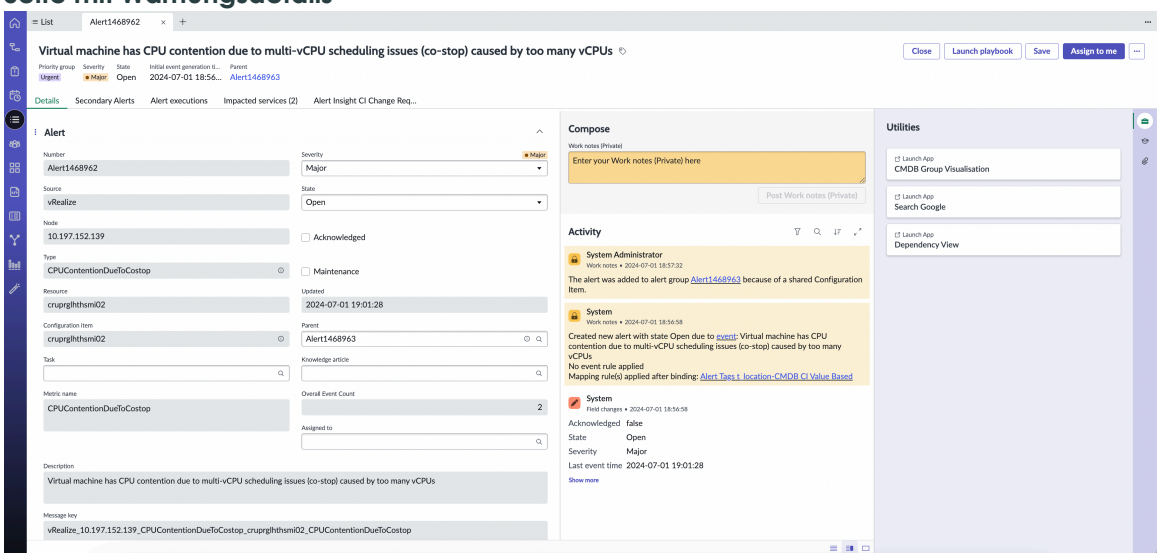
Listenseite



Datensatzansicht

Greifen Sie auf detaillierte Informationen für eine Warnung zu, indem Sie die entsprechende Warnungsnummer auswählen, um den Datensatz zu öffnen.

Seite mit Warnungsdetails



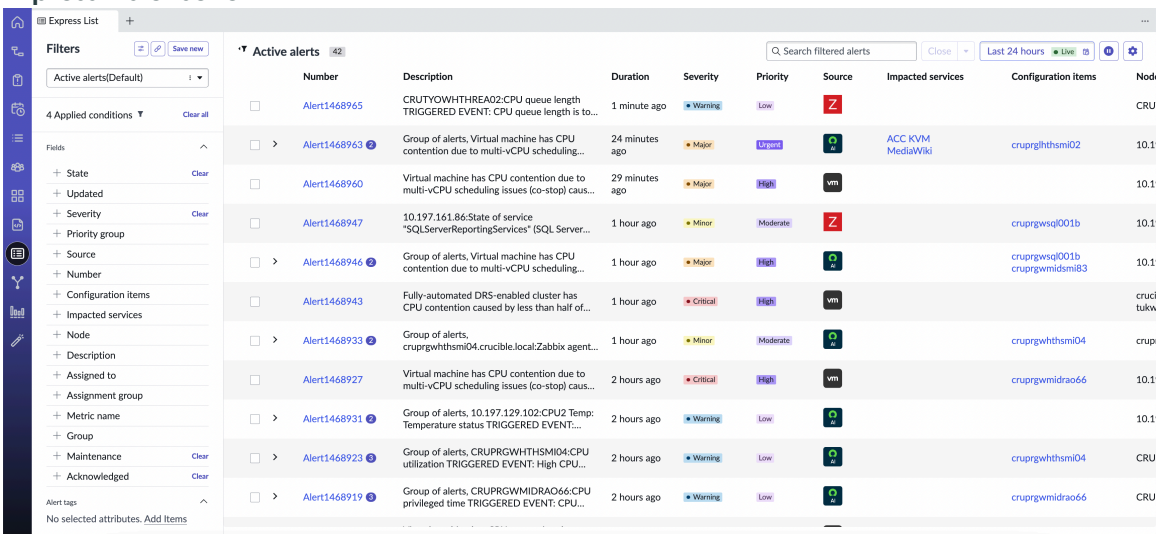
Express-Liste

Die Express-Liste bietet schnelle Warnungsinformationen für eine effiziente Überwachung, Lösung, Folgenbewertung, Nachverfolgung und Berichterstellung für Incidents.

Um auf Informationen in der Express-Liste zuzugreifen, wählen Sie das Symbol für die Express-Liste ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Express-Listenseite

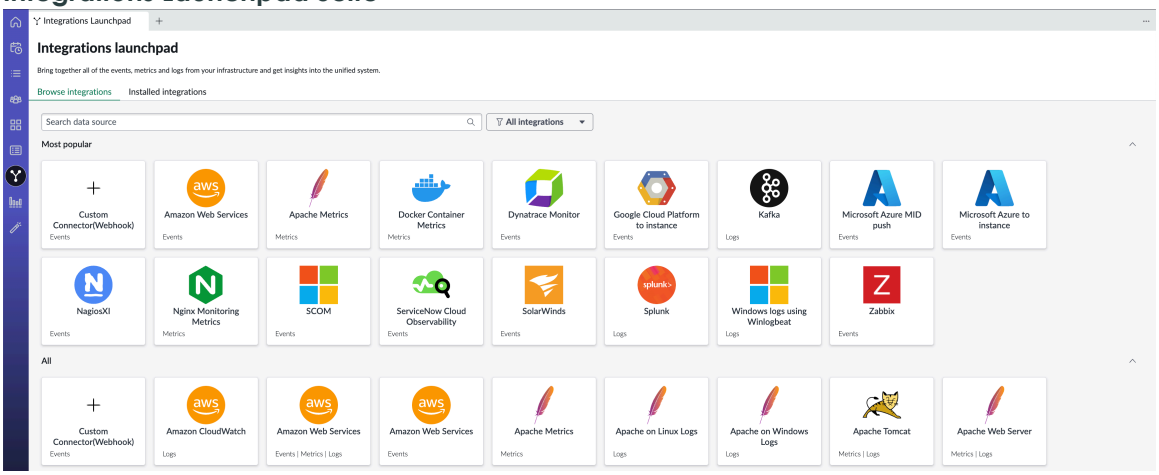


Integrations Launchpad

Integrations Launchpad fasst Ereignisse, Metriken und Protokolle aus Ihrer -Infrastruktur zusammen und bietet Einblicke in ein einheitliches System.

Um auf Informationen zu Integrations Launchpadzuzugreifen, wählen Sie das Symbol Integrations Launchpad ( ).

Integrations Launchpad Seite



Warnungsautomatisierung

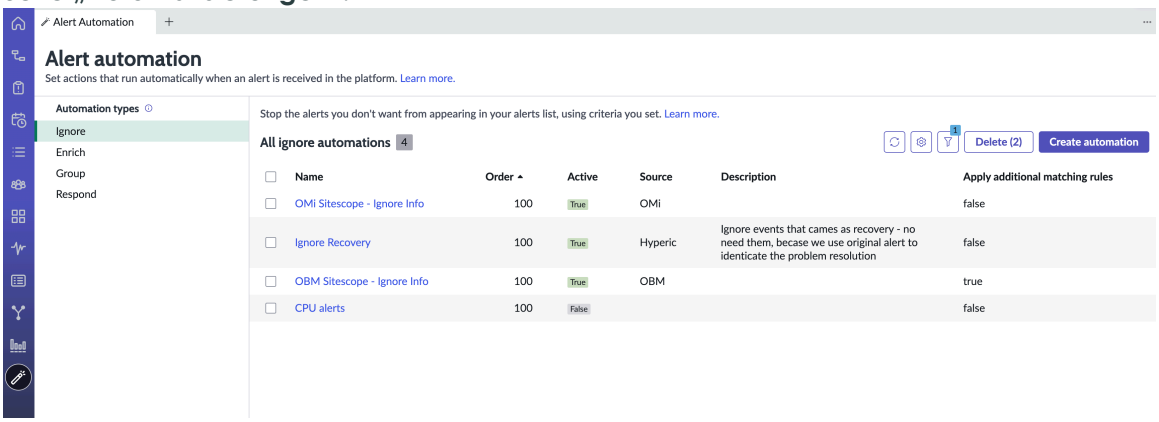
Automatisierungen optimieren Prozesse und ermöglichen eine rechtzeitige Reaktion auf potenzielle Probleme durch Ignorieren, Anreichern, Gruppieren und Reagieren auf Warnungen. Sie reduzieren die Anzahl manueller Eingriffe, senken das Fehlerrisiko und geben IT-Teams mehr Raum für strategische Aufgaben. Dadurch werden die Systemzuverlässigkeit und die Kundenzufriedenheit erhöht.

Um auf Informationen zu Automatisierungen zuzugreifen, wählen Sie das Symbol für Warnungsautomatisierungen ( ).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „Automatisierungen“.

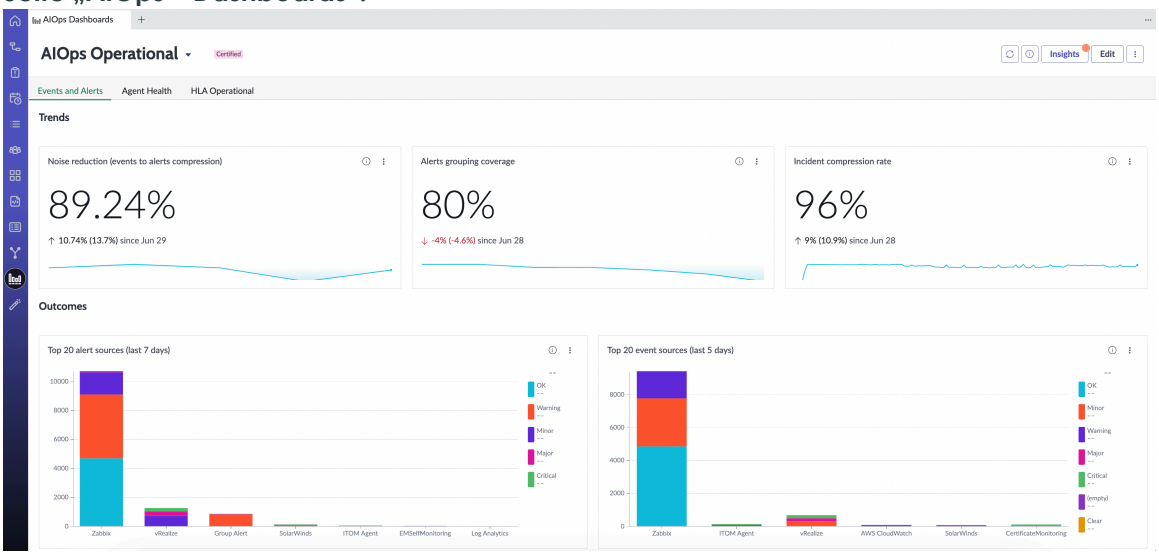


AIOps – Dashboards

Die AIOps-Dashboards bieten umfassende Visualisierungen kritischer Betriebsdaten. Sie können KPIs überwachen, die Serviceintegrität nachverfolgen und wertvolle Kontextinformationen zur IT-Umgebung abrufen, um proaktiv auf Probleme reagieren zu können.

Um auf Informationen in Dashboards zuzugreifen, wählen Sie das AIOps-Dashboard-Symbol ( ).

Seite „AIOps – Dashboards“.



Service Operations-Arbeitsbereich für ITOM konfigurieren

Konfigurieren Sie Service Operations-Arbeitsbereich für ITOM, um IT-Warnungsvolumes effizient zu verwalten und den Arbeitsbereich zur Verbesserung der Servicebereitstellung und der operativen Transparenz anzupassen.

Service Operations-Arbeitsbereich für ITOM ist ein zentralisierter Hub, der zur Optimierung IT Operations Management von den Schwerpunkt auf die Verarbeitung und Lösung von Warnungen legt. Mithilfe dieses Arbeitsbereichs können Administratoren den Prozess der Überwachung, Selektierung und Lösung von Warnungen optimieren und so die Servicebereitstellung und die betriebliche Effizienz verbessern.

Hinweis: Durch die Installation der Anwendung AIOps Experience [sn_sow_aiops] erhalten Sie Service Operations-Arbeitsbereich für ITOM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie Informationen zu Abonnements für ITOM Service Operations-Arbeitsbereicherhalten möchten, überprüfen Sie das Abonnement ITOM-Integrität unter Abonnement für ITOM Health.

Beim Einrichten von Service Operations-Arbeitsbereichist es wichtig, IT Operations Management (ITOM) für die Verwaltung von Warnungen und IT Service Management (ITSM) für die Lösung von Incidents und die Bereitstellung von Services zu konfigurieren. Dieses integrierte Setup gewährleistet den Zugriff auf alle Funktionen und erleichtert die umfassende Verwaltung des IT-Betriebs und der Servicequalität.

Weitere Informationen zu den ITSM -Konfigurationen finden Sie unter Service Operations-Arbeitsbereich für ITSM konfigurieren .

Installieren Sie Service Operations-Arbeitsbereich für die Anwendung ITOM .

Sie können die Anwendung AIOps-Experience [sn_sow_aiops] installieren, um Service Operations-Arbeitsbereich für ITOM abzurufen, wenn Sie die Administratorrolle innehaben.Die Anwendung enthält Demodaten und installiert die zugehörigen ServiceNow® Store-Anwendungen, falls sie nicht bereits installiert sind.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfen Sie die Anwendungsliste der AIOps-Experience in ServiceNow Store auf Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen sowie zur Releasekompatibilität.
- Service Operations Workspace bietet Unterstützung für Domänentrennung. Details finden Sie unter Domain Separation und Ereignismanagement.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit dem Plugin „AIOps Experience“ [sn_sow_aiops] installiert.

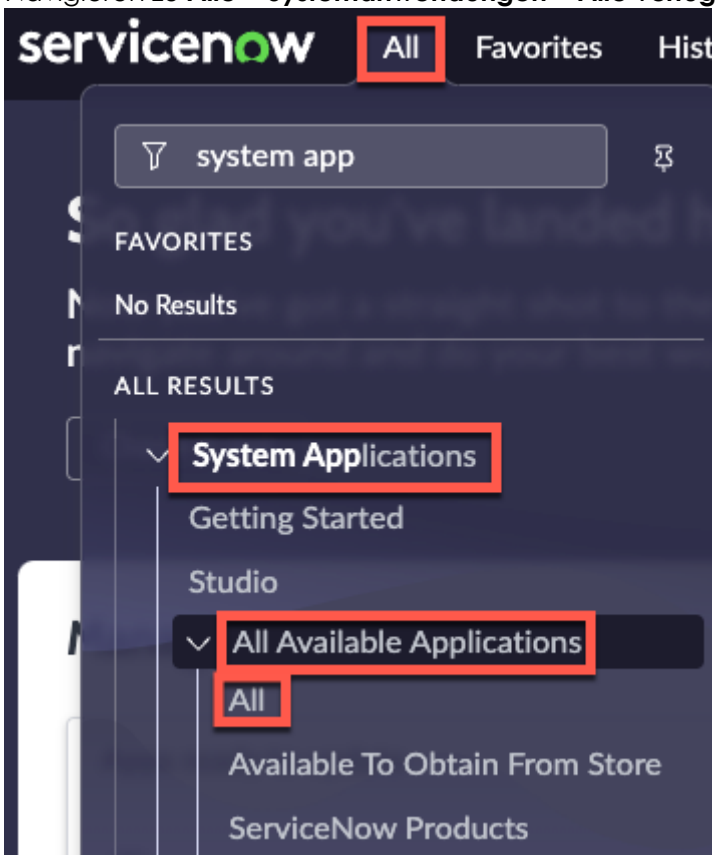
- Rollen
- Plugins

Weitere Informationen finden Sie unter Mit AIOps-Experience installierte Komponenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der AIOps-Experience [sn_sow_aiops].

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wahlweise: Wenn Demodaten verfügbar sind und Sie diese installieren möchten, aktivieren Sie das Kontrollkästchen **Demodaten laden**.
   Demodaten sind Beispieldatensätze, die Anwendungsfunktionen für die gängigen Anwendungsfälle veranschaulichen. Laden Sie die Demodaten, wenn Sie die Anwendung zum ersten Mal auf einer Entwicklungs- oder Testinstanz installieren.

   Wichtig: Wenn Sie die Demodaten nicht während der Installation laden, stehen sie nicht zum späteren Laden zur Verfügung.

6. Wählen Sie **Installieren** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Passen Sie die Homepage Service Operations-Arbeitsbereich für ITOM an

Sie können die auf den Unterseiten der im Basissystem verfügbaren Homepage angezeigten Daten anpassen. Für alle visuellen Stiländerungen müssen Sie eine Kopie dieser Zielseite erstellen und sie bearbeiten.

Begrüßungstext auf der Zielseite ändern

Passen Sie die Header-Nachricht an, die Teil des Begrüßungstextes auf der Homepage ist. Dies führt zu einer personalisierteren Anwender-Experience, vermittelt den Besuchern das Gefühl, willkommen und wertgeschätzt zu werden, und kann auch dazu beitragen, den richtigen Ton und Kontext für die präsentierten Informationen zu finden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin oder admin

Warum und wann dieser Vorgang ausgeführt wird

Das Daten-Broker-Serverskript „Service Desk-Mitarbeiterschicht abrufen“ ruft die `SOWServiceDeskAgentShift`-Skripteinbindungen auf, um die Schichtinformationen im Begrüßungstext anzuzeigen.

Während der Anzeigetext für die Standardzielseite angepasst werden kann, können Sie visuelle Stiländerungen am Text nur vornehmen, wenn Sie eine Kopie der Zielseite erstellen.

Angenommen, Sie haben bis Montag, den 21. März Rufbereitschaft. Sie können Ihre Begrüßungen entsprechend Ihrem Rufbereitschaftsstatus aktualisieren.

Header

Prozedur

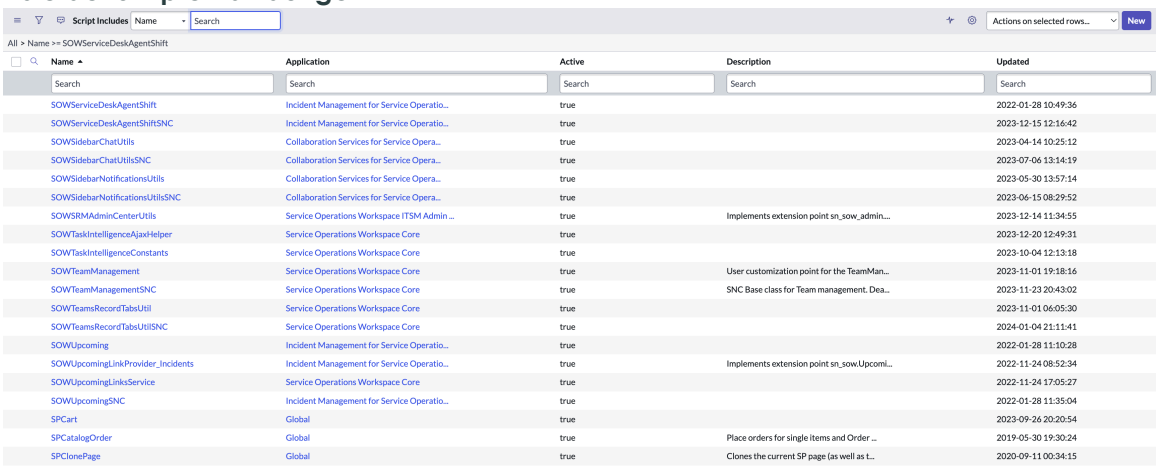
1. Navigieren zu **Alle** > **Service Operations-Arbeitsbereich Admin Center** > **Übersicht**.
2. Wählen Sie auf der Registerkarte **Übersicht** im Abschnitt **Ersteinrichtung** die Option **Zielseite konfigurieren**.
3. Wählen Sie im Formular „Zielseite“ neben **Begrüßungen** die Option **Konfigurieren**.
   Das Formular „Skripteinbindungen“ wird für SOWServiceDeskAgentShift angezeigt, das intern SOWServiceDeskAgentShiftSNC aufruft.
4. Kopieren Sie den Wert des Felds **Skript** von SOWServiceDeskAgentShiftSNC.

   a. Navigieren zu **Alle** > **Systemdefinition** > **Skripteinbindungen**.

   b. Öffnen Sie in der Liste der Skripteinbindungen den Eintrag „SOWServiceDeskAgentShiftSNC“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

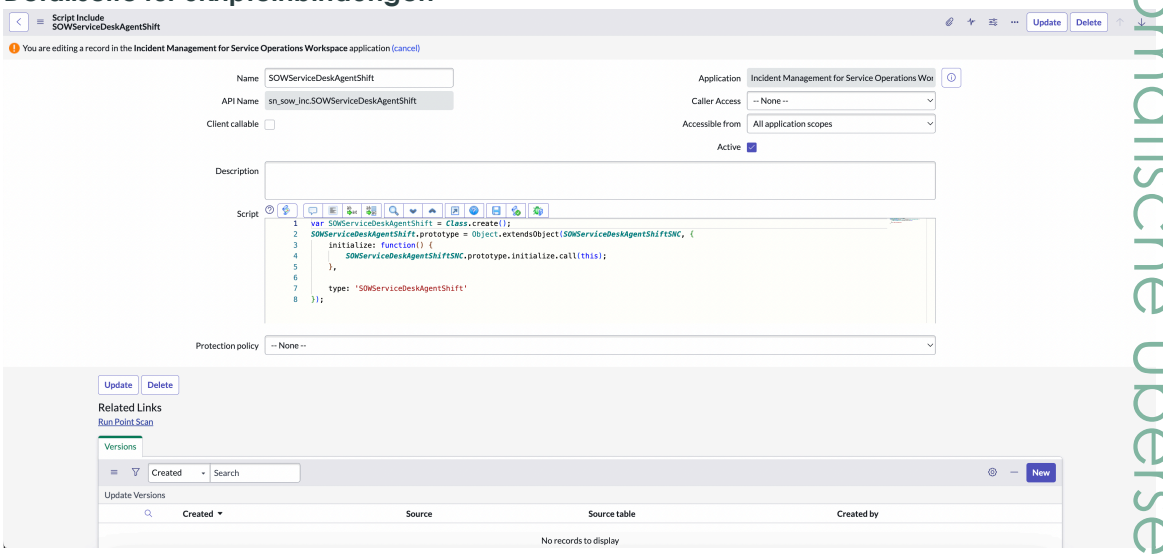
Liste der Skripteinbindungen



Name	Application	Active	Description	Updated
SOWServiceDeskAgentShift	Incident Management for Service Operatio...	true		2022-01-28 10:49:36
SOWServiceDeskAgentShiftSNC	Incident Management for Service Operatio...	true		2023-12-15 12:16:42
SOWSidebarChatUtils	Collaboration Services for Service Opera...	true		2023-04-14 10:25:12
SOWSidebarChatUtilsSNC	Collaboration Services for Service Opera...	true		2023-07-06 13:14:19
SOWSidebarNotificationsUtils	Collaboration Services for Service Opera...	true		2023-05-30 13:57:14
SOWSidebarNotificationsUtilsSNC	Collaboration Services for Service Opera...	true		2023-06-15 08:29:52
SOWSRMAdminCenterUtils	Service Operations Workspace ITSM Admin ...	true	Implements extension point sn_sow_admin....	2023-12-14 11:34:55
SOWTaskIntelligenceAjaxHelper	Service Operations Workspace Core	true		2023-12-20 12:49:31
SOWTaskIntelligenceConstants	Service Operations Workspace Core	true		2023-10-04 12:13:18
SOWTeamManagement	Service Operations Workspace Core	true	User customization point for the TeamMan...	2023-11-01 19:18:16
SOWTeamManagementSNC	Service Operations Workspace Core	true	SNC Base class for Team management. Dea...	2023-11-23 20:43:02
SOWTeamsRecordTabsUtil	Service Operations Workspace Core	true		2023-11-01 06:05:30
SOWTeamsRecordTabsUtilSNC	Service Operations Workspace Core	true		2024-01-04 21:11:41
SOWUpcoming	Incident Management for Service Operatio...	true		2022-01-28 11:10:28
SOWUpcomingLinkProvider_Incidents	Incident Management for Service Operatio...	true	Implements extension point sn_sow.Upcomi...	2022-11-24 08:52:34
SOWUpcomingLinksService	Service Operations Workspace Core	true		2022-11-24 17:05:27
SOWUpcomingSNC	Incident Management for Service Operatio...	true		2022-01-28 11:35:04
SPCart	Global	true		2023-09-26 20:20:54
SPCatalogOrder	Global	true	Place orders for single items and Order ...	2019-05-30 19:30:24
SPClonePage	Global	true	Clones the current SP page (as well as t...	2020-09-11 00:34:15

c. Kopieren Sie den Wert des Felds **Skript**.

Detailseite für Skripteinbindungen



5. Bearbeiten Sie das Skript SOWServiceDeskAgentShift.

a. Navigieren zu **Alle** > **Systemdefinition** > **Skripteinbindungen**.

b. Öffnen Sie in der Liste der Skripteinbindungen den Eintrag „SOWServiceDeskAgentShift“.

c. Fügen Sie den Wert des Felds **Skript** ein, den Sie aus SOWServiceDeskAgentShiftSNC kopiert haben.

```
initialize: function() {

    this.PLUGINS = {

      ON_CALL: "com.snc.on_call_rotation",

      SHIFT_PLANNING: "com.sn_shift_planning"

    };
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    this.DAYS_AHEAD =
gs.getProperty('com.snc.on_call_rotation.upcoming_rota_days', 30);

    this.DATE_FORMAT = gs.getDateFormat();

    this.TIME_FORMAT = gs.getTimeFormat();

    this.WFO_SCHEMA_IDENTIFIER = 'readInTimezone';

    this.WFO_ONCALL_TYPE_IDENTIFIER = 'oncallAPIReadInTimezone';

    this.WEEK_DAY_FORMAT = 'EEEE';

    this.FORMAT = {

      SERVICE_DESK_HEADER: 'SERVICE_DESK_HEADER'

    };

    this.DATE_TIME_FORMAT_FULL = "full";

  },



  getUpcomingShift: function(userId, outputFormat, wfoShift) {

    var upcomingShifts, gd = new GlideDate();

    var from = gd.getDisplayValueInternal();

    gd.addDaysLocalTime(this.DAYS_AHEAD);

    var to = gd.getDisplayValueInternal();

    var mayBeWFOUser = userId == gs.getUserID() ?
gs.hasRole("sn_shift_planning.agent") : true;

    if (GlidePluginManager.isActive(this.PLUGINS.SHIFT_PLANNING) &&
mayBeWFOUser && wfoShift)

      upcomingShifts = this.getWFOShifts(from, to, userId);

    var isWFOResponseValid = Array.isArray(upcomingShifts) &&
upcomingShifts.length > 0;

    if (!isWFOResponseValid &&
GlidePluginManager.isActive(this.PLUGINS.ON_CALL))

      upcomingShifts = this.getOnCallShifts(from, to, userId);

    return this.getFormattedShift(upcomingShifts, outputFormat);

  },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 getWFOShifts: function(from, to, userId) {
   var smUtil = new sn_shift_planning.ScheduleManagerUtil();
   var defaultEventCategories = [
     smUtil.WORK_CATEGORY_SYS_ID,
     smUtil.ON_CALL_CATEGORY_SYS_ID
   ];
   var params = {
     "assignmentGroups": "",
     "individualAgents": userId,
     "startDate": from,
     "endDate": to,
     "published": true,
     "eventCategories": defaultEventCategories,
     "filter": {
       "sn_shift_planning_agent_schedule": {
         "event": ["8d03fd9b0f310010717cc562ff767e4a",
"936319993bd02010e81a4ee1f3efc419"]
       }
     }
   };
   var upcomingShifts = [];
   try {
     var agentScheduleRESTAPIUtils = new
sn_shift_planning.AgentScheduleRESTAPIUtils();
     var spans =
agentScheduleRESTAPIUtils.retrieveAgentSchedulesFromParams(params);
     if (spans && spans.shiftData && spans.shiftData.user &&
spans.shiftData.user.data && spans.shiftData.user.data.length > 0 &&
spans.shiftData.user.data[0].schedules) {
       var schedules = spans.shiftData.user.data[0].schedules,
         arrayUtil = new global.ArrayUtil();
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        for (var schedule in schedules)

          upcomingShifts = arrayUtil.union(upcomingShifts,
 schedules[schedule]);

      }

    } catch (e) {

      gs.error("SOWServiceDeskAgentShiftSNC: Error fetching WFO
 shifts");

    }



    return upcomingShifts;

  },



  getOnCallShifts: function(from, to, userId) {

    var onCallCommon = new global.OnCallCommon();

    var onCallGroups = onCallCommon.getMyGroups();

    var spans = new global.OCRotationV2(null,
 global.OCRotationV2.DEFAULT_FORMAT_OPTION).setStartDate(from).setEndD
ate(to).setUserIds(userId).setGroupIds(onCallGroups).getSpans();

    var upcomingShifts = [];

    for (var i = 0; i < spans.length; i++)

      if ((spans[i].type == "roster" || spans[i].type == "override")
 && spans[i].user_id == userId)

        upcomingShifts.push(spans[i]);

    return upcomingShifts;

  },



  getFormattedShift: function(upcomingShifts, outputFormat) {

    if (gs.nil(upcomingShifts))

      return;

    switch (outputFormat) {

      case this.FORMAT.SERVICE_DESK_HEADER:
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        return this.getServiceDeskFormattedShift(upcomingShifts);
      default:
        return upcomingShifts;
    }
  },

 getServiceDeskFormattedShift: function(upcomingShifts) {
    var response = {
      shiftText: "",
      nearestShift: {}
    };
    var startAttr = "start",
      endAttr = "end",
      isOnCall = true;
    var dateFormat = 'EEEE, MMM dd',
      timeFormat = 'hh:mm a';
    var isWFOSchema = Array.isArray(upcomingShifts) &&
upcomingShifts.length > 0 && this.WFO_SCHEMA_IDENTIFIER in
upcomingShifts[0];
    if (isWFOSchema)
      startAttr = "scheduledStartTime", endAttr = "scheduledEndTime";
    response.nearestShift = this.getNearestShift(upcomingShifts,
startAttr, endAttr);
    if (response.nearestShift) {
      if (isWFOSchema) {
        if (response.nearestShift.schedule
&& !(this.WFO_ONCALL_TYPE_IDENTIFIER in
response.nearestShift.schedule))
          isOnCall = false;
      }
      if (isOnCall) {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        if (response.nearestShift.isCurrent) {

          if (response.nearestShift.roster_name)

            response.shiftText = gs.getMessage("You are on-call until
{0} as {1}",
[this.getFormattedDateTime(response.nearestShift[endAttr]),
response.nearestShift.roster_name]);

          else

            response.shiftText = gs.getMessage("You are on-call until
{0}", [this.getFormattedDateTime(response.nearestShift[endAttr])]);

        } else {

          if (response.nearestShift.roster_name)

            response.shiftText = gs.getMessage("Your
next on-call shift starts on {0} as {1}",
[this.getFormattedDateTime(response.nearestShift[startAttr]),
response.nearestShift.roster_name]);

          else

            response.shiftText = gs.getMessage("Your next on-call
shift starts on {0}",
[this.getFormattedDateTime(response.nearestShift[startAttr])]);

        }

      } else {

        if (response.nearestShift.isCurrent) {

          response.shiftText = gs.getMessage("Your shift ends on {0}",
[this.getFormattedDateTime(response.nearestShift[endAttr])]);

        } else

          response.shiftText = gs.getMessage("Your next shift starts
on {0}",
[this.getFormattedDateTime(response.nearestShift[startAttr])]);

      }

    }



    return response;

  },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 getNearestShift: function(upcomingShifts, startAttr, endAttr) {

   if (gs.nil(upcomingShifts) || gs.nil(startAttr) ||
gs.nil(endAttr))

     return;

   var nearestShift;

   upcomingShifts.sort(function(shift_1, shift_2) {

     var gdt1 = new GlideDateTime();

     gdt1.setDisplayValueInternal(shift_1[startAttr]);

     var gdt2 = new GlideDateTime();

     gdt2.setDisplayValueInternal(shift_2[startAttr]);

     return GlideDateTime.subtract(gdt2, gdt1).getNumericValue();

   });

   var currentDateTime = new GlideDateTime(),

     startDateTime = new GlideDateTime(),

     endDateTime = new GlideDateTime();

   for (var i = 0; i < upcomingShifts.length; i++) {


startDateTime.setDisplayValueInternal(upcomingShifts[i][startAttr] +
"");

     endDateTime.setDisplayValueInternal(upcomingShifts[i][endAttr] +
"");

     if (currentDateTime.onOrBefore(endDateTime)) {

       nearestShift = upcomingShifts[i];

       if (currentDateTime.onOrAfter(startDateTime))

         nearestShift.isCurrent = true;

       else

         nearestShift.isCurrent = false;

       break;

     }

   }

   return nearestShift;
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  },

  getFormattedDateSpan: function(date, dateFormat, timeFormat) {
    var formattedDate = this.getFormattedDate(date, dateFormat);
    var dateAmPmTime = this.getFormattedTime(date, timeFormat);
    return formattedDate + " " + dateAmPmTime;
  },

  getFormattedDate: function(inputDate, format) {
    var date = new GlideDateTime();
    date.setDisplayValueInternal(inputDate);
    format = !format ? this.DATE_FORMAT : format;
    var gd = date.getLocalDate();
    return gd.getByFormat(format);
  },

  getFormattedTime: function(inputDate, format) {
    var date = new GlideDateTime();
    date.setDisplayValueInternal(inputDate);
    format = !format ? this.TIME_FORMAT : format;
    var gt = date.getLocalTime();
    return gt.getByFormat(format);
  },

  getFormattedDateTime: function(date) {
    var dateTime = new GlideDateTime();
    dateTime.setDisplayValueInternal(date);
    return dateTime.getDisplayValueLang(this.DATE_TIME_FORMAT_FULL);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  },



 endsToday: function(inputDate) {

   var inputGdt = new GlideDateTime();

   inputGdt.setDisplayValueInternal(inputDate);

   return new GlideDateTime().getLocalDate().getValue() ==
inputGdt.getLocalDate().getValue();

 },



 endingTomorrow: function(inputDate) {

   var inputGdt = new GlideDateTime();

   inputGdt.setDisplayValueInternal(inputDate);

   var tomorrowDateTime = new GlideDateTime();

   tomorrowDateTime.addDaysLocalTime(1);

   return tomorrowDateTime.getLocalDate().getValue() ==
inputGdt.getLocalDate().getValue();

 },
```

d. Bearbeiten Sie den folgenden Teil des Skripts wie erwähnt.

```
     if (isOnCall) {

       if (response.nearestShift.isCurrent) {

         if (response.nearestShift.roster_name)

           response.shiftText = gs.getMessage("You are on-call until
{0} as {1}",
[this.getFormattedDateTime(response.nearestShift[endAttr]),
response.nearestShift.roster_name]);

         else

           response.shiftText = gs.getMessage("You are on-call until
{0}", [this.getFormattedDateTime(response.nearestShift[endAttr])]);

       } else {

         if (response.nearestShift.roster_name)

           response.shiftText = gs.getMessage("Your
next on-call shift starts on {0} as {1}",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
[this.getFormattedDateTime(response.nearestShift[startAttr]),
response.nearestShift.roster_name]);

          else

            response.shiftText = gs.getMessage("Your next on-call
shift starts on {0}",
[this.getFormattedDateTime(response.nearestShift[startAttr])]);

        }

      } else {

        if (response.nearestShift.isCurrent) {

          response.shiftText = gs.getMessage("Your shift ends on {0}",
[this.getFormattedDateTime(response.nearestShift[endAttr])]);

        } else

          response.shiftText = gs.getMessage("Your next shift starts
on {0}",
[this.getFormattedDateTime(response.nearestShift[startAttr])]);

      }
```

6. Wählen Sie **Aktualisieren**.

Ändern Sie die Karten der ersten Ebene im Abschnitt Service Operations-Arbeitsbereich für ITOM Übersicht

Passen Sie die in den Karten der ersten Ebene angezeigten Daten im Abschnitt Übersicht an, indem Sie verschiedene Parameter wie Headerbezeichnung, Datenquelle, Metrik, Feld für Gruppierung und viewAllQuery konfigurieren. Dies ermöglicht eine maßgeschneidertere und relevantere Anzeige von Informationen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren Sie zu **sys_ux_client_script_include.list**.
2. Wählen Sie in der Liste „UX-Client-Skripteinbindungen“ die Definition `SowEMLandingPageUtilsSNC` für Client-Skripteinbindungen aus.
3. Bearbeiten Sie im Formular „UX-Client-Skript-Einbeziehung“ das Feld **Skript**.
   Beispiel:

```
}
  };
 const labelMap = {
     'em_alert': {
         'alerts_assigned_to_you': {
             '1': 'Alerts assigned to you - Urgent',
             '2': 'Alerts assigned to you - High',
             '3': 'Alerts assigned to you - Moderate',
             '4': 'Alerts assigned to you - Low'
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            },
            'open_alerts': {
                '1': 'Open alerts - Urgent',
                '2': 'Open alerts - High',
                '3': 'Open alerts - Moderate',
                '4': 'Open alerts - Low'
            },
            'team_alerts_assigned': 'Assigned team alerts - to ',
            'team_alerts_unassigned': {
                '1': 'Unassigned team alerts - Urgent',
                '2': 'Unassigned team alerts - High',
                '3': 'Unassigned team alerts - Moderate',
                '4': 'Unassigned team alerts - Low'
            }
        }
```

4. Klicken Sie auf **Aktualisieren**.

Erstellen Sie eine Kopie der Zielseite Service Operations-Arbeitsbereich für ITOM .

Nehmen Sie visuelle Stiländerungen an den Unterseiten auf der Homepage vor. Dadurch wird die allgemeine Anwender-Experience verbessert, indem eine einheitliche und visuell ansprechende Anwenderoberfläche bereitgestellt, die Navigation verbessert und sichergestellt wird, dass wichtige Informationen leicht zugänglich und ansprechend sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin oder ui_builder_admin

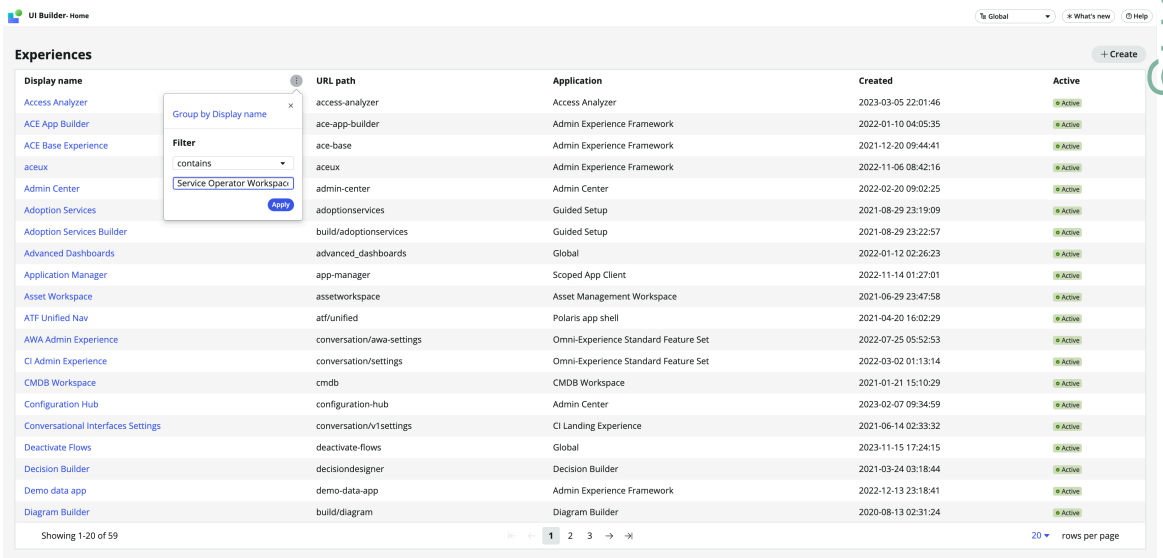
Warum und wann dieser Vorgang ausgeführt wird

Eine Seite ist Inhalt, der sich unter einer bestimmten URL befindet. Wenn ein Anwender die URL öffnet, wird ihm basierend auf der von Ihnen festgelegten Zielgruppe, den Bedingungen und der Reihenfolge eine andere Variante dieser Seite angezeigt.

Prozedur

1. Navigieren zu **Alle** > **Now-Experience-Framework** > **UI Builder**.
2. Filtern und suchen Sie im Feld **Anzeigename** nach **Service Operations-Arbeitsbereich**.

   Die Seite „Experiences“ wird geöffnet.

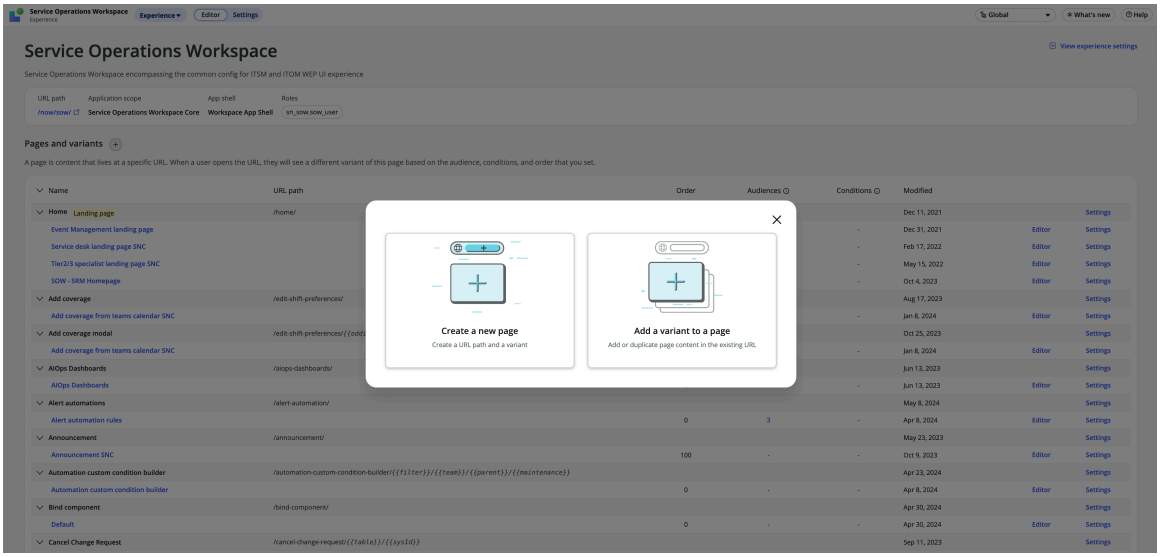


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

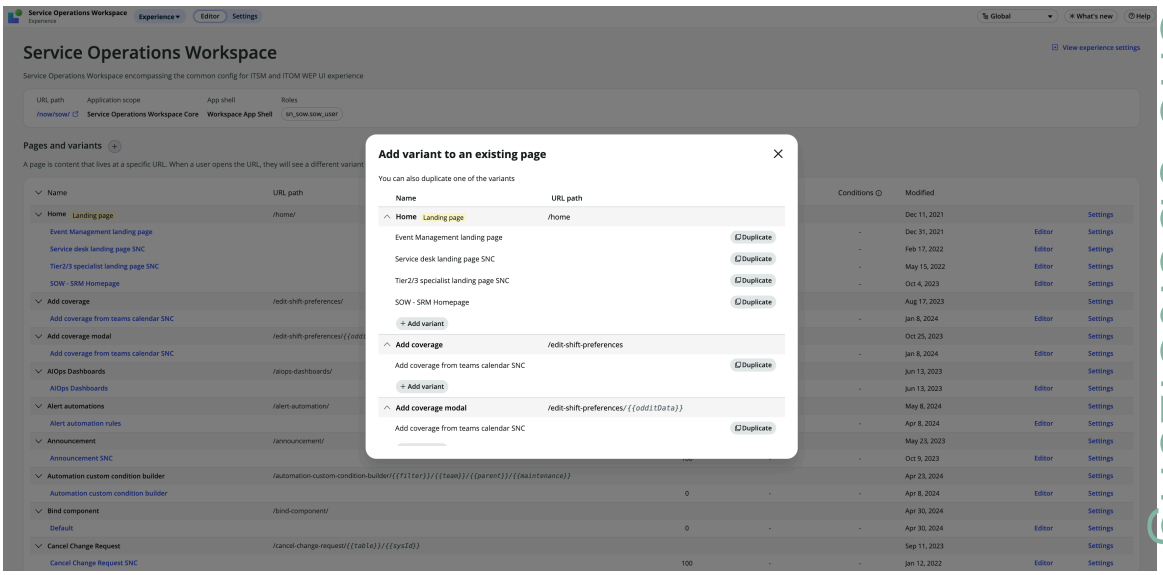
3. Öffnen Sie **den Service Operations-Arbeitsbereich,** indem Sie ihn auswählen.

4. Wählen Sie neben **Seiten und Varianten**das Plus-Symbol (⊕).



5. Wählen Sie **Variante zu Seite hinzufügen**aus.

   Das Fenster Variante zu vorhandener Seite hinzufügen wird geöffnet.



6. Um ein Duplikat des Seiteninhalts im vorhandenen URL-Pfad zu erstellen, wählen Sie **Duplizieren** aus, und befolgen Sie die Schritte.

Öffnen Sie Ihre konfigurierbare Arbeitsbereich-Experience in UI Builder

Greifen Sie zur Bearbeitung auf die Oberfläche Ihres konfigurierbaren Arbeitsbereichs in UI Builder zu.

Vorbereitungen
Erforderliche Rolle: admin, ui_builder_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Navigationsfilter zu **Alle** > **Now-Experience-Framework** > **UI Builder**.
2. Wählen Sie **Experiences**.
3. Wählen Sie Ihre Experience aus.

Ergebnisse

Ihre konfigurierbare Experience wird in UI Builder geöffnet.

Zur Homepage Service Operations-Arbeitsbereich umleiten

Ermöglichen Sie eine schnelle Aufgabenpriorisierung, indem Sie Service Desk-Mitarbeiter unmittelbar nach der Anmeldung bei der Instanz ServiceNow auf die -Homepage leiten. Dies verbessert die Workflow-Effizienz, indem Service Desk-Mitarbeitern sofortiger Zugriff auf wichtige Tools und Informationen gewährt wird, was die rechtzeitige Lösung kritischer Aufgaben und Probleme erleichtert.

Vorbereitungen

Stellen Sie sicher, dass der Wert von *glide.login.home property* auf `/now/nav/ui/home` gesetzt ist. Diese Eigenschaft gibt die Standard-Homepage an, die bei der Anmeldung angezeigt wird.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Wählen Sie **Alle** aus, und suchen Sie nach `sys_properties.list`.
2. Fügen Sie die Eigenschaft *sn_sow.service_desk_groups* hinzu.
3. Geben Sie im Feld **Wert** die sys_id der Benutzergruppe ein, zu der der Operator gehört.

   Hinweis: Wenn Sie mehrere Service Desk-Gruppen angeben möchten, fügen Sie im Wertfeld eine durch Kommas getrennte Liste mit Gruppen-Sys-IDs hinzu.

4. Wählen Sie **Aktualisieren**.

Öffnen Sie Ihre konfigurierbare Arbeitsbereich-Experience in UI Builder

Greifen Sie zur Bearbeitung auf die Oberfläche Ihres konfigurierbaren Arbeitsbereichs in UI Builder zu.

Vorbereitungen

Erforderliche Rolle: admin, ui_builder_admin

Prozedur

1. Navigieren Sie im Navigationsfilter zu **Alle** > **Now-Experience-Framework** > **UI Builder**.
2. Wählen Sie **Experiences**.
3. Wählen Sie Ihre Experience aus.

Ergebnisse

Ihre konfigurierbare Experience wird in UI Builder geöffnet.

Service Operations-Arbeitsbereich

Service Operations-Arbeitsbereich überwacht Services in Ihrer Ereignismanagement -Umgebung, sodass Sie deren Status überprüfen und diejenigen identifizieren können,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bei denen das Risiko einer suboptimalen Leistung besteht. Dadurch können Sie Probleme umgehend beheben.

Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Sie können den Service Operations-Arbeitsbereich so konfigurieren, dass er bis zu 24 Stunden angemeldet bleibt. Weitere Informationen finden Sie unter Benutzersitzungen verwalten .

Zeigen Sie Informationen zur Integrität des Anwendungsservice in an Service Operations-Arbeitsbereich

Überwachen Sie die Integrität von Services, und filtern Sie die Informationen, die Sie anzeigen möchten, damit Sie sich auf die relevantesten Daten konzentrieren und schnell fundierte Entscheidungen treffen können.

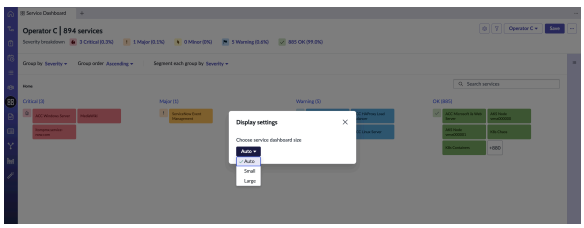
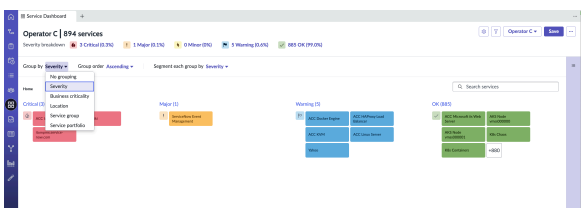
Vorbereitungen

Erforderliche Rolle: evt_mgmt_user oder evt_mgmt_admin

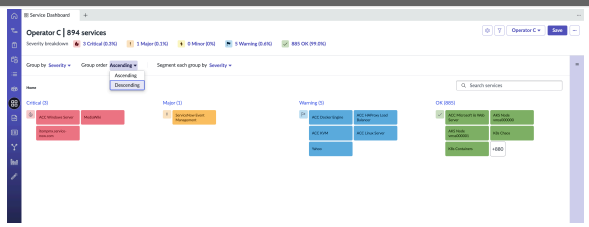
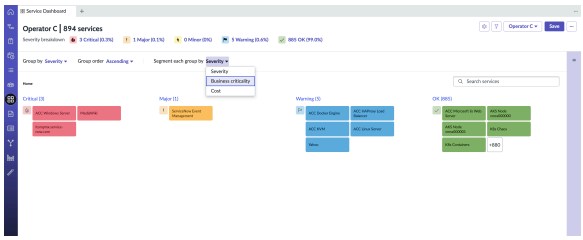
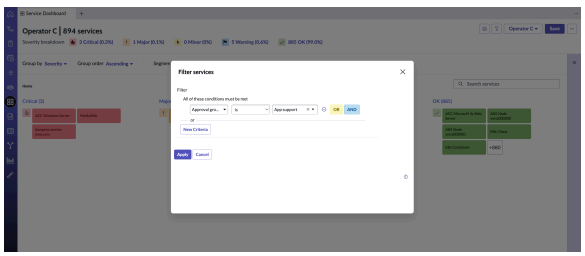
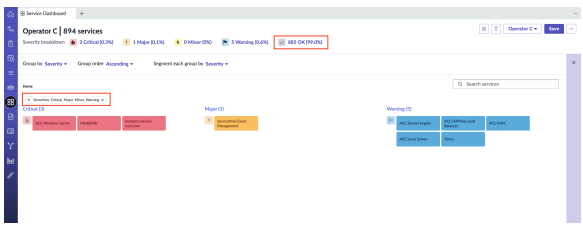
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Service-Dashboard-Symbol ( ). Die Seite „Service-Dashboard“ wird angezeigt.
3. Führen Sie nach Bedarf die folgenden Aktionen aus.

Funktionen und Aktionen

Funktionen	Aktionen
Vergrößern oder verkleinern Sie die Kacheln.	**a.** Wählen Sie das Symbol für die Anzeigeeinstellungen ( ) aus. **b.** Wählen Sie im Popup-Fenster **Anzeigeeinstellungen** die Größe aus. 
Gruppieren Sie Services nach ausgewählten Kriterien	Wählen Sie den Pfeil neben **Gruppieren nach,** und wählen Sie dann die Kriterien aus, nach denen Sie Services gruppieren möchten. 
Gruppenreihenfolge	Wählen Sie den Pfeil neben **Gruppenreihenfolge** und dann die Kriterien aus, nach denen Sie Services gruppieren möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionen	Aktionen
	
Jede Gruppe segmentieren nach	Segmentieren Sie jede Gruppe nach Schweregrad, Geschäftskritikalität und Kosten, um sie zu kategorisieren und basierend auf diesen Attributen in verschiedene Gruppen zu organisieren. 
Filtern Sie Informationen	Filtern Sie die im Dashboard angezeigten Informationen, um sicherzustellen, dass Sie sich auf relevante Daten für eine effektive Überwachung konzentrieren. ◦ Um einen globalen Filter festzulegen, wählen Sie das Filtersymbol ( ), legen Sie die globale Filterbedingung fest, fügen Sie Filterbedingungen hinzu, und wählen Sie **Anwenden**aus.  ◦ Um einen Schweregrad aus der Anzeige auszuschließen, wählen Sie ihn im Menüband **„Schweregradaufgliederung“**. Herausgefilterte Schweregrade werden abgeblendet angezeigt. Um einen abgeblendeten Schweregrad in der Anzeige wiederherzustellen, wählen Sie ihn einfach erneut aus. 

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Benutzeransicht in Service Operations-Arbeitsbereich

Erstellen Sie eine Anwenderansicht in Service Operations-Arbeitsbereich, und passen Sie sie an, um das Anzeigen von Informationen im gewünschten Format zu ermöglichen.

Vorbereitungen

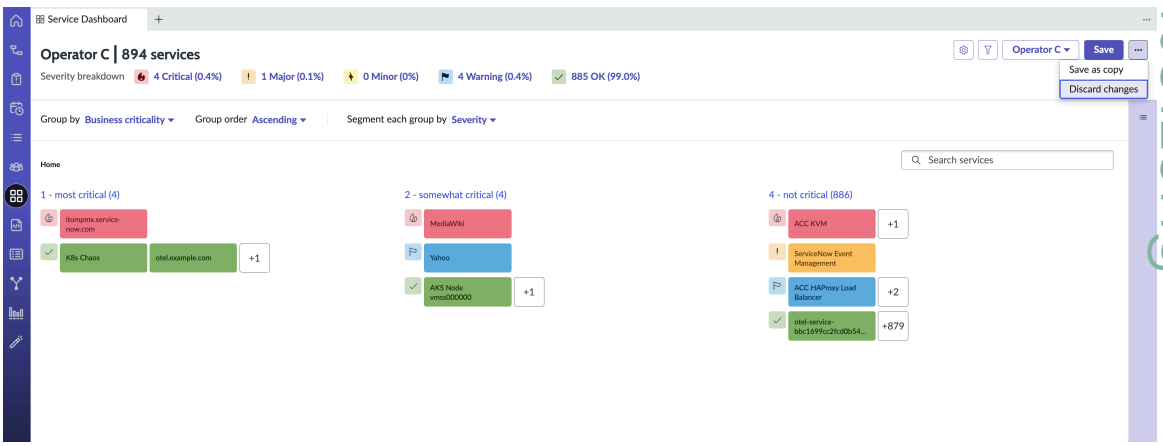
Hinweis: Die Schnittstelle Betreiber-Arbeitsbereich ist nur für Kunden verfügbar, die ein Upgrade von einem Release vor Release Utah durchgeführt haben. Neue Kunden ab dem Release Utah können Service Operations-Arbeitsbereich für ITOMverwenden, das eine erweiterte Anwenderoberfläche für die Verwaltung von Warnungen bietet.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Service-Dashboard-Symbol ( ).
   Die Seite „Service-Dashboard“ wird angezeigt.
3. So können Sie das Aussehen des Dashboards anpassen: Wählen Sie Ausgabekriterien aus den Filtern **Gruppieren nach**, **Gruppenreihenfolge** bzw. **Jede Gruppe segmentieren nach**, oder wählen Sie die relevante **Schweregradaufgliederung** aus.
   Auswählen von **Servicegruppe** > **Alle** im Filter **Gruppieren nach** zeigt alle Servicegruppen an.
4. Konfigurieren Sie die Informationen, die für die Ansicht angezeigt werden sollen, indem Sie auf das Symbol für Filter-Services ( ) klicken und einen globalen Filter festlegen. Beispielsweise können Sie einen Filter so konfigurieren, dass nur die Services angezeigt werden, die einem bestimmten Benutzer zugewiesen sind.

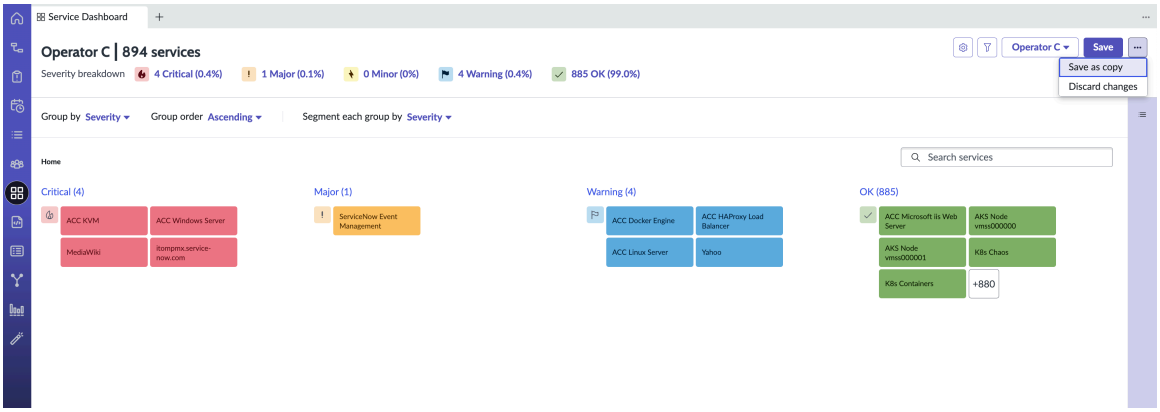
   Hinweis: Um Ihre Änderungen zu verwerfen und den zuletzt gespeicherten Status der Ansicht wiederherzustellen, wählen Sie das Symbol „Weitere Aktionen“ ( ), und wählen Sie **Änderungen verwerfen**.



5. Speichern Sie Ihre neue Ansicht, indem Sie auf das Symbol „Weitere Aktionen“ ( ) neben der Schaltfläche **Speichern** klicken und **Als Kopie speichern**auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



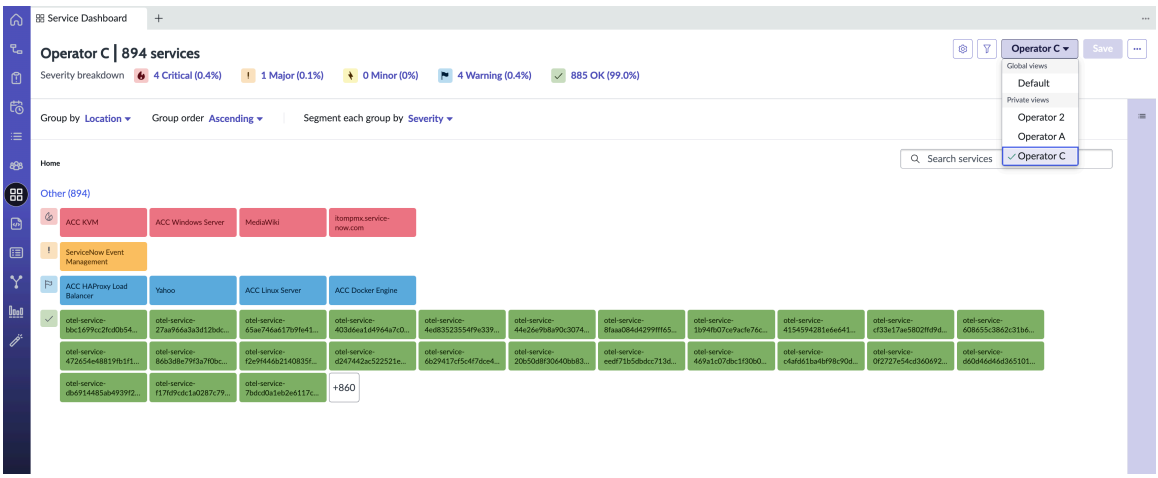
6. Im Dialogfeld „Als Kopie speichern“ geben Sie den Namen Ihrer Ansicht in das Feld **Ansichtsname** ein.

   Die Ansicht wird als **private Ansicht** gespeichert (nur für den angemeldeten Benutzer sichtbar) und kann verwendet werden.

   Ansichten werden in die folgenden Kategorien gruppiert:

   - **Globale Ansichten**: Für alle Benutzer sichtbar. Nur ein Ereignismanagement Administrator kann globale Ansichten erstellen.
   - **Private Ansichten**: Nur für den angemeldeten Benutzer sichtbar.

   Hinweis: Sie können zwischen verschiedenen Ansichten wechseln, indem Sie eine Ansicht aus der Liste neben der Schaltfläche **Speichern** auswählen.



Löschen Sie eine Benutzeransicht in Service Operations-Arbeitsbereich

Löschen Sie eine Service Operations-Arbeitsbereich -Benutzeransicht, die Sie nicht mehr benötigen. Sie führen diese Aktion über das Menü Ereignismanagement außerhalb von Service Operations-Arbeitsbereich aus.

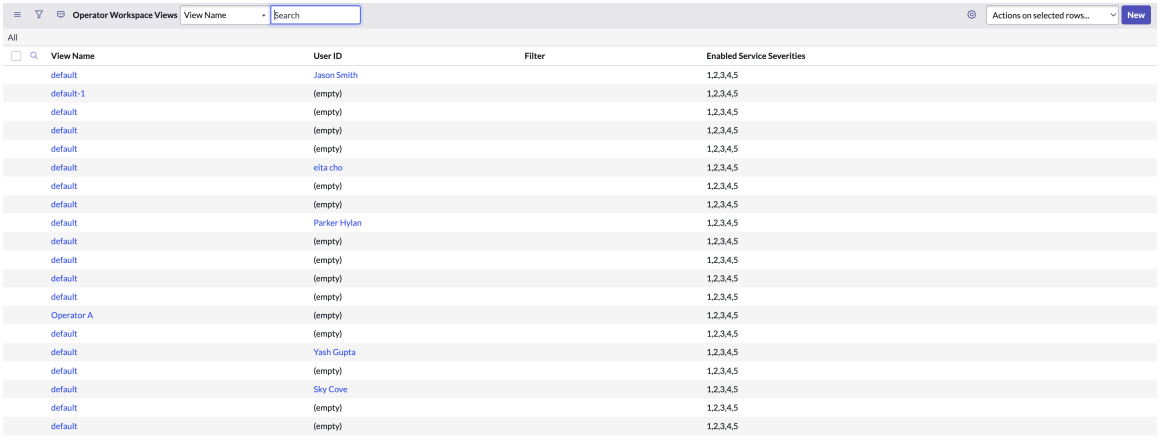
Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

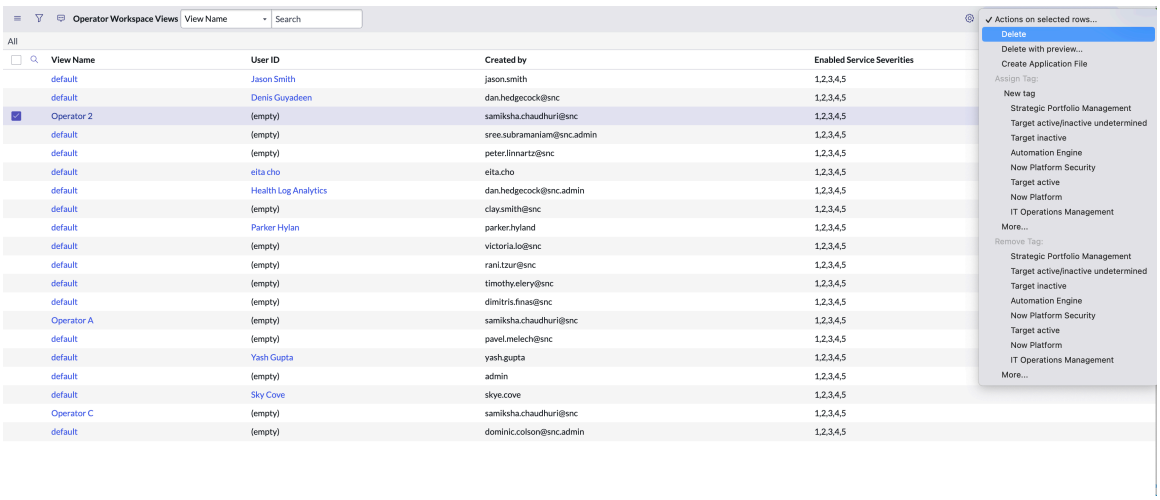
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Suchen Sie in Ihrer Instanz Ereignismanagement im Navigationsbereich nach *noc_user_view.list*.
   Die Seite Operator-Arbeitsbereichansichten wird geöffnet.



2. Aktivieren Sie das Kontrollkästchen neben der Ansicht, die Sie löschen möchten.
3. Wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option **Löschen aus**.



Automatische Übersetzung

Zeigen Sie Details zu Anwendungsservices in an Service Operations-Arbeitsbereich

Zeigen Sie umfassende Informationen zu einem Anwendungsservice an, einschließlich Name, Geschäftsrelevanz, Eigentum, Prozess- und Betriebsstatus, Details zur Traffic-basierten Discovery, Discovery-Status und relevante Kommentare. Dies ermöglicht eine gründliche Analyse des aktuellen Status und der Nutzung von Anwendungsservices, sorgt für Klarheit in Bezug auf Besitz und Relevanz und erleichtert die effektive Priorisierung von Ressourcen und Aktionen.

Vorbereitungen

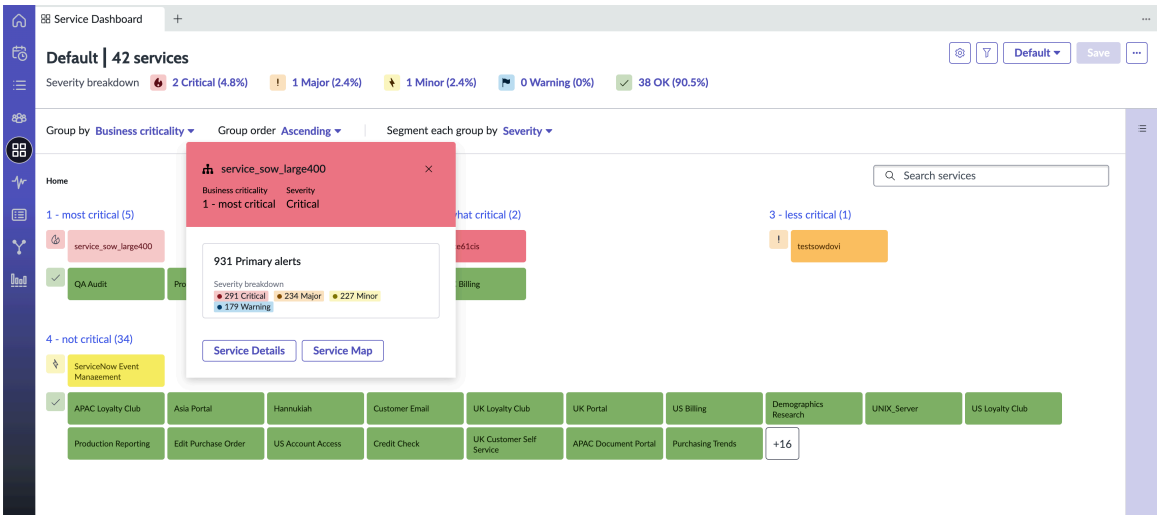
Erforderliche Rolle: evt_mgmt_user, evt_mgmt_operator oder evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

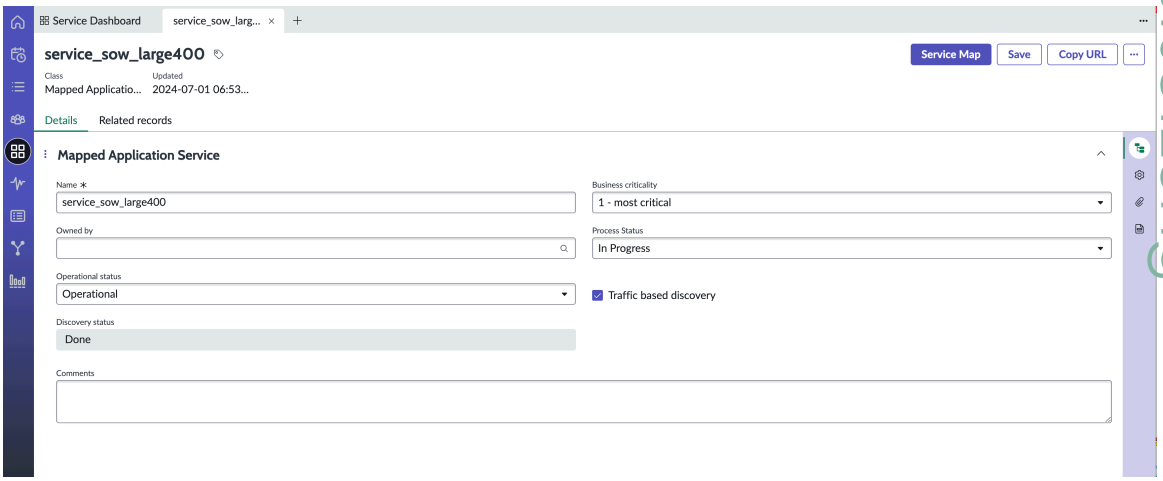
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Service-Dashboard-Symbol ( ).
   Die Seite „Service-Dashboard“ wird angezeigt.
3. Wählen Sie eine Servicekachel aus.
   In einem Popup-Fenster werden die Geschäftskritikalität und der Schweregrad eines Service angezeigt.



4. Wählen Sie **Servicedetails** aus.
   Standardmäßig ist die Registerkarte **Details** ausgewählt.

   Die Detailseite enthält umfassende Informationen zu einem Anwendungsservice.



   Weitere Informationen zu diesen Feldern finden Sie unter Detailseite des Anwendungsservice.

Primäre Warnungen anzeigen, die einem Service zugeordnet sind

Zeigen Sie die einem Service zugeordneten primären Warnungen an, um Probleme mit dem Service zu beheben.

Automatische Übersetzung

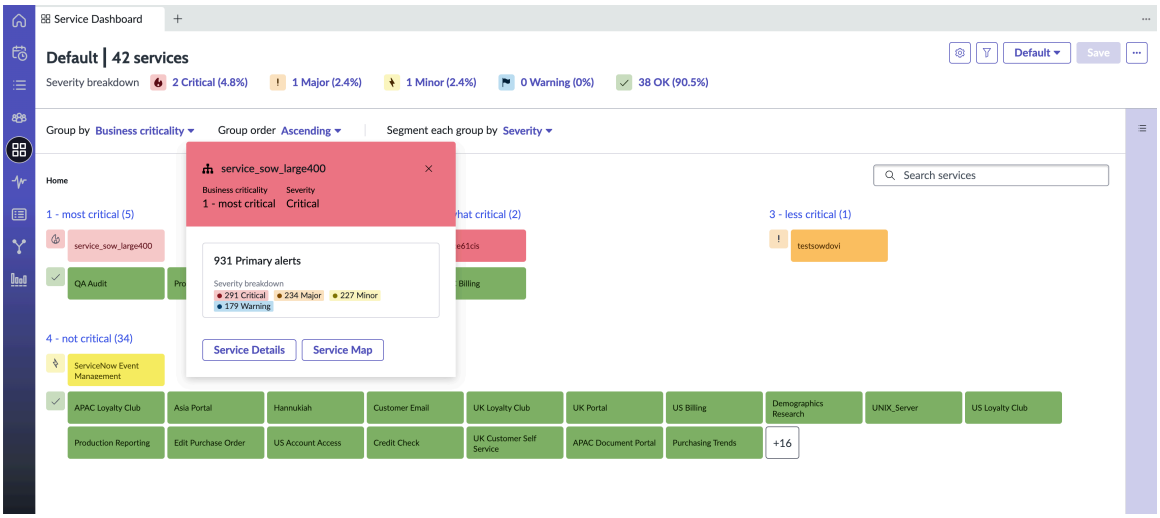
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

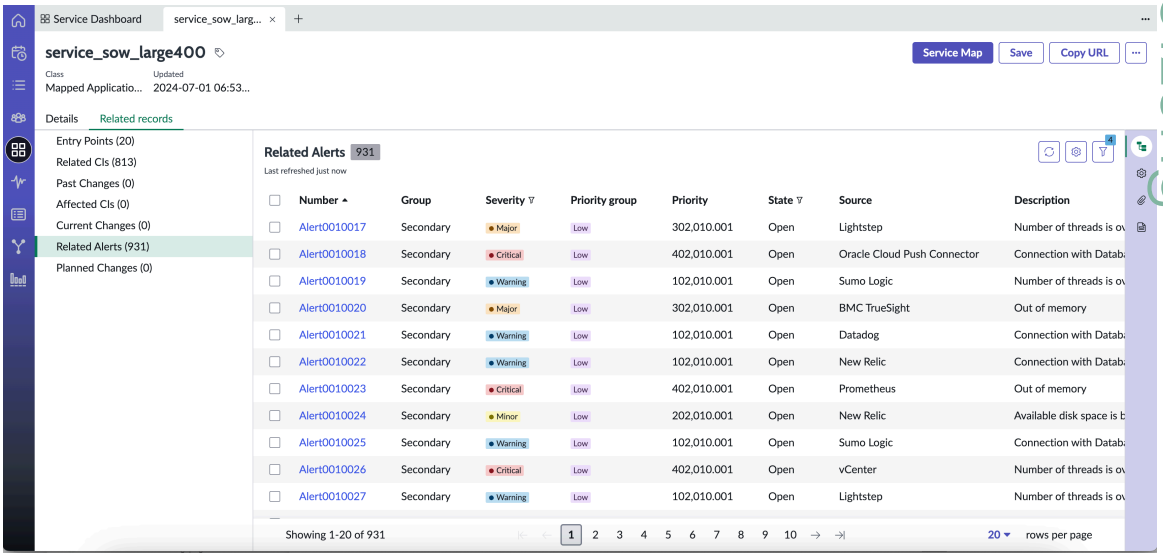
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Service-Dashboard-Symbol ( ).
   Die Seite „Service-Dashboard“ wird angezeigt.
3. Wählen Sie eine Servicekachel aus.
   In einem Popup-Fenster werden die Geschäftskritikalität und der Schweregrad eines Service angezeigt.



4. Wählen Sie **Servicedetails** aus.
   Standardmäßig ist die Registerkarte **Details** ausgewählt.
5. Wählen Sie die Registerkarte **Zugehörige Datensätze** aus.
6. Wählen Sie im linken Bereich **Zugehörige Warnungen**aus.



Zeigen Sie Details zu einer Warnung an, indem Sie die entsprechende Nummer in der Spalte **Nummer** auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Liste in Service Operations-Arbeitsbereich für ITOMerstellen

Passen Sie Listen in Service Operations-Arbeitsbereich an, indem Sie neue Listen erstellen, ihre Reihenfolge ändern, ihren Inhalt ändern oder Listen nach Bedarf löschen. Diese Flexibilität ermöglicht es Anwendern, Informationen entsprechend ihren spezifischen Anforderungen zu organisieren. Dies ermöglicht eine einfachere Navigation, einen schnelleren Zugriff auf relevante Daten und ein optimiertes Workflow-Management.

Vorbereitungen

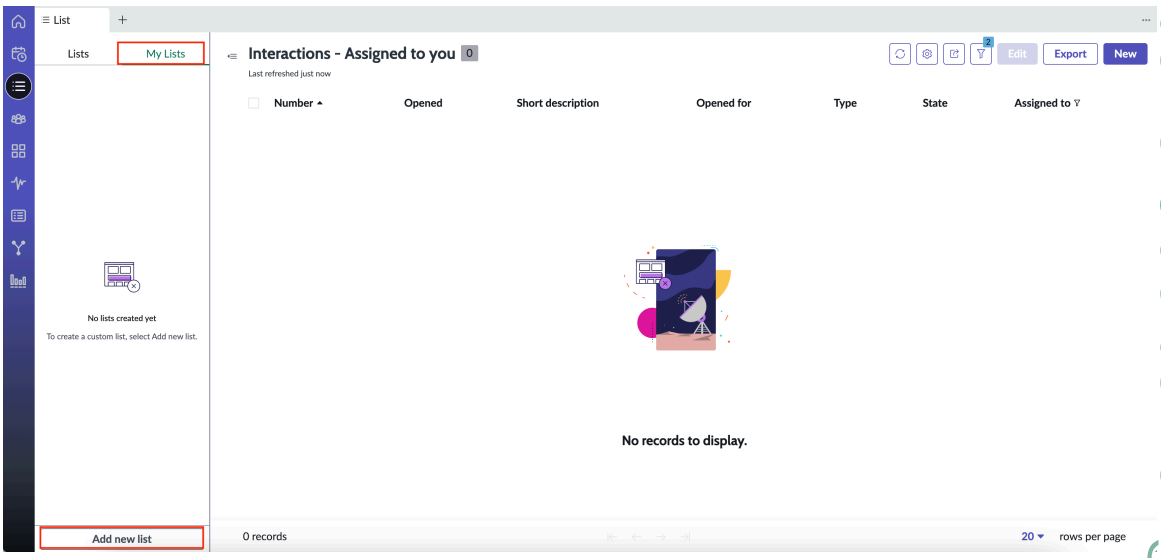
Erforderliche Rolle: itil

Warum und wann dieser Vorgang ausgeführt wird

Erstellen Sie anwenderdefinierte Gruppierungen von Datensätzen, die auf der **Registerkarte** Listen aufgeführt sind, z. B. Incidents, die an ein bestimmtes Unternehmen gebunden sind. Passen Sie vorhandene Listen an, oder erstellen Sie neue, die ausschließlich unter der Registerkarte **„Meine Listen“** für die personalisierte Organisation sichtbar sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol ( ).
3. Wählen Sie die Registerkarte **Meine Listen** aus.
4. Wählen Sie **Neue Liste hinzufügen**.



5. Erstellen Sie eine Liste, indem Sie sie entweder auf eine vorhandene Liste stützen oder eine neue erstellen.
   - Um die Liste auf Grundlage einer vorhandenen Liste anzulegen, wählen Sie **Mit vorhandener beginnen** aus.
   - Um eine neue Liste zu erstellen, wählen Sie **Selbst erstellen** aus.
6. Füllen Sie die Felder des Formulars aus.
   Weitere Informationen zu den Feldern finden Sie unter Erstellen Sie Listenfelder.
7. Wählen Sie **Erstellen** aus.
   Die Liste wird auf der Registerkarte **Meine Listen** angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

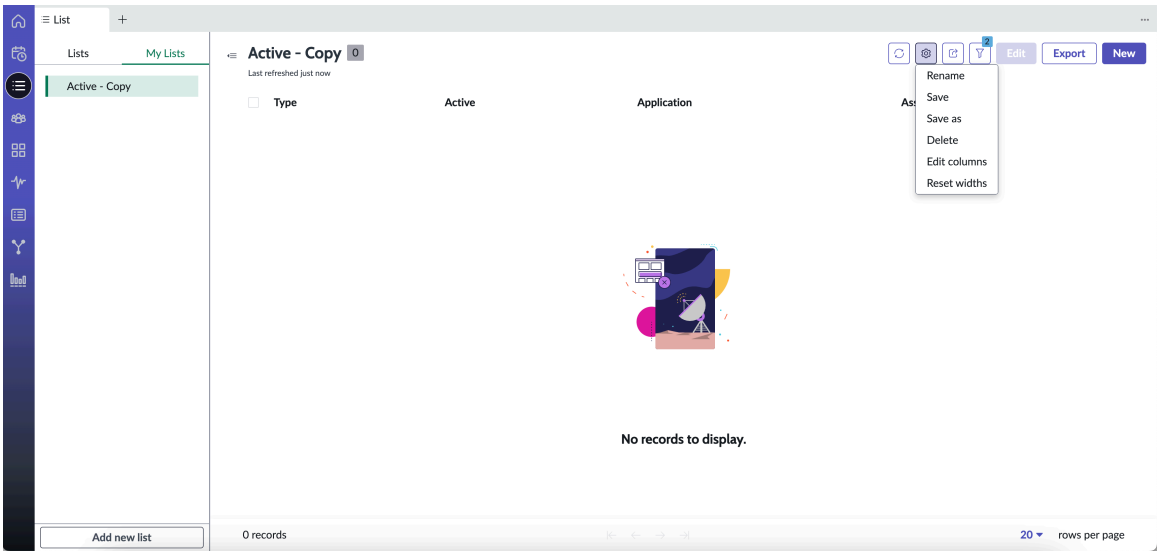
Benennen Sie eine Liste in Service Operations-Arbeitsbereich in ITOMum

Benennen Sie eine Liste um, damit sie ihren Inhalt oder Zweck besser widerspiegelt. Diese Anpassung ermöglicht es Bedienern, Listennamen an ihrer Workflow-Terminologie auszurichten, was die Übersichtlichkeit und Benutzerfreundlichkeit verbessert.

Vorbereitungen
Erforderliche Rolle: itil

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol ( ).
3. Wählen Sie die Registerkarte **Meine Listen** aus.
4. Wählen Sie die Liste aus, die Sie umbenennen möchten.
5. Wählen Sie das Einstellungssymbol ( ) und dann **Umbenennen**.



6. Benennen Sie im Popup-Fenster **Umbenennen** im Feld **Titel** den Namen der Liste um, und wählen Sie **Speichern**aus.
   Die Liste wird umbenannt.

Liste in Service Operations-Arbeitsbereich für ITOMneu anordnen

Ordnen Sie Listen neu an, um Informationen zu priorisieren und die Workflow-Organisation zu verbessern.

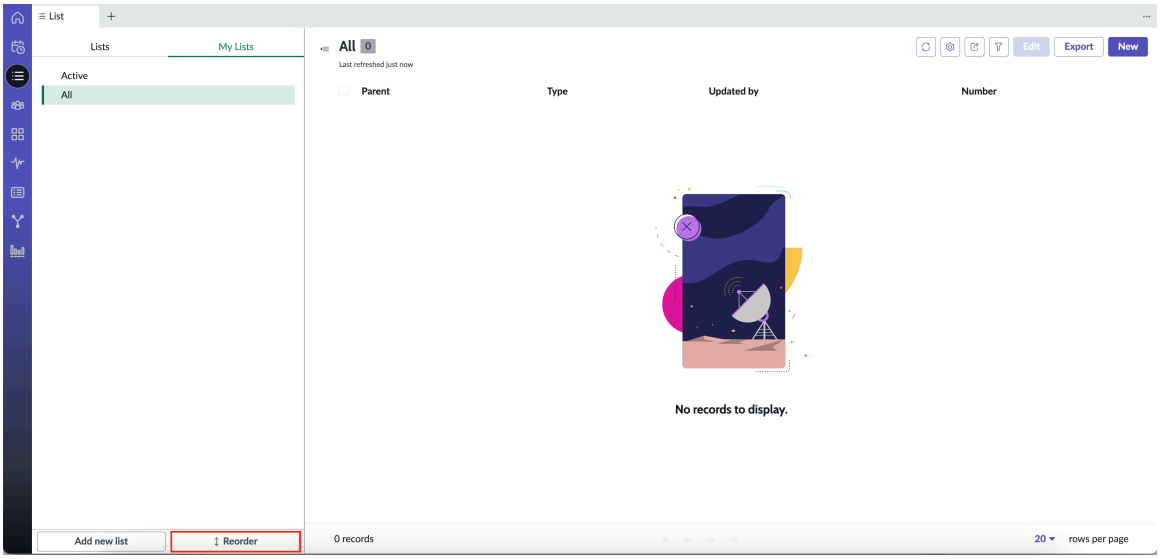
Vorbereitungen
Erforderliche Rolle: itil

Prozedur

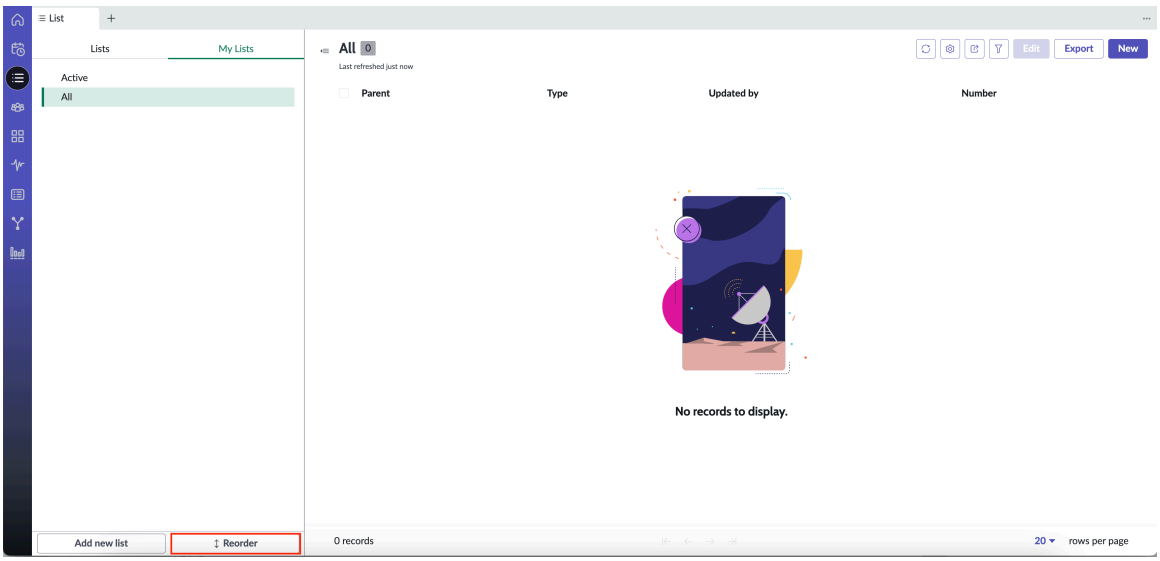
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol ( ).
3. Wählen Sie die Registerkarte **Meine Listen** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie die Liste aus, die Sie neu anordnen möchten.
5. Wählen Sie **Neu anordnen**, um die Position der Liste anzupassen.



Automatische Übersetzung

Liste in Service Operations-Arbeitsbereich für ITOMlöschen

Löschen Sie eine Liste, um Datensätze effizient zu verwalten, Ordnung in Ihrem Arbeitsbereich zu schaffen und Informationen organisiert zu halten.

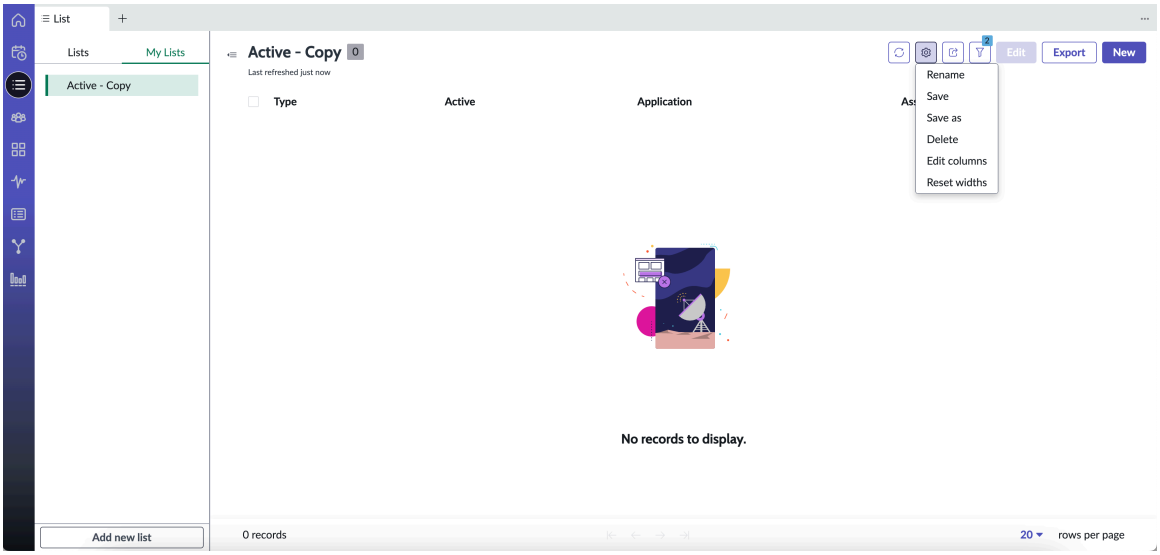
Vorbereitungen

Erforderliche Rolle: itil

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol ( ).
3. Wählen Sie die Registerkarte **Meine Listen** aus.
4. Wählen Sie die Liste aus, die Sie löschen möchten.
5. Wählen Sie das Einstellungssymbol ( ) und dann **Löschen aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Wählen Sie im Bestätigungsfenster **Löschen aus**.
   Die Liste wird gelöscht.

Zeigen Sie eine einheitliche Servicezuordnung und die Auswirkungspfade in an Service Operations-Arbeitsbereich

Visualisieren Sie Beziehungen zwischen Configuration Items (CIs) und Warnungen mit Echtzeitaktualisierungen und detaillierten Auswirkungspfaden. Verbessern Sie die Problembehandlung und die proaktive Verwaltung, indem Sie Ursachen und Abhängigkeiten für erkannte Services und Anwendungsservices schnell identifizieren.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_user, evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Die erweiterte Servicezuordnung in Service Operations-Arbeitsbereich zeigt den betroffenen Pfad einer Warnung an, damit Sie ihre Auswirkungen auf einen Service schnell bewerten können. Sie können auf die erweiterte Servicezuordnung direkt über das Service-Dashboard, den Vorschaubereich oder einen betroffenen Service in der Express-Liste zugreifen.Die Servicezuordnung bietet verschiedene Anzeigemodi:

- Für einen Service mit bis zu 60 CIs werden unabhängig vom Warnungsstatus in der Zuordnung alle CIs angezeigt.
- Für einen Service mit mehr als 60 CIs ohne Warnungen zeigt die Zuordnung bis zu 60 CIs an.
- Für einen Service mit mehr als 60 CIs mit Warnungen zeigt die Zuordnung den betroffenen Pfad der neuesten Warnung mit dem höchsten Schweregrad an.

Sie können auch eine breitere Ansicht der Servicetopologie in der Servicezuordnung für bis zu 250 CIs unabhängig von Warnungen untersuchen. Wählen Sie für eine breitere Ansicht **Löschen** und dann einen Modus mit bis zu 60 oder bis zu 250 Knoten aus.

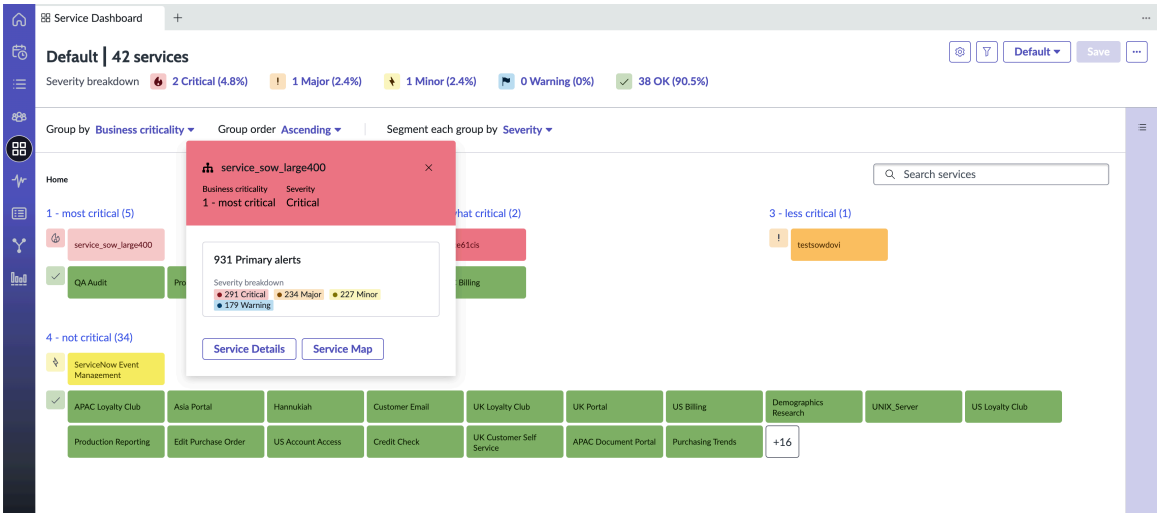
Hinweis: Administratoren können weiterhin die Legacy-Servicezuordnung verwenden, um die Weitergabe von Schweregraden zu verwalten. Greifen Sie auf die Zuordnung zu, indem Sie zu navigieren **Services** > **Anwendungsservices**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

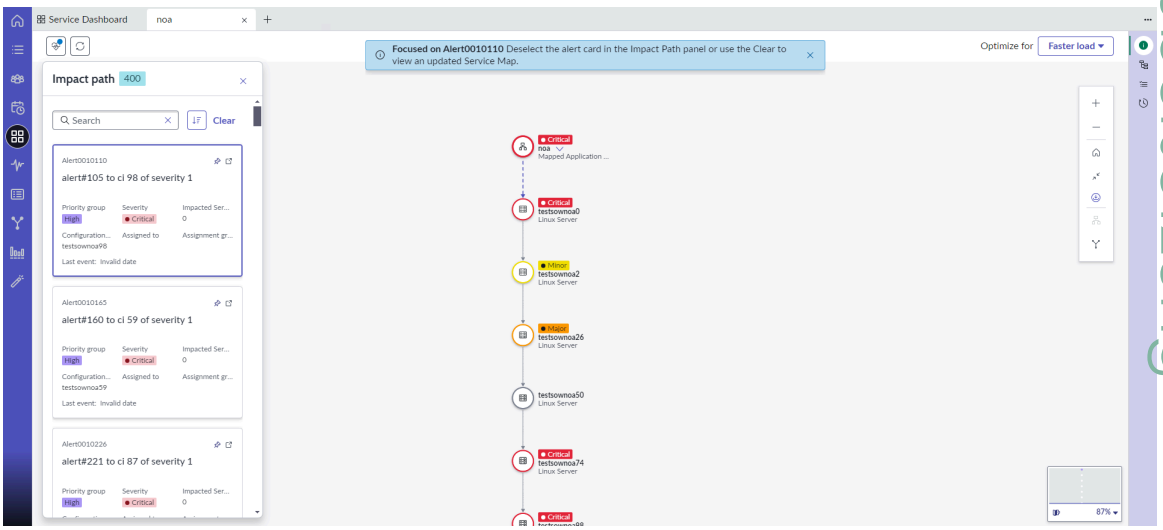
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Service-Dashboard-Symbol ( ).
   Die Seite „Service-Dashboard“ wird angezeigt.
3. Wählen Sie eine Servicekachel aus.
   In einem Popup-Fenster werden die Geschäftskritikalität und der Schweregrad eines Service angezeigt.



4. Wählen Sie **Servicezuordnung**aus.

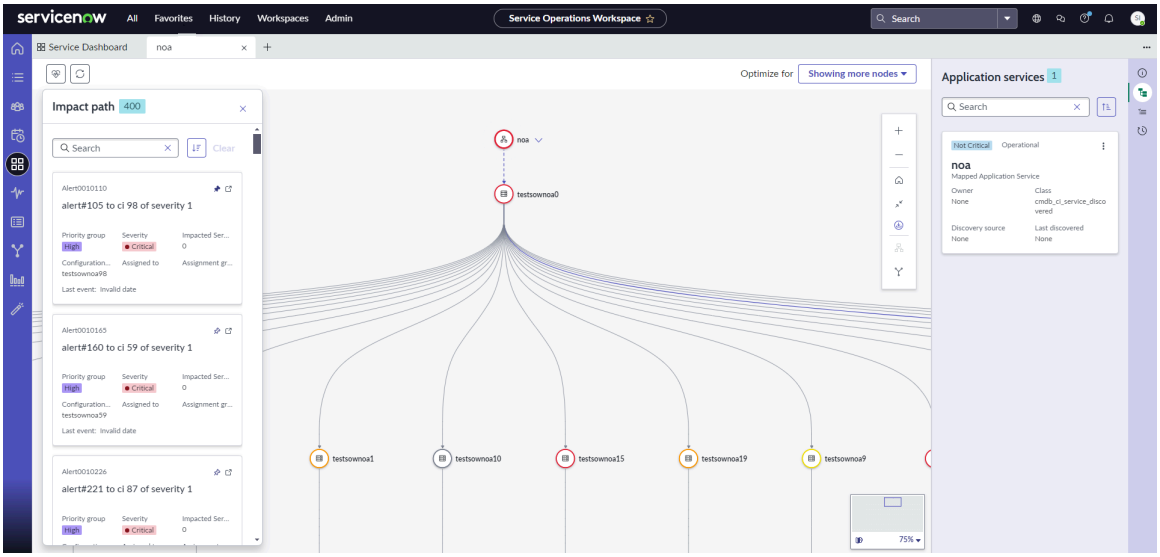
   Die Anwendungszuordnung wird zusammen mit den CI-Beziehungen angezeigt.



Hinweis: Je nach Größe des Service zeigt die einheitliche Übersicht entweder die vollständige Zuordnung (wenn sie bis zu 60 CIs enthält) oder einen Auswirkungspfad, der zur kritischsten Warnung führt (für Zuordnungen mit mehr als 60 CIs). Bei großen Karten können Sie weitere CIs anzeigen, indem Sie die vorhandene Auswahl löschen und zur Optimierungsoption **Anzeige weiterer Knoten** navigieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

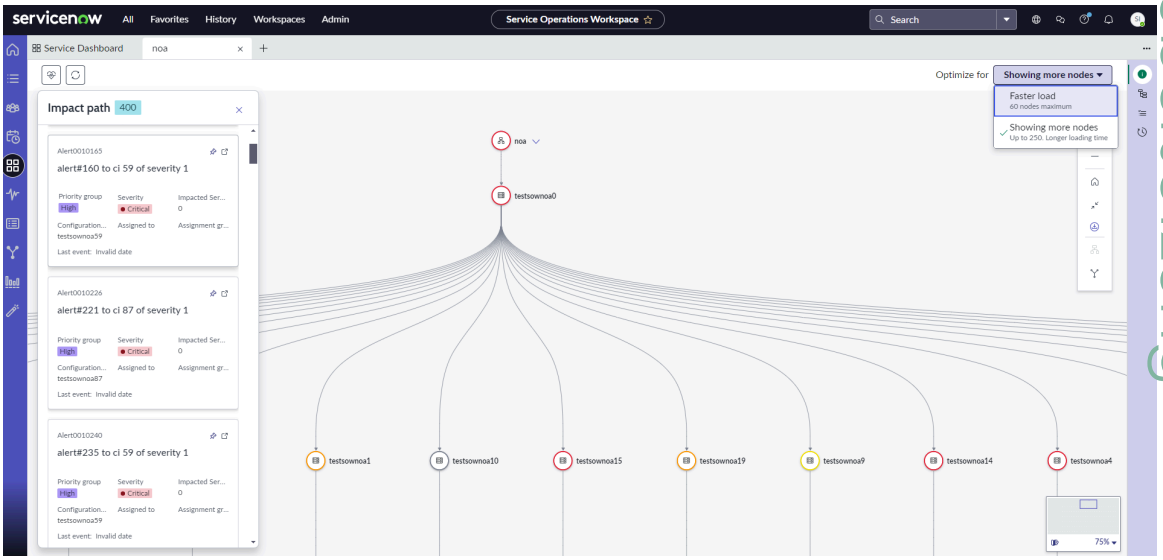


Wenn der Bereich „Auswirkungspfad“ geschlossen ist, können Sie ihn öffnen, indem Sie das Auswirkungspfad-Symbol ( ) wählen.

5. Navigieren Sie zwischen Warnungen, indem Sie eine Warnungskarte auswählen.

Alternativ können Sie die Suchfunktion verwenden, um eine Warnung anhand der Beschreibung, des CI oder der Warnungsnummer zu finden und sich auf ihren Auswirkungspfad zu konzentrieren.

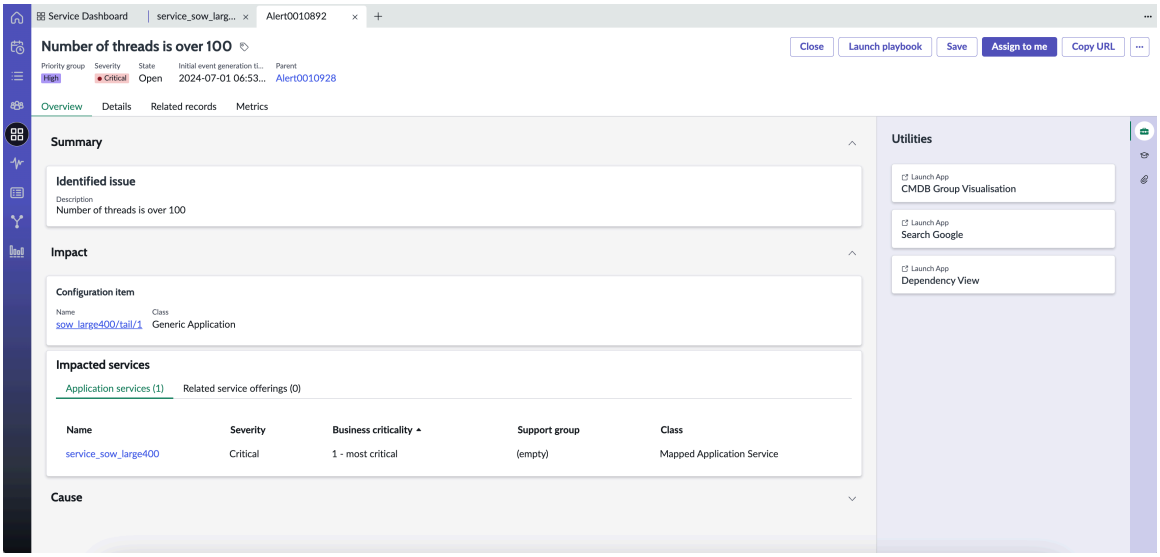
Wenn Sie eine Warnungskachel auswählen, wird die einheitliche Übersicht für diese Warnung angezeigt. Um zur vollständigen Zuordnung für den Service zurückzukehren, wählen Sie **Löschen**.



6. Um Warnungsdetails anzuzeigen, wählen Sie auf der Warnungskarte das Symbol zum Öffnen des Datensatzformulars ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Seite mit den Warnungsdetails wird geöffnet.



Konfigurieren Sie Einstellungen für die automatische Aktualisierung von Warnungslisten

Richten Sie Einstellungen für die automatische Aktualisierung für Warnungslisten ein, um Echtzeitaktualisierungen und eine nahtlose Überwachung sicherzustellen. Dies erhöht die Genauigkeit und Aktualität der angezeigten Informationen, was kürzere Antwortzeiten ermöglicht und die allgemeine Zuverlässigkeit und Leistung des Systems verbessert.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig werden Warnungen in den Warnungslisten automatisch aktualisiert, immer wenn eine Aktion für eine Warnung ausgeführt wird. Sie können die Zeit in Sekunden konfigurieren, nach der die Warnungsliste nach einer Aktion aktualisiert wird. Sie können auch die automatische Aktualisierung deaktivieren oder konfigurieren, wie oft die Warnungsliste aktualisiert wird. Das ist nützlich, wenn ständig viele Warnungen verarbeitet werden, um ein zu häufiges Aktualisieren zu verhindern.

Hinweis: Legen Sie die Berechtigungen der Leserolle auf die Ereignismanagement-Benutzer (evt_mgmt_user) fest. Andernfalls ist die Eigenschaft nicht verfügbar.

Prozedur

1. Navigieren Sie zu **Alle**, und geben Sie im Suchfeld `sys_properties_list.do`ein.

   Das Fenster „Systemeigenschaften“ wird geöffnet.

2. Suchen Sie nach den folgenden Eigenschaften, und konfigurieren Sie ihre Werte nach Bedarf.

Eigenschaften, um die Aktualisierung der Warnungsliste zu konfigurieren

Eigenschaft	Beschreibung
`evt_mgmt.ai_refresh_time_to_wait_after_manual_action`	Aktualisierungszeit der Warnungsliste (in Millisekunden), nachdem eine manuelle Aktion für die Warnung ausgeführt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Beschreibung
	Wenn mehrere Aktionen nacheinander ausgeführt wurden, beginnt die Aktualisierungszeit nach der letzten Aktion von neuem. Dadurch wird sichergestellt, dass die Warnungsliste den aktuellen Status widerspiegelt und umgehend nach Benutzerinteraktionen aktualisiert wird.
`evt_mgmt.ai_refresh_time_interval`	Wenn innerhalb des definierten Zeitintervalls (5.000 Millisekunden) ein Warnungsupdate empfangen wird, erfolgt für Updates während dieses Zeitraums keine sofortige Aktualisierung. Stattdessen führt das System am Ende des Zeitintervalls eine weitere Aktualisierung durch, um sicherzustellen, dass die Warnungsliste die neuesten verfügbaren Informationen widerspiegelt.
`evt_mgmt.disable_lists_auto_refresh`	Deaktiviert den automatischen Aktualisierungsprozess der Warnungslisten. Sie können eine neue Liste auf der Seite **Automatische Aktualisierung von Warnungslisten** erstellen, indem Sie im Navigationsbereich *em_alert_lists_auto_refresh.list* eingeben. Um eine automatische Aktualisierung der Liste zu verhindern, deaktivieren Sie die Option **Aktualisierung aktivieren**.

Automatische Übersetzung

Warnungsmetriken konfigurieren

Konfigurieren Sie die Metriken, die für Warnungen Service Operations-Arbeitsbereich vom Typ sichtbar sein sollen, oder verwenden Sie die mit dem Basissystem konfigurierten Metriken, um sich auf relevante Daten zu konzentrieren und die Fehlerbehebung zu beschleunigen.

Vorbereitungen

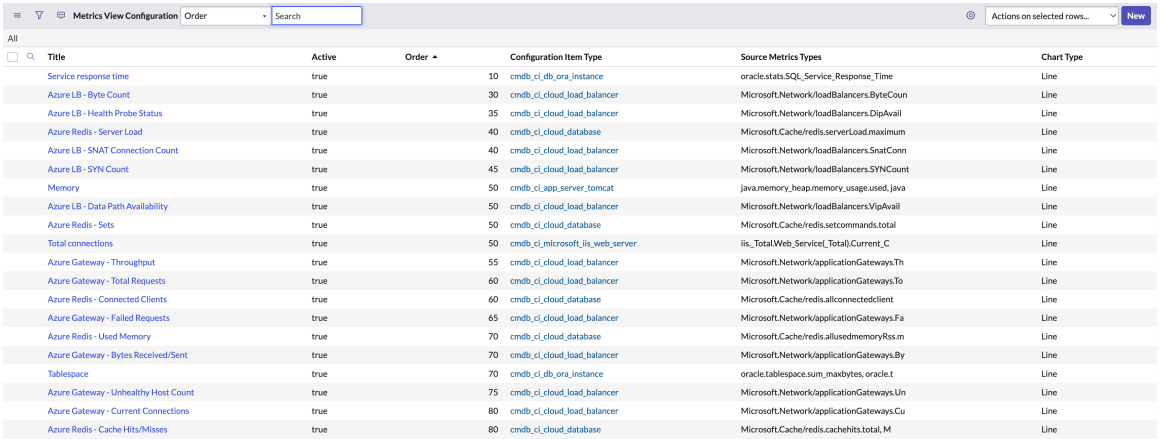
Stellen Sie sicher, dass das Plugin „Metrikdaten“ (sn_metrics_ng) installiert ist.

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Konfiguration der Metrikansicht**.



Title	Active	Order	Configuration Item Type	Source Metrics Types	Chart Type
Service response time	true	10	cmdb_ci_db_ora_instance	oracle.stats.SQL_Service_Response_Time	Line
Azure LB - Byte Count	true	30	cmdb_ci_cloud_load_balancer	Microsoft.Network/loadBalancers.ByteCoun	Line
Azure LB - Health Probe Status	true	35	cmdb_ci_cloud_load_balancer	Microsoft.Network/loadBalancers.DipAvail	Line
Azure Redis - Server Load	true	40	cmdb_ci_cloud_database	Microsoft.Cache/redis.serverLoad.maximum	Line
Azure LB - SNAT Connection Count	true	40	cmdb_ci_cloud_load_balancer	Microsoft.Network/loadBalancers.SnatConn	Line
Azure LB - SYN Count	true	45	cmdb_ci_cloud_load_balancer	Microsoft.Network/loadBalancers.SYNCount	Line
Memory	true	50	cmdb_ci_app_server_tomcat	java.memory_heap.memory_usage.used, java	Line
Azure LB - Data Path Availability	true	50	cmdb_ci_cloud_load_balancer	Microsoft.Network/loadBalancers.VipAvail	Line
Azure Redis - Sets	true	50	cmdb_ci_cloud_database	Microsoft.Cache/redis.setcommands.total	Line
Total connections	true	50	cmdb_ci_microsoft_iis_web_server	iis_Total.Web_Service(_Total).Current_C	Line
Azure Gateway - Throughput	true	55	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.Th	Line
Azure Gateway - Total Requests	true	60	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.To	Line
Azure Redis - Connected Clients	true	60	cmdb_ci_cloud_database	Microsoft.Cache/redis.allconnectedclient	Line
Azure Gateway - Failed Requests	true	65	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.Fa	Line
Azure Redis - Used Memory	true	70	cmdb_ci_cloud_database	Microsoft.Cache/redis.allusedmemoryRss.m	Line
Azure Gateway - Bytes Received/Sent	true	70	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.By	Line
Tablespace	true	70	cmdb_ci_db_ora_instance	oracle.tablespace.sum_maxbytes, oracle.t	Line
Azure Gateway - Unhealthy Host Count	true	75	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.Un	Line
Azure Gateway - Current Connections	true	80	cmdb_ci_cloud_load_balancer	Microsoft.Network/applicationGateways.Cu	Line
Azure Redis - Cache Hits/Misses	true	80	cmdb_ci_cloud_database	Microsoft.Cache/redis.cachehits.total, M	Line

2. Wählen Sie auf der Seite „Konfiguration der Metrikansicht“ die Option **Neu** aus.
3. Füllen Sie die Felder des Formulars aus.
   Weitere Informationen zu diesen Feldern finden Sie unter Felder des Formulars „Konfiguration der Metrikansicht“.
4. Wählen Sie **Absenden**.

Zeigen Sie Warnungsmetriktrends in an Service Operations-Arbeitsbereich

Zeigen Sie die Metriken für eine Warnung an, und passen Sie den Zeitbereich an, um die Trends für die Warnung oder das zugehörige Configuration Item (CI) anzuzeigen. Dies ermöglicht genauere Analysen und ermöglicht eine schnellere Entscheidungsfindung.

Vorbereitungen

Stellen Sie sicher, dass das Plugin „Metrikdaten“ (sn_metrics_ng) installiert ist.

Konfigurieren Sie die Metriken, die für die Warnung angezeigt werden sollen, wie in Warnungsmetriken konfigurieren beschrieben.

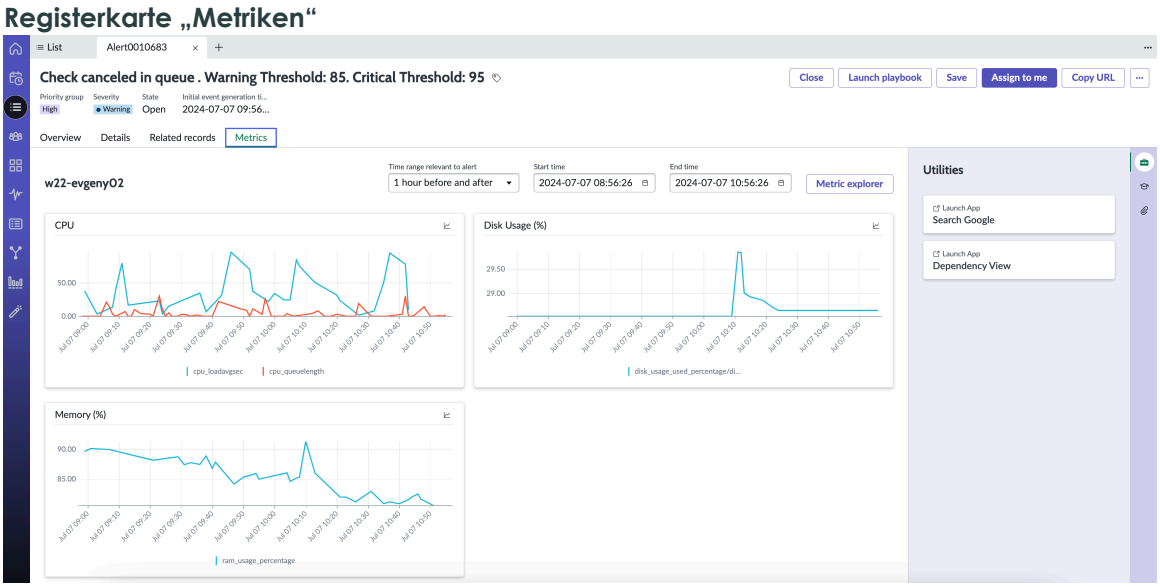
Erforderliche Rolle: evt_mgmt_admin

Prozedur

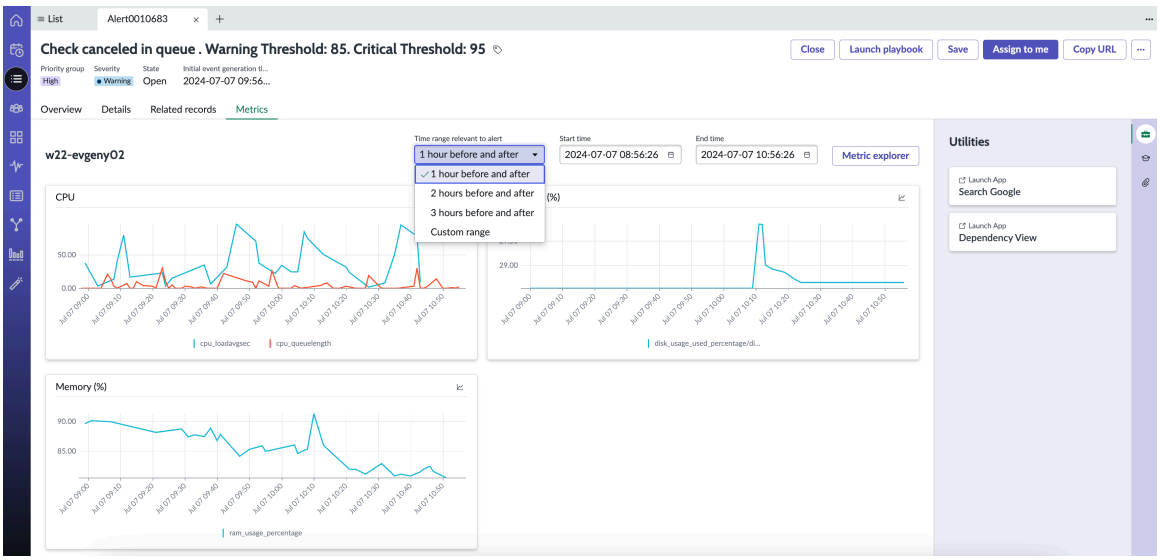
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol ( ).
3. Auswahlvorgang **Listen** > **Warnungen** > **Alle Warnungen**.
   Die Seite „Warnungen – Alle Warnungen“ wird geöffnet.
4. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
   Die Warnung wird auf einer separaten Registerkarte geöffnet und zeigt die Registerkarte **Übersicht** an.
5. Wählen Sie die Registerkarte **Metriken** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Konfigurieren Sie in den Feldern über den Metrikdiagrammen den Zeitbereich für die Metriken der Warnung.



Um die Metrikanzeige anzupassen, konfigurieren Sie im die folgenden Eigenschaften **Systemeigenschaften** > **Alle Eigenschaften** Seite:

- *ws_metric.widgets_number_limit*: Geben Sie die Anzahl der Widgets/Datensätze an, die auf der Registerkarte „Metriken“ angezeigt werden können.
- *ws_metric.datasets_per_widget_limit*: Geben Sie die Anzahl der Diagramme/Datensätze an, die in einem Diagramm angezeigt werden dürfen.

Feldname	Beschreibung
Relevanter Zeitbereich für Warnung	Dauer für die Berechnung von Metriken rund um die Warnung.
Startzeit	Startdatum und -uhrzeit für Metrikberechnungen.

Automatische Übersetzung

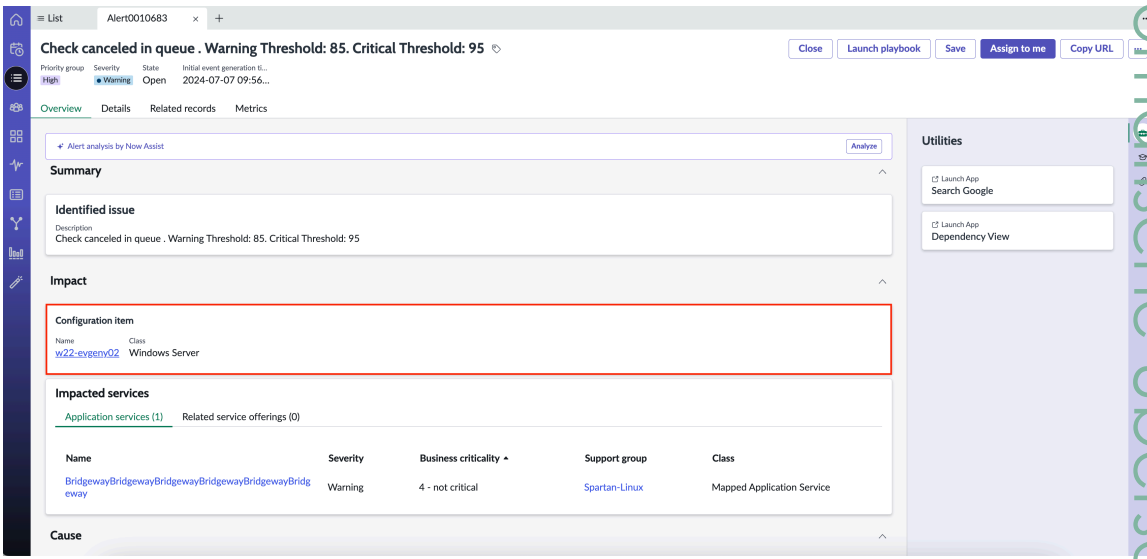
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Beschreibung
Endzeit	Enddatum und -uhrzeit für Metrikberechnungen.

7. Wählen Sie einen Parameter unter einem Diagramm aus, um die Daten des angegebenen Parameters im Diagramm auszublenden.
8. Wahlweise: Wählen Sie die Schaltfläche **Explorer für Einblicke**, um Metriken anzuzeigen, indem Sie sie per Drag-and-Drop auf eine Zeitleiste ziehen.
9. Wählen Sie **Speichern**.
10. Wahlweise: Zeigen Sie einen Zeitbereich für das CI einer Warnung an.

    a. Wählen Sie die Registerkarte **Übersicht** aus.

    b. Wählen Sie im Abschnitt „Auswirkung“ auf der Karte **Konfigurationselement** den Link zum CI unter dem Feld **Name**.



    c. Wählen Sie die Registerkarte **Metriken** aus.

    d. Wählen Sie **Speichern**.

Zeigen Sie die CI-Integrität in an Metric Explorer

Zeigen Sie den Zustand und die Leistung des CI einer Warnung mit Metric Exploreran, um bei der Behebung von Problembereichen im CI zu helfen.

Vorbereitungen

Alle Plugins im Zusammenhang mit Ereignismanagement, Metrikdatenund Metric Explorersind erforderlich.

Erforderliche Rollen:

- Um in Metric Explorer auf Metrikdaten-Metriken zugreifen zu können, sind die Rollen workspace_agent und itil erforderlich.
- Zum Konfigurieren des Metrikensatzes, der in Metric Explorer für eine Klasse angezeigt wird, ist die Rolle admin oder evt_mgmt_admin erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

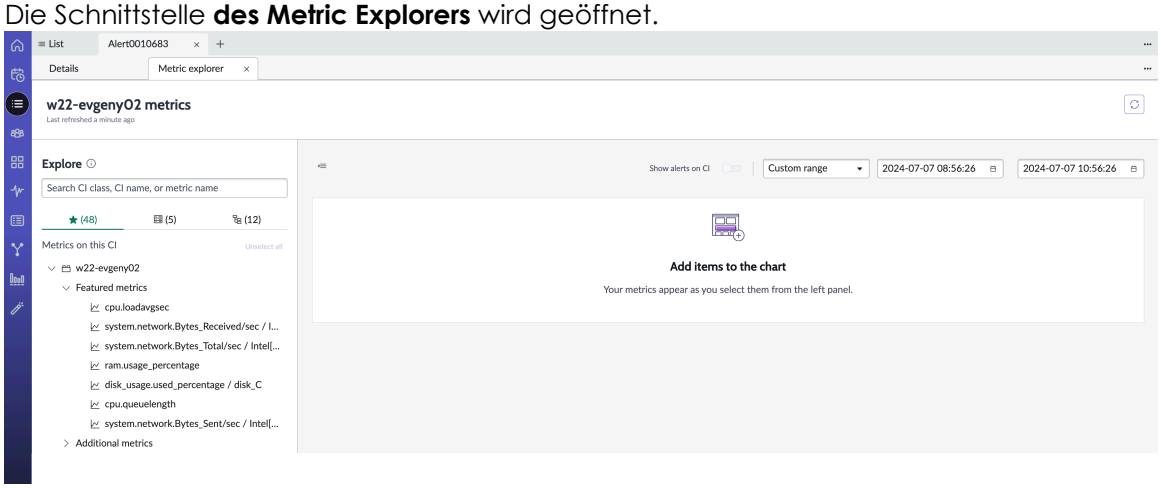
Metric Explorer zeigt die folgenden Metrikdaten -Daten an:

- Diagramme, Kontrollgrenzen und Zusammenfassungen für Schlüsselmetriken für Configuration Items (CIs) an einem zentralen Ort.
- Zusammenfassung von Metriken für CIs mit Ressourcen in einer einzigen konsolidierten Zeitreihe
- Möglichkeiten für Administratoren zur Konfiguration, welche Metriktypen für jede CI-Klasse angezeigt werden

Metriken werden nur für Warnungen angezeigt, die ein CI enthalten.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Listensymbol ( ).
3. Auswahlvorgang **Listen** > **Warnungen** > **Alle Warnungen**.
   Die Seite „Warnungen – Alle Warnungen“ wird geöffnet.
4. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
   Die Warnung wird auf einer separaten Registerkarte geöffnet und zeigt die Registerkarte **Übersicht** an.
5. Wählen Sie die Registerkarte **Metriken** aus.
6. Wählen Sie die Schaltfläche **Metric Explorer**.
   Die Schnittstelle **des Metric Explorers** wird geöffnet.



Hinweis: Sie können auch auf die Unterregisterkarte **Metriken** und die Schaltfläche **Metriken-Explorer** zugreifen, wenn Sie ein CI auswählen.

7. Wählen Sie Metriken im Abschnitt „Untersuchen“ aus, um die Metriken im Diagrammformat im Abschnitt **„Anwenderdefiniertes Diagramm“** anzuzeigen.
   Metriken sind in die folgenden Unterregisterkarten unterteilt:

Abschnittsunterregisterkarten erkunden

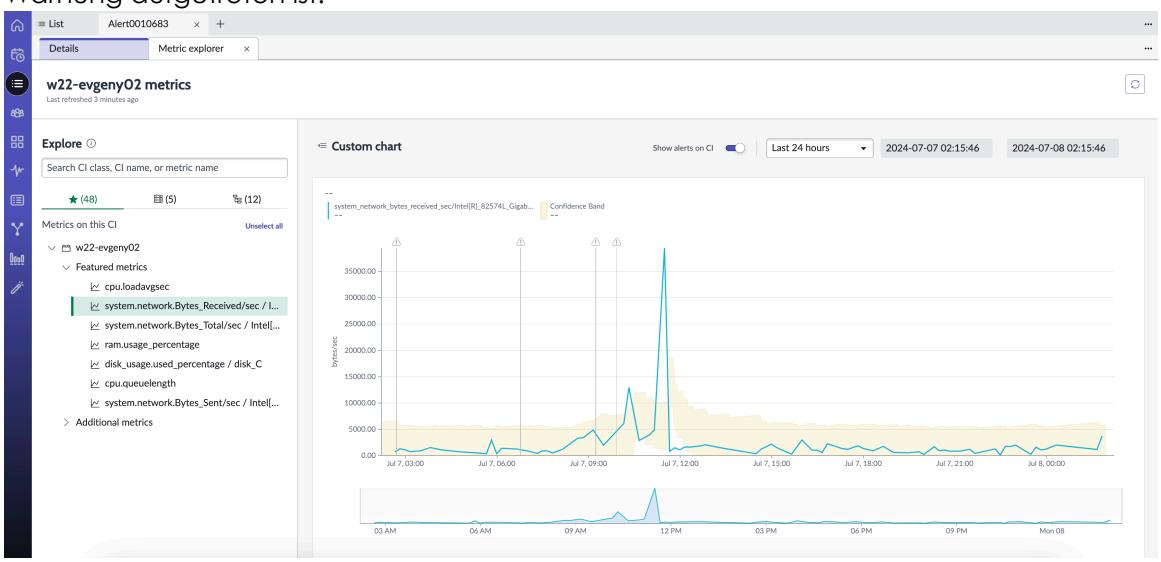
Unterregisterkarte	Beschreibung
★	Zeigt Metriken für das aktuelle CI an.
	Zeigt Metriken für andere CIs auf demselben Host an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterregisterkarte	Beschreibung
	Zeigt Metriken zu Einstiegspunkten an, die sich auf den Service beziehen, auf den sich das CI auswirkt. **Hinweis:** Bei der Arbeit mit großen Mengen von Einstiegspunkten (100.000 oder mehr) kann das Sammeln von Einstiegspunktmetriken zu einer Systemverschlechterung führen. Um dies zu verhindern, erstellen Sie die Eigenschaft *sn_disable_selection_entry_point* (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**) und legen Sie diese Option auf **„true“** fest, um die Metrikensammlung für Einstiegspunkte zu deaktivieren.

8. Konfigurieren Sie im Abschnitt **Anwenderdefiniertes Diagramm** einen Zeitbereich, für den Sie die angezeigten Metriken anzeigen möchten.
9. Beschriften Sie Warnungen im anwenderdefinierten Diagramm, indem Sie die Option **Warnungen in CI anzeigen** aktivieren.

   Ein Warnungssymbol (⚠) wird oben im Diagramm an dem Punkt angezeigt, an dem die Warnung aufgetreten ist.



Bereitschaftsplanung in Service Operations-Arbeitsbereich für ITOM

ITOM Service Operations-Arbeitsbereich unterstützt Sie beim Erstellen und Verwalten von Rufbereitschaftsschichten und -zeitplänen. Der Rufbereitschaftszeitplan bestimmt, wer zu einem bestimmten Zeitpunkt Rufbereitschaft hat. Erfahren Sie, wie Sie Rufbereitschaftskalender und Eskalationsrichtlinien konfigurieren, um bei kritischen Problemen rechtzeitig zu reagieren, Ausfallzeiten zu reduzieren und die Servicekontinuität zu gewährleisten. Die Optimierung dieser Prozesse verbessert die Bereitschaft des Teams, minimiert Unterbrechungen und verbessert die Servicezuverlässigkeit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte mit der Bereitschaftsplanung

Um die Bereitschaftsplanung für Warnungen zu aktivieren, fügen Sie zuerst die Warnungstabelle [em_alert] in die Liste der Auslöserregel-Tabellenkonfigurationen ein. Weitere Informationen finden Sie unter Warnungstabelle hinzufügen, um Bereitschaftsplanung für Service Operations-Arbeitsbereich für ITOMzu aktivieren.

Teams in Service Operations-Arbeitsbereich

Verwenden Sie das Teams-Menü ( ) in Service Operations-Arbeitsbereich, um alle Teams anzuzeigen. Wählen Sie eine Teamkarte aus, um den Zeitplan eines Teams anzuzeigen und zu verwalten und um Eskalationsrichtlinien und Teameinstellungen für eine ausgewählte Schicht zu definieren. Diese Funktion stellt sicher, dass Ihr Team weiß, wer Rufbereitschaft hat und verantwortlich ist, sodass Sie sicher sein können, dass kritische Warnungen oder Incidents bestätigt werden. Informationen zum Erstellen von Schichten finden Sie unter Rufbereitschaftsschicht für Teams erstellen .

Warnungstabelle hinzufügen, um Bereitschaftsplanung für Service Operations-Arbeitsbereich für ITOMzu aktivieren

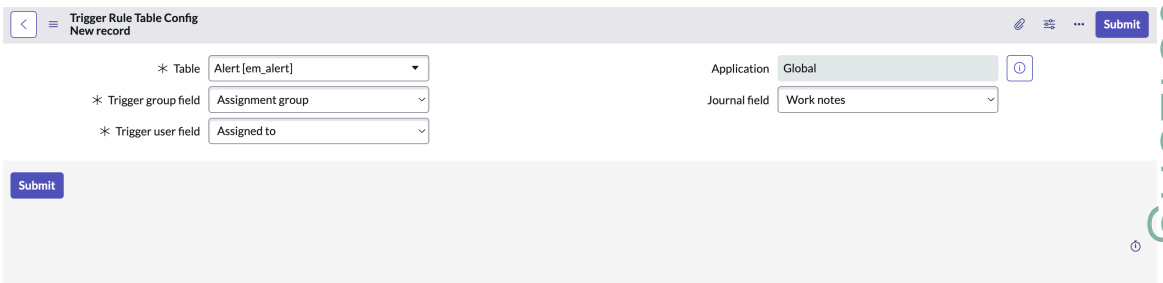
Aktivieren Sie die Bereitschaftsplanung, indem Sie die Warnungstabelle [em_alert] in die Liste „Auslöserregel-Tabellenkonfiguration“ aufnehmen. Dies ermöglicht das Erstellen von Schichten und das Implementieren von Eskalationsauslösern und -richtlinien, um sicherzustellen, dass Teams umgehend auf Warnungen reagieren und die Betriebskontinuität aufrechterhalten können.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren Sie zu **Alle**, und geben Sie im Suchfeld `trigger_rule_table_cfg.list`ein. Die Seite Auslöserregel-Tabellenkonfigurationen wird geöffnet.
2. Füllen Sie im Formular die Felder mit den folgenden Werten aus.



   - Wählen Sie im Feld **Tabelledie Option Warnung [em_alert]**aus.
   - Wählen Sie im Feld **Auslösergruppedie Option Zuweisungsgruppe**aus.
   - Wählen Sie im Feld **AuslöseranwenderZugewiesen an aus**.
   - Wählen Sie im Feld **Journaldie Option Arbeitsnotizen**aus.
3. Wählen Sie **Absenden**.

Nächste Maßnahme

Erstellen Sie eine Rufbereitschaftsschicht für Ihr Team .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Service Operations-Arbeitsbereich für ITOM verwenden

Service Operations-Arbeitsbereich für ITOM bietet eine einheitliche Plattform, die verschiedene Anwendungen integriert und sich auf die optimierte Warnungsverwaltung spezialisiert hat. Verwalten Sie IT Operations-Workflows nahtlos und bearbeiten Sie Warnungen effizient, um optimale Leistung und Produktivität zu gewährleisten.

Beim Einrichten von Service Operations-Arbeitsbereichist es wichtig, IT Operations Management (ITOM) für die Verwaltung von Warnungen und IT Service Management (ITSM) für die Lösung von Incidents und die Bereitstellung von Services zu konfigurieren. Dieses integrierte Setup gewährleistet den Zugriff auf alle Funktionen und erleichtert die umfassende Verwaltung des IT-Betriebs und der Servicequalität.

Weitere Informationen zu den Aufgaben in ITSMfinden Sie unter Service Operations-Arbeitsbereich for ITSM .

Integrations Launchpad in Service Operations-Arbeitsbereich für ITOM

Integrations Launchpad zeigt alle Ereignismanagement -Connector-Integrationen, mit denen Anwender Ereignisse von externen oder internen Geräten abrufen oder übertragen können. Dieser zentralisierte Hub vereinfacht Ereignismanagement, indem er Integrationsoptionen an einem Ort bündelt.

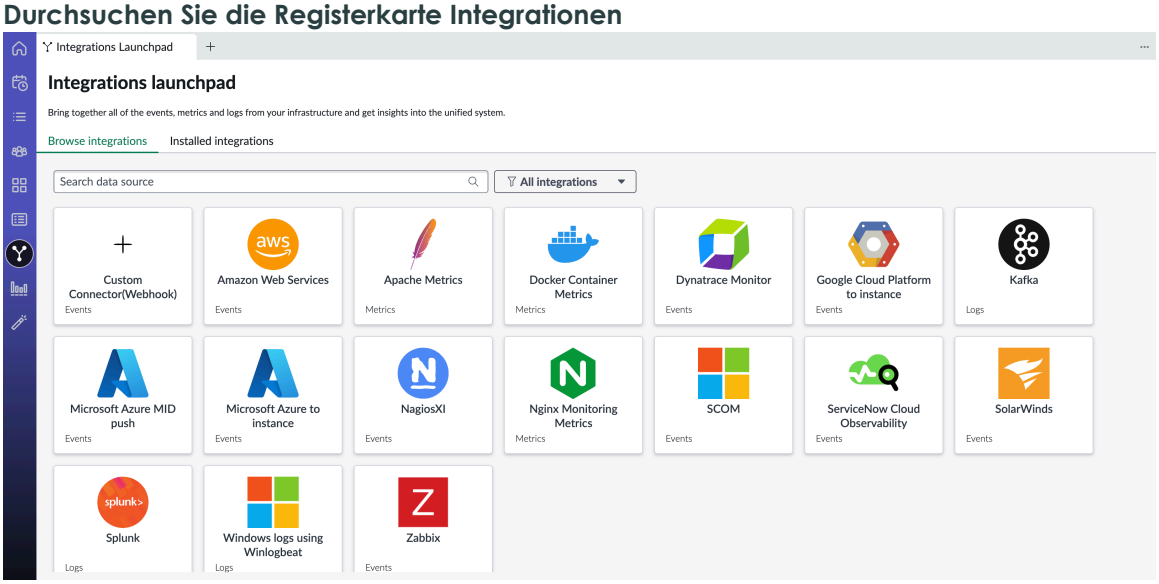
Integrations Launchpad optimiert den Prozess der Verwaltung und Nutzung von Event-Connectors, erhöht die betriebliche Effizienz und stellt eine nahtlose Integration von Event-Daten aus verschiedenen externen Quellen sicher. Diese Zentralisierung hilft Benutzern, eine bessere Kontrolle und Transparenz über ihr Ereignismanagement -Ökosystem zu behalten.

Durchsuchen Sie die Registerkarte Integrationen

Zeigt alle Pull-, Push- und anwenderdefinierten Connector-Integrationen an, einschließlich Connectors, die im Store ServiceNow und von Drittanbietern verfügbar sind. Diese Registerkarte enthält:

- Suchfeld: Ermöglicht das schnelle Finden einer bestimmten Datenquelle durch Eingabe von Schlüsselwörtern, verbessert die Effizienz und spart Zeit.
- Liste „Alle Integrationen“: Organisiert Integrationen in Kategorien wie Alle Integrationen, Ereignisse (Push, Pull, Anwenderdefiniert), Metriken (ACC-M) und Protokolle (HLA). Diese Kategorisierung erleichtert Benutzern das Durchsuchen der Liste und das Auswählen des relevanten Integrationstyps, den sie benötigen.

Durchsuchen Sie die Registerkarte Integrationen

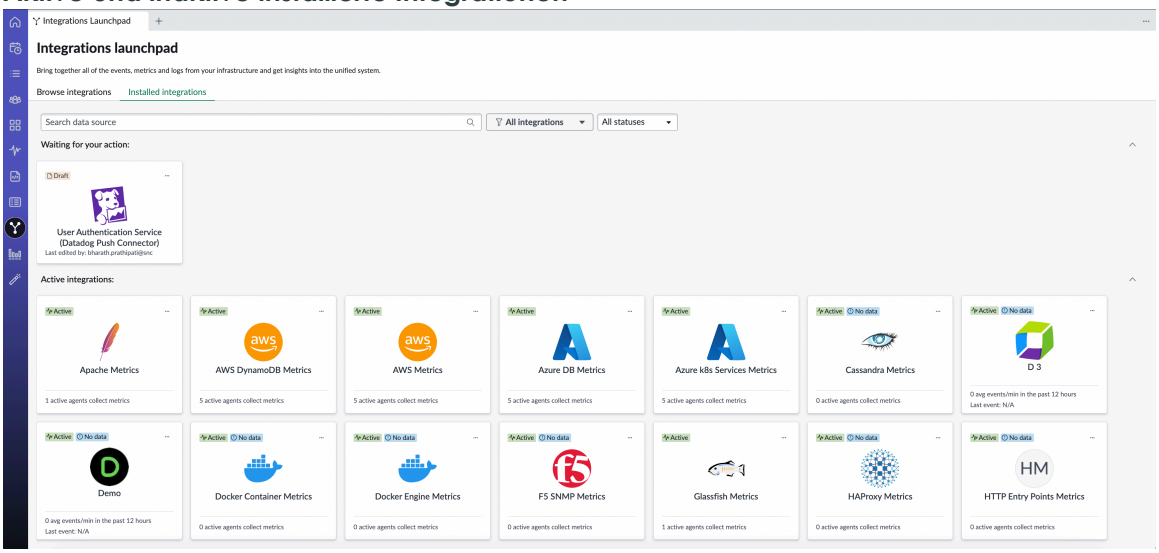


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

Registerkarte Installierte Integrationen

Aktive und inaktive installierte Integrationen



Listet alle vom Anwender konfigurierten Integrationen auf, sowohl aktive als auch inaktive. Diese Registerkarte enthält:

- Suchfeld: Hilft Anwendern, durch Eingabe von Stichwörtern schnell eine bestimmte Datenquelle zu finden, verbessert die Effizienz und spart Zeit.
- Liste „Alle Integrationen“: Organisiert Integrationen in Kategorien wie Alle Integrationen, Ereignisse (Push, Pull, Anwenderdefiniert), Metriken (ACC-M) und Protokolle (HLA). Diese Kategorisierung erleichtert Benutzern das Durchsuchen der Liste und das Auswählen des relevanten Integrationstyps, den sie benötigen.
- Liste aller Status: Ermöglicht das Filtern von Integrationen nach ihrem Status – „Alle Status“, „Aktiv“, „Inaktiv“, „Entwurf“ oder „Keine Daten“. Dies hilft Benutzern, Integrationen basierend auf ihrem aktuellen Status schnell zu identifizieren und zu verwalten.

Integrationsstatus und Beschreibung

Status	Beschreibung
Alle Status	Alle Integrationsstatus
Aktiv	Aktive Integrationen, die erfolgreich installiert wurden
Inaktiv	Inaktive Integrationen, die erfolgreich installiert wurden
Entwurf	In Bearbeitung befindliche Integrationen mit einer Konfiguration, die gestartet, aber nicht abgeschlossen wurde
Keine Daten	Integrationen, die erfolgreich ohne Daten installiert wurden

Konfigurieren Sie einen Pull-Connector

Konfigurieren Sie Pull-Connectors, die ein Skript, eine Connector-Definition und eine Connector-Instanz erfordern, um Ereignisse von externen Geräten abzurufen. Diese Connectors automatisieren den Datenabrufprozess und stellen die nahtlose Integration externer Ereignisse in Ihr System sicher, um eine effiziente Überwachung und Verwaltung zu ermöglichen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

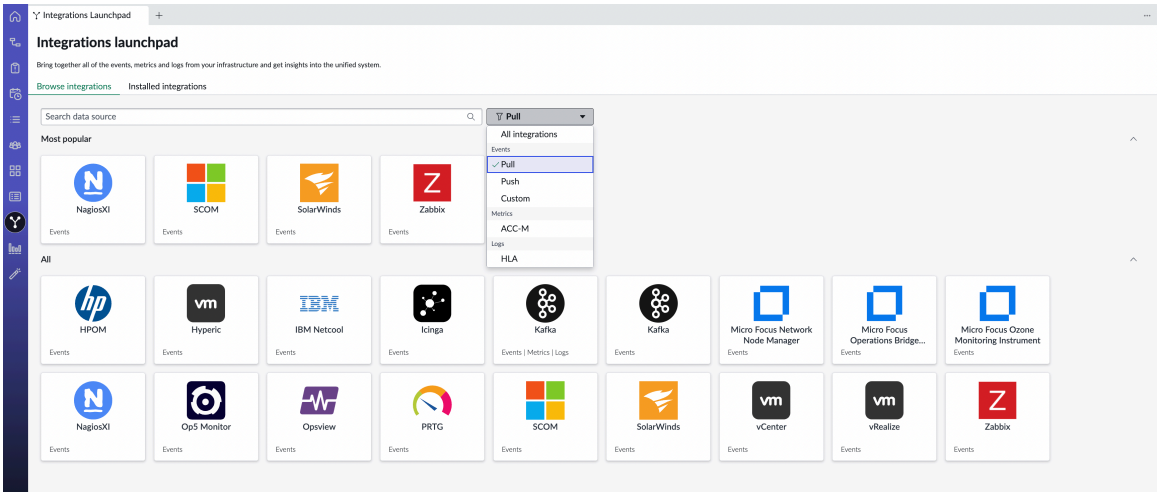
Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

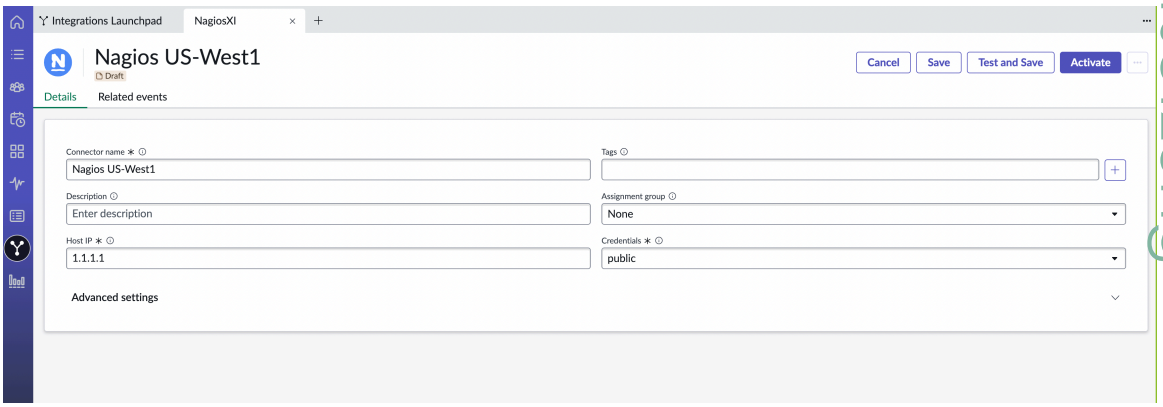
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( ).
3. Wählen Sie auf der Registerkarte **Integrationen** durchsuchen die Dropdown-Liste **Alle Integrationen** und dann **Abrufen aus**.
   Es werden nur Pull-Connector-Kacheln angezeigt.

Pull-Connectors



4. Wählen Sie eine Pull-Connector-Kachel aus.
   Wenn sich ein Popup-Menü öffnet, wählen Sie die Daten aus, die von diesem Connector nachverfolgt werden sollen, und wählen Sie **Fortsetzen**aus.

Detailseite zum Abrufen von Connectors



5. Geben Sie auf der Registerkarte **Details** im Feld **Connector-Name** einen eindeutigen Namen für den Connector-Typ ein.
6. Wahlweise: Geben Sie im Feld **Tags** Tags ein, um Connectors dieses Typs auf Express-Listezu finden und zu identifizieren.

   Um zusätzliche Tags hinzuzufügen, wählen Sie das Pluszeichen ( ) neben dem Feld **Tags**.
   Das Fenster „Tags hinzufügen“ wird geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Geben Sie im Feld **Schlüssel** einen Tag-Schlüssel ein.

b. Geben Sie im Feld **Wert** einen Tag-Wert ein.

c. Wählen Sie **Hinzufügen**.

7. Wahlweise: Geben Sie im Feld **Beschreibung** kurze Informationen zu diesem Connector ein.
8. Wahlweise: Wählen Sie in der Dropdown-Liste **Zuweisungsgruppe** die Gruppe oder das Team aus, die bzw. das für die Verwaltung und Wartung des Connectors verantwortlich ist.
9. Geben Sie im Feld **Host-IP** die IP-Adresse ein, die zur Auswahl des entsprechenden MID-Server für die Kommunikation mit dem Ereignisquellhost verwendet wird.
Sie können den Hostnamen anstelle der Host-IP verwenden.
10. Wählen Sie in der Dropdown-Liste **Anmeldeinformationen** die gültigen Anmeldeinformationen für den Zugriff auf den Ereignisquellhost aus.
Um neue Anmeldeinformationen zu erstellen, wählen Sie **Neue Anmeldeinformationen erstellen** und fahren mit dem Prozess fort.
11. Wahlweise: Wenn Sie die -Konfigurationen an bestimmte Anforderungen anpassen möchten, wählen Sie **Erweiterte Einstellungen**, und füllen Sie das Formular aus.

Feld	Beschreibung
Verbundener MID-Server	Legen Sie fest, ob das System den optimalen MID-Server auswählt oder ob Sie einen bestimmten MID-Server selbst auswählen sollen. Führen Sie dies nur durch, wenn Sie Änderungen an MID-Server vornehmen müssen. Lassen Sie es andernfalls leer, und lassen Sie das System das optimale MID-Serverauswählen.
Zeitplan für Ereignissammlung (Sekunden)	Geben Sie die Häufigkeit in Sekunden ein, die angibt, wie oft das System nach neuen Ereignissen aus der externen Ereignisquelle suchen soll. Der Wert darf nicht niedriger sein als die minimale Zeitplaneigenschaft, die standardmäßig 120 Sekunden beträgt.
Protokoll	Definiert das Kommunikationsprotokoll, das zum Abrufen von Ereignissen von externen Geräten verwendet wird.
severity_by_state_type	Bestimmt den Schweregrad, der Ereignissen zugewiesen ist, basierend auf ihrem Statustyp.
time_zone	Gibt die Zeitzone an, die zum Aufzeichnen und Anzeigen von Ereigniszeitstempeln verwendet wird.
offset_min	Legt den Zeitversatz für den Ereignisabruf fest, um eine genaue Synchronisierung sicherzustellen.
Port	Überprüfen Sie die Standardwerte für Ihren Connector-Typ, z. B. Portdetails oder Zeitformate, und ändern Sie sie nach Bedarf. Standardwerte von Ihrem Connector sind ausgefüllt. Gibt die Portnummer an, die für die Kommunikation mit externen Geräten verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
max_fetch_interval_min	Begrenzt das maximale Intervall zwischen Ereignisabrufvorgängen.
initial_sync_in_days	Legt die Dauer für den ersten Synchronisierungsprozess beim Abrufen von Verlaufsdaten fest.

12. Wahlweise: Testen Sie den Connector, bevor Sie ihn aktivieren, indem Sie **Test und Speichern**auswählen.
13. Um den Connector zu speichern, wählen Sie **Speichern**.
14. Um den Pull-Connector zu aktivieren, wählen Sie **Aktivieren**aus.
    Der Pull-Connector ist aktiviert, und seine Kachel wird auf der Registerkarte **Installierte Integrationen** angezeigt.

Nächste Maßnahme

Um die erfolgreiche Konfiguration des Pull-Connectors und den Flow von Ereignissen im System zu bestätigen, wählen Sie die Registerkarte **Zugehörige Ereignisse**. Wenn das Setup erfolgreich ist, fahren Sie mit **Automatisierung hinzufügen**, um eine Warnungsautomatisierung einzurichten. Einzelheiten zur Registerkarte **Zugehörige Ereignisse** finden Sie unter Überprüfen Sie die Integrations- und Konfigurationsintegrität, Informationen zur Automatisierung von Warnungen finden Sie unter Warnungsautomatisierung in Service Operations-Arbeitsbereich für ITOM.

Konfigurieren Sie einen Push-Connector

Integrieren Sie mit einem Push-Connector, um eine Verbindung zu einer externen Ereignisquelle herzustellen und Ereignisinformationen an Ihre ServiceNow -Instanz zu übertragen.

Vorbereitungen

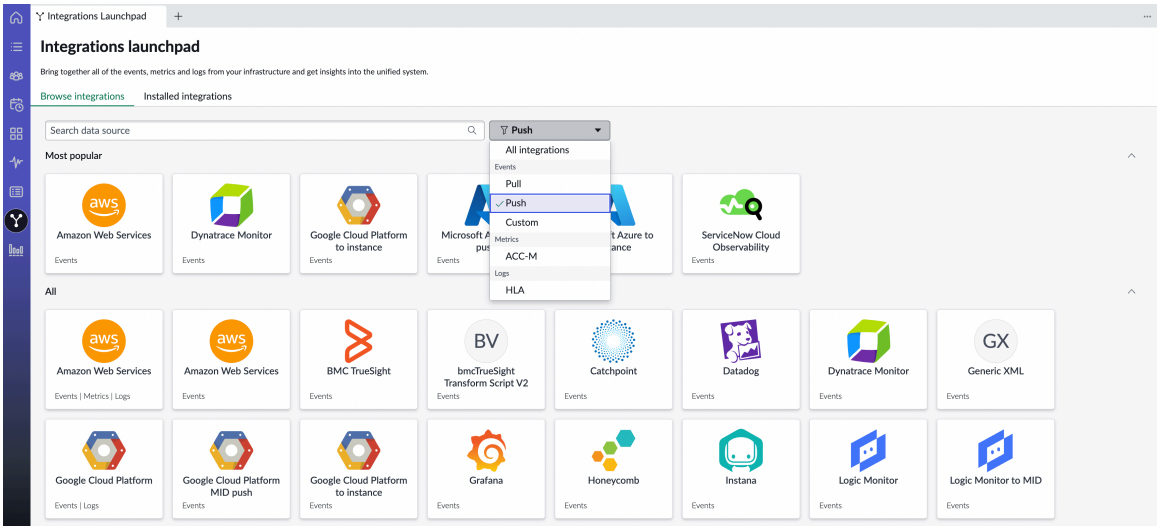
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Wählen Sie auf der Registerkarte **Integrationen** durchsuchen die Dropdown-Liste **Alle Integrationen** und dann **Push**aus.
   Es werden nur Push-Connector-Kacheln angezeigt.

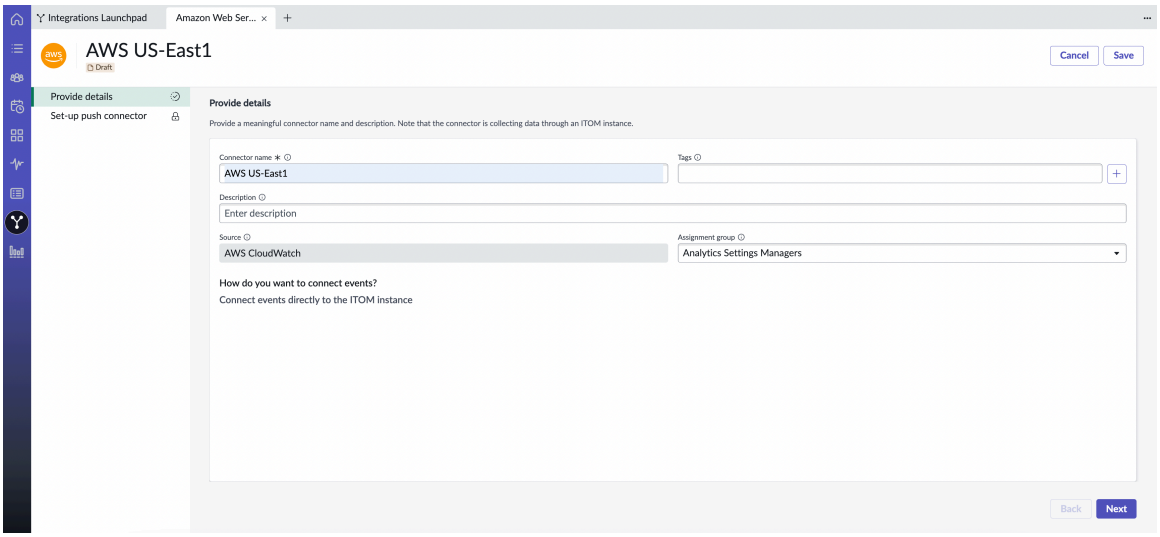
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Push-Connectors



4. Wählen Sie eine Kachel des Push-Connector-Typs aus.
5. Geben **Sie** im Bildschirm Details bereitstellen Details zum Connector-Typ an.

Detailseite für Push-Connectors



a. Geben Sie im Feld **Connector-Name** einen eindeutigen Namen für den Connector-Typ ein.

b. Wahlweise: Geben Sie im Feld **Tags** Tags ein, um Connectors dieses Typs auf Express-Listezu finden und zu identifizieren.
Um zusätzliche Tags hinzuzufügen, wählen Sie das Pluszeichen neben dem Feld **Tags**. Das Fenster „Tags hinzufügen“ wird geöffnet.

i. Geben Sie im Feld **Schlüssel** einen Tag-Schlüssel ein.

ii. Geben Sie im Feld **Wert** einen Tag-Wert ein.

iii. Wählen Sie **Hinzufügen**.

c. Wahlweise: Geben Sie im Feld **Beschreibung** Informationen zur Identifizierung dieses Connector-Typs ein.

Automatische Übersetzung

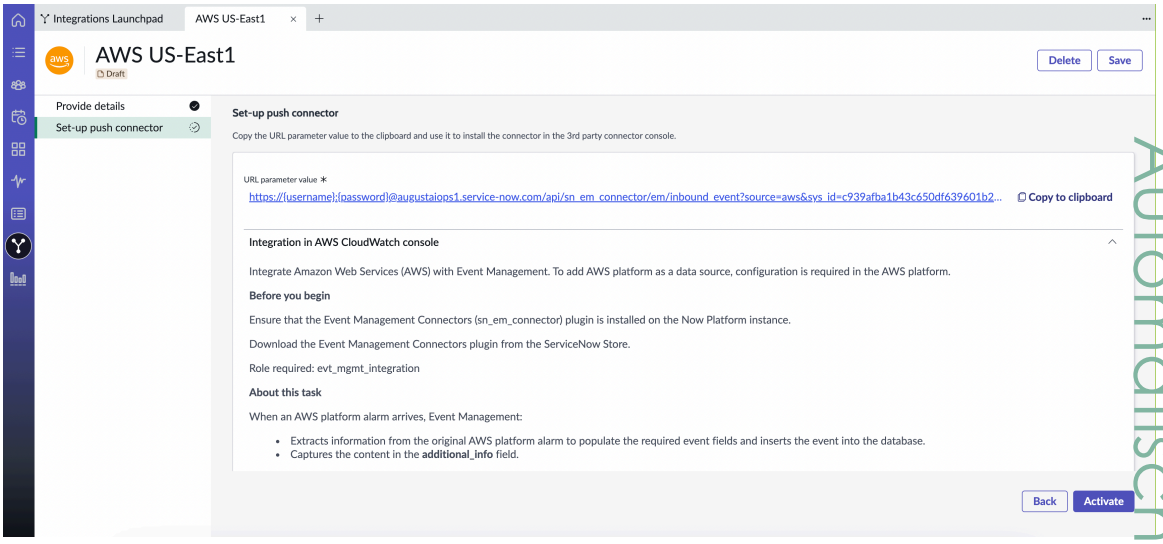
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Stellen Sie sicher, dass der Lieferantenname im Feld **Quelle** korrekt ist.

e. Wahlweise: Wählen Sie in der Dropdown-Liste **Zuweisungsgruppe** die Gruppe oder das Team aus, die bzw. das für die Verwaltung und Wartung des Push-Connectors verantwortlich ist.

f. Wählen Sie **Weiter**.

Der Connector wird im Entwurfsmodus gespeichert, und der Prozess fährt mit dem Abschnitt Push-Connector einrichten fort.



6. Wählen Sie im Feld **URL-ParameterwertIn Zwischenablage kopieren**, um den automatisch generierten URL-Parameterwert in die Zwischenablage zu kopieren.

Diese URL wird von dem Code generiert, der von der Instanz ServiceNow und dem Connector-Typ abhängt, um Ereignisse vom Drittanbieter-Connector zu empfangen. Durch das Einfügen der URL in die Konfiguration des Drittanbieter-Connectors wird ein Webhook erstellt, über den Ereignisse an die Instanz ServiceNow gesendet werden können.

7. Wählen Sie **Aktivieren** und dann **OK**aus.

8. Zeigen Sie auf der Registerkarte **Details** die Connector-Details und den URL-Link an, und befolgen Sie die Schrittanweisungen, um den Connector eines Drittanbieters mit Ereignismanagementzu integrieren.
Der Connector wird gespeichert, und es wird eine Benachrichtigung gesendet, sobald der Connector aktiv ist.

Nächste Maßnahme

Um die erfolgreiche Konfiguration des Pull-Connectors und den Flow von Ereignissen im System zu bestätigen, wechseln Sie zur Registerkarte **Zugehörige Ereignisse**. Wenn das Setup erfolgreich ist, fahren Sie mit **Automatisierung hinzufügen**, um eine Warnungsautomatisierung einzurichten. Einzelheiten zur Registerkarte **Zugehörige Ereignisse** finden Sie unter Überprüfen Sie die Integrations- und Konfigurationsintegrität, Informationen zur Automatisierung von Warnungen finden Sie unter Warnungsautomatisierung in Service Operations-Arbeitsbereich für ITOM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie einen anwenderdefinierten Connector

Authentifizieren Sie Ihren anwenderdefinierten Connector als Datenquelle, um die Übertragung von Ereignisinformationen an die Instanz ServiceNow zu ermöglichen. Definieren Sie den anwenderdefinierten Connector, indem Sie die zugehörigen Details und Zuordnungsfelder angeben. Dadurch können die extrahierten Informationen aus den Ereignisnachrichten Ihres anwenderdefinierten Connectors die erforderlichen Ereignisfelder ausfüllen. Erstellen Sie abschließend eine URL für den anwenderdefinierten Connector-Webhook, und stellen Sie sie bereit.

Vorbereitungen

- Stellen Sie sicher, dass das Plugin Ereignismanagement „ Connectors (sn_em_connector) in der Instanz Now Platform installiert ist. Weitere Informationen finden Sie unter Konfigurieren Sie Ereignismanagement die -Connectors.
- Stellen Sie sicher, dass die Konfigurationselemente für die von Ihrem anwenderdefinierten Connector verwalteten Hosts in der Instanz Now Platform vorhanden sind. Diese CIs können physisch oder virtuell sein und entweder manuell erstellt oder mittels IP-Erkennung oder Cloud-Discovery erkannt werden. Weitere Informationen finden Sie unter Auf Cloud-Umgebungen für ITOM-Produkte zugreifen.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Um mit der Übertragung von Ereignisinformationen an Ihre Instanz ServiceNow zu beginnen, müssen Sie Ihre Instanz Now Platform als REST-Endpunkt mit einem Standard-Webhook in Ihrem anwenderdefinierten Connector festlegen.

Durch die Bereitstellung von Connector-Details und Zuordnungsfeldern definieren Sie den anwenderdefinierten Connector. Die extrahierten Informationen aus den Ereignisnachrichten des anwenderdefinierten Connectors füllen dann die erforderlichen Ereignisfelder aus und fügen das Ereignis in die Datenbank ein.

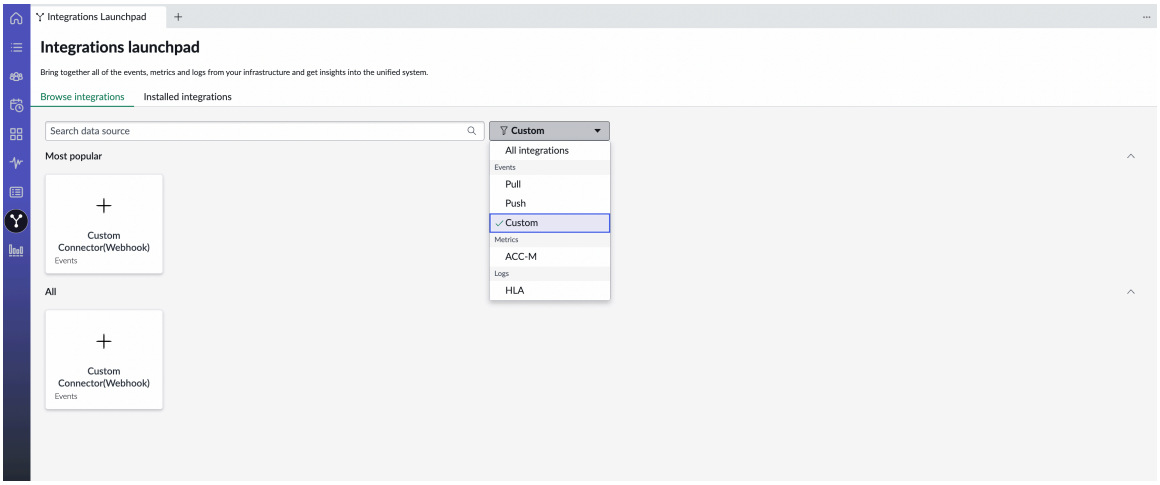
Die URL wird vom Code basierend auf der Instanz ServiceNow und dem anwenderdefinierten Connector generiert. Verwenden Sie diese URL, um einen Webhook zu erstellen, mit dem Ihr anwenderdefinierter Connector Ereignisse an die Instanz ServiceNow senden kann.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Wählen Sie auf der Registerkarte **Integrationen** durchsuchen die Dropdown-Liste **Alle Integrationen** und dann **Anwenderdefiniert**aus.
   Es werden nur anwenderdefinierte Connector-Kacheln angezeigt.

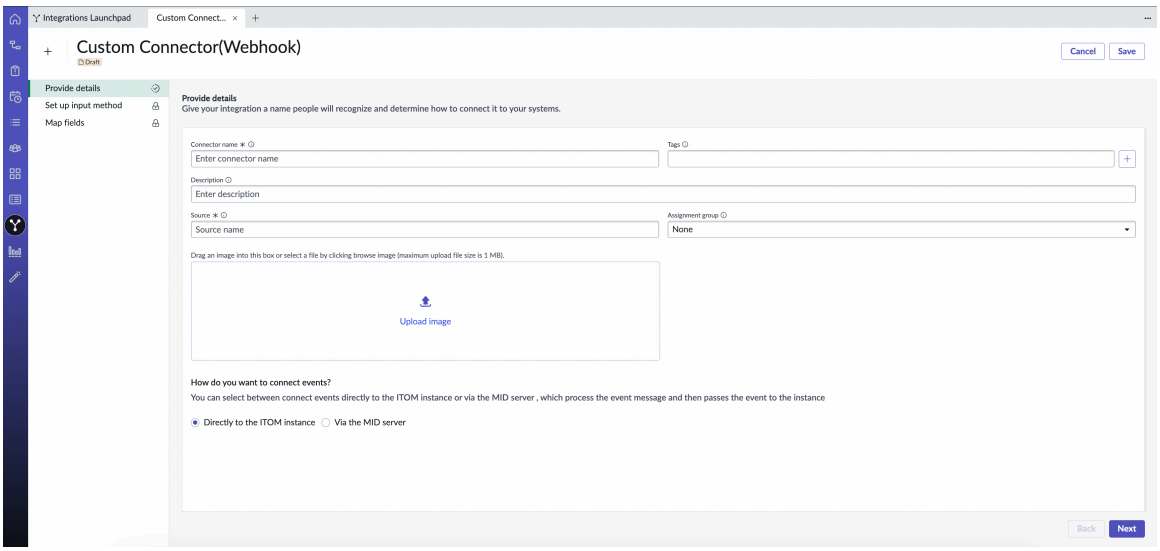
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Push-Connectors



4. Wählen Sie eine Kachel des anwenderdefinierten Connector-Typs aus.
5. Geben Sie auf der Seite **„Details bereitstellen“** die Details für den Connector an.

Detailseite für anwenderdefinierte Connectors



a. Geben Sie im Feld **Connector-Name** einen eindeutigen Integrationsnamen für den Connector ein.

b. Wahlweise: Geben Sie im Feld **Tags** Tags ein, um Connectors dieses Typs auf Express-Listezu finden und zu identifizieren.

   Um zusätzliche Tags hinzuzufügen, wählen Sie das Pluszeichen (+) neben dem Feld **Tags**. Das Fenster „Tags hinzufügen“ wird geöffnet.

   i. Geben Sie im Feld **Schlüssel** einen Tag-Schlüssel ein.

   ii. Geben Sie im Feld **Wert** einen Tag-Wert ein.

   iii. Wählen Sie **Hinzufügen**.

c. Wahlweise: Geben Sie im Feld **Beschreibung** kurze Informationen zu diesem Connector ein.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Geben Sie im Feld **Quelle** den Lieferanten ein, der zum Sammeln von Ereignissen aus der externen Quelle verwendet wird.

Das Feld **Quelle** identifiziert den Connector und dient als Bezeichner, um die Quelle von Ereignissen und Warnungen zu erkennen, sobald der Connector aktiv ist.

e. Wahlweise: Wählen Sie in der Dropdown-Liste **Zuweisungsgruppe** die Gruppe oder das Team aus, die bzw. das für die Verwaltung und Wartung des Connectors verantwortlich ist.

6. Wahlweise: Ziehen Sie ein Bild, oder laden Sie es hoch, um es in Ihrer Connector-Kachel anzuzeigen.

- Ziehen Sie ein Bild in das Feld.
- Navigieren Sie zur Bilddatei, indem Sie **Bild hochladen** auswählen, und wählen Sie dann die Datei aus.

Die maximale Uploadgröße beträgt 1 MB.

7. Legen Sie fest, ob Sie Ereignisse direkt mit der Instanz ITOM oder über eine MID-ServerInstanz verbinden möchten.

- Um Ereignisse direkt an die Instanz ITOM zu senden, wählen Sie **Direkt zur ITOM-Instanz**aus.
- Um Ereignisse über einen MID-Serverzu senden, der das Ereignis verarbeitet und dann an die Instanz übergibt, wählen Sie **Über den MID-Server**aus.

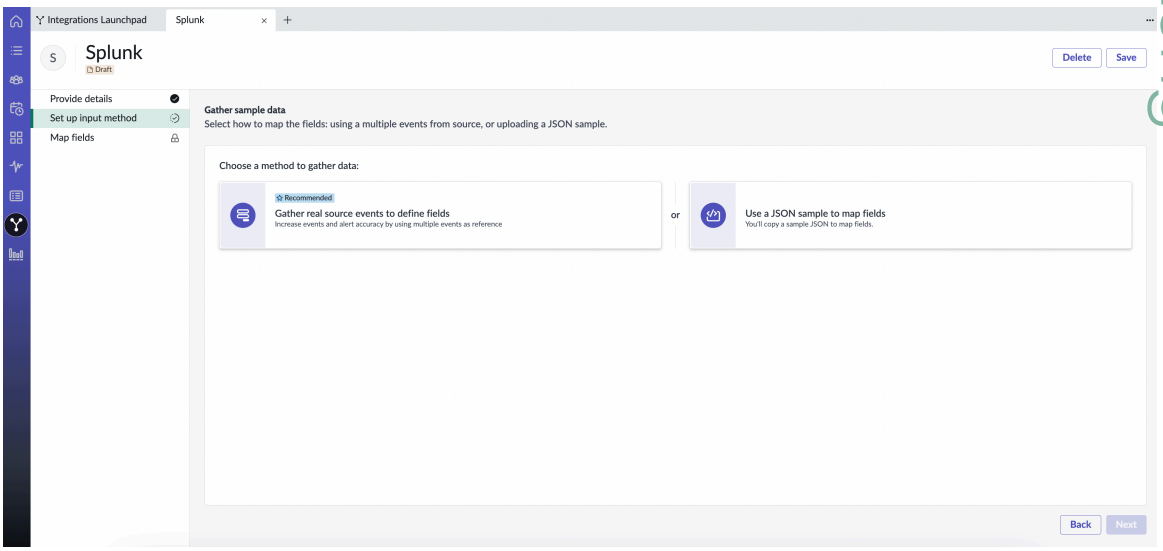
  Wenn ein MID-Server vorhanden ist, wählen Sie im Feld **MID-Server auswählen** einen verfügbaren MID-Server aus, der mit einem Ereignis-Listener verbunden ist.

  Wenn Sie ein MID-Servererstellen müssen, wählen Sie eine der folgenden Optionen aus.

  - **MID-Webservererweiterung konfigurieren**
  - **MID-Webservice-Ereignis konfigurieren – Collector-Kontext**

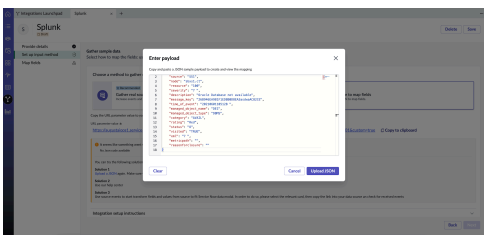
  Weitere Informationen finden Sie unter MID-Webservererweiterung konfigurieren und MID-WebService-Event-Sammlerkontext konfigurieren.

8. Wählen Sie **Weiter**.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

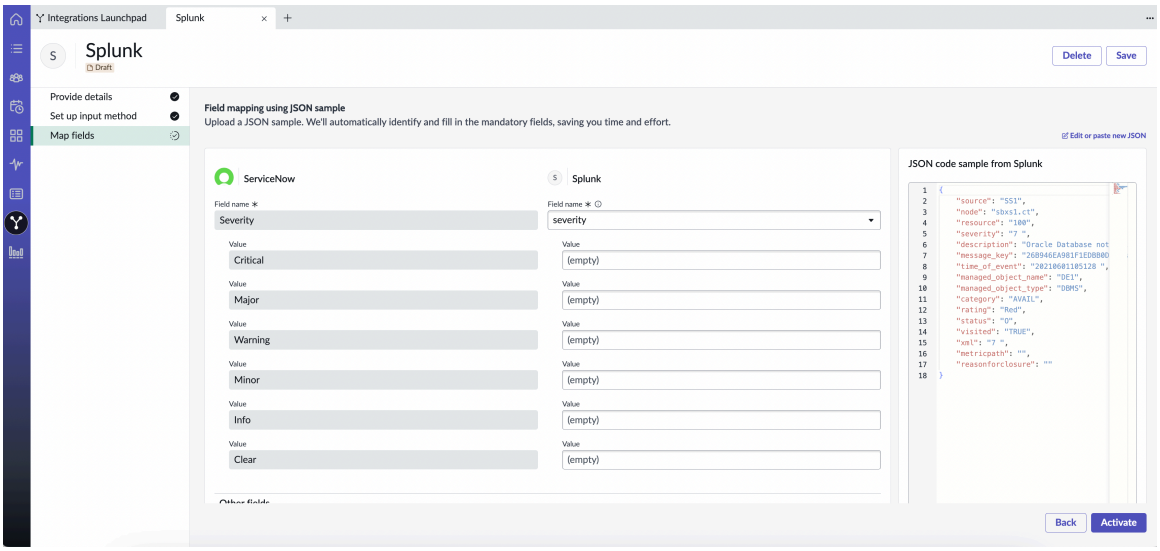
9. Wählen Sie auf der Seite **„Eingabemethode einrichten“** eine Methode zum Sammeln von Ereignisdaten aus.

Methode	Beschreibung
Sammeln Sie echte Quellereignisse, um Felder zu definieren	**a.** Wählen Sie **Echte Quellereignisse sammeln, um Felder zu definieren**. **Hinweis:** Durch das Sammeln von Ereignissen aus echten Quellen von Ihrem anwenderdefinierten Connector erhöhen Sie die Genauigkeit von Ereignissen und Warnungen, indem Sie mehrere Ereignisse als Referenz zum Definieren der Felder verwenden. **b.** Wählen Sie **In Zwischenablage kopieren** und kopieren Sie die URL. **c.** Fügen Sie die URL in das Webhook-Setup Ihres anwenderdefinierten Connectors ein, um einen Webhook zu erstellen, mit dem Ihr anwenderdefinierter Connector Ereignisse an die Instanz ServiceNow senden kann. Geben Sie Ihre Anmeldeinformationen für die Standardauthentifizierung in die Webhook-Konfiguration des Überwachungssystems ein (z. B. Anwendername und Passwort). Mit dem -Webhook kann Ihr anwenderdefinierter Connector Ereignisse an die -Instanz senden. **d.** Wählen Sie **Auf Ereignisse prüfen aus**. Die Anzahl der Ereignisse wird angezeigt. Das Ereignis erstellt JSON-Dateien, die Sie durchsuchen können, nachdem Sie **Weiter**ausgewählt haben.
JSON-Beispiel für die Zuordnung von Feldern verwenden	**a.** Wählen Sie **JSON-Beispiel zum Zuordnen von Feldern verwenden aus**. **Hinweis:** Wählen Sie diese Option nur aus, wenn Sie über ein JSON-Beispiel verfügen. **b.** Kopieren Sie im Dialogfeld **„Payload eingeben“** Ihre JSON-Beispiel-Payload, und fügen Sie sie ein, um die Zuordnung zum Zuordnen der Felder zu erstellen und anzuzeigen.  **c.** Wählen Sie **JSON hochladen**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Methode	Beschreibung
	d. Wählen Sie **Bearbeiten oder neue JSON einfügen** aus, um die hochgeladene JSON zu bearbeiten oder eine neue einzufügen. **e.** Wählen Sie **In Zwischenablage kopieren** und kopieren Sie die URL. **f.** Fügen Sie die URL in das Webhook-Setup Ihres anwenderdefinierten Connectors ein, um einen Webhook zu erstellen, mit dem Ihr anwenderdefinierter Connector Ereignisse an die Instanz ServiceNow senden kann. Geben Sie Ihre Anmeldeinformationen für die Standardauthentifizierung in die Webhook-Konfiguration des Überwachungssystems ein (z. B. Anwendername und Passwort). Mit dem -Webhook kann Ihr anwenderdefinierter Connector Ereignisse an die -Instanz senden.

10. Wählen Sie **Weiter**.
    Die Seite wird geöffnet, auf der Sie Felder zuordnen können.



11. Geben Sie auf der Seite **„Felder zuordnen** " in der Spalte mit den Connector-Feldnamen mindestens einen Wert ein, der den Schweregradwerten entspricht, die in der Spalte „ ServiceNow **Schweregradfeld** " aufgeführt sind.
12. Geben Sie auf der Seite **„Felder zuordnen** " in der Spalte mit den Connector-Feldnamen mindestens einen Wert ein, der den Schweregradwerten entspricht, die in der Spalte „ ServiceNow **Schweregradfeld** " aufgeführt sind.

    Sie können den Schweregradwert aus dem JSON-Codebeispiel eingeben. Um einen Schweregradwert festzulegen, müssen Sie mit der Nutzlast Ihres anwenderdefinierten Connectors und den von ihm unterstützten Schweregradtypen vertraut sein. Die Schweregradwerte der empfangenen Ereignisse müssen mit den generierten Ereignissen in Ihrem System übereinstimmen.

    Aktivieren Sie das System, um Ereignisse aus eingehenden Daten korrekt zu erstellen, indem Sie die Felder in Ihrem JSON-Codebeispiel den Feldern ServiceNow zuordnen. Die Informationen **zum Schweregrad** und **zum Nachrichtenschlüssel** werden automatisch

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ausgefüllt, um Ihnen Zeit und Aufwand zu sparen. Der **Nachrichtenschlüssel** stellt den richtigen Bezeichner für die Ereignisse bereit, um sicherzustellen, dass die Deduplizierung ordnungsgemäß funktioniert und keine redundanten Warnungen generiert werden.

13. Wahlweise: Um mehrere JSON-Dateien anzuzeigen, wählen Sie den Pfeil über dem JSON-Beispiel.
14. Wahlweise: Geben Sie im Abschnitt Andere Felder in der Spalte Ihr Connector anwenderdefinierte Ereignisparameter an, die optional sind, aber zusätzliche Informationen zum Ereignis liefern.
    Wenn Sie die optionalen Informationen nicht angeben, lassen Sie das Feld leer.

    a. Geben Sie im Feld **Beschreibung** eine aussagekräftige Warnungsbeschreibung ein.

    b. Geben Sie im Feld **Metrikname** einen Metriknamen ein, mit dem Sie Ereignisse den Leistungsmetriken oder KPIs zuordnen können, die die Warnung ausgelöst haben.

    c. Geben Sie im Feld **Knoten** einen Knotenwert ein, der für die CI-Bindung verwendet werden soll.

    d. Geben Sie im Feld **Ereigniszeit** die Erstellungszeit des Ereignisses des anwenderdefinierten Connectors ein.
    Wenn die Ereigniszeit nicht zugeordnet ist, verwendet das System die Standardereigniszeit.

    e. Wählen Sie im Feld **Einstellungen für Ereigniszeit** das Zeitformat und die Zeitzone des Ereignisse aus.
    - **Zeitformat**: Ein GlideDateTime-Feld im UTC- oder GMT-Format mit einer maximalen Länge von 40 Zeichen.
    - **Zeitzone**: Zeiten werden in Coordinated Universal Time (UTC) gespeichert und basierend auf der Systemzeitzone global angezeigt.

15. Aktivieren und speichern Sie den Connector, indem Sie **Aktivieren** und dann im Bestätigungs-Popup-Fenster **OK** auswählen.
    Sie können die Connector-Details auf der Registerkarte **Details** und Ihre Feldzuordnungen auf der **Registerkarte Feldzuordnung** anzeigen.

Ergebnisse

Nachdem der -Connector aktiviert wurde, beginnen Ereignisse von Ihrer anwenderdefinierten Connector-Konsole in die Instanz ServiceNow zu fließen. Das Plugin extrahiert Informationen aus der ursprünglichen Ereignisnachricht des anwenderdefinierten Connectors, um die erforderlichen Ereignisfelder auszufüllen, und fügt das Ereignis in die Datenbank ein. Um die Ereignisse in Ihrer Instanz Now Platform anzuzeigen, navigieren Sie zu Alle Ereignisse. Weitere Informationen finden Sie unter Events anzeigen.

Nächste Maßnahme

Um zu überprüfen, ob der Prozess erfolgreich abgeschlossen wurde und Ereignisse in das System fließen, zeigen Sie die zugehörigen Ereignisse auf der Registerkarte **Zugehörige Ereignisse** an. Wenn das Setup erfolgreich ist, fahren Sie mit **Automatisierung hinzufügen**, um eine Warnungsautomatisierung einzurichten. Informationen zur Warnungsautomatisierung finden Sie unter Warnungsautomatisierung in Service Operations-Arbeitsbereich für ITOM.

Überprüfen Sie die Integrations- und Konfigurationsintegrität

Überprüfen Sie Ihre Ereignisse, um sicherzustellen, dass Warnungen wie beabsichtigt erstellt werden. Starten Sie diesen Prozess, indem Sie den Integritätsstatus Ihrer Integration

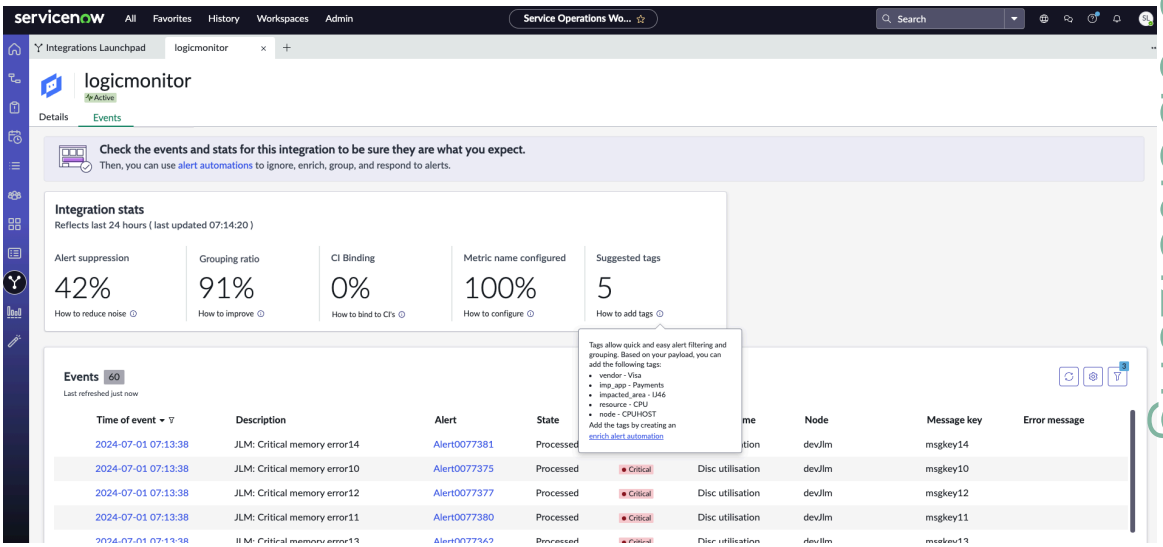
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

überprüfen. Dies stellt nützliche Statistiken bereit, um hervorzuheben, wo Sie Verbesserungen vornehmen können, um Warnungen mit relevantem Geschäftskontext anzureichern, sie zur besseren Reduzierung des Datenrauschens zu gruppieren, kritische Warnungen umgehend zu eskalieren und Ihr Team zu benachrichtigen, damit eine schnelle Reaktion und Lösung erreicht ist.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Integritätsstatusmetriken geben an, wie effektiv Warnungsautomatisierungen Kontext hinzufügen und Rauschen reduzieren, was den Betreibern hilft, die durchschnittliche Zeit bis zur Reparatur (MTTR) zu verkürzen. Wenn Sie eine neue Integration hinzufügen, überprüfen Sie diese Metriken, bewerten Sie die Raten, und entwickeln Sie neue Regeln, um die Reduzierung des Datenrauschens und die allgemeine Systemleistung zu verbessern.

Prozedur
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Wählen Sie auf der Registerkarte **Integrationen** durchsuchen die Dropdown-Liste **Alle Integrationen** und dann nach Bedarf **Abrufen** oder **Push** aus.
4. Wählen Sie eine Pull-, Push- oder anwenderdefinierte Kachel des Connector-Typs aus. Wenn sich ein Popup-Menü öffnet, wählen Sie die Daten aus, die von diesem Connector nachverfolgt werden sollen, und wählen Sie **Fortsetzen**aus.
5. Wählen Sie die Registerkarte **Zugehörige Ereignisse**.



6. Zeigen Sie im Abschnitt „Health state“ (Integritätsstatus) die Daten für Warnungen und die zugehörigen Attribute an.

Warnungsattribute

Warnungsattribut	Beschreibung
Warnungsunterdrückung	Das Unterdrückungsverhältnis gibt den Anteil der erstellten Warnungen im Vergleich zu den empfangenen Ereignissen an. Die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsattribut	Beschreibung
	Reduzierung unerwünschter Warnungen kann durch Deduplizieren oder Ignorieren erreicht werden. ◦ Deduplizierung: Das Feld **„message_key“** ist ein eindeutiger Bezeichner für eine Warnung im Quellüberwachungssystem. Sie dienen der Deduplizierung und der Erkennung von Fluktuationen bei Warnungen. Wenn das Quellereignis keine zuverlässigen eindeutigen Werte bereitstellt, können Sie den Standardwert verwenden oder einen eigenen erstellen. Wenn der Nachrichtenschlüssel nicht definiert ist, lautet der Standardnachrichtenschlüssel <Source + Node + Type + Resource + Metric Name>. Die Richtlinie sieht vor, dass die Ereignisquelle die Felder <Source + Node + Type + Resource + Metric Name> automatisch ausfüllt und den Nachrichtenschlüssel generiert. Diese Praxis ermöglicht eine bessere Verteilung der Ereignisverarbeitung auf Instanz-Worker und Knoten. Wenn das Quellereignis keine Werte für diese Felder bereitstellt, stellen Sie sicher, dass sie mithilfe von Transformationsregeln ausgefüllt werden. Diese Aktion, die sich nicht auf die Ereignisverarbeitung auswirkt, ist für die Deduplizierung wichtig. Füllen Sie so viele dieser Felder wie möglich aus, bevor Sie das Ereignis an die Instanz senden. Dadurch werden die Verteilung von Ereignissen auf die Prozessor-Worker verbessert, was Durchsatz und Skalierbarkeit verbessert. Weitere Informationen zur Deduplizierung finden Sie unter Ereignismanagement-Konfigurationspräferenzen. Informationen zum Festlegen des Nachrichtenschlüssels in Ihrer anwenderdefinierten Connector-Integration finden Sie unter Konfigurieren Sie einen anwenderdefinierten Connector. ◦ Warnungsereignisregeln ignorieren: Filtern Sie Warnungen von niedriger Qualität heraus, indem Sie eine Automatisierung zum Ignorierenerstellen.
Warnungs-Komprimierungsrate	Wenn Sie Warnungen gruppieren, ist eine hohe Komprimierungsrate wünschenswert, da dadurch weniger Warnungen verbleiben, die Ihr Betriebsteam überprüfen und bearbeiten muss. Dies kann die Effizienz des Teams verbessern. Die Komprimierungsrate wird berechnet als 1 – (Anzahl der Warnungsgruppen + Anzahl der nicht gruppierten Warnungen)/ Gesamtzahl der Warnungen. Weitere Informationen zur Warnungszusammenfassung finden Sie unter Warnungsgruppierung. Eine Möglichkeit, die Komprimierungsrate von Warnungen zu verbessern, ist die Definition einer neuen Gruppierungsautomatisierung.
CI-Bindung	Der Prozentsatz der Warnungen, die erfolgreich an ein Configuration Item (CI) in Ihrer CMDB gebunden wurden, ist entscheidend. Zielen Sie darauf ab, dass diese Zahl bei oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsattribut	Beschreibung
	nahe 100 % liegt, um die Gruppierung von Warnungen, die Ursachenanalyse, die Zuweisung und vieles mehr zu verbessern. Um einen Host, einen Computer oder ein beliebiges Gerät mit einer IP zu binden, füllen Sie das Feld **Knoten** mit einem eindeutigen Hostnamen, FQDN, IP oder MAC-Adresse aus. Dies kann innerhalb der Integration selbst oder durch Erstellen einer ergänzenden Automatisierung erfolgen. Bei komplexeren Szenarien können Sie die knotenbasierte Bindung mithilfe von Ereignisregeln überschreiben. Weitere Informationen zur CI-Bindung finden Sie unter Warnungen an CIs binden.
Metrikname wurde konfiguriert	Zeigt den Prozentsatz der Warnungen an, für die ein Metrikname definiert ist. Es ist wichtig, nahe 100 % anzustreben, da dies standardmäßig in unserem automatisierten Korrelationsalgorithmus verwendet wird. Dies kann innerhalb der Integration selbst oder durch Erstellen einer ergänzenden Automatisierungerreicht werden.
Vorgeschlagene Tags	Stellt vorgeschlagene Warnungs-Tags basierend auf der Integrationsnutzlast bereit. Warnungstags sind strukturierte Felder, die Sie definieren können, um das Filtern und Gruppieren von Warnungen zu erleichtern. Die Tags werden in *sn_itom_integ_app_recommendation_tags_suggestion*gespeichert, und nur die fünf beliebtesten Tags werden angezeigt. Wenn Sie die Ergebnisse des Vorschlagsmechanismus verfeinern möchten, können Sie die Eigenschaft *sn_itom_integ_app.evt_mgmt_tag_suggestion_ignore_keys*verwenden, die eine Liste von Feldnamen oder Stichwörtern in Kleinbuchstaben anzeigt, die durch Kommas getrennt sind und beim Scannen zusätzlicher Warnungsinformationen nach Tag-Vorschlägen ignoriert werden sollen. Der Standardwert ist „Zeit“.

7. Stellen Sie im Abschnitt Ereignisse sicher, dass Ihre Ereignisse wie erwartet Warnungen generieren.

   Stellen Sie sicher, dass Warnungsfelder und Tags ordnungsgemäß ausgefüllt sind, damit die Warnungen in Express-Listeleichter gelesen und gefiltert werden können. Vergewissern Sie sich, dass die Schweregradwerte den Erwartungen Ihres Betriebsteams entsprechen und dass Felder und Tags zur leichteren Gruppierung in allen Quellen einem standardisierten Format entsprechen.

   Durch die Überprüfung der Warnungsgenerierung können Sie sicher sein, dass Ihr System ordnungsgemäß konfiguriert ist, um beachtenswerte Vorkommnisse zu erkennen und Sie darüber zu benachrichtigen. Informationen zu den Feldern im Abschnitt „Ereignisse“ finden Sie unter Felder für Integritätsereignisse für Integration und Konfiguration.

Nächste Maßnahme

Nachdem Sie nun Warnungen von den Ereignissen bestätigt haben, können Sie den Warnungsautomatisierungsprozess initiieren, indem Sie **Automatisierung hinzufügen**auswählen. Sie gelangen zum Automatisierungsschritt „Ignorieren“, in dem Sie irrelevante oder falsch positive Warnungen ignorieren können. Fahren Sie anschließend mit dem Anreichern, Gruppieren und Automatisieren von Antworten fort. Dieser Prozess umfasst

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

das Transformieren von Rohwarnungen in ein für ServiceNowverständliches Format, das Gruppieren der Warnungen und das Eskalieren von Warnungen, um eine sofortige Antwort vom entsprechenden Team oder der entsprechenden Person zu gewährleisten. Weitere Informationen zur Warnungsautomatisierung finden Sie unter Warnungsautomatisierung in Service Operations-Arbeitsbereich für ITOM.

Aktivieren Sie die Integration

Durch das Aktivieren der Integration können Sie eine zuvor deaktivierte Connector-Integration aktivieren und ihre Funktionalität wiederherstellen. Mit dieser Funktion können Sie Daten-Flows und Integrationsaktivitäten nahtlos fortsetzen und so Kontinuität und effizientes Ereignismanagement sicherstellen, ohne die Integration neu konfigurieren zu müssen.

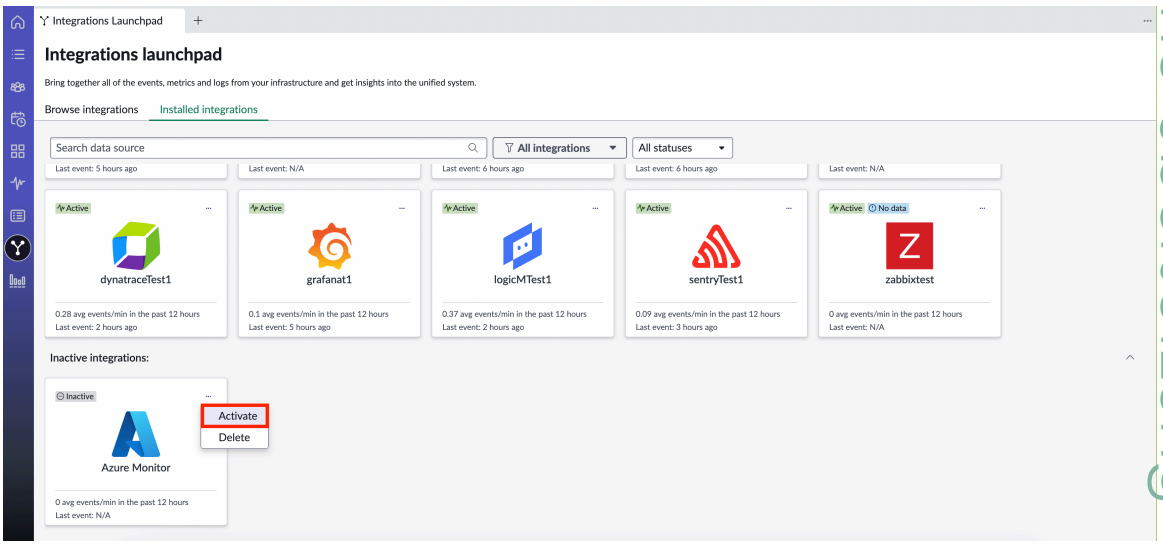
Vorbereitungen

Stellen Sie sicher, dass die Integration deaktiviert ist.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Wählen Sie die Registerkarte **Installierte Integrationen**.
4. Wählen Sie für die Integration, die Sie aktivieren möchten, das Symbol mit den Ellipsen (•••) und dann **Aktivieren**aus.



Die ausgewählte Integration ist aktiviert, und ihr Status wird auf der Installationskachel als **Aktiv** angezeigt.

Integration deaktivieren

Integration deaktivieren ermöglicht es Ihnen, eine aktive Connector-Integration vorübergehend zu deaktivieren, ohne sie zu löschen. Mit dieser Funktion können Sie Integrationen effektiver verwalten, indem der Datenfluss bei Bedarf angehalten, unnötige Ereignisverarbeitungen reduziert und die Systemleistung verbessert wird.

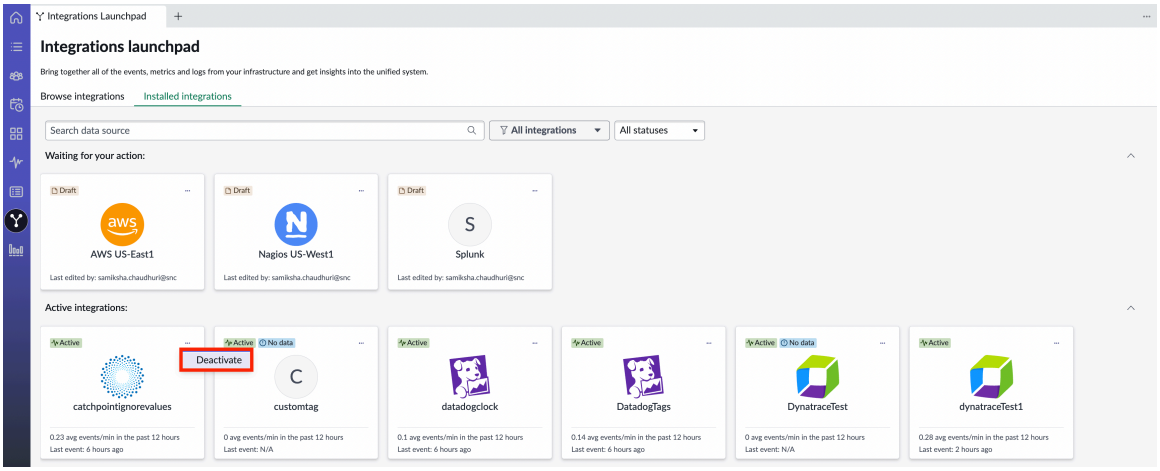
Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Wählen Sie die Registerkarte **Installierte Integrationen**.
4. Wählen Sie für die Integration, die Sie deaktivieren möchten, das Symbol mit den Ellipsen (•••) und dann **Deaktivieren**aus.



Die ausgewählte Integration ist deaktiviert, und ihr Status wird auf der Installationskachel als **Inaktiv** angezeigt.

Löschen Sie die Integration

Integration löschen ermöglicht es Ihnen, eine Connector-Integration dauerhaft aus Ihrem System zu entfernen. Diese Funktion hilft Ihnen, ein übersichtliches und organisiertes System zu gewährleisten, indem sie nicht verwendete oder veraltete Integrationen entfernt, Ressourcen freisetzt und potenzielle Übersichtlichkeit reduziert.

Vorbereitungen

Stellen Sie sicher, dass die Integration deaktiviert ist.

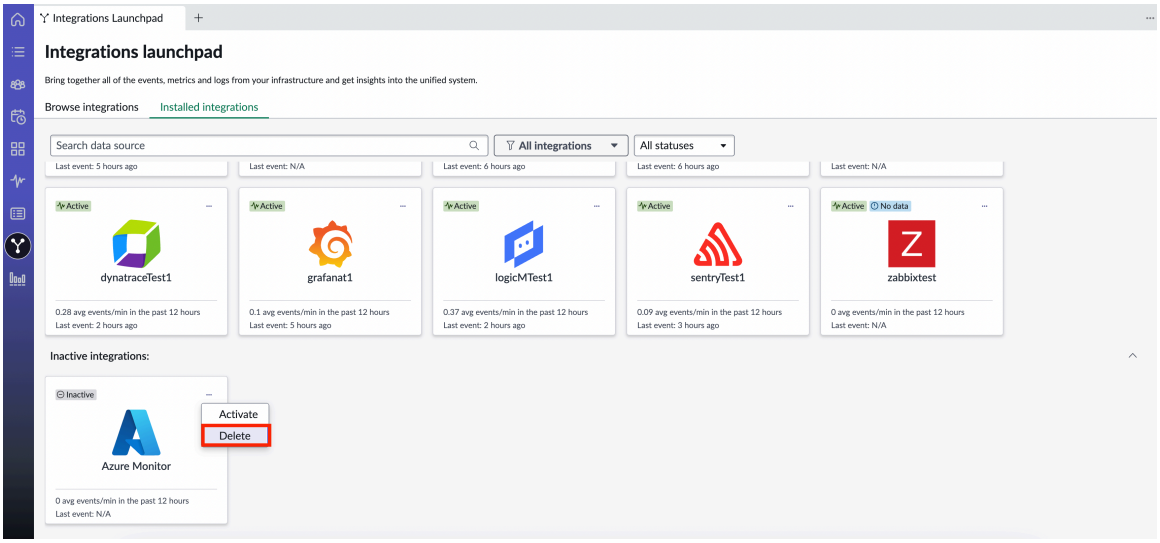
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie im linken Bereich das Integrations-Launchpad-Symbol ( )
3. Wählen Sie die Registerkarte **Installierte Integrationen**.
4. Wählen Sie für die Integration, die Sie löschen möchten, das Symbol mit den Ellipsen (•••) und dann **Löschen aus**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie im Bestätigungsfenster **Löschen**.
   Die Integration wird gelöscht.

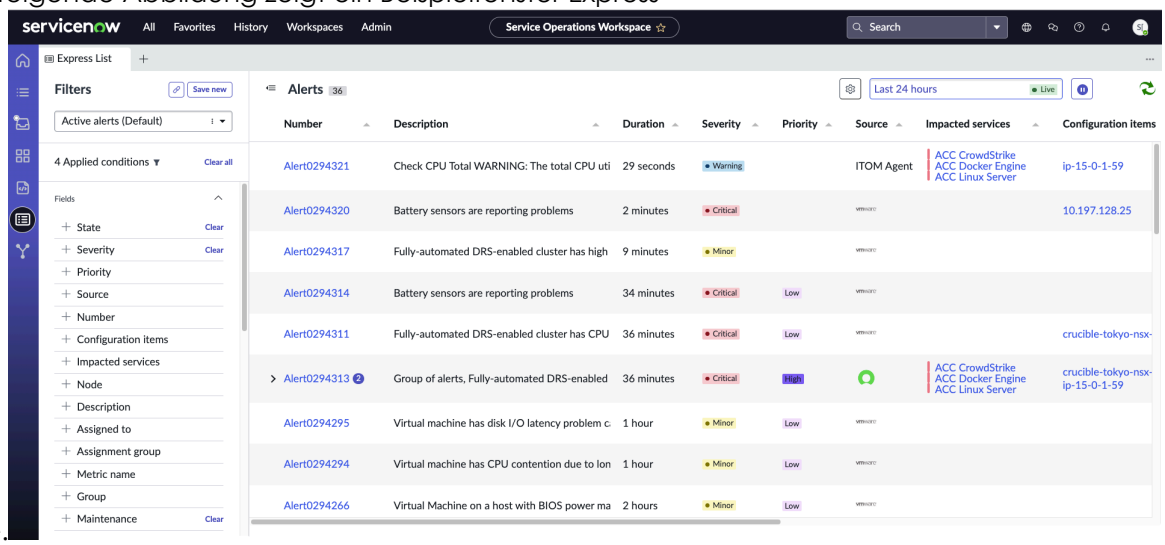
Express-Liste in Service Operations-Arbeitsbereich für ITOM

Mit der Funktion ServiceNow Ereignismanagement Express-Liste können Sie Integritätsprobleme im gesamten Rechenzentrum für Service Operations-Arbeitsbereichidentifizieren. Enthält eine Liste mit Kurzinformationen zu Warnungen, mit denen Sie Systeme und Services effizienter überwachen, Warnungen lösen, die Auswirkungen auf Warnungen bewerten, Probleme nachverfolgen und Incidents melden können.

Einführung in Ereignismanagement Express-Liste

Die sortierbare Warnungsliste im Bereich Express-Liste reduziert die Anzahl der Klicks, die für den Zugriff auf Warnungsinformationen erforderlich sind. Wenn Sie das Kontrollkästchen einer Warnung aktivieren, wird ein Vorschaubereich geöffnet, in dem Sie Daten anzeigen können, die bei der Priorisierung, der Erfolgsrealisierung und der Ursachenanalyse helfen. Sie können den Bereich Express-Liste einfach ändern, um die Anzeige mithilfe einer bereitgestellten Feldliste einzugrenzen, zusätzliche Warnungsinformationen anzuzeigen und übereinstimmende Warnungen herauszufiltern oder anzuzeigen. Sie können auch den angezeigten Zeitbereich ändern.

Die folgende Abbildung zeigt ein Beispielfenster Express-Liste.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Express-Liste – Vorteile

Im Bereich Express-Liste können Operatoren die folgenden Aktionen effizienter ausführen:

- **Überwachungssysteme oder Anwendungsservices** Überwachung der Leistung und Fähigkeit von Computersystemen, um etwaige Diskrepanzen zu erkennen.
- **Warnungen lösen**. Sie arbeiten an Diskrepanzen, um Probleme zu beheben und das effiziente Funktionieren der IT-Infrastruktur zu fördern.
- **Probleme nachverfolgen**. Nachverfolgung und Dokumentation von Fehlern und Lösungen im Detail sowie Meldung von Incidents.
- **Melden von Incidents**. Eskalation komplexer Probleme an die Führungsebene, andere IT-Ressourcen, Drittparteien oder Lieferanten.

Warnungsinformationen, die im Vorschaubereich Express-Liste angezeigt werden

Im Vorschaubereich Express-Liste werden im Bereich Express-Liste zusätzliche Warnungsinformationen angezeigt. Mit diesen Informationen können Sie eine Bewertung durchführen, die zur Lösung von Incidents beiträgt, ohne mehrere Warnungsformulare öffnen zu müssen.

Auf der Registerkarte **Info** im Vorschaubereich werden die folgenden Informationen für eine ausgewählte Warnung angezeigt:

- Warnungsnummer (Link)
- Status
- Dauer
- Konfigurationselemente (mit Links)
- Metrikname
- Knoten
- Ressource
- Quelle
- Zugewiesen an
- Zuweisungsgruppe
- Letztes Update
- Betroffene Services

  Weitere Informationen finden Sie unter Zeigen Sie Daten zu betroffenen Services im Vorschaubereich in an Express-Liste.

- Zusätzliche Information
- Anwenderdefiniertes Feld

Sie können zusätzliche Warnungsinformationen anzeigen, indem Sie eines der verknüpften Elemente auswählen.

Auf der Registerkarte **Warnungen in Gruppe** im Vorschaubereich werden Warnungsinformationen für eine ausgewählte Warnmeldungsgruppe angezeigt. Informationen für jede Warnung werden in einer Kachel mit zusätzlichen Optionen für jede Warnung in der Gruppe angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Jede Kachel zeigt die folgenden Warnungsinformationen an:

- Warnungsnummer (Link)
- Status
- Schweregrad
- Konfigurationselemente
- Dauer
- Metrikname

Durch Anpassen des Zeitbereichs der Warnungsanzeige

Sie können den Zeitbereich der angezeigten Warnungen bestimmen. Der Standardzeitbereich sind die letzten 24 Stunden. Die Liste wird mit neuen Warnungen aktualisiert, bis Sie das Pausierungssymbol ( ) wählen. Wenn Sie die aktuelle Bereichseinstellung oben rechts auswählen, wird ein Dialogfeld mit Optionen für Datums- und Uhrzeitbereiche angezeigt:

- Gesamte Zeit: Die letzten 90 Tage
- Letzte 24 Stunden
- Letzte Woche
- Letzte 12 Stunden
- Letzte Stunde
- Letzte 15 Minuten
- Anwenderdefiniert: Ermöglicht die Auswahl eines Datums- und Uhrzeitbereichs aus dem Popup-Kalender.

Zugehörige Informationen

Von verwendete Rollen Express-Liste

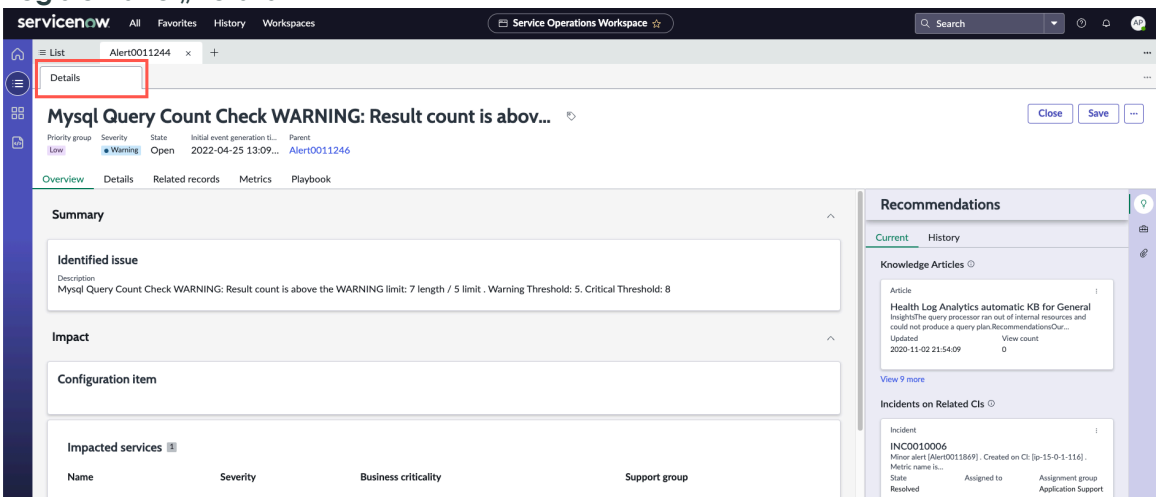
Warnungen in Service Operations-Arbeitsbereich

Auf der Benutzeroberfläche von Service Operations-Arbeitsbereich wird eine Warnungsliste mit weiteren Details zu bestimmten Warnungen angezeigt.

Wenn Sie in der Warnungsliste auf eine Warnung klicken, wird die Registerkarte **Details** der ausgewählten Warnung angezeigt, und im Warnungstitel wird das Problem angezeigt, das die Warnung verursacht hat (das identifizierte Problem). Auf der resultierenden Seite werden nur die für die Warnung relevanten Unterregisterkarten angezeigt. Beispielsweise wird die Option **Warnungen in Gruppe** nur für Warnungsgruppen auf der Registerkarte **Zugehörige Datensätze** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Details“



In der folgenden Tabelle werden die Bereiche im Warnungsformular beschrieben.

Bereiche im Warnungsformular

Funktion	Beschreibung
Kopfzeile	Der Header enthält die folgenden Details: • Beschreibung: Der Text aus dem Feld **Beschreibung** der Warnung wird angezeigt. • Prioritätsgruppe: Die Prioritätsgruppe, zu der die Warnung gehört. • Schweregrad: Der Schweregrad der Warnung. • Status: Der Status der Warnung. • Generierungszeit des ersten Events: Datum und Uhrzeit der Generierung des ersten Ereignisses. • Übergeordnet: Die primäre Warnung in der Gruppe (nur relevant für untergeordnete Warnungen in einer Gruppe). • Gruppe: Gruppentyp, zu dem die Warnung gehört (nur relevant für Warnungen in einer Gruppe). • Aufgabe: Nummer des Incidents, dem die Warnung zugeordnet ist. Die angezeigten Informationen variieren je nach Warnungstyp.
Registerkarte Übersicht	Wenn Sie eine Warnung mit zugewiesenem CI anzeigen, wird diese Registerkarte beim Auswählen der Warnung geöffnet. Die angezeigten Informationen variieren je nach Typ der Warnung (gruppiert, sekundär oder primär). Wenn Sie die App Health Log Analytics installiert haben, gehören Health Log Analytics-Warnungen und komponentenbasierte Warnungen zu den Warnungstypen.

Weisen Sie Warnungen in zu Express-Liste

Weisen Sie Warnungen in Express-Liste sich selbst, einer anderen Person oder einer Zuweisungsgruppe zu, um die Arbeitslast Ihres Unternehmens zu verteilen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

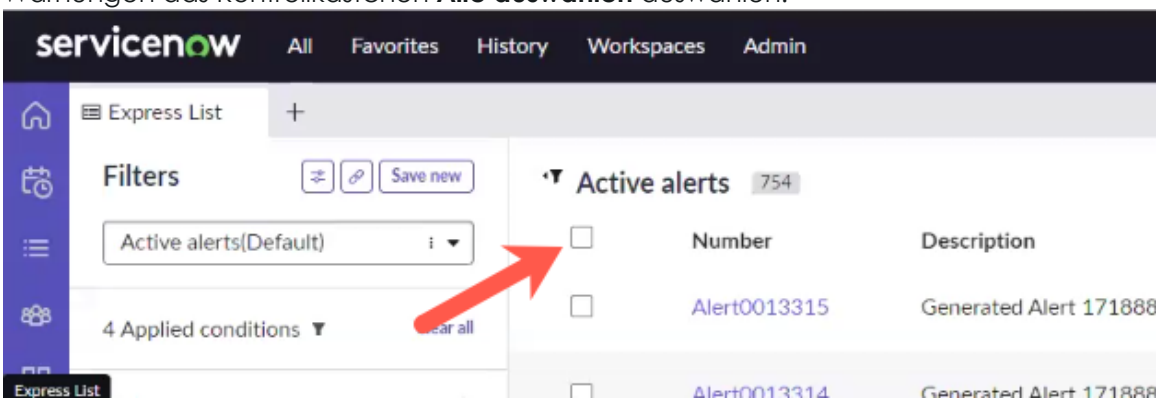
Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

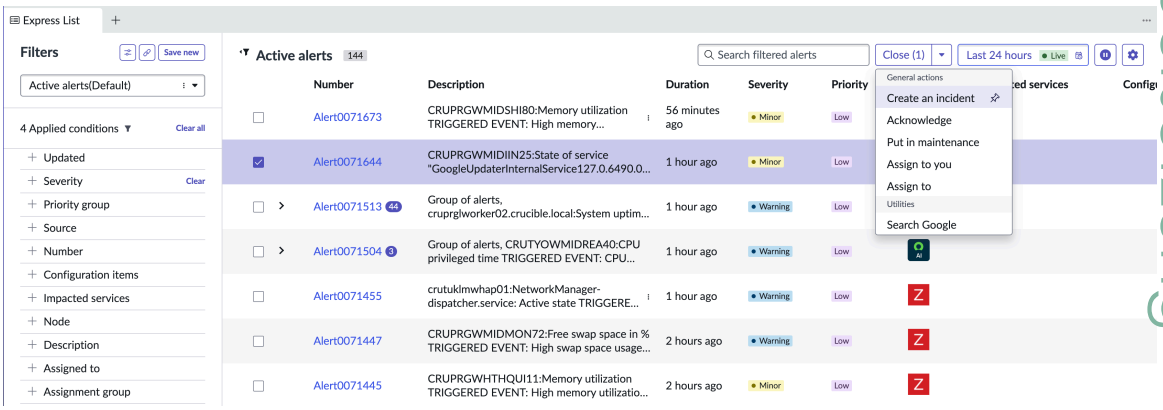
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Aktivieren Sie das Kontrollkästchen neben der Warnungsnummer, die Sie zuweisen möchten.

   Hinweis: Sie können die Aktion für bis zu 1.000 Warnungen gleichzeitig ausführen, indem Sie in der Liste Aktive Warnungen das Kontrollkästchen **Alle auswählen** auswählen.



4. Wählen Sie die Dropdown-Liste **Schließen aus**.



5. Führen Sie eine der folgenden Aktionen aus.

Zuweisung	Aktionen
Sie selbst	Wählen Sie **Ihnen zuweisen** und dann **OK-** aus.
Jemand anderes	**a.** Wählen Sie **Zuweisen an aus**. **b.** Wählen Sie im Feld **Zugewiesen** an den Namen der Person aus, der Sie die Warnung zuweisen möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zuweisung	Aktionen
	c. (Optional) Geben Sie im Feld **Arbeitsnotizen** Informationen zur Zuweisung oder Warnung ein. **d.** Wählen Sie **Zuweisen** aus<number> Schaltfläche „ Warnungen “.
Zuweisungsgruppe	**a.** Wählen Sie **Zuweisen an aus**. **b.** Wählen Sie den Namen der Gruppe im Feld **Zuweisungsgruppe** aus. **c.** Wählen Sie im Feld **Zugewiesen** an den Namen der Person aus, der Sie die Warnung zuweisen möchten. **d.** (Optional) Geben Sie im Feld **Arbeitsnotizen** Informationen zur Zuweisung oder Warnung ein. **e.** Wählen Sie **Zuweisen** aus<number> Schaltfläche „ Warnungen “.

Ergebnisse

Die zugewiesene Person wird in der Spalte **Zugewiesen an** angezeigt, und die Zuweisungsgruppe wird in der Spalte **Zuweisungsgruppe** im Bereich Express-Liste angezeigt.

Express-Liste-Tastenkürzel

Verwenden Sie Tastenkombinationen, um häufige Aktionen in Express-Listeschnell auszuführen.

Navigationsverknüpfungen

Aktion	Tastenkombination
Zur vorherigen/nächsten Zeile wechseln	Pfeil nach oben/unten
Fokus nach vorn zwischen anklickbaren Elementen verschieben	Tab-Taste
Verschiebt den Fokus zwischen anklickbaren Elementen zurück	Umschalt + Tabulatortaste

Aktionsverknüpfungen

Aktion	Tastenkombination
Öffnen Sie einen Warnungsdatensatz	Wahltaste/Alt + R
Bestätigen Sie eine Warnung	Wahltaste/Alt + K
Weisen Sie sich selbst eine Warnung zu	Wahltaste/Alt + Y
Warnungen schließen	Wahltaste/Alt + X
Incident erstellen	Wahltaste/Alt + I
Freitextsuche	Wahltaste/Alt + S
Live-Aktualisierungen anhalten/neu starten	Wahltaste/Alt + L

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktionsverknüpfungen (Fortsetzung)

Aktion	Tastenkombination
Vorschaubereich öffnen/schließen	Eingabe

Auswahlverknüpfungen

Aktion	Tastenkombination
Erweitern/reduzieren Sie eine ausgewählte Gruppe von Warnungen	Platz
Wählen Sie mehrere nebeneinander liegende Warnungszeilen aus	Umschalt + Pfeiltaste nach oben/unten
Wählen Sie mehrere separate Warnungszeilen aus	Befehlstaste/Steuerung + Pfeiltaste nach oben/unten
Aktivieren Sie einen ausgewählten Link oder eine ausgewählte Schaltfläche	Eingabe

Hinweis: Die Informationen in diesem Abschnitt sind auch als produktinterne Hilfe im Bereich Hilfe-Center für Express-Listeverfügbar.

Verwenden Sie eine zugewiesene Express-Liste Ansicht

Arbeiten Sie mit einer Ansicht Express-Liste, die Ihnen von Ihrem Administrator Ereignismanagement zugewiesen wurde, um sicherzustellen, dass Sie sich auf bestimmte Services, Prioritäten oder Warnungen konzentrieren.

Vorbereitungen

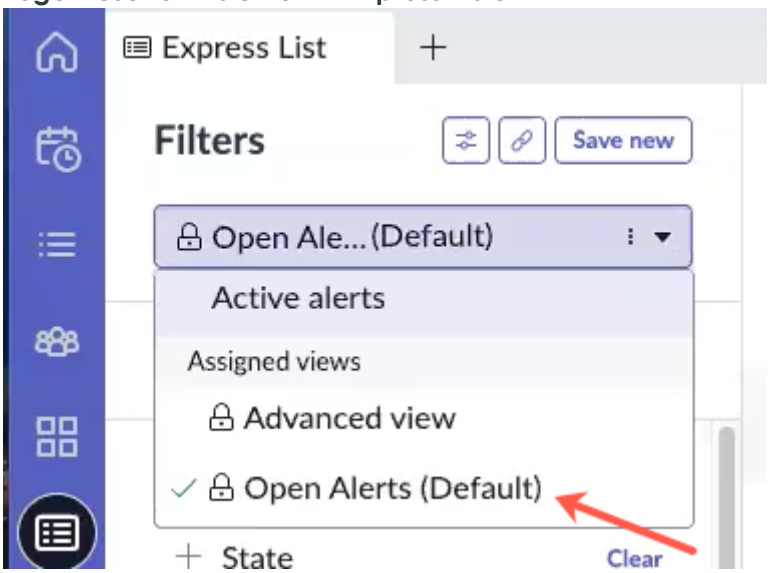
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Wählen Sie in der Dropdown-Liste im Bereich Filter eine Ansicht Express-Liste aus, die Ihnen zugewiesen wurde.
   Ihre Standardansicht ist als Standard markiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugewiesene Ansichten in Express-Liste



Hinweis: Der Administrator Ereignismanagement hat Ihnen möglicherweise mehr als eine Ansicht zugewiesen. Sie können zwischen Ihren Ansichten wechseln und Ansichten ändern und speichern, die nicht Ihre Standardansicht sind. Sie können Ihre Standardansicht nicht ändern oder freigeben oder Einstellungen in einer der Ihnen zugewiesenen Ansichten überschreiben.

Im Filterbereich werden die vordefinierten Filter aufgelistet. In der Tabelle Express-Liste werden die Spalten angezeigt, die für die ausgewählte Ansicht konfiguriert wurden.

Zugehörige Informationen

Express-Liste -Ansichten werden für Benutzer und Benutzergruppen konfiguriert

Fügen Sie Express-Liste -Spalten hinzu, oder ändern Sie sie

Fügen Sie der Anzeige Ereignismanagement Express-Liste Spalten hinzu, um die Liste der angezeigten Warnungen zu fokussieren, oder ändern Sie die vorhandenen Spalten, die angezeigt werden.

Vorbereitungen

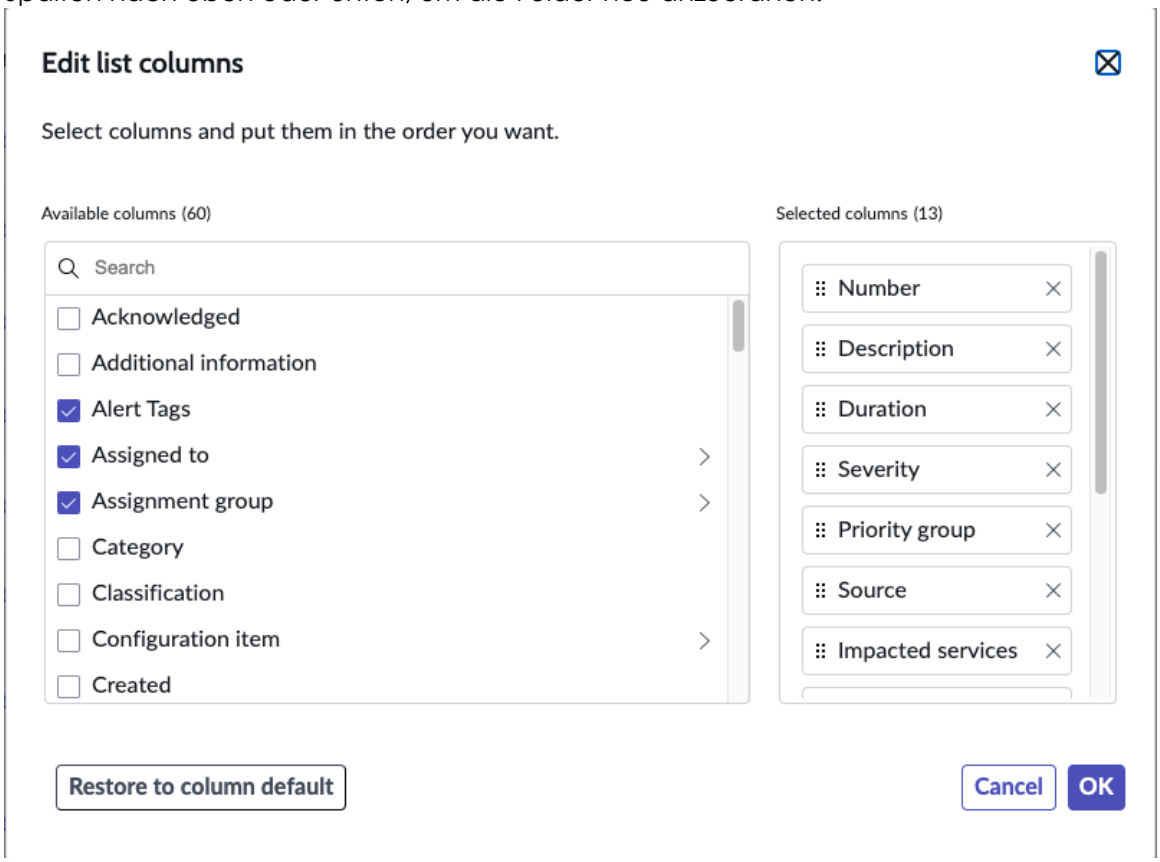
Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Bearbeiten Sie die Standardspalten im Bereich.
   a. Wählen Sie das Zahnradsymbol ( ).
   b. Wählen Sie in der Liste **Verfügbare Spalten** die gewünschten Spalten aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Ziehen Sie in der Liste **Ausgewählte Spalten** die ausgewählten Spalten nach oben oder unten, um die Felder neu anzuordnen.



d. Wahlweise: Wählen Sie **Auf Spaltenstandard zurücksetzen,** um die Spalten in den Standardstatus zurückzusetzen.

e. Wählen Sie **OK**.

4. Wahlweise: Ändern Sie die Spaltenbreite, Reihenfolge und Sortierrichtung direkt im Bereich Express-Liste.

Option	Aktion
Spaltenbreite	Zeigen Sie auf die rechte Seite der Spalte, bis der bidirektionale Pfeil angezeigt wird, und ziehen Sie die Spalte auf die gewünschte Breite.
Spaltenreihenfolge	Wählen Sie den Spaltenheader aus, und ziehen Sie ihn an die gewünschte Stelle.
Spaltensortierung	Wählen Sie den Spaltenheader und dann den Pfeil aus. Die Pfeilrichtung gibt die Sortierreihenfolge an. Jede Auswahl des Pfeils ändert die Sortierrichtung.

Ergebnisse

Das Layout wird automatisch in der Tabelle „Benutzereinstellung“ [sys_user_preference] gespeichert. Wenn Sie die Liste erneut öffnen, werden die gleichen Spalten und die gleiche Reihenfolge angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie dem Vorschaubereich Express-Liste anwenderdefinierte Felder hinzu

Fügen Sie anwenderdefinierte Felder aus der Tabelle „Warnung“ [em_alert] dem Infovorschaubereich Express-Liste hinzu, um Warnungsinformationen nachzuverfolgen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

Prozedur

1. Navigieren zu **Systemeigenschaften** > **Alle Eigenschaften**.
2. Wählen Sie in der Liste **„Systemeigenschaften“evt_mgmt.express_list.custom_fields**aus.

   Wenn eine Nachricht zum Anwendungsbereich angezeigt wird, wählen Sie **hier,** um den Datensatz bearbeiten zu können.
3. Geben Sie im Feld **Wert** den anwenderdefinierten Namen aus der Warnungstabelle [em_alert] ein.
   Wenn Sie mehr als ein Feld angeben möchten, trennen Sie die Feldnamen durch Kommas.
4. Wählen Sie **Aktualisieren**.
5. Wahlweise: Zeigen Sie die anwenderdefinierten Felder im Vorschaubereich an:
   a. Wählen Sie in der primären Navigation das Symbol Express-Liste ( ).
   b. Wählen Sie eine Zeile oder das Informationssymbol am Anfang einer Zeile aus.

Ergebnisse
Auf der Registerkarte Info im Vorschaubereich werden die anwenderdefinierten Felder am unteren Rand der Feldliste angezeigt.

Bestätigen Sie angezeigte Warnungen in Express-Liste

Bestätigen Sie Warnungen, die Sie angezeigt haben, um im Bereich Express-Liste Übersicht zu schaffen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

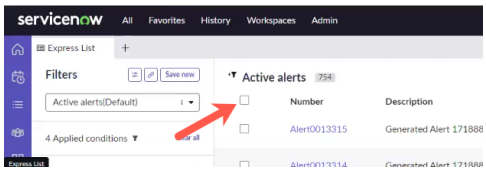
Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

Warum und wann dieser Vorgang ausgeführt wird
Verwenden Sie Bestätigen, um anzugeben , dass die Warnung bekannt ist und vorübergehend ignoriert werden kann. Verwenden Sie Bestätigen nicht, um eine Warnung mit einem Handlungsbedarf zu versehen.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Bestätigen Sie ausgewählte Warnungen.
   Sie können Warnungen unabhängig davon bestätigen, ob Sie im Hauptbereich oder im Vorschaubereich arbeiten. Der Vorschaubereich wird nur geöffnet, wenn eine einzelne Warnung oder Warnmeldungsgruppe ausgewählt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standort	Aktion
Der Bereich Express-Liste .	**a.** Wählen Sie im Bereich Express-Liste die zu bestätigende Warnung aus. Sie können mehr als eine Warnungszeile auswählen. **Hinweis:** Sie können die Aktion für bis zu 1.000 Warnungen gleichzeitig ausführen, indem Sie in der Liste Aktive Warnungen das Kontrollkästchen **Alle auswählen** auswählen.  Um die einzelnen Warnungen innerhalb einer Gruppe anzuzeigen, wählen Sie das Checker-Symbol (›) am Anfang der Zeile der Warnmeldungsgruppe. **b.** Wählen Sie in der Dropdown-Liste **Schließen** oben rechts in der Warnungsliste **die Option Bestätigen aus**.
Der Vorschaubereich Express-Liste für Gruppenwarnungen	**a.** Aktivieren Sie ein Kontrollkästchen für eine Warnmeldungsgruppenzeile. **b.** Wählen Sie auf der Registerkarte **Warnungen in Gruppe** eine Warnungskachel aus. **c.** Wählen Sie das Symbol „Weitere Aktionen“ (⋮). **d.** Wählen Sie **Bestätigen**aus.

Ergebnisse
Die Warnung wird bestätigt, und ihr Status wird oben im Vorschaubereich angezeigt.

Eingehende Warnungen überwachen

Sie können eingehende Warnungen in Service Operations-Arbeitsbereichüberwachen. Sie können Warnungen auch auf der Oberfläche Ereignismanagement überwachen und verwalten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin, evt_mgmt_operator

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Zeigen Sie die Warnungsinformationen an.

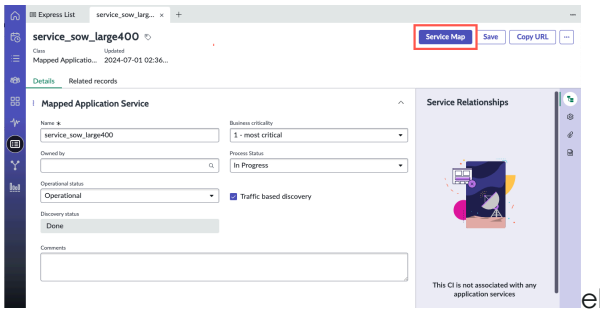
Spaltenüberschriften Warnungen

Spaltenüberschrift	Beschreibung
Nummer	Eindeutige ID, die von Ereignismanagement generiert wird, um die Warnung zu identifizieren.
Gruppe	Ein Eintrag in dieser Spalte gibt an, dass die zugeordnete Warnung ein Mitglied einer Warnungsgruppe ist. Warnungen, die keinen Eintrag in dieser Spalte haben, sind nicht gruppierte Warnungen. ◦ **Automatisiert**: Werden automatisch durch Warnungszusammenfassung zusammengefasst. Eine virtuelle Warnung wird der Gruppe als primäre Warnung der Gruppe hinzugefügt. ◦ **Regelbasiert**: Warnmeldungsgruppe, die als Ergebnis einer vom Anwender konfigurierten Korrelationsregel erstellt wurde. ◦ **Manuell**: Diese Warnung ist ein Mitglied einer Warnungsgruppe, die beim Klicken mit der rechten Maustaste auf eine Warnung und als sekundäre Einstellung für die ausgewählte primäre Warnung gebildet wird. ◦ **CMDB**: CIs ohne Verlaufsdaten, die durch Warnungszusammenfassung basierend auf CI-Beziehungen in der CMDB aggregiert wurden. ◦ **Sekundär**: Diese Warnung ist eine Komponente einer Warnungsgruppe. Die Warnung an der Spitze der Gruppe wird als primäre Warnung bezeichnet. Wenn **Korrelierte Warnungen** ausgewählt ist, werden die sekundären Warnungen, die sich unter der primären Warnung befinden, nicht angezeigt, wodurch die Warnungsliste übersichtlicher und leichter zu überprüfen ist. ◦ **Keine**: Diese Warnung ist eine nicht gruppierte Warnung. Damit eine nicht gruppierte Warnung Mitglied einer Gruppe wird, klicken Sie mit der rechten Maustaste darauf, und wählen Sie im Thema **Zu Gruppen hinzufügen** aus. Wählen Sie die Warnung aus, und klicken Sie auf **Ausgewählte hinzufügen**. ◦ **Text**: Diese Warnung ist ein Mitglied einer Warnmeldungsgruppe, die basierend auf der Ähnlichkeit ihres Texts oder ihrer Beschreibung erstellt wurde. ◦ **Log Analytics**: Diese Warnung ist ein Mitglied einer Log Analytics-Warnungsgruppe. ◦ **Komponentenbasiert**: Diese Warnung ist ein Mitglied einer Log Analytics-Gruppe, die basierend auf den betroffenen IT-Komponenten oder Services erstellt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spaltenüberschrift	Beschreibung
	◦ **Tag-Cluster**: Diese Warnung ist ein Mitglied einer Warnmeldungsgruppe, die basierend auf allgemeinen Tags oder Bezeichnungen erstellt wurde, die ihnen zugewiesen sind. ◦ **Netzwerkverkehr**: Diese Warnung ist ein Mitglied einer Warnmeldungsgruppe, die basierend auf Netzwerkdatenverkehrverbindungen zwischen Prozessen von Host-CIs erstellt wurde.
Schweregrad	Der Schweregrad des Events. Der Wert für dieses Feld wird aus dem Event kopiert, es sei denn, das Event schließt die Warnung. In diesem Fall wird der vorherige Schweregrad für die Berichterstellung beibehalten. ◦ **Kritisch**: Es ist eine sofortige Aktion erforderlich. Die Ressource funktioniert entweder nicht, oder kritische Probleme stehen unmittelbar bevor. ◦ **Schwerwiegend**: Wichtige Funktionen sind stark beeinträchtigt, oder es ist eine Leistungsverschlechterung aufgetreten. ◦ **Geringfügig**: Ein partieller, nicht kritischer Verlust der Funktionalität oder es ist eine Leistungsverschlechterung aufgetreten. ◦ **Warnung**: Es ist Aufmerksamkeit erforderlich, obwohl die Ressource noch funktionsfähig ist. ◦ **OK**: Eine Warnung wird erstellt. Die Ressource ist weiterhin funktionsfähig. ◦ **Löschen**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
Prioritätsgruppe	Gibt an, welche Warnungen zuerst behandelt werden sollen. Die Priorität wird für alle offenen Warnungen berechnet, woraufhin diese einer von vier Prioritätskategorien zugeordnet werden.
Priorität	Wert, der als Leitfaden für die Priorität der Warnung dient, basierend auf einer Anzahl von kumulierten Kategorien. Beispielsweise Warnungsstatus und geschäftliche Relevanz.
Quelle	Eventüberwachungssoftware, die das Event generiert hat, z. B. SolarWinds oder SCOM. Optional können Sie eine Beschreibung eingeben, z. B. `Gruppenwarnung`. Dieses Feld hat eine maximale Länge von 100.
Beschreibung	Die Warnungsbeschreibung.
Knoten	Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, die dem Ereignis zugeordnet ist, z. B. IBM-ASSET. Dieses Feld hat eine maximale Länge von 100.
Konfigurationselement	JSON-Zeichenfolge, die ein Konfigurationselement darstellt. Beispiel: {„Name“: „SAP ORA01“, „Typ“: „Oracle“}. Der CI-Bezeichner, der das Event generiert hat, wird im Feld **Zusätzliche Informationen** angezeigt. Dieses Feld hat eine maximale Länge von 1000. Klicken Sie auf das , um die Warnung in der Abhängigkeitsansicht zu öffnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spaltenüberschrift	Beschreibung
Betroffene Services	Listet die Services auf, die von dieser Warnmeldungsgruppe betroffen sind. Wählen Sie einen betroffenen Service aus, um den zugehörigen Datensatz anzuzeigen. **Hinweis:** Sie können auf die Servicezuordnung in Service Operations-Arbeitsbereich direkt aus dem betroffenen Serviceformular zugreifen, indem Sie **Servicezuordnung**auswählen. In der Servicezuordnung wird der Auswirkungspfad von Warnungen angezeigt, sodass Sie ihre Auswirkungen auf den Service schnell bewerten können. Weitere Informationen finden Sie unter Zeigen Sie eine einheitliche Servicezuordnung und die Auswirkungspfade in an Service Operations-Arbeitsbereich.  el-imp-service-open-map.png
Metrikname	Eindeutiger Name, der beschreibt, welche Metriken erfasst werden und für welche die Warnung erstellt wurde.
Reserviert	Zeigt an, ob sich die von der Warnung betroffene Ressource in Wartung befindet. Gültige Werte sind `true` oder `false`.
Aufgabe	Die entsprechende Aufgabe für die Warnung, z. B. Incident, Change oder Problem.
Übergeordnet	Verweis auf übergeordnete Warnung.
Generierungszeit des ersten Events	Zeit des ersten Ereignisses im Remote-System

Nächste Maßnahme

Wenn Operational Intelligence aktiviert ist, klicken Sie mit der rechten Maustaste auf eine Warnung, und klicken Sie dann auf **Metriken anzeigen**, um den integrierten Explorer für Einblicke und die Dependency Views-Zuordnung für das CI zu öffnen, das der Warnung zugeordnet ist.

Zugehörige Informationen

- Metrikdaten
- Warnungsinformationen anzeigen
- Warnungsgruppierungstypen und -erstellungsmethoden

Schließen Sie eine Warnung in Express-Liste

Schließen Sie Warnungen manuell direkt im Bereich Express-Liste oder im Vorschaubereich, ohne darauf zu warten, dass sie automatisch geschlossen werden, wenn Sie die Ursache bereits kennen oder das Problem behoben haben.

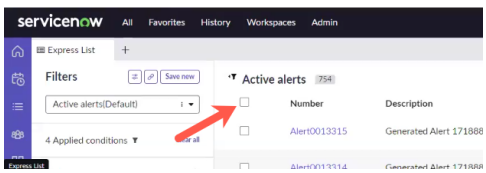
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Schließen Sie ausgewählte Warnungen.
   Sie können Warnungen unabhängig davon schließen, ob Sie im Hauptbereich oder im Vorschaubereich arbeiten. Der Vorschaubereich wird nur geöffnet, wenn eine einzelne Warnung oder Warnmeldungsgruppe ausgewählt ist.

Standort	Aktion
Der Bereich Express-Liste .	**a.** Wählen Sie im Bereich Express-Liste die Warnung aus. Sie können mehr als eine Warnungszeile auswählen. **Hinweis:** Sie können die Aktion für bis zu 1.000 Warnungen gleichzeitig ausführen, indem Sie in der Liste Aktive Warnungen das Kontrollkästchen **Alle auswählen** auswählen.  Um die einzelnen Warnungen innerhalb einer Gruppe anzuzeigen, wählen Sie das Checker-Symbol ( ) am Anfang der Zeile der Warnmeldungsgruppe. **b.** Wählen Sie in der Dropdown-Liste **Schließen** oben rechts in der Warnungsliste **die Option Warnung schließen aus**.
Der Vorschaubereich Express-Liste für Gruppenwarnungen	**a.** Wählen Sie eine Warnmeldungsgruppenzeile aus. **b.** Wählen Sie auf der Registerkarte **Warnungen in Gruppe** eine Warnungskachel aus. **c.** Wählen Sie das Symbol „Weitere Aktionen“ ( ). **d.** Wählen Sie **Warnung schließen aus**.

Ergebnisse
Die Warnung wird geschlossen, und ihr Status wird oben im Vorschaubereich angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Incident aus einer Warnung in Express-Liste

Erstellen Sie einen Incident aus einer Warnung direkt im Bereich Express-Liste, wodurch Sie nicht mehr zum Incident-Datensatz navigieren müssen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Erstellt einen Incident aus einer ausgewählten Warnung.
   a. Wählen Sie im Bereich Express-Liste die Warnung aus.

      Hinweis: Um die einzelnen Warnungen innerhalb einer Gruppe anzuzeigen, wählen Sie das Checker-Symbol (›) am Anfang der Zeile der Warnmeldungsgruppe.

   b. Wählen Sie in der Dropdown-Liste **Schließen** unter Korrekturaktionen **die Option Incident erstellen aus**.
   Aus der ausgewählten Warnung wird ein Incident erstellt, und eine Bestätigungsmeldung wird angezeigt.
4. Wahlweise: Zeigen Sie einen erstellten Incident an, indem Sie **Incident anzeigen** in der Bestätigungsnachricht wählen.

Einen Incident mit Now Assist in Express-Listeerstellen

Erstellen Sie mithilfe von Now Assisteinen Incident mit einer visuell lesbaren, KI-generierten Beschreibung.

Vorbereitungen

Derzeit ist diese Funktion für Warnungen CMDBvom Typ , Log Analyticssowie für tagbasierte und komponentenbasierte Warnungen verfügbar.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol Express-Liste ( ) aus.
3. Erstellt einen Incident aus einer ausgewählten Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie im Bereich Express-Liste die Warnung aus.

Hinweis: Um die einzelnen Warnungen innerhalb einer Gruppe anzuzeigen, wählen Sie das Checker-Symbol (›) am Anfang der Zeile der Warnmeldungsgruppe.

b. Wählen Sie in der Dropdown-Liste **Schließen** unter Korrekturaktionen **die Option Incident mit Now Assist erstellen aus**.

Aus der ausgewählten Warnung wird ein Incident mit einer visuell lesbaren, KI-generierten Beschreibung erstellt, und eine Bestätigungsmeldung wird angezeigt.

4. Wahlweise: Zeigen Sie den erstellten Incident an, indem Sie **Incident anzeigen** in der Bestätigungsnachricht oder im Warnungsvorschaubereich auswählen.

Fügen Sie einem Incident in Warnungen hinzu Express-Liste

Fügen Sie einem vorhandenen Incident in Express-ListeWarnungen hinzu.

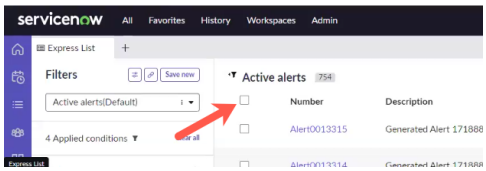
Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Fügen Sie einem vorhandenen Incident eine Warnung hinzu.
   Sie können einem Incident Warnungen hinzufügen, unabhängig davon, ob Sie im Hauptfenster oder im Vorschaubereich arbeiten. Der Vorschaubereich wird nur geöffnet, wenn eine einzelne Warnung oder Warnmeldungsgruppe ausgewählt ist.

Standort	Aktion
Der Bereich Express-Liste.	**a.** Wählen Sie in der Liste Aktive Warnungen die Warnung aus. Sie können mehr als eine Warnung auswählen. **Hinweis:** Sie können die Aktion für bis zu 1.000 Warnungen gleichzeitig ausführen, indem Sie in der Liste Aktive Warnungen das Kontrollkästchen **Alle auswählen** auswählen.  Um die einzelnen Warnungen in einer Gruppe anzuzeigen, wählen Sie das Che-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standort	Aktion
	cker-Symbol (›) am Anfang der Zeile der Warnmeldungsgruppe. **b.** Wählen Sie in der **Dropdown** -Liste Schließen oben rechts in der Warnungsliste **die Option Mit Incident verknüpfen**aus. **c.** Geben Sie die Nummer des incident ein, dem Sie die ausgewählte Warnung hinzufügen möchten. **Hinweis:** Sie können auch das Dienstprogramm Suchen verwenden, um nach dem Incident zu suchen und ihn auszuwählen. **d.** Wählen Sie **Aktualisieren**.
Der Vorschaubereich Express-Liste für Gruppenwarnungen	**a.** Wählen Sie eine Warnmeldungsgruppenzeile aus. **b.** Wählen Sie auf der Registerkarte **Warnungen in Gruppe** eine Warnungskachel aus. **c.** Wählen Sie das Symbol „Weitere Aktionen“ (⋮). **d.** Wählen Sie **Mit Incident verknüpfen**. **e.** Geben Sie die Nummer des incident ein, dem Sie die ausgewählte Warnung hinzufügen möchten. **Hinweis:** Sie können auch das Dienstprogramm Suchen verwenden, um nach dem Incident zu suchen und ihn auszuwählen. **f.** Wählen Sie **Aktualisieren**.

Die ausgewählte Warnung oder Warnungen werden dem Incident hinzugefügt, und eine Bestätigungsmeldung wird angezeigt.

4. Wahlweise: Zeigen Sie den Incident an, indem Sie **Incident öffnen** in der Bestätigungsnachricht wählen.

Schalten Sie die Warnungen eines CI in stumm Express-Liste

Schalten Sie die Warnungen eines CI in Express-Liste stumm, um zu vermeiden, dass Warnungen ausgegeben werden, wenn das CI ersetzt oder aktualisiert wird.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

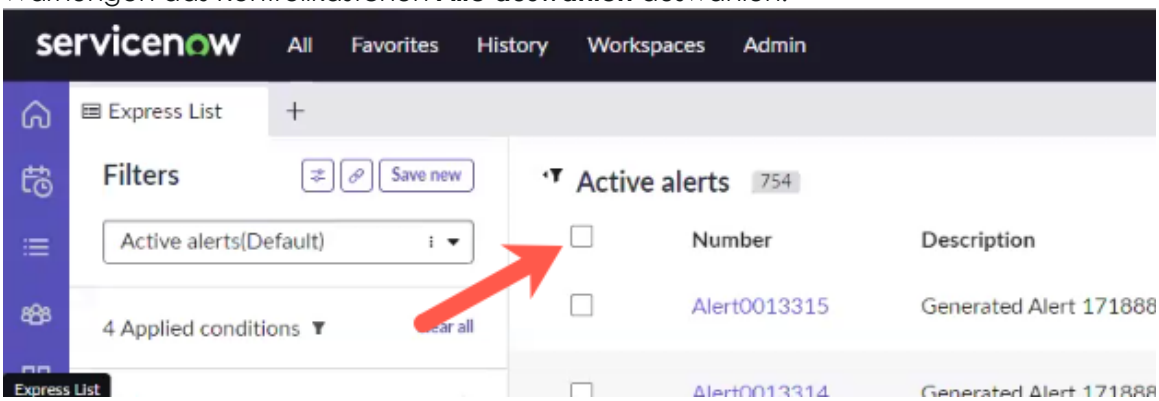
Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Aktivieren Sie das Kontrollkästchen für die Warnungszeile.

Hinweis: Sie können die Aktion für bis zu 1.000 Warnungen gleichzeitig ausführen, indem Sie in der Liste Aktive Warnungen das Kontrollkästchen **Alle auswählen** auswählen.



4. **Wählen** Sie in der Dropdown-Liste Schließen **die Option In Wartung setzen aus**.

Ergebnisse

Warnungen werden für die Konfigurationselemente dieser Warnung stummgeschaltet.

Warnungen in den Status „Wartung“ versetzen

Indem Sie eine Warnung in den Status „Wartung“ versetzen, geben Sie an, dass verschiedene Probleme mit den CIs der Warnung behandelt werden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Mit **aktiven Warnungen**filtern.
4. Wählen Sie eine Warnung aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Aktivieren Sie auf der Unterregisterkarte **Details** das Kontrollkästchen **Wartung**, um die Warnung in den Status „Wartung“ zu versetzen.
6. Klicken Sie auf **Speichern**.

Warnungen in den Status „Bestätigt“ versetzen

Indem Sie eine Warnung in den Status „Bestätigt“ versetzen, geben Sie an, dass Probleme mit der Warnung behoben werden müssen.

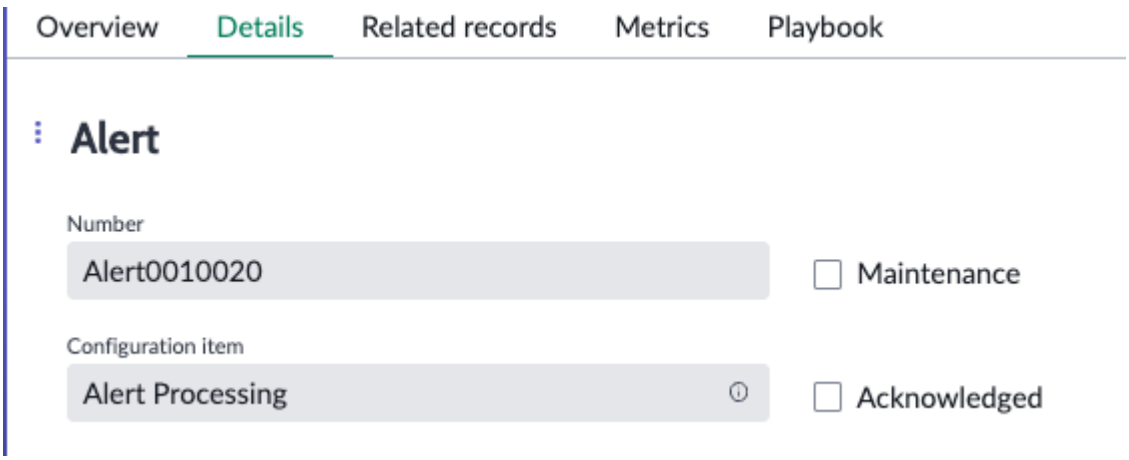
Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Mit **aktiven Warnungen**filtern.
4. Wählen Sie eine Warnung aus.



5. Aktivieren Sie auf der Unterregisterkarte **Details** das Kontrollkästchen **Bestätigt**, um die Warnung in den Status „Bestätigt“ zu versetzen.
6. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrigieren Sie eine Warnung in Express-Liste

Führen Sie eine Korrekturaktion aus, um ein Problem manuell in einer Warnung direkt im Bereich Express-Liste zu beheben.

Vorbereitungen

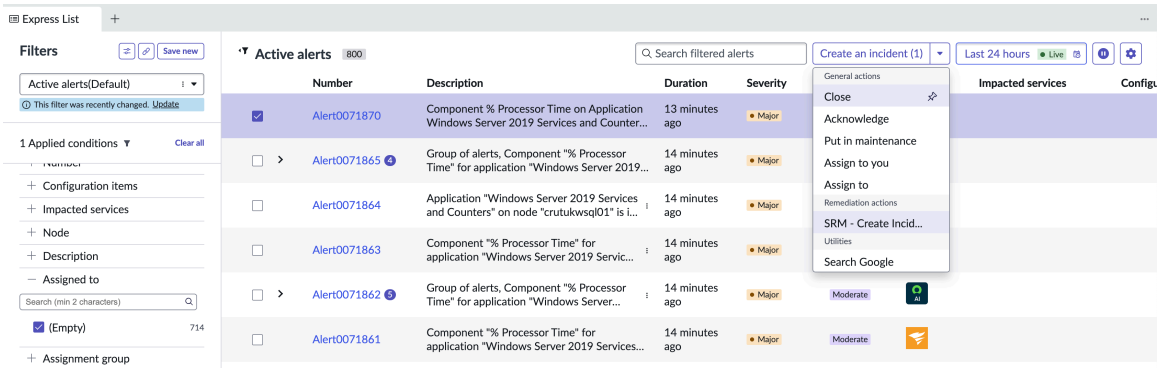
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
4. Wählen Sie in der **Dropdown** -Liste Schließen die Korrekturaktion für die Warnung aus.

Hinweis: Wenn die Liste leer ist, sind keine Korrekturaktionen verfügbar.



Zeigen Sie Metriken für eine Warnung an

Durch das Anzeigen von Metriken können Sie Verlaufsdaten verstehen, die sich auf das CI einer Warnung beziehen.

Vorbereitungen

- Installieren Sie das Plugin Operational Intelligence (com.snc.sa.metric).
- Konfigurieren Sie die Metriken, die für die Warnung angezeigt werden sollen, wie in Warnungsmetriken konfigurieren beschrieben.

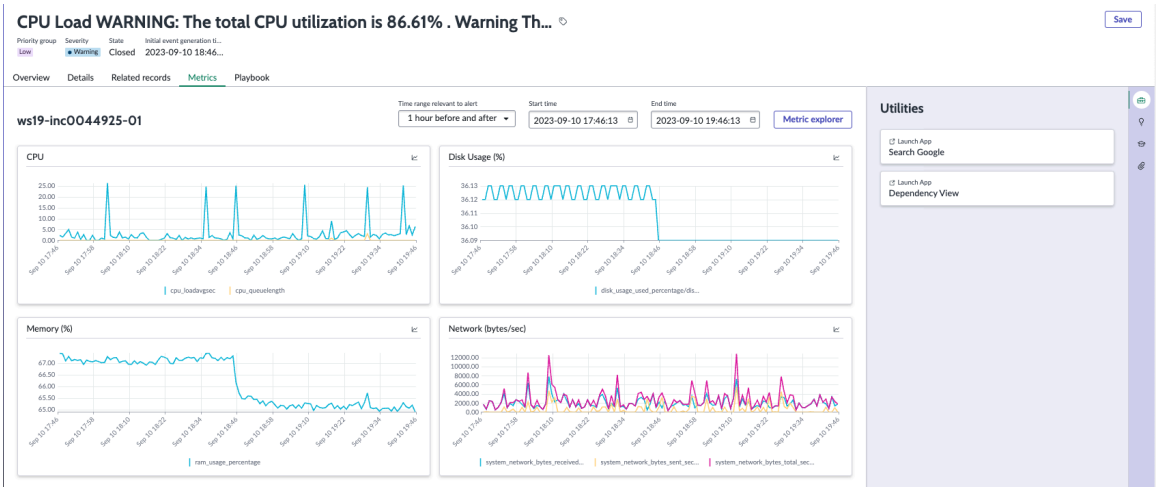
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Wählen Sie eine Warnung aus, um sie zu öffnen.
4. Klicken Sie auf die Unterregisterkarte **Metriken**.
   Die konfigurierten Metriken werden auf der Seite angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Um die Metrikanzeige anzupassen, konfigurieren Sie im die folgenden Eigenschaften **Systemeigenschaften** > **Alle Eigenschaften** Seite:

- *ws_metric.widgets_number_limit*: Geben Sie die Anzahl der Widgets/Datensätze an, die auf der Registerkarte „Metriken“ angezeigt werden können.
- *ws_metric.datasets_per_widget_limit*: Geben Sie die Anzahl der Diagramme/ Datensätze an, die in einem Diagramm angezeigt werden dürfen.

5. Wählen Sie in der Liste **Zeitbereich relativ zur Warnung** den Zeitbereich aus, für den die Metriken zur Warnung angezeigt werden sollen:
   - 1 Stunde vorher und nachher (Standardeinstellung)
   - 3 Stunden davor und danach
   - 5 Stunden davor und danach
   - Benutzerdefinierter Bereich (zum Konfigurieren eines benutzerdefinierten Zeitraums für die Metriken)
6. Klicken Sie auf einen Parameter unter einem Diagramm, um die Daten des Parameters im Diagramm auszublenden.
7. Wahlweise: Klicken Sie auf die Schaltfläche **Explorer für Einblicke**, um Metriken anzuzeigen, indem Sie sie mittels Drag-and-Drop auf der Zeitleiste ablegen.

Zugehörige Informationen

Metrikwerte im Explorer für Einblicke anzeigen

Zeigen Sie Details zu den Auswirkungen und der Ursache einer Warnung in an Express-Liste

Zeigen Sie Informationen zu einer Warnung auf der Registerkarte „Übersicht“ der Warnung in Express-Liste an.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
   Die Warnung wird auf einer separaten Registerkarte geöffnet und zeigt die Registerkarte **Übersicht** an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Zeigen Sie Warnungsinformationen auf der Registerkarte **Übersicht** an.

Registerkarte Übersicht

Abschnitt	Beschreibung
Zusammenfassung	Enthält eine Beschreibung der ausgewählten Warnung und beschreibt, warum der Sachverhalt als Problem betrachtet wird.
Auswirkung	Listet das Konfigurationselement und alle von der Warnung betroffenen Services auf. Die Kachel **Betroffene Services** enthält die folgenden untergeordneten Registerkarten: ◦ **Anwendungsservices:** Die von der Warnung betroffenen Anwendungsservices. Einzelheiten zu Anwendungsservices finden Sie unter Anwendungsservices . ◦ **Related service offerings (Zugehörige Serviceangebote):** Die Serviceangebote, die mit den von der Warnung betroffenen Anwendungsservices verbunden sind. Anwendungsservices und die zugehörigen Serviceangebote werden auf einer Viele-zu-viele-Basis angezeigt. Das heißt: Mehrere Serviceangebote können sich auf einen oder mehrere Anwendungsservice(s) beziehen, und mehrere Anwendungsservices können sich auf ein oder mehrere Serviceangebot(e) beziehen.
Ursache	Listet die Protokolleigenschaften mit Informationen auf, die zum Warnungsproblem beitragen, sowie wahrscheinliche Ursachen für die Warnung.

Zeigen Sie die Abhängigkeitsansichten-Karte für CMDB-Warnungen in der Express-Liste an

Die Karte „Abhängigkeitsansichten“ bietet Einblicke in die Art und Weise und den Grund für die Gruppierung von Warnungen und unterstützt sowohl die Problembehandlung als auch die proaktive Verwaltung. Zeigt die verbindenden CIs unter CMDB-Warnungen innerhalb einer Gruppe an. Selbst wenn ein CI nicht Teil der Gruppe ist, wird es in der Zuordnung angezeigt, wenn es eine Verbindung zu anderen Warnungs-CIs innerhalb der Gruppe herstellt.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user, evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation entweder das Listensymbol ( ) oder das Express-Liste -Symbol ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie für eine Warnung, für die Sie die CI-Abhängigkeitsansicht anzeigen möchten, in den Spalten Konfigurationselemente das Konfigurationselement aus.
4. Wählen Sie im Fenster mit den Konfigurationselementen **Abhängigkeitsansicht öffnen aus**. Sie können die Abhängigkeitsansicht der CMDB-Warnungen anzeigen.

Zeigen Sie Daten zu betroffenen Services im Vorschaubereich in an Express-Liste

Zeigen Sie im Vorschaubereich zusätzliche Informationen zu betroffenen Services an, die an Warnungen gebunden sind.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Aktivieren Sie in der Liste Aktive Warnungen das Kontrollkästchen einer Warnung.
4. Öffnen Sie im Vorschaubereich die Registerkarte Info.
5. Bewegen Sie den Mauszeiger über den Abschnitt Betroffene Services, um Informationssymbole anzuzeigen.

6. Wählen Sie das entsprechende Symbol aus, um zusätzliche Informationen zu einem betroffenen Service anzuzeigen.

Symbole für betroffene Serviceinformationen

Symbol	Name	Beschreibung
ⓘ	Information	Zeigt den Schweregrad, die Geschäftskritikalität und eine Kurzbeschreibung des betroffenen Service an. In diesem Popup-Fenster können Sie die Servicezuordnung in Service Operations-Arbeitsbereich öffnen, indem Sie **Servicezuordnung anzeigen**wählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symbol	Name	Beschreibung
		 In der Servicezuordnung wird der Auswirkungspfad von Warnungen angezeigt, sodass Sie ihre Auswirkungen auf den Service schnell bewerten können. Weitere Informationen finden Sie unter Zeigen Sie eine einheitliche Servicezuordnung und die Auswirkungspfade in an Service Operations-Arbeitsbereich. Wenn für diesen Service Metrikdaten vorhanden sind, können Sie den Metric Explorer aus dem Popup öffnen, indem Sie **Zugehörige Metriken anzeigen**auswählen.
	Kontaktperson/gruppe	Zeigt den Namen des Besitzers des betroffenen Service und die ihm zugewiesene Supportgruppe an.

Zeigen Sie Daten zu Konfigurationselementen im Vorschaubereich in an Express-Liste

Zeigen Sie im Vorschaubereich Express-Liste zusätzliche Details zu Configuration Items (CIs) an, die an Warnungen gebunden sind.

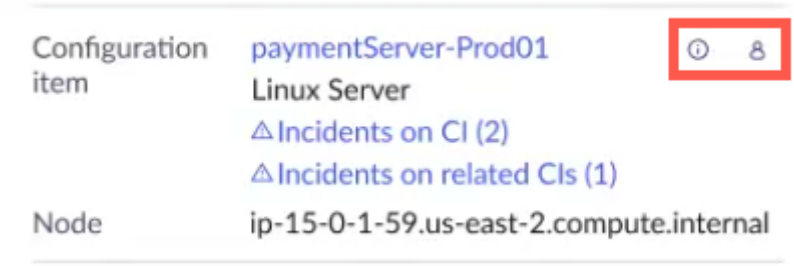
Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Aktivieren Sie in der Liste Aktive Warnungen das Kontrollkästchen für eine Warnung.
4. Öffnen Sie im Vorschaubereich die Registerkarte Info.
5. Bewegen Sie den Mauszeiger über den Abschnitt Konfigurationselement, um Informationssymbole anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Zeigen Sie zusätzliche Informationen zu einem CI an, indem Sie das entsprechende Symbol wählen.

Informationssymbole für Configuration Item

Symbol	Name	Beschreibung
ⓘ	Information	Zeigt die Klasse, die IP-Adresse, den Standort und die Umgebung des CI an.
👤	Kontaktperson/gruppe	Zeigt den Namen des Besitzers des CI, die ihm zugewiesene Supportgruppe und die Avatare der einzelnen Teammitglieder an.

7. Wahlweise: Zeigen Sie an, wie das aktuelle CI mit anderen CIs verbunden ist, indem Sie **CI-Topologie anzeigen** im Bereich mit zusätzlichen Informationen auswählen.
Die Karte **der Abhängigkeitsansicht** wird geöffnet. Die Zuordnung stellt die Beziehungen zwischen CIs visuell dar, sodass Sie verstehen, wie verschiedene Komponenten miteinander verbunden sind.

Blenden Sie geschlossene Warnungen in aus Express-Liste

Wählen Sie aus, ob die geschlossenen Warnungen in einer Warnmeldungsgruppe sowie die offenen Warnungen im Vorschaubereich und in der Link-Ansicht angezeigt werden sollen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Wählen Sie in der Liste Aktive Warnungen eine Warnmeldungsgruppe aus.

   Im Vorschaubereich wird die Standardanzeige angezeigt:

   - Auf der Registerkarte „Alerts“ (Warnungen) und in der Zeitleistenansicht werden nur die offenen Warnungen angezeigt. Die geschlossenen Warnungen werden ausgeblendet.
   - Die Linkansicht zeigt die Attribute offener und geschlossener Warnungen an.
4. Ändern Sie auf der entsprechenden Registerkarte die Anzeige.

   Im Vorschaubereich Registerkarte Warnungen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Zeigen Sie sowohl die offenen als auch die geschlossenen Warnungen an, indem Sie den **Umschalter „Geschlossene Warnungen** ausblenden“ in die Position „Geschlossen“ schalten.

b. (Optional) Sortieren Sie die angezeigten Warnungen nach Zeit oder Schweregrad, indem Sie das Sortiersymbol ( ) und dann das entsprechende Menüelement auswählen.

Hinweis: Wenn Sie den Umschalter umschalten oder die Warnungen in der Zeitleistenansicht sortieren, wird die Registerkarte Warnungen entsprechend Ihrer Auswahl angepasst.

In Link-Ansicht: Zeigen Sie nur die Attribute offener Warnungen an, während Sie die Attribute geschlossener Warnungen ausblenden, indem Sie den **Umschalter Attribute geschlossener Warnungen** ausblenden auf die Position „Offen“ schalten.

Warnungsanalyse von Now Assist in Express-Listeanzeigen

Zeigen Sie eine von ServiceNow® Now Assist erstellte Warnungsanalyse mit generativer KI an. Warnungsanalysen enthalten eine visuell lesbare Kurzbeschreibung der Warnung und technische Informationen, mit denen Sie Warnungen effektiver untersuchen können.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in der Funktion Now Assist. Weitere Informationen finden Sie unter Installieren Sie das Plugin Now Assist for IT Operations Management (ITOM)..
- Zeigen Sie wichtige Informationen zur Anwendung ServiceNow® Now Assist für IT Operations Management (ITOM) in Now Assist für IT Operations Management (ITOM)an .

Hinweis: Derzeit analysiert Now Assist für ITOM nur Tag-basierte, regelbasierte, Log Analyticsund Network Traffic Korrelation Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Wählen Sie in der Liste „Aktive Warnungen“ links neben einer Warnung das Informationssymbol ( ).
4. Wählen Sie auf der Registerkarte „Info“ des Vorschaubereichs **Analysieren** in Warnungsanalyse nach Now Assistaus.
5. Zeigen Sie die in der Warnungsanalyse bereitgestellten Informationen an.

Hinweis: Warnungsanalysen werden in englischer Sprache bereitgestellt, unabhängig davon, welche Sprache in der Warnungsbeschreibung verwendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wahlweise: Verwenden Sie die Warnungsanalysesymbole, um zugehörige Aufgaben auszuführen.

Symbole für Warnungsanalysen

Symbol	Beschreibung
	Kopieren Sie den Inhalt der Warnungsanalyse in die Zwischenablage.
	Aktualisieren Sie die Warnungsanalyse. **Hinweis:** Durch das Aktualisieren werden die Ergebnisse neu generiert. Vergangene Ergebnisse werden gelöscht.

Generieren eines Falls aus einer Warnung

Ermöglichen Sie eine schnelle Lösung, indem Sie manuell oder automatisch Fälle aus Warnungen generieren.

Kundenservice-Management bietet Integration mit ITOM Ereignismanagement. Diese Integration ermöglicht Ihnen, die Kunden-Experience zu verbessern, indem Sie Strukturen aufbrechen, die zwischen den Prozessen und Systemen bestehen, die von Front-Line-Kundenservice- und Back-Office-Betriebsteams verwendet werden. Indem Sie proaktiv Probleme überwachen und Fälle erstellen, können Sie Kundenprobleme besser korrelieren und so schneller Antworten liefern.

Mit der Integration zwischen den Anwendungen Kundenservice-Management und Ereignismanagement können Sie für die von einer Warnung betroffene Kunden-Installationsbasis einen Fall erstellen. Weitere Informationen finden Sie unter Proaktiven Fall manuell aus einer Warnung erstellen . Sie können auch eine Warnungsregel aktivieren, um automatisch einen proaktiven Fall aus einer Warnung zu erstellen, wenn ein Incident erstellt wird. Weitere Informationen finden Sie unter Warnungsregel aktivieren, um automatisch einen proaktiven Fall aus einer Warnung zu erstellen .

Entfernen Sie Warnungen aus einer Warnmeldungsgruppe in Express-Liste

Entfernen Sie sekundäre Warnungen aus einer Warnmeldungsgruppe direkt aus dem Bereich Express-Liste oder aus dem Vorschaubereich.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

Hinweis: Die Rolle „evt_mgmt_user“ ist schreibgeschützt und verfügt nicht über die Berechtigung zum Ausführen dieser Aktion.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Entfernen Sie eine sekundäre Warnung aus einer Warnmeldungsgruppe.
   Sie können Warnungen aus einer Gruppe entfernen, unabhängig davon, ob Sie im Hauptbereich oder im Vorschaubereich arbeiten. Der Vorschaubereich wird nur geöffnet, wenn eine einzelne Warnung oder Warnmeldungsgruppe ausgewählt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Standort	Aktion
Der Bereich Express-Liste .	**a.** Klicken Sie in der Liste „Aktive Warnungen“ am Anfang einer oder mehrerer Warnungsgruppenzeilen auf das Checker-Symbol (›), um die in der Gruppe enthaltenen Warnungen anzuzeigen. **b.** Wählen Sie eine oder mehrere sekundäre Warnungen aus. **c.** Wählen Sie in der Dropdown-Liste **Schließen** oben rechts in der Liste die **Option Aus Gruppe entfernen aus**. **Hinweis:** Wenn Sie versuchen, die einzige sekundäre Warnung aus einer Warnmeldungsgruppe zu entfernen und dadurch die Gruppierung der Gruppe aufzuheben, wird eine Meldung angezeigt, mit der Sie die Aktion rückgängig machen können.
Der Vorschaubereich Express-Liste für eine Gruppe von Warnungen	**a.** Wählen Sie auf der Registerkarte **Warnungen in Gruppe** eine Warnungskachel aus. **b.** Wählen Sie das Symbol „Weitere Aktionen“ (⋮). **c.** Wählen Sie **Aus Gruppe entfernen aus**.

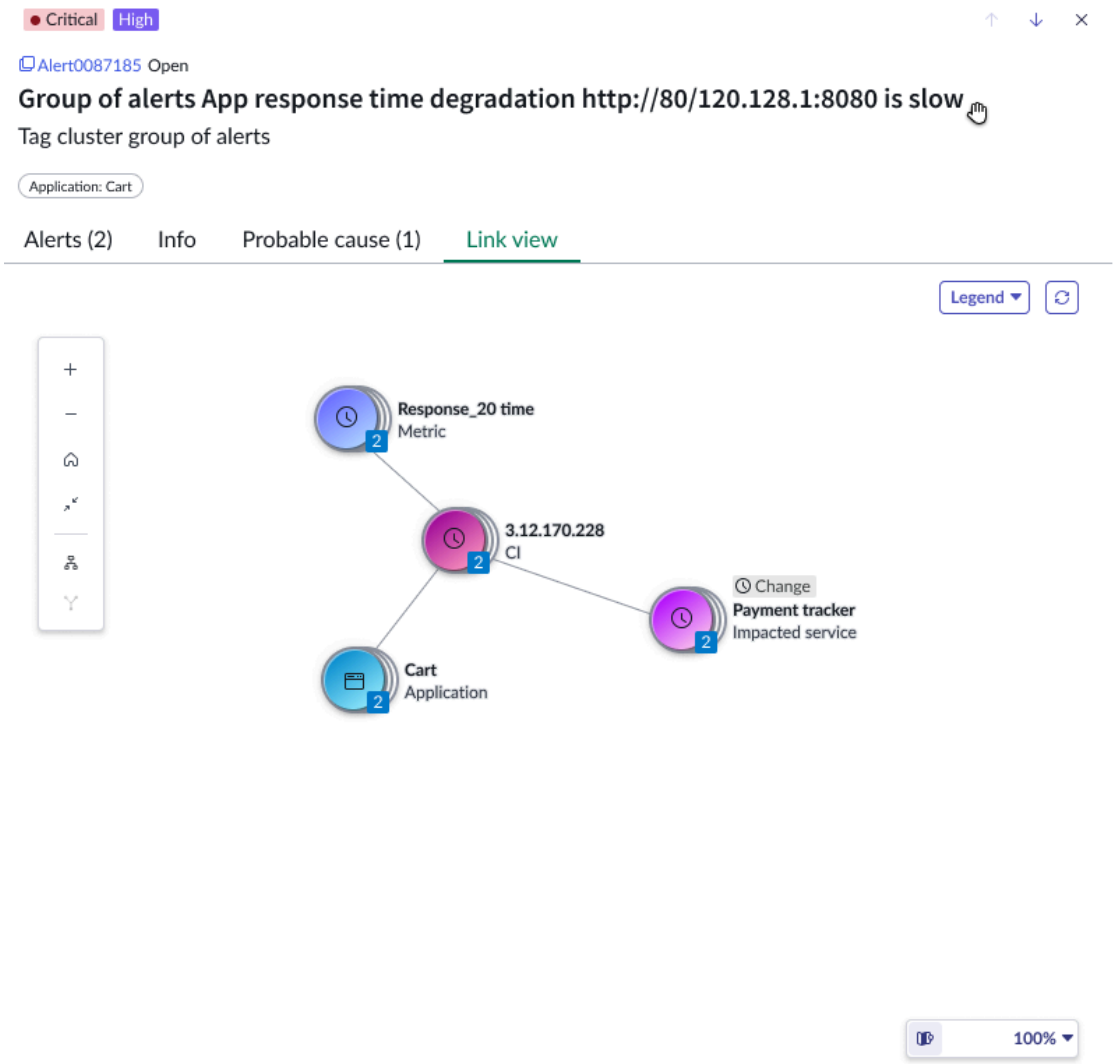
Links zwischen Warnungen in Warnmeldungsgruppen in anzeigen Express-Liste

Verschaffen Sie sich mit der Link-Ansicht ein besseres Verständnis der Beziehungen zwischen Warnungen in -Warnungsgruppen in Express-Liste. Die Linkansicht bietet eine visuelle Darstellung der Beziehungen zwischen den Warnungen in einer Gruppe.

Wenn Ereignismanagement eine Warnmeldungsgruppe generiert, zeigt die Linkansicht, wie die Attribute der Warnungen in der Gruppe verknüpft sind. Die farbigen Tags stehen für Configuration Items (CIs) und andere Umgebungselemente im Zusammenhang mit den Warnungen. Die in der Link-Ansicht angezeigten Informationen sind verfügbar, ohne dass ein ausgefülltes Configuration Management Database (CMDB)erforderlich ist. Wenn jedoch CMDB ausgefüllt ist, bietet die Linkansicht einen Mehrwert, indem die wahrscheinliche Ursache der Warnungen und der Service angegeben werden, auf den sich die Warnmeldungsgruppe auswirkt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Warnmeldungsgruppe in der Linkansicht

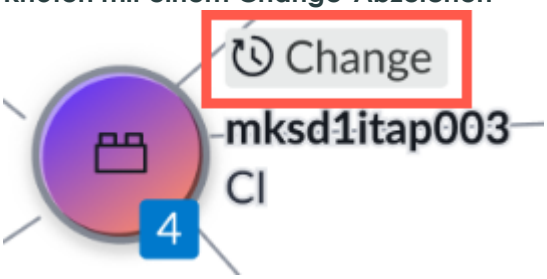


Sie können sich auf Ihre Interessenbereiche konzentrieren, indem Sie die Knoten in der Linkansicht an andere Positionen ziehen. Wenn Sie eine Warnmeldungsgruppe aktualisieren, werden neu angeordnete Knoten wieder an ihrer ursprünglichen Position angezeigt. Daher wird die Linkansicht nicht automatisch aktualisiert, sondern wartet darauf, dass Sie dies manuell tun. Wenn sich eine Warnung für ein CI auf einen Service in Configuration Management Database (CMDB)auswirkt, zeigt die Linkansicht den betroffenen Service an. So können Sie ihn für eine schnelle Selektierung auf einen Blick anzeigen.

Ein gestapelter Knoten zeigt an, dass mehrere Knoten für dasselbe Tag zugeordnet wurden. Wenn dasselbe Schlüssel-Wert-Paar in mehr als einer Warnung vorkommt, wird der entsprechende Knoten mit einem Abzeichen angezeigt. Wenn beispielsweise dasselbe Schlüssel-Wert-Paar in zwei Warnungen angezeigt wird, zeigt das Abzeichen auf dem Knoten die Nummer 2 an, wie im Zahlungstracker-Knoten in der Beispielabbildung für eine Warnmeldungsgruppe zu sehen ist. Wenn ein Knoten kein Abzeichen aufweist, wurde das Schlüssel-Wert-Paar nur in einer Warnung angezeigt. Eine aktive Change-Anforderung, eine wahrscheinliche Ursache für die Warnung, wird durch ein Change-Abzeichen gekennzeichnet.

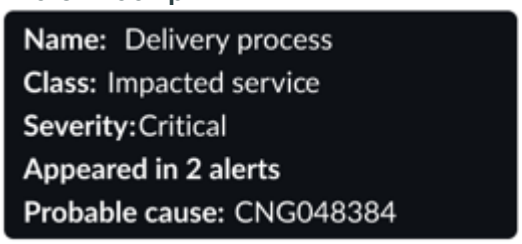
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Knoten mit einem Change-Abzeichen



Die Legende der Linkansicht listet die Bedeutung der verwendeten Symbole und Farben auf und ermöglicht Ihnen das Umschalten zwischen Ein- und Ausblenden von Tag-Typen, um das Rauschen zu reduzieren. Darüber hinaus beschreibt die Legende die Bedeutung der verschiedenen Zeilen, die die Warnungsattribute verbinden. Attribute, die mit einer durchgezogenen Linie verknüpft sind, teilen eine oder mehrere Warnungen, während Attribute, die mit einer gestrichelten Linie verknüpft sind, durch Gruppierungskriterien korreliert sind. Eine Beschreibung der einzelnen Tags finden Sie unter Attribute in der Linkansicht Express-Liste .. Wenn Sie den Mauszeiger über einen Knoten bewegen, wird ein Tooltip angezeigt, der den Namen des Tags, seine Klasse, seinen Schweregrad, die Anzahl der Warnungen, in denen er angezeigt wurde, und ggf. die Angabe, ob die Warnung primär oder sekundär ist, oder die wahrscheinliche Ursache der Warnung enthält.

Knoten-Tooltip



Derzeit wird die Linkansicht für tagbasierte, regelbasierte, CMDB-basierte und netzwerkdatenverkehrsbasierte Warnmeldungsgruppen unterstützt. Weitere Informationen finden Sie unter:

- Links zwischen Warnungen in Tag-basierten Warnmeldungsgruppen anzeigen
- Links zwischen Warnungen in regelbasierten Warnmeldungsgruppen anzeigen
- Links zwischen Warnungen in CMDB-basierten Warnmeldungsgruppen anzeigen
- Links zwischen Warnungen in auf Datenverkehr basierenden Warnmeldungsgruppen im Netzwerk anzeigen

Zugehörige Informationen

Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

Links zwischen Warnungen in Tag-basierten Warnmeldungsgruppen anzeigen

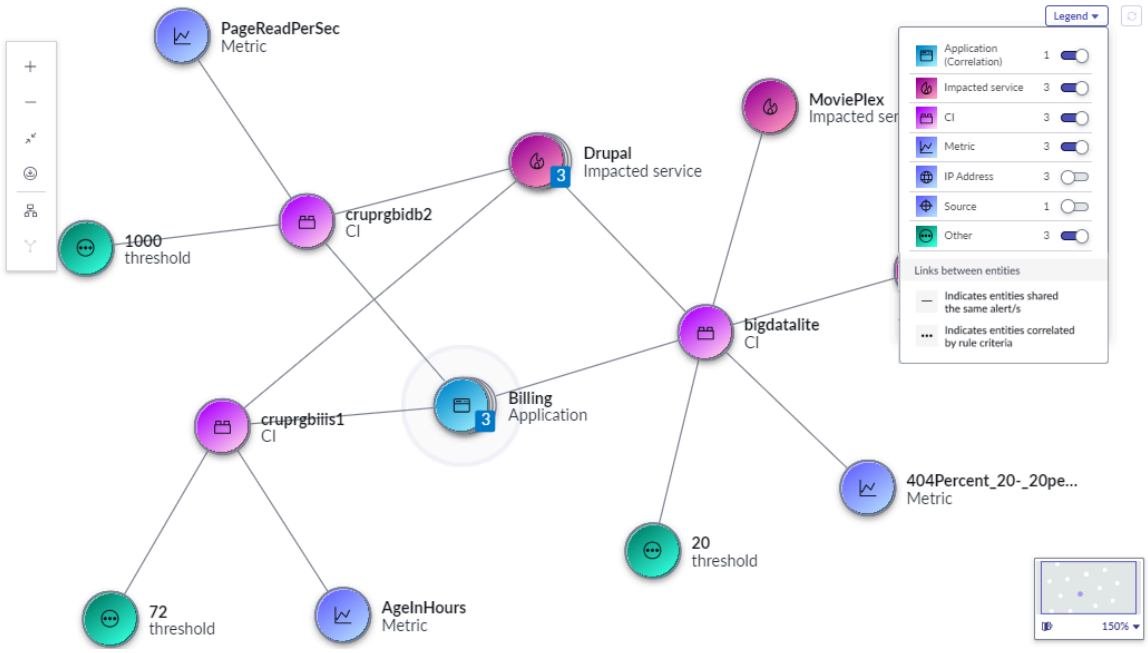
Zeigen Sie mithilfe der Linkansicht die Verbindungen zwischen Warnungen in einer Tag-basierten Warnungsgruppe in Express-Liste an. Die Linkansicht zeigt, wie die Attribute der Warnungen in der Gruppe miteinander verknüpft sind.

Wenn Sie Warnungs-Tags festgelegt haben und Ereignismanagement eine Warnungsgruppe basierend auf Tag-basierten Regeln generiert hat, bietet die Linkansicht eine visuelle Darstellung der Beziehungen zwischen den Warnungen in der Gruppe. Die farbigen Tags in der Ansicht stehen für Configuration Items (CIs) und andere Umgebungselemente im Zusammenhang mit den Warnungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine Tag-basierte Warnmeldungsgruppe in der Linkansicht



In diesem Beispiel ist das definierende Tag für die Korrelation Application (Anwendung) mit den Tags der relevanten CIs verknüpft. Eine Korrelation kann jedoch durch ein beliebiges Tag oder eine Kombination aus zwei Tags definiert werden, z. B. Ressourcen- und Metrikname. Wenn in der Linkansicht das definierende Tag fehlt, basierte die Korrelation auf Informationen, die nicht in der Ansicht dargestellt werden, z. B. die Beschreibung. Jeder CI-Knoten ist weiter mit den Tags verknüpft, die in derselben Warnung wie dieses CI angezeigt wurden.

In einer Warnmeldungsgruppe, die aus Tag-Regeln generiert wurde, bedeuten Knoten, die mit einer gestrichelten Linie verbunden sind, eine ungefähre, „unscharfe“ Übereinstimmung. Dies bedeutet, dass die Knoten korreliert wurden, wenn die Übereinstimmung mit der Tag-Regel nicht genau, aber nahe genug war, um signifikant zu sein. Dies kann beispielsweise passieren, wenn ein Standort, eine E-Mail-Adresse oder ein IP-Muster ähnlich genug sind, um als Übereinstimmung zu gelten.

Die Legende der Linkansicht listet die Bedeutung der Symbole und Farben auf, die zur Darstellung der Tags verwendet werden, und die Anzahl der eindeutigen Knoten. In der Legende sind definierende Tags als Korrelation gekennzeichnet. Sie können zwischen dem Ein- und Ausblenden von Tag-Typen umschalten, um das Rauschen zu reduzieren. Eine Beschreibung der einzelnen Tags finden Sie unter Attribute in der Linkansicht Express-Liste ..

Zugehörige Informationen

Links zwischen Warnungen in Warnmeldungsgruppen in anzeigen Express-Liste

Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

Links zwischen Warnungen in regelbasierten Warnmeldungsgruppen anzeigen

Zeigen Sie mithilfe der Linkansicht die Verbindungen zwischen Warnungen in einer regelbasierten Warnmeldungsgruppe in Express-Liste an. Die Linkansicht zeigt, wie die Attribute der Warnungen in der Gruppe miteinander verknüpft sind.

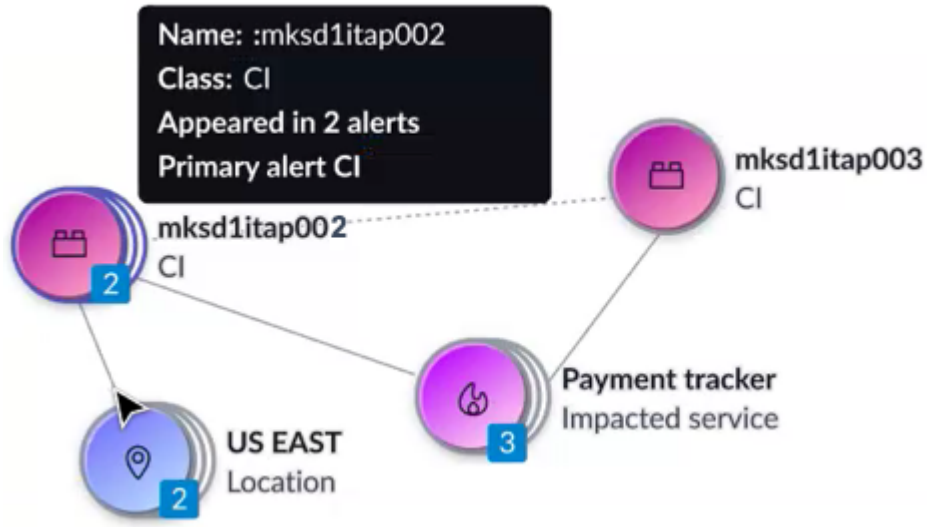
Wenn Sie Warnungsregeln festgelegt haben und Ereignismanagement basierend auf diesen Regeln eine Warnmeldungsgruppe generiert hat, bietet die Linkansicht eine visuelle Darstellung der Beziehungen zwischen den Warnungen in der Gruppe. Die farbigen Tags

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in der Ansicht stehen für Configuration Items (CIs) und andere Umgebungselemente im Zusammenhang mit den Warnungen.

Beispiel für eine regelbasierte Warnmeldungsgruppe in der Linkansicht



Regelbasierte Warnmeldungsgruppen bestehen aus einer primären Warnung und mindestens einer sekundären Warnung. Die primäre Warnung wird direkt generiert und in der Linkansicht als Startknoten dargestellt. Sekundäre Warnungsknoten sind durch eine gestrichelte Linie mit dem Startknoten verbunden. Dies zeigt an, dass sie nicht dieselbe Warnung teilen, aber mithilfe von Regelkriterien korreliert sind. Eine durchgezogene Linie zwischen den Knoten zeigt an, dass die verbundenen Knoten dieselbe Warnung oder mehrere Warnungen gemeinsam verwenden.

Wenn sich eine Warnung für ein CI auf einen Service in Configuration Management Database (CMDB)auswirkt, zeigt die Linkansicht den betroffenen Service an. So können Sie ihn für eine schnelle Selektierung auf einen Blick anzeigen. Wenn Sie den Mauszeiger über einen Knoten bewegen, wird ein Tooltip angezeigt, der den Namen des Tags, seinen Typ, die Anzahl der Warnungen, in denen es angezeigt wurde, und ob es sich um eine primäre oder sekundäre Warnung handelt.

Zugehörige Informationen

Links zwischen Warnungen in Warnmeldungsgruppen in anzeigen Express-Liste

Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

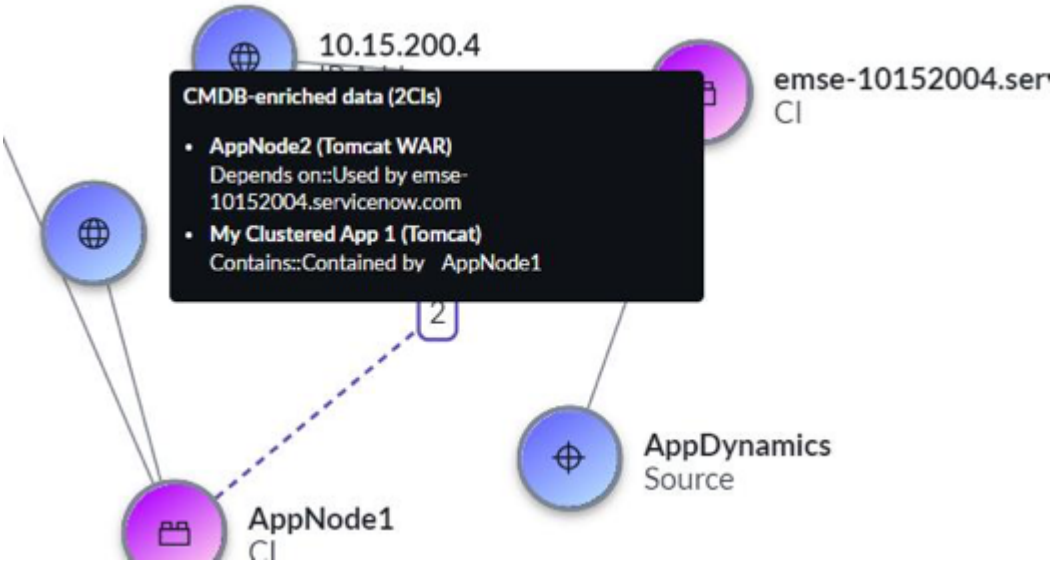
Links zwischen Warnungen in CMDB-basierten Warnmeldungsgruppen anzeigen

Zeigen Sie die Verbindungen zwischen Warnungen in -Warnungsgruppen in Express-Liste an, die basierend auf der Nähe von Configuration Items (CIs) in Configuration Management Database (CMDB)erstellt wurden. Die Linkansicht zeigt, wie die Attribute der Warnungen in der Gruppe miteinander verknüpft sind.

Wenn innerhalb eines bestimmten Zeitrahmens Warnungen für CIs auftreten, die sich in der Topologie CMDB nahe beieinander befinden, generiert Ereignismanagement eine CMDB-basierte Warnmeldungsgruppe. Ereignismanagement korreliert CIs in einer Servicezuordnung, wenn sie durch maximal drei andere CIs getrennt sind. Die farbigen Tags in der Linkansicht bieten eine visuelle Darstellung der CIs und anderer Umgebungselemente in Bezug auf die Warnungen in der Gruppe.

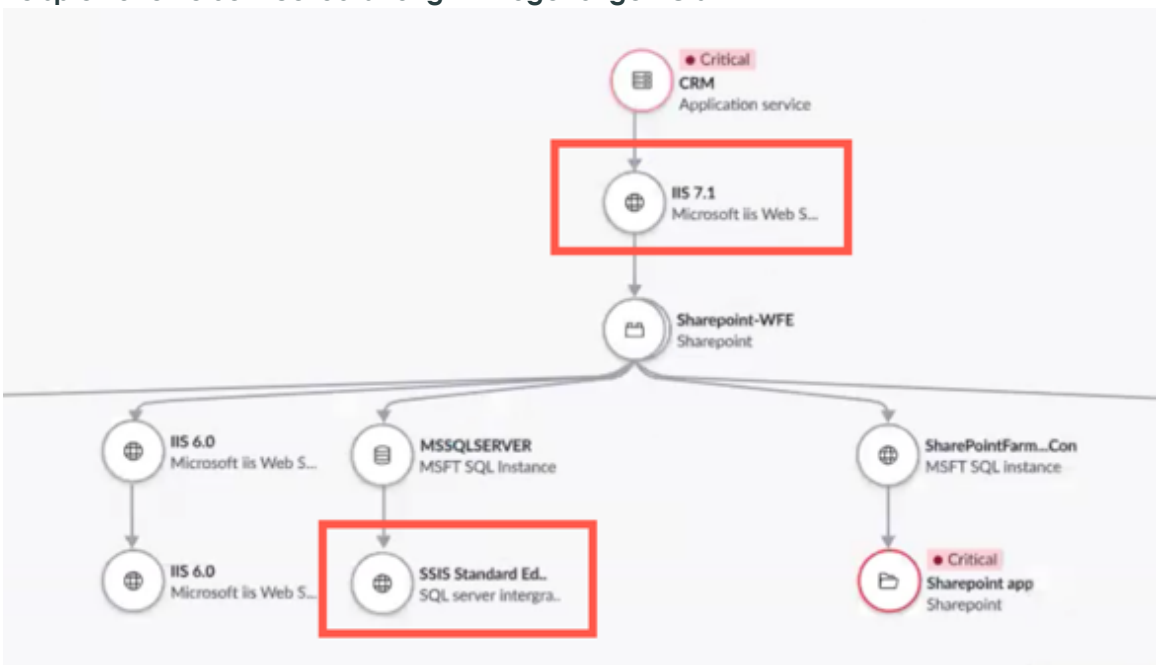
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine CMDB-basierte Warnmeldungsgruppe in der Linkansicht



In dieser Beispiel-Linkansicht einer CMDB-basierten Warnmeldungsgruppe zeigt die gestrichelte Linie mit der Zahl 2 zwischen den CIs an, dass die CIs nicht direkt verbunden sind, aber durch zwei CIs in der Servicezuordnung in der Topologie CMDB getrennt sind. Die Beispielservicezuordnung CMDB zeigt auch korrelierte CIs, die durch zwei CIs getrennt sind.

Beispiel für eine Servicezuordnung mit zugehörigen CIs



Zugehörige Informationen

Links zwischen Warnungen in Warnmeldungsgruppen in anzeigen Express-Liste

Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

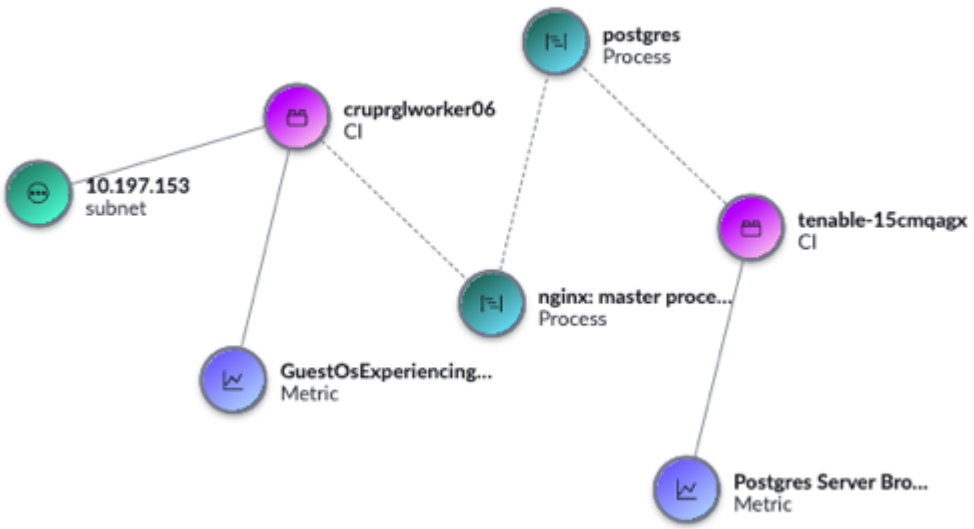
Links zwischen Warnungen in auf Datenverkehr basierenden Warnmeldungsgruppen im Netzwerk anzeigen

Zeigen Sie mithilfe der Link-Ansicht die Verbindungen zwischen Warnungen in auf Netzwerkdatenverkehr basierenden Warnungsgruppen in Express-Liste an. Auf Netzwerkverkehr basierende Warnmeldungsgruppen werden erstellt, indem die Verbindungen des Netzwerkverkehrs zwischen Prozessen auf allen Hosts analysiert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Durch ML-Service-Mapping identifizierte Servicekandidaten gruppieren Warnungen basierend auf Netzwerkdatenverkehrsverbindungen zwischen Prozessen. Die Linkansicht zeigt eine kontextbezogene Ansicht der Netzwerk-Incidents basierend auf diesen Gruppen direkt verbundener Prozesse. Servicekandidaten sind potenzielle Sammlungen von Prozessen in Ihrer IT-Umgebung, die basierend auf ihren Netzwerkverbindungen und Interaktionen identifiziert werden.

Beispiel für eine auf Datenverkehr basierende Warnmeldungsgruppe in der Linkansicht



In dieser Beispiel-Linkansicht einer auf Netzwerkdatenverkehr basierenden Warnmeldungsgruppe zeigen die gestrichelten Linien an, dass verbundene Prozesse für die CIs ausgeführt werden. Attribute, die mit einer durchgezogenen Linie verknüpft sind, teilen eine oder mehrere Warnungen.

Zugehörige Informationen

Links zwischen Warnungen in Warnmeldungsgruppen in anzeigen Express-Liste

Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

Zeigen Sie Links zwischen Warnungen in einer Gruppe in an Express-Liste

Wenn eine Warnungsgruppe generiert wird, können Sie anhand einer visuellen Darstellung ihrer Beziehungen in der Linkansicht besser nachvollziehen, wie die Warnungen in der Gruppe verknüpft sind.

Vorbereitungen

Eine Übersicht über die Link-Ansicht in Express-Listefinden Sie unter Links zwischen Warnungen in Warnmeldungsgruppen in anzeigen Express-Liste.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol Express-Liste ( ).
3. Wählen Sie in den Feldern im interaktiven Filterbereich **Gruppe** und dann das Kontrollkästchen für die Warnungsgruppen aus, die Sie anzeigen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Derzeit wird die Linkansicht für tagbasierte, regelbasierte, CMDB-basierte und netzwerkdatenverkehrsbasierte Warnmeldungsgruppen unterstützt.

- **Tag-Cluster**
- **Regelbasiert**
- **CMDB**
- **Netzwerkverkehr**

4. Wählen Sie in der Liste **Aktive Warnungen** die Beschreibung einer Warnungsgruppe aus. Der Vorschaubereich wird auf der Registerkarte **Warnungen in Gruppe** geöffnet, auf der alle zugehörigen Warnungen in der ausgewählten Gruppe aufgelistet sind.
5. Navigieren Sie zu **Linkansicht**.
6. Zeigen Sie die Beziehungen zwischen allen Warnungen in der ausgewählten Gruppe an.
7. Wahlweise: Führen Sie die folgenden optionalen Aufgaben aus.

Aufgabe	Aktion
Konzentrieren Sie sich auf einen Interessenbereich	Wählen Sie einen oder mehrere Knoten aus, und ordnen Sie sie in der Link-Ansicht neu an, indem Sie sie an eine neue Position ziehen. **Hinweis:** Nach dem Aktualisieren der Warnmeldungsgruppe werden die Knoten wieder an ihrer ursprünglichen Position angezeigt.
Aktualisieren Sie die Warnmeldungsgruppe	Wählen Sie **Aktualisieren**aus. Wenn Sie die Warnmeldungsgruppe aktualisiert haben, werden neu angeordnete Knoten wieder an ihrer ursprünglichen Position angezeigt. Neu hinzugefügte Knoten werden als Neu markiert. **Hinweis:** Die Schaltfläche **„Aktualisieren“** ist aktiviert, wenn neue Daten für die Warnmeldungsgruppe verfügbar sind. Die Linkansicht wird nicht automatisch aktualisiert.
Zeigen Sie die Bedeutung von Symbolen und Farben an	Wählen Sie die Legende der Linkansicht aus. (Optional) Die Legende gibt auch die Anzahl der eindeutigen Knoten an, die pro Tag angezeigt werden. Eine Beschreibung der einzelnen Tags finden Sie unter Attribute in der Linkansicht Express-Liste ..

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

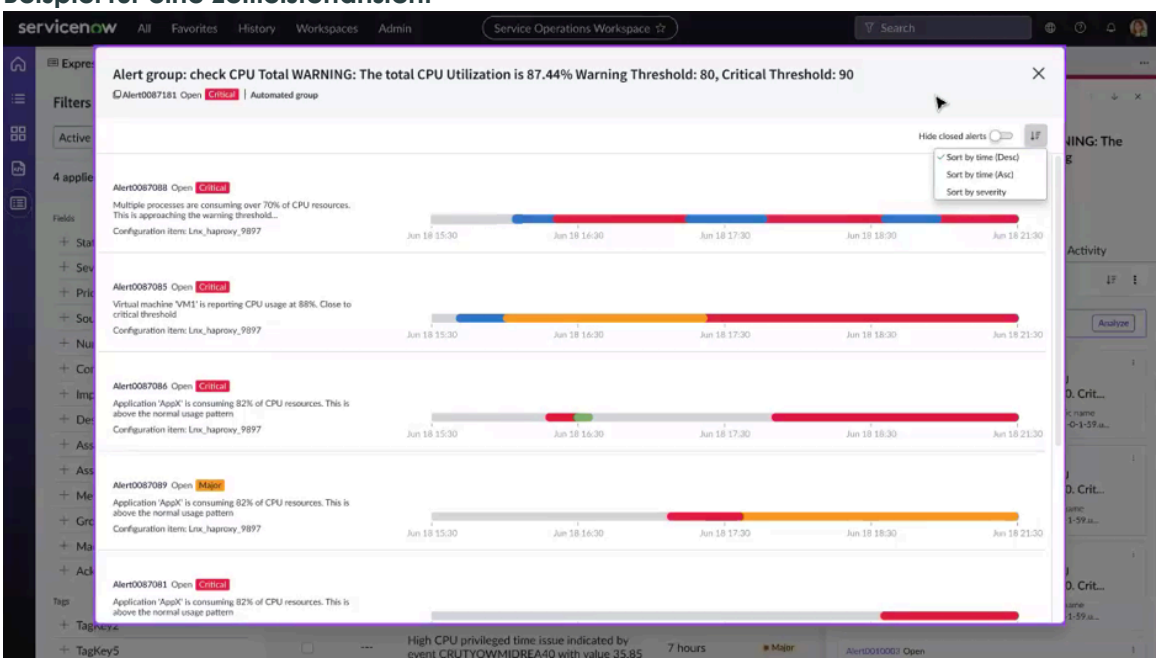
Aufgabe	Aktion
Reduzieren Sie das Rauschen	Schalten Sie in der Legende der Linkansicht zwischen dem Ein- und Ausblenden eines Tag-Typs um.
Zeigen Sie Informationen zu einer Warnung an	Bewegen Sie den Mauszeiger über einen Knoten, um einen Tooltip mit Informationen anzuzeigen.

Durchsuchen von chronologischen Daten zu den Warnungen in einer Warnmeldungsgruppe in Express-Liste

Visualisieren Sie die chronologische Abfolge von Ereignissen innerhalb einer Warnmeldungsgruppe in Express-Liste mithilfe der Zeitleistenansicht. Diese Funktion bietet einen umfassenden Überblick darüber, wann die Warnungen aufgetreten sind, wie sich der Schweregrad geändert hat, und andere relevante Daten für eine effiziente Selektierung und die durchschnittliche Zeit bis zur Lösung (Mean Time to Resolution, MTTR).

In der Zeitleistenansicht wird jede Warnung durch einen Balken dargestellt, sodass Sie die Reihenfolge des Auftretens, Schweregradübergänge und den Abschlussstatus schnell erkennen können. Die Zeitleiste beginnt mit der Erstellung der ersten Warnung und wird bis zum aktuellen Zeitpunkt fortgesetzt.

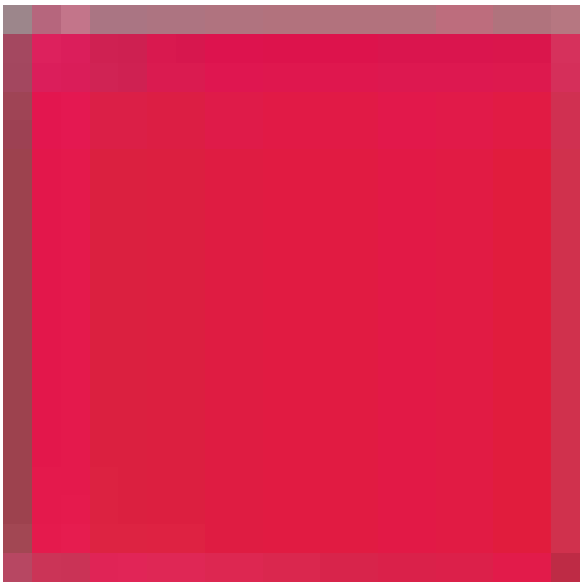
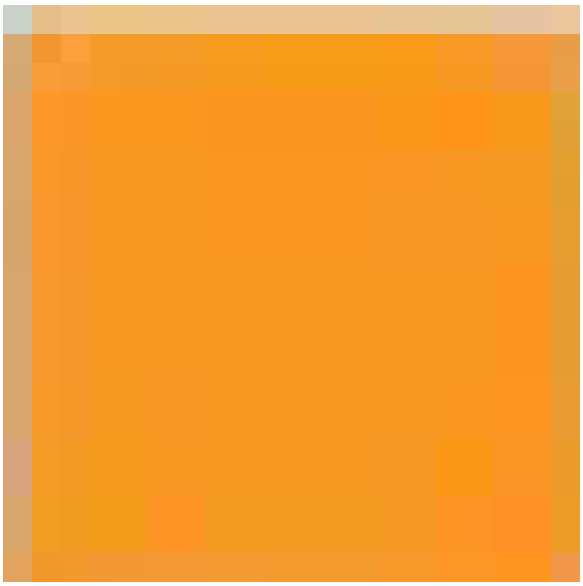
Beispiel für eine Zeitleistenansicht



In den Balken werden Standardschweregradfarben verwendet, wobei grauen Segmente Zeiträume vor dem Erstellen der Warnung oder nach dem Schließen anzeigen. Wenn Sie den Mauszeiger über einen Schweregradbalken bewegen, wird ein Tooltip mit den wichtigsten Warnungsdetails angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

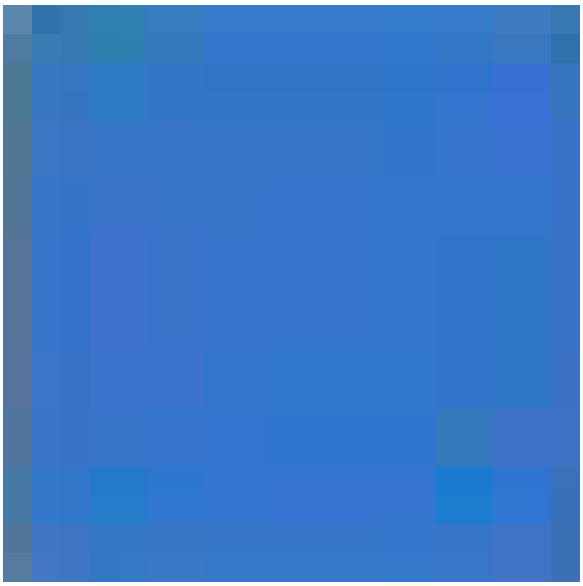
Schweregradbereich nach Farbe in der Zeitleistenansicht

Farbe	Schweregrad
	Kritisch
	Hoher

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

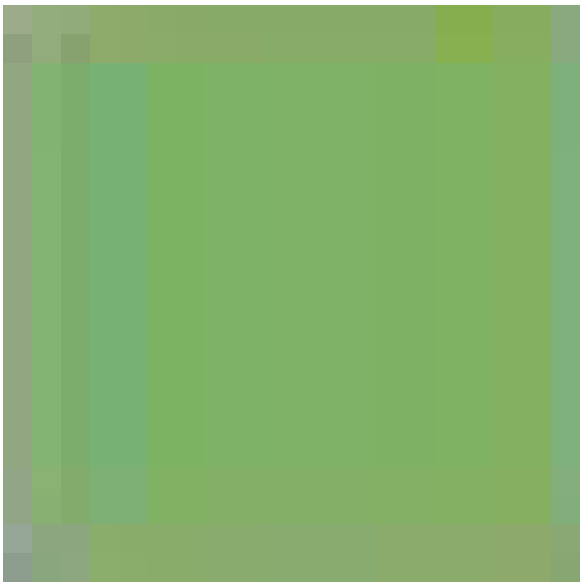
Schweregradbereich nach Farbe in der Zeitleistenansicht (Fortsetzung)

Farbe	Schweregrad
	Geringer
	Warnung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schweregradbereich nach Farbe in der Zeitleistenansicht (Fortsetzung)

Farbe	Schweregrad
	OK

Der Titel der Zeitleistenansicht für eine Warnmeldungsgruppe fasst die Beschreibung, Nummer, den Status, den Schweregrad und den Gruppierungstyp der Gruppe zusammen, abgeleitet von der primären Warnung. Für jede Warnung in der Gruppe werden detaillierte Informationen wie Warnungsnummer, Status, Schweregrad, eine kurze Beschreibung und das zugehörige Configuration Item (CI) oder Knoten (falls verfügbar) angezeigt.

Zugehörige Informationen

Zeigen Sie eine Zeitleiste der Warnungen in einer Warnmeldungsgruppe an

Zeigen Sie eine Zeitleiste der Warnungen in einer Warnmeldungsgruppe an

Erhalten Sie Einblicke in die Reihenfolge der Ereignisse im Zusammenhang mit einem Problem, indem Sie chronologische Informationen der Warnungen in einer Warnmeldungsgruppe in Express-Listeanzeigen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol Express-Liste ( ).
3. Wählen Sie in der Liste Aktive Warnungen für eine Warnung das Informationssymbol (.
4. Wählen Sie auf der Registerkarte Warnungen des Vorschaubereichs **die Zeitleistenansicht**aus.
5. Analysieren Sie die in der Zeitleistenansicht bereitgestellten Informationen.
6. Wahlweise: Sortieren Sie die angezeigten Warnungen nach aufsteigender oder absteigender Zeit oder nach Schweregrad.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie das Sortiersymbol ( ).

b. Wählen Sie die bevorzugte Sortieroption aus dem Popup-Menü aus.

7. Wahlweise: Zeigen oder verbergen Sie geschlossene Warnungen, indem Sie den Schieberegler **Geschlossene Warnungen ausblenden** umschalten.

Zugehörige Informationen

Durchsuchen von chronologischen Daten zu den Warnungen in einer Warnmeldungsgruppe in Express-Liste

Suchen Sie mithilfe der Freitextsuche nach Warnungsdatensätzen in Express-Liste .

Führen Sie eine Freitextsuche nach Warnungsdatensätzen in einer gefilterten Liste von Warnungen durch.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Ereignismanagement durchsucht die Warnungen, die derzeit in Express-Liste angezeigt werden, basierend auf den von Ihnen festgelegten Filtern und dem von Ihnen festgelegten Zeitbereich. Es durchsucht die folgenden vordefinierten Felder (auch wenn sie nicht sichtbar sind): Metrikname, Knoten, Warnungsnummer, Warnungstags und Beschreibung. Der eingegebene Text wird als einzelne Zeichenfolge und nicht als einzelne Wörter behandelt.

Die Ergebnisse entsprechen sowohl den von Ihnen angewendeten Filtern als auch der Zeichenfolge, die Sie in das Suchfeld eingegeben haben. In den resultierenden Warnungsdatensätzen wird die gesamte gesuchte Zeichenfolge hervorgehoben, und die verfügbaren Filter zeigen die Anzahl der Datensätze an, die mit der Zeichenfolge übereinstimmen. Letzte Suchvorgänge werden gespeichert und sind über das Suchfeld zugänglich.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.

2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).

3. Geben Sie im Feld Suchen den Freitext ein, nach dem gesucht werden soll.
Die Freitextzeichenfolge muss zwischen 3 und 50 Zeichen lang sein. Bei der Suche wird nicht zwischen Groß- und Kleinschreibung unterschieden.

4. Wählen Sie das Häkchen-Symbol , oder drücken Sie **die Eingabetaste**, um die Suche durchzuführen.

Aktionen zum Beheben von Warnungsproblemen in Service Operations-Arbeitsbereich für ITOMausführen

Beheben Sie das zugrunde liegende Problem einer Warnung, indem Sie vordefinierte Korrekturaufgaben ausführen, um eine schnellere Problemlösung und eine konsistente Lösung sicherzustellen.

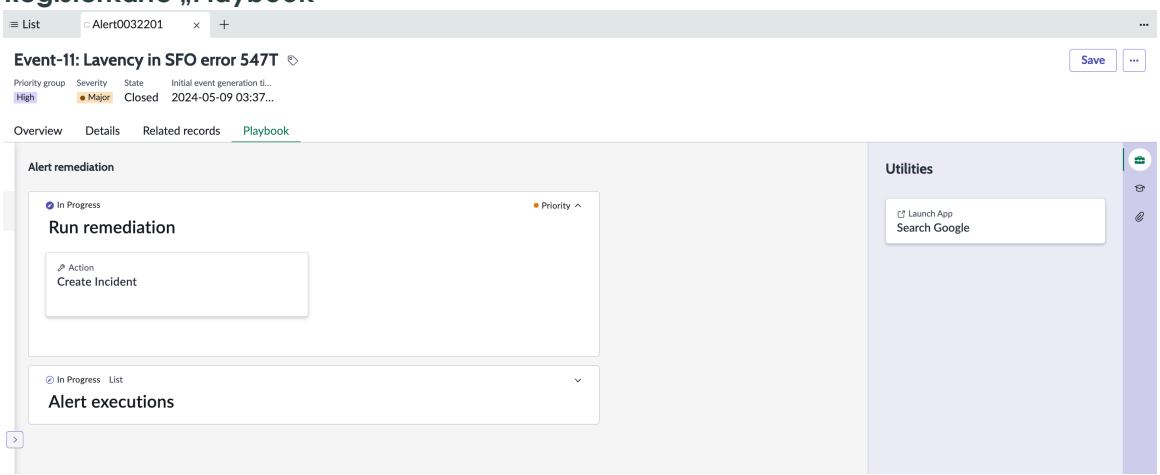
Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
   Die Warnung wird auf einer separaten Registerkarte geöffnet und zeigt die Registerkarte **Übersicht** an.
4. Wählen Sie **Playbook starten aus**.
5. Wählen Sie die Registerkarte **Playbook** aus.
   Auf der Karte **„Korrektur ausführen“** werden die verfügbaren Korrekturaktionen angezeigt.

Registerkarte „Playbook“



6. Wählen Sie die Kachel aus, die der Aktion entspricht, die Sie ausführen möchten.
   Die ausgewählte Aktion wird auf der Karte **Warnungsausführungen** angezeigt.

Ergebnisse

Wenn die Aktion abgeschlossen ist, wird sie unter dem Abschnitt „Warnungs-Fehlerkorrektur“ auf der Karte **Abgeschlossen** angezeigt.

Webanwendung für eine Warnung in Service Operations-Arbeitsbereich für ITOMstarten

Starten Sie eine Webanwendung, die in einer Warnungsverwaltungsregel konfiguriert wurde, um schnell auf die erforderlichen Tools zuzugreifen und Antwortzeiten und Effizienz zu verbessern.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

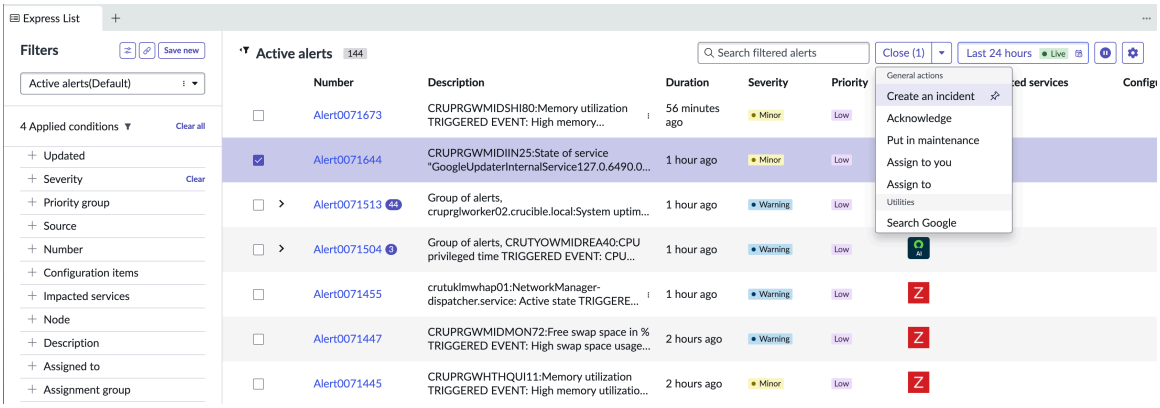
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.

   Die Warnung wird auf einer separaten Registerkarte geöffnet, auf der die untergeordnete Registerkarte **Übersicht** angezeigt wird. Im rechten Bereich ist standardmäßig die Registerkarte **Dienstprogramme** ausgewählt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie im Abschnitt „Dienstprogramme“ die Webanwendung aus, um sie zu starten.

Filtern der Warnungsanzeige im Bereich Express-Liste

Mit Filtern können Sie verschiedene Ansichten von kategorisierten Warnungen erstellen und eine gezielte Liste von Warnungen erstellen, die priorisiert und fokussiert werden sollen. So sparen Sie Zeit und minimieren Ablenkungen.

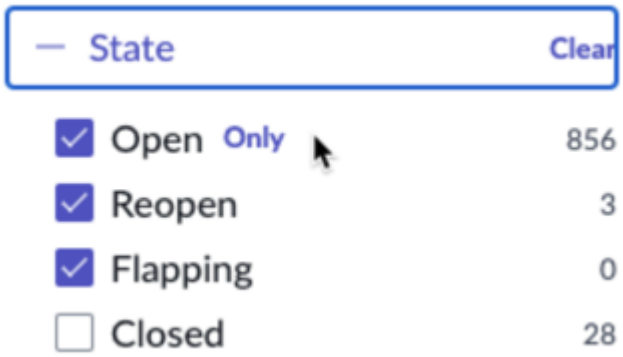
Mit den Feldern im interaktiven Filterbereich auf der linken Seite können Sie verschiedene Ansichten im Bereich Express-Liste erstellen. Standardfilter:

- Status
- Schweregrad
- Priorität
- Quelle
- Nummer
- Konfigurationselement
- Anzahl der betroffenen Services
- Knoten
- Beschreibung
- Zugewiesen an
- Zuweisungsgruppe
- Metrikname
- Gruppe
- Wartung

Sie können interaktiv anzeigen, was passiert, wenn Sie eines der Felder hinzufügen oder entfernen. Die Zahlen neben jedem Attribut geben die Anzahl der zurückgegebenen Warnungen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Im Filterbereich Express-Liste können Sie die folgenden Aktionen ausführen:

- Fügen Sie der Standardfilterliste Filter hinzu, oder entfernen Sie sie, um sich auf die angewendeten Filter zu konzentrieren. Die häufigsten Filter sind Status, Priorität, CI und Betroffene Services.
- Warnungs-Tags hinzufügen oder entfernen. Mit Tags können Sie Warnungen ohne Erkennung oder Zugriff auf die CMDB einfach identifizieren und gruppieren.
- Nach Zeichenfolgen-, Zahlen- oder Datumsattributen filtern.
- Speichern, löschen, als Standard zuweisen oder das Filterlayout freigeben.
- Warnungen herausfiltern oder anzeigen, die einer ausgewählten Warnung entsprechen.

Filtern Sie die Anzeige Express-Liste anhand von Attributen

Filtern Sie die Anzeige Express-Liste mithilfe des interaktiven Filterbereichs Express-Liste nach Text-, Zahlen- und Datumsattributen. Erstellen Sie eine gezielte Liste von Warnungen, um sie zu priorisieren und auf die Sie sich konzentrieren können.

Vorbereitungen

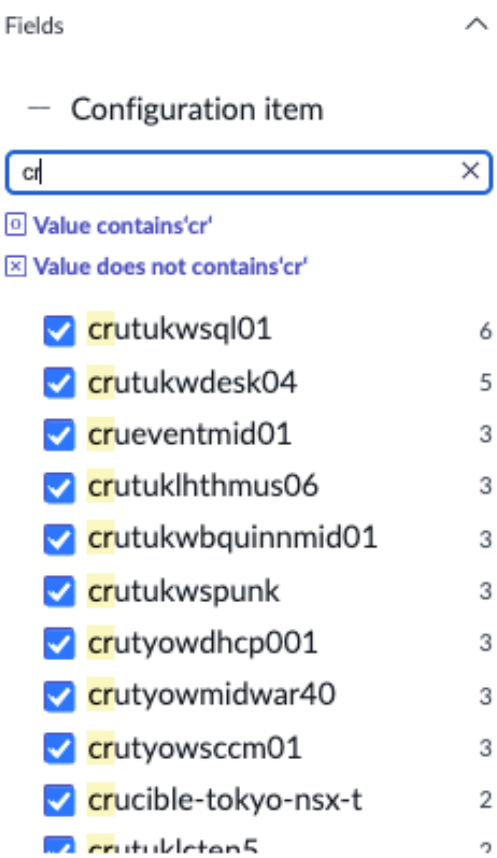
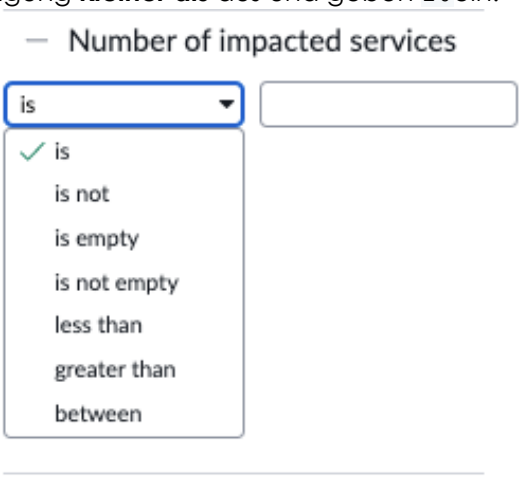
Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol für die Express-Liste ( ).
3. Wählen Sie im Bereich Filter auf der linken Seite je nach Filtertyp aus, ob nach Text-, Zahlen- oder Datumsattributen gefiltert werden soll.

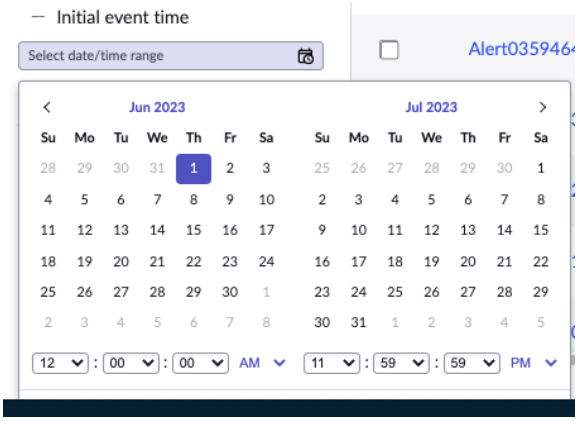
Filterattributtyp	Aktion
Text	Suchen Sie Elemente anhand des Namens, indem Sie die ersten Zeichen eingeben, um die Elemente anzuzeigen, die mit diesen Zeichen beginnen. Wählen Sie dann die Werte aus, die im Bereich

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filterattributtyp	Aktion
	Express-Liste angezeigt werden sollen. 
Anzahl der betroffenen Services	Geben Sie eine Bedingung ein, um Warnungen entsprechend der Anzahl der Warnungen im ausgewählten Filter anzuzeigen. Um beispielsweise Warnungen anzuzeigen, von denen weniger als 10 Services betroffen sind, wählen Sie die Bedingung **kleiner als** aus und geben `10`ein. 

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Filterattributtyp	Aktion
Datum	Zeigen Sie Warnungen gemäß dem ausgewählten Datums- und Uhrzeitbereich im Popup-Kalender im Bereich Express-Liste an. 

Filtern Sie die Anzeige Express-Liste durch Hinzufügen oder Entfernen von Feldern

Im Bereichsfilter Express-Liste mithilfe des interaktiven Filterbereichs Felder hinzufügen oder entfernen. Verwenden Sie Filter, um verschiedene Ansichten von kategorisierten Warnungen zu erstellen.

Vorbereitungen

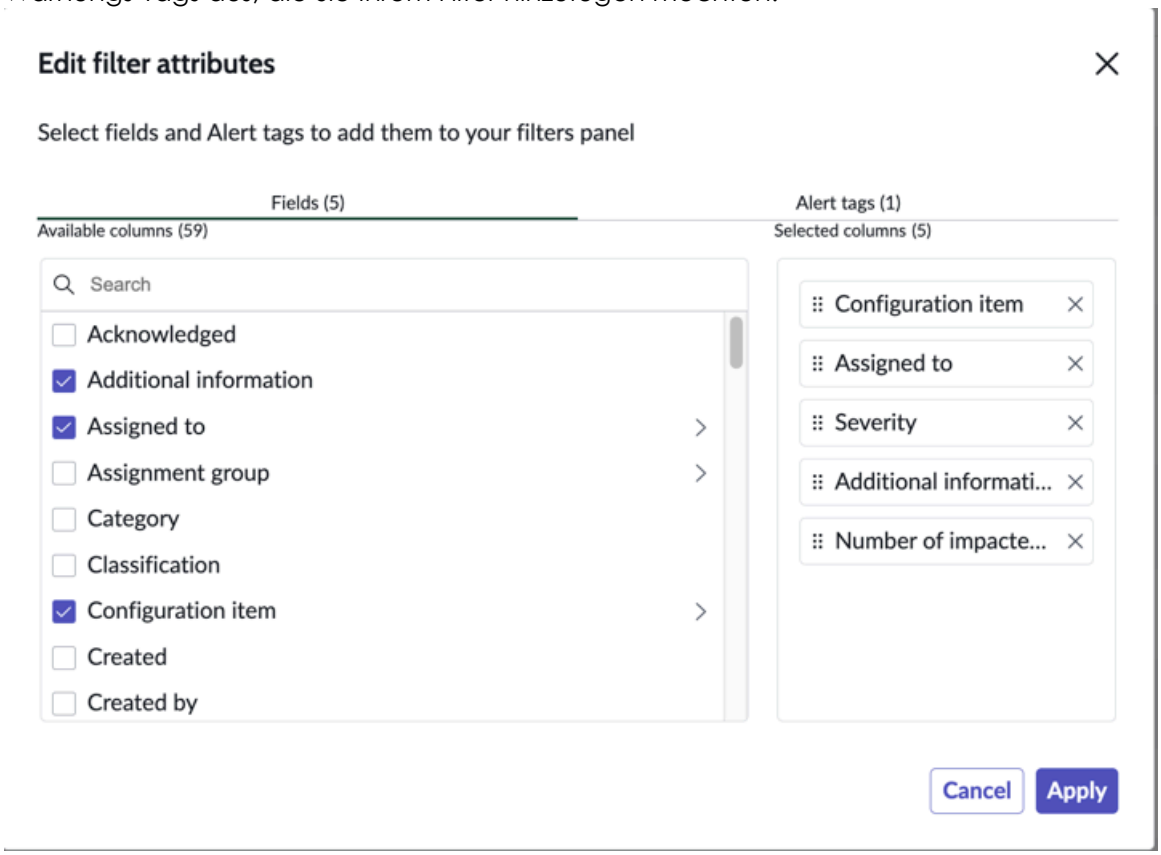
Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol für die Express-Liste ( ).
3. Wählen Sie im linken Filterbereich das Symbol Filterattribute bearbeiten ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie im Dialogfeld **„Filterattribute bearbeiten“** Felder oder Warnungs-Tags aus, die Sie Ihrem Filter hinzufügen möchten.



Die Registerkarte **Felder** wird standardmäßig angezeigt und zeigt die Anzahl der ausgewählten Felder an.

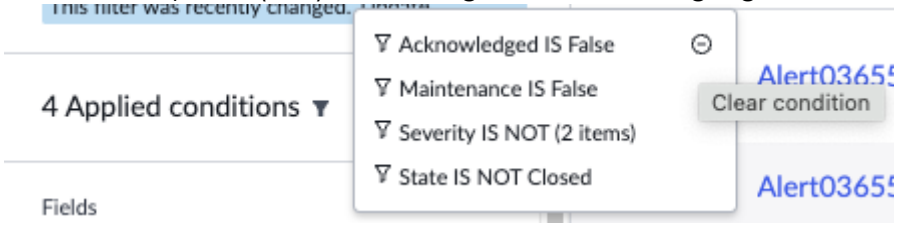
Die Anzahl der verfügbaren Felder wird oben in der Spalte neben **Verfügbare Spalten**angezeigt.

Die ausgewählten Felder werden in der rechten Spalte angezeigt. Die Anzahl der ausgewählten Spalten wird oben in der Spalte neben **Ausgewählte Spalten**angezeigt.

5. Wahlweise: Suchen Sie ein bestimmtes Feld, indem Sie dessen Namen in das **Suchfeld** eingeben.
6. Wahlweise: Ordnen Sie die Reihenfolge der ausgewählten Spalten neu an, indem Sie sie in der rechten Spalte nach oben oder unten ziehen.
7. Wahlweise: Entfernen Sie eine Spalte, indem Sie neben ihrem Namen das **X** wählen.
8. Wählen Sie **Übernehmen**.
9. Wahlweise: Löschen Sie einen Filter, indem Sie neben diesem Filternamen **Löschen** wählen. **„Löschen“** wird nur angezeigt, wenn Sie eines der Attributkontrollkästchen des ausgewählten Filters aktiviert oder deaktiviert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Wahlweise: Zeigen Sie die angewendeten Bedingungen an, indem Sie das Filtersymbol ( ) neben **Angewendete Bedingungen**wählen.



11. Wahlweise: Entfernen Sie eine Bedingung, indem Sie das Symbol **Bedingung löschen**( ) wählen.

Ergebnisse

Alle ausgewählten Felder werden im Bereich **Filter** in der Spalte **Felder** angezeigt.

Kategorisieren Sie die in angezeigten Warnungen Express-Liste

Erstellen Sie verschiedene Ansichten von Warnungen, indem Sie in Express-Liste Tags hinzufügen, damit Sie Warnungen ohne Discovery oder Zugriff auf die CMDB einfach identifizieren und gruppieren können.

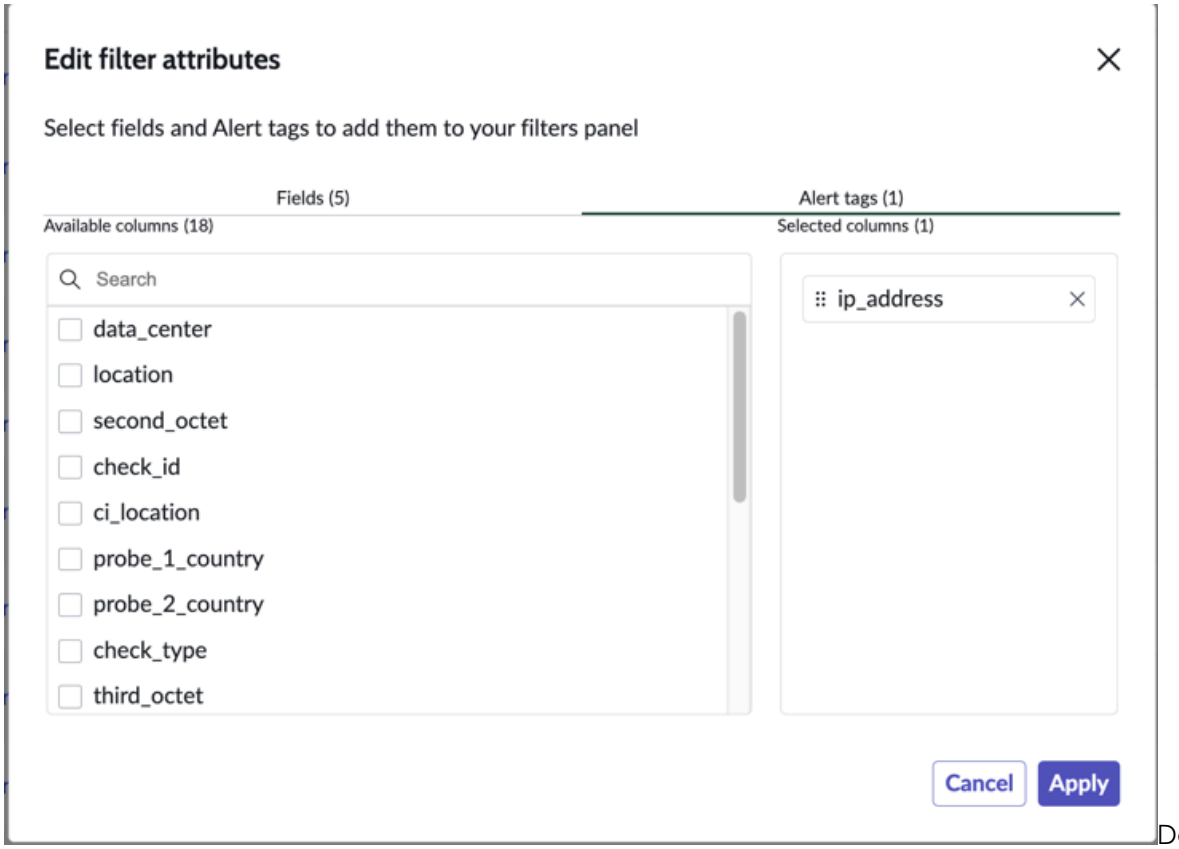
Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol für die Express-Liste ( ).
3. Wählen Sie im linken Filterbereich das Symbol **Filterattribute bearbeiten** ( ).
4. Wählen Sie im Dialogfeld **„Filterattribute bearbeiten“** die Registerkarte **Warnungs-Tags**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Titel der Registerkarte **Warnungs-Tags** zeigt die Anzahl der ausgewählten Warnungs-Tags an.

Die linke Spalte zeigt die Anzahl der verfügbaren Tags im Spaltentitel **Verfügbare Spalten** an.

Die ausgewählten Tags werden in der rechten Spalte angezeigt. Die Anzahl der ausgewählten Tags wird im Spaltentitel **Ausgewählte Spalten** angezeigt.

5. Wahlweise: Suchen Sie ein bestimmtes Tag, indem Sie dessen Namen in das **Suchfeld** eingeben.
6. Wahlweise: Ordnen Sie die ausgewählten Tags neu an, indem Sie sie in der rechten Spalte nach oben oder unten ziehen.
7. Wahlweise: Heben Sie die Auswahl eines Tags auf, indem Sie das (**X**) daneben auswählen.
8. Wählen Sie **Übernehmen**.

Ergebnisse
Alle ausgewählten Tags werden im Bereich **Filter** unter der Registerkarte **Warnungs-Tags** angezeigt.

Herausfiltern oder übereinstimmende Warnungen anzeigen

Erstellen Sie verschiedene Ansichten von kategorisierten Warnungen in Express-Liste, indem Sie Warnungen anzeigen oder herausfiltern, die einer ausgewählten Warnung entsprechen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol für die Express-Liste ( ).
3. Klicken Sie mit der rechten Maustaste auf eine Warnungszeile.
4. Übereinstimmungswarnungen abgleichen oder herausfiltern.
   - Zeigen Sie übereinstimmende Warnungen an, indem Sie im Kontextmenü **Übereinstimmungen anzeigen** wählen.
   - Filtern Sie übereinstimmende Warnungen heraus, indem Sie im Kontextmenü **Filter Out (Herausfiltern)** auswählen.

Speichern Sie einen anwenderdefinierten Filter in Express-Liste

Speichern Sie Ihre anwenderdefinierte Ansicht kategorisierter Warnungen in Express-Liste, um sie erneut zu verwenden, freizugeben oder als Standardansicht festzulegen. Beim Speichern Ihrer anwenderdefinierten Ansicht werden alle Filter, Tags und Bedingungen gespeichert.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator, evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol für die Express-Liste ( ).
3. Sobald Sie einen Filter eingerichtet haben, den Sie wiederverwenden, als Standardansicht festlegen oder für andere freigeben möchten, speichern Sie den Filter.
   Weitere Informationen zum Filtern der Warnungsanzeige Express-Liste finden Sie in den folgenden Themen:
   - Filtern Sie die Anzeige Express-Liste anhand von Attributen
   - Filtern Sie die Anzeige Express-Liste durch Hinzufügen oder Entfernen von Feldern
   - Herausfiltern oder übereinstimmende Warnungen anzeigen

   a. Wählen Sie in Express-Liste die **Option Neu speichern aus**.

   b. Geben Sie im Dialogfeld **„Neuen Filter speichern“** im Feld **Filtername** einen Namen für den Filter ein.

   c. Wahlweise: Machen Sie diesen Filter zu Ihrem Standardfilter, indem Sie **Als Standard festlegen**auswählen.

   d. Wählen Sie **Speichern**, um den Filter zu speichern.
4. Wahlweise: Geben Sie einen gespeicherten Filter frei, indem Sie den zugehörigen Link kopieren, um ihn an andere zu senden.

   a. Wählen Sie im Bereich **Filter** den Filter aus der Dropdown-Liste aus.

   b. Wählen Sie das Symbol „Link in Zwischenablage kopieren“ ( ).
5. Wahlweise: Legen Sie einen gespeicherten Filter als Standardfilter fest.

   a. Wählen Sie im Bereich **Filter** den Filter aus der Dropdown-Liste aus.

   b. Wählen Sie das Aktionssymbol Moder A( ) und anschließend **Als Standard festlegen**.
6. Wahlweise: Löscht einen gespeicherten Filter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie im Bereich **Filter** den Filter aus der Dropdown-Liste aus.

b. Wählen Sie das Aktionssymbol Moder A(⋮) und anschließend **Filter löschen**.

Anzeigen einer Warnungsgruppenanalyse durch Now Assist in Express-Liste

Zeigen Sie eine Analyse von Warnungsgruppen in Express-Listean, die von ServiceNow® Now Assist mithilfe von KI generiert wurde. Die Analyse hilft Ihnen, die Art der Warnungsgruppe, den Grund für die Korrelation der Warnungen in der Gruppe und das weitere Vorgehen im Nachbesserungsprozess besser zu verstehen.

Die KI-gesteuerte Warnungsgruppenanalyse bietet eine vereinfachte, visuell lesbare Beschreibung der Gruppe und technische Informationen, mit denen Sie sie effizienter untersuchen können. Die bereitgestellten Informationen basieren auf Beschreibungen und Configuration Item (CI)-Details, die sich auf die einzelnen Warnungen in der Gruppe beziehen. Die Warnmeldungsgruppenanalyse wird für die folgenden Warnmeldungsgruppentypen unterstützt:

Tag-basierte Warnmeldungsgruppen

Tags helfen bei der Kategorisierung von Warnungen basierend auf allgemeinen Attributen, z. B. betroffene Systeme oder Services. Warnungen in tagbasierten Warnmeldungsgruppen teilen bestimmte Tags, um auf Ähnlichkeiten bei den Problemen hinzuweisen. Die Warnungsanalyse für diese Gruppen enthält die gemeinsam genutzten Tags, die zur Korrelation der Warnungen in der Gruppe verwendet wurden. Sie gewährt auch Einblicke in die Gründe für die Gruppierung dieser Warnungen. Darüber hinaus bietet die Analyse Vorschläge für eine Vorgehensweise, basierend auf den Ähnlichkeiten zwischen den Tags.

CMDB-Warnungsgruppen

Wenn eine Warnung für ein CI in Configuration Management Database (CMDB)erstellt wird, sucht Ereignismanagement nach Warnungen in anderen CIs, die in der Topologie CMDB eng mit ihm verbunden sind. Eine offene topologische Beziehung zwischen CIs lässt auf eine gegenseitige Abhängigkeit zwischen Komponenten in der IT-Infrastruktur schließen und trägt zur Warnungskorrelation bei. Wenn eine Beziehung zwischen CIs gefunden wird, wird eine Warnmeldungsgruppe CMDB erstellt. Die -Warnungsanalyse für Warnmeldungsgruppen CMDB erläutert die Art der Gruppe und den Grund für ihre Bildung sowie die Beziehungen zwischen den CIs. Außerdem erhalten Sie technische Informationen, mit denen Sie entscheiden können, auf welche Warnungen sich die Untersuchung konzentrieren soll.

Log Analytics-Warnungsgruppen

Wenn Ereignismanagement mehrere Log Analytics -Warnungen identifiziert, die miteinander in wichtiger Beziehung stehen, werden sie in einer Gruppe Log Analytics gruppiert. Das System generiert eine Gruppe Log Analytics, wenn die Warnungen Log Analytics eine oder mehrere Beziehungen im Zusammenhang mit Zeit, Metadaten, Nachrichtentext und Trend teilen. Die -Warnungsanalyse für Warnmeldungsgruppen Log Analytics basiert auf der Analyse der von Health Log Analyticsbereitgestellten Anomalieinformationen und den Beschreibungen, CIs und Tags der Warnungen in der Gruppe.

Auf Netzwerkverkehr basierende Warnmeldungsgruppen

Die Methode zur auf Datenverkehr basierenden Warnungsgruppierung im Netzwerk gruppiert Warnungen, indem der Netzwerkverkehr zwischen Prozessen auf mehreren Hosts analysiert wird. Sie nutzt durch ML-Service-Mapping identifizierte Servicekandidaten, um die Warnungen zu gruppieren. Die Warnungsanalyse für auf Netzwerkdatenverkehr basierende Warnungsgruppen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

enthält eine Beschreibung für alle Warnungen in der Gruppe und die Verbindungen zwischen ihnen.

Anzeigen einer Warnungsgruppenanalyse von Now Assist in Express-Liste

Zeigen Sie eine von ServiceNow® Now Assist erstellte Warnmeldungsgruppenanalyse mit generativer KI an. Die Analyse bietet eine vereinfachte, visuell lesbare Beschreibung der Warnmeldungsgruppe und technische Informationen, mit denen Sie die Warnmeldungsgruppe effizienter untersuchen können.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in der Funktion Now Assist. Weitere Informationen finden Sie unter Installieren Sie das Plugin Now Assist for IT Operations Management (ITOM)..
- Zeigen Sie wichtige Informationen zur Anwendung ServiceNow® Now Assist für IT Operations Management (ITOM) in Now Assist für IT Operations Management (ITOM)an .

Hinweis: Derzeit analysiert Now Assist für ITOM nur Tag-basierte, regelbasierte, Log Analytics- und Netzwerkdatenverkehrskorrelations-Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol Express-Liste ( ) aus.
3. Wählen Sie in der Liste Aktive Warnungen das Informationssymbol ( ) links neben einer Warnungsgruppe, um den Vorschaubereich anzuzeigen.
4. Wählen Sie auf der Registerkarte „Info“ des Vorschaubereichs **Analysieren** in Warnungsanalyse nach Now Assistaus.
5. Zeigen Sie die in der Warnungsanalyse bereitgestellten Informationen an.

   Hinweis: Warnungsanalysen werden in englischer Sprache bereitgestellt, unabhängig davon, welche Sprache in den Warnungsbeschreibungen verwendet wird.

6. Wahlweise: Verwenden Sie die Warnungsanalysesymbole, um zugehörige Aufgaben auszuführen.

Symbole für Warnungsanalysen

Symbol	Beschreibung
	Kopieren Sie den Inhalt der Warnungsanalyse in die Zwischenablage.
	Aktualisieren Sie die Warnungsanalyse. **Hinweis:** Durch das Aktualisieren werden die Ergebnisse neu generiert. Vergangene Ergebnisse werden gelöscht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Anzeigen einer Warnungsgruppenanalyse durch Now Assist in Express-Liste

Aktualisieren Sie eine Warnungsbeschreibung in Express-Liste basierend auf der Analysezusammenfassung Now Assist .

Bei der Überprüfung von -Warnungsgruppen oder einzelnen Warnungen in Express-Listekönnen Sie die Warnungsbeschreibung auf eine visuell lesbare Zusammenfassung aktualisieren, die von Now Assistgeneriert wurde.

Warum und wann dieser Vorgang ausgeführt wird

Das Aktualisieren der Warnungsbeschreibung ist für die Warnungstypen verfügbar:

- Tag-basierte Warnmeldungsgruppe.
- Regelbasierte Warnmeldungsgruppe.
- CMDB-Korrelationswarnungsgruppe.
- Korrelationswarnmeldungsgruppe für Netzwerkdatenverkehr.
- Log Analytics für einzelne Warnungen und Warnungsgruppen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der Navigationsleiste das Symbol Express-Liste ( ) aus.
3. Wählen Sie in der Liste Aktive Warnungen das Informationssymbol ( ) einer Warnung.
4. Wählen Sie auf der Registerkarte „Info“ des Vorschaubereichs **Analysieren** in Warnungsanalyse nach Now Assistaus.
5. Überprüfen Sie die visuell lesbare, KI-generierte Zusammenfassung in der Warnungsanalyse.

   Hinweis: Die Warnungsanalyse wird in englischer Sprache bereitgestellt, unabhängig davon, welche Sprache in der Warnungsbeschreibung verwendet wird.

6. Wählen Sie auf der Registerkarte „Info“ des Vorschaubereichs **Beschreibung aktualisieren**, um die Beschreibung basierend auf dem Zusammenfassungsinhalt der Warnmeldungsgruppe zu aktualisieren.
   Der KI-generierte Zusammenfassungsinhalt ersetzt die ursprüngliche Beschreibung der Warnmeldungsgruppe.

Von verwendete Rollen Express-Liste

Detaillierte Informationen zu allen Rollen, die auf die Funktion Express-Liste in Service Operations-Arbeitsbereichzugreifen können.

Rollentitel	Beschreibung	Enthält Rollen
Event Management-Administrator [evt_mgmt_admin]	Hat Lese- und Schreibzugriff auf alle Ereignismanagement-Funktionen zum Konfigurieren von Ereignismanagement.	• evt_mgmt_user • template_editor_global

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel	Beschreibung	Enthält Rollen
	Hinweis: Seien Sie vorsichtig mit der Rolle evt_mgmt_admin, da sie zur Administratorrolle hochgestuft werden kann.	
Ereignismanagement-Operator [evt_mgmt_operator]	In Kombination mit den Berechtigungen evt_mgmt_user kann von auch Vorgänge für Warnungen wie Bestätigen, Schließen, Öffnen eines incident und Ausführen von Remediationen aktivieren.	evt_mgmt_user
Event-Teamoperator [evt_team_operator]	Verwaltet Vorgänge Ereignismanagement innerhalb eines bestimmten Teams, wie im Feld **Zuweisungsgruppe** definiert. Mit dieser Rolle kann der Bediener Warnungen ausschließlich für das ihm zugewiesene Team lesen und schreiben. Darüber hinaus kann der Operator Konfigurationsänderungen speziell für sein Team vornehmen, einschließlich Updates für Warnungsautomatisierung und Integrations Launchpad. **Hinweis:** Die Rolle evt_team_operator muss einer Zuweisungsgruppe zugewiesen werden, um Warnungen für diese Gruppe anzuzeigen und zu verwalten. Wenn die Rolle erstellt, aber keinen Gruppen zugeordnet ist, denen Warnungen zugewiesen sind, kann der Bediener keine Warnungen sehen.	
Ereignismanagement-Benutzer [evt_mgmt_user]	Hat schreibgeschützten Zugriff auf alle Funktionen Ereignismanagement von . Die enthaltene Rolle itil gewährt Zugriff auf die	ITIL

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel	Beschreibung	Enthält Rollen
	Verwaltung von Incidents, die aus Warnungen erstellt werden. Kann nur Express-Listeanzeigen.	
Event Management Integrator [evt_mgmt_integration]	Hat Zugriff auf die Tabellen Event [em_event] und Registered Nodes [em_registered_nodes], um sie mit externen Ereignisquellen zu integrieren.	

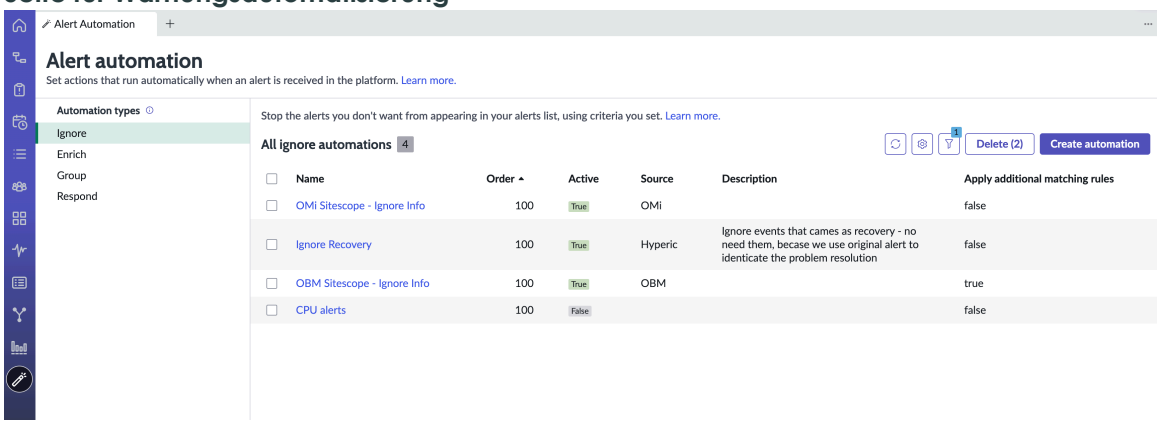
Warnungsautomatisierung in Service Operations-Arbeitsbereich für ITOM

Die Automatisierung von Warnungen ist von entscheidender Bedeutung, da Unternehmen mit einer steigenden Anzahl von Warnungen und komplexen IT-Infrastrukturen arbeiten müssen. Die manuelle Warnungsverarbeitung ist langsam, fehleranfällig und ineffizient, was den Bedarf an automatisierten Systemen unterstreicht. Automatisierung kann die durchschnittliche Zeit bis zur Lösung von Warnungen, die Servicezuverlässigkeit und die Personalressourcen besser skalieren.

Warnungsautomatisierungen unterstützen auch zentralisierte Administratoren und verteilte Teamrollen. Dadurch können qualifizierte Teams Selfservice-Instanzen durchführen und ihre eigenen Warnungsautomatisierungen erstellen. Beispielsweise können Sie Site Reliability Engineers (SREs) Zugriff gewähren. Mitglieder von Teams können Automatisierungen für ihr eigenes Team und ihre eigenen Warnungen verwalten, ohne andere Teams zu beeinträchtigen.

Für Anwender, die mit unserer klassischen Experience vertraut sind, bietet die Warnungsautomatisierung eine einfachere Anwenderoberfläche und besseren Teamsupport für Ereignisregeln, tagbasierte Clustering-Definitionen und Warnungsverwaltungsregeln. Einige erweiterte Funktionen sind derzeit nur für Administratoren in der klassischen Experience verfügbar. Diese beiden Experiences verwenden dieselben Back-End-Tabellen. Sie können die Experience verwenden, die für Sie am besten geeignet ist. Änderungen an einer Experience aktualisieren auch die andere.

Seite für Warnungsautomatisierung



Typen der Warnungsautomatisierung

Derzeit bietet Service Operations-Arbeitsbereich ITOM die folgenden Automatisierungstypen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Automatisierung ignorieren: Reduzieren Sie irrelevante oder falsch positive Warnungen, verwalten Sie die Warnungsermüdung effizient, indem Sie verrauschte Benachrichtigungen herausfiltern, und ermöglichen Sie Teams, sich auf kritische Probleme zu konzentrieren.
2. Automatisierung ergänzen: Rohwarnungen mit Kontextinformationen ergänzen, um sie informativer und umsetzbarer zu machen. Vereinfacht ausgedrückt bedeutet dies, dass die von Überwachungstools generierten Rohereignisse in ein gängiges Standardformat umgewandelt werden, um die automatisierte Gruppierung und Reaktion zu unterstützen.
3. Gruppenautomatisierung: Gruppieren Sie mehrere zugehörige Warnungen in einer einzigen primären Warnung, um das Warnungsrauschen zu reduzieren und die Ursache zu identifizieren.
4. Automatisierung der Reaktion: Reagieren Sie automatisch auf Warnungen, indem Sie die entsprechenden Stakeholder benachrichtigen, eskalieren Sie sie nach Bedarf, oder führen Sie Korrekturmaßnahmen aus. Legen Sie fest, wie und wann Warnungen basierend auf Schweregrad oder Typ eskaliert werden. Integrieren Sie in Drittparteisysteme, um Fälle zu erstellen und Benachrichtigungen zu senden oder Korrekturaktionen auszuführen.

Prozess-Flow der Warnungsautomatisierung

Sie können damit beginnen, indem Sie über das Integrations-Launchpad Warnungen oder Ereignisse von Überwachungssystemen an ServiceNow senden. Hier stellen Administratoren Verbindungen zwischen ServiceNow und Überwachungstools her. Diese Integrationen ermöglichen die Erfassung überwachter Daten und generieren Ereignisse aus Drittanbieterquellen.

Wenn Warnungen von ServiceNowempfangen werden, werden Warnungsautomatisierungen in der auf der Seite angezeigten Reihenfolge ausgeführt. Zuerst ignorieren wir Warnungen, um das Rauschen zu reduzieren. Als Nächstes ergänzen wir Warnungen mit zusätzlichem Kontext und gruppieren die Warnungen dann anhand des hinzugefügten Kontexts. Schließlich reagieren wir auf Warnungen, indem wir eskalieren oder Nachbesserungen durchführen. Für jeden Typ können mehrere Automatisierungen vorhanden sein. Jede Automatisierung wird basierend auf bestimmten Auslöserbedingungen ausgeführt und führt bestimmte Aktionen aus. Warnungen werden nur dann automatisiert, wenn sie empfangen werden. Wir wenden keine Automatisierungen auf vergangene Warnungen an.

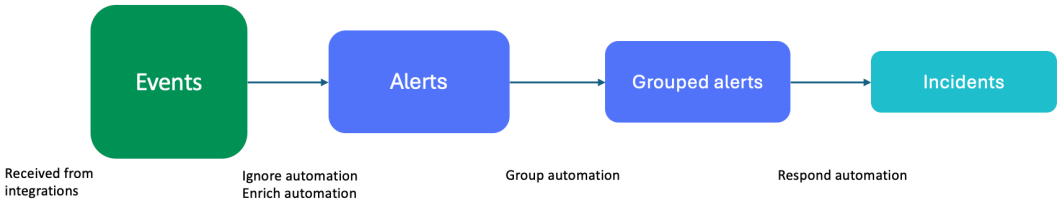
In der Warnungsanreicherungsphase fügen Administratoren Warnungen die erforderlichen Felder hinzu oder extrahieren sie aus Warnungen, um wichtige Informationen für eine schnelle Lösung bereitzustellen. Dadurch wird sichergestellt, dass Warnungen alle relevanten Details enthalten, die für eine effektive Reaktion auf Incidents erforderlich sind. Administratoren fügen Warnungen Kontext hinzu, indem sie sie ändern und normalisieren. Dies verbessert die Korrelation von Warnungen und erleichtert das Identifizieren von Mustern und potenziellen Bedrohungen.

Die angereicherten und zusammengestellten Warnungen werden dann auf Grundlage vordefinierter Kriterien gruppiert und zugehörige Warnungen konsolidiert. Dies reduziert die Ermüdung durch Warnungen und ermöglicht eine effiziente Nachbesserung. Schließlich lösen eskalierte Warnungen über verschiedene Kanäle Benachrichtigungen an Stakeholder aus, um eine rechtzeitige Kommunikation und Reaktion auf kritische Warnungen zu gewährleisten.

Das folgende Diagramm veranschaulicht diesen Prozessablauf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsautomatisierung: Reduzierung von Rauschen und Verbesserung der Lösungszeit



Dieser umfassende Prozess zur Automatisierung von Warnungen kann das Warnungsrauschen reduzieren, die durchschnittliche Zeit bis zur Lösung (Mean Time to Resolution, MTTR) verbessern, die Servicezuverlässigkeit erhöhen und die Produktivität der Mitarbeiter steigern.

Automatisierung für „Ignorieren“ erstellen

Die Automatisierung des Ignorierens optimiert den Prozess des Ignorierens irrelevanter oder falsch positiver Warnungen aus Überwachungssystemen und verwaltet die Warnungsermüdung effizient, indem unnötige Benachrichtigungen herausgefiltert werden. Dadurch können sich Teams auf kritische Probleme konzentrieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin oder srm_responder

Warum und wann dieser Vorgang ausgeführt wird

Automatisierungen ignorieren das Filtern von Warnungen aus Quellüberwachungssystemen, die bestimmten Bedingungen entsprechen. Separat ignoriert Ereignismanagement Warnungen, die ein doppeltes Nachrichtenschlüsselfeld haben oder bei denen der Schweregrad **Klar**ist.

Für Anwender, die mit der klassischen Ereignismanagement Experience vertraut sind, bieten Automatisierungen ignorieren eine einfachere Schnittstelle mit erweitertem Support für Teams im Abschnitt „Ereignisfilter“ von Ereignisregeln.

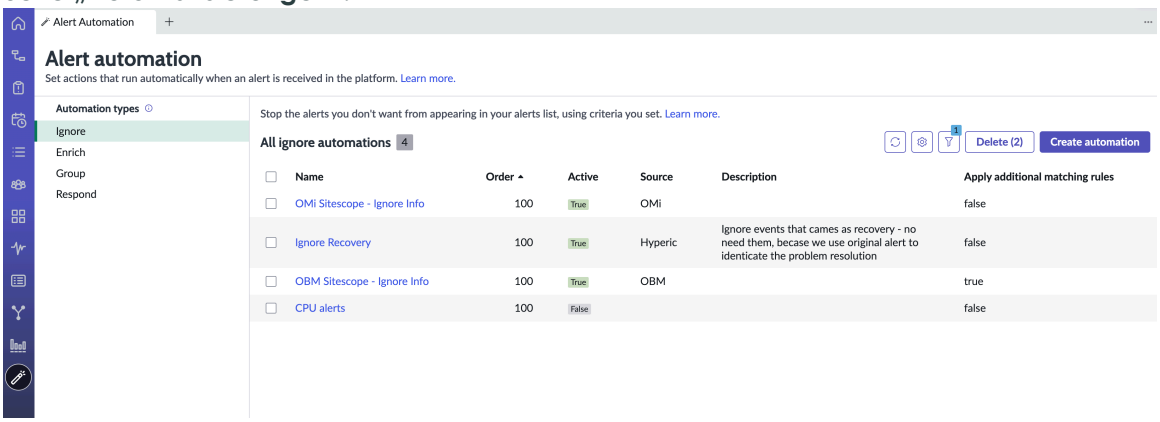
Hinweis: Warnungen vor dem Anreichern zu ignorieren, verbessert die Leistung und vereinfacht den Verarbeitungs-Flow. Der Bedingungsfilter in „Automatisierungen ignorieren“ gilt nur für das ursprüngliche Ereignis, nicht für das angereicherte. Ergänzungsautomatisierungen können verhindern, dass Automatisierungen zum Ignorieren ausgeführt werden, wenn **die Option „Andere Ergänzungswarnungsautomatisierungen nicht ausführen“** auf „falsch“ festgelegt ist, sie für dieselbe Quelle gelten, einen niedrigeren Wert haben und den Filterbedingungen entsprechen. Um Konflikte zu vermeiden, berücksichtigen Sie dies am besten beim Erstellen von Ergänzungen oder Ereignisregeln.

Prozedur

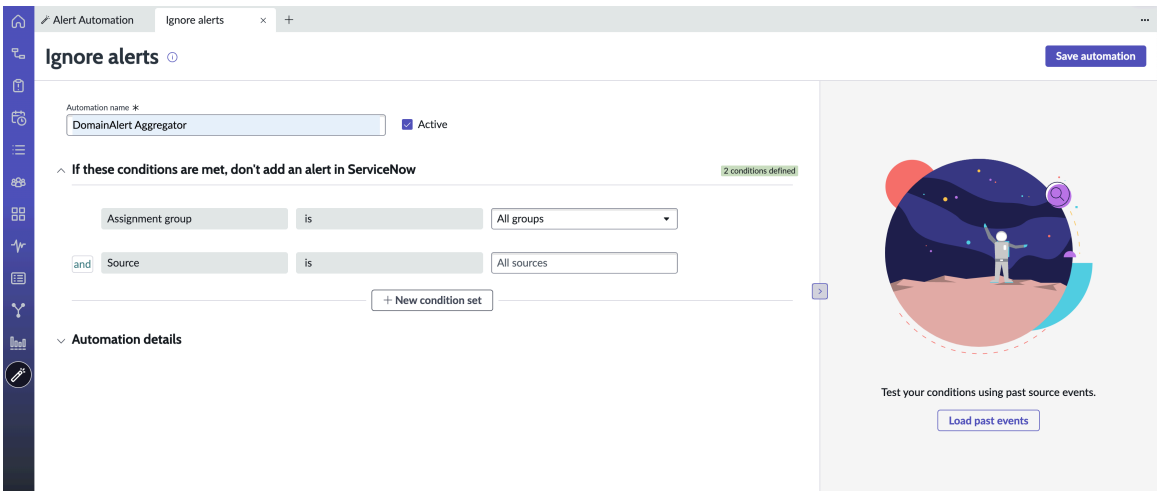
1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol für Warnungsautomatisierung ( ).
3. Wählen Sie auf der Seite „Warnungsautomatisierung“ unter **„Automatisierungstypen“**die Option **Ignorieren**aus.
   Die Seite „Warnungen ignorieren“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „Automatisierungen“.



4. Wählen Sie **Automatisierung erstellen aus**.



5. Geben Sie im Feld **Automatisierungsname** den Namen der Automatisierung für das Ignorieren von Warnungen ein.
6. Aktivieren Sie die Automatisierung, indem Sie den Umschalter **Aktiv** umschalten.
7. Richten Sie im Abschnitt **Wenn diese Bedingungen erfüllt sind, keine Warnung in ServiceNow hinzufügen** Sie Filterkriterien ein, um die Ereignisse zu identifizieren, die Sie erfassen möchten.
   a. Wählen Sie im Feldmenü **Zuweisungsgruppe** die Zuweisungsgruppe aus, um zu bestimmen, welche Teamwarnungen die Automatisierung auslösen.

      Die **Zuweisungsgruppe** stellt ein bestimmtes Team dar, das für die Bearbeitung bestimmter Warnungen verantwortlich ist. Durch die Auswahl einer Zuweisungsgruppe stellen Sie sicher, dass nur die Warnungen, die diesem bestimmten Team zugewiesen sind, die Automatisierung auslösen. Auf diese Weise ist die Automatisierung zielgerichtet und wird nur für relevante Warnungen aktiviert, die dem ausgewählten Team zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn Sie bei der Instanz mit einer Administratorrolle angemeldet sind (evt_mgmt_admin), sind alle Zuweisungsgruppen verfügbar. Darüber hinaus können Sie **Alle Gruppen** auswählen, um das Generieren von Warnungen für eine der verfügbaren Gruppen zu aktivieren.
- Wenn Sie ein Operator sind, ist nur die Gruppe verfügbar, der Sie angehören.
- Nur Mitglieder der ausgewählten Gruppe oder Administratoren können die Automatisierung aktualisieren oder löschen.

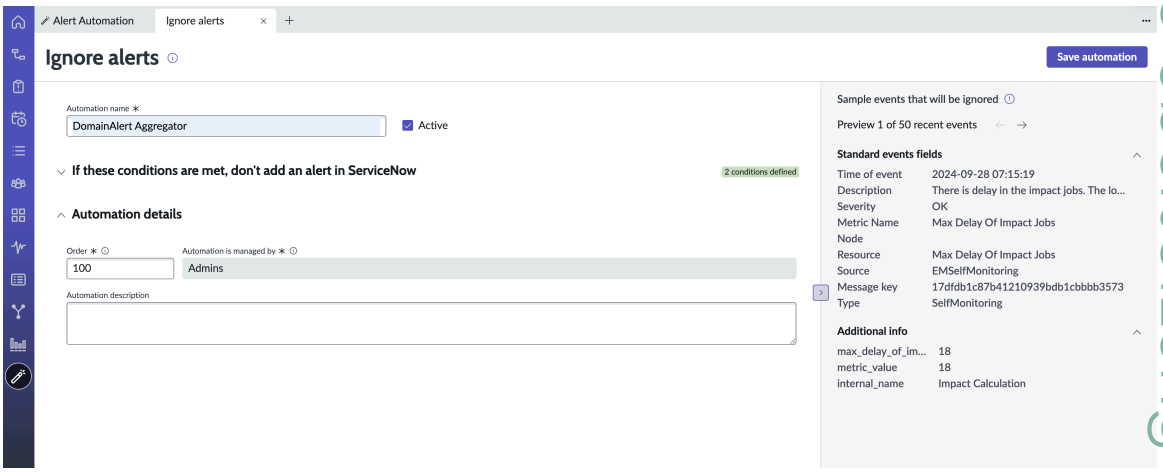
b. Wählen Sie im Menü **Quelle** das Überwachungstool aus, von dem aus die Warnung generiert wird.

c. Richten Sie die Bedingungen ein, indem Sie das Feld, den Operator und den Feldwert auswählen. Fügen Sie dann weitere Bedingungen mit ODER- oder UND-Operatoren hinzu.

Um einen weiteren Satz Bedingungen hinzuzufügen, wählen Sie **+ Neuer Bedingungssatz**aus. Sie können ein zusätzliches Informationsfeld auch manuell hinzufügen, wenn Sie es nicht in der Dropdown-Liste sehen.

8. Um zu überprüfen, ob Sie die richtigen Ereignisse ignorieren, oder um Beispiele für Felder anzuzeigen, die zum Festlegen der Bedingungen verwendet werden können, wählen Sie **Frühere Ereignisse laden**aus.
Sie können eine Vorschau der Details einiger vergangener Ereignisse anzeigen.

9. Geben Sie im Abschnitt **„Automatisierungsdetails“** eine Beschreibung für Reihenfolge und Automatisierung an.



a. Geben Sie im Feld **Reihenfolge** die Automatisierungsreihenfolge ein.

Hinweis: Automatisierungen werden in der Reihenfolge von der niedrigsten zur höchsten ausgeführt.

Das Feld **„Automatisierung wird verwaltet von** “ zeigt das Team oder die Zuweisungsgruppe an, das bzw. die diese Automatisierung besitzt, bearbeitet und löschen kann. Die Zuweisungsgruppe ist mit der im Abschnitt „ **Wenn diese Bedingungen erfüllt sind“** definierten Gruppe identisch.

b. Geben Sie im Feld **Automatisierungsbeschreibung** eine kurze Beschreibung der Automatisierung ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

10. Wählen Sie **Automatisierung speichern aus**.
    Es wird eine Benachrichtigung angezeigt, wenn die Automatisierung erfolgreich gespeichert wurde. Andernfalls wird eine Fehlermeldung angezeigt. Die von Ihnen erstellte Automatisierung zum Ignorieren wird auf der Seite **„Warnungen ignorieren“** angezeigt, auf der Sie die vorhandene Automatisierung anzeigen, bearbeiten oder löschen können.

Nächste Maßnahme

Sie können Rohereignisse in ein verständliches Format umwandeln, indem Sie Ergänzungsautomatisierung erstellenerstellen.

Ergänzungsautomatisierung erstellen

Die Anreicherung von Warnungen umfasst die Umwandlung von Rohereignissen aus Überwachungstools in ein Standardformat, um die automatisierte Gruppierung und Reaktion zu unterstützen. Dies umfasst das Extrahieren von Feldern aus langen Warnungsnutzlasten oder deren Zusammenfassung in einem standardisierten Format. Darüber hinaus können Sie Tags erstellen, bei denen es sich um Metadaten handelt, die Warnungen hinzugefügt werden, um das Filtern und Gruppieren zu erleichtern.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin oder srm_responder

Warum und wann dieser Vorgang ausgeführt wird

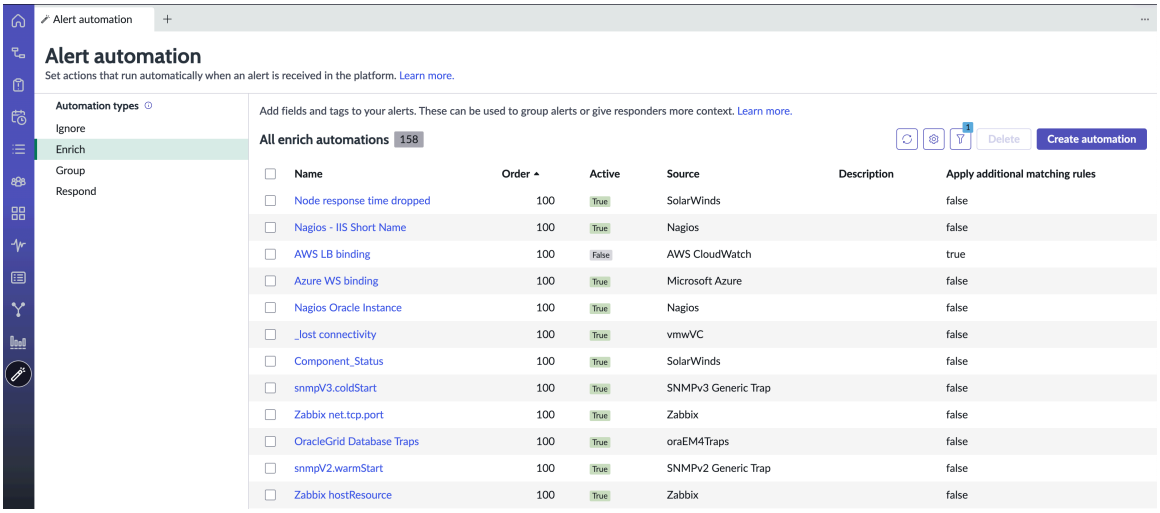
Beim Extrahieren werden Werte aus Ereignis-Payloadfeldern abgerufen und in Warnungsausgabefelder eingefügt, während beim Verfassen mehrere Warnungsfelder in einem kombiniert werden. Weitere Informationen finden Sie unter Warnungsfelder werden extrahiert und erstellt.

Für Anwender, die mit der klassischen Ereignismanagement -Experience vertraut sind, bietet die Ergänzungsautomatisierung eine einfachere Schnittstelle mit besserer Teams-Unterstützung für den Transformations- und Erstellungsschritt von Ereignisregeln. Ereignisregeln bieten erweiterte Funktionen wie Bindungsüberschreibungen, die derzeit nur für Administratoren verfügbar sind. Administratoren können Warnungen auch mit Zuordnungsregeln für Ereignisfelder anreichern. Darüber hinaus wird durch das Ändern von Warnungswerten eine Ereignisfeld-Zuordnungsregel mit dem Zuordnungstyp **Feld zuordnen und Wert transformieren (Einzelfeld)**erstellt. Diese Regel ist mit der Ereignisregel verknüpft und wird gleichzeitig ausgeführt. Dies ermöglicht eine optimierte Zuordnung und Transformation von Ereignisdaten, um Warnungen zu ergänzen.

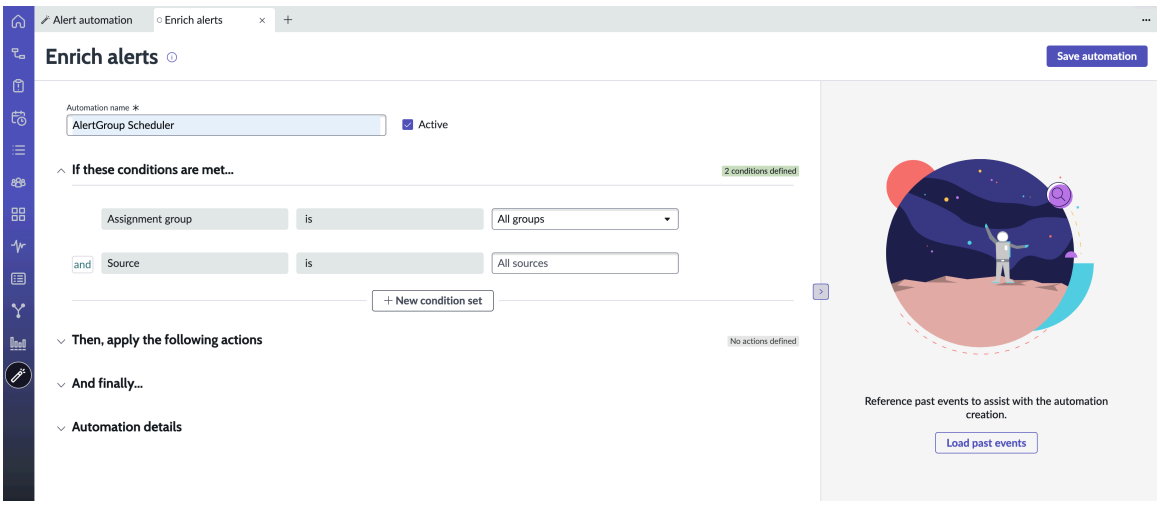
Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol für Warnungsautomatisierung ( ).
3. Wählen Sie auf der Seite „Warnungsautomatisierung“ unter **„Automatisierungstypen“die Option Erweitern**aus.
   Die Seite „Warnungen ergänzen“ wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wählen Sie **Automatisierung erstellen aus**.
5. Geben Sie im Feld **Automatisierungsname** den Namen der Automatisierung für die Anreicherung von Warnungen ein.



6. Aktivieren Sie die Automatisierung, indem Sie das Kontrollkästchen **Aktiv** aktivieren.
7. Um mit der Ausführung anderer Ergänzungsautomatisierungen mit denselben Filterbedingungen fortzufahren, nachdem diese Automatisierung ausgeführt wurde, aktivieren Sie den Umschalter **„Ausführung von Automatisierungen dieses Typs fortsetzen“**. Wenn diese Option deaktiviert ist, wird die Ausführung zusätzlicher Automatisierungen dieses Typs beendet, nachdem diese Automatisierung einmal ausgeführt wurde. Wenn die Automatisierung von einem Administrator verwaltet wird, wird die Ausführung von Automatisierungen im Besitz des Administrators beendet, die Ausführung von Automatisierungen im Besitz anderer Zuweisungsgruppen wird jedoch fortgesetzt.
8. Richten Sie im Abschnitt **Wenn diese Bedingungen erfüllt sind** Filterkriterien ein, um die Warnungen zu identifizieren, die Sie ergänzen möchten.

   Die Bedingung wird anhand des vom Quellüberwachungssystem empfangenen Rohereignisses ausgewertet und berücksichtigt keine angereicherten Felder.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie im Feldmenü **Zuweisungsgruppe** die Zuweisungsgruppe aus, um zu bestimmen, welche Teamwarnungen die Automatisierung auslösen.

Die **Zuweisungsgruppe** stellt ein bestimmtes Team dar, das für die Bearbeitung bestimmter Warnungen verantwortlich ist. Durch die Auswahl einer Zuweisungsgruppe stellen Sie sicher, dass nur die Warnungen, die diesem bestimmten Team zugewiesen sind, die Automatisierung auslösen. Auf diese Weise ist die Automatisierung zielgerichtet und wird nur für relevante Warnungen aktiviert, die dem ausgewählten Team zugeordnet sind.

Hinweis:

- Wenn Sie bei der Instanz mit einer Administratorrolle angemeldet sind (evt_mgmt_admin), sind alle Zuweisungsgruppen verfügbar. Darüber hinaus können Sie **Alle Gruppen** auswählen, um das Generieren von Warnungen für eine der verfügbaren Gruppen zu aktivieren.
- Wenn Sie ein Operator sind, ist nur die Gruppe verfügbar, der Sie angehören.
- Nur Mitglieder der ausgewählten Gruppe oder Administratoren können die Automatisierung aktualisieren oder löschen.

b. Wählen Sie im Menü **Quelle** das Überwachungstool aus, von dem aus die Warnung generiert wird.

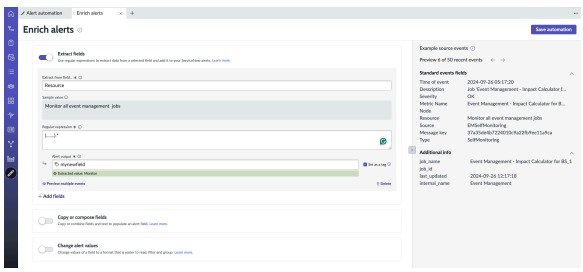
c. Richten Sie die Bedingungen ein, indem Sie das Feld, den Operator und den Feldwert auswählen. Fügen Sie dann weitere Bedingungen mit ODER- oder UND-Operatoren hinzu.

Um einen weiteren Satz Bedingungen hinzuzufügen, wählen Sie **+ Neuer Bedingungssatz**aus. Sie können ein zusätzliches Informationsfeld auch manuell hinzufügen, wenn Sie es nicht in der Dropdown-Liste sehen.

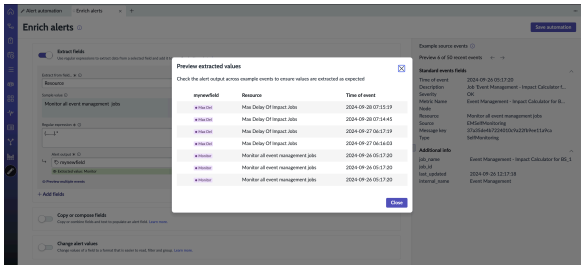
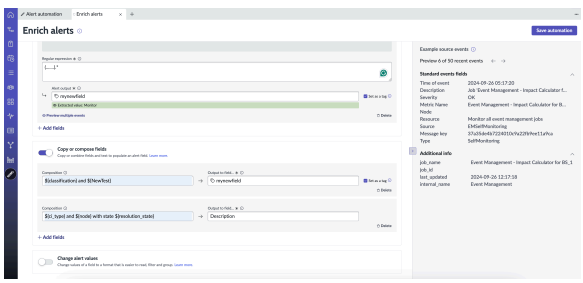
9. **Wählen Sie im Abschnitt Dann wenden Sie die folgenden Aktionen** an die Automatisierungsaktionen aus, die von dieser Automatisierung ausgelöst werden. Sie müssen mindestens eine Aktion auswählen.
   - **Warnungsfelder extrahieren**: Ruft Warnungsfeldwerte aus der Ereignisnutzlast ab und platziert sie in einem Warnungsausgabefeld.
   - **Felder kopieren oder verfassen**: Führt verschiedene Warnungsfelder, Tags und Text zusammen, um eine zusammengesetzte Warnungsausgabe zu generieren.
   - **Warnungswerte ändern**: Ordnet den aktuellen Wert von Warnungsfeldern den angegebenen neuen Werten zu.

Option	Aktion
Warnungsfelder extrahieren	**a.** Aktivieren Sie den Umschalter **Warnungsfelder extrahieren**. **b.** Wählen Sie im Menü **Quelleingabefeld** einen Wert aus. Das Menü zeigt die Standardereignisfelder, zusätzliche Informationen und Tags an. Anschließend wird der Feldwert angezeigt. Sie können auch manuell einen Feldnamen eingeben, der nicht angezeigt wird, und Ihren eigenen Wert hinzufügen. Im Beispielfenster für Quellereignisse wird ein Beispiel für die neuesten Ereignisse in Ihrem System angezeigt. Wenn keine Ereignisse angezeigt werden, können Sie ein Ereignis erstellen (siehe Event-Regel erstellen oder bearbeiten) .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	c. Erstellen Sie im Feld **Regulärer Ausdruck** einen regulären Ausdruck, um den Wert zu extrahieren, den Sie extrahieren möchten. **Hinweis:** Sie können Text unter Verwendung der Formatkonventionen für reguläre Ausdrücke (reguläre Ausdrücke) verfassen. Verwenden Sie eine oder mehrere Erfassungsgruppen mit Klammern, um Teile der Eingabe zu extrahieren. Erfassungsgruppen im regulären Ausdruck werden Warnungsausgaben basierend auf der Reihenfolge zugewiesen, in der sie angezeigt werden. Der reguläre Ausdruck muss mit der gesamten Eingabe übereinstimmen. Erwägen Sie daher, Ihren regulären Ausdruck an beiden Enden mit `.*` zu versehen. Beispiel: `(\w+).acme.com.*` erfasst den Hostnamen in einem vollqualifizierten Domänennamen. Der Parser für die Regex-Engine ist mit Perl-kompatiblen regulären Ausdrücken (PCRE) kompatibel. **d.** Wählen Sie im Feld **Warnungsausgabe** ein Warnungsfeld oder ein Warnungs-Tag aus. Sie können auch manuell einen neuen Feldnamen eingeben. Wenn Sie ein Warnungs-Tag hinzufügen möchten, aktivieren Sie das Kontrollkästchen **Als Tag** festlegen. **Tipp:** Erstellen Sie Warnungs-Tags, die zur einfacheren Filterung und Gruppierung von Quellen gemeinsam genutzt werden können, z. B. die sofort einsatzbereiten Tags.  **e.** Wählen Sie **Vorschau mehrerer Ereignisse anzeigen,** um sicherzustellen, dass der reguläre Ausdruck (regulärer Ausdruck) allgemeingültig genug ist, um Werte in vielen Beispielen korrekt zu extrahieren.

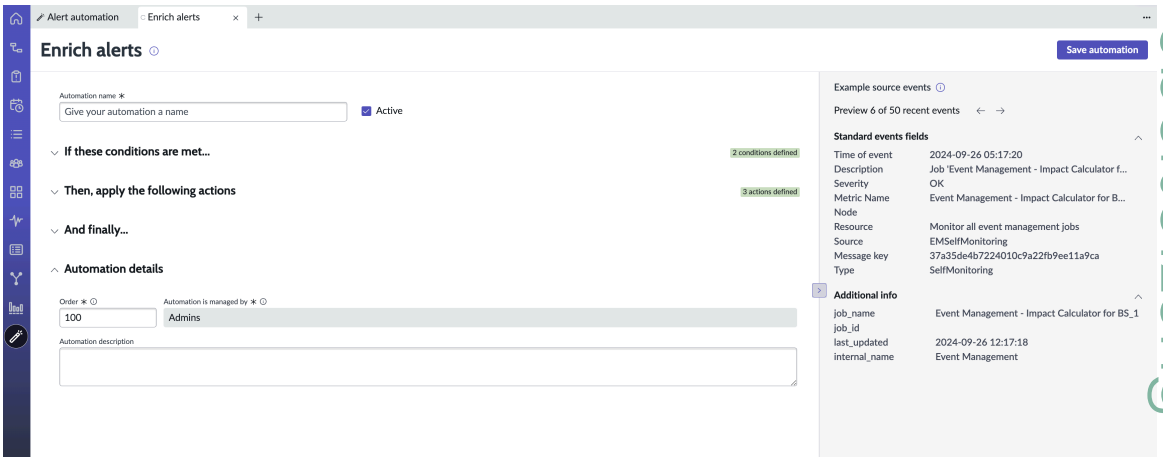
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
	Hinweis: Diese Option ist nur verfügbar, wenn Beispielquellereignisse verfügbar sind und mit dem regulären Ausdrucksfilter übereinstimmen.  Um zusätzliche Felder für die Extraktion einzubeziehen, wählen Sie **+ Felder hinzufügen aus**.
Felder kopieren oder verfassen	**a.** Aktivieren Sie den Umschalter **Felder kopieren oder verfassen**. **b.** Wählen Sie im Menü **Quelleingabefeld** Warnungsfelder und/oder Warnungs-Tags aus, geben Sie manuell einen Feldnamen ein, oder fügen Sie sogar Freitext hinzu. Warnungsfelder werden im Syntaxformat `${field}` angezeigt. **c.** Wählen Sie im Feld **Warnungsausgabe** ein vorhandenes Warnungsfeld oder Warnungs-Tag aus, oder geben Sie manuell ein Warnungsfeld ein. Das Feld **Warnungsausgabe** ist eine angereicherte Warnung, die die zusammengesetzten Warnungsdaten enthält. Um die Gruppierung zu erleichtern, können Sie ein Tag aus dem Menü auswählen. Wenn Sie den neuen Feldnamen als Tag für die Gruppierung verwenden möchten, aktivieren Sie das Kontrollkästchen **Als Tag festlegen**. **Tipp:** Erstellen Sie Warnungs-Tags, die zur einfacheren Filterung und Gruppierung von Quellen gemeinsam genutzt werden können, z. B. die sofort einsatzbereiten Tags.  Um zusätzliche Warnungsdatenzusammensetzungen zu erstellen, wählen Sie **+ Felder hinzufügen aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktion
Warnungswerte ändern	**a.** Aktivieren Sie den Umschalter **Change alert values (** Warnungswerte ändern). **b.** Geben Sie im **Feld Warnungsfeld**das Feld in der Warnung ein, für das Sie Werte zuordnen möchten. **c.** Geben Sie im Feld **Von Wert** den ursprünglichen Wert in das Warnungsfeld ein, das Sie ändern möchten. **d.** Geben Sie im Feld **Bis Wert** den neuen Wert ein, der den ursprünglichen Wert im Warnungsfeld ersetzt. Um weitere Feldwerte hinzuzufügen, wählen Sie **+ Wert hinzufügen**. Um weitere Felder zur Zuordnung hinzuzufügen, wählen Sie **+ Feld zu Zuordnung hinzufügen**aus.

10. Um mit der Ausführung anderer Ergänzungsautomatisierungen mit denselben Filterbedingungen nach der Ausführung dieser Automatisierung fortzufahren, wählen Sie im **Abschnitt „Andere Ergänzungswarnungsautomatisierungen ausführen“**aus.
Wenn Sie **Keine weiteren Automatisierungen von Ergänzungswarnungen ausführen**auswählen, wird die Ausführung zusätzlicher Automatisierungen dieses Typs beendet, nachdem diese Automatisierung einmal ausgeführt wurde. Wenn die Automatisierung von einem Administrator verwaltet wird, wird die Ausführung von Automatisierungen im Besitz des Administrators beendet, die Ausführung von Automatisierungen im Besitz anderer Zuweisungsgruppen wird jedoch fortgesetzt.
11. Geben Sie im Abschnitt **„Automatisierungsdetails“** eine Beschreibung für Reihenfolge und Automatisierung an.



a. Geben Sie im Feld **Reihenfolge** die Automatisierungsreihenfolge ein.

Hinweis: Automatisierungen werden in der Reihenfolge von der niedrigsten zur höchsten ausgeführt. Stellen Sie sicher, dass es keine Ergänzungsautomatisierungen mit einer niedrigeren Ordnungszahl gibt, die über übereinstimmende Bedingungen verfügen und für **die „Zusätzliche Automatisierungen dieses Typs anwenden“** auf „falsch“ festgelegt ist. Andernfalls kann dies die Ausführung nachfolgender Automatisierungen verhindern.

Das Feld **„Automatisierung wird verwaltet von** “ zeigt das Team oder die Zuweisungsgruppe an, das bzw. die diese Automatisierung besitzt, bearbeitet und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

löschen kann. Die Zuweisungsgruppe ist mit der im Abschnitt „ **Wenn diese Bedingungen erfüllt sind“** definierten Gruppe identisch.

b. Geben Sie im Feld **Automatisierungsbeschreibung** eine kurze Beschreibung der Automatisierung ein.

12. Wählen Sie **Automatisierung speichern aus**.
Es wird eine Benachrichtigung angezeigt, wenn die Automatisierung erfolgreich gespeichert wurde. Andernfalls wird eine Fehlermeldung angezeigt. Die von Ihnen erstellte Ergänzungsautomatisierung wird auf der Seite „Warnungen ergänzen“ angezeigt, auf der Sie die vorhandene Automatisierung anzeigen, bearbeiten oder löschen können.

Nächste Maßnahme

Sie können Warnungen effektiver verwalten, indem Sie ähnliche Warnungen mithilfe von Automatisierung für das Erstellen von Gruppengruppieren.

Zugehörige Informationen

Warnungsfelder werden extrahiert und erstellt

Warnungsfelder werden extrahiert und erstellt

Durch Extrahieren und Verfassen können Sie verwalten, was in der Warnungsausgabe angezeigt wird, wodurch das Filtern, Gruppieren und Lesen erleichtert wird. Mit der Warnungsautomatisierung können Sie Werte aus dem Warnungsfeld der Ereignisnutzlast extrahieren und in einem Warnungsausgabefeld platzieren. Beim Verfassen können Sie mehrere Warnungsfelder in einem einzigen Ausgabefeld zusammenführen.

Warnungsfelder werden extrahiert

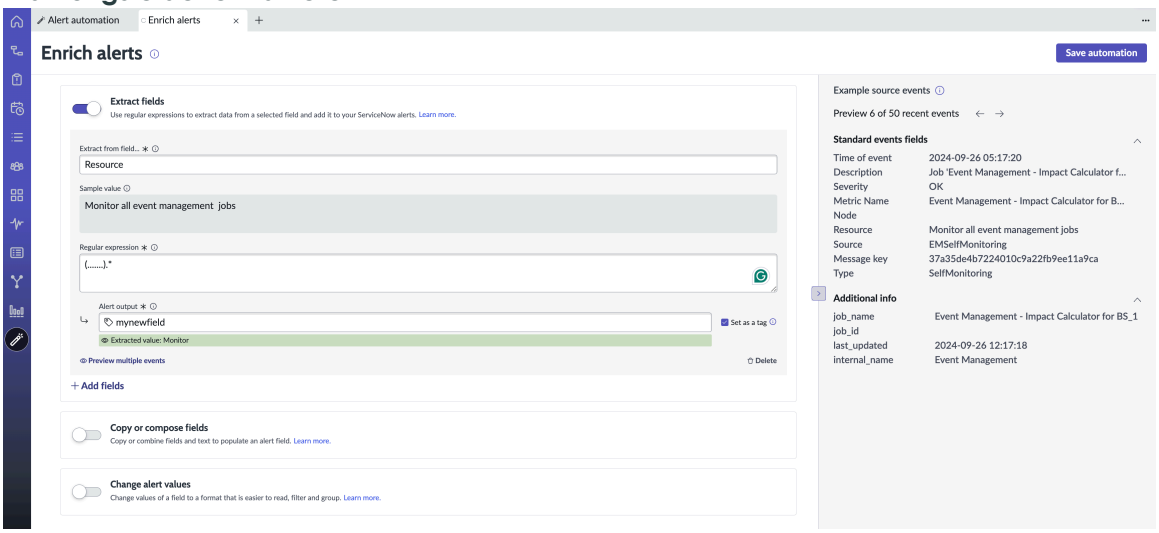
Warnungsbenachrichtigungen enthalten häufig relevante Kontexte, die in Ereignis-Payloads eingebettet sind. Durch Anreichern von Warnungsausgaben mit Werten aus der vorhandenen Nutzlast können Sie die Bedeutung von Warnungen besser verstehen und die geeigneten Lösungsschritte bestimmen. Beispielsweise enthält ein Hostname in der Regel wichtige Informationen wie Service, Knoten, Cluster, Rechenzentrum und Domäne. Um den Wert für ein Cluster-Tag basierend auf eingehenden Hostdaten automatisch hinzuzufügen, können Sie nur die Clusterdaten extrahieren.

Verwenden Sie beim Extrahieren von Warnungsfeldern reguläre Ausdrücke (reguläre Ausdrücke), um Wertformeln zu erstellen. Mit regulären Ausdrücken können Sie die relevanten Teile der Nutzlast genau identifizieren und erfassen, wodurch aussagekräftige und umsetzbare Warnungsbenachrichtigungen erstellt werden.

Hinweis: Sie können Text unter Verwendung der Formatkonventionen für reguläre Ausdrücke (reguläre Ausdrücke) verfassen. Verwenden Sie eine oder mehrere Erfassungsgruppen mit Klammern, um Teile der Eingabe zu extrahieren. Erfassungsgruppen im regulären Ausdruck werden Warnungsausgaben basierend auf der Reihenfolge zugewiesen, in der sie angezeigt werden. Der reguläre Ausdruck muss mit der gesamten Eingabe übereinstimmen. Erwägen Sie daher, Ihren regulären Ausdruck an beiden Enden mit `.*` zu versehen. Beispiel: `(\w+).acme.com.*` erfasst den Hostnamen in einem vollqualifizierten Domänennamen. Der Parser für die Regex-Engine ist mit Perl-kompatiblen regulären Ausdrücken (PCRE) kompatibel.

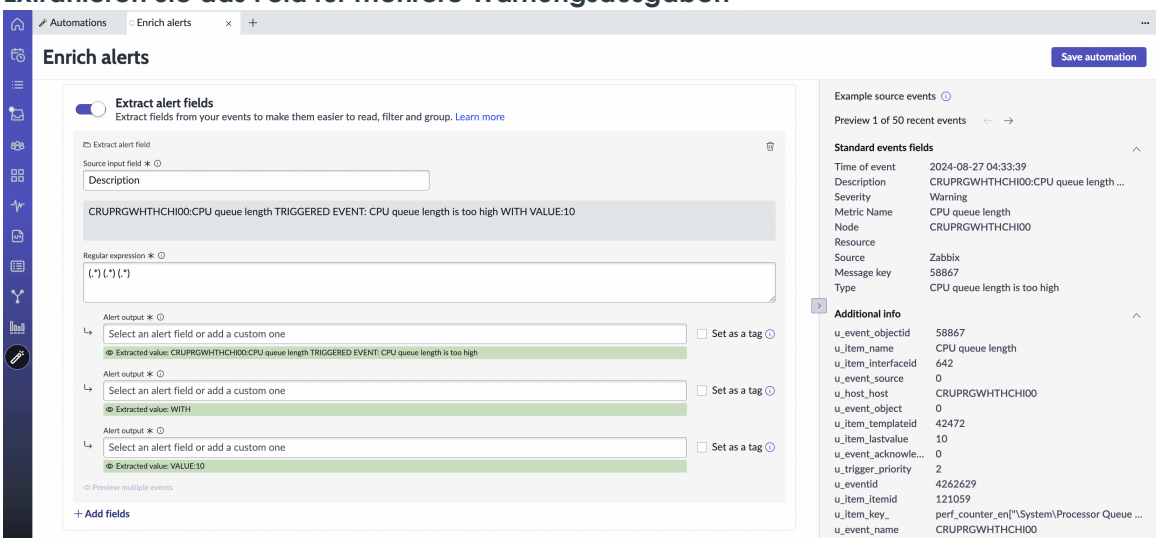
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warnungsfelder extrahieren



Wenn Sie mehrere Erfassungsgruppen mit Klammern verwenden, wird jeder extrahierte Wert in einem separaten Ausgabefeld angezeigt.

Extrahieren Sie das Feld für mehrere Warnungsausgaben



Zeigen Sie eine Vorschau der Warnungsausgabe für Beispielereignisse an, um sicherzustellen, dass die Werte wie erwartet extrahiert werden, indem Sie **Vorschau mehrerer Ereignisse**auswählen.

Hinweis: Diese Option ist nur verfügbar, wenn Beispielquellereignisse verfügbar sind und mit dem regulären Ausdrucksfilter übereinstimmen.

Beispiel: Warnungsfelder werden extrahiert

Angenommen, Sie müssen nur sechs Buchstaben aus einem bestimmten Feld eines Ereignisses extrahieren und in einem neuen Warnungsfeld namens `mynewfield`anzeigen. Sie sollten dieses neue Warnungsfeld auch für die spätere Verwendung bei der Warnungsgruppierung mit Tags versehen. So können Sie dies erreichen:

- **Quelleingabefeld**: Wählen Sie das Ereignisfeld aus, aus dem Sie Daten extrahieren möchten. In diesem Fall lautet das Feld **Resource**.
- **Regulärer Ausdruck**: Verwenden Sie einen regulären Ausdruck, um den bestimmten Teil, den Sie benötigen, aus dem Wert des ausgewählten Felds zu extrahieren. Wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

beispielsweise der Wert des Ressourcenfelds „Zabbix-Integration“ enthält und Sie „Zabbix“ extrahieren möchten, muss Ihr regulärer Ausdruck (……).* lauten.

- **Warnungsausgabe**:
  - Wählen Sie ein vorhandenes Warnungsfeld, ein vorhandenes Warnungs-Tag, oder geben Sie manuell einen neuen Feldnamen ein. In diesem Fall geben wir einen neuen Feldnamen `mynewfield`ein.
  - Legen Sie `„mynewfield“` als Tag für die spätere Verwendung in der Tag-basierten Gruppierung fest. Beachten Sie das Tag, das vor dem Feldnamen angezeigt wird.

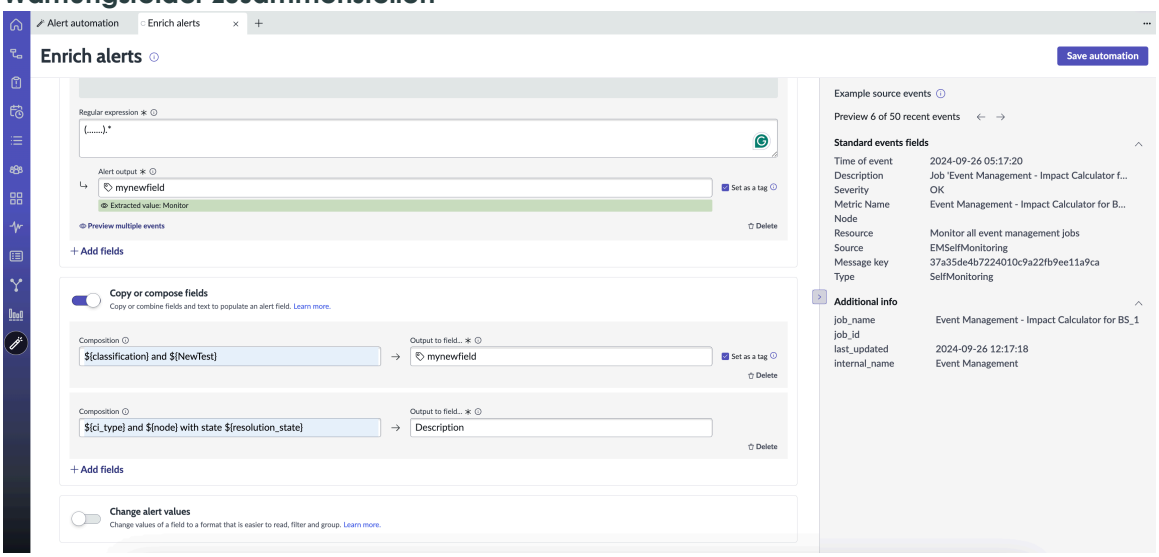
  Nachdem Sie den regulären Ausdruck auf den Wert des ausgewählten Felds (in diesem Fall den Wert des Felds **Ressource**) angewendet haben, überprüfen Sie das extrahierte Wort, das unter dem Feld **Warnungsausgabe** angezeigt wird. Beispielsweise sollte „Zabbix“ angezeigt werden, wenn der reguläre Ausdruck richtig übereinstimmt.

- **Mehrere Ereignisse in der Vorschau anzeigen**: Durch die Vorschau mehrerer Ereignisse können Sie überprüfen, ob der reguläre Ausdruck Daten aus einer Reihe von Beispielereignissen extrahiert. Dies hilft festzustellen, ob Anpassungen des regulären Ausdrucks erforderlich sind.

Warnungsfelder werden erstellt

Beim Erstellen einer Warnungsausgabe können Sie Felder, Tags oder Freitext auswählen oder manuell eingeben, die einbezogen werden sollen. Diese Daten können leicht gelesen, gefiltert und gruppiert werden, um Warnungen besser verwalten und verstehen zu können.

Warnungsfelder zusammenstellen



Beispiel: Warnungsfelder werden erstellt

Angenommen, Sie möchten zwei Eingabefelder haben, die Daten verfassen und in zwei verschiedenen Warnungsausgabefeldern anzeigen. In einem Szenario soll der Quellwert aus einem vorhandenen Warnungsfeld zusammen mit einem neuen Feld stammen, das den zusammengesetzten Wert in einem neuen Warnungsausgabefeld anzeigt. Sie planen auch, das neue Warnungsausgabefeld für die spätere Verwendung in der Tag-basierten Gruppierung mit Tags zu versehen. Im anderen Szenario kombinieren Sie vorhandene Felder mit Freitext und wählen die Warnungsausgabe aus, die in einem vorhandenen Warnungsfeld angezeigt werden soll. So können Sie dies erreichen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Szenario 1:

  1. **Quelleingabefeld**: Wählen Sie ein vorhandenes Warnungsfeld aus, fügen Sie den Text „und“ hinzu, und geben Sie anschließend einen neuen Feldnamen ein, z. B. `NewTest`. Beispiel: ${classification} und ${NewTest}.

     Beachten Sie, dass Warnungsfelder im Syntaxformat `${field}` angezeigt werden. Sie können den Feldnamen auch aus der Dropdown-Liste auswählen. Die Syntax wird dann automatisch hinzugefügt.

  2. **Warnungsausgabe**: Geben Sie den Namen des neuen Warnungsfelds ein, in dem Sie die Werte aus den Eingabefeldern anzeigen möchten. Nennen wir es beispielsweise `mynewfield`.

     Legen Sie `„mynewfield“` als Tag für die spätere Verwendung in der Tag-basierten Gruppierung fest. Beachten Sie das Tag, das vor dem Feldnamen angezeigt wird.

- Szenario 2:

  1. **Quelleingabefeld**: Wählen Sie vorhandene Warnungsfelder aus, und fügen Sie einen beliebigen Freitext für die Darstellung im Warnungsausgabefeld hinzu. Beispiel: ${ci_type} und ${node} mit Status ${resolution_state}.

     Warnungsfelder werden im Syntaxformat `${field}` angezeigt. Sie können den Feldnamen auch aus dem Dropdown-Feld auswählen. Die Syntax wird dann automatisch hinzugefügt.

  2. **Warnungsausgabe**: Wählen Sie ein vorhandenes Warnungsfeld aus, in dem Sie die Werte aus den Eingabefeldern anzeigen möchten. Wählen Sie beispielsweise **Beschreibung**aus.

Aktionen zum Beheben von Warnungsproblemen in Service Operations-Arbeitsbereich für ITOMausführen

Beheben Sie das zugrunde liegende Problem einer Warnung, indem Sie vordefinierte Korrekturaufgaben ausführen, um eine schnellere Problemlösung und eine konsistente Lösung sicherzustellen.

Vorbereitungen

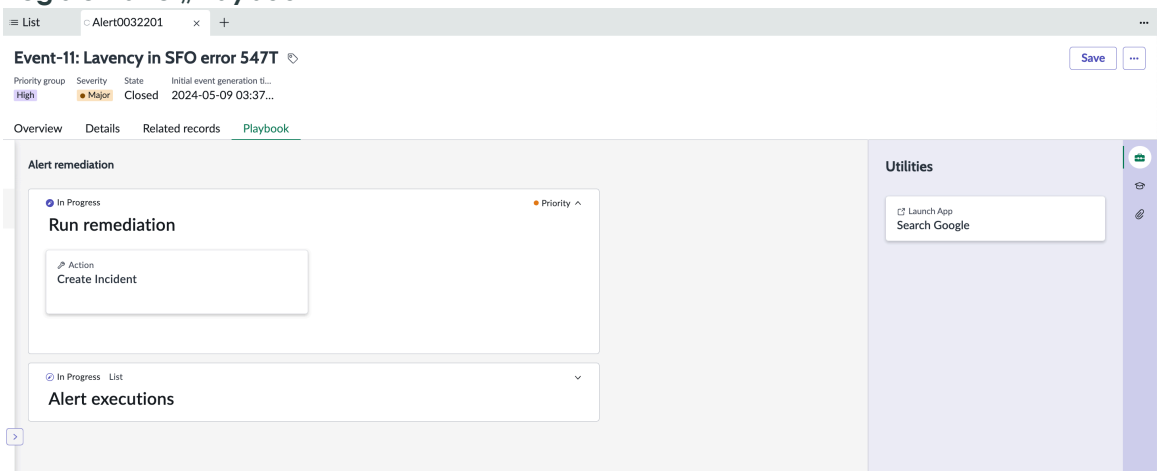
Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol für die Express-Liste ( ).
3. Wählen Sie die Warnungsnummer aus, um sie zu öffnen.
   Die Warnung wird auf einer separaten Registerkarte geöffnet und zeigt die Registerkarte **Übersicht** an.
4. Wählen Sie **Playbook starten aus**.
5. Wählen Sie die Registerkarte **Playbook** aus.
   Auf der Karte **„Korrektur ausführen“** werden die verfügbaren Korrekturaktionen angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Playbook“



6. Wählen Sie die Kachel aus, die der Aktion entspricht, die Sie ausführen möchten. Die ausgewählte Aktion wird auf der Karte **Warnungsausführungen** angezeigt.

Ergebnisse

Wenn die Aktion abgeschlossen ist, wird sie unter dem Abschnitt „Warnungs-Fehlerkorrektur“ auf der Karte **Abgeschlossen** angezeigt.

Automatisierung für das Erstellen von Gruppen

Durch die Gruppierungsautomatisierung können Sie Warnungen effektiver verwalten, indem Sie ähnliche Warnungen sammeln. Dies erleichtert das Erkennen von Mustern, das schnelle Identifizieren von Problemen und das effiziente Reagieren. Durch diese Organisation von Warnungen können Sie das Warnungsrauschen reduzieren, Ursachen identifizieren und sie den entsprechenden Teams zuweisen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin oder srm_responder

Warum und wann dieser Vorgang ausgeführt wird

Die Gruppierung dieser Methode ist am nützlichsten, wenn Warnungen gemeinsame Daten oder Tags gemeinsam nutzen, z. B. nach einem Knoten oder Standort. Sie können Felder oder Tags verwenden, die über eine Ergänzungsautomatisierung ausgefüllt wurden. Dies ist die beste Möglichkeit, Warnungen zu gruppieren, wenn Ihre CMDB oder Servicezuordnungen unausgereift sind. Dies ergänzt unsere anderen Gruppierungsalgorithmen, einschließlich Warnungskorrelationsregeln, CMDB, ML und textbasierte Gruppierung. Warnungen werden nach ihrer ersten Übereinstimmung gruppiert, und Sie können die Prioritätsreihenfolge dieser Algorithmen über die Systemeigenschaft steuern. Informationen zur Reihenfolge der Korrelationslogik finden Sie unter Konfigurieren Sie die Reihenfolge der Warnungskorrelationslogik.

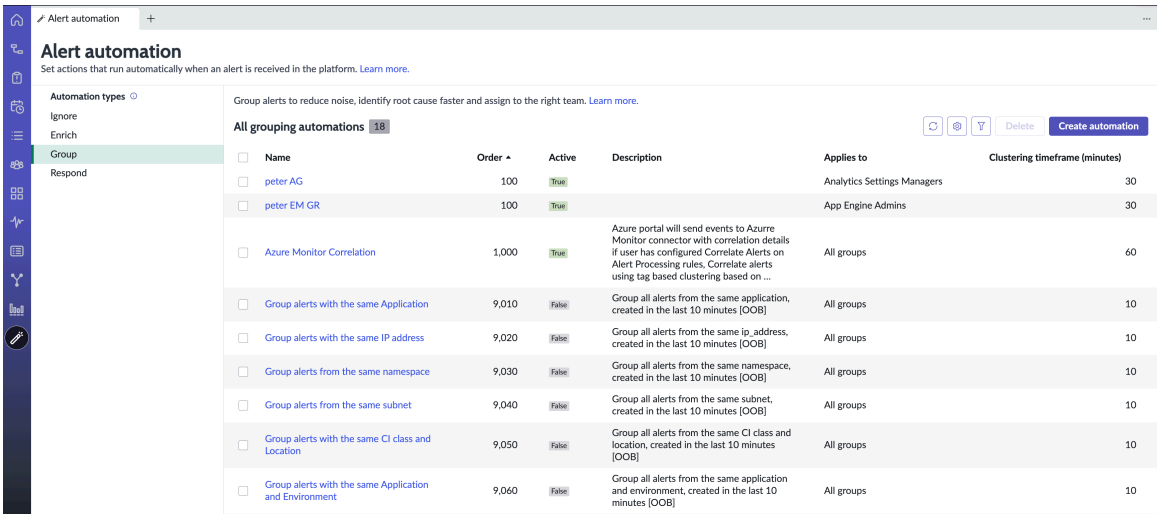
Die Warnungsautomatisierung bietet auch eine Simulationsfunktion, mit der Sie testen können, wie viele Warnungsgruppen gebildet werden, wie viele nicht gruppiert werden und welche Komprimierungsrate verwendet wird. Eine höhere Komprimierungsrate bedeutet, dass Ihr Team produktiver ist und die Ursachen möglicherweise schneller identifizieren kann. Berücksichtigen Sie jedoch, ob die Gruppen genau, betrieblich korrekt und den richtigen Teams zugewiesen sind. Sie können die Gruppenkriterien anpassen, bis Sie mit den resultierenden Gruppen zufrieden sind.

Für Benutzer, die mit der klassischen Ereignismanagement -Experience vertraut sind, bietet diese Funktion eine einfachere Oberfläche mit verbesserter Teamunterstützung für die Erstellung von Tag-basierten Warnungs-Clustering-Definitionen.

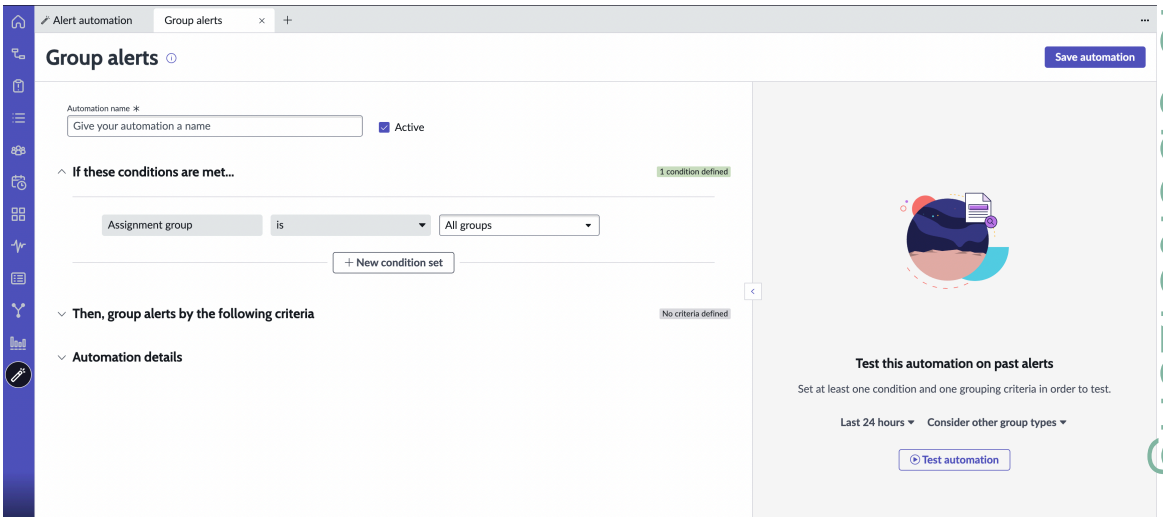
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol für Warnungsautomatisierung ( ).
3. Wählen Sie auf der Seite „Warnungsautomatisierung“ unter **Automatisierungstypen**die Option **Gruppe**aus.
   Die Seite Gruppenwarnungen wird angezeigt.



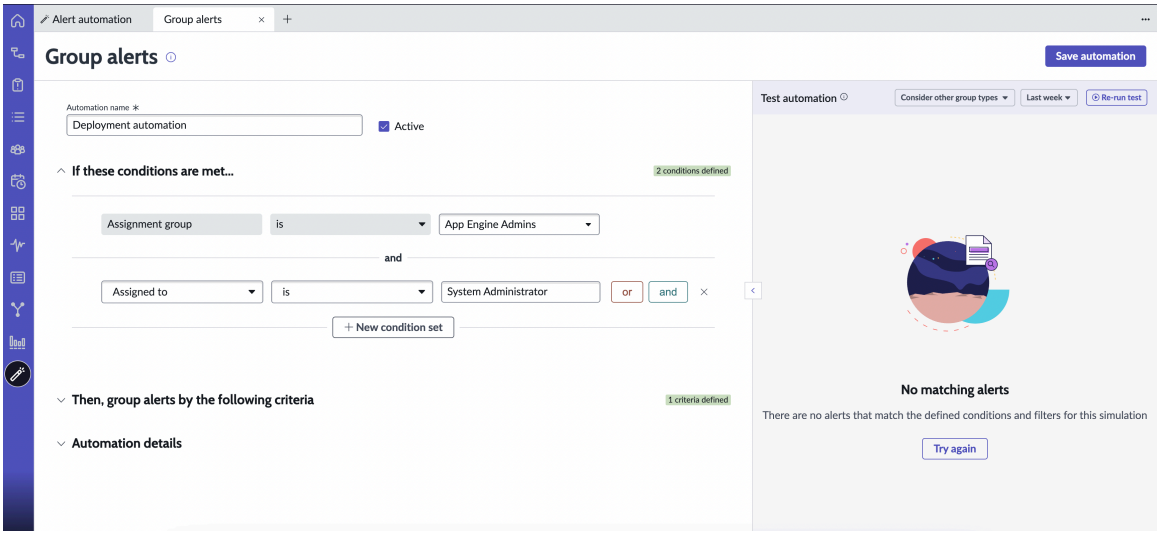
4. Wählen Sie **Automatisierung erstellen aus**.



5. Geben Sie im Feld **Automatisierungsname** den Namen der Automatisierung für die Gruppierung von Warnungen ein.
6. Aktivieren Sie die Automatisierung, indem Sie das Kontrollkästchen **Aktiv** aktivieren.
7. Richten Sie im Abschnitt **Wenn diese Bedingungen erfüllt sind** Filterkriterien ein, um die Warnungen zu identifizieren, die Sie gruppieren möchten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



a. Wählen Sie im Feldmenü **Zuweisungsgruppe** die Zuweisungsgruppe aus, um zu bestimmen, welche Teamwarnungen die Automatisierung auslösen.

Die **Zuweisungsgruppe** stellt ein bestimmtes Team dar, das für die Bearbeitung bestimmter Warnungen verantwortlich ist. Durch die Auswahl einer Zuweisungsgruppe stellen Sie sicher, dass nur die Warnungen, die diesem bestimmten Team zugewiesen sind, die Automatisierung auslösen. Auf diese Weise ist die Automatisierung zielgerichtet und wird nur für relevante Warnungen aktiviert, die dem ausgewählten Team zugeordnet sind.

Hinweis:

- Wenn Sie bei der Instanz mit einer Administratorrolle angemeldet sind (evt_mgmt_admin), sind alle Zuweisungsgruppen verfügbar. Darüber hinaus können Sie **Alle Gruppen** auswählen, um das Generieren von Warnungen für eine der verfügbaren Gruppen zu aktivieren.
- Wenn Sie ein Operator sind, ist nur die Gruppe verfügbar, der Sie angehören.
- Nur Mitglieder der ausgewählten Gruppe oder Administratoren können die Automatisierung aktualisieren oder löschen.

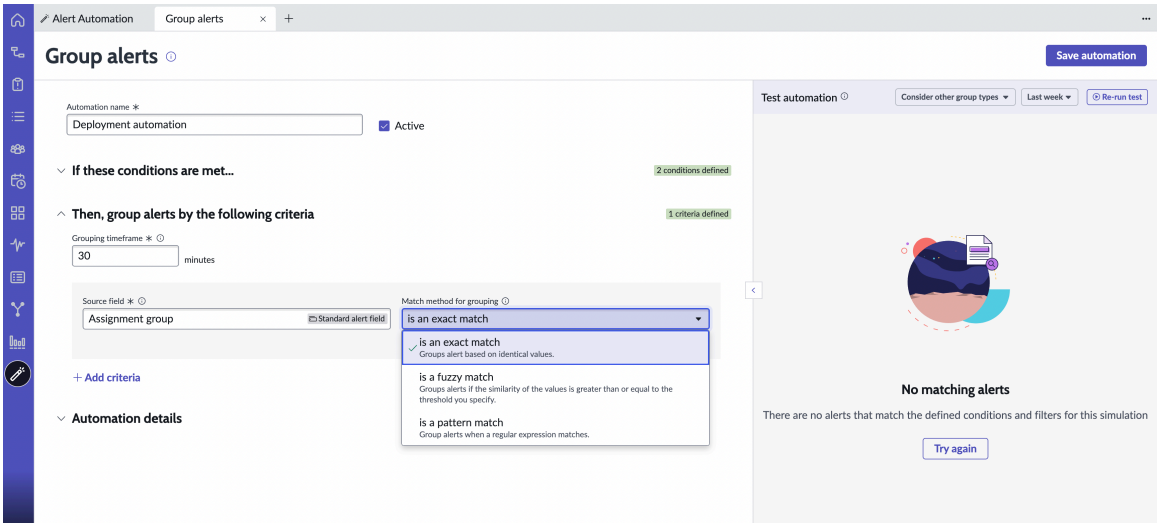
b. Richten Sie die Bedingungen ein, indem Sie das Feld, den Operator und den Feldwert auswählen. Fügen Sie dann weitere Bedingungen mit ODER- oder UND-Operatoren hinzu. Sie müssen neben der Zuweisungsgruppe mindestens einen weiteren Filter hinzufügen.

Tipp: Wählen Sie einen spezifischeren Filter aus, um die Leistung zu verbessern.

Um einen weiteren Satz Bedingungen hinzuzufügen, wählen Sie **+ Neuer Bedingungssatz**aus. Sie können ein zusätzliches Informationsfeld auch manuell hinzufügen, wenn Sie es nicht in der Dropdown-Liste sehen.

8. Führen Sie im Abschnitt **Dann, gruppieren Sie Warnungen nach den folgenden Kriterien** aus die folgenden Schritte aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



a. Geben Sie im Feld **Gruppierungszeitraum** die Dauer (in Minuten) an, nach der Warnungen gesammelt und gruppiert werden müssen.

b. Wählen Sie im Menü **Quellfeld** die Quelle aus, aus der Sie die Warnungen gruppieren möchten.

> **Hinweis:** Sie können manuell einen Feldnamen hinzufügen und den Typ des Felds auswählen. Zu den verfügbaren Optionen gehören das Feld „Zusätzliche Informationen“, das Warnungs-Tag und das CI-Tag. Diese Flexibilität ermöglicht es Ihnen, die erfassten Informationen an Ihre spezifischen Anforderungen anzupassen.

c. Wählen Sie im Feld **Übereinstimmungsmethode für Gruppierung** eine der folgenden Optionen aus: Warnungen basierend auf einer genauen Übereinstimmung, einer Fuzzy-Übereinstimmung oder einer Musterübereinstimmung gruppieren.

Wenn Sie im Gruppierungsfeld einen Wert für die Fuzzy-Übereinstimmungsmethode auswählen, wird das Feld **Ähnlichkeitsschwellenwert (Prozentsatz)** sichtbar. Warnungen werden gruppiert, wenn ihre Ähnlichkeit größer oder gleich dem angegebenen Prozentsatz ist, basierend auf der Bearbeitungsentfernung.

Wenn Sie beispielsweise Warnungen aus den USA, CA und USA, NY haben und die Warnungen nach Ländern gruppieren möchten, legen Sie das Feld **Quelle** auf USA fest. Wenn die **Übereinstimmungsmethode für Gruppierung** eine Fuzzy-Übereinstimmung ist und der **Ähnlichkeitsschwellenwert (Prozentsatz)** 50 % beträgt, werden Warnungen gruppiert, wenn sie mindestens zu 50 % ähnlich sind, d. h., sie teilen das Land „USA“ als gemeinsames Attribut.

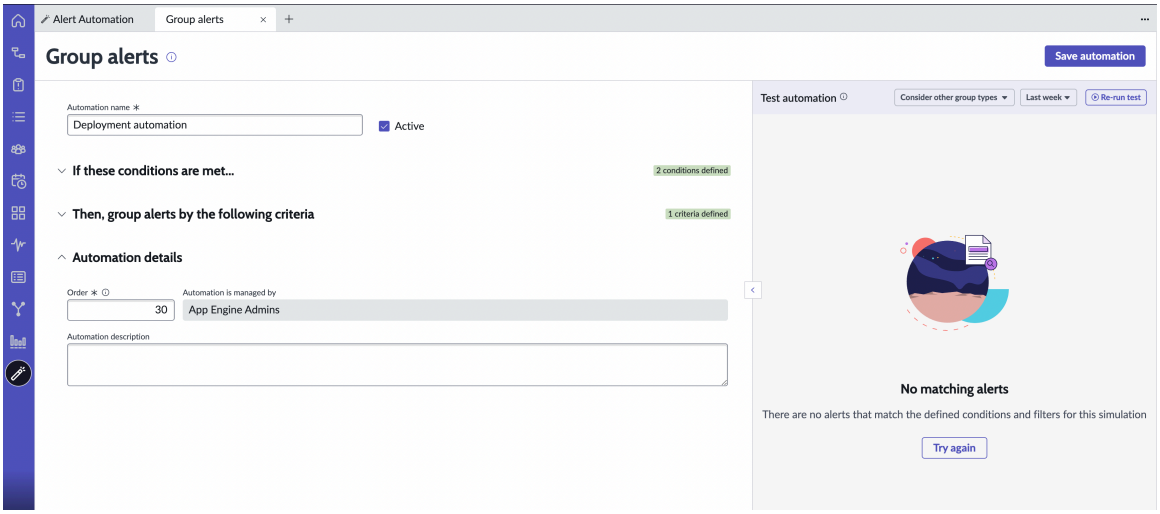
d. Wenn Sie im Gruppierungsfeld einen Wert für die Musterübereinstimmungsmethode auswählen, wird das Musterübereinstimmungsfeld sichtbar. Warnungen werden gruppiert, wenn das angegebene Muster übereinstimmt. Weitere Informationen finden Sie unter Musterabgleich .

Verwenden Sie Sternchen (*) in der Suchzeichenfolge, um eine beliebige Anzahl von Zeichen zu finden, oder ein Fragezeichen (?), um ein einzelnes Zeichen zu finden. Alles andere in der Suchzeichenfolge stimmt mit sich selbst überein. Verwenden Sie beispielsweise „HTTP-Fehler 5??“. um alle HTTP 500-Fehler abzugleichen.

Um zusätzliche Felder für die Gruppierung einzubeziehen, wählen Sie **+ Kriterien hinzufügen aus**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Geben Sie im Abschnitt **„Automatisierungsdetails“** eine Beschreibung für Reihenfolge und Automatisierung an.



   a. Geben Sie im Feld **Reihenfolge** die Automatisierungsreihenfolge ein.

      Hinweis: Warnungen werden basierend auf der ersten Übereinstimmung gruppiert und in der Reihenfolge von der niedrigsten zur höchsten Zahl ausgeführt. Das Feld **„Automatisierung wird verwaltet von** “ zeigt das Team oder die Zuweisungsgruppe an, das bzw. die diese Automatisierung besitzt, bearbeitet und löschen kann. Die Zuweisungsgruppe ist mit der im Abschnitt „ **Wenn diese Bedingungen erfüllt sind“** definierten Gruppe identisch.

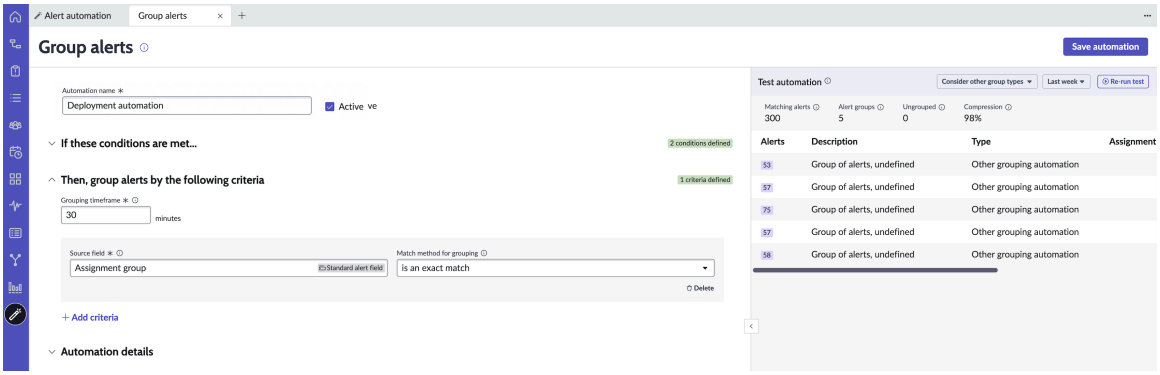
   b. Geben Sie im Feld **Automatisierungsbeschreibung** eine kurze Beschreibung der Automatisierung ein.

10. Um zu testen, ob die Warnungsgruppierung ordnungsgemäß funktioniert, navigieren Sie zu **Diese Automatisierung bei früheren Warnungen testen**, wählen Sie den Zeitrahmen für die Simulation aus der Dropdown-Liste aus, wählen Sie aus, ob Sie andere Gruppierungstypen berücksichtigen möchten, und wählen Sie dann **Automatisierung testen**aus.

    Hinweis: Im Menü Andere Gruppentypen berücksichtigen können Sie entweder **Nur diese Automatisierung** oder **Andere Gruppentypen berücksichtigen**auswählen. Wenn Sie **Diese Automatisierung auswählen, werden nur** andere Warnungsgruppentypen ignoriert, während die Option **Andere Gruppentypen berücksichtigen** alle Automatisierungen der Warnungsgruppierung einbezieht, z. B. tagbasierte, automatisierte, textbasierte und CMDB-basierte Warnungsgruppierung.

    Während der Simulation werden sowohl die gruppierten als auch die nicht gruppierten Warnungen für den angegebenen Zeitraum angezeigt. Wenn Warnungen gruppiert sind, wird die Anzahl der gruppierten Warnungen angezeigt. Sie können diese Nummer auswählen, um die gruppierten Warnungen anzuzeigen. Wenn Sie eine einzelne Warnung auswählen, werden außerdem die Details zu dieser spezifischen Warnung angezeigt.
    Sie können auch alle Bedingungen für die Gruppierung von Warnungen oder Feldwerte ändern und den Prozess erneut initiieren, indem Sie **Test erneut ausführen**auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Im Header des Abschnitts „Testautomatisierung“ wird außerdem Folgendes angezeigt: übereinstimmende Warnungen, Warnungsgruppen, nicht gruppierte Warnungen und Komprimierung.

- **Übereinstimmende Warnungen**: Die Gesamtzahl der übereinstimmenden Warnungen vor der Gruppierung, die den für diese Automatisierung definierten Bedingungen entsprechen.
- **Warnungsgruppen**: Die Anzahl der Gruppen, die mehr als eine Warnung enthalten, die den Automatisierungsbedingungen entspricht. Die kleinere Zahl in Klammern gibt die Anzahl der von dieser Automatisierung erstellten Gruppen an.
- **Nicht gruppiert**: Die Anzahl der Warnungen, die den Automatisierungsbedingungen entsprechen und nicht gruppiert bleiben.
- **Komprimierung**: Die prozentuale Reduzierung der Anzahl der Gesamtwarnungen durch Gruppierung, berechnet als 1 - (Warnmeldungsgruppen + nicht gruppiert) /Warnungen insgesamt. Sie können die Komprimierungsrate verbessern, indem Sie Ihre Warnungen in verwandte Probleme gruppieren. Die kleinere Zahl in Klammern gibt den Prozentsatz der übereinstimmenden Warnungen an, die von dieser Automatisierung komprimiert werden.

Im Abschnitt „Testautomatisierung“ werden drei wichtige Spalten angezeigt: **Beschreibung**, **Typ**und **Zeit**. In der Spalte **„Beschreibung** “ werden die Details der Warnmeldungsgruppen beschrieben. Vor der Spalte **„Beschreibung** “ gibt eine Zahl die Gesamtzahl der in dieser Gruppe enthaltenen Warnungen an. **Der Typ** gibt die Kategorie der Gruppierung an, z. B. Diese Gruppierungsautomatisierung, Andere Gruppierungsautomatisierung, CMDB-Gruppe oder Einzelne Warnung, um nur einige zu nennen. Wenn Sie **Andere Gruppierungsautomatisierung** auswählen, gelangen Sie zur entsprechenden Automatisierungsseite, auf der die Gruppe generiert wurde. Außerdem wird in der Spalte **Zeit** angezeigt, wann der Test durchgeführt wurde.

Wichtig: Sie können die Simulation von Warnungen sowohl in Ihrer Test- als auch in der Produktionsinstanz ausführen. Die Testautomatisierung simuliert die Automatisierung mit bis zu 200 aktuellen Warnungen, die den angegebenen Bedingungen entsprechen. Es berücksichtigt nur Gruppen, bei denen alle Warnungen die Bedingungen für diese Automatisierung erfüllen. Während der tatsächlichen Laufzeit können jedoch zusätzliche Gruppierungsalgorithmen angewendet werden.

11. Wählen Sie **Automatisierung speichern aus**.
    Es wird eine Benachrichtigung angezeigt, wenn die Automatisierung erfolgreich gespeichert wurde. Andernfalls wird eine Fehlermeldung angezeigt. Die von Ihnen erstellte Gruppenautomatisierung wird auf der Seite „Gruppenwarnungen“ angezeigt, auf der Sie die vorhandene Automatisierung anzeigen, bearbeiten oder löschen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Sie können Warnungen eskalieren, bei denen eine schnellere Reaktion von Teams oder Einzelpersonen erforderlich ist, indem Sie die Antwortautomatisierungimplementieren.

Löscht eine Automatisierung

Löschen Sie eine Automatisierung, um eine automatisierte Warnungsbehandlungsregel endgültig aus Ihrem System zu entfernen.

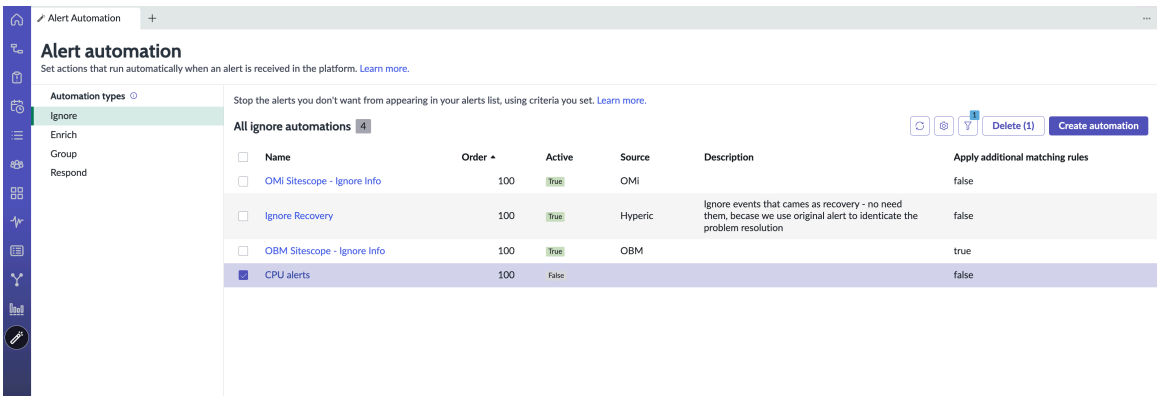
Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin oder srm_responder

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der primären Navigation das Symbol für Warnungsautomatisierung ( ).
3. Wählen Sie auf der Seite „Warnungsautomatisierung“ unter **„Automatisierungstypen“**den Automatisierungstyp aus, den Sie löschen möchten, z. B. Ignorieren, Anreichern, Gruppieren oder Antworten.

   Die Seite für diesen Automatisierungstyp wird geöffnet und zeigt alle vorhandenen Automatisierungen an.
4. Um eine Automatisierung zu löschen, aktivieren Sie das Kontrollkästchen neben ihrem Namen, und wählen Sie dann **Löschen aus**.



5. Wählen Sie im Bestätigungsfenster **Löschen**.
   Die Warnung wird endgültig gelöscht.

AIOps – Dashboards in Service Operations-Arbeitsbereich für ITOM

Die AIOps-Dashboards bieten umfassende Visualisierungen kritischer Betriebsdaten. Sie können Leistungskennzahlen (Key Performance Indicators, KPIs) überwachen, die Serviceintegrität nachverfolgen und wertvolle Kontextinformationen zur gesamten IT-Umgebung gewinnen. Diese Dashboards bieten umsetzbare Einblicke, die eine proaktive Reaktion auf potenzielle Probleme ermöglichen.

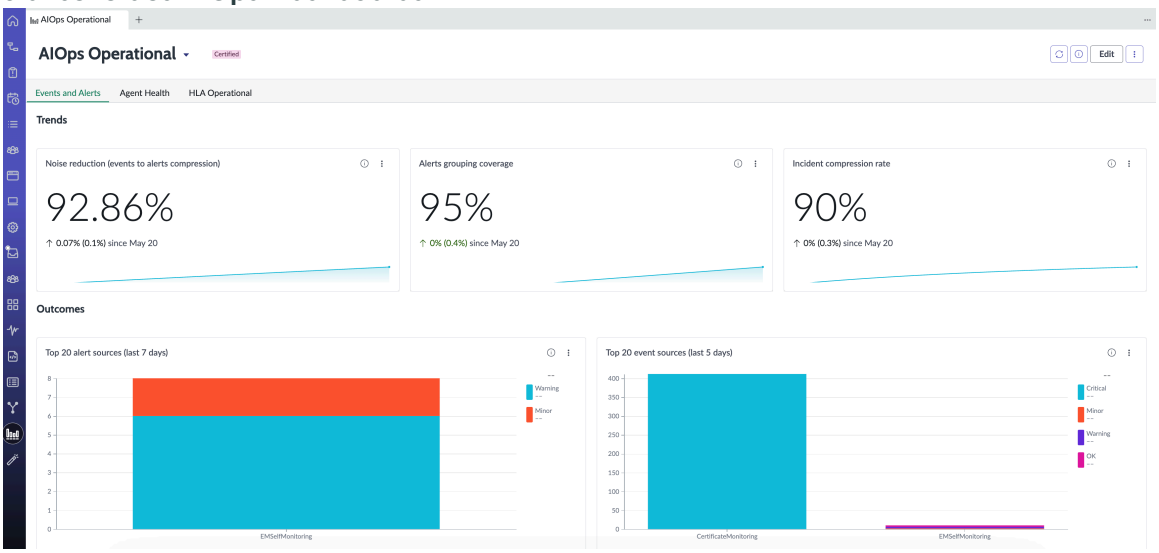
Die wichtigsten Vorteile der Verwendung der AIOps-Dashboards:

- Konfigurieren Sie die Dashboards so, dass sie sich auf die Metriken und Daten konzentrieren, die für Ihre Rolle am relevantesten sind.
- Nutzen Sie die interaktive visuelle Darstellung kritischer Betriebsdaten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

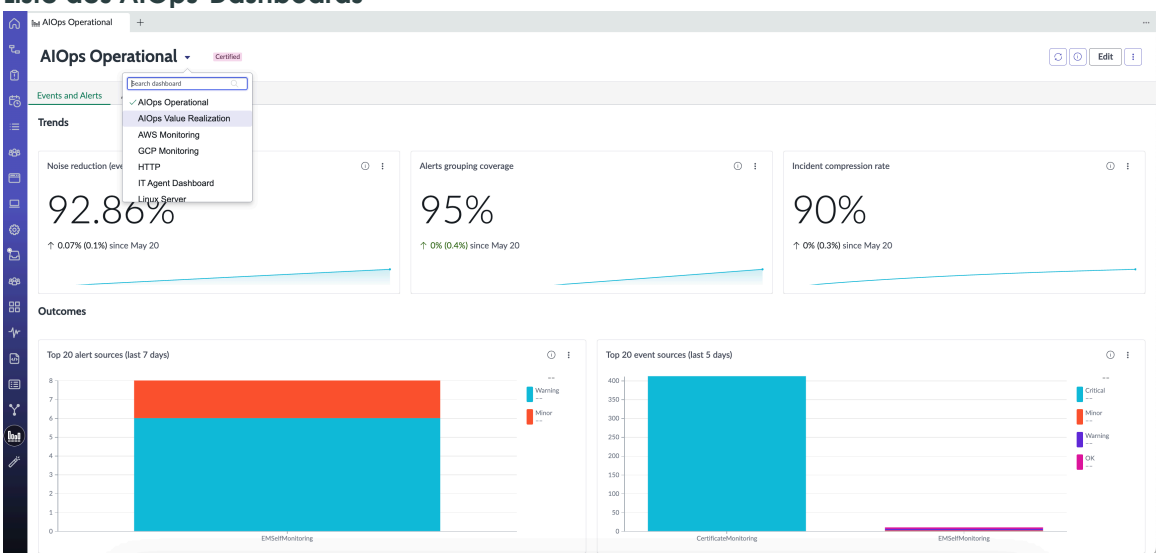
- Überwachen Sie KPIs, Serviceintegritätsmetriken und andere wichtige Leistungsdaten auf einen Blick.
- Nutzen Sie umsetzbare Einblicke aus der Datenanalyse für eine bessere Entscheidungsfindung.

Startseite des AIOps-Dashboards



Um Dashboards für AIOps-Vorgänge, z. B. AIOps-Wertrealisierung, anzuzeigen, wählen Sie die Liste „AIOps-Operativ“ und dann den Namen des Dashboards aus.

Liste des AIOps-Dashboards



AIOps – Wertrealisierungs-Dashboard

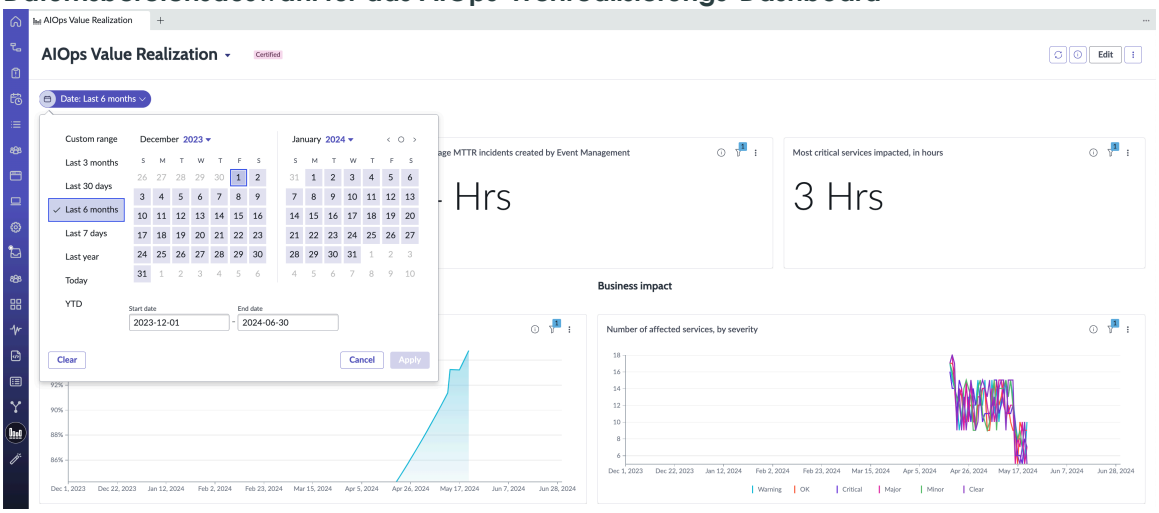
Das Dashboard für die Wertrealisierung von AIOps verwendet Performance Analytics, um einen umfassenden Einblick in die Geschäftsergebnisse von Warnungen, Ereignissen und Incidents zu bieten. Es bietet Metriken wie die Reduzierung des Datenrauschens (Ereignisse zu Warnungskomprimierung), die durchschnittliche MTTR für von Ereignismanagement erstellte Incidents [var.event-mgmt] und die wichtigsten betroffenen Services nach Stunden.

Das Dashboard „AIOps-Wertrealisierung“ enthält eine Kalenderfunktion, mit der Anwender verschiedene Datumsbereiche auswählen können, z. B. anwenderdefinierte Daten, die letzten 3 Monate, die letzten 30 Tage, die letzten 6 Monate, die letzten 7 Tage, das letzte Jahr, heute und Jahr -to-date (seit Jahresbeginn). Sie können ein anwenderdefiniertes

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Start- und Enddatum angeben und diese Auswahl anwenden, um Berichte speziell für den ausgewählten Datumsbereich anzuzeigen. Diese Funktion ermöglicht eine maßgeschneiderte Analyse und Berichterstellung basierend auf bestimmten interessanten Zeiträumen.

Datumsbereichsauswahl für das AIOps-Wertrealisierungs-Dashboard



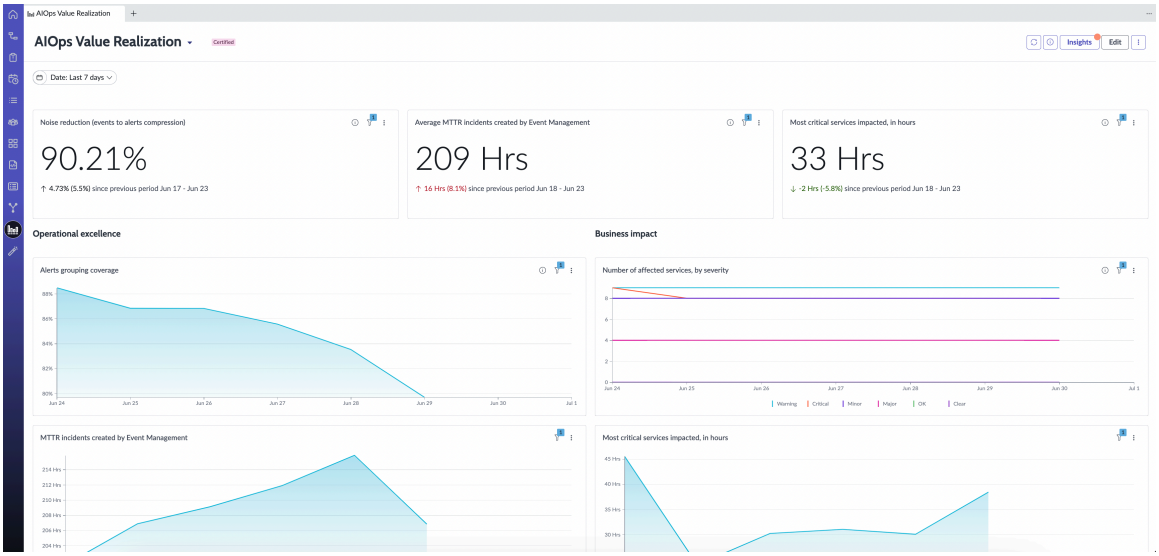
Das Dashboard „AIOps-Wertrealisierung“ bietet wichtige Einblicke und Metriken, die für die betriebliche Effizienz und die Bewertung der Geschäftsauswirkungen entscheidend sind. Es enthält Funktionen wie Rauschunterdrückung, um die Fokus auf kritische Probleme zu erhöhen, indem die Konvertierungen von Ereignissen in Warnungen reduziert werden. Die Nachverfolgung der durchschnittlichen MTTR für Incidents und das Messen der Ausfallzeit für kritische Services tragen zur Verbesserung der betrieblichen Effizienz und zur Priorisierung von Lösungen bei. Das Dashboard ist in die Abschnitte „Operative Exzellenz“ und „Geschäftsauswirkung“ kategorisiert. Es bietet detaillierte Informationen zur Gruppierung von Warnungen, zur schnellen Lösung von von Anwendern gemeldeten kritischen Incidents und zur Quantifizierung der Serviceauswirkungen nach Schweregrad, um die Betriebsstabilität zu optimieren.

Führen Sie den Auftrag „[PA EM] Verlaufsdatensammlung“ einmal aus, um die teilweise Erfassung von Verlaufsdaten Ereignismanagement zu aktivieren:

1. Navigieren zu **Alle** > **Performance Analytics** > **Datenerfasser** > **Aufträge**.
2. Wählen Sie [PA EM] Verlaufsdatensammlung aus.
3. Wählen Sie **Jetzt ausführen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Übersicht über die wichtigsten Funktionen des AIOps-Wertrealisierungs-Dashboards



Voraussetzungen

Stellen Sie sicher, dass die Anwendung Ereignismanagement installiert ist.

Erforderliche Now Platform-Rollen

- evt_mgmt_admin
- evt_mgmt_operator

Greifen Sie auf das Dashboard „AIOps-Wertrealisierung“ zu

Öffnen Sie das Dashboard mit einer der folgenden Methoden:

- Navigieren zu **Alle** > **AIOps – Dashboards** > **AIOps – Wert** > **Wertrealisierung**.
- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das AIOps-Dashboards-Symbol ( ). Wählen Sie dann im Dropdown-Menü **„AIOps – Operativ“die Option AIOps-Wertrealisierung**aus.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrer Organisation dieses Dashboard verwenden würden, finden Sie in den folgenden Anwendungsfällen.

Anwender	Dashboard-Verwendung
evt_mgmt_admin oder admin	Bearbeiten Sie das Dashboard, und erteilen Sie Anzeige- und Freigabeberechtigungen.
evt_mgmt_operator oder admin	Zeigen Sie das -Dashboard an, und überprüfen Sie Datensatzdetails, um die geschäftlichen Auswirkungen von Warnungen, Ereignissen und Incidents zu visualisieren und nachzuverfolgen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aufgliederungen

Im Dashboard „Wertrealisierung“ von AIOps sind folgende Aufgliederungen verfügbar:

- Operative Exzellenz
- Geschäftsauswirkung

Berichte

Titel	Typ	Beschreibung
Reduzierung des Datenrauschens (Ereignisse zu Warnungskomprimierung)	Liniendiagramm	Die Komprimierungsrate von Ereignissen zu Warnungserstellung: Eine höhere Zahl bedeutet, dass weniger Warnungen erstellt werden.
Durchschnittliche von erstellte MTTR-Incidents Ereignismanagement	Liniendiagramm	Die durchschnittliche durchschnittliche Zeit bis zur Reparatur eines incident, der von Ereignismanagementerstellt wurde: Eine niedrigere Zahl bedeutet eine höhere Effizienz des IT-Teams.
Die meisten betroffenen Services in Stunden	Liniendiagramm	Gesamtzeit, in der die wichtigsten Business Services Ihrer Organisation betroffen sind: Eine höhere Zahl bedeutet, dass zeitkritischere Services von offenen Warnungen betroffen sind.
Warnungsgruppierungsabdeckung	Liniendiagramm	Prozentsatz der Gesamtzahl der Warnungen, die gruppiert sind: Eine höhere Zahl bedeutet, dass mehr Warnungen korreliert und in einer Warnmeldungsgruppe gruppiert werden.
Anzahl der betroffenen Services nach Schweregrad	Liniendiagramm	Die Anzahl der Services, die von Warnungen betroffen sind, gruppiert nach Schweregrad, z. B. die Anzahl der Services, bei denen pro Tag kritische Probleme auftreten.
Anzahl der neuen P1-Incidents in überwachten Services, die von Anwendern erstellt wurden	Liniendiagramm	Anzahl der Incidents, die für von Ereignismanagementüberwachte Services erstellt wurden: Eine niedrigere Zahl bedeutet, dass weniger

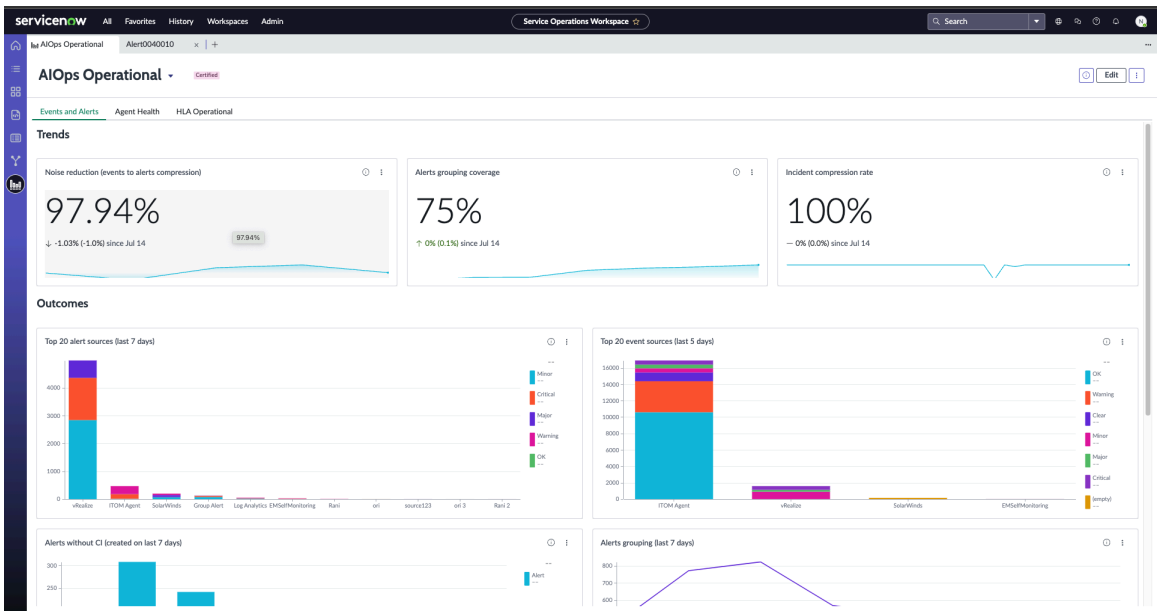
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
		Benutzer von einem Serviceausfall oder einer Leistungsverschlechterung betroffen sind.

Dashboard für Ereignisse und Warnungen

Das Dashboard für Ereignisse und Warnungen bietet mithilfe von Performance Analytics Echtzeittransparenz für Ereignisse und Warnungen in Ereignismanagementund zeigt wichtige Trends, Ergebnisse und die am stärksten betroffenen Configuration Items an. Hervorgehoben sind Metriken wie Reduzierung des Datenrauschens, Abdeckung durch Warnungsgruppierungen und häufigste Warnungsquellen.



Führen Sie den Auftrag „[PA EM] Verlaufsdatensammlung“ einmal aus, um die teilweise Erfassung von Verlaufsdaten Ereignismanagement zu aktivieren:

1. Navigieren zu **Alle** > **Performance Analytics** > **Datenerfasser** > **Aufträge**.
2. Wählen Sie [PA EM] Verlaufsdatensammlung aus.
3. Wählen Sie **Jetzt ausführen**.

Voraussetzungen

Stellen Sie sicher, dass die Anwendung Ereignismanagement installiert ist.

Erforderliche Now Platform-Rollen

- evt_mgmt_admin
- evt_mgmt_operator

Greifen Sie auf das Dashboard Ereignisse und Warnungen zu

Öffnen Sie das Dashboard mit einer der folgenden Methoden:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Navigieren zu **Alle** > **AIOps – Dashboards** > **AIOps – Operativ** > **Ereignisse und Warnungen**.
- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das AIOps-Dashboard-Symbol ( ).

  Standardmäßig ist die Registerkarte **Ereignisse und Warnungen** ausgewählt.

Anwendungsfälle

Beispiele dafür, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten, finden Sie in diesen Anwendungsfällen.

Anwender	Dashboard-Verwendung
evt_mgmt_admin oder admin	Bearbeiten Sie das Dashboard, und erteilen Sie Anzeige- und Freigabeberechtigungen.
evt_mgmt_operator oder admin	Zeigen Sie das -Dashboard und Details der darin enthaltenen Datensätze an, um Ereignisse, Warnungen, Trends, Ergebnisse und die am stärksten betroffenen Konfigurationselemente in Ihrer Organisation zu visualisieren und nachzuverfolgen.

Aufgliederungen

Im Dashboard für Ereignisse und Warnungen sind folgende Aufgliederungen verfügbar:

- Trends
- Ergebnisse

Berichte

Titel	Typ	Beschreibung
Reduzierung des Datenrauschens (Ereignisse zu Warnungskomprimierung)	Liniendiagramm	Die Komprimierungsrate von Ereignissen bis zur Warnungserstellung. Je höher die Zahl, desto weniger Warnungen werden erstellt.
Warnungsgruppierungsabdeckung	Liniendiagramm	Der Prozentsatz der Warnungen, die im Laufe der Zeit zu gruppierten Warnungen zusammengefasst wurden.
Incident-Komprimierungsrate	Liniendiagramm	Der Prozentsatz der Incidents, die aus Warnungen erstellt wurden.
20 häufigste Warnungsquellen (letzte 7 Tage)	Balkendiagramm	Die Anzahl der Warnungen pro Quelle, kategorisiert

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
		nach Schweregrad in den letzten 7 Tagen
Top 20 Ereignisquellen (letzte 5 Tage)	Balkendiagramm	Die Anzahl der Ereignisse pro Quelle, kategorisiert nach Schweregrad für die letzten 5 Tage.
Warnungen ohne CI (in den letzten 7 Tagen erstellt)	Liniendiagramm	Die Anzahl der Warnungen ohne CI-Bindung, die in den letzten 7 Tagen erstellt wurden.
Warnungsgruppierung (letzte 7 Tage)	Balkendiagramm	Die Verteilung gruppierter Warnungen in den letzten 7 Tagen.

Am häufigsten betroffene Konfigurationselemente

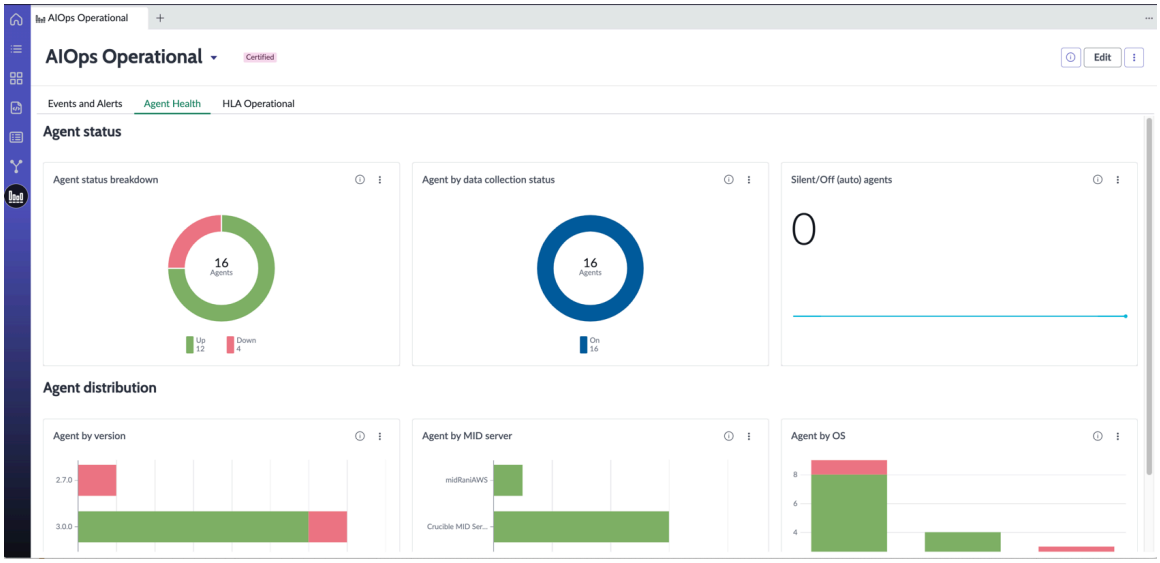
Der Abschnitt „Am stärksten betroffene Konfigurationselemente“ des Dashboards für Ereignisse und Warnungen bietet eine umfassende Übersicht über die Configuration Items (CIs), die am stärksten von dem Problem betroffen sind. In diesem Abschnitt werden wichtige Details aufgelistet, z. B. der Name jedes CI, die Anzahl der zugehörigen Warnungen, ihre Klassifizierung (z. B. Anwendungsservice) und ihr Standort. Darüber hinaus identifiziert es den Besitzer und die Supportgruppe, die für jedes CI verantwortlich sind, und ermöglicht so eine gezielte und effiziente Lösung von Incidents. Durch Hervorhebung der am stärksten betroffenen CIs hilft dieser Abschnitt bei der Priorisierung kritischer Assets und Ressourcen. So wird sichergestellt, dass die schwerwiegendsten Probleme umgehend behoben werden, um die Systemstabilität und -leistung aufrechtzuerhalten.

Agent Health-Dashboard

Das Dashboard „Agent Health“ bietet Einblick in den Status und die Verteilung der in Ihrem System installierten Agents. Damit können Sie schnell die Anzahl der bereitgestellten Service Desk-Mitarbeiter und deren Verteilung bewerten und Ihre Arbeit effizienter priorisieren.

Das folgende Beispiel zeigt, welche Agents in Ihrem System derzeit aktiv sind, welche Agents für die Datenerfassung konfiguriert sind und welche Agents die Datenerfassung aufgrund des Erreichens des CPU-Schwellenwerts (Still/Aus) gestoppt haben. Außerdem werden die -Agents nach Version, Betriebssystem und verbundenem MID-Serverangezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Voraussetzungen

Die Anwendung Agent Client Collector muss installiert sein.

Erforderliche Now Platform-Rollen

Ein Benutzer muss über die Rolle agent_client_collector_admin verfügen, um alle Widgets im Dashboard anzuzeigen.

Greifen Sie auf das Dashboard Ereignisse und Warnungen zu

Öffnen Sie das Dashboard mit einer der folgenden Methoden:

- Navigieren zu **Alle** > **AIOps – Dashboards** > **AIOps – Operativ** > **Agent-Integrität**.
- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das AIOps-Dashboard-Symbol ( ). Wählen Sie dann die Registerkarte **Agent Health (Agent** -Integrität).

- Nach dem Upgrade auf Discovery-Administratorarbeitsbereich Version 1.3.1 (Store August 2024) können Sie zu navigieren **Arbeitsbereiche** > **Discovery-Administratorarbeitsbereich** > **Einblicke** und verwenden Sie das erweiterte Dashboard.

Anwendungsfall

Beispiele dafür, wie verschiedene Personen in Ihrer Organisation dieses Dashboard verwenden würden, finden Sie im Anwendungsfall in der folgenden Tabelle.

Dashboard-Anwendungsfall

Anwender	Dashboard-Verwendung
Administrator	Einblick in den Status der Service Desk-Mitarbeiter.

Aufgliederungen

Für die Agent-Integrität sind folgende Aufgliederungen verfügbar:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Agent-Status: Der Status der derzeit in Ihrem System bereitgestellten Agents.
- Agent-Verteilung: Verteilung der Agents nach Versionsnummer des Agent, MID-Server, dem der Agent zugewiesen ist, und Betriebssystem, unter dem der Agent arbeitet.

Berichte

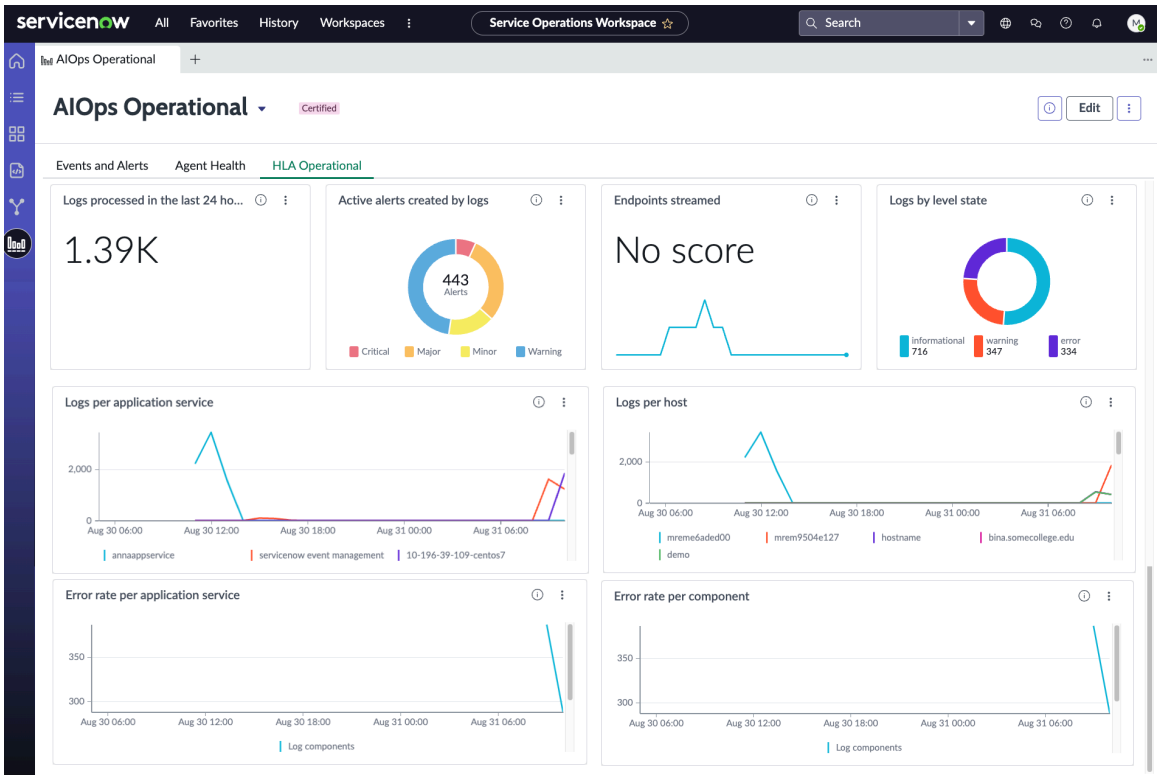
Titel	Typ	Beschreibung
Aufgliederung des Agentenstatus	Kreisdiagramm	In Ihrem System bereitgestellte Agents, die aktiv und inaktiv sind. Wählen Sie die entsprechende Farbe im Widget aus, um eine Liste der aktiven oder inaktiven Service Desk-Mitarbeiter anzuzeigen.
Agent nach Status der Datensammlung	Kreisdiagramm	In Ihrem System bereitgestellte Agents mit aktivierter und deaktivierter Datenerfassung. Wählen Sie die entsprechende Farbe im Widget aus, um eine Liste der Agents mit aktivierter oder deaktivierter Datenerfassung anzuzeigen.
Agenten stummschalten/ deaktivieren (automatisch)	Liniendiagramm	Agents, die das Sammeln von Daten automatisch beendet haben, nachdem sie den Schwellenwert für die CPU-Auslastung überschritten hatten. Der Schwellenwert für die CPU-Auslastung kann in der Konfigurationsdatei `acc.yml` konfiguriert werden. Weitere Informationen zur Konfigurationsdatei `acc.yml` finden Sie unter Konfigurationsdateioptionen.
Agent nach Version	Balkendiagramm	Aufgliederung der bereitgestellten Agents nach Versionsnummer.
Agent von *MID-Server*	Balkendiagramm	Aufgliederung der bereitgestellten Service Desk-Mitarbeiter gemäß den *MID-Server*, denen sie zugewiesen sind.
Agent nach Betriebssystem	Balkendiagramm	Aufgliederung der bereitgestellten Service Desk-Mitarbeiter nach den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
		Betriebssystemen, unter denen sie arbeiten.

Dashboard für HLA-Vorgänge

Das Dashboard Health Log Analytics Vorgänge verwendet Performance Analytics, damit Sie Protokolldaten, Warnungen und Fehlerrateninformationen in Service Operations-Arbeitsbereich überwachen und Probleme beheben können, sobald sie im System auftreten.



Voraussetzungen

Stellen Sie sicher, dass die Anwendung Health Log Analytics installiert ist.

Erforderliche Now Platform-Rollen

- evt_mgmt_admin
- evt_mgmt_operator

Greifen Sie auf das Dashboard HLA-Vorgänge zu

Öffnen Sie das Dashboard mit einer der folgenden Methoden:

- Navigieren zu **Alle** > **AIOps – Dashboards** > **AIOps – Operativ** > **HLA – Operativ**.
- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das AIOps-Dashboard-Symbol ( ). Zeigen Sie dann das Dashboard HLA-Vorgänge an.

Anwendungsfälle

Die folgenden Anwendungsfälle veranschaulichen, wie verschiedene Personen in Ihrem Unternehmen dieses Dashboard verwenden könnten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwender	Dashboard-Verwendung
evt_mgmt_admin	Bearbeitet das Dashboard und erteilt Ansichts- und Freigabeberechtigungen
evt_mgmt_operator oder evt_mgmt_admin	Überwacht das Dashboard, um HLA-Protokoll- und Warnungsdaten, Fehlerraten und andere relevante Informationen zu visualisieren und nachzuverfolgen.

Aufgliederungen

Im Dashboard „HLA-Vorgänge“ sind folgende Aufgliederungen verfügbar:

- HLA-Übersicht
- Fehlerrate

Berichte

Titel	Typ	Beschreibung
Verarbeitete Protokolle	Balkendiagramm	Die Anzahl der Protokolle, die im ausgewählten Zeitraum verarbeitet und analysiert wurden. Standardmäßig visualisiert das Dashboard Protokolldaten, die in den letzten 24 Stunden erfasst wurden.
Von Protokollen erstellte aktive Warnungen	Tabelle	Detaillierte Daten zu allen derzeit aktiven Warnungen.
Endpunkte gestreamt	Liniendiagramm	Die Anzahl der Endpunkte (IPs, Netzwerke und Geräte), die in Health Log Analyticsgestreamt werden, nach Anwendungsservice.
Protokolle nach Ebenenstatus	Balkendiagramm	Der Schweregrad der Protokolle für die Streamingquellen.
Protokolle pro Anwendungsservice	Liniendiagramm	Die Anzahl der Protokolle, die für jeden Anwendungsservice im ausgewählten Zeitraum gestreamt wurden. Überwachen Sie diese Daten, um sicherzustellen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Titel	Typ	Beschreibung
		dass die Protokolldaten für jeden Anwendungsservice wie erwartet gestreamt werden.
Protokolle pro Host	Liniendiagramm	Die Anzahl der verarbeiteten Protokolle für jeden Host im ausgewählten Zeitraum. Überwachen Sie diese Daten, um Hosts zu erkennen, die mehr oder weniger Daten als erwartet protokollieren.
Fehlerrate pro Anwendungsservice	Liniendiagramm	Die Anzahl der Protokolle mit Fehlern für jeden Anwendungsservice, der im ausgewählten Zeitraum analysiert wurde. Überwachen Sie diese Daten, um die Fehler weiter zu untersuchen. **Hinweis:** Health Log Analytics erstellt automatisch Warnungen für Fehleranomalien.
Fehlerrate pro Komponente	Liniendiagramm	Die Anzahl der Protokolle mit Fehlern für jede Komponente, die im ausgewählten Zeitraum analysiert wurden. Überwachen Sie diese Daten, um sicherzustellen, dass die Fehlerrate für jede Komponente normal ist.

Service Operations-Arbeitsbereich wird für ITOM Log Analytics verwendet

Zeigen Sie die Warnungen an, die Health Log Analytics im Service Operations-Arbeitsbereichgeneriert, und bearbeiten Sie sie.

Auf der Übersichtsregisterkarte Maßnahmen für Health Log Analytics-Warnungen ergreifen

Starten Sie den Fehlerkorrekturprozess über die Registerkarte **Übersicht** in Service Operations-Arbeitsbereich. Diese Registerkarte enthält Informationen zu Warnungen, Protokolldaten, die dem anomalen Verhalten zugeordnet sind, zu CIs, die die auslösende Metrik generiert haben, und zu Services, die von den Warnungen betroffen sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_user oder evt_mgmt_admin

Prozedur

1. Wählen Sie in Service Operations-Arbeitsbereich das Listensymbol ( ) aus.
2. Wählen Sie die entsprechende Liste in der Unterliste „Warnungen“ aus, und navigieren Sie zu der gewünschten Warnung oder Gruppe.

   Alle Health Log Analytics-Warnungen weisen in der Spalte **Quelle** den Wert **Log Analytics** auf. Durch den Wert in der Spalte **Gruppe** wird die Art der Log Analytics-Warnung identifiziert. Unter Typs von Health Log Analytics Warnungen finden Sie eine detailliertere Beschreibung der einzelnen Arten von Warnungen oder Gruppen.

   Tipp: Um die Vorschau einer Warnung in der Liste anzuzeigen, klicken Sie auf das zugehörige Info-Symbol ( ).

3. Wählen Sie die Warnungsnummer aus.

   Die Registerkarte **Übersicht** wird angezeigt.

4. Zeigen Sie den Abschnitt der Registerkarte **Übersicht** an, der die Informationen enthält, die Sie benötigen.

   Eine Beschreibung der Abschnitte und Karten finden Sie unter Abschnitte und Karten auf der Registerkarte „Warnungsübersicht“ in Health Log Analytics.

   Hinweis: Da in einigen Abschnitten der Registerkarte **Übersicht** nur ein Teil der Informationen zu sehen ist, enthalten viele Abschnitte einen Link, über den Sie andere oder vollständigere Informationen aufrufen können.

Abschnitte und Karten auf der Registerkarte „Übersicht“ für eine komponentenbasierte Warnung

Die Registerkarte **Übersicht** in Service Operations-Arbeitsbereich hilft Ihnen, komponentenbasierte Warnungen zu verstehen.

Eine detaillierte Beschreibung von Komponentenbasierte Warnungen finden Sie unter Typs von Health Log Analytics Warnungen.

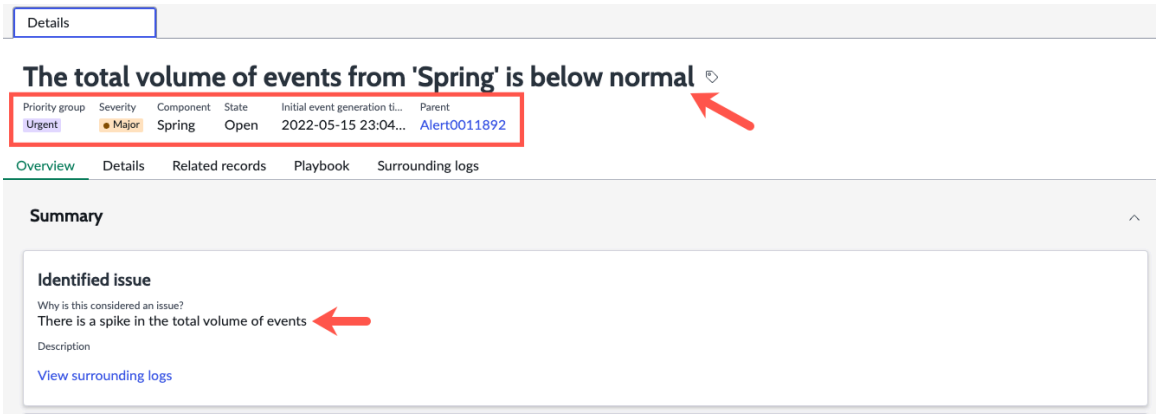
Zusammenfassung

Identifiziertes Problem

Auf dieser Karte wird das Problem beschrieben, das zu der Warnung geführt hat. Das identifizierte Problem wird auf der Karte und im Titel der Warnung angezeigt. Informationen zur Warnung werden im Banner angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identifiziertes Problem



Wählen Sie **Umgebende Protokolle anzeigen** aus, um Protokollnachrichten anzuzeigen, die für die Warnung relevant sind. Weitere Informationen finden Sie unter Protokollzeilen rund um eine Anomalie analysieren.

Abweichung

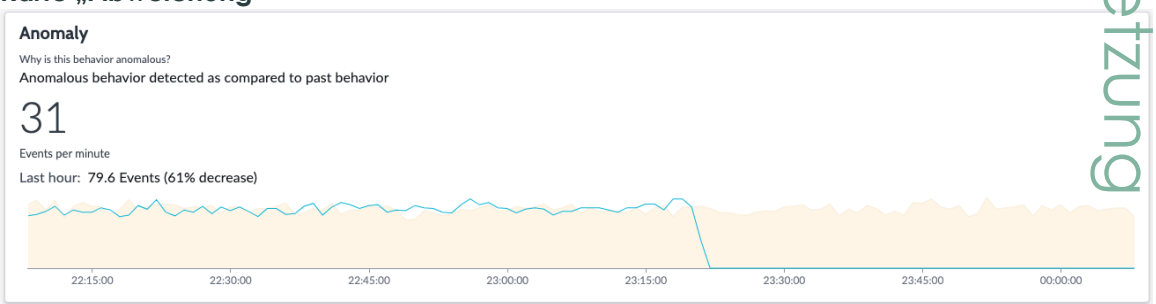
Auf dieser Karte wird die anomale Aktivität dargestellt, die zur Warnung geführt hat.

- Die blaue Linie zeigt die aktuelle anomale Aktivität an.
- In einigen Diagrammen zeigt der hell schattierte Bereich das erwartete Verhalten (erlernte Baseline) an.

  Ein pfirsichfarbener Bereich stellt die Baselinewerte für die gleiche Stunde einen Tag früher dar. Ein rosa schattierter Bereich zeigt die Werte für den gleichen Zeitraum in der vorherigen Woche an.

In diesem Beispiel zeigt der pfirsichfarben schattierte Bereich die Daten des vorherigen Tags zur gleichen Stunde. Das Abfallen des Metrikwerts (Ereignisse pro Minute) ist deutlich sichtbar.

Karte „Abweichung“



Weitere Informationen zu den Arten von Anomalien, die auftreten können, finden Sie unter Arten von anomalem Verhalten.

Auswirkung

Konfigurationselemente

Diese Karte enthält Informationen zu den CIs, die von der Warnung betroffen sind.

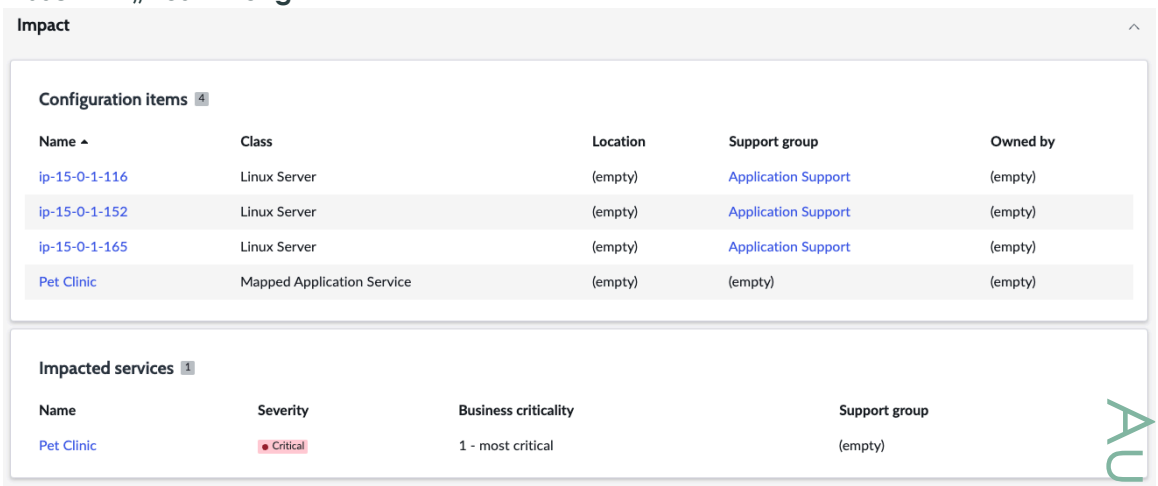
Betroffene Services

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Karte enthält Informationen zu den Services, die von der Warnung betroffen sind.

Abschnitt „Auswirkung“



Ursache

Aussagekräftige Protokolleigenschaften

Auf dieser Karte zeigt jedes Balkendiagramm die Verteilung der Werte für eine einzelne Protokolleigenschaft, die zur Anomalie beigetragen hat. Jeder Eigenschaftswert ist einer Farbe zugeordnet. Die Länge eines Farbbalkens entspricht dem Prozentsatz, der den Eigenschaftswert im Vergleich zu allen anderen Werten für die Eigenschaft darstellt.

Aussagekräftige Protokolleigenschaften

Abschnitte und Karten auf der Registerkarte „Übersicht“ für eine Log Analytics-Gruppe

Mithilfe der Registerkarte **Übersicht** in Service Operations-Arbeitsbereich können Sie Log Analytics-Gruppen korrekt interpretieren.

Eine detaillierte Beschreibung von Log Analytics-Gruppen finden Sie unter Typs von Health Log Analytics Warnungen.

Automatische Übersetzung

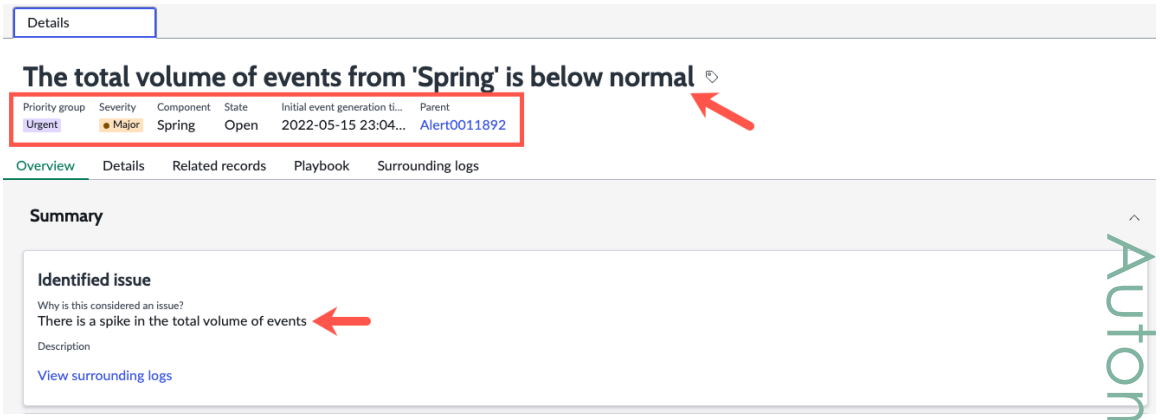
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammenfassung

Identifiziertes Problem

Auf dieser Karte wird das Problem beschrieben, das zu der Warnung geführt hat. Das identifizierte Problem wird auf der Karte und im Titel der Warnung angezeigt. Informationen zur Warnung werden im Banner angezeigt.

Identifiziertes Problem



Wählen Sie **Korrelationen anzeigen** aus, um die Liste der Korrelationen anzuzeigen, die sich auf die Log Analytics-Warnungen beziehen.

Liste „Korrelationen“

Während der ersten Analyse werden Warnungen bewertet. Jede Korrelation in Protokolldaten einer Warnung mit einer anderen Warnung trägt zur Punktzahl einer Warnung bei. Je höher die Punktzahl, desto wahrscheinlicher ist es, dass die Warnung als Log Analytics-Warnung in Log Analytics-Gruppeaufgenommen wird.

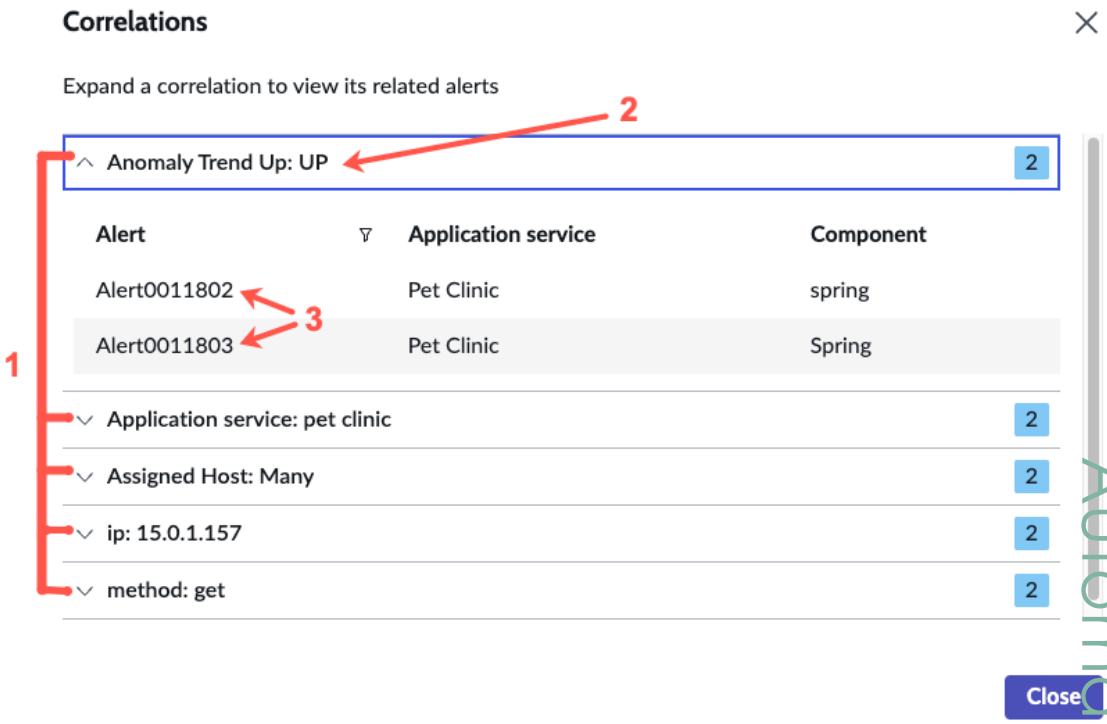
Die folgenden Arten von Daten werden berücksichtigt, wenn untersucht wird, ob Warnungen miteinander in Beziehung stehen:

- Zeit: Alle Events traten innerhalb eines konfigurierten Zeitintervalls auf.
- Metadaten: Die Warnungen haben übereinstimmende Werte in Protokollzeile-Metadaten. Beispielsweise beziehen sich alle Warnungen auf denselben Host.
- Nachrichtentext: Der Nachrichtentext in den Protokolldaten ist zwischen Warnungen ähnlich oder identisch.
- Trend: Die Warnungen zeigen eine ähnliche Tendenz bei Werten oder Raten. Beispielsweise steigt ein bestimmter Metrikwert in allen Warnungen an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Korrelationen

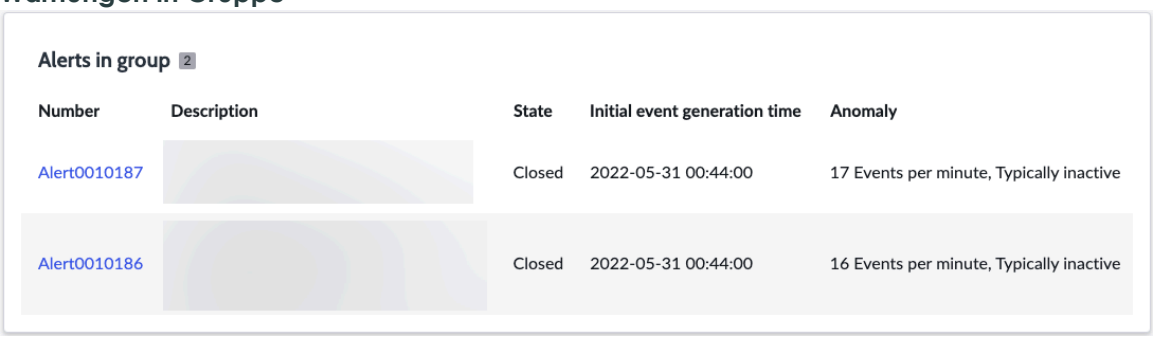


1. Liste der Korrelationen: Die erste Korrelation in der Liste wird erweitert, um die einzelnen Log Analytics-Warnungen anzuzeigen, die korrelieren, und Protokollkorrelator, die die Warnungen gemeinsam nutzen.
2. Ein einzelner Protokollkorrelator: Der Bezeichner für eine Gruppe von zugehörigen Log Analytics-Warnungen. Die Warnungen werden nach den Daten oder Metadaten der Protokollzeile gruppiert, die in mehreren Warnungen identisch sind (z. B. IP-Adresse, Hostname oder Benutzername). Die Zahl in dem blauen Quadrat ist die Anzahl der miteinander in Beziehung stehenden Warnungen.
3. Log Analytics-Warnungen, die korreliert sind.

Warnungen in Gruppe

Bei einer Log Analytics-Warnung werden auf der Karte Warnungen in Gruppe die Log Analytics-Warnungen angezeigt, die unter der Log Analytics-Warnung gruppiert sind. Wählen Sie eine Log Analytics-Warnung aus, um die zugehörigen Details anzuzeigen.

Warnungen in Gruppe



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wählen Sie **Alle anzeigen** aus, um die Liste aller Log Analytics-Warnungen in der Gruppe und relevante Informationen zu ihnen anzuzeigen. Sie können die Liste „Warnungen in Gruppe“ auch anzeigen, indem Sie die Registerkarte **Zugehörige Datensätze** und dann **Warnungen in Gruppe** auswählen. Weitere Informationen finden Sie unter Zeigen Sie die Liste der Log Analytics-Warnungen in einer Log Analytics-Gruppe an

Auswirkung

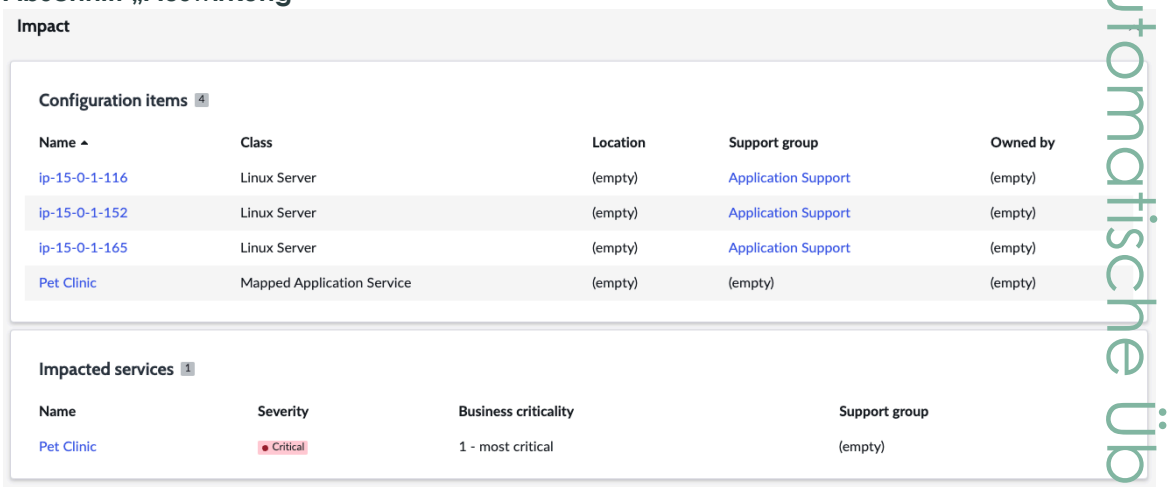
Konfigurationselemente

Diese Karte enthält Informationen zu den CIs, die von der Warnung betroffen sind.

Betroffene Services

Diese Karte enthält Informationen zu den Services, die von der Warnung betroffen sind.

Abschnitt „Auswirkung“



Zeigen Sie die Liste der Log Analytics-Warnungen in einer Log Analytics-Gruppe an

Zeigen Sie die Liste aller Log Analytics-Warnungen in einem Log Analytics-Gruppe auf der Registerkarte **Zugehörige Datensätze** an.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_user oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Eine detaillierte Beschreibung von Log Analytics -Gruppen und Log Analytics-Warnungen finden Sie unter Typs von Health Log Analytics Warnungen.

Prozedur

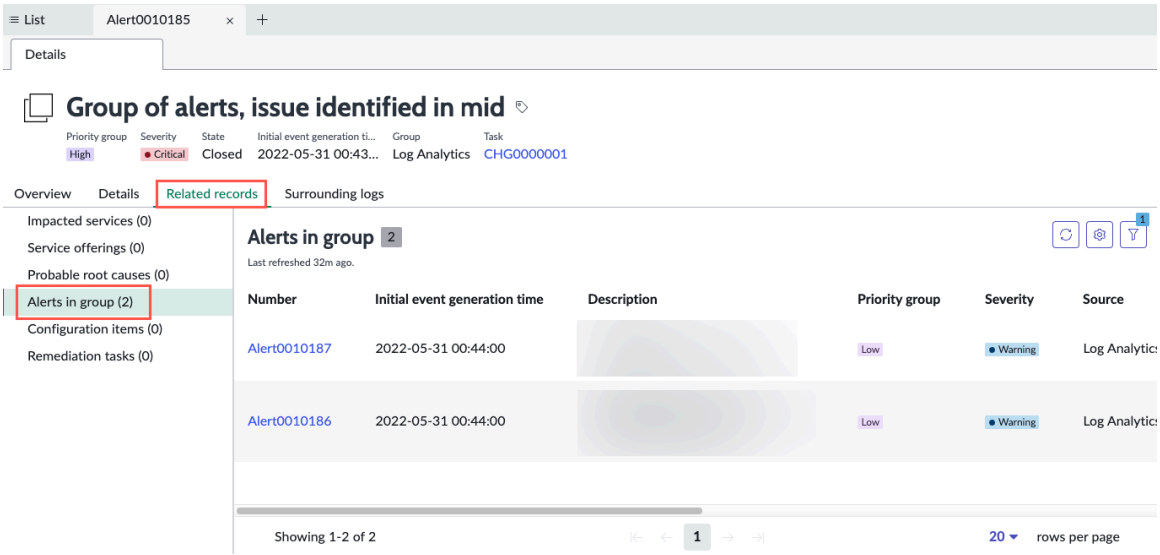
1. Wechseln Sie auf der Registerkarte **„Übersicht“** für eine Log Analytics-Warnung zur Karte **Warnungen in Gruppe**, und wählen Sie den Link **Alle anzeigen** aus.

   Der Abschnitt **Warnungen in Gruppe** auf der Registerkarte **Zugehörige Datensätze** wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Warnungen in Gruppe“ auf der Registerkarte „Zugehörige Datensätze“



2. Für jede Log Analytics-Warnung in Log Analytics-Gruppesind die in der Tabelle beschriebenen Informationen verfügbar.

Warnungen in Gruppe

Spalte	Beschreibung
Nummer	Die Nummer der Warnung. Wählen Sie die Nummer aus, um detaillierte Informationen zu einer Warnung anzuzeigen. Dieses Feld wird automatisch festgelegt.
Generierungszeit des ersten Events	Die Zeit, zu der das Ereignis, von dem die Warnung generiert wurde, zuerst aufgetreten ist. **Hinweis:** Dies ist die Verarbeitungszeit des ServiceNow-Systems, nicht die Zeit des Quellsystems.
Gruppe	Typ der Gruppe, zu der die Warnung gehört: eine eigenständige Log Analytics-Warnung oder eine Komponentenbasierte Warnung.
Beschreibung	Anomales Muster oder anomale Metrik, die die Generierung der Warnung verursacht haben.
Schweregrad	Schweregradwert für die Warnung. Verfügbare Werte:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	◦ **Kritisch**: Es ist eine sofortige Aktion erforderlich. Entweder funktioniert die Ressource nicht, oder es drohen kritische Probleme. ◦ **Schwerwiegend**: Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung hat sich verschlechtert. ◦ **Gering**: Die Leistung hat sich verschlechtert, oder es liegt ein partieller, nichtkritischer Verlust der Funktionalität vor. ◦ **Warnung**: Die Ressource funktioniert zwar noch, bedarf aber der Aufmerksamkeit. ◦ **Info**: Eine Informationsnachricht. Eine Warnung wird erstellt, die Ressource ist jedoch weiterhin funktionsfähig. ◦ **Löschen oder Gelöst**: Keine Aktion erforderlich. Aus diesem Event wird keine Warnung erstellt. Vorhandene Warnungen werden geschlossen.
Prioritätsgruppe	Prioritätsgruppe, die die Reihenfolge angibt, in der Warnungen gelöst werden sollen. Die Auswahlmöglichkeiten lauten wie folgt: ◦ **Dringend** ◦ **Hoch** ◦ **Mittel** ◦ **Niedrig** Der Wert der Prioritätsgruppe ist wichtiger als der Schweregrad allein. Beispielsweise sollte eine Warnung mit hoher Priorität und niedrigem Schweregrad vor einer Warnung mit niedriger Priorität und hohem Schweregrad behandelt werden. Informationen zur Berechnung der Priorität finden Sie unter Warnungspriorität.
Status	Verarbeitungsstatus der Warnung. Neu generierte Warnungen befinden sich im Status **Offen**. Andere Status lauten wie folgt: ◦ **Erneut öffnen**: Eine zuvor geschlossene Warnung wurde erneut geöffnet und erfordert Ihre Aufmerksamkeit. ◦ **Flatternd**: Die Warnung erhält identische Events, die mit hoher Häufigkeit aus derselben Quelle eintreffen. Dieser Status kann dazu führen, dass eine Warnung aus dem Status „Geschlossen“ erneut

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	geöffnet wird, was zu einer Anhäufung von Changes mit den Status „Offen“ und „Geschlossen“ führt. ◦ **Geschlossen**: Die Warnung wurde geschlossen und erfordert keine weitere Aktion. Sie schließen eine Warnung, wenn sie behoben wurde.
Konfigurationselement	CI in der CMDB. Das CI wird von der Warnung angewendet.
Knoten	Knotenfeld, das in der Protokollnachricht empfangen wurde. Das in der Protokollnachricht beschriebene Event ist auf diesem Knoten aufgetreten. Oft ist der Knoten der Name des CI, das der Warnung zugeordnet ist. Zum Beispiel ein Computername, eine IP-Adresse, ein FQDN oder eine MAC-Adresse.
Quelle	Alle Health Log Analytics-Warnungen weisen den Wert **Log Analytics** in der Spalte **„Quelle“** auf, um anzugeben, dass die App Health Log Analytics die Warnung generiert hat.
Metrikname	Name der Metrik, deren anomales Verhalten zu der Warnung geführt hat. Zum Beispiel *`I/O request`* für den Fall, dass die E/A-Anforderung länger als 15.000 ms dauerte.
Aktualisiert	Zeitpunkt der letzten Aktualisierung der Informationen oder des Status der Warnung.

Informationen auf der Registerkarte „Übersicht“ für eine Log Analytics-Warnung

Mithilfe der Registerkarte **Übersicht** in Service Operations-Arbeitsbereich können Sie Log Analytics-Warnungen korrekt interpretieren.

Eine detaillierte Beschreibung von Log Analytics-Warnungen finden Sie unter Typs von Health Log Analytics Warnungen.

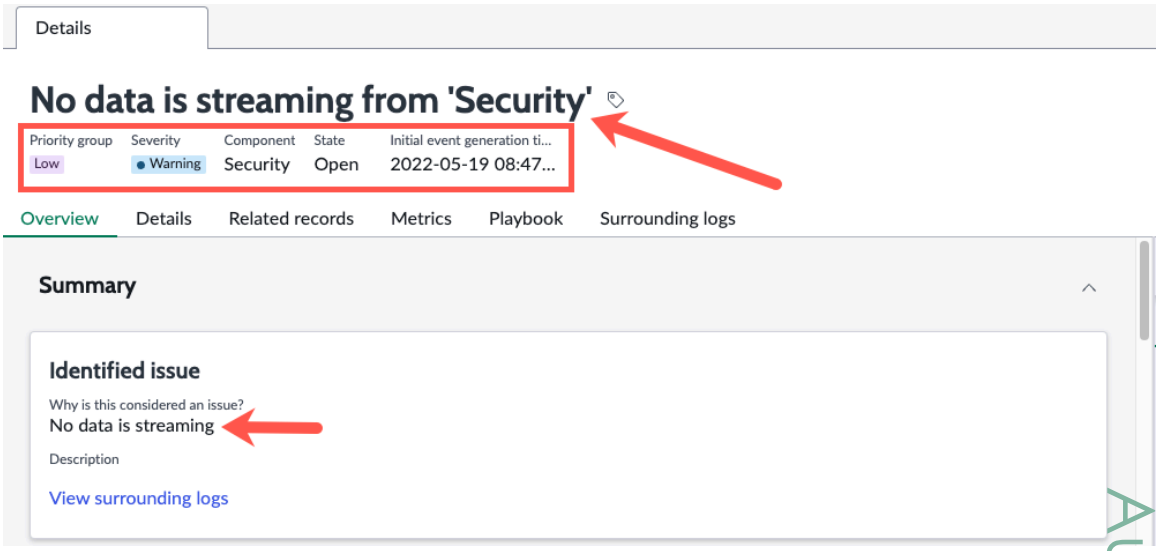
Zusammenfassung

Identifiziertes Problem

Auf dieser Karte wird das Problem beschrieben, das zu der Warnung geführt hat. Das identifizierte Problem wird auf der Karte und im Titel der Warnung angezeigt. Informationen zur Warnung werden im Banner angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Identifiziertes Problem



Wählen Sie **Umgebende Protokolle anzeigen** aus, um die Protokollzeilen anzuzeigen, die von einer Minute vor bis eine Minute nach der Warnung generiert wurden. Weitere Informationen finden Sie unter Protokollzeilen rund um eine Anomalie analysieren.

Abweichung

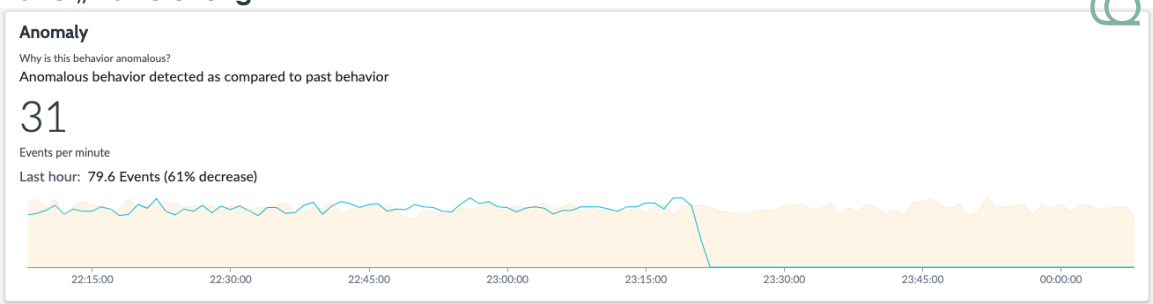
Auf dieser Karte wird die anomale Aktivität dargestellt, die zur Warnung geführt hat.

- Die blaue Linie zeigt die aktuelle anomale Aktivität an.
- In einigen Diagrammen zeigt der hell schattierte Bereich das erwartete Verhalten (erlernte Baseline) an.

  Ein pfirsichfarbener Bereich stellt die Baselinewerte für die gleiche Stunde einen Tag früher dar. Ein rosa schattierter Bereich zeigt die Werte für den gleichen Zeitraum in der vorherigen Woche an.

In diesem Beispiel zeigt der pfirsichfarben schattierte Bereich die Daten des vorherigen Tags zur gleichen Stunde. Das Abfallen des Metrikwerts (Ereignisse pro Minute) ist deutlich sichtbar.

Karte „Abweichung“



Weitere Informationen zu den Arten von Anomalien, die auftreten können, finden Sie unter Arten von anomalem Verhalten.

Auswirkung

Konfigurationselemente

Automatische Übersetzung

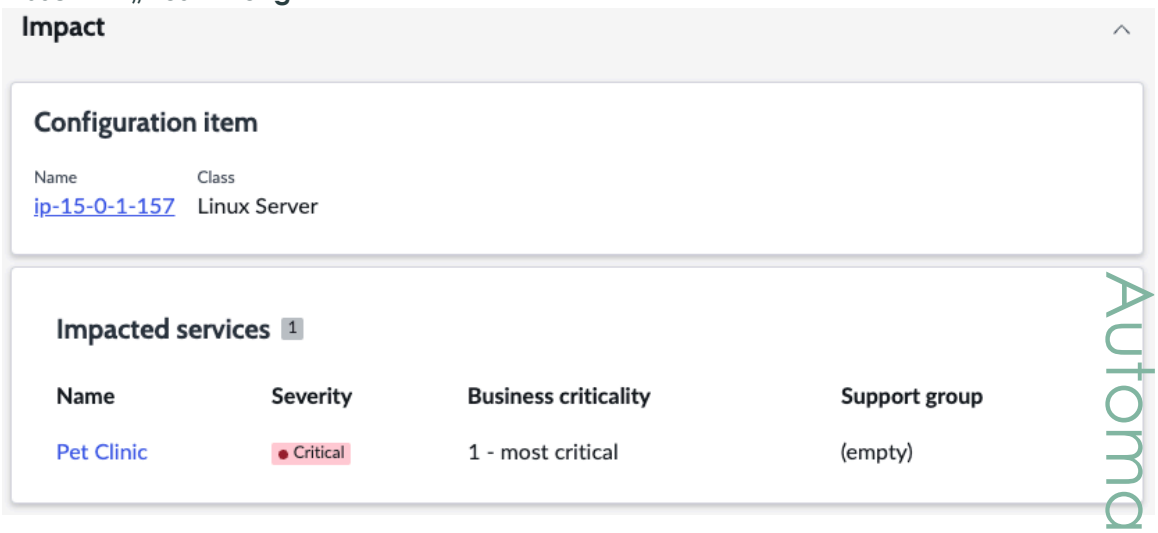
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diese Karte enthält Informationen zu den CIs, die von der Warnung betroffen sind.

Betroffene Services

Diese Karte enthält Informationen zu den Services, die von der Warnung betroffen sind.

Abschnitt „Auswirkung“

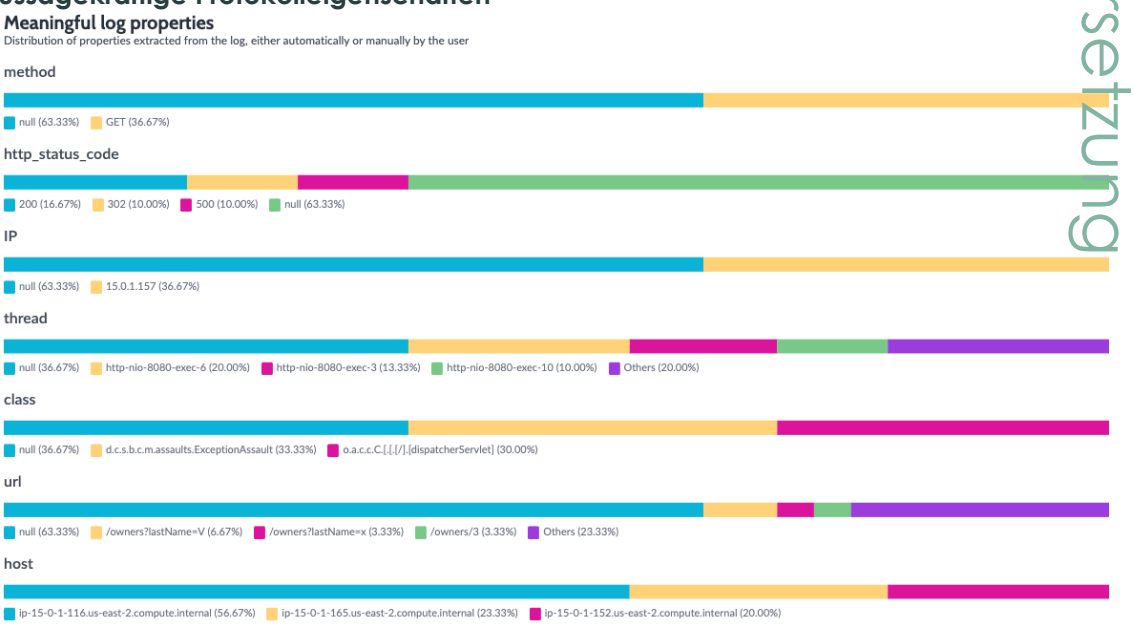


Ursache

Aussagekräftige Protokolleigenschaften

Auf dieser Karte zeigt jedes Balkendiagramm die Verteilung der Werte für eine einzelne Protokolleigenschaft, die zur Anomalie beigetragen hat. Jeder Eigenschaftswert ist einer Farbe zugeordnet. Die Länge eines Farbbalkens entspricht dem Prozentsatz, der den Eigenschaftswert im Vergleich zu allen anderen Werten für die Eigenschaft darstellt.

Aussagekräftige Protokolleigenschaften



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Protokollzeilen analysieren, um die Ursache einer Warnung zu identifizieren

Wenn Health Log Analytics eine Anomalie identifiziert, gibt die Anzeige der die Anomalie umgebenden Protokolle Hinweise auf den Status fehlerhafter Systeme. Mithilfe dieser Informationen können Sie die Ursache einer Warnung eingrenzen.

Bei der Anzeige einer Log Analytics -Warnung werden auf der Registerkarte **Umgebende Protokolle** die Protokollzeilen aufgelistet, die eine Minute vor und eine Sekunde nach dem Auftreten der Anomalie generiert wurden. Die Protokollzeilen beziehen sich auf die Metrik oder das Muster, die bzw. das die Warnung ausgelöst hat. Die Liste wird nach der entsprechenden Komponente gefiltert.

Sie können den Zeitbereich der angezeigten Protokollzeilen ändern, um beispielsweise Protokolle von mehr als einer Minute vor der Anomalie oder von mehr als einer Sekunde danach zu untersuchen.

Hinweis: Protokolle, die die Anomalie umgeben, werden aufbewahrt und sind nach Erstellung der Warnung 30 Tage lang verfügbar. Diese Protokolle werden vom System nicht gelöscht, wenn der globale Aufbewahrungszeitraum der Protokolle abgelaufen ist. Wenn der Aufbewahrungszeitraum abgelaufen ist, sind die umgebenden Protokolle nur auf der Registerkarte **Umgebende Protokolle** und nicht im Protokoll-Viewer verfügbar.

Health Log Analytics ermöglicht Ihnen die grafische Anzeige der anomalen Protokolldaten im Protokoll-Viewer, auf den Sie über Service Operations-Arbeitsbereichzugreifen. Der Protokoll-Viewer zeigt ein Diagramm der Häufigkeit der anomalen Protokollzeilen während einer Minute vor und eine Minute nach der Warnung Log Analytics an und listet die zugehörigen Protokollzeilen auf. Er zeigt automatisch die Abfrage im Zusammenhang mit der Anomalie, der ausgewählten Komponente und dem entsprechenden Zeitfilter an. Weitere Informationen finden Sie unter Protokolle für Warnung werden in der Protokollanzeige überprüft.

Zugehörige Informationen

Protokollzeilen rund um eine Anomalie analysieren

Protokollzeilen rund um eine Anomalie analysieren

Zeigen Sie die Protokollzeilen um eine Anomalie an, um die Ursache einer Log Analytics-Warnung zu identifizieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie in Service Operations-Arbeitsbereich eine Log Analytics-Warnung.
2. Wählen Sie die Registerkarte **Umgebende Protokolle** aus, und überprüfen Sie die Informationen.
   Auf der Registerkarte wird die Liste der Protokollzeilen angezeigt, die eine Minute vor und eine Sekunde nach der Log Analytics-Warnung erzeugt wurden. Eine Erklärung der Informationen auf der Registerkarte finden Sie unter Umgebende Protokollregisterkartenfelder.
3. Wahlweise: Zeigen Sie mit einer der folgenden Methoden einen anderen Zeitraum der Protokollzeilen an:
   - Aktualisieren Sie den Zeitbereich relativ zur Warnung auf einen vorgegebenen Zeitbereich in der Liste **Bereich auswählen**.
   - Geben Sie mithilfe der Zeitauswahl eine **Startzeit** oder **Endzeit** an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wahlweise: Um die anomalen Protokolldaten als Funktion der Zeit grafisch anzuzeigen, wählen Sie **Protokoll-Viewer** aus.
   Weitere Informationen finden Sie unter Protokolle für Warnung werden in der Protokollanzeige überprüft.

Protokolle für Warnung werden in der Protokollanzeige überprüft

Auf der Registerkarte **Protokoll-Viewer** können Sie die Protokolle nach einer Warnung nach Zeitstempel oder Zeitbereich durchsuchen und die Anomaliehäufigkeit innerhalb eines bestimmten Zeitraums visualisieren. Durch das Anpassen der angezeigten Daten und das Anpassen von Zeitfiltern können Sie das Framework, in dem die Anomalie aufgetreten ist, besser verstehen und die Ursache schneller finden.

Der Protokoll-Viewer zeigt alle mit der Log Analytics-Warnung verbundenen Daten an. Angezeigt werden die Abfrage, die sich auf die Anomalie, die ausgewählte Komponente und den entsprechenden Zeitfilter bezieht. Sie können die angezeigten Daten personalisieren und den Zeitbereich manuell anpassen, ohne die anderen Einstellungen zu beeinträchtigen. Die angewendeten Filter werden im Bereich **Filter** angezeigt. Sie können Filter nach Bedarf hinzufügen oder entfernen, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Der **Protokoll-Viewer** zeigt ein Diagramm der Häufigkeit anomaler Protokollzeilen während einer Minute vor und eine Minute nach der Warnung Log Analytics an und listet die zugehörigen Protokolldaten auf. Diese Informationen helfen Ihnen, Trends im Vorfeld und nach dem Ereignis zu identifizieren, und bieten Kontext für die Ursachenanalyse.

Während Sie die Protokolle für eine Warnung im **Protokoll-Viewer**analysieren, können Sie die Abfrage ändern, um die Suche zu optimieren, nützliche Suchvorgänge speichern und sie für andere freigeben. Eine Beschreibung der Informationen, die in der **Protokoll-Viewer** -Tabelle angezeigt werden, finden Sie unter Felder der Protokoll-Viewer-Tabelle.

In der **Protokollanzeige**können Sie folgende Aufgaben ausführen:

- Protokolldaten für eine Warnung anzeigen

  Zeigen Sie ein Diagramm der Häufigkeit anomaler Protokollzeilen und der zugehörigen Protokolldaten an.

- Suche nach Protokolldaten definieren, speichern und teilen

  Optimieren Sie die Suchabfrage, um die Ursachen des Problems zu ermitteln, und speichern und teilen Sie nützliche Suchvorgänge.

- Gespeicherte Suche verwenden oder ändern

  Verwenden Sie eine gespeicherte Suche. Als Besitzer einer gespeicherten Suche können Sie die Suchwerte ändern und Ihre Änderungen speichern.

- Im Protokoll-Viewer angezeigte Suchergebnisse filtern

  Wenden Sie Filter an, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

- Protokoll-Viewer-Tabelle anpassen

  Fügen Sie der Tabelle Spalten hinzu, oder entfernen Sie sie, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Wenn Sie in den Protokolldaten eine wichtige Metrik entdecken, können Sie damit eine neue Log Analytics Warnungsregel definieren. Weitere Informationen finden Sie unter Log Analytics-Warnungsregel hinzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Protokollzeilen analysieren, um die Ursache einer Warnung zu identifizieren

Protokolldaten für eine Warnung anzeigen

Zeigen Sie im Protokoll-Viewer ein Diagramm der Häufigkeit anomaler Protokollzeilen und der zugehörigen Protokolldaten an.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie die Registerkarte **Log viewer** (Protokoll-Viewer) mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Wählen Sie beim Anzeigen von Protokolleinträgen für eine Warnung auf der Registerkarte **Umgebende Protokolle** den **Protokoll-Viewer**.
2. Wahlweise: Personalisieren Sie die angezeigten Daten und ihre Darstellung im Protokoll-Viewer.
   - Im Protokoll-Viewer angezeigte Suchergebnisse filtern, um nur die Daten anzuzeigen, die Sie anzeigen möchten.
   - Protokoll-Viewer-Tabelle anpassen, indem Sie Spalten hinfügen oder entfernen.

   Diese Funktionen werden unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store .
3. Analysieren Sie protokollbasierte Anomalien und den hinzugefügten Kontext, um die durchschnittliche Zeit bis zur Reparatur (MTTR) zu verkürzen. Angenommen, Sie finden eine Protokollzeile mit Fehlern in einer Konfigurationsdatei. Auf der Karte **Anomalie** zeigt eine plötzliche Spitze im Diagramm an, wo die Konfigurationsdatei die Fehler generiert. Auf der Karte **Aussagekräftige Protokolleigenschaften** können Sie aus den Protokollen extrahierte zusätzliche Schlüssel-Wert-Paare anzeigen und die betroffenen Anwendungsservices und die zugehörigen Serviceangebote auf der Karte **Betroffene Services** herausfinden. Um den Kontext zu vergrößern, sollten Sie die Protokolle untersuchen, die die Anomalie umgeben, nach der Konfigurationsdatei suchen und den Zeitrahmen ermitteln, in dem die Probleme aufgetreten sind.

Nächste Maßnahme

Verwenden Sie zusätzliche Funktionen im Protokoll-Viewer, um Ihre Suche zu verfeinern oder Warnungen zu definieren.

- Ändern Sie die Suchabfrage, um die Suche zu optimieren und nützliche Suchen zu speichern. Weitere Informationen finden Sie unter Suche nach Protokolldaten definieren, speichern und teilen.
- Wenn Sie in den Protokolldaten wichtige Beziehungen entdecken, wählen Sie **Warnung definieren**, um die Art der Warnung zu definieren, die von den Daten ausgelöst werden soll. Anweisungen dazu finden Sie unter Log Analytics-Warnungsregel hinzufügen.

Zugehörige Informationen

Protokolle für Warnung werden in der Protokollanzeige überprüft

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suche nach Protokolldaten definieren, speichern und teilen

Definieren, speichern und teilen Sie Suchen nach Protokolldaten, um die Ursachen von Log Analytics-Warnungen zu ermitteln.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie den **Protokoll-Viewer** mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Wählen Sie beim Anzeigen von Protokolleinträgen für eine Warnung auf der Registerkarte **Umgebende Protokolle** den **Protokoll-Viewer**.
2. Definieren Sie eine Suche.

   a. Wählen Sie auf Auswahlsymbol ( ), und wählen Sie **Neue Suche** aus.

   b. Legen Sie die Werte der Suchparameter in den Suchfeldern fest.

Suchfelder

Suchfeld	Beschreibung
Abfrage	Suchabfrage. **Tipp:** Der Protokoll-Viewer nutzt die Suchmaschine Elasticsearch. Sie können daher im Feld **Abfrage** beliebige unterstützte Suchbegriffstrukturen verwenden.
Komponente	Logische Komponente von Serviceinstanz, die das Event generiert hat. Mehrere CIs können manchmal dieselbe Funktion ausführen.
Zeitbereich	Zeitbereich, der beim Anzeigen der zurückgegebenen Daten auf die X-Achse angewendet werden soll. Die von Ihnen angegebene Einstellung wird in den Feldern **Start time** (Startzeit) und **End time** (Endzeit) angezeigt. Verwenden Sie eine der folgenden Methoden: ▪ Wählen Sie einen Zeitraum aus der Liste aus. ▪ Klicken Sie auf **Benutzerdefinierter Bereich**, um über die Auswahl für Datum und Uhrzeit einen Bereich anzugeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Suchfeld	Beschreibung
	Hinweis: Sie können die Einstellungen in den Feldern **Startzeit** und **Endzeit** manuell ändern. Der ausgewählte Zeitraum, der in **Bereich auswählen** angezeigt wird, ändert sich dann zu „Benutzerdefinierter Bereich“. Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store . **Hinweis:** Gespeicherte Suchen enthalten keine Einstellungen für den Zeitbereich.

c. Klicken Sie auf **Search** (Suchen).

Das System gibt die vollständige Liste der Protokollzeilen zurück, die den Suchwerten entsprechen. Die Informationen werden im Diagramm „Ergebnisse im Zeitverlauf“ angezeigt.

3. Wahlweise: Speichern Sie die Suche.
Die gespeicherte Suche enthält die ausgewählten Filter. Weitere Informationen zu Filtern finden Sie unter Im Protokoll-Viewer angezeigte Suchergebnisse filtern.

Hinweis: Gespeicherte Suchen enthalten keine Einstellungen für den Zeitbereich.

a. Wählen Sie **Save As** (Speichern unter).

b. Geben Sie im Feld **Search name** (Suchname) einen eindeutigen und beschreibenden Namen für die Suche ein, und klicken Sie dann auf **Save** (Speichern).

Hinweis: Wenn Sie Health Log Analytics Die Anwendung Health Log Analytics Viewer, Version 20.0.11 – Juli 2021, verfügbar im ServiceNow Store verwenden, können Sie eine Warnungsregel definieren, ohne die Suche zu speichern. Weitere Informationen finden Sie unter Log Analytics-Warnungsregeln hinzufügen.

4. Wahlweise: Geben Sie die gespeicherte Suche für eine Zuweisungsgruppe frei.

a. Wählen Sie **Freigeben**.

b. Wählen Sie eine Zuweisungsgruppe aus der Liste aus.

c. Wählen Sie **Speichern**.

Zugehörige Informationen

Gespeicherte Suche verwenden oder ändern

Log Analytics-Warnungsregel hinzufügen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gespeicherte Suche verwenden oder ändern

Verwenden Sie eine gespeicherte Suche nach Protokolldaten, um die Ursachen einer Warnung besser zu verstehen. Als Besitzer einer gespeicherten Suche können Sie die Suchwerte ändern und Ihre Änderungen speichern.

Vorbereitungen

Hinweis: Wenn Sie nicht der Besitzer der gespeicherten Suche sind, speichern Sie die Suche unter einem anderen Namen. Anschließend können Sie Suchwerte aktualisieren, Ihre Änderungen speichern und die Suche für andere freigeben.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie den **Protokoll-Viewer** mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Wählen Sie beim Anzeigen von Protokolleinträgen für eine Warnung auf der Registerkarte **Umgebende Protokolle** den **Protokoll-Viewer**.
2. Verwenden Sie eine gespeicherte Suche.
   a. Wählen Sie auf Auswahlsymbol ( ), und wählen Sie **Suche laden** aus.
   b. Wählen Sie im Dialogfeld „Suche laden“ den Namen der zu ladenden Suche aus. Das System gibt die vollständige Liste der Protokollzeilen zurück, die den Suchwerten entsprechen, und zeigt die Informationen im Diagramm mit den Ergebnisse im Zeitverlauf an.
3. Wahlweise: Aktualisieren Sie die gespeicherte Suche.
   a. Klicken Sie auf das Auswahlsymbol ( ), und wählen Sie dann in der Dropdown-Liste die Option **Meine Suchen verwalten** aus.
   b. Ändern Sie die Einstellungen.

Formular „Meine Suchen verwalten“

Feld	Beschreibung
Name	Name der gespeicherten Suche.
Abfrage	Suchabfrage. (Optional) Der Protokoll-Viewer nutzt die Elasticsearch-Such-Engine. Sie können daher im Feld **Query** (Abfrage) beliebige unterstützte Suchbegriffstrukturen verwenden.
Zuweisungsgruppe	Zuweisungsgruppen, die auf die Suche zugreifen können. Die Mitglieder der Gruppen können die Suche verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Filter	Spaltenfilter im Standardformat (`field1=value1, field2=value2, field3=value3, ...`).
Aktualisiert	Datum und Uhrzeit der Aktualisierung der Suche. (Optional) Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store .

Um Änderungen an den Suchwerten rückgängig zu machen, wählen Sie das Auswahlsymbol ( ) und dann **Änderungen verwerfen** aus. Die Änderungen, die Sie an den Suchwerten vorgenommen haben, werden verworfen. Sie können die Sucheinstellungen weiterhin aktualisieren.

c. Speichern Sie die aktualisierte Suche.

i. Wählen Sie **Speichern unter** aus.

ii. Geben Sie im Feld **Search name** (Suchname) einen eindeutigen und beschreibenden Namen für die Suche ein, und klicken Sie dann auf **Save** (Speichern).

Im Protokoll-Viewer angezeigte Suchergebnisse filtern

Wenden Sie auf den **Protokoll-Viewer** Filter an, um nur die gewünschten Daten anzuzeigen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_user oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store .

Prozedur

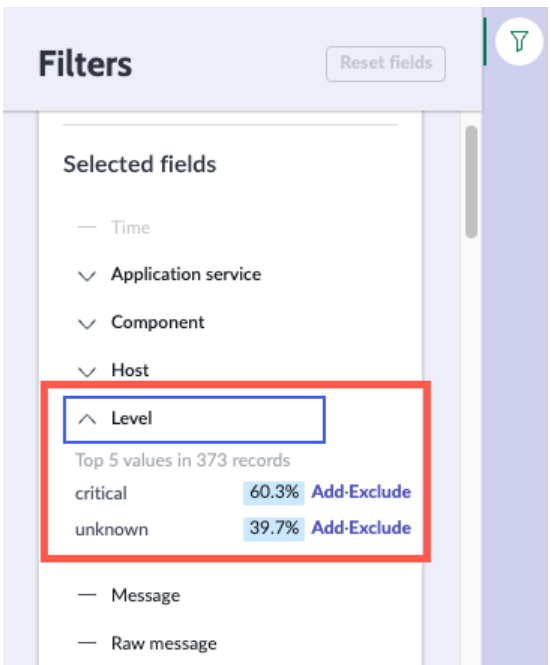
1. Öffnen Sie den **Protokoll-Viewer** mit einer der folgenden Methoden:

- Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das Protokoll-Viewer-Symbol ( ).
- Wählen Sie beim Anzeigen von Protokolleinträgen für eine Warnung auf der Registerkarte **Umgebende Protokolle** den **Protokoll-Viewer**.

2. Definieren Sie eine Suche, und führen Sie diese aus.
Weitere Informationen finden Sie unter Suche nach Protokolldaten definieren, speichern und teilen.

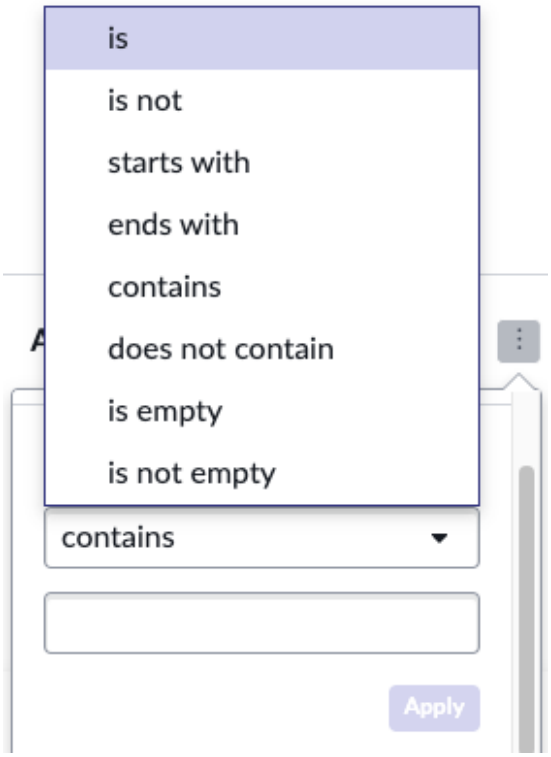
3. Filtern Sie die Suchergebnisse auf eine der folgenden Arten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
Filter mithilfe der Feldliste hinzufügen	**a.** Wählen Sie das Filtersymbol ( ) aus. Die Liste „Ausgewählte Felder“ enthält die Felder, die derzeit als Spalten in der Tabelle **Protokoll-Viewer** angezeigt werden. Standardmäßig enthält die Tabelle die folgenden Spalten: Anwendungsservice, Komponente, Host, Ebene, Nachricht, Rohnachricht und Zeit. Die Liste „Verfügbare Felder“ enthält alle verbleibenden Felder, die vom System aus dem Protokoll extrahiert wurden. **b.** Wählen Sie ein Feld in der Liste aus. **Hinweis:** Mit der Suchoption können Sie nach einem bestimmten Feld suchen. Die fünf wichtigsten Werte, die das System in den Datensätzen für dieses Feld gefunden hat, werden zusammen mit dem Prozentsatz ihrer Häufigkeit angezeigt.  **c.** Definieren Sie einen Filter für einen Wert im Feld. ▪ Um nur Daten anzuzeigen, die einen Wert enthalten, wählen Sie **Hinzufügen**. Um beispielsweise den Filter **[Ebene][ist] [kritisch]** festzulegen, wählen Sie **Hinzufügen** für den Wert „kritisch“ im Feld „Ebene“ aus.

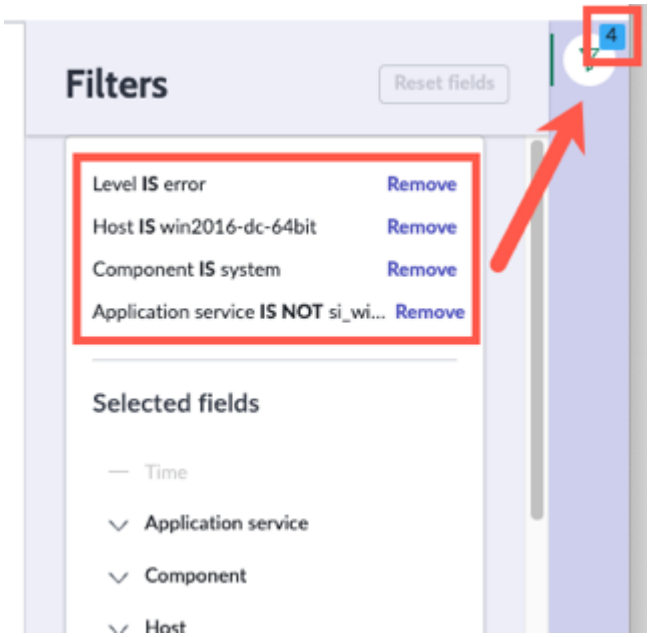
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	▪ Um negative Filter zu erstellen, die Daten ausschließen, die einen bestimmten Wert enthalten, wählen Sie **Ausschließen**. Um beispielsweise den Filter **[Ebene][ist nicht][kritisch]** festzulegen, wählen Sie **Ausschließen** für den Wert „kritisch“ im Feld „Ebene“ aus.
Filter aus der Tabelle **Protokoll-Viewer** hinzufügen	**a.** Wählen Sie in einem Spaltenheader das Symbol „Weitere Aktionen“ (⋮). **b.** Wählen Sie im Dialogfeld den Operator aus, und geben Sie die Filterbedingungen für das Feld an.  **c.** Wählen Sie **Übernehmen**. Ein Filtersymbol im Spaltenheader zeigt an, dass ein Filter für dieses Feld gilt.

Der angewendete Filter wird oben im Bereich **Filter** angezeigt. Die Gesamtanzahl der angewendeten Feldwertfilter im Symbol **Filter** wird angepasst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Wahlweise: Entfernen Sie einen Filter auf eine der folgenden Arten.
   - Im Bereich **Filter**:
     a. Suchen Sie den Filter, den Sie entfernen möchten.
     b. Wählen Sie **Entfernen**.
   - In einem Spaltenheader:
     a. Wählen Sie das Symbol „Weitere Aktionen“ (⋮).
     b. Wählen Sie den Filter aus, den Sie entfernen möchten.
     c. Wählen Sie **Filter entfernen**.

Protokoll-Viewer-Tabelle anpassen

Fügen Sie der Tabelle **Protokoll-Viewer** Spalten hinzu, oder entfernen Sie sie, um nur die Daten anzuzeigen, die Sie anzeigen möchten.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store .

Prozedur
1. Öffnen Sie den **Protokoll-Viewer** mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Wählen Sie beim Anzeigen von Protokolleinträgen für eine Warnung auf der Registerkarte **Umgebende Protokolle** den **Protokoll-Viewer**.
2. Wählen Sie das Filtersymbol ( ), um den Bereich **Filter** anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Liste „Ausgewählte Felder“ enthält die Felder, die derzeit als Spalten in der Tabelle **Protokoll-Viewer** angezeigt werden. Standardmäßig enthält die Tabelle die folgenden Spalten: Anwendungsservice, Komponente, Host, Ebene, Nachricht, Rohnachricht und Zeit. Die Felder „Verfügbar“ enthalten alle verbleibenden Felder, die das System aus dem Protokoll extrahiert hat.

In der Anwendung Service Operations-Arbeitsbereich Log Analytics, Version 21.2.7 – November 2022 und höher, verfügbar im ServiceNow Store , wird die Spalte Protokollnachricht hinzugefügt und die Spalte Rohnachricht standardmäßig nicht mehr angezeigt. Sie können die Spalte „Rohnachricht“ zur Tabelle hinzufügen, indem Sie sie im Bereich **Filter** auswählen.

3. Fügen Sie der Tabelle **Protokoll-Viewer** Spalten hinzu, oder entfernen Sie Spalten.
   - Um der Tabelle eine Spalte hinzuzufügen, wählen Sie das gleichnamige Feld in der Liste „Verfügbare Felder“ und dann das Symbol zum Hinzufügen ( ) aus.

     Das hinzugefügte Feld wird als Spalte in der Tabelle angezeigt. Es wird jetzt in der Liste „Ausgewählte Felder“ aufgeführt.
   - Um eine Spalte aus der Tabelle zu entfernen, wählen Sie das gleichnamige Feld in der Liste „Ausgewählte Felder“ und dann das Symbol zum Entfernen ( ) aus.

     Die entsprechende Spalte wird aus der Tabelle entfernt. Das entfernte Feld wird der Liste „Verfügbare Felder“ hinzugefügt.

     Wenn Sie die Daten nach bestimmten Werten in einem Feld gefiltert haben, werden diese Daten auch dann angezeigt, wenn das Feld nicht mehr ausgewählt ist. Weitere Informationen zum Filtern von Daten finden Sie unter Im Protokoll-Viewer angezeigte Suchergebnisse filtern.

     Hinweis: Die Spalte „Zeit“ kann nicht aus der Tabelle entfernt werden.

4. Wahlweise: Passen Sie die maximale Anzahl von Zeichen pro Feld in der Tabelle an.
   a. Navigieren zu **Health Log Analytics** > **Health Log Analytics-Verwaltung** > **Systemeigenschaften**.
   b. Öffnen Sie den Eigenschaftendatensatz *sn_occ.log_viewer.max.characters*.
   c. Bearbeiten Sie den Standardwert im Feld **Wert**.
   d. Wählen Sie **Aktualisieren**.

Ergebnisse

Die Tabelle **Protokoll-Viewer** zeigt die benutzerdefinierte Ansicht ab der laufenden Sitzung solange an, bis Sie die Einstellungen ändern.

Warnungsregeln Log Analytics werden hinzugefügt, geändert oder gelöscht

Fügen Sie eine Warnungsregel hinzu, die eine Warnung für eine angegebene Metrik generiert, ändern oder löschen Sie sie.

Weitere Informationen finden Sie unter Mithilfe von Warnungsregeln steuern, wann Health Log Analytics Warnungen generiert.

Log Analytics-Warnungsregel hinzufügen

Definieren Sie eine Warnungsregel Log Analytics, wenn Sie auf Protokolldaten stoßen, die eine Warnung generieren sollen. Die Warnungsregel generiert eine Warnung für eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

angegebene Metrik mit einem von Ihnen angegebenen Schwellenwert und legt die Eigenschaften der generierten Warnung fest.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie den **Protokoll-Viewer** mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Wählen Sie beim Anzeigen von Protokolleinträgen für eine Warnung auf der Registerkarte **Umgebende Protokolle** den **Protokoll-Viewer**.
2. Definieren Sie eine Suche, und führen Sie diese aus.
   Weitere Informationen finden Sie unter Suche nach Protokolldaten definieren, speichern und teilen.
3. Wenn eine Suche Protokolldaten zurückgibt, die eine Warnung generieren sollten, klicken Sie auf **Speichern** oder **Speichern unter**, um die Suche zu speichern.

   Hinweis: Wenn Sie Health Log Analytics Die Anwendung Health Log Analytics Viewer, Version 20.0.11 – Juli 2021, verfügbar im ServiceNow Store verwenden, müssen Sie diesen Schritt nicht ausführen.

4. Greifen Sie auf das Formular zum Erstellen einer Warnungsregel zu, indem Sie oben rechts auf der Registerkarte **Protokoll-Viewer** die Option **Warnung definieren** auswählen.
5. Geben Sie im Formular den Namen und die Beschreibung für die Warnungsregel an.
   Der Name wird auf der Anomaliekarte für generierte Warnungen angezeigt.
6. Bestimmen Sie, ob die Regel Warnungen generiert, wenn die Schwellenwertbedingungen in den Protokolldaten erfüllt sind, indem Sie das Feld **Status** festlegen.
   Um die Regel zu aktivieren, wählen Sie **Aktiviert**aus.
7. Wenn Sie die Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, installiert haben, legen Sie die Schweregradwert für die von dieser Warnungsregel generierte Warnung.Option fest.
   - **Niedrig**: Die Ressource funktioniert zwar noch, bedarf aber der Aufmerksamkeit.
   - **Mittel**: Die Leistung hat sich verschlechtert, oder es liegt ein partieller, nichtkritischer Verlust der Funktionalität vor.
   - **Hoch**: Wichtige Funktionalität ist schwer beeinträchtigt, oder die Leistung hat sich verschlechtert.
   - **Kritisch**: Es ist eine sofortige Aktion erforderlich. Entweder funktioniert die Ressource nicht, oder es drohen kritische Probleme.
8. Wenn Sie die Anwendung Health Log Analytics, Version 20.0.11 - Juli 2021, und die Anwendung Health Log Analytics Viewer, Version 20.0.4 - Juli 2021, installiert haben, geben Sie die Details für die Abfrage ein.

Abfragedetails

Feld	Beschreibung
Ihre Abfrage	Die Abfrage, nach der in den Protokolldaten gesucht werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Standardmäßig ist dies die Abfrage, die im Protokoll-Viewer definiert wurde. Sie können die Abfrage ändern, indem Sie Suchanforderungen hinzufügen. Um nach allen Abfragen zu suchen, geben Sie ein Sternchen (*) an.
Aktive Filter	Die für die Abfrage im Protokoll-Viewer definierten Filter. Sie können die Filter löschen.
Komponente	Die Komponente, für die diese Warnungsregel gilt. Standardmäßig ist dies die Komponente, die im Protokoll-Viewer definiert wurde. Sie können eine andere Komponente auswählen, indem Sie in der Komponentenzeile das Suchsymbol ( ) wählen und dann die erforderliche Komponente aus der Liste auswählen.

9. Füllen Sie die Felder aus, die sich auf den Schwellenwert beziehen, der die Warnungsregel auslöst.

Schwellenwert

Feld	Beschreibung
Operator	Mathematischer Vergleichsoperator, der festlegt, wie die Trefferanzahl eine Warnung dieser Art auslöst. Dieses Feld wird automatisch auf „Größer als“ festgelegt.
Trefferanzahl	Anzahl der übereinstimmenden Protokolleinträge, die als Auslöser für eine solche Warnung dienen.
Zeitraum	Zeitraum, über den die Trefferanzahl gemessen wird. Die Zeit wird in den Einheiten gemessen, die durch den Wert **Time unit** (Zeiteinheit) vorgegeben wird.
Time unit (Zeiteinheit)	Einheiten des Zeitraums. Dieses Feld wird automatisch auf Minuten gesetzt.
Persistenz	Zeitraum, über den die angegebene Trefferanzahl pro Zeiteinheit bestehen bleiben muss, um eine Warnung dieser Art auszulösen. Dieses Feld wird automatisch auf 1 Minute gesetzt.

10. Wählen Sie **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ändern Sie eine definierte Warnungsregel Log Analytics .

Ändern Sie eine Log Analytics Warnungsregel, die Sie definiert haben.

Vorbereitungen

Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store .

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie den **Protokoll-Viewer** mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Wählen Sie beim Anzeigen von Protokolleinträgen für eine Warnung auf der Registerkarte **Umgebende Protokolle** den **Protokoll-Viewer**.
2. Öffnen Sie eine definierte Warnung.
   a. Wählen Sie oben rechts auf der Registerkarte **Protokoll-Viewer** das Auswahlsymbol ( ), und wählen Sie dann in der Dropdown-Liste die Option **Meine definierten Warnungen verwalten** aus.
   b. Wählen Sie in der Tabelle **Definierte Warnungen** die Warnungsregel aus, die Sie ändern möchten.
3. Aktualisieren Sie im Formular die Einstellungen.
   Eine Beschreibung der Einstellungen finden Sie unter Log Analytics-Warnungsregel hinzufügen.
4. Wählen Sie **Speichern** aus, um die Änderungen zu speichern.

Löschen Sie eine definierte Warnungsregel Log Analytics .

Löschen Sie eine von Ihnen definierte Warnungsregel Log Analytics, wenn sie nicht mehr benötigt wird.

Vorbereitungen

Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 20.0.11 – Juli 2021, und der Anwendung Health Log Analytics Viewer, Version 20.0.4 – Juli 2021, verfügbar im ServiceNow Store .

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie den **Protokoll-Viewer** mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Wählen Sie beim Anzeigen von Protokolleinträgen für eine Warnung auf der Registerkarte **Umgebende Protokolle** den **Protokoll-Viewer**.
2. Öffnen Sie eine definierte Warnung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie oben rechts auf der Registerkarte **Protokoll-Viewer** das Auswahlsymbol ( ), und wählen Sie dann in der Dropdown-Liste die Option **Meine definierten Warnungen verwalten** aus.

b. Wählen Sie in der Tabelle **Definierte Warnungen** die Warnung aus, die Sie löschen möchten.

3. Wählen Sie **Löschen**.

Einer Warnung in eine höhere oder niedrigere Bedeutung zuweisen Health Log Analytics

Kennzeichnen Sie eine Warnung als bedeutungsvoll oder unbedeutend, oder stellen Sie der Metrik, die an der Generierung beteiligt war, die normale Wichtigkeit wieder her.

Warnung als signifikant markieren

Sorgen Sie dafür, dass eine Warnung eher in eine Log Analytics-Gruppe aufgenommen wird, wenn sich die zugeordnete Metrik anomal verhält, indem Sie die Warnung als aussagekräftig kennzeichnen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Öffnen Sie in Service Operations-Arbeitsbereicheine Warnung vom Log Analytics Typ , und wählen Sie dann **ML-Feedback anwenden** > **Als signifikant markieren**.
2. Bestätigen Sie die Aktion im Dialogfeld.

   Hinweis: Die Verarbeitung dieses Feedbacks kann einige Sekunden dauern.

3. Wahlweise: Stellen Sie die signifikante Warnung wieder her.
   Wenn Sie nicht mehr möchten, dass die signifikante Warnung besonders behandelt wird, können Sie die normale Relevanz der Warnungsmetrik wiederherstellen. Weitere Informationen finden Sie unter Normale Wichtigkeit einer Warnungsmetrik wiederherstellen.

Irrelevante Warnungen stummschalten

Beseitigen Sie störende neue Warnungen für unwichtige Probleme, indem Sie sie stummschalten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie eine Warnung stummschalten, die auf der Stichwortmetrik oder der Musterschweregradmetrik basiert, schaltet das System die Metrik im dominanten Muster stumm. Das dominante Muster ist das Hauptmuster, das die Anomalie hervorruft. Nur für die angegebene Quelle werden bei anomalem Verhalten für die Metrik, die der stummgeschalteten Warnung zugeordnet ist, keine Warnungen mehr generiert. Sie können auch die Metrik, die einer unwichtigen Warnung zugeordnet ist, für alle Komponenten des Anwendungsservice stummschalten. Eine Komponente kann aus mehreren CIs bestehen, die dieselbe Funktion ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie in Service Operations-Arbeitsbereich die Log Analytics-Warnung, die Sie nicht mehr sehen möchten.
2. Auswahlvorgang **ML-Feedback anwenden**
3. Schalten Sie die der Warnung zugeordnete Metrik mit einer der folgenden Aktionen stumm:
   - Wählen Sie **Warnungsmetrik stummschalten** aus, um die Metrik nur für die angegebene Quelle stummzuschalten.
   - Wählen Sie **Warnungsmetriken für alle Komponenten stummschalten** aus, um die Metriken für alle Komponenten des Anwendungsservice stummschalten.
4. Bestätigen Sie die Aktion im Dialogfeld.

   Hinweis: Die Verarbeitung dieses Feedbacks kann einige Sekunden dauern.

5. Wahlweise: Stellen Sie die stummgeschaltete Warnung wieder her.
   Wenn Sie nicht mehr möchten, dass die stummgeschaltete Warnung besonders behandelt wird, können Sie die normale Relevanz der Warnungsmetrik wiederherstellen. Weitere Informationen finden Sie unter Normale Wichtigkeit einer Warnungsmetrik wiederherstellen.

Zugehörige Informationen

Liste der stummgeschalteten Metriken anzeigen

Sensitivität bei ähnlichen Anomalien verringern

Verringern Sie bei der Health Log Analytics-Anomalie-Erkennung die Sensitivität gegenüber Anomalien wie denjenigen, durch die die aktuelle Log Analytics-Warnung ausgelöst wurde.

Vorbereitungen

Hinweis: Diese Funktionalität ist für Kundenwarnungen und Warnungen hinsichtlich neuer Signale nicht verfügbar.

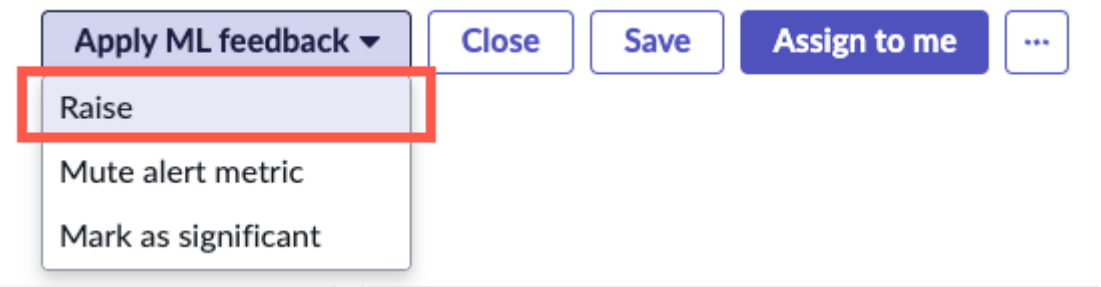
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Durch Auswahl der Option „Raise“ (Erhöhen) wird der Rückmeldungsschwellenwert für die Generierung von Warnungen erhöht, wenn von Health Log Analytics zukünftige Anomalien identifiziert werden, die derjenigen ähneln, die zu dieser Warnung geführt hat.

Prozedur

1. Öffnen Sie in Service Operations-Arbeitsbereicheine Warnung vom Log Analytics Typ , und wählen Sie dann **ML-Feedback anwenden** > **Erhöhen**.



2. Bestätigen Sie die Aktion im Dialogfeld.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Verarbeitung dieses Feedbacks kann einige Sekunden dauern.

3. Wahlweise: Stellen Sie die normale Sensitivität gegenüber Anomalien wie derjenigen wieder her, durch die diese Warnung ausgelöst wurde.
   a. Wählen Sie beim Anzeigen der Warnung **Feedback entfernen** aus.
   b. Bestätigen Sie die Aktion im Dialogfeld.

Normale Wichtigkeit einer Warnungsmetrik wiederherstellen

Stellen Sie die normale Signifikanz der Metrik wieder her, die an der Generierung einer Log Analytics-Warnung beteiligt ist. Verwenden Sie diese Option, wenn eine Warnung nicht mehr besonders behandelt werden soll, die stummgeschaltet, als signifikant markiert oder deren Sensitivität gegenüber ähnlichen Anomalien verringert wurde.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Wählen Sie beim Anzeigen einer Log Analytics -Warnung in Service Operations-Arbeitsbereich**die Option ML-Feedback wiederherstellen aus**.
2. Bestätigen Sie die Aktion im Dialogfeld.

Ergebnisse
Die Metrik, die der Warnung zugeordnet ist, nimmt wieder ihre normale Relevanz an.

Dashboards zur Echtzeitvisualisierung von Protokolldaten

Health Log Analytics ermöglicht Ihnen die Erstellung von Protokolldaten-Dashboards und -visualisierungen in Echtzeit für eine verbesserte Datenüberwachung und eine schnellere Identifizierung von Abweichungen.

Protokolldaten-Dashboards und -visualisierungen können Ihnen ein allgemeines visuelles Verständnis wichtiger Probleme vermitteln, wenn sie im System auftreten. Die Health Log Analytics-Datenquelle Ihrer Wahl wird dazu verwendet, die für die Visualisierung bereitgestellten Daten zu erfassen. Die Protokolldaten werden direkt aus den gespeicherten Protokollen übernommen, sodass Sie Dashboards für jeden Aspekt der Daten erstellen können, der Sie interessiert. Durch die Visualisierung der Komponenten, von denen Protokolle generiert werden, erhalten Sie beispielsweise einen Hinweis auf die Anzahl der vollständig integrierten Komponenten.

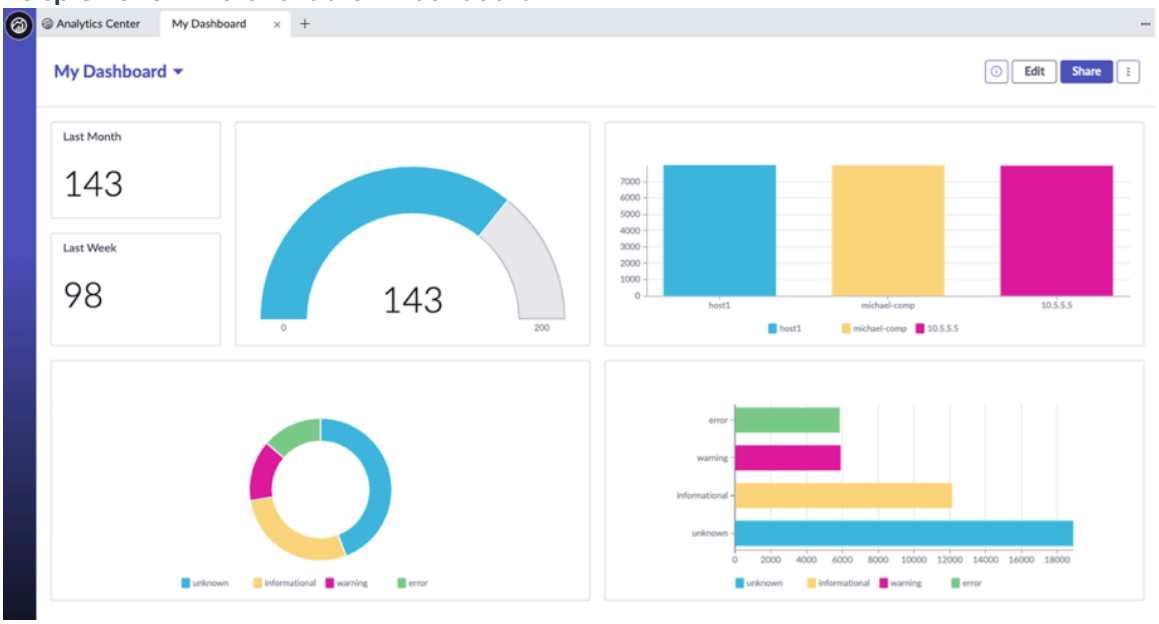
Die Daten können in verschiedenen Arten von Grafiken und Diagrammen dargestellt werden. Sie können den Zeitbereich und die anderen Einstellungen der Visualisierung nach Bedarf anpassen.

Diese Funktionalität wird in der Anwendung Service Operations-Arbeitsbereich Log Analytics, Version 21.2.7 – November 2022 und höher, unterstützt und ist vom Platform Analytics Workspace abhängig, der im ServiceNow Store verfügbar ist.

Alternativ zur Definition eines eigenen Dashboards können Sie die AIOps-Dashboards verwenden, die umfassende Visualisierungen kritischer Betriebsdaten bieten. Weitere Informationen finden Sie unter AIOps – Dashboards in Service Operations-Arbeitsbereich für ITOM.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für ein Protokolldaten-Dashboard



Protokolldaten-Dashboards und -visualisierungen erstellen

Erstellen Sie Dashboards und Visualisierungen für Health Log Analytics-Protokolldaten in Echtzeit, um Probleme leichter zu identifizieren und zu verstehen.

Vorbereitungen

Diese Funktionalität wird in der Anwendung Service Operations-Arbeitsbereich Log Analytics, Version 21.2.7 – November 2022 und höher, unterstützt und ist vom Platform Analytics Workspace abhängig, der im ServiceNow Store verfügbar ist.

Ausführliche Informationen zum Erstellen und Arbeiten mit Dashboards finden Sie unter Dashboards im Analytics Center .

Hinweis: Alternativ zur Definition eines eigenen Dashboards können Sie die AIOps-Dashboards verwenden, die umfassende Visualisierungen kritischer Betriebsdaten bieten. Weitere Informationen finden Sie unter AIOps – Dashboards in Service Operations-Arbeitsbereich für ITOM.

Erforderliche Rolle: evt_mgmt_operator oder viz_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Platform Analytics-Arbeitsbereich**.
2. Wählen Sie auf der Seite Analytics Center die Registerkarte **Dashboards** aus.
   Auf dieser Registerkarte können Sie alle Dashboards anzeigen, für die Sie in Ihrer Instanz Zugriffsrechte haben. Sie können die Dashboard-Kacheln filtern, um die Anzahl der sichtbaren Elemente zu begrenzen.

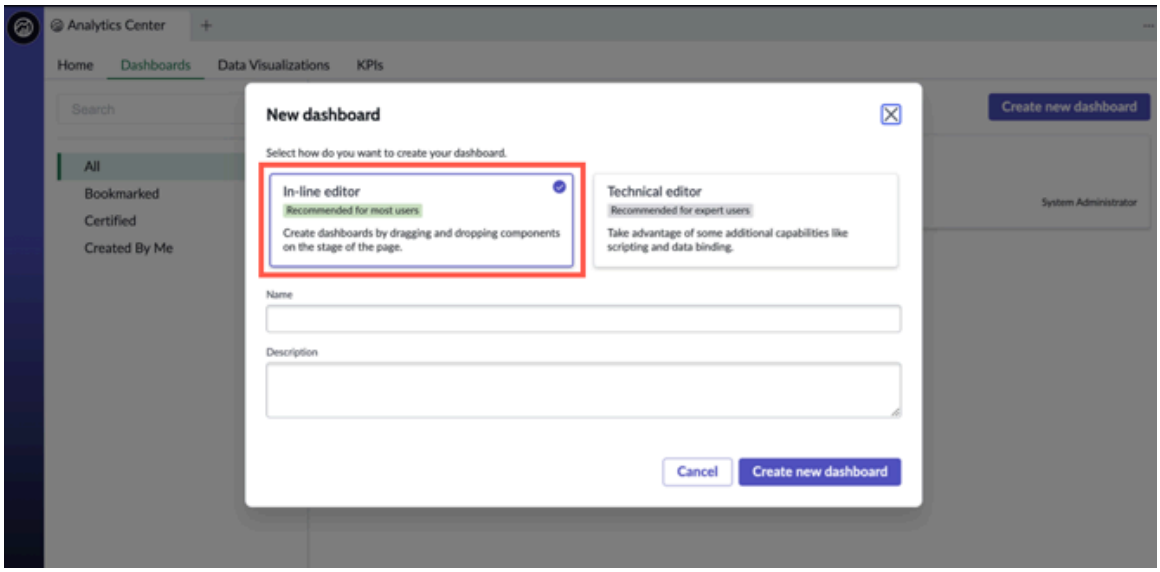
   Hinweis: Wenn Sie ein vorhandenes Dashboard verwenden möchten, wählen Sie das Dashboard hier aus, um es zu öffnen. Erstellen Sie andernfalls ein Dashboard, wie im weiteren Verlauf dieses Verfahrens beschrieben.

3. Erstellen Sie ein Dashboard.
   a. Wählen Sie **Neues Dashboard erstellen** aus.
   b. Wählen Sie im Dialogfeld „Neues Dashboard“ die Option **Inline-Editor** aus, und geben Sie einen Namen und eine optionale Beschreibung für das Dashboard an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Vom Inline-Editor wird Ihre Arbeit nicht automatisch gespeichert. Achten Sie darauf, dass Sie die Arbeit regelmäßig speichern.



c. Wählen Sie **Neues Dashboard erstellen** aus.

4. Fügen Sie dem Dashboard ein Element hinzu.
Es stehen verschiedene Elemente zur Verfügung, mit denen Sie die Informationen im Dashboard organisieren und ausfüllen können. Weitere Informationen finden Sie unter Analytics Center-Dashboard-Elemente .

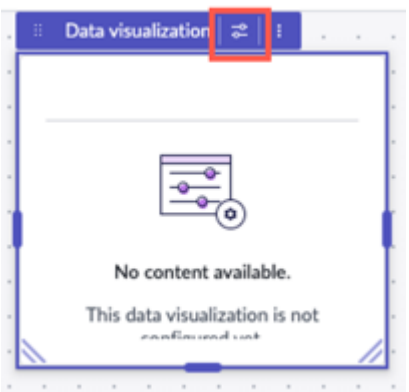
a. Wählen Sie **Neues Element hinzufügen** aus.

b. Wählen Sie aus den verfügbaren Elementen die Option **Datenvisualisierung** aus.
Das Element **Datenvisualisierung** wird im Dashboard angezeigt und kann dort bearbeitet werden.

Hinweis: Sie können auf die Ecken des Elements klicken und daran ziehen, um die Größe zu ändern.

5. Bearbeiten Sie das Element.

a. Wählen Sie auf dem Element das Symbol für Einstellungen aus:



Das Konfigurationsfenster wird geöffnet.

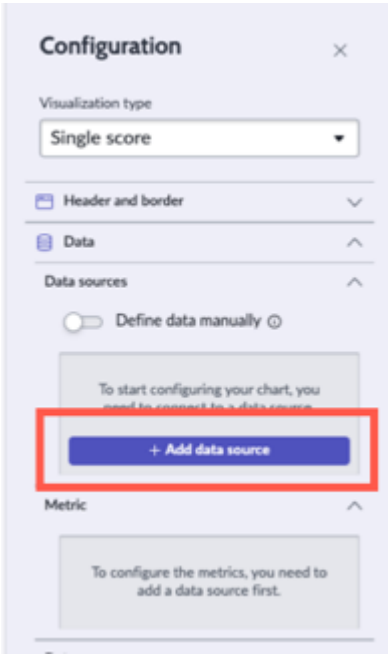
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Wählen Sie aus der Liste **Visualisierungstyp** den Typ der visuellen Darstellung aus, die Sie für die Protokolldaten wünschen.
Sie können aus verschiedenen Arten von Grafiken und Diagrammen auswählen.

Ausführliche Informationen finden Sie unter Datenvisualisierungen im Analytics Center .

c. Wählen Sie im Abschnitt „Daten“ die Option **+ Datenquelle hinzufügen** aus.

Die Health Log Analytics-Datenquelle, die Sie auswählen, wird dazu verwendet, die für die Visualisierung bereitgestellten Protokolldaten zu erfassen.



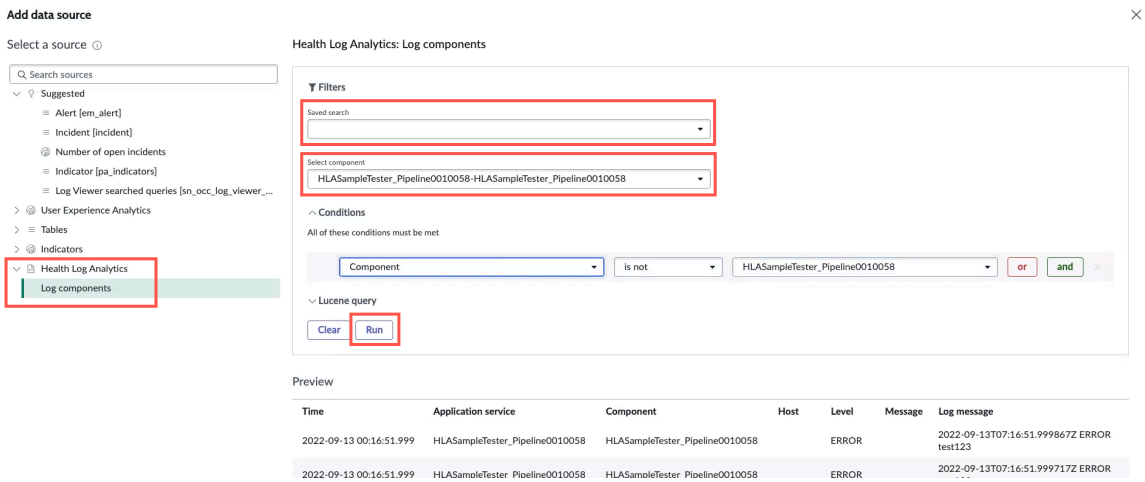
d. Wählen Sie die Datenquelle Health Log Analytics „ Protokollkomponenten aus.

e. Wählen Sie die erforderliche Datenquelle aus diesen Optionen aus:

- Gespeicherte Suchvorgänge: Eine Liste aller Suchvorgänge, die Sie im Protokoll-Viewer gespeichert haben.
- Komponente auswählen – eine Liste aller Komponenten, die Daten an Health Log Analyticsstreamen.

f. Verwenden Sie Bedingungen, eine Lucene-Abfrage oder beides, um das Datensegment anzugeben, an dem Sie interessiert sind, und wählen Sie dann **Ausführen**aus.

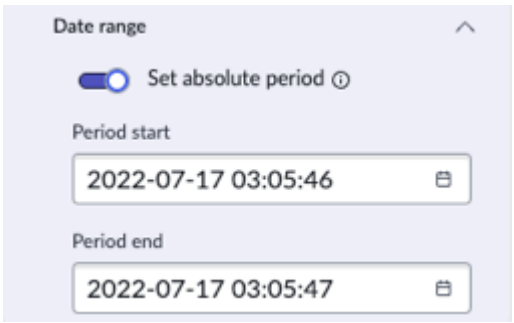
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



g. Wählen Sie **Diese Quelle hinzufügen** aus, um die ausgewählte Health Log Analytics-Datenquelle hinzuzufügen.
Die angegebene Visualisierung wird im **Datenvisualisierungselement** angezeigt.

h. Wahlweise: Legen Sie feste Start- und Enddaten fest, um den Zeitbereich der angezeigten Daten anzupassen.

(Optional)



i. Wählen Sie im Abschnitt „Datumsbereich“ die Option **Absoluten Zeitraum festlegen** aus.

ii. Geben Sie das Start- und Enddatum für den absoluten Zeitraum in den entsprechenden Kalendern an.

i. Wahlweise: Passen Sie die anderen Einstellungen der Visualisierung nach Bedarf an.

(Optional) Um detaillierte Informationen zu den Einstellungen für alle Visualisierungstypen zu erhalten, wählen Sie den Link für den entsprechenden Typ unter Datenvisualisierungen im Analytics Center aus.

j. Wahlweise: Fügen Sie nach Bedarf weitere Elemente hinzu.

k. Wählen Sie **Speichern** aus, um die Änderungen zu speichern, und setzen Sie die Bearbeitung fort.

l. Wählen Sie **Bearbeitungsmodus beenden** aus, um die Bearbeitung zu beenden und das Dashboard anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Geben Sie ein Platform Analytics -Dashboard frei

Überwachen Sie visualisierte Protokolldaten in einem vordefinierten Dashboard

Verwenden Sie Visualisierungen, um Protokolldaten im integrierten Dashboard für Vorgänge in Service Operations-Arbeitsbereich Log Analytics zu überwachen und Probleme zu beheben, sobald sie im System auftreten.

Vorbereitungen

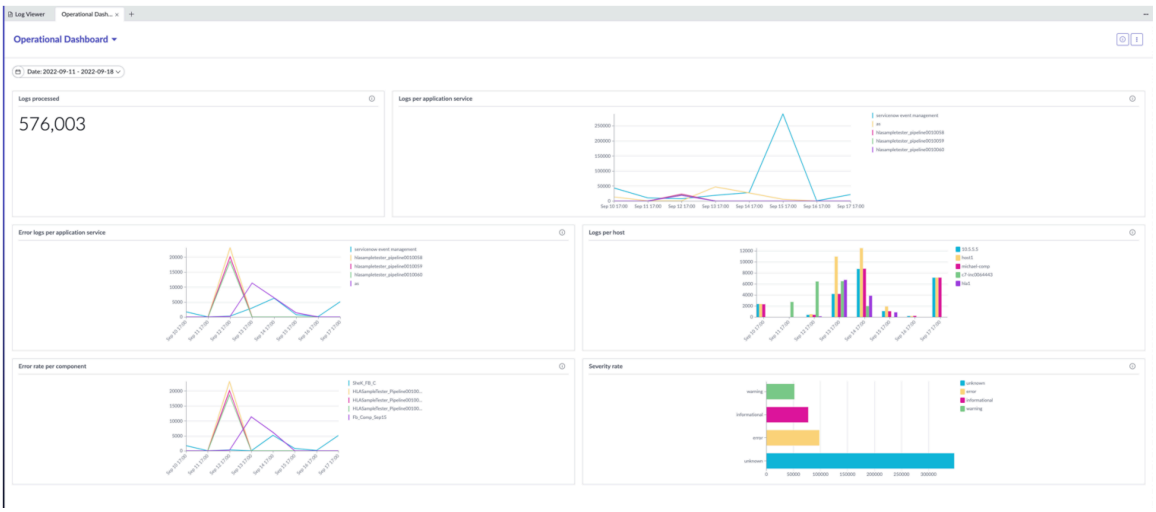
Erforderliche Rolle: evt_mgmt_operator oder viz_admin

Wichtig: Ab dem Vancouver-Release ist diese Funktion veraltet und wird durch AIOps Dashboard für HLA-Vorgängeersetzt. Weitere Informationen zu AIOps-Dashboards finden Sie unter AIOps – Dashboards in Service Operations-Arbeitsbereich für ITOM. Sie können auch ein anwenderdefiniertes Dashboard nach Ihren Anforderungen erstellen. Weitere Informationen finden Sie unter Protokolldaten-Dashboards und -visualisierungen erstellen.

Prozedur

1. Öffnen Sie den **Protokoll-Viewer** mit einer der folgenden Methoden:
   - Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich** und wählen Sie das Protokoll-Viewer-Symbol ( ).
   - Wählen Sie beim Anzeigen von Protokolleinträgen für eine Warnung auf der Registerkarte **Umgebende Protokolle** den **Protokoll-Viewer**.
2. Wählen Sie das Auswahlsymbol oben rechts auf der Registerkarte **Protokoll-Viewer** und dann **Manage my Dashboards (Meine Dashboards verwalten)** in der Dropdown-Liste. Die Registerkarte **Dashboard für Vorgänge** wird angezeigt.

   Standardmäßig visualisiert das Dashboard Protokolldaten, die in den letzten 24 Stunden erfasst wurden.



3. Wahlweise: Ändern Sie den Zeitraum, für den Daten angezeigt werden, indem Sie den gewünschten Bereich in der Dropdown-Liste **Datum** auswählen.
   Sie können einen anwenderdefinierten Bereich angeben, indem Sie **Anwenderdefiniert** und dann das gewünschte Start- und Enddatum auswählen.
4. Überwachen Sie die visualisierten Protokolldaten, und verwenden Sie sie, um Probleme zu identifizieren und zu beheben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard für Vorgänge

Name	Beschreibung	Verwendung der Daten
Verarbeitete Protokolle	Die Anzahl der Protokolle, die im ausgewählten Zeitraum verarbeitet und analysiert wurden.	Stellen Sie sicher, dass die Protokolldaten wie erwartet gestreamt werden.
Protokolle pro Anwendungsservice	Die Anzahl der Protokolle, die für jeden Anwendungsservice im ausgewählten Zeitraum gestreamt wurden.	Stellen Sie sicher, dass Protokolldaten für jeden Anwendungsservice wie erwartet gestreamt werden.
Fehlerrate pro Anwendungsservice	Die Anzahl der Protokolle mit Fehlern für jeden Anwendungsservice im ausgewählten Zeitraum. **Hinweis:** Health Log Analytics erstellt automatisch Warnungen für Fehleranomalien.	Identifizieren Sie Fehler in den Protokollen.
Protokolle pro Host	Die Anzahl der verarbeiteten Protokolle für jeden Host im ausgewählten Zeitraum.	Identifizieren Sie Hosts, die mehr oder weniger Daten als erwartet protokollieren.
Fehlerrate pro Komponente	Die Anzahl der Protokolle mit Fehlern für jede Komponente im ausgewählten Zeitraum.	Stellen Sie sicher, dass die Komponenten eine normale Fehlerrate aufweisen.
Schweregrad	Der Schweregrad der Protokolle für die Streamingquellen.	Stellen Sie sicher, dass die Raten der Stufen „Kritisch“ und „Fehler“ den Erwartungen entsprechen.

KB-Artikel einer Log Analytics-Warnung hinzufügen

Fügen Sie Ihren eigenen KB-Artikel (Knowledge Base) einer Warnung hinzu, die von Health Log Analytics generiert wurde. Sie können beispielsweise zusätzliche Informationen angeben, die zur Lösung des zugrunde liegenden Problems beitragen können.

Vorbereitungen

Diese Funktion wird in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, und in der Anwendung Health Log Analytics Viewer, Version 21.0.0 – Dezember 2021 und später, unterstützt. Diese Anwendungen sind im ServiceNow Store verfügbar.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie eine Log Analytics-Warnung.

   a. Wählen Sie in Service Operations-Arbeitsbereich das Listensymbol ( ) aus.

   b. Wählen Sie die entsprechende Liste in der untergeordneten Liste „Warnungen“ aus, und navigieren Sie zu der gewünschten Warnung.
   In der Liste **Alle Warnungen** weisen alle von Health Log Analytics generierten Warnungen in der Spalte **Quelle** den Wert **Log Analytics** auf.

   c. Wählen Sie die Warnungsnummer aus.

2. Wählen Sie oben rechts auf der Registerkarte **Details** das Symbol für weitere Aktionen ( ) und dann in der Liste die Option **Create KB article for this issue** (KB-Artikel für dieses Problem erstellen) aus.
3. Füllen Sie die Felder des Formulars aus.

Formular „Neues Wissen erstellen“

Feld	Beschreibung
Knowledge Base	Die Knowledge Base, in der der neue KB-Artikel gespeichert wird. Standardmäßig ist dieser Wert die Health Log Analytics-Knowledge Base.
Workflow	(Schreibgeschützt) Der Status des KB-Artikels. Wenn Sie den Artikel veröffentlichen, ändert sich sein Status automatisch von „Entwurf“ in „Veröffentlicht“.
Kategorie	Die Kategorie der Komponente, die die Warnung verursacht hat.
Kurzbeschreibung	Zusammenfassung des KB-Artikels.
Artikeltext	Inhalt des KB-Artikels.

4. Wählen Sie **Speichern**.
5. Wenn der Inhalt des Artikels endgültig ist, wählen Sie **Veröffentlichen** aus.

Ergebnisse

Der KB-Artikel wird der ausgewählten Warnung hinzugefügt. Sie können den Artikel im Seitenbereich von Agent Assist suchen und anzeigen. Health Log Analytics verwendet Ihren Artikel auch, um ähnliche Warnungen mit derselben Ereignis-ID-Eigenschaft oder demselben Warnungsmuster zu verbessern.

Service Operations-Arbeitsbereich für ITOM Referenz

Referenzthemen enthalten zusätzliche Informationen zu ServiceNow Service Operations-Arbeitsbereich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit AIOps-Experience installierte Komponenten

Bei der Aktivierung der Anwendung AIOps-Experience [sn_sow_aiops] werden verschiedene Arten von Komponenten installiert, einschließlich Anwenderrollen und Plugins.

Hinweis: In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Für diese Funktion sind Demodaten verfügbar.

Installierte Rollen

Rollentitel [Name]	Beschreibung	Enthält Rollen
evt_mgmt_user	Verwaltet den Warnungslebenszyklus und führt grundlegende Vorgänge aus, z. B. das Anzeigen von Warnungen.	ITIL
evt_mgmt_operator	Verwaltet Warnungen, einschließlich Aufgaben wie das Schließen und Bestätigen von Warnungen.	evt_mgmt_user
evt_team_operator	Verwaltet Vorgänge Ereignismanagement innerhalb eines bestimmten Teams, wie im Feld **Zuweisungsgruppe** definiert. Mit dieser Rolle kann der Bediener Warnungen ausschließlich für das ihm zugewiesene Team lesen und schreiben. Darüber hinaus kann der Operator Konfigurationsänderungen speziell für sein Team vornehmen, einschließlich Updates für die Warnungsautomatisierung und das Integrations-Launchpad.	sn_sow_alert_rules.automation_create_nonglobal sn_sow_alert_rules.automation_delete_nonglobal

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rollentitel [Name]	Beschreibung	Enthält Rollen
	Hinweis: Die Rolle evt_team_operator muss einer Zuweisungsgruppe zugewiesen werden, um Warnungen für diese Gruppe anzuzeigen und zu verwalten. Wenn die Rolle erstellt, aber keinen Gruppen zugeordnet ist, denen Warnungen zugewiesen sind, kann der Bediener keine Warnungen sehen.	
evt_mgmt_admin	Konfiguriert Eigenschaften und Regeln für Ereignismanagement und richtet sie ein.	evt_mgmt_user und evt_mgmt_operator

Installierte Plugins

Plugin	Beschreibung
Ereignismanagement [com.glideapp.itom.snac]	Bietet serviceorientierte Verfügbarkeit und überwacht Ereignisse über eine intuitive Konsole.
Performance Analytics – Premium [com.snc.pa.em]	Stellt wichtige sofort einsatzbereite Leistungskennzahlen (Key Performance Indicators, KPIs) bereit, um Ereignismanagement-Prozesse zu überwachen und zu verbessern. Beachten Sie, dass die Aktivierung dieses Plugins in Produktionsinstanzen möglicherweise eine separate Performance Analytics -Lizenz erfordert.
Performance Analytics Inhaltspaket – Ereignismanagement [com.snc.pa.premium]	Enthält wichtige sofort einsatzbereite Leistungskennzahlen (Key Performance Indicators, KPIs). Für die Aktivierung dieses Plugins in Produktionsinstanzen ist möglicherweise eine separate Performance Analytics -Lizenz erforderlich.

Informationen zur Rückkehr zum Verfahren finden Sie unter Installieren Sie Service Operations-Arbeitsbereich für die Anwendung ITOM ..

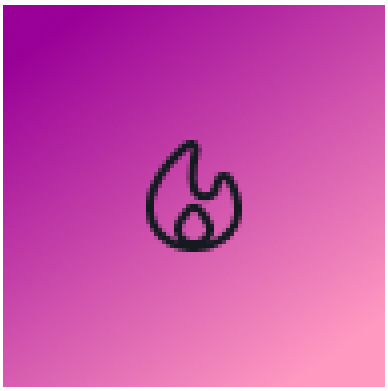
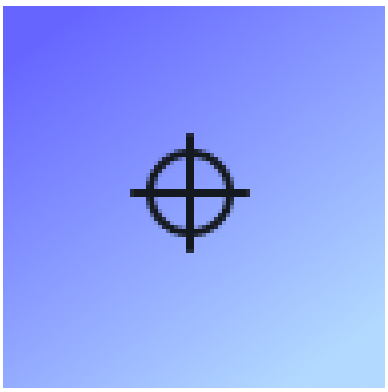
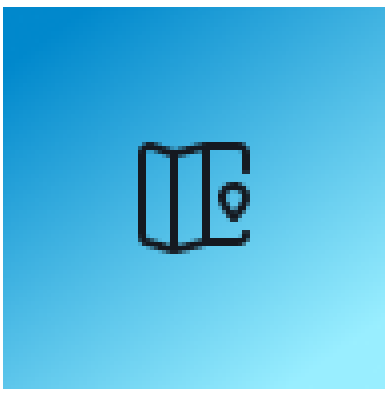
Attribute in der Linkansicht Express-Liste .

Die Tabelle listet die Knotenattribute auf , die in der Link-Ansicht verfügbar sind, sowie ihr Symbol und ihre Beschreibung.

Hinweis: Attribut ist ein allgemeiner Begriff, der Felder und Tags darstellt, die in Warnungen oder Configuration Items (CI) zu finden sind.

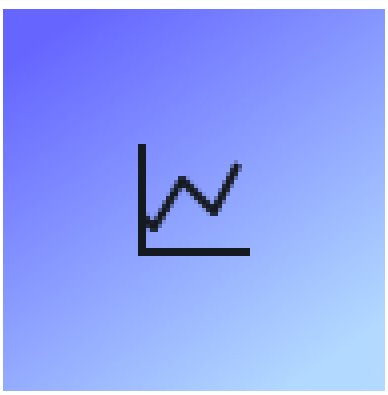
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute in der Linkansicht

Attributname.	Symbol	Beschreibung
Betroffener Service		Service in Configuration Management Database (CMDB), der von einer Warnung für ein CI betroffen ist,
Ressource		Knotenressource, die für das Ereignis relevant ist. Beispiel: Datenträger C, CPU-1, der Name eines Prozesses oder Services. Maximale Länge: 100 Zeichen
Quelle		Ereignis-Überwachungssoftware, von der das Ereignis generiert wurde, z. B. SolarWinds oder SCOM. Maximale Länge: 100 Zeichen
Region		Vordefiniertes -Attribut, das aus der Connector-Nutzlast extrahiert wurde.

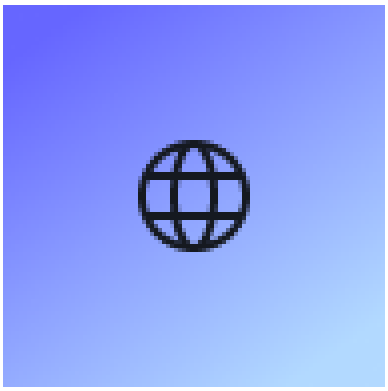
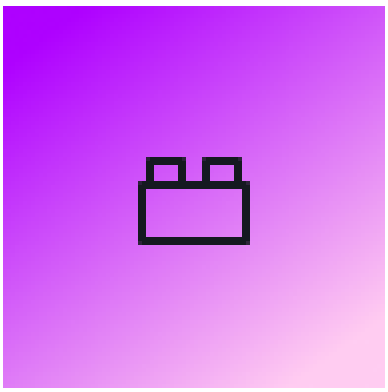
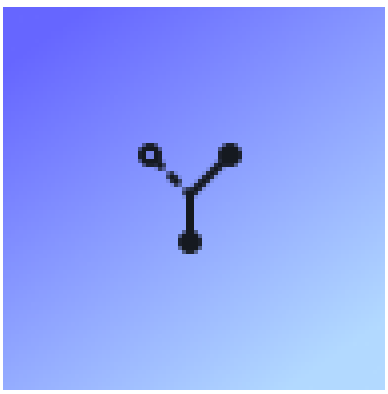
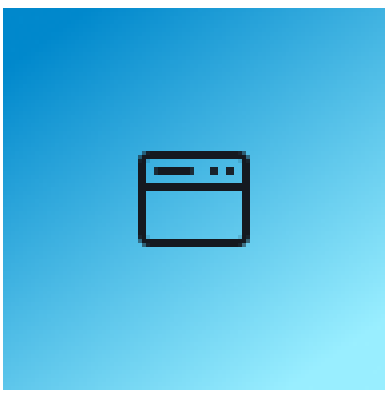
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute in der Linkansicht (Fortsetzung)

Attributname.	Symbol	Beschreibung
Standort		Vordefiniertes -Attribut, das aus der Connector-Nutzlast extrahiert wurde.
Zuweisungsgruppe		Warnungszuweisungsgruppe.
Umgebung		Vordefiniertes -Attribut, das aus der Connector-Nutzlast extrahiert wurde.
Metrik		Eindeutiger Name, der beschreibt, welche Metrikdaten erfasst werden.

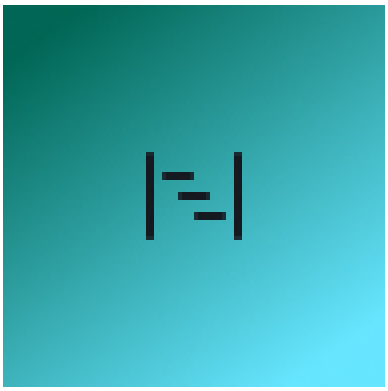
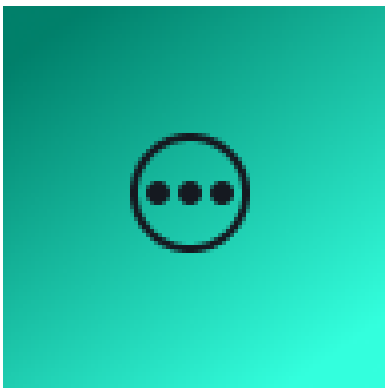
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute in der Linkansicht (Fortsetzung)

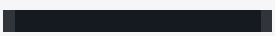
Attributname.	Symbol	Beschreibung
IP-Adresse		Vordefiniertes -Attribut, das aus der Connector-Nutzlast extrahiert wurde.
CI		JSON-Zeichenfolge, die ein Konfigurationselement darstellt. Beispiel: `{"name":"SAP ORA01","type":"Oracle"}` ({"Name": "SAP ORA01", "Typ": "Oracle"}). Der CI-Bezeichner, der das Event generiert hat, wird im Feld Zusätzliche Informationen angezeigt. Maximale Länge: 1.000 Zeichen
Knoten		Knotenname, vollqualifizierter Domänenname (FQDN), IP-Adresse oder MAC-Adresse, die dem Ereignis zugeordnet ist, z. B. IBM-ASSET. Maximale Länge: 100 Zeichen
Anwendung		Vordefiniertes -Attribut, das aus der Connector-Nutzlast extrahiert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attribute in der Linkansicht (Fortsetzung)

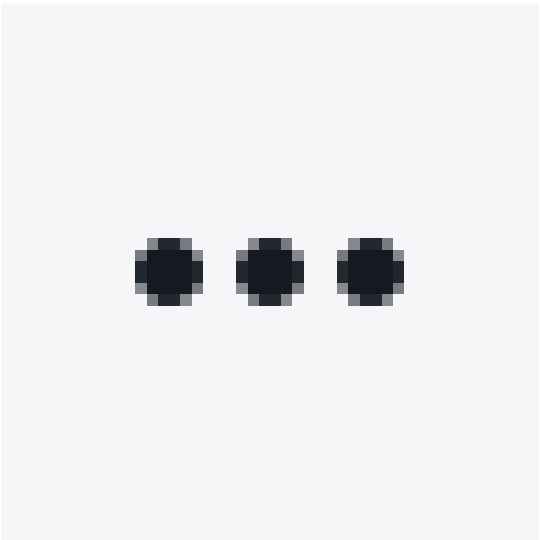
Attributname.	Symbol	Beschreibung
Prozess		Ein Prozess oder ein Cluster von Prozessen, die auf dem Host ausgeführt werden und durch die Horizontal-Discovery identifiziert werden.
Sonstige **Hinweis:** Dieses Attribut ist anwenderdefiniert. Alle anderen -Attribute sind im System vordefiniert.		Anwenderdefiniertes Attribut. **Hinweis:** Alle anderen -Attribute sind im System vordefiniert.

Linien, die Attribute verknüpfen

Verknüpfung	Visuelle Darstellung	Beschreibung
Durchgezogene Linie		Durchgezogene Linie, die Attribute in der Linkansicht verknüpft und anzeigt, dass die Attribute eine oder mehrere Warnungen gemeinsam nutzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linien, die Attribute verknüpfen (Fortsetzung)

Verknüpfung	Visuelle Darstellung	Beschreibung
Gepunktete Linie		Gepunktete Linie, die Attribute in der Linkansicht verknüpft und anzeigt, dass die Attribute durch Gruppierungskriterien korreliert sind.

Warnungsfeldzuordnung auf der Seite „Antworten“.

Die Felder, die auf der Seite „Antworten“ konfiguriert werden sollen, wenn eine Aktion ausgewählt wird, die von einer Warnungsautomatisierung ausgelöst werden soll.

Wählen Sie Felder für Automatisierungsaktionen aus

Feld	Beschreibung
Incident-Feldname	Name des Felds, das im Incident angezeigt wird.
Feld zuordnen	Option, die angibt, wie das Incident-Feld zugeordnet werden soll: • **Gleich wie**: Das ausgewählte Incident-Feld hat denselben Wert wie das angegebene Warnungsfeld. • **Zu**: Das ausgewählte Incident-Feld wird auf einen angegebenen Wert festgelegt.
Warnungsfeldwert	Wert, der im Warnungsfeld festgelegt wird: • Wenn Sie in der Spalte „Zuordnungsfeld“ **Identisch mit** auswählen, wird der Wert des Warnungsfelds, der im Incident-Feld angezeigt werden soll, auch in der Spalte „Incident-Feldname“ angezeigt. • Wenn Sie in der Spalte „Zuordnungsfeld“ **Bis** auswählen, geben Sie den Warnungsfeldwert ein, der im angegebenen Incident-Feld angezeigt werden soll.

Informationen zur Rückkehr zum Verfahren finden Sie unter #unique_1716.

Detailseite des Anwendungsservice

Stellt umfassende Informationen zu einem Anwendungsservice bereit, einschließlich Name, Geschäftskritikalität, Eigentum, Prozess- und Betriebsstatus, Details zur datenverkehrsbasierten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery, Discovery-Status und relevanten Kommentaren. Dies ermöglicht eine gründliche Analyse des aktuellen Status und der Nutzung von Anwendungsservices, sorgt für Klarheit in Bezug auf Besitz und Relevanz und hilft bei der effektiven Priorisierung von Ressourcen und Aktionen.

Felder der Detailseite des Anwendungsservice

Feld	Beschreibung
Name	Name des Anwendungsservice.
Business-Relevanz	Wichtigkeitsgrad des Service für Business Operations.
Eigentum von	Person oder Team, die für die Verwaltung und Überwachung des Service verantwortlich ist.
Prozessstatus	Aktuelle Phase oder Status der operativen Prozesse des Service.
Betriebsstatus	Aktuelle Phase oder Zustand der operativen Prozesse des Service, die angeben, ob er reibungslos funktioniert oder Probleme auftreten.
Verkehrsbasierte Discovery	Option zum Identifizieren von Serviceinstanzen basierend auf Netzwerkdatenverkehrsmustern.
Discovery-Status	Fähigkeit des Systems, den Service in seinem Netzwerk zu finden und zu erkennen.
Kommentare	Zusätzliche Hinweise oder relevante Informationen zum Service, die für das Verständnis seiner Verwaltung oder Nutzung hilfreich sein können.

Informationen zur Rückkehr zum Verfahren finden Sie unter Zeigen Sie Details zu Anwendungsservices in an Service Operations-Arbeitsbereich.

Erstellen Sie Listenfelder

Erstellen Sie anwenderdefinierte Listen mit Feldern, die auf Ihre Bedürfnisse zugeschnitten sind.

Welches Formular Sie ausfüllen, hängt davon ab, ob Sie Ihre Liste auf eine vorhandene Liste setzen (**Von vorhandener beginnen**) oder eine neue Liste erstellen (**Eigene erstellen**).

Von vorhandenem Formular starten

Feld	Beschreibung
Liste	Vorhandene Liste, die Sie ändern möchten.
Listenname	Name für Ihre Liste. Der Standardname in diesem Feld ist der Name der vorhandenen Liste im Feld **Liste** mit dem Anhang `„- Kopie“`.
Spalten auswählen	Datensatzfelder, die in die Listenansicht aufgenommen werden sollen. Die Spalten aus der von Ihnen ausgewählten Liste werden angezeigt. Sie können Spalten hinzufügen oder entfernen, um die Liste zu ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von vorhandenem Formular starten (Fortsetzung)

Feld	Beschreibung
Filter hinzufügen	Bedingung für das Filtern der Liste. Standardmäßig werden die auf die ausgewählte Liste angewendeten Bedingungen angezeigt. Sie können diese Bedingung ändern.

Eigenes Formular erstellen

Feld	Beschreibung
Listenname	Name für Ihre Liste.
Quelle auswählen	Quelltabelle für die Datensätze.
Spalten auswählen	Die in der Liste anzuzeigenden Spalten. Dieses Feld wird mit Spalten aus einer Arbeitsbereich-Listenansicht gefüllt, falls vorhanden. Wenn keine Arbeitsbereichsliste vorhanden ist, werden die Spalten mit der Standardlistenansicht der ausgewählten Tabelle ausgefüllt.
Filter hinzufügen	Bedingung für das Filtern der Liste.

Wie Sie zum Verfahren zurückkehren, erfahren Sie unter Liste in Service Operations-Arbeitsbereich für ITOMerstellen

Felder des Formulars „Konfiguration der Metrikansicht“

Definieren Sie, wie Metriken in Service Operations-Arbeitsbereichangezeigt werden.

Formular „Konfiguration der Metrikansicht“

Feld	Beschreibung
Titel	Name der Metrik
Aktiv	Option zum Aktivieren der Metrik.
Auftrag	Numerischer Wert, der die Reihenfolge der Metriken auf der Seite angibt.
Configuration Item-Typ	Typ des Konfigurationselements. Verfügbare Optionen sind: • cmdb_ci_app_server_tomcat • cmdb_ci_metric_extension • cmdb_ci_app_win_server
Quellmetriktypen	Metriktypen, die von der Metrik überwacht werden sollen. Klicken Sie auf das Schlosssymbol ( ), um die Liste der Quellmetriktypen zu entsperren und die zu überwachenden Metriktypen auszuwählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Konfiguration der Metrikansicht“ (Fortsetzung)

Feld	Beschreibung
Diagrammtyp	Typ des Diagramms, in dem die Metrik in Service Operations-Arbeitsbereichdargestellt wird, entweder **Linie** oder **gestapelter Balken**.

Informationen zur Rückkehr zum Verfahren finden Sie unter Warnungsmetriken konfigurieren.

Felder für Integritätsereignisse für Integration und Konfiguration

Füllen Sie die Ereignisfelder aus, um Details wie Ereigniszeit, Beschreibung, Warnungsnummer, Status, Schweregrad, Metrikname, Knoten, Nachrichtenschlüssel und Fehlermeldung zu erfassen. Dies ermöglicht eine genaue Nachverfolgung, effektives Incident-Management und verbessert die Fehleranalyse.

Ereignisfelder

Feld	Beschreibung
Zeit des Ereignisses	Gibt an, wann das Ereignis aufgetreten ist.
Beschreibung	Stellt Details zum Ereignis oder Incident bereit.
Warnung	Gibt die Warnungsnummer an, die basierend auf dem Ereignis ausgelöst wird.
Status	Beschreibt den aktuellen Status des Ereignisses (z. B. offen, geschlossen).
Schweregrad	Gibt den Schweregrad des Ereignisses an (z. B. kritisch, Warnung).
Metrikname	Gibt die spezifische Metrik an, die dem Ereignis zugeordnet ist.
Knoten	Gibt den Knoten oder das Gerät im Zusammenhang mit dem Ereignis an.
Nachrichtenschlüssel	Eindeutiger Bezeichner für die Ereignisnachricht.
Fehlermeldung	Stellt zusätzliche Informationen über alle mit dem Ereignis verknüpften Fehler bereit.

Informationen zur Rückkehr zum Verfahren finden Sie unter Überprüfen Sie die Integrations- und Konfigurationsintegrität.

Pull-Connector-Felder

Füllen Sie die Felder für die erweiterten Einstellungen des Pull-Connectors aus, um den Abruf und die Synchronisierung von Ereignissen basierend auf bestimmten Anforderungen wie Verbindungseinstellungen, Ereignishäufigkeit und Zeitzoneneinstellungen zu optimieren.

Felder „Erweiterte Einstellungen“

Feld	Beschreibung
Verbundener MID-Server	Legen Sie fest, ob das System den optimalen MID-Server auswählt oder ob Sie einen bestimmten MID-Server selbst auswählen sollen. Führen Sie dies nur durch, wenn Sie Änderungen an MID-Server vornehmen müssen. Lassen Sie es andernfalls

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder „Erweiterte Einstellungen“ (Fortsetzung)

Feld	Beschreibung
	leer, und lassen Sie das System das optimale MID-Serverauswählen.
Zeitplan für Ereignissammlung (Sekunden)	Geben Sie die Häufigkeit in Sekunden ein, die angibt, wie oft das System nach neuen Ereignissen aus der externen Ereignisquelle suchen soll. Der Wert darf nicht niedriger sein als die minimale Zeitplaneigenschaft, die standardmäßig 120 Sekunden beträgt.
Protokoll	Definiert das Kommunikationsprotokoll, das zum Abrufen von Ereignissen von externen Geräten verwendet wird.
severity_by_state_type	Bestimmt den Schweregrad, der Ereignissen zugewiesen ist, basierend auf ihrem Statustyp.
time_zone	Gibt die Zeitzone an, die zum Aufzeichnen und Anzeigen von Ereigniszeitstempeln verwendet wird.
offset_min	Legt den Zeitversatz für den Ereignisabruf fest, um eine genaue Synchronisierung sicherzustellen.
Port	Überprüfen Sie die Standardwerte für Ihren Connector-Typ, z. B. Portdetails oder Zeitformate, und ändern Sie sie nach Bedarf. Standardwerte von Ihrem Connector sind ausgefüllt. Gibt die Portnummer an, die für die Kommunikation mit externen Geräten verwendet wird.
max_fetch_interval_min	Begrenzt das maximale Intervall zwischen Ereignisabrufvorgängen.
initial_sync_in_days	Legt die Dauer für den ersten Synchronisierungsprozess beim Abrufen von Verlaufsdaten fest.

Informationen zur Rückkehr zum Verfahren finden Sie unter Konfigurieren Sie einen Pull-Connector.

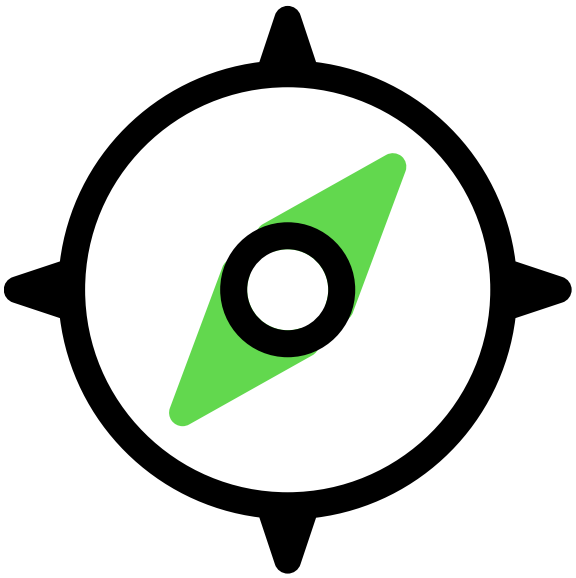
Synthetische Überwachung

Die Anwendung ServiceNow®Synthetische Überwachung ermöglicht es Unternehmen, die Leistung und Verfügbarkeit wichtiger Services proaktiv zu verwalten und zu verbessern. Durch die Simulation von Anwendertransaktionen an API-Endpunkten identifiziert diese Lösung Leistungsengpässe, trägt zur Sicherstellung der Betriebszeit bei und optimiert die Anwender-Experience.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

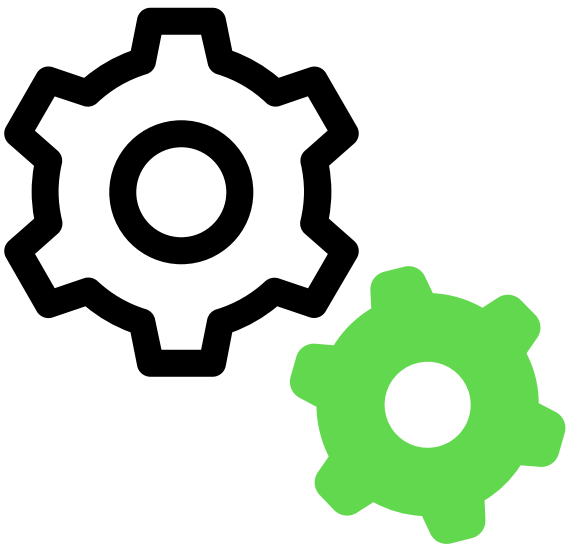
Erste Schritte

Untersuchen



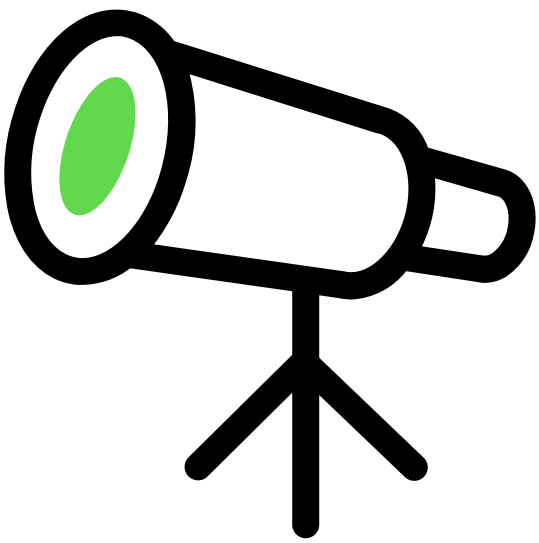
Erfahren Sie mehr über Synthetische Überwachung

Konfigurieren



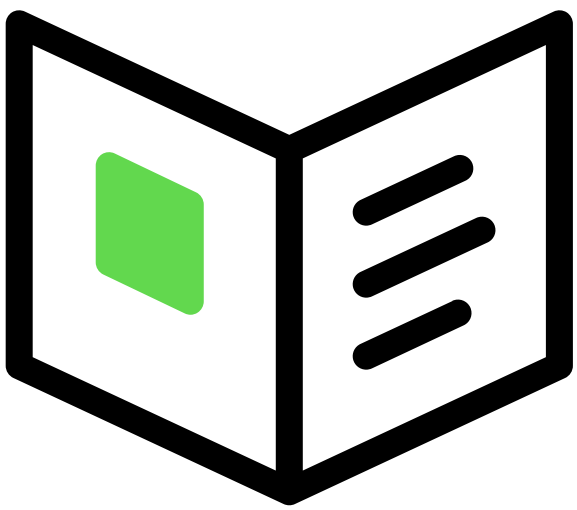
Fügen Sie Anwender hinzu, und erstellen und verwalten Sie einen Synthetic Monitor

Identifizieren



Verwenden Sie Synthetische Überwachung, um Leistungsprobleme zu identifizieren

Referenz



Hier finden Sie Referenzinformationen zu Synthetische Überwachung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hilfreiche Ressourcen

Einige ServiceNow -Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

ServiceNow Community

ServiceNow Community

Customer Success Center

Customer Success Center

Entwickler

developer.servicenow.com

Impact

http://impact.servicenow.com

ServiceNow University

ServiceNow University

NowCreate

Now Create

Partner

https://www.servicenow.com/partners.html

ServiceNow

http://www.servicenow.com

ServiceNow Store

ServiceNow Store

Unterstützung

- https://support.servicenow.com/now
- Known Error-Portal

Synthetische Überwachung erkunden

Erfahren Sie, wie Synthetische Überwachung proaktives, automatisiertes Testen von Serviceendpunkten ermöglicht. Durch die Simulation von Benutzerinteraktionen können Fehler, Leistungsprobleme und Ausfälle erkannt werden, bevor sie sich auf echte Benutzer auswirken.

Synthetische Überwachung – Übersicht

Synthetic Monitors rufen kontinuierlich HTTP-Endpunkte in Configuration Management Database (CMDB) auf, um die Verfügbarkeit und Antwortzeiten zu testen. Wenn ein Test fehlschlägt, werden Sie möglicherweise vor Endpunktproblemen gewarnt, bevor Ihre Kunden dies tun.

Sie können beispielsweise einen Monitor erstellen, der den `GET`-HTTP-Endpunkt eines Service testet. Sie können diese Überwachung so konfigurieren, dass sie jede Minute ausgeführt wird, und einen Test mit dem Statuscode 200 als Erfolg festlegen. Bei entsprechender Konfiguration kann eine Warnung generiert und über Ereignismanagement gesendet werden, wenn ein Test fehlschlägt. Sie können auch den Schweregrad der Warnung konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Synthetische Überwachung -Tests werden von einem Agent Client Collector (ACC) ausgeführt, der in Ihrem Netzwerk bereitgestellt wird.

Hinweis: Die HTTP-Endpunkte müssen in der Tabelle „HTTP-Endpunkte“ [cmdb_ci_endpoint_http] vorhanden sein.

Synthetische Überwachung Anwender

Synthetische Überwachung Anwender

Anwender	Beschreibung
Synthetische Überwachung Administrator (Administratorrolle)	Weist Rollen zu, erstellt und bearbeitet Überwachungen und zeigt Überwachungstests und ihre Ergebnisse an.
Serviceverantwortlicher (Editor-Rolle)	Erstellt und bearbeitet Überwachungen und kann auch Überwachungstests und deren Ergebnisse anzeigen.
Network Operation Center (NOC) Operator (Betrachterrolle)	Überwacht Tests und deren Ergebnisse.

Synthetische Überwachung – Workflow

Synthetic-Überwachungs-Workflow

Administratoren, Serviceverantwortliche und NOC-Operatoren verwenden Synthetische Überwachung auf folgende Weise:

1. Als Serviceverantwortlicher bestimmen Sie, welche Endpunkte basierend auf der Geschäftskritikalität überwacht werden sollen.
2. Als Administrator oder Serviceverantwortlicher konfigurieren Sie den Monitor und überprüfen dann die Ergebnisse der Tests, die der Monitor sendet. Wenn die Ergebnisse nicht erfolgreich sind, führen Sie eine Fehlerbehebung bei der Konfiguration durch. Sie können auch eine Warnung erstellen, die ausgelöst wird, wenn ein Test fehlschlägt.
3. Als Serviceverantwortlicher oder -operator überwachen Sie die Tests und reagieren auch auf generierte Warnungen. Sie können zugehörige Configuration Items (CIs) anzeigen, um mit der Selektierung des Problems zu beginnen, wenn ein Test fehlschlägt.

Synthetische Überwachung – Vorteile

Synthetische Überwachung – Vorteile

Vorteil	Funktion	Anwender
Zeigen Sie aggregierte Überwachungsinformationen an. Zeigen Sie die Homepage Synthetische Überwachung an, auf der Sie folgende Möglichkeiten haben:	Zeigen Sie zusammengefasste Informationen zu den Monitoren an.	Betreiber, Serviceverantwortliche

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Synthetische Überwachung – Vorteile (Fortsetzung)

Vorteil	Funktion	Anwender
• Zeigen Sie eine zusammengefasste Ansicht aller Überwachungen an • Zeigen Sie den aktuellen Status aller Überwachungen an. • Ruft Detailinformationen zu einem Monitor ab		
Visualisieren Sie Synthetic-Testergebnisse. Zeigen Sie die Detailseite für einen Monitor an, auf der Sie Folgendes sehen können: • Aktueller Status und Konfiguration des Monitors. • Diagramme, die Testerfolg und Antwortzeit anzeigen. • Zugeordnete CIs, die der Ausgangspunkt für die Untersuchung fehlgeschlagener Tests sein können. • Ein Verlaufsprotokoll von Synthetic-Test-Ausführungen, einschließlich Details und Antworttext.	Zeigen Sie einen Monitor und seine Tests an.	Betreiber, Serviceverantwortliche
Erhalten Sie Echtzeitbenachrichtigungen für Ausfälle, bevor sie sich auf Anwender auswirken.	Konfigurieren Sie optional Warnungen, wenn Tests nicht erfolgreich sind.	Betreiber, Serviceverantwortliche
Teilen Sie Einblicke mit Stakeholdern.	Zeigen Sie aggregierte Überwachungsinformationen an.	Betreiber, Serviceverantwortliche
Aktualisieren Sie die Monitore entsprechend Ihren Geschäftsanforderungen.	Vorhandene Überwachungen bearbeiten, einschließlich Deaktivierung.	Servicebesitzer

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Synthetische Überwachung finden Sie unter:

- Synthetische Überwachung konfigurieren
- Synthetische Überwachung verwenden
- Synthetische Überwachung – Referenz

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Synthetische Überwachung konfigurieren

Planen und konfigurieren Sie Ihre -Implementierung von Synthetische Überwachung.

Konfiguration – Übersicht

Synthetische Überwachung installieren

Sie können die Anwendung Synthetische Überwachung (`com.snc.uib.sow_ Synthetics`) installieren, wenn Sie die Administratorrolle innehaben.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfung des folgenden Elements: Synthetische Überwachung Anwendungsliste in ServiceNow Store, um Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Releasekompatibilität zu erhalten.
- Configuration Items (CI) müssen sich in der Tabelle CMDB HTTP-Endpunkte [cmdb_ci_endpoint_http] befinden, die Sie überwachen möchten.
- Wenn Ihr Endpunkt eine Authentifizierung erfordert, müssen sich die konfigurierten Anmeldeinformationen in der Tabelle „Anmeldeinformationen“ [discovery_credentials] befinden.

> **Hinweis:** Synthetische Überwachung unterstützt nur API-Schlüssel-Anmeldeinformationen und Anmeldeinformationen für die Standardauthentifizierung.

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Die folgenden Elemente werden mit Synthetische Überwachung installiert:

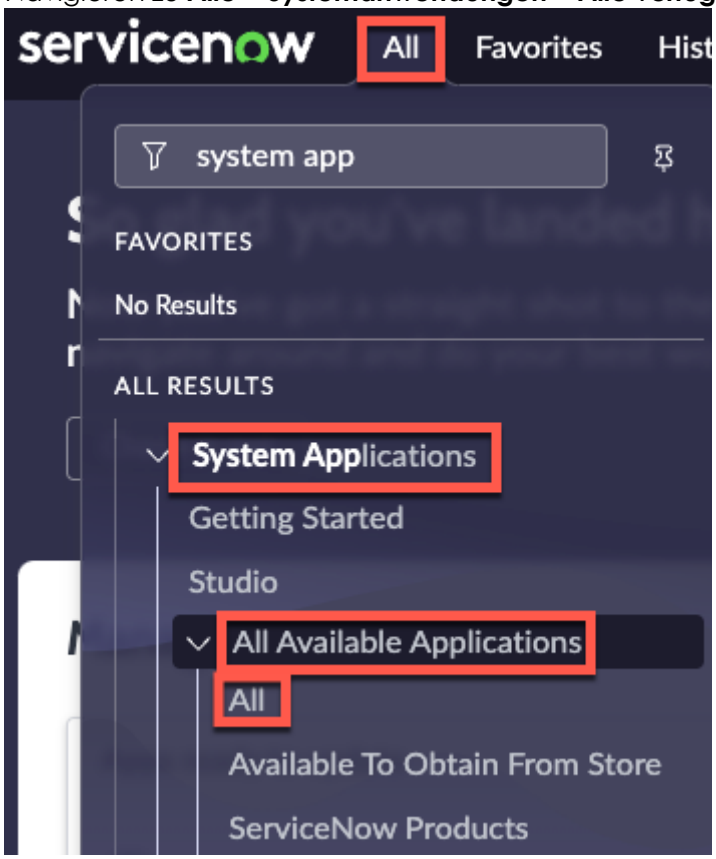
- Plugins
- Rollen
- Tabellen

Weitere Informationen finden Sie unter Mit Synthetische Überwachung installierte Komponenten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Synthetische Überwachung (com.snc.uib.sow_ Synthetics).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

   In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Nächste Maßnahme

Erstellen Sie Synthetische Überwachung Standorte

Erstellen Sie Synthetische Überwachung Standorte

Erstellen Sie einen Standort Synthetische Überwachung, der einem Synthetic Monitor zugewiesen werden soll, indem Sie mindestens einen Agent Agent Client Collector zu einer Gruppe hinzufügen, die zum Ausführen der Synthetic-Prüfungen verwendet wird. Der für einen Synthetic Scheck konfigurierte Ort bestimmt diese Gruppe.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Mindestens ein Agent Client Collector -Agent (ACC), der den Zustand und die Leistung der mit Synthetische Überwachung zu überwachenden HTTP-Endpunkte überwacht, muss mit Ihrer Glide-Instanz verbunden sein.

Hinweis:

- Wenn Ihr Synthetic Monitor einen privaten HTTP-Endpunkt testet, darf Ihr Standort nur ACC-Agents enthalten, die sich innerhalb der gleichen Netzwerkgrenzen wie der HTTP-Endpunkt befinden.
- Wenn Ihr Monitor einen HTTP-Endpunkt aus verschiedenen Rechenzentren, Cloud-Anbietern oder geografischen Regionen testet, muss für jedes ein anderer Standort verwendet werden.

Erforderliche Rolle: Synthetics. Synthetics_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können beliebig viele Standorte erstellen, Sie müssen jedoch mindestens einen Standort haben, um einen Synthetic Monitor zu erstellen.

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* > **Konfigurationen**.
2. Navigieren zu **Setup der Synthetics-Überwachung** > **Verwalten Sie Standorte**.
3. Wählen Sie **Neuen Standort erstellen aus**.
4. Erweitern Sie die Karte „Standortdetails“, und geben Sie einen eindeutigen Namen und eine optionale Beschreibung für diesen Standort ein.
   Aus der Beschreibung sollte eindeutig hervorgehen, wo die ACC-Agents an diesem Standort ausgeführt werden. Beispiel: `US-1-east-cluster`.
5. Erweitern Sie die Karte Agents auswählen, und wählen Sie mindestens einen Service Desk-Mitarbeiter für diesen Standort aus.
6. Wählen Sie **Speichern**.

Nächste Maßnahme

Erstellen und bearbeiten Sie einen Synthetic Monitor

Erstellen und bearbeiten Sie einen Synthetic Monitor

Erstellen oder bearbeiten Sie einen Synthetic Monitor, um die Verfügbarkeit und Leistung Ihrer HTTP-Endpunkte zu testen, bevor Ihre Kunden Probleme entdecken.

Vorbereitungen

Zum Hosten des Monitors müssen mindestens ein Standort erstellt werden. Um einen Standort zu erstellen, rufen Sie mindestens einen Standortauf.

Erforderliche Rolle: Synthetics. Synthetics_editor oder Synthetics. Synthetics_admin

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* und wählen Sie das Symbol Synthetische Überwachung ( ).
2. Erstellen Sie auf der Seite „Übersicht“ entweder einen Synthetic Monitor, oder bearbeiten Sie einen vorhandenen Monitor.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um einen Synthetic-Monitor zu erstellen, wählen Sie **Neu**aus.
- Um einen vorhandenen Monitor zu bearbeiten, wählen Sie den Monitor aus, den Sie bearbeiten möchten, und wählen Sie dann die Registerkarte **Details**.

3. Füllen Sie die Felder des Formulars aus.

a. Geben Sie im Abschnitt Überwachungsdetails einen eindeutigen Namen und eine Beschreibung für die Überwachung ein.

b. Füllen Sie die Felder im Abschnitt „HTTP-Einstellungen“ aus.

Abschnitt „HTTP-Einstellungen“.

Feld	Beschreibung
HTTP-Methode	HTTP-Methode, die Sie für den Endpunkt überwachen möchten.
HTTP-Endpunkt-CI	CI, das der Monitor testen soll. **Hinweis:** Der HTTP-Endpunkt muss in der Tabelle „HTTP-Endpunkte“ [cmdb_ci_endpoint_http] vorhanden sein.
Zugehöriges Service-CI	Anwendungsservice-CI im Zusammenhang mit dem HTTP-Endpunkt. Der eingegebene Wert wird zum Erstellen oder Aktualisieren der CI-Beziehung zwischen dem HTTP-Endpunkt und dem Anwendungsservice verwendet.
Abfrageparameter	Zeichenfolge von Abfrageparametern, die in die Anforderungs-URL aufgenommen werden sollen. **Hinweis:** Die Zeichenfolge darf das führende Fragezeichen nicht enthalten. Verwenden Sie beispielsweise `id=xyz&customer=myco` anstelle von `?id=xyz&customer=myco`.
Anmeldeinformationen	Anmeldeinformationen erforderlich, wenn der Endpunkt eine Authentifizierung erfordert.
Header	Schlüssel-Wert-Paare für die Header der HTTP-Anforderung. Sie können mehrere Paare hinzufügen.
Textkörper	Text, der verwendet wird, wenn die API einen Nachrichtentext erwartet, z. B. ein JSON-Fragment.

c. Wählen Sie im Abschnitt Standorte einen Standort aus, den Sie zuvor erstellt haben, oder verwenden Sie den Link, um einen zu erstellen.
Weitere Informationen zum Erstellen eines Standorts finden Sie unter Erstellen Sie Synthetische Überwachung Standorte.

d. Geben Sie im Abschnitt „Assertion“ einen HTTP-Statuscode ein, der den Test als Erfolg definiert.
Wenn beispielsweise ein erfolgreicher Test bedeuten soll, dass der Endpunkt einen HTTP `200 OK`– Code zurückgibt, geben Sie `200`ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Geben Sie im Abschnitt „Häufigkeit“ die Anzahl der Minuten zwischen den einzelnen Testausführungen ein.

f. Wahlweise: Erstellen Sie im Abschnitt „Warnungseinstellungen“ eine Warnung, die sendet, wenn der Test fehlschlägt, indem Sie den Umschalter aktivieren und einen Warnungsschweregrad für den Fehler auswählen.

4. Wählen Sie **Speichern**.

Ergebnisse
Auf der Seite „Übersicht“ für den Synthetic Monitor werden die Ergebnisse der Tests angezeigt, die der Monitor ausführt. Details siehe Synthetische Überwachung verwenden.

Synthetic-Monitore verwalten

Deaktivieren oder löschen Sie einen Synthetic Monitor, nachdem Sie ihn erstellt haben.

Vorbereitungen
Erforderliche Rolle: Synthetics. Synthetics_Editor

Prozedur
1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* und wählen Sie das Symbol Synthetische Überwachung ( ).
2. Um einen Monitor zu bearbeiten, führen Sie eine der folgenden Aktionen aus.

Option	Beschreibung
Bearbeiten Sie die Konfiguration	Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie einen Synthetic Monitor.
Löschen Sie Überwachungen	Wählen Sie auf der Zielseite Synthetic-Überwachung einen oder mehrere zu löschende Monitore aus, und wählen Sie **Löschen**aus.
Deaktivieren Sie einen Monitor	Wählen Sie auf der Registerkarte **Details** für den Monitor den Umschalter aus, um einen Monitor ein- oder auszuschalten, und wählen Sie dann **Speichern**aus.

Synthetische Überwachung verwenden

Von Synthetic Monitoren ausgeführte Tests ermöglichen es Servicebesitzern und -betreibern, die Leistung des Serviceendpunkts im großen Rahmen anzuzeigen.

Übersicht über die Verwendung von Synthetische Überwachung

Als Serviceverantwortlicher können Sie mit Synthetische Überwachung die Endpunkte Ihres Service überwachen und sicherstellen, dass er verfügbar ist und die erwartete Leistung erbringt. Sie können sich benachrichtigen lassen, wenn synthetische Tests fehlschlagen, um Probleme schnell zu beheben. Sie können Trends bei den Erfolgsraten und Antwortzeiten der HTTP-API anzeigen.

Als Operator können Sie Synthetische Überwachung für die Selektierung von Problemen verwenden. Wenn Sie erfahren, dass für einen Service Probleme gemeldet wurden, können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie Testergebnisse für die Endpunkte dieses Service anzeigen. Wenn Tests fehlschlagen oder die Antwortzeiten langsam sind, kann dies ein Grund sein, dies zu untersuchen.

Identifizieren Sie Systemprobleme mit Synthetische Überwachung

Erfahren Sie, wie Sie mit Synthetische Überwachung den Status und die Integrität Ihrer Überwachungen anzeigen und so feststellen, wann ein Problem vorliegt.

Zeigen Sie zusammengefasste Informationen zu den Monitoren an

Die Zielseite Synthetische Überwachung zeigt eine Übersicht aller erstellten Überwachungen, einschließlich inaktiver Überwachungen.

Von hier aus können Sie den Status für alle Ihre Monitore anzeigen. Durch Auswahl einer Karte oben wird die Liste der Überwachungen gefiltert. Beispielsweise können Sie nur die Monitore anzeigen, bei denen ein Fehler aufgetreten ist oder die sich in einem unbekannten Status befinden.

Standardmäßig wird die Liste der Überwachungen nach dem Zeitstempel in der Spalte **Aktualisiert** sortiert. Sie können einen anderen Spaltenheader auswählen, um nach dieser Kategorie zu sortieren.

Wenn Sie einen Monitor auswählen, können Sie Details zu den Tests des Monitors anzeigen, einschließlich Details, Konfiguration und zugehöriger Configuration Items (CIs).

Zeigen Sie einen Monitor und seine Tests an

Um die Details eines Monitors und die Ergebnisse seiner Tests anzuzeigen, wählen Sie einen Monitor auf der Zielseite Synthetische Überwachung aus. Die Seite „Monitordetails“ enthält wichtige Informationen, die zum Verständnis der Leistung des Monitors erforderlich sind.

Verwenden Sie die Informationen im Header, um den grundlegenden Zustand des Monitors zu verstehen, einschließlich seines Status und des Zeitpunkts der letzten Ausführung eines Tests.

Verwenden Sie die Konfigurationskarte, um die grundlegenden Konfigurationsparameter des Monitors zu verstehen. Wenn sich ein Monitor in einem `unbekannten` Status befindet, können Sie mit dem Endpunktlink überprüfen, ob der richtige Endpunkt für den Monitor ausgewählt wurde. Ein `unbekannter` Status tritt häufig aufgrund eines Problems mit dem zugehörigen Agent Client Collector (ACC)-Proxy auf.

Zeigen Sie einzelne Tests an

Auf der Karte „Metriken“ werden zwei Diagramme angezeigt, mit denen Sie die Integrität der einzelnen vom Monitor ausgeführten Tests nachvollziehen können. Das **Erfolgsquotendiagramm** zeigt für jeden Test den Wert `1` an, wenn er erfolgreich war, und den Wert `0`, wenn er fehlgeschlagen ist. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um weitere Details anzuzeigen.

Das **Antwortzeitdiagramm** zeigt die Zeit in Millisekunden, die für den Empfang einer Antwort vom Endpunkt benötigt wurde. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um Details anzuzeigen.

Hinweis: Die Testergebnisse werden 21 Tage lang gespeichert.

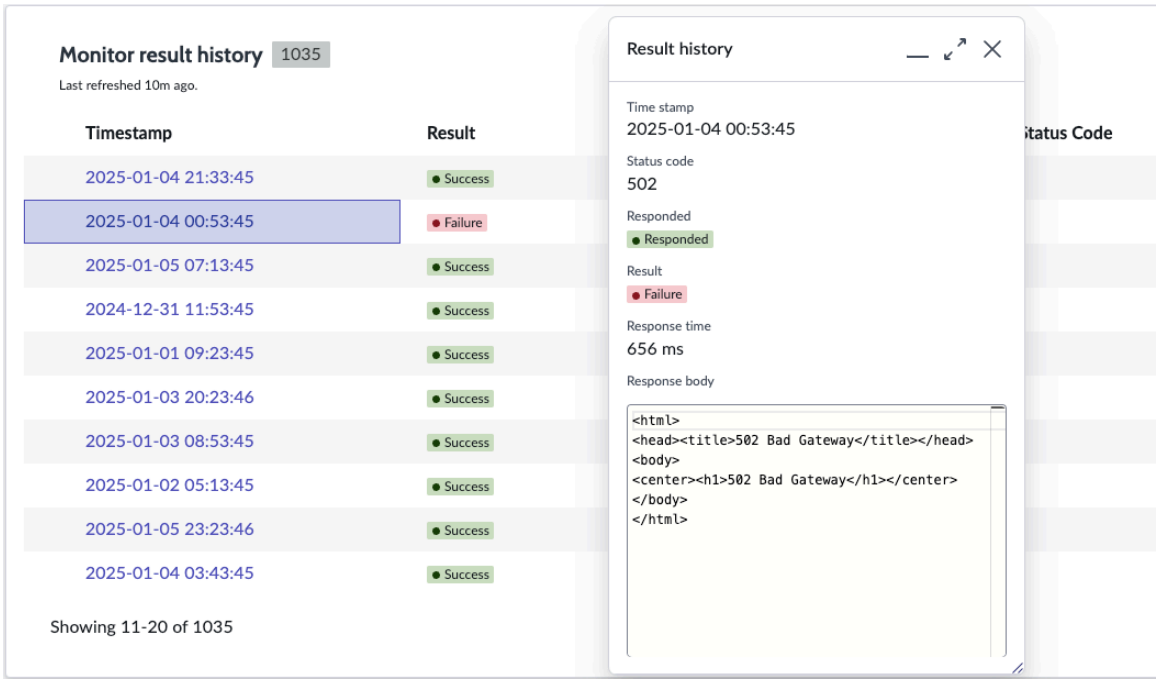
In der Tabelle **„Überwachungsergebnisverlauf“** werden die einzelnen Tests aufgelistet. Standardmäßig wird die Tabelle nach Zeitstempel von den neuesten zu den ältesten sortiert. Sie können nach jeder Spalte sortieren, um bei der Suche nach Problemen zu helfen. Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

können beispielsweise nach **Ergebnis** sortieren, um alle Fehler gemeinsam anzuzeigen, oder nach **Antwortzeit** sortieren, um die Tests mit der höchsten Latenz anzuzeigen.

Wenn Sie einen Fehler oder eine hohe Latenz feststellen, wählen Sie einen Test aus, um Details anzuzeigen, einschließlich des Antworttexts, der helfen kann, Probleme zu erklären.

Antworttext im Detailmodal



Zeigen Sie aggregierte Überwachungsinformationen an

Zeigen Sie Informationen zu allen Ihren Synthetic-Monitoren an.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* und wählen Sie das Symbol Synthetische Überwachung ( ).
2. Um die Liste der Überwachungen zu filtern, wählen Sie oben auf der Seite eine Karte aus. Um beispielsweise nur wenige Monitore zu überwachen, bei denen die Tests fehlgeschlagen sind, wählen Sie die Karte **Fehlgeschlagen**.
3. Um Details zu den einzelnen vom Monitor ausgeführten Tests anzuzeigen, wählen Sie einen Monitornamen aus.
   Die Detailseite des Monitors wird geöffnet. Weitere Informationen zu dieser Seite finden Sie unter Zeigen Sie die Testergebnisse eines Monitors an.
4. Um die Liste der Überwachungen zu exportieren, wählen Sie **Exportieren**.
   Sie können in die folgenden Dateiformate exportieren:
   - XLSX
   - CSV
   - JSON
   - PDF

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie die Testergebnisse eines Monitors an

Zeigen Sie die Ergebnisse der von einem Monitor ausgeführten Tests zusammen mit Konfigurationsdetails und zugehörigen Configuration Items (CIs) an.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* und wählen Sie das Symbol Synthetische Überwachung ( ).
2. Wählen Sie einen Monitor aus der Liste aller Monitore aus.
3. Zeigen Sie die Gesamtintegrität der Überwachung im Header an, der ihren Status und wann sie zuletzt ausgeführt und aktualisiert wurde.
4. Zeigen Sie auf der Karte **Konfiguration** eine Übersicht über die Konfiguration des Monitors an.
   - Um die vollständige Konfiguration anzuzeigen, verwenden Sie die Registerkarte **Details**. Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie einen Synthetic Monitor.
   - Um die Integrität des zugeordneten CI anzuzeigen, wählen Sie den Link.
5. Zeigen Sie auf der Karte **Metriken** Integritätsmetriken für den Monitor an.
   Das **Erfolgsquotendiagramm** zeigt für jeden Test den Wert `1` an, wenn er erfolgreich war, und den Wert `0`, wenn er fehlgeschlagen ist. Das **Antwortzeitdiagramm** zeigt die Zeit in Millisekunden, die für den Empfang einer Antwort vom Endpunkt benötigt wurde. Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um Details anzuzeigen
   - Um den Zeitraum zu ändern, verwenden Sie das Dropdown-Menü.
   - Um die Zeichen zu aktualisieren, verwenden Sie das Kontextmenü.
6. Zeigen Sie den Status jedes Tests auf der Karte **Überwachungsergebnisverlauf an**.
   Um die Details für einen Test anzuzeigen, wählen Sie den zugehörigen Zeitstempel aus. Weitere Informationen zu den Testdetails finden Sie unter Zeigen Sie Testdetails an.

   Hinweis: Das Filtern der Liste wirkt sich auf die in den Metrikdiagrammen angezeigten Daten aus.

Zeigen Sie Testdetails an

Zeigen Sie die Ergebnisse eines einzelnen Synthetic-Tests an, der von einem Monitor ausgeführt wurde.

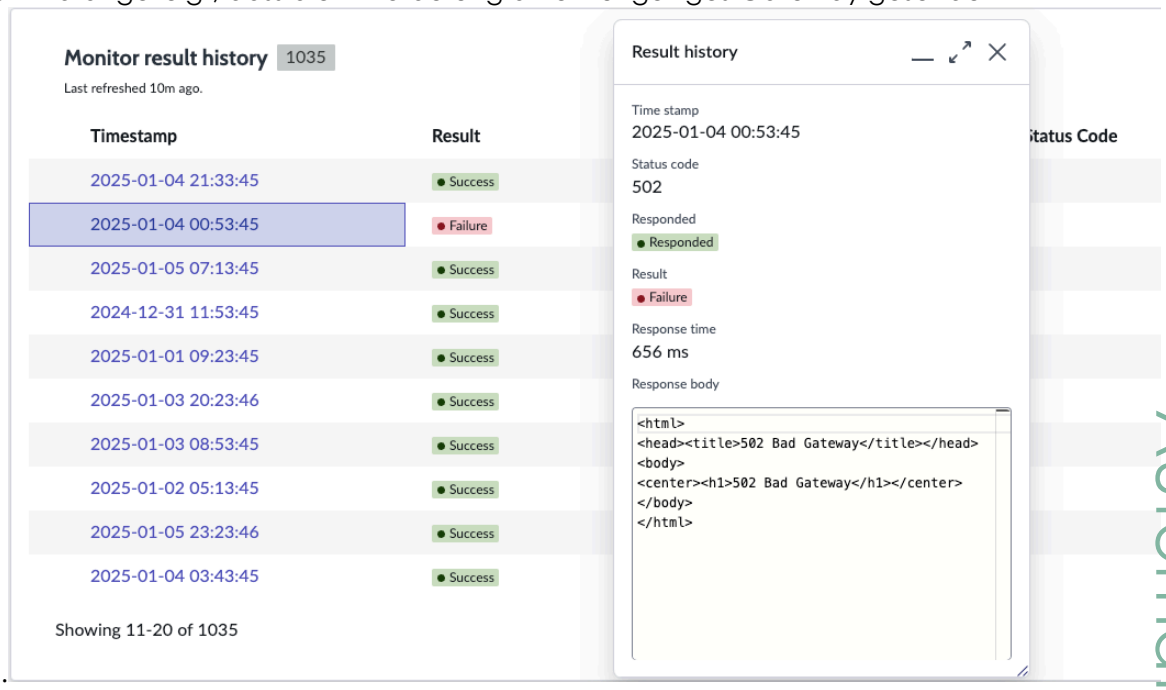
Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > *Service Operations-Arbeitsbereich* und wählen Sie das Symbol Synthetische Überwachung ( ).
2. Wählen Sie einen Monitor aus der Liste aller Monitore aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie einen Test aus der Liste der Tests aus.
   Das Modal zeigt Informationen zum Test an, einschließlich eines Antworttexts. In diesem Beispiel wird angezeigt, dass die Anforderung an ein ungültiges Gateway gesendet wurde.



Synthetische Überwachung – Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Synthetische Überwachung, z. B. installierte Komponenten und Seitendetails.

Mit Synthetische Überwachung installierte Komponenten

Bei der Aktivierung des Synthetische Überwachung-Plugins werden verschiedene Arten von Komponenten installiert, einschließlich Tabellen und Benutzerrollen.

Installierte Rollen

Rolle	Beschreibung	Enthält Rollen
Synthetic-Monitor-Viewer [sn_ Synthetics. Synthetics_viewer]	Zeigt Testkonfigurationen und deren Ergebnisse an.	• cmdb_read • sn_sow.sow_user • agent_client_collector_user • sn_ Synthetics.credential_reader
Synthetic-Monitor-Editor [sn_ Synthetics. Synthetics_editor]	Erstellt und bearbeitet Tests. Zeigt Testkonfigurationen und deren Ergebnisse an.	• credential_admin • sn_cmdb_editor • sn_ Synthetics. Synthetics_ Viewer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Rolle	Beschreibung	Enthält Rollen
Synthetic Monitor-Administrator [sn_ Synthetics. Synthetics_admin]	Weist Rollen zu. Erstellt und bearbeitet Tests. Zeigt Testkonfigurationen und deren Ergebnisse an.	• agent_client_collector_admin • sn_ Synthetics. Synthetics_ Editor

Installierte Tabellen

Tabelle	Beschreibung
Überprüfen sn_ Synthetics Check	Konfigurationsinformationen für Synthetic Checks.
Prüfen Sie den Ausführungsort [sn_ Synthetics_check_execution_location]	Konfiguration des Ausführungsorts für Synthetic Checks.
Einzelne API sn_ Synthetics_check_single_api	Zusätzliche Konfigurationsinformationen und Ergebnisse der letzten Ausführung für Synthetic-Prüfungen einer einzelnen API.
Einzelner API-Header [sn_ Synthetics_check_single_api_header]	Schlüssel-Wert-Paare von Anforderungsheadern für Synthetic-Prüfungen einer einzelnen API.
Einzelne API zur Richtlinie [sn_ Synthetics_check_single_api_policy]	Synthetic-Prüfungsdaten einer einzelnen API und zugehörige Agent Client Collector -Richtlinien (ACC).
Einzelnes API-Ergebnis [sn_ Synthetics_check_single_api_result]	Ergebnisse aus jeder Synthetic-Scheck-Ausführung.
Synthetic Private Speicherorte sn_ Synthetics_private_location]	Definitionen der für Synthetische Überwachungverfügbaren ACC-Agent-Proxy-Cluster. Erweitert die Tabelle „Proxy-Agent-Cluster“ [sn_agent_cluster].

Domänentrennung und Synthetische Überwachung

Domänentrennung wird für Synthetische Überwachung unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Domain Separation und Übersicht über Synthetische Überwachung .

Domänentrennung ist in allen Aspekten der Anwendung Synthetische Überwachung vorhanden. Benutzer, die zu einer bestimmten Domäne gehören, sehen nur die Daten, die in ihrer eigenen Domäne vorhanden sind.

So funktioniert Domain Separation in Synthetische Überwachung

Wenn Daten in Synthetische Überwachungdurch Domänen getrennt sind, können Benutzer die Überwachungsdaten nur in ihrer eigenen Domäne konfigurieren und anzeigen. Standardmäßig werden alle Benutzer und Datensätze auf die übergeordnete Domäne festgelegt, es sei denn, der Administrator weist sie einer bestimmten Domäne zu.

Sie definieren die domänengetrennte Umgebung, wenn Sie Ihre Dateneingaben konfigurieren. Alle relevanten Datensätze und Datenverarbeitungsvorgänge im Programm-Flow Synthetische Überwachung befinden sich in derselben Domäne wie die Dateneingabe. Der Domänenname einer Dateneingabe wird in der Spalte Domäne angezeigt, die in den Tabellen in Ihrer Instanz angezeigt wird.

Die Verwendung der Domänentrennung in Ihrer Instanz ist für Synthetische Überwachung transparent. Die Anwendung verwaltet alle Aspekte der Daten, z. B. die Überwachungskonfigurationen und Ergebnisse. Wenn eine Eigenschaft geändert wird, wirkt sich der neue Wert nur auf neue Quellen in der spezifischen Domäne aus.

Beim Einrichten Agent Client Collector von (ACC) für nicht gehostete Synthetic-Prüfungen benötigen die Domänen und, die nicht gehostete Synthetics unterstützen, einen eigenen ACC-Cluster und MID-Server, die von einem Benutzer in dieser Domäne erstellt werden. Der ACC-Cluster und MID-Server müssen in einer untergeordneten Domäne erstellt werden.

Zugehörige Informationen

Domänentrennung für Service Provider

Zielseite von Synthetische Überwachung

Lesen Sie den folgenden, um zu verstehen, was auf der Zielseite Synthetische Überwachung angezeigt wird, auf der Sie zusammengefasste Informationen zu Ihren Synthetic Monitors anzeigen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informationen zusammenfassen

Die Karten zeigen zusammengefasste Informationen für alle Überwachungen an, unabhängig davon, ob sie aktiv sind oder nicht. Wählen Sie eine Karte aus, um die Liste „Monitore“ zu filtern.

Aggregatkarten

Kartentitel	Beschreibung
Gesamtanzahl Überwachungen	Gesamtzahl der erstellten Überwachungen.
Bestanden	Gesamtanzahl von Überwachungen, die den Wert zurückgegeben haben, der als Assertion der Überwachung festgelegt wurde, z. B. der Statuscode `200`.
Fehlgeschlagen	Anzahl der Gesamtüberwachungen, die einen anderen Wert als den als Assertion konfigurierten Wert zurückgegeben haben.
Ausstehend	Gesamtanzahl der Überwachungen im Status „Ausstehend“. Überwachungen werden vor der Ausführung des ersten Tests auf **Ausstehend** gesetzt.
Angehalten	Gesamtanzahl der Überwachungen, die sich im Status „Angehalten“ befinden. Angehaltene Überwachungen sind diejenigen, die auf der Konfigurationsseite auf **Überwachung deaktiviert** festgelegt wurden.
Unbekannt	Gesamtanzahl von Überwachungen, die aufgrund eines Problems mit dem zugehörigen Proxy Agent Client Collector (ACC) nicht ausgeführt werden.

Überwachungsliste

Standardmäßig zeigt diese Liste alle erstellten Überwachungen an. Sie können eine Karte oben auf der Seite auswählen, um nach einer Liste von Überwachungen mit diesem Status zu filtern. Wählen Sie einen Monitor aus, um die zugehörige Detailseite anzuzeigen.

Detailseite eines Synthetic-Monitors

Lesen Sie den folgenden, um zu verstehen, wie Sie auf der Detailseite eines Synthetic Monitors die Ergebnisse seiner Tests anzeigen.

Header

Der Header bietet eine Übersicht über den Monitor.

Artikel	Beschreibung
Überwachungsname	Name, der dem Monitor bei seiner Erstellung zugewiesen wurde.
Aktiviert	Angabe, ob die Überwachung aktiv ist.
Status	Status der letzten Testausführung. Die folgenden Werte sind möglich: • Ausstehend: Der Monitor wartet auf die Ausführung des ersten Tests, basierend auf der konfigurierten Frequenz. • Erfolg: Der Test wurde ausgeführt und hat die von Ihnen festgelegten Assertionskriterien erfüllt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Artikel	Beschreibung
	• Unbekannt: Der Test konnte aufgrund eines Problems mit dem zugehörigen Agent Client Collector (ACC)-Proxy nicht ausgeführt werden. • Fehler: Der Test wurde ausgeführt, hat jedoch die Assertionskriterien nicht erfüllt. Wählen Sie einen Zeitstempel-Link, um den Antworttext mit weiteren Informationen zum Test anzuzeigen.
Letzter Test ausgeführt	Zeitstempel, der angibt, wann der letzte Test abgeschlossen wurde.
Zuletzt aktualisiert	Zeitstempel, der angibt, wann die Überwachung zuletzt bearbeitet und gespeichert wurde.

Registerkarte „Übersicht“

Die Registerkarte **Übersicht** bietet eine zusammengefasste Ansicht aller Tests, die der Monitor ausgeführt hat. Diese Registerkarte zeigt Folgendes:

- Konfigurationskarte: Aktuelle Grundkonfiguration des Monitors.
- Metrikenkarte: Diagramme, die die Leistung jedes Tests für den in der Zeitauswahl ausgewählten Zeitraum anzeigen.
- Ergebnisverlauf überwachen: Alle von der Überwachung ausgeführten Tests und ihre Ergebnisse.

Registerkarte „Details“

Auf der Registerkarte **Details** können Sie einen Monitor erstellen oder einen vorhandenen Monitor bearbeiten. Weitere Informationen finden Sie unter Erstellen und bearbeiten Sie einen Synthetic Monitor.

Registerkarte „Configuration Item“.

Auf der Registerkarte **Konfigurationselement** wird der HTTP-Endpunkt angezeigt, der derzeit dem Monitor zugeordnet ist.

CSDM-Richtlinien auf ITOM-Integrität anwenden

ITOM-Integrität hilft Ihnen, die Integrität von Services in Ihrer Organisation nachzuverfolgen und aufrechtzuerhalten. Die Referenz ITOM-Integrität CSDM dient als grundlegende Blaupause für die Aufrechterhaltung eines optimalen IT-Betriebs durch Standardisierung von Datenmodellen und Prozessen. Das Hauptziel besteht darin, Ihnen das Verständnis der beiden Hauptfähigkeiten zu erleichtern, die innerhalb des CSDM -Frameworks zusammenarbeiten.

ITOM-Integrität besteht aus zwei Hauptfähigkeiten, die das Framework CSDM verwenden.

Ereignismanagement

Ereignismanagement sammelt Warnungen von Infrastrukturereignissen, die von Überwachungstools von Drittanbietern erfasst wurden. Ereignismanagement verwendet von Discovery gesammelte IT-bezogene Informationen, um Warnungen CIs zuzuordnen. Basierend auf den erfassten Informationen stellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ereignismanagement Dashboards bereit, die eine konsolidierte Ansicht aller Serviceeinfluss-Events anzeigen.

Erkennung von Metrikanomalien

Analysiert Ihre IT-Infrastruktur proaktiv, um Probleme zu erkennen und Serviceausfälle zu verhindern. Mithilfe von erweitertem maschinellem Lernen zur Analyse von Informationen über Ihre IT-Infrastruktur ermittelt die Anwendung automatisch dynamische Schwellenwerte und identifiziert Anomalien, die auf potenzielle Serviceausfälle hindeuten.

Informationen zum Einrichten von CSDM finden Sie unter Implementierung des Frameworks CSDM in Phasen .

Weitere Informationen zum Framework CSDM finden Sie unter Lernen Sie das Framework CSDM kennen .

ITOM-Integrität Überlegungen zum CSDM Framework

ITOM-Integrität wird am CSDM -Framework ausgerichtet, um eine standardisierte Datenverwaltung sicherzustellen und den IT-Betrieb zu optimieren.

Bei der Implementierung des Frameworks ITOM-Integrität für CSDM sind folgende wichtige Punkte zu berücksichtigen.

Identifizieren der notwendigen Konfigurationselemente (Configuration Items, CI) für optimale Ereignismanagement -Vorteile

Ereignismanagement nutzt Configuration Items (CIs), die vom Betriebsteam überwacht werden, um Warnungen mit dem entsprechenden CI zu korrelieren und ihre Auswirkungen auf den überwachten Service zu bewerten.

Definition technischer Services in Ereignismanagement

Services für dynamische CI-Gruppen, früher bekannt als Technische Services, nutzen die Fähigkeit CMDB CI-Gruppe, um die CMDBabzufragen und eine effiziente Gruppierung von Configuration Items (CIs) für verschiedene operative Zwecke zu ermöglichen.

Erkennen gängiger Anwendungsfälle für den Service „Dynamische CI-Gruppe“.

In Ereignismanagement (EM) fungiert der Service „Dynamische CI-Gruppe“ als logischer Gruppierungsmechanismus für Configuration Items (CIs) und bietet Technologie- oder Serviceverantwortlichen Einblicke in den Integritätsstatus der gruppierten Entitäten.

ITOM-Integrität und CSDM-Tabellen

ITOM-Integrität nutzt und verwaltet die Tabellen CSDM, während verschiedene Produkte ServiceNow von den Betrieb verbessern und ihm Mehrwert bringen.

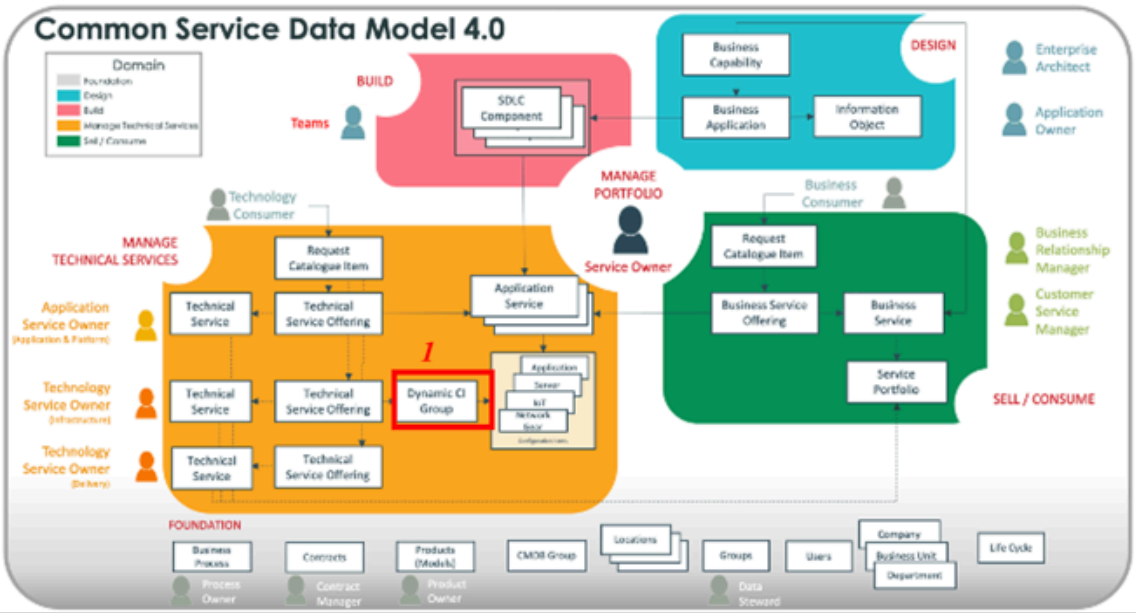
Von ITOM-Integrität verwaltete CSDM-Tabellen

ITOM-Integrität verwaltet die folgenden Tabellen:

- Tabelle „Zugeordneter Anwendungsservice“ [cmdb_ci_service_discovered]
- Tabelle für Konfigurationselemente [ci_*]
- Tabelle „Dynamische CI-Gruppe“ [cmdb_ci_query_based_service]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von ITOM verwaltete CSDM-Tabellen



Mit installierte Plugins oder Anwendungen ITOM-Integrität

Tabellen, die die Plugins oder Anwendungen auflisten, die mit den -Anwendungen ITOM-Integrität installiert werden. Wenn Sie Ihre Anwendung aktualisieren, werden alle neu erforderlichen Anwendungsabhängigkeiten installiert.

Ereignismanagement

Mit Ereignismanagement (com.glideapp.itom.snac) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Inhalt der Warnungsverwaltung (com.em-alert-mgmt-content)	Enthält alle erforderlichen Basissystem-Subflows, die zur Behebung von Warnungen verwendet werden können.
ITOM Lizenzierung (com.snc.itom.license)	Zentrale Komponenten für das Lizenzierungsmodell ITOM, das berechnet und anzeigt, wie viele Abonnements für ITOM -Anwendungen Ihr Unternehmen erworben und verbraucht.
MID-Webserver (com.snc.sa.mid.webserver)	Eine MID-Server-Erweiterung, die die Entwicklung von REST APIs zum Senden von Ereignissen und Metriken an den MID-Server ermöglicht. Zudem ermöglicht das Plugin die Kommunikation zwischen MID-Server und Agent Client Collector.
Serviceanalytik (com.snc.sa.analytics)	Stellt Warnungsanalysen basierend auf maschinellem Lernen (ML) und Topologielernen bereit.
Ereignismanagement und Service-Mapping Core (com.snc.service-watch)	Besteht aus den gemeinsamen Komponenten von Ereignismanagement und Service-Mapping.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Ereignismanagement (com.glideapp.itom.snac) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
Engine für tag-basiertes Alarm-Clustering (sn_em_tback)	Stellt eine Zero-Code-Methode bereit, die die Gruppierung von Warnungen vereinfacht und Warnungskorrelation durchführt, ohne dass CMDB, Modelltraining oder Feinabstimmung erforderlich sind.
Regel-Management für Warnmeldungen (sn_em_arm)	Ermöglicht Anwendern von Ereignismanagement, automatisch auf Warnungen zu reagieren. Eine Warnungsverwaltungsregel bestimmt die erforderliche Warnungsantwort.

Health Log Analytics

Mit Health Log Analytics (sn_occ) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Gemeinsame Komponenten für Integrationen für CMDB (sn_cmdb_int_util)	Enthält eine Sammlung von Dienstprogrammfunktionen, die eine allgemeine Methode für die Verarbeitung von Schlüsselattributen CMDB bereitstellen und für alle zertifizierten CMDB -Integrationen verfügbar sind.
ITOM Cloud Services Core (sn_itom_cloud_svc)	Generiert relevante Themen für Mandanten, damit sie Daten aus ihrer Kundeninfrastruktur automatisch an ServiceNow übertragen können. Diese Themen sind hauptsächlich für die Verwendung mit dem Hermes Messaging Service vorgesehen.
Service Operations-Arbeitsbereich ITOM Apps (sn_sow_itom_cont)	Ein konfigurierbarer Arbeitsbereich mit einer einheitlichen Experience für mehrere IT Operations Management-Workflows. Sie können den Lebenszyklus von Warnungen in IT Operations Management-Workflows durch eine einfache, intuitive und übersichtliche Anwenderoberfläche, automatisierte Empfehlungen und eine zielgerichtete Experience verwalten.
Health Log Analytics Kern (com.glideapp.itom.occultus)	Wichtige Komponenten für die bereichsbezogene Anwendung Health Log Analytics.
Microsoft Teams Spoke für ServiceNow IntegrationHub (com.sn.ms_teams.ah)	Stellt Aktionen bereit, die ein -Prozessanalyst beim Entwerfen von Flows verwenden kann, um das Senden von Nachrichten zu Incident- und Problem-Datensätzen ServiceNow

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Health Log Analytics (sn_occ) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
	an einen Kanal Microsoft Teams zu automatisieren.
Slack Webhooks Spoke for ServiceNow IntegrationHub (com.sn.slack.ah)	Verwenden Sie Slack-Webhooks, um Nachrichten zu senden und Details für ServiceNow-Incidents, Probleme und Änderungen bei Slack-Kanälen aufzuzeichnen.
Normalisierungsdatenservices Client (com.glide.data_services_canonicalization.client)	Sorgt für Konsistenz, indem überprüft wird, ob die Datensätze für ein bestimmtes Unternehmen mit der Liste der Standard-Unternehmensnamen übereinstimmen. Wenn das Plugin ein Unternehmensnamensfeld mit einer Variante dieses Namens findet, ersetzt es den Standardnamen.

Service Reliability Management

Mit Service Reliability Management (sn_sow_srm) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Service Operations-Arbeitsbereich Service Reliability Management (SRM) Common (sn_sow_srm_common)	Stellt allgemeine Dienstprogramme und Konfigurationseinstellungen bereit, die von Service Reliability Management verwendet werden, z. B. Kernfunktionen für die Verwaltung von Teams und Services sowie für die Metrikberechnung für Services.
Service Reliability Management (Globale Abhängigkeiten) (com.snc.srm)	Unterstützt globale Skripts und Dienstprogramme für Service Reliability Management für Service Operations-Arbeitsbereich.
Ereignismanagement (com.glideapp.itom.snac)	Hilft Ihnen, Integritätsprobleme in Business-Services und Infrastrukturen in einer einzigen Managementkonsole zu identifizieren. Ereignismanagement bietet intelligente Ereignis- und Warnungsverarbeitung, einschließlich automatischer Warnungsbehebung, Zusammenfassung und Ursachenanalyse (RCA).
Service Operations-Arbeitsbereich ITOM Apps (sn_sow_itom_cont)	Ein konfigurierbarer Arbeitsbereich mit einer einheitlichen Experience für mehrere IT Operations Management-Workflows. Sie können den Lebenszyklus von Warnungen in IT Operations Management-Workflows durch eine einfache, intuitive und übersichtliche Anwenderoberfläche, automatisierte Empfehlungen und eine zielgerichtete Experience verwalten.
Bereitschaftsplanung (com.snc.on_call_rotation)	Bietet die Möglichkeit, Rufbereitschaftszeitpläne und Eskalationsbäume zu erstellen. Wenn ein Incident erstellt wird, können Sie die Eskalation dynamisch an eine Bereitschaftsressource weiterleiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Service Reliability Management (sn_sow_srm) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
SOW – Warnungsautomatisierung (sn_sow_alert_rules)	Bietet Bedienern in Service Operations-Arbeitsbereich die Möglichkeit, Warnungsautomatisierungen für ihr Team zu erstellen und zu verwalten. Diese Automatisierung kann zum Anreichern, Verarbeiten und Gruppieren von Warnungen verwendet werden.
Servicelevel-Zielmanagement für Service Operations-Arbeitsbereich (sn_sow_slo)	Enthält Funktionen zum Überwachen und Verwalten der Serviceintegrität mithilfe von Servicelevel-Indikatoren (SLIs), Servicelevel-Zielen (SLOs) und Fehlerbudgets.

Service Operations-Arbeitsbereich für ITOM

Mit Service Operations-Arbeitsbereich ITOM Apps (sn_sow_itom_cont) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Service Operations-Arbeitsbereich Kern (sn_sow)	Kernfähigkeiten und Arbeitsbereichskonfigurationen für Service Operations-Arbeitsbereich.
Ereignismanagement Kern (sn_em_ai)	Ermöglicht das Nachverfolgen und Überwachen von Warnungen im ServiceNow Mitarbeiterbereich.
Service Operations-Arbeitsbereich Integrations-Launchpad (sn_itom_integ_app)	Bietet eine neue und verbesserte Experience zum Anzeigen, Konfigurieren und Verwalten aller verfügbaren ITOM-Integrität-Integrationen.
Service Operations-Arbeitsbereich Warnungsverwaltung (sn_sow_em)	Eine detaillierte Warnungsdatensatzseite mit zusätzlichen Daten wie den Registerkarten „Schneller Überblick“, „Playbook“ und „Metriken“.
Service Operations-Arbeitsbereich Express-Liste (sn_itom_aiops_list)	Eine zentralisierte und konsolidierte Plattform, mit der Bediener Warnungen an einem Ort selektieren, analysieren und beheben können. Express-Liste bietet eine Live-Ansicht von Warnungen, dynamische Filterung, ein Vorschaufenster mit zusätzlichem Kontext und wichtigen Details zu jeder Warnung sowie automatisierte technische Analysen mit Now Assist.
Service Operations-Arbeitsbereich Log Analytics (sn_sow_hla)	Ein Protokoll-Viewer in Service Operations-Arbeitsbereich. Die Anwendung enthält auch die anwenderdefinierte Datenquelle Elasticsearch für Dashboards Performance Analytics (PA).
AIOps-Dashboards (sn_aiops_dashboard)	Bietet umfassende Visualisierungen von kritischen Betriebsdaten und umsetzbaren Einblicken, die eine proaktive Reaktion auf potenzielle Probleme erleichtern. Die Anwendung richtet sich an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Service Operations-Arbeitsbereich ITOM Apps (sn_sow_itom_cont) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
	mehrere Personen ITOM mit unterschiedlichen Anforderungen. So können Sie Leistungskennzahlen (Key Performance Indicators, KPIs) überwachen, die Serviceintegrität nachverfolgen und wertvolle Kontextinformationen zur gesamten IT-Umgebung gewinnen.
Ereignismanagement Connectors (sn_em_connector)	Eine Sammlung vordefinierter Schnittstellen (Connectors) für die Erfassung von Ereignissen aus Überwachungstools von Drittanbietern oder Agent Client Collector in einer ServiceNow-Instanz.
Service Operations-Arbeitsbereich UI-Komponenten (sn_itom_uib_comp)	Ein verbundenes Repository zur Aufbewahrung gemeinsamer interner UI-Komponenten.

Metrikdaten

Mit Metrikdaten aktivierte Plugins (com.snc.sa.metric)

Plugin-Name	Beschreibung
Operational Intelligence - Überwachung der Erweiterungsintegrität (com.snc.sa.metric.health)	Enthält einige Funktionen, die Selbstüberwachungsfunktionen für die Metrikdaten -Komponenten in MID-Serveraktivieren.
Highcharts Reporting (com.glide.highcharts)	Stellt einige UI-Funktionen für Metrikdatenbereit.
Ereignismanagement (com.glideapp.itom.snac)	Hilft Ihnen, Integritätsprobleme in Business-Services und Infrastrukturen in einer einzigen Managementkonsole zu identifizieren. Ereignismanagement bietet intelligente Ereignis- und Warnungsverarbeitung, einschließlich automatischer Warnungsbehebung, Zusammenfassung und Ursachenanalyse (RCA).
ITOM UI-Komponenten (com.snc.itom.ui)	Gemeinsam genutzte UI-Komponenten für ITOM -Produkte, die UI-Funktionen für Metrikdatenbereitstellen.
MID-Server Verteilter Cluster (com.snc.agent.distributed.cluster)	Aktiviert die Verwaltung der MID-Cache-Komponente von Metrikdaten in der Instanz ServiceNow.
v3-Komponenten auflisten (com.glide.ui.list_v3_components)	Stellt einige UI-Funktionen für Metrikdaten und Komponenten bereit, die für die Liste v3 erforderlich sind, einschließlich REST-Endpunkte, -Richtlinien und -Vorlagen.
MetricBase (com.snc.textil)	Die Datenbank, in der die Metrikrohdaten wie CPU-Auslastung und freier Datenträger gespeichert werden und in der die Modellanpassung für die Anomalie-Erkennung erfolgt.
MID-Webserver (com.snc.sa.mid.webserver)	Eine MID-Server-Erweiterung, die die Entwicklung von REST APIs zum Senden von Ereignissen und Metriken

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Metrikdaten aktivierte Plugins (com.snc.sa.metric) (Fortsetzung)

Plugin-Name	Beschreibung
	an den MID-Server ermöglicht. Zudem ermöglicht das Plugin die Kommunikation zwischen MID-Server und Agent Client Collector.

Agent Client Collector

Mit Agent Client Collector Framework (sn_agent) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Agent Client Collector Globale Dienstprogramme (com.snc.sa.accutils)	Eine Reihe von Dienstprogrammen mit globalem Umfang, die bereichsübergreifende Transaktionen zwischen Agent Client Collector Framework und einer Instanz ServiceNow erleichtern.
Konfigurationsverwaltung für bereichsbezogene Apps (CMDB) (com.snc.cmdb.scoped)	Bietet bereichsbezogenen Anwendungen Zugriff auf Identifizierungs-Engine-APIs.
MID-Webserver (com.snc.sa.mid.webserver)	Eine MID-Server-Erweiterung, die die Entwicklung von REST APIs zum Senden von Ereignissen und Metriken an den MID-Server ermöglicht. Zudem ermöglicht das Plugin die Kommunikation zwischen MID-Server und Agent Client Collector.

Mit Agent Client Collector-Überwachung (sn_itmon) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Agent Client Collector Framework (sn_agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
Metrikdaten (sn_metrics_ng)	Eine Begleitanwendung für das Plugin der Familie Metrikdaten, die zusätzliche Funktionen und Verbesserungen bietet.
Service Operations-Arbeitsbereich Metric Explorer (sn_itom_metric_exp)	Ermöglicht Betreibern, das Metrikverhalten zu untersuchen und verschiedene Metriken für Hosts, Anwendungen und Services zu vergleichen und zu korrelieren, um Probleme zu beheben und die Ursache zu finden.
Ereignismanagement (com.glideapp.itom.snac)	Hilft Ihnen, Integritätsprobleme in Business-Services und Infrastrukturen in einer einzigen Managementkonsole zu identifizieren. Ereignismanagement bietet intelligente Ereignis- und Warnungsverarbeitung, einschließlich automatischer Warnungsbehebung, Zusammenfassung und Ursachenanalyse (RCA).
Metrikdaten (com.snc.sa.metric)	Bietet die Möglichkeit, Anwendungsmetrikdaten zu erfassen, zu untersuchen und zu analysieren sowie Anomalien zu identifizieren und anzuzeigen. Metrikdaten generiert Anomaliewarnungen, die zu IT-Warnungen hochgestuft werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Agent Client Collector-Überwachung (sn_itmon) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
	können und im Dashboard Service Operations-Arbeitsbereich und im Serviceintegritäts-Dashboard angezeigt werden können.

Mit Agent Client Collector Visibility – Inhalt (sn_acc_visibility) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Agent Client Collector Visibility – Inhalt Inhalt (sn_acc_vis_content)	Bietet agentbasierte Infrastruktur-Discovery und sammelt Software Asset Management (SAM)-Metriken zur Unterstützung der Anwendungen Discovery und Digitale Endanwender-Experience (DEX).
Discovery (com.snc.discovery)	Erkennt Anwendungen und Geräte in Ihrem Netzwerk und aktualisiert dann die CMDB mit den gefundenen Informationen.
Agent Client Collector Framework (sn_agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
CMDB CI-Klassenmodelle (sn_cmdb_ci_class)	Fügt Klassenmodelle hinzu, die die CMDB-Klassenhierarchie erweitern, einschließlich Klassenbeschreibungen, Identifizierungsregeln, Bezeichnereinträge und abhängige Beziehungen, falls zutreffend. Anwendungen wie Discovery und Service-Mapping können diese Klassenerweiterungen verwenden, um Konfigurationselemente (CIs) auszufüllen und verschiedene Technologien und Software zu erkennen.

Mit Agent Client Collector Log Analytics (sn_accl) installierte Anwendungen

Anwendungsname	Beschreibung
Agent Client Collector-Überwachung (sn_itmon)	Bietet die Möglichkeit, Ihre Configuration Items (CIs) zu überwachen. Diese Anwendung enthält vordefinierte Überwachungsprüfungen und -richtlinien, die auf den Agent angewendet werden.
Health Log Analytics (sn_occ)	Hilft Ihnen, Probleme schneller zu lösen, indem maschinell generierte Protokolldaten in Echtzeit erfasst, analysiert und korreliert werden, um IT-Probleme vorherzusagen, bevor sie sich auf Sie auswirken.

Mit Agent Client Collector Security Incident Response (sn_secops_acc) installierte Plugins oder Anwendungen

Plugin- oder Anwendungsname	Beschreibung
Security Incident Response (sn_si)	Ermöglicht Ihnen, den Lebenszyklus Ihrer Security Incidents von der ersten Priorisierung bis zur Eindämmung und Lösung zu verwalten und zu automatisieren. Verwenden Sie die automatisierten Workflows, um schnell und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Agent Client Collector Security Incident Response (sn_secops_acc) installierte Plugins oder Anwendungen (Fortsetzung)

Plugin- oder Anwendungsname	Beschreibung
	konsistent zu reagieren und Trends und Engpässe anhand der Daten zu verstehen, die von analysegesteuerten Dashboards und umfassenden Berichterstellungssystemen bereitgestellt werden.
Sicherheitssupport Orchestration (sn_sec_cmn_orch)	Abhängigkeit für die Anwendungen Vulnerability Response und Security Incident Response.
Threat Intelligence Support Common (sn_ti)	Ermöglicht es Ihnen, Kompromittierungsindikatoren (IoCs) zu finden und Security Incidents mit Threat Intelligence-Daten anzureichern. Threat Intelligence ermöglicht Ihnen den Zugriff auf die STIX-Daten (Struktuierte Bedrohungsinformationen) Ihres Unternehmens und bietet einen Referenzpunkt dafür.
Agent Client Collector Spoke (sn_acc_spoke)	Stellt ein Framework zum Schreiben von anwenderdefinierten Workflows oder Automatisierungen bereit, die für Agents oder CIs ausgeführt werden sollen.
Security Support Core (com.snc.security_support.core)	Bietet ein robustes Kerndatenmodell und UI-Framework speziell für Security Operations-Integrationen. Dieses umfassende Modell dient als Rückgrat für die nahtlose Integration verschiedener Sicherheitstools und -systeme und sorgt für einen reibungslosen Datenfluss und einen effizienten Betrieb.
Security Support Common (sn_sec_cmn)	Aktiviert die Kernfunktionalität, die von den Security Operations -Anwendungen verwendet wird.
Security Integration Framework (sn_sec_int)	Verwaltet die allgemeine Funktionalität für Security Operations -Integrationen, einschließlich Security Incident Response und Vulnerability Response. Mit dem Security Integration Framework können Sie vorhandene Features und Funktionen verwenden, ohne sie erneut implementieren zu müssen.
Agent Client Collector Framework (sn_agent)	Verwaltet Agent Client Collector in der ServiceNow-Instanz und auf dem MID-Server.
Vulnerability Response Abhängigkeiten (com.snc.si_dep)	Aktiviert alle abhängigen Plugins, die zur Unterstützung der Anwendung Vulnerability Response erforderlich sind.

Zugehörige Informationen

- Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate
- Mit installierte Plugins oder Anwendungen ITOM-Transparenz
- Mit aktivierte Plugins ITOM-Optimierung
- Mit Now Assist für ITOM installierte Anwendungen

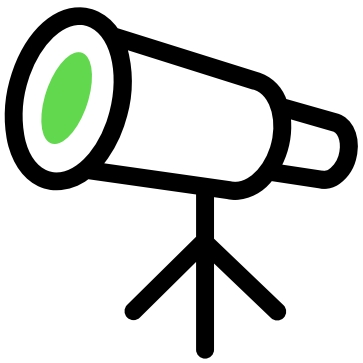
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector

Agent Client Collector ist ein Agent, der auf Infrastrukturkomponenten installiert wird. Agent Client Collector basiert auf einem Sensu-Framework, mit dem Sie Überwachungsprüfungen aus der Community übernehmen und erweitern können. Der Agent führt Befehle auf den Computern aus, auf denen er installiert ist, und sendet über den MID-Server Ausgabedaten an die ServiceNow®-Instanz, wobei Events und Metriken in der entsprechenden Datenbank gespeichert werden.

Sehen Sie sich dieses Video an, um einen Überblick über die Funktionsweise von Agent Client Collector zu erhalten.

Agent Client Collector – Übersicht. Das Video ist etwa vier Minuten und acht Sekunden lang.

Agent Client Collector Framework	Agent Client Collector-Überwachung	Agent Client Collector Visibility – Inhalt
		
Analysieren Sie CI-Daten, die an die Instanz gesendet werden, und stellen Sie Daten für andere Agent Client Collector -Anwendungen bereit.	Überwachen Sie Ihre Serviceverfügbarkeit, und stellen Sie sicher, dass Ihre Infrastruktur und ihre Anwendungen ordnungsgemäß ausgeführt werden.	Erfassen Sie Hostdaten auf Servern mit Agent Client Collector Visibility – Inhalt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Log Analytics	Security Incident Response	Live-CI-Ansicht
Streamen Sie Protokolldaten von den Hosts Linux und Windows an eine Instanz ServiceNow.	Automatisieren Sie die Erfassung von Daten zur Ergänzung von Security Incidents und Antwortaktionen mit Agent Client Collector.	Zeigen Sie Live-Daten für CIs im Zusammenhang mit Incidents an, um Incidents zu beheben.

Agent Client Collector Framework

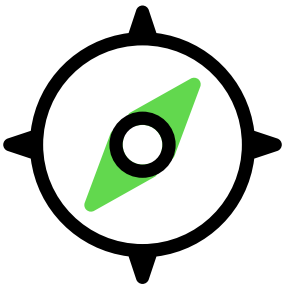
Die Anwendung Agent Client Collector Framework (ACC-F) verwaltet die -Agent-Installation für Ihre Infrastrukturkomponenten und ermöglicht das Senden von Ausgabedaten an die Instanz ServiceNow® über MID-Server. Zusätzlich zu MID-Servermüssen Sie Configuration Management Database für bereichsbezogene Apps (CMDB) installieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

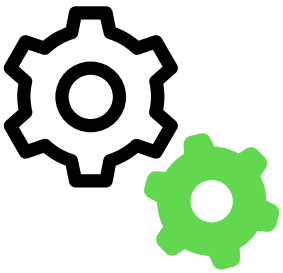
Erste Schritte

Untersuchen



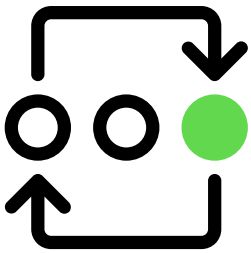
Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen der Anwendung Agent Client Collector Framework kennen.

Konfigurieren



Konfigurieren Sie die Funktionen und Komponenten, um Agent Client Collector Frameworkzu aktivieren.

Arbeiten Sie mit Prüfungen und Richtlinien



Machen Sie sich mit der Arbeit mit Prüfungen vertraut, um Daten aus den Komponenten des Agent zu sammeln.

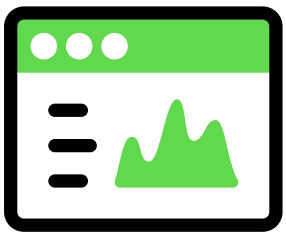
Datensammlung

Aktivieren Sie das Sammeln von Daten von Hosts Agent Client Collector.

Agent Client Collector Protokolle

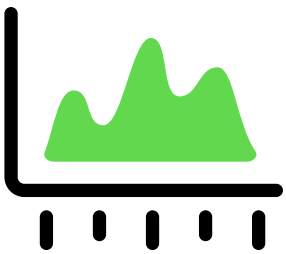
Verfolgen Sie Ereignisse in Ihrem System mithilfe von Agent Client Collector -Protokollen nach

Agent Client Collector Integritätsdashboard



Überwachen Sie den Status der Service Desk-Mitarbeiter in Ihrem System.

Agent Client Collector Funktionsmatrix



Zeigen Sie die Verfügbarkeitsfunktionen Agent Client Collector an.

Referenz

Rufen Sie zusätzliche Details zu Feldbeschreibungen, Konfigurationseigenschaften und Protokollebenen ab.

Problembehandlung und Hilfe

- Stellen oder beantworten Sie Fragen im Community-Forum von Agent Client Collector.
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Framework erkunden

Agent Client Collector Framework (ACC-F) ist eine leistungsstarke Lösung zur Überwachung der Leistung und Integrität von Infrastrukturkomponenten mithilfe von Agents, die auf Servern und Geräten installiert sind. Die Lösung erfasst und sendet kritische Systemdaten zur Analyse an ServiceNow und ermöglicht so eine proaktive Verwaltung und Fehlerbehebung bei Konfigurationselementen (Configuration Items, CI).

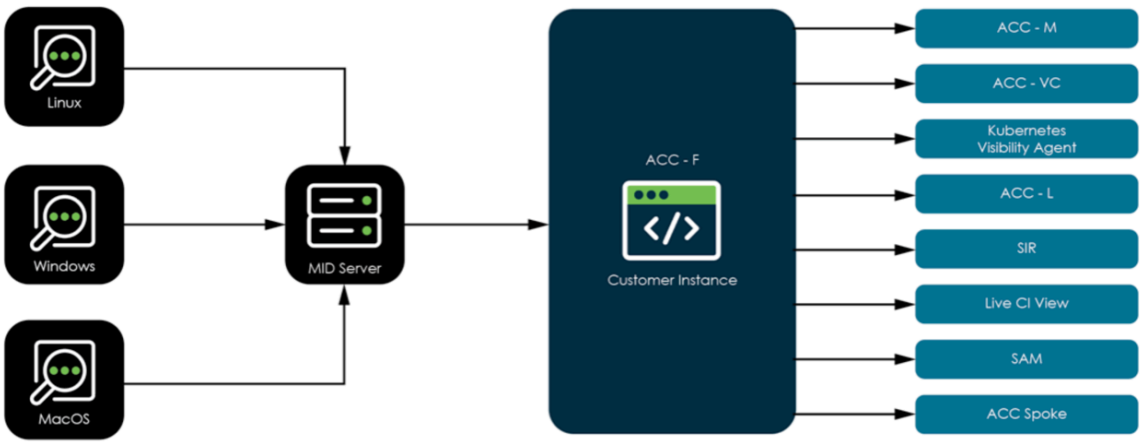
Agent Client Collector Framework – Übersicht

Mit Agent Client Collector Framework können Organisationen den Zustand ihrer -Infrastruktur durch -Agents überwachen und verwalten, die auf wichtigen Systemen installiert sind. Diese Agents führen auf den Computern, auf denen sie installiert sind, vordefinierte Befehle aus und senden die resultierenden Daten über einen dedizierten ServiceNow® an die Instanz MID-Serverzurück. Das -Framework ermöglicht die nahtlose Verwaltung von Agent Client Collector und MID-Serverund speichert Ereignisdaten und Leistungsmetriken in der entsprechenden Datenbank. ACC-F gewährt Einblicke in die CI-Leistung und hilft Unternehmen, Probleme schnell zu erkennen und zu lösen, wodurch die betriebliche Effizienz und die Systemzuverlässigkeit verbessert werden.

Agent Client Collector Framework – Workflow

In der folgenden Abbildung werden das Layout und der Datenfluss in der Anwendung Agent Client Collector Framework beschrieben.

Sammeln und Verteilen von Daten mit ACC-F



1. Installation des Agent: Der Agent wird auf Infrastrukturkomponenten wie Servern, Geräten und Netzwerkgeräten installiert. Diese Agents sind für die Ausführung von Systembefehlen und die Erfassung von Leistungsdaten vom Hostcomputer verantwortlich. ACC-F wird in der Instanz ServiceNow® des Kunden bereitgestellt.
2. Datensammlung: Der -Agent führt vordefinierte Skripts oder Abfragen (Prüfungen) für die -Infrastrukturkomponenten aus, um verschiedene Systemmetriken und Ereignisse zu erfassen. Dazu gehören Leistungsdaten wie CPU-Auslastung, Auslastung des Arbeitsspeichers, Speicherplatz und Netzwerkaktivität. Der Agent sammelt auch Fehlerprotokolle und Systemwarnungen.
3. MID-Server -Kommunikation: Der Service Desk-Mitarbeiter sendet die gesammelten Daten über einen dedizierten ServiceNow an die Instanz MID-Server. MID-Server fungiert als sichere Kommunikationsbrücke zwischen der Infrastruktur und der ServiceNow-Plattform und stellt sicher, dass Daten zuverlässig und sicher übertragen werden.
4. Datenspeicher: Nach dem Empfang der Daten speichert die Instanz ServiceNow die Ereignisse und Leistungsmetriken in der entsprechenden Datenbank. Diese Daten werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dann den entsprechenden Configuration Items (CIs) in ServiceNow CMDB Configuration Management Database (CMDB)zugeordnet, was eine effiziente Nachverfolgung und Berichterstellung ermöglicht.

5. Datenanalyse und Berichterstellung: Die gesammelten Daten werden innerhalb der Instanz ServiceNow analysiert und dort zu Überwachungs-, Problembehandlungs- und Berichterstellungszwecken verwendet. Diese Analyse hilft dabei, potenzielle Probleme oder Verbesserungsbereiche zu identifizieren und Warnungen oder Aktionen auszulösen, um Probleme proaktiv zu lösen.
6. Feedbackschleife: Basierend auf der Analyse kann das System Korrekturmaßnahmen auslösen, z. B. das Ausführen von Korrekturskripts, das Neukonfigurieren von Einstellungen oder das Benachrichtigen verantwortlicher Teams zwecks weiterer Untersuchungen. Das Feedback wird an das System zurückgeführt, was eine kontinuierliche Überwachung und Optimierung ermöglicht.

Agent Client Collector Framework – Vorteile

Agent Client Collector Framework stellt Daten für andere Agent Client Collector -Komponenten bereit.

Vorteil	Funktion	Anwender
Überwachen Sie den Zustand, die Leistung und die Verfügbarkeit Ihres Systems durch die automatisierte Erfassung von Ereignissen und Metriken und nutzen Sie automatisierte Konfigurationen.	Agent Client Collector-Überwachung	NOC-Benutzer, Ereignismanagement Administrator
Verfolgen Sie den Serverbestand, die Softwareinstallationen und die Nutzung kontinuierlich ohne Administratorzugriff und minimale Netzwerkkommunikation.	Agent Client Collector Visibility – Inhalt	CMDB-/Discovery-Administrator
Erfassen Sie detaillierte Bestandsdaten von Geräten, die nicht mit Ihrem Netzwerk verbunden sind oder in isolierten Umgebungen (mit Luftspalt) ausgeführt werden.	Agent Client Collector Framework-Lösung zur Verwaltung von Konfigurationselementen mit Luftspalt	CMDB-/Discovery-Administrator
Minimieren Sie die Zeit für die Selektierung von Incidents durch direkten Zugriff auf Live-Gerätedetails und zu behebende Interaktionen.	Live-CI-Daten mit Agent Client Collector anzeigen	ITSM-Anwender
Lösen Sie Remoteaktionen für verwaltete Geräte ohne zusätzliche Anmeldeinformationen oder Netzwerkkommunikation aus.	Agent Client Collector Security Incident Response	Automatisierungsexperte
Streamen Sie Protokolldaten in Ihre -Instanz, um Probleme vorherzusagen und zu lösen, bevor sie auftreten, und um die Auswirkungen auf die Benutzer zu minimieren.	Agent Client Collector Log Analytics	Agent Client Collector-Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Framework – Anwendungsfall

Der Anwendungsfall Agent Client Collector Framework zeigt, wie eine Finanzorganisation Agent Client Collector Framework zur Unterstützung der Discovery von IT-Assets verwenden kann.

Übersicht über Anwendungsfälle

Ein führendes Finanzunternehmen benötigt eine robuste IT-Erkennungslösung, um die Compliance zu wahren, kritische Systeme zu sichern und eine steigende Zahl von Remote-Mitarbeitern zu verwalten. Anfangs vertraute das Unternehmen zwar auf agentenlose Discovery-Methoden, bei denen MID Servers Systeme abfragt und die CMDB füllt, doch war mit erheblichen Herausforderungen konfrontiert. Diese Einschränkungen wirkten sich auf die Fähigkeit aus, sichere Umgebungen und Remote-Endpunkte effektiv zu überwachen, was zu potenziellen Sicherheits- und Compliance-Risiken führte.

Herausforderungen

- Eingeschränkter Serverzugriff: Die Sicherheitsrichtlinien der Finanzorganisation haben MID Servers daran gehindert, Verbindungen zu zentralen Bankservern und vertraulichen Finanzdatenbanken zu initiieren. Dadurch wurde die agentlose Discovery für diese Assets mit hoher Sicherheit unzureichend.
- Transparenz von Remote-Mitarbeitern: Aufgrund der steigenden Anzahl von Remote-Mitarbeitern des Unternehmens werden viele Laptops und Mobilgeräte von Mitarbeitern außerhalb des Unternehmensnetzwerks betrieben. Die agentenlose Discovery konnte keine Daten von diesen Endpunkten erfassen, was zu toten Winkeln bei der Asset-Nachverfolgung und Compliance-Überwachung führte.
- Regulatorische Compliance: Finanzinstitute sind strengen Vorschriften (z. B. PCI, DSS und SOX) ausgesetzt, die detaillierte und überprüfbare Asset-Daten erfordern. Die agentenlose Discovery hatte Probleme, diese Anforderungen zu erfüllen, insbesondere was die eingehende Überwachung und Richtliniendurchsetzung angeht.

Lösungen

Um diese Herausforderungen zu meistern, implementierte die Finanzorganisation einen Agent-basierten Discovery-Ansatz.

- Agent-Bereitstellung auf kritischen Servern: Auf Core-Banking-Servern und vertraulichen Finanzdatenbanken wurden Agents installiert. Dies ermöglichte eine kontinuierliche und sichere Überwachung, ohne die Zugriffsbeschränkungen zu verletzen.
- Remote-Endpunktverwaltung: Agents, die auf Remote-Laptops von Mitarbeitern bereitgestellt werden, ermöglichen standortunabhängig eine Datenerfassung und -überwachung in Echtzeit. Dadurch wurde sichergestellt, dass alle Geräte, auch solche außerhalb des Unternehmensnetzwerks, in die Asset-Discovery einbezogen wurden.
- Erweiterte Datenerfassung: Die Service Desk-Mitarbeiter erfassten detaillierte Systeminformationen und setzten Sicherheitsrichtlinien direkt für jedes Asset durch. So stellten sie die Compliance mit gesetzlichen Standards sicher und verbesserten die Audit-Bereitschaft.

Ergebnisse

- Umfassende Transparenz von Assets: Die Organisation erreichte vollständige Transparenz in ihrer IT-Umgebung, einschließlich sicherer Rechenzentren und Remote-Endpunkte. Dadurch wurden tote Winkel reduziert und die Entscheidungsfindung für IT-Betriebs- und Sicherheitsteams verbessert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Verbesserte Compliance und Audit-Bereitschaft: Die Agent-basierte Discovery lieferte granulare, überprüfbare Daten, die die strengen gesetzlichen Anforderungen erfüllen. Dadurch wurde das Compliance-Reporting optimiert und das Risiko von gesetzlichen Strafen reduziert.
- Verbesserte Sicherheitslage: Durch die Durchsetzung von Richtlinien auf Endpunktebene hat das Unternehmen seine Cybersicherheitsmaßnahmen gestärkt und vertrauliche Finanzdaten vor potenziellen Bedrohungen geschützt.

Dieser Ansatz ermöglichte es dem Finanzinstitut, die Kontrolle über ihre IT-Umgebung zu behalten, ihre Remote-Mitarbeiter effektiv zu unterstützen und die Einhaltung von Branchenvorschriften sicherzustellen – kritische Faktoren für den Schutz sensibler Finanzvorgänge und die Wahrung des Vertrauens der Kunden.

Agent Client Collector-Architektur

Agent Client Collector ist ein ServiceNow-Agent, der zur Überwachung der Infrastruktur und der installierten Anwendungen Ihres Unternehmens auf Windows-, Linux- und macOS-Geräten installiert ist.

Agent Client Collector -Architektur für Übersicht

Agent Client Collector basiert auf einem Sensu-Framework und wird mit Überwachungsfunktionen für Server, Datenbanken, Anwendungsserver und Middleware installiert. Außerdem wird die Erweiterung der Überwachung durch zusätzliche Prüfungen der Sensu-Community oder Nagios-kompatibler Plugins unterstützt, sodass Sie die Überwachung an Ihre Bedürfnisse anpassen können.

Überwachung mit Prüfungen und Richtlinien

Der Agent führt Prüfungen auf dem Host aus, um relevante Daten zu sammeln und sie in Ereignisse oder Metriken umzuwandeln. Diese Prüfungen sind in ServiceNow definiert und mit Überwachungsrichtlinien verknüpft. Eine Richtlinie ist eine Kombination aus den überwachten Configuration Items (CIs) und den Prüfungen, die für diese CIs ausgeführt werden. Die Prüfungen sind mit Richtlinien verknüpft, um verschiedene Aspekte des Systems zu überwachen.

Sie können Prüfungsinstanzen anpassen, indem Sie z. B. die Häufigkeit anpassen oder Parameter wie Anmeldeinformationen für Datenbanken angeben, ohne die ursprüngliche Prüfungsdefinition zu beeinträchtigen. Die Anpassung einer Prüfinstanz wird nur für die Prüfinstanz wirksam, die der Richtlinie zugeordnet ist, und ändert nicht die globale Prüfdefinition. Diese Anpassung stellt Flexibilität bei der Überwachung verschiedener CIs in verschiedenen Szenarien sicher.

Datenerfassung und -übertragung

Nach der Installation sammelt der Agent Informationen über seinen Host und seine Prozesse. Der Agent pusht die gesammelten Daten über ServiceNow in die Instanz MID-Server. MID-Server dient als Brücke zwischen dem -Agenten und der Instanz ServiceNow und stellt sicher, dass die Daten transformiert und sicher zur Verarbeitung gesendet werden.

Auf der -Instanz werden CIs für den Host und Anwendungen erstellt, die anhand der laufenden Prozesse klassifiziert werden (z. B. MicrosoftMicrosoft Azure Event Hubs SQL Server). Sobald diese CIs erstellt wurden, werden die mit den CIs verknüpften aktiven Überwachungsrichtlinien auf den Agent MID-Serverheruntergeladen, der die Richtlinien dann zur Ausführung an den Agent sendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenspeicherung und -verwendung

Die Ergebnisse der Prüfungen werden in der Instanz ServiceNow gespeichert:

- CI-Daten: CMDB für Konfigurationselemente.
- Ereignisdaten: Ereignistabelle (z. B. Warnungen, die durch Schwellenwertverstöße ausgelöst werden).

Diese Daten können für Überwachung, Warnungen und Berichterstellung genutzt werden. Die Integration gewährleistet Echtzeittransparenz in Bezug auf den Zustand Ihrer Infrastruktur und Anwendungen und ermöglicht gleichzeitig die proaktive Erkennung und Behebung von Problemen.

1. Definieren Sie eine Überwachungsrichtlinie in der Instanz ServiceNow.
2. MID-Server ruft die Prüfinstanzen aus der -Instanz ab und übergibt sie an den -Service Desk-Mitarbeiter.
3. Der Service Desk-Mitarbeiter führt die Prüfungen durch, sammelt Daten und sendet die Ergebnisse zurück an MID-Server.
4. MID-Server sendet die gesammelten Daten an die Instanz ServiceNow, wo sie in der Tabelle CMDB oder der Ereignistabelle gespeichert werden.

Die Befehle und deren Konfigurationen, die für den Agent ausgeführt werden, werden als **Prüfungen** bezeichnet. Im Umfang des Agent sind standardmäßig **Prüfungsdefinitionen** enthalten, die einen bestimmten Befehl und die standardmäßige Häufigkeit festlegen, mit der er ausgeführt wird. Prüfungen werden für die Instanz definiert und über den MID-Server an den Agent übergeben.

Eine **Richtlinie** ist eine Kombination der durch Agent Client Collector überwachten CIs und der Prüfungen, die für diese CIs ausgeführt werden. Sie verknüpfen Prüfungsdefinitionen mit Richtlinien. Diese Prüfungsdefinitionen werden dann als **Prüfungsinstanzen** bezeichnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Prüfungsinstanzen entsprechend Ihren Anforderungen anpassen. Passen Sie beispielsweise das Ausführungsintervall oder die für die Richtlinie spezifischen Parameter an, z. B. die Anmeldeinformationen für den Zugriff auf eine MySQL-Datenbank. Die Anpassung einer Prüfungsinstanz wird nur für die mit der Richtlinie verknüpfte Prüfungsinstanz wirksam, wirkt sich also nicht auf die ursprüngliche Prüfungsdefinition oder bereits erstellte Prüfungsinstanzen in anderen Richtlinien aus.

Agent Client Collector-Plugins

Ein Plugin Agent Client Collector ist ein Skript oder eine Gruppe von Skripts, welche die Fähigkeiten von Agent Client Collectorerweitern. Plugins verbessern die Überwachung, indem sie Metriken sammeln, spezielle Prüfungen durchführen und Ereignisse basierend auf Bedingungen auslösen, z. B. die Überwachung der Warteschlangengröße einer Anwendung, wenn diese 60 % oder 80 % erreicht. Plugins gewährleisten eine skalierbare, anpassbare Überwachung, um sie an sich ändernde Infrastruktur- oder Anwendungsanforderungen anzupassen.

Plugin-check-Abhängigkeit

Plugins sind eng mit Prüfungen in Agent Client Collector Frameworkintegriert. Zwischen dem Plugin und der Prüfung wird eine Abhängigkeit erstellt, um sicherzustellen, dass das Plugin zusammen mit der zugehörigen Prüfung ausgeführt wird.

- Plugin-Abhängigkeit: Ein Plugin kann einer oder mehreren Prüfungen zugeordnet werden und umgekehrt, wobei Prüfungen von mehreren Plugins abhängen können.
- Ausführung: Plugins und Prüfungen werden auf demselben Agent ausgeführt und arbeiten Hand in Hand, um Daten zu sammeln, Spezialaufgaben auszuführen oder die erforderlichen Ereignisse auszulösen

Plugins werden erstellt und verwaltet

Sie können nach Bedarf Plugins Agent Client Collector erstellen, um die Überwachung an Ihre spezifische Umgebung anzupassen. Diese Plugins sind normalerweise als TAR.GZ-Dateien formatiert, die die Skripts enthalten, die die Funktionalität des Plugins definieren.

- Plugin-Erstellung: Anwenderdefinierte Plugins werden entwickelt und in TAR.GZ-Dateien paketiert.
- Integration mit Prüfungen: Nach der Erstellung wird das Plugin in Prüfungen integriert, indem die entsprechenden Abhängigkeiten hergestellt werden. So wird sichergestellt, dass das Plugin und die Prüfung zusammen ausgeführt werden.
- Anpassung: Plugins können an die spezifischen Anforderungen Ihrer Überwachungsanforderungen angepasst werden, unabhängig davon, ob detailliertere Metriken hinzugefügt, Systemschwellenwerte überprüft oder anwenderdefinierte Ereignisse generiert werden sollen.

Vorinstallierte Plugins

Agent Client Collector Framework enthält eine Reihe vorinstallierter Plugins, die grundlegende Funktionen für allgemeine Überwachungsaufgaben bereitstellen, z. B. das Sammeln von Standardmetriken oder die Überwachung wichtiger Systemparameter. Ausführlichere Informationen zu den Plugins, die im Lieferumfang von Agent Client Collector als Teil von ITOM-Integritätenthalten sind, finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Verifizieren Sie die Datenerfassung in Agent Client Collector

Erfassen Sie Daten, indem Sie wichtige Informationen aus dem Hostsystem eines Service Desk-Mitarbeiters erfassen, bevor Sie Prüfungen oder Richtlinien ausführen. Dieser Prozess stellt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

sicher, dass Agent Client Collector über genaue und aktuelle Daten zur -Infrastruktur, den Prozessen und den Anwendungen verfügt, die auf dem -Host ausgeführt werden.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Gesammelte Daten werden als Configuration Item (CI)-Daten gespeichert, die als Grundlage für Überwachung, Warnungen und Metrikdaten in der Instanz ServiceNow® dienen.

Bevor Prüfungen und Richtlinien ausgeführt werden können, sammelt Agent Client Collector Daten zu:

- Hostsystemdetails (z. B. Hardware und Betriebssystemversion des Systems)
- Installierte Anwendungen und Services
- Ausführen von Prozessen
- Metriken zur Ressourcenauslastung (z. B. CPU, Arbeitsspeicher und Festplattenauslastung)

Gesammelte Daten werden in der Instanz ServiceNow entweder in der Tabelle CMDB (Configuration Management Database) oder in der Ereignistabelle gespeichert.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
2. Suchen Sie auf der Seite „Agent Client Collectors“ nach der Spalte **Hostdatensammlung** für einen Agent.
   Ein grünes Gesammelt-Symbol Collected zeigt an, dass die Datenerfassung für den jeweiligen Agent erfolgreich war.

Prüfungen und Richtlinien

Eine Prüfung ist eine Kombination aus einem Befehl und der zugehörigen Konfiguration. Die Prüfung wird auf den Geräten von Agent Client Collectorausgeführt, um Daten von diesen Geräten zu sammeln.

Überprüfungen

Prüfungen werden mit dem Basissystem bereitgestellt. Mit diesen Befehlen werden Skripts ausgeführt, die Überwachungsdaten für Ihre Betriebssysteme und Anwendungen bereitstellen. Der Standardname einer Prüfung gibt den Gegenstand der Überwachung/ Messung, die Entität und die Überwachungsdaten an. Beispielsweise prüft eine Prüfung mit dem Namen *os.linux.check-system-cpu* die CPU-Daten in einem Linux -System. Der in der Prüfung identifizierte Befehl wird auf dem überwachten Gerät ausgeführt und liefert eine Ausgabe und einen Status. Jeder einzelne Scheck wird als **Scheckdefinition**bezeichnet. Nach der Zuordnung zu Richtlinien werden Prüfungsdefinitionen als **Prüfungsinstanzen**bezeichnet.

Sie können Prüfungsinstanzen entsprechend Ihren Anforderungen anpassen. Passen Sie beispielsweise das Ausführungsintervall oder die für die Richtlinie spezifischen Parameter an, z. B. die Anmeldeinformationen für den Zugriff auf eine MySQL-Datenbank. Die Anpassung einer Prüfungsinstanz wird nur für die mit der Richtlinie verknüpfte Prüfungsinstanz wirksam, wirkt sich also nicht auf die ursprüngliche Prüfungsdefinition oder bereits erstellte Prüfungsinstanzen in anderen Richtlinien aus.

Die folgenden Prüfungstypen gehören zum Lieferumfang des Ereignismanagement-Basissystems:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Event**: Das Ergebnis der Prüfung wird in ein Ereignismanagement-Event umgewandelt.
- **Metrik**: Die Werte aus dem Prüfungsergebnis werden in Metriken umgewandelt.

Einzelheiten zu den Standardprüfungen Agent Client Collector Framework finden Sie unter Standardprüfungen des Agent Client Collector-Framework.

Einzelheiten zu den Standardprüfungen und -richtlinien für Agent Client Collector-Überwachung finden Sie unter Agent Client Collector-Überwachung – Standardprüfungen und Richtlinien.

Einzelheiten zu den Standardprüfungen und -richtlinien für Agent Client Collector Visibility – Inhalt finden Sie unter Agent Client Collector Visibility – Inhalt – Standardprüfungen und Richtlinien.

Wenn auf den Geräten des Agent keine Prüfungen ausgeführt werden, befindet sich der Agent möglicherweise im CPU-Schutzmodus. Der CPU-Schutzmodus wird automatisch aktiviert, wenn die CPU-Auslastung eines Geräts zu hoch ist. In diesem Fall lautet der Datenerfassungsstatus des Agent **Aus (automatisch)**. Überprüfen Sie die Agent-Protokolle, um die problematischen Prüfungen zu ermitteln. Sie können problematische Prüfungen manuell deaktivieren, oder Sie können die Schwellenwerte für den CPU-Schutzmodus in der Datei `acc.yml` des Agent ändern und die Datensammlung für den Agent manuell fortsetzen. Details zu den Schwellenwerten für den CPU-Schutzmodus finden Sie unter Agent Client Collector-CPU-Schutzschwellenwerte. Einzelheiten zum manuellen Deaktivieren der Datensammlung finden Sie unter Agent Client Collector-Datensammlung anhalten.

Im Basissystem gibt der Beendigungsstatus des Events wie folgt seinen Schweregrad an:

- 0 = OK
- 1 = WARNUNG
- 2 = KRITISCH

Sie können zusätzliche Schweregrade hinzufügen (z. B. SCHWERWIEGEND und GERINGFÜGIG), indem Sie ein benutzerdefiniertes Skript ausführen. Die folgenden Beendigungsstatus geben diese Schweregrade an:

- 13 = SCHWERWIEGEND
- 14 = GERINGFÜGIG

Berechtigungen zum Ausführen von Prüfbefehlen

Wenn der ServiceNow-Basissystembenutzer keine Berechtigungen zum Ausführen bestimmter Prüfbefehle hat, gehen Sie für die entsprechenden Betriebssysteme wie folgt vor:

- Unter Linux: Erteilen Sie Benutzer servicenow die Berechtigung, den Befehl mit `sudo`-Berechtigungen auszuführen. Stellen Sie sicher, dass die folgenden sudo-Konfigurationsanforderungen erfüllt sind:
  - tty-Anforderungen und Passwortanforderungen deaktiviert
  - Alle Umgebungsvariablen beibehalten
  - Zur Ausführung von Befehlen Unterstützung eines dynamischen PATH

  Beispielkonfiguration in der Datei `/etc/sudoers` :

```
Cmnd_Alias ACC_F = /usr/sbin/dmidecode -s
 baseboard-serial-number, /usr/sbin/dmidecode -s
 chassis-serial-number, /usr/sbin/dmidecode -s
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 system-serial-number, /usr/sbin/dmidecode -s system-uuid, /usr/sbin/ss
 -tanp
servicenow ALL=(root)
 SETENV: /
var/cache/servicenow/agent-client-collector/osquery/bin/osqueryi *,
 ACC_F
Defaults:servicenow !requiretty
Defaults exempt_group += servicenow
```

Hinweis: Befehlspfade können variieren. Einzelheiten zu diesem Thema finden Sie im sudoers-Handbuch.

- Die Zeichenfolge `SETENV:` ermöglicht dem Benutzer servicenow die Beibehaltung von Umgebungsvariablen.
- Durch die Zeichenfolge `!requiretty` wird tty deaktiviert.
- Durch Hinzufügen des Benutzers servicenow zu `exempt_group` werden die Passwortanforderungen umgangen und dynamische PATH-Variablen zur Ausführung von sudo-Befehlen aktiviert.

Stellen Sie sicher, dass Sie in der Prüfungsdefinition im Abschnitt zu den Prüfbefehlparametern den Prüfungsparameter *must_sudo* mit dem Wert **true** konfigurieren.

- In einem macOS -System: Stellen Sie sicher, dass der Benutzer, der den Agent-Service ausführt, zu einer Benutzergruppe mit Berechtigungen zum Abfragen aller TCP-Verbindungen auf dem Host gehört.
- In einem Windows -System: Fügen Sie mithilfe der Anwenderverwaltung Windows den ServiceNow-Anwender den Gruppen mit den entsprechenden Berechtigungen hinzu, damit der Benutzer die erforderlichen Befehle ausführen kann.

Richtlinien

Eine **Richtlinie** ist eine Kombination aus den von Agent Client Collector überwachten CIs und den Prüfungsdefinitionen, die für diese CIs ausgeführt werden.

Damit eine einzelne Richtlinie mehrere Anmeldeinformationen unterstützt, weisen Sie der Richtlinie einen Alias für Anmeldeinformationen zu. Wenn Sie beispielsweise MySQL-Server für Linux und Windows mit unterschiedlichen Anmeldeinformationen haben, müssen Sie für jeden Anmeldeinformationstyp separate Richtlinien erstellen. Wenn Sie jedoch einen Alias für Anmeldeinformationen verwenden, können Sie dem Alias eine einzelne Richtlinie zuweisen. Der Agent ordnet dann die relevanten Anmeldeinformationen der überwachten Anwendung zu. Weitere Informationen zu Aliassen für Anmeldeinformationen finden Sie unter Alias für Verbindungen und Anmeldeinformationen erstellen .

Von Richtlinien mit einer Überprüfung auf Ereignistyp generierte Warnungen werden automatisch geschlossen, wenn die CI-Überwachung aufgrund eines der folgenden Gründe beendet wird:

- Deaktivierung der Richtlinie
- Deaktivierung der Prüfung, die die Warnung verursacht hat
- Löschung der Prüfung aus der Richtlinie
- Löschung der Richtlinie
- Änderung des Richtlinienfilters, der die überwachten CIs bestimmt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sichere Parameter in der Agent Client Collector

Sichere Parameter in Agent Client Collector (ACC) beziehen sich auf die sichere Übergabe sensibler Daten wie Anwendernamen, Passwörter und API-Schlüssel während der Prüfungsausführung, ohne dass die vertraulichen Daten in der Befehlszeile verfügbar gemacht werden. Parameter werden über die Standardeingabe (STDIN) an das Skript übergeben, wodurch sie in Protokollen oder anderen Prozessen ausgeblendet werden, die Befehlszeilenargumente erfassen könnten.

Je nach verwendeter Codierungssprache kann die Implementierung sicherer Parameter variieren. Beispiel: Unter Linux wird in Bash der Befehl *read* (*read <variable_name>*) verwendet, wobei *<variable_name>* durch den in STDIN eingegebenen Wert ersetzt wird.

Sicherer Parameterdatenfluss

1. Sichere Parameter erstellen: Definieren Sie sichere Parameter in der Instanz, die auf Anmeldeinformationen verweisen, die geschützt werden müssen (z. B. Anwendernamen und Passwörter). Details finden Sie unter Sichere Parameter für Prüfungen erstellen.
2. Sichere Parameter konfigurieren: Legen Sie einen **Reihenfolgewert** fest, um die Reihenfolge zu bestimmen, in der Anmeldeinformationen an die Standardeingabe übergeben werden.
3. Anmeldeinformationen übergeben: Übertragen Sie Anmeldeinformationen von MID-Server an den -Agent, je nachdem, welchem Scheck sie zugewiesen sind. Wenn die Prüfung ausgeführt wird, übergibt der Agent die gesicherten Parameter mit STDIN an das Skript in der Reihenfolge, die durch den in der Instanz konfigurierten Wert für die **Reihenfolge** angegeben ist.
4. Prüfung ausführen: Bei der Ausführung senden die Agents die sicheren Parameter über STDIN in der angegebenen Reihenfolge an das Skript.
5. Skript ausführen: Das Skript ruft die sicheren Parameter aus STDIN ab und verwendet sie, um es mit den gesicherten Anmeldeinformationen auszuführen.

Vorteile von sicheren Parametern

- Erhöhte Sicherheit: Die Übergabe vertraulicher Daten wie Anwendernamen und Passwörter direkt in der Befehlszeile stellt eine Sicherheitsbedrohung dar, da sie nicht autorisiertem Zugriff oder böswilligen Anwendern ausgesetzt sein könnten. Sichere Parameter stellen sicher, dass diese Daten sicher verarbeitet und ausgeblendet werden.
- Offenlegung von Daten verhindern: Bei Verwendung sicherer Parameter werden die Anmeldeinformationen in der Befehlszeile nicht im Nur-Text-Format geschrieben, wodurch das Risiko vermieden wird, dass sie in Protokollen oder Prozesslisten erfasst werden.
- Datenflusssteuerung: Sichere Parameter ermöglichen die kontrollierte und anpassbare Übergabe von Anmeldeinformationen an das Skript und stellen so die korrekte Verarbeitung und das richtige Timing vertraulicher Informationen sicher.

Agent Client Collector Konfigurationsdatendateien

Konfigurationsdatendateien speichern dynamische Instanzdaten, z. B. Details der virtuellen Maschine, die Prüfungsdefinitionen während der Ausführung verwenden. Dadurch wird sichergestellt, dass Prüfungen mit aktuellen und genauen Informationen über die überwachte Instanz durchgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Struktur der Konfigurationsdatendateien

- Anhangsbasiert: Eine Konfigurationsdatendatei enthält einen einzelnen Anhang mit Instanzdaten, z. B. Azure VM-Details.
- Synchronisierung: Wenn ein Anhang hinzugefügt oder gelöscht wird, wird die Datendatei für alle MID Servers synchronisiert, die mit Agent Client Collectorkonfiguriert sind. Wenn eine Datei oder ihr Anhang gelöscht wird, wird sie auch aus MID-Serverentfernt.
- Zugriffspunkt: Auf die Konfigurationsdatendateien kann auf MID-Server unter `static/cache/config-files`zugegriffen werden.

Von Konfigurationsdatendateien verwendete Prüfungsdefinitionen

- Prüfungsdefinition: Einzelne Prüfungseinträge werden als Prüfungsdefinitionen bezeichnet. Beispielsweise überprüft *`os.linux.check-system-cpu`* die CPU auf Systemen Linux von .
- Zugriff auf Prüfungsdefinitionen: Auf Prüfungsdefinitionen kann über zugegriffen werden **Alle** > **Agent Client Collector** > **Konfiguration** > **Prüfungsdefinitionen**.

Dateizuordnung

- Downloadprozess: Wenn eine Prüfung ausgeführt wird, lädt der Agent die Konfigurationsdatendatei herunter, die dieser Prüfung zugeordnet ist.
- Domänenspezifische Synchronisierung: Dateien werden nur mit Agents innerhalb derselben Domäne synchronisiert, wodurch eine sichere und lokalisierte Datenverarbeitung gewährleistet wird.

Arbeiten mit Konfigurationsdatendateien

Konfigurationsdatendateien dienen als Repository für dynamische Instanzdaten, die von Prüfungsdefinitionen bei der Ausführung verwendet werden. Diese Dateien stellen sicher, dass Prüfungen mit genauen Echtzeitinformationen zu den überwachten Systemen oder Instanzen ausgeführt werden. Konfigurationsdatendateien funktionieren wie folgt:

- Instanzspezifische Daten speichern: Konfigurationsdatendateien speichern dynamische Instanzdaten, z. B. Details der virtuellen Maschine, Serverkonfigurationen und andere systemspezifische Informationen. Diese Daten werden während der Ausführung von Prüfungsdefinitionen verwendet, um sicherzustellen, dass die neuesten Informationen verfügbar sind.
- Prüfungsdefinitionen erstellen: Eine Prüfungsdefinition wird mit einer zugehörigen Konfigurationsdatendatei erstellt. Beispielsweise kann eine Prüfungsdefinition, die die CPU-Daten eines Systems überwacht, Konfigurationsdaten enthalten, die die Systemumgebung beschreiben, um sicherzustellen, dass für Prüfungen genaue und relevante Instanzdaten verwendet werden.
- Mit MID Serverssynchronisieren: Wenn eine Konfigurationsdatendatei hinzugefügt oder aktualisiert wird, wird sie mit allen MID Servers synchronisiert, die mit Agent Client Collectorkommunizieren. Wenn die Datei oder der Anhang gelöscht wird, wird sie/er auch aus MID Serversentfernt, wodurch die Konsistenz und aktuelle Datenverfügbarkeit sichergestellt wird.
- Mit aktualisierten Daten ausführen: Während der Ausführung lädt der Agent Agent Client Collector die relevante Konfigurationsdatendatei aus dem MID-Serverherunter. Der Service Desk-Mitarbeiter verwendet diese Daten, um die Prüfung auszuführen und so den Zugriff auf die aktuellen und genauesten Instanzinformationen sicherzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Daten speichern und aufrufen: Konfigurationsdatendateien werden im Verzeichnis MID-Server im Verzeichnis „`static/cache/config-files`" gespeichert. Dieser Speicherort erleichtert den Zugriff und die Verwaltung und stellt sicher, dass die für Prüfungen erforderlichen Daten bei Bedarf immer verfügbar sind.

Agent Client Collector Protokolle

Agent Client Collector ACC-Protokolle () spielen eine entscheidende Rolle bei der Überwachung der Aktivität und Leistung des Agent. Protokolle bieten wertvolles Feedback zur Identifizierung potenzieller Probleme, insbesondere wenn die Leistung des Service Desk-Mitarbeiters nicht optimal ist. Indem sie Einblicke in Problembereiche gewähren, sind diese Protokolle für die Fehlersuche und -behebung von entscheidender Bedeutung und verbessern letztendlich die Gesamteffektivität des Agent.

Agent Client Collector ACC-Protokolle () bieten wichtige Vorteile für die Überwachung und Wartung der Leistung von Service Desk-Mitarbeitern.

- Konfigurierbare Schweregrade: Mit Agent Client Collector -Protokollen können Sie die Schweregrade für die Überwachung konfigurieren, einschließlich *`Error`*, *`Debug`*und *`Info`*. Diese Flexibilität hilft, sich auf bestimmte Bereiche zu konzentrieren, z. B. auf die Nachverfolgung von Fehlern oder die Diagnose von Problemen.
- Protokollaufbewahrungsverwaltung: Sie können Protokollaufbewahrungsrichtlinien einrichten, die festlegen, wie oft Protokolle gelöscht werden, um Systemressourcen zu schonen. Dadurch wird sichergestellt, dass die Protokolle verwaltbar bleiben und die Systemleistung nicht beeinträchtigt werden.
- Identifizierung von Leistungsproblemen: Protokolle bieten wertvolle Einblicke, um Bereiche zu identifizieren, in denen der Service Desk-Mitarbeiter möglicherweise Probleme hat, und tragen so zur Verbesserung der Leistung des Service Desk-Mitarbeiters bei.

Einzelheiten zum Auffinden und Verwalten von Agent Client Collector -Protokollen finden Sie unter Agent Client Collector-Protokolle anzeigen.

Agent Client Collector-API

Verwenden Sie die API Agent Client Collector (ACC), um einen Flow zu erstellen, der einen `osquery` -Befehl auf Agents ausführt und die Ergebnisse verarbeitet. Mithilfe der ACC-API können Sie die Abfrage von Agent-Daten automatisieren und die Verarbeitung der Ergebnisse optimieren. Dadurch lässt sich die Systemleistung leichter überwachen und verwalten.

Das System unterstützt OSQuery 5.7.0 und bietet Kompatibilität mit einer Reihe von Abfragen für eine effiziente Datenerfassung.

Die ACC-API ermöglicht die nahtlose Integration und Automatisierung der Ausführung von Abfragen und der Verwaltung von Service Desk-Mitarbeitern. So funktioniert es:

1. osquery-Befehle ausführen: Sie können die ACC-API verwenden, um osquery-Befehle an Service Desk-Mitarbeiter zu senden. Diese Befehle erfassen eine Vielzahl von System- und Leistungsdaten von den Zielcomputern.
2. Ergebnisse verarbeiten: Nachdem der Befehl osquery auf den Agents ausgeführt wurde, verarbeitet die ACC-API die Ergebnisse und gibt die erforderlichen Daten zurück. Diese Daten können zu Überwachungs-, Problembehandlungs- oder Berichterstellungszwecken verwendet werden.
3. Unterstützung für osquery 5.7.0: Die ACC-API ist mit osquery 5.7.0 kompatibel. Dadurch wird sichergestellt, dass sie die neuesten Funktionen und Verbesserungen unterstützt, sodass Sie erweiterte Abfragefunktionen für die erweiterte Datenerfassung nutzen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. API-Funktionen aktivieren: Um die ACC-API zu verwenden, aktivieren Sie die Agent- und Richtlinien-APIs. Auf diese Weise können Sie verschiedene Aspekte Ihrer Agents konfigurieren und verwalten, einschließlich Kommunikation, Datenerfassung und Abfrageausführung.

Weitere Informationen zu Agent-APIs finden Sie unter Agent-APIs aktivieren .

Weitere Informationen zum Aktivieren von Richtlinien-APIs finden Sie unter Richtlinien-APIs aktivieren .

Agent Client Collector Integritätsscan-Suite für Instanzen

Die Scan-Suite für Integritätsinstanzen Agent Client Collector (ACC) besteht aus Prüfungen, die Anomalien und andere Probleme erkennen, die in Ihrer Instanz auftreten können. Diese Prüfungen sollen den allgemeinen Zustand und die Leistung von ACC sicherstellen und potenzielle Probleme proaktiv identifizieren, bevor sie sich auf den Systembetrieb auswirken.

Die Instanz-Scan-Suite für die ACC-Integrität besteht aus den folgenden Prüfungen.

Prüfungen der ACC Health Instance Scan Suite

Name überprüfen	Beschreibung
ACC-Duplikat-Agent für Host-CI	Identifiziert Configuration Items (CIs), die mehreren aktiven Service Desk-Mitarbeitern zugeordnet sind, und weist auf potenzielle Probleme bei der CI-Identifizierung hin. Erfordert den Import von `global.ACCInstanceScanUtil` für Instanzen, die dem Release Xanadu oder früher zugeordnet sind.
ACC-Fehler-Framework	Überprüft, ob „ACCErrorManager“ erstellt wurde, wodurch der entsprechenden bereichsbezogenen ACC-App Fehler zugeordnet werden können. Erkennt, ob eine Automatisierungsquellanwendung, eine Automatisierungsfehlerkategorie und ein Automatisierungsfehlercode für die Anwendung Agent Client Collector Framework vorhanden sind.
ACC – nach geänderten Skripteinbindungen suchen	Erkennt modifizierte Agent Client Collector Framework -Skripteinbindungen, die nach dem Upgrade möglicherweise geändert wurden. Erfordert den Import von `global.ACCInstanceScanUtil` für Instanzen, die dem Release Xanadu oder früher zugeordnet sind.
ACC hat Upgrades übersprungen	Meldet Upgrades, die seit dem letzten Upgrade übersprungen wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfungen der ACC Health Instance Scan Suite (Fortsetzung)

Name überprüfen	Beschreibung
	Erfordert den Import von `global.ACCInstanceScanUtil` für Instanzen, die dem Release Xanadu oder früher zugeordnet sind.
ACC verifiziert die Ordnerhierarchie des Plugins	Validiert die korrekte Erstellung von ACC-Plugin-Ordnern und markiert doppelte Ordner, die Synchronisierungsprobleme verursachen können.
ACC – Anzahl aktiver Richtlinien	Zählt die Anzahl der aktiven veröffentlichten Richtlinien und empfiehlt, wenn die Zahl über 300 liegt, Richtlinienkonsolidierung, um die Leistung zu verbessern.
ACC – Verbindung zwischen Agent und MID	Überprüft die Verbindung von 1.000 Agents pro 1 GB Java Virtual Machine (JVM), um sicherzustellen, dass MID-Server nicht überlastet wird. Bei Überlastung zusätzliche JVMs konfigurieren oder Agents auf andere MID Serversverteilen.
ACC verifiziert die Übereinstimmung der CI-Anzahl „sn_agent“.	Stellt sicher, dass die Datensätze in den Tabellen „sn_agent_ci_extended_info“ und „sn_agent_cmdb_ci_agent“ übereinstimmen, wodurch die Datenkonsistenz für Service Desk-Mitarbeiter sichergestellt wird.

Weitere Informationen zum Importieren der Skripteinbindung `global.ACCInstanceScanUtil` finden Sie im Artikel Skripteinbindung ACCInstanceScanUtil [KB1630132] in der Now Support Knowledge Base.

Weitere Informationen zu Instanzscans finden Sie unter Instance Scan .

Einzelheiten zur Ausführung der Instanzscan-Suite für Integrität Agent Client Collector finden Sie unter Führen Sie einen Suite-Scan aus .

Domain Separation und Agent Client Collector

Domänentrennung wird für Agent Client Collector (ACC) unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

So funktioniert Domain Separation in Agent Client Collector

Die Domänentrennung in ACC ermöglicht die Isolierung von Daten, die von Agent Client Collector erfasst wurden, in einer bestimmten Domäne. Daher können nur Benutzer innerhalb dieser Domäne auf diese Daten zugreifen und sie anzeigen. In ähnlicher Weise sind Agents und die zugehörigen Konfigurationen an bestimmte Domänen gebunden, um sicherzustellen, dass sich Vorgänge innerhalb einer Domäne nicht auf andere auswirken oder an sie weitergegeben werden. Dadurch entsteht eine organisiertere und sicherere Umgebung für die Verwaltung mehrerer Gruppen, Geschäftsbereiche oder Regionen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Datensicherheit und Datenschutz: Die Beschränkung des Datenzugriffs basierend auf Domänen reduziert das Risiko von nicht autorisiertem Zugriff und domänenübergreifendem Datenverlust und stellt sicher, dass vertrauliche Informationen innerhalb der festgelegten Domäne bleiben.
- Zugriffskontrolle: Durch die Isolierung von Domänen können Organisationen strenge Zugriffskontrollen erzwingen, sodass nur bestimmte Benutzer oder Teams die für ihre Domäne relevanten Daten anzeigen oder mit ihnen interagieren können.

Anwendungsfälle für Domain Separation in Agent Client Collector

- Abteilungsübergreifende Zusammenarbeit mit Datenisolierung: IT- und Finanzabteilungen können ihre jeweiligen Systeme unabhängig voneinander ohne Datenüberschneidungen überwachen. Wenn beispielsweise ein Problem mit einem Server im Zahlungsverarbeitungssystem auftritt, kann die Finanzabteilung in ihrer Domäne bestimmte Prüfungen ohne Eingreifen der IT-Abteilung ausführen.
- Regulatorische Compliance: Domain Separation hilft bei der Einhaltung von Vorschriften wie DSGVO oder SOX, indem sichergestellt wird, dass nur autorisiertes Personal auf vertrauliche Daten zugreifen kann. Beispielsweise kann die Compliance-Abteilung regulatorische Prüfungen überwachen, während der Zugriff auf IT-Infrastrukturdaten eingeschränkt ist.
- Incident-Management und Problembehandlung: Die IT kann Netzwerkprobleme beheben, während die Finanzabteilung die Transaktionssysteme überwacht. Durch die Domänentrennung können beide Abteilungen unabhängig voneinander arbeiten, was eine schnellere Lösung ermöglicht und die Offenlegung von Daten verhindert.

Zugehörige Informationen

Domänentrennung für Service Provider

Anwendungsfall: Optimierung der Datenisolierung und -überwachung durch Domain Separation

Die Optimierung der Datenisolierung und -überwachung mit Domain Separation stellt sicher, dass Finanzinstitute vertrauliche Informationen schützen, die betriebliche Effizienz verbessern und die Compliance durch sichere Trennung von Abteilungsdaten gewährleisten.

Übersicht über Anwendungsfälle

In einem großen Finanzinstitut müssen Abteilungen wie IT, Finanzen, Compliance und HR ihre Systeme unabhängig voneinander verwalten und gleichzeitig vertrauliche Daten schützen. Agent Client Collector (ACC) sammelt Daten von verschiedenen Agents auf Servern und Geräten, und Domain Separation stellt sicher, dass die Daten jeder Abteilung sicher isoliert sind. Dadurch können Abteilungen ihre eigene Überwachung, Problembehandlung und Berichterstellung verwalten, wodurch das Risiko von domänenübergreifenden Interferenzen oder nicht autorisiertem Zugriff erheblich reduziert wird.

Herausforderungen ohne Domain Separation

- Datenschutz- und Sicherheitsrisiken: Sensible Daten könnten nicht autorisierten Anwendern zugänglich sein. Beispielsweise könnten IT-Mitarbeiter versehentlich auf Finanz- oder Gehaltsabrechnungsdaten zugreifen und dadurch Datenschutzrichtlinien verletzen.
- Operative Ineffizienz: Abteilungen müssen Konfigurationen gemeinsam nutzen, was die Verwaltung und Behebung von Problemen erschwert und zu Verwirrung und Ineffizienzen führt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Compliance-Probleme: Die Erfüllung der gesetzlichen Anforderungen für die Datenisolierung wäre schwierig, was zu Compliance-Verstößen führen würde.
- Erhöhtes Risiko der Datenbeschädigung: Gemeinsam genutzte Umgebungen können zu unbeabsichtigten Datenbeschädigungen führen, da Changes in einer Abteilung sich auf andere auswirken können.

Lösung

- Datenisolierung: Jede Abteilung verfügt über eine dedizierte Domäne, wodurch sichergestellt wird, dass von Mitarbeitern gesammelte Daten nur innerhalb dieser Domäne zugänglich sind.
- Unabhängige Konfiguration und Überwachung: Abteilungen legen ihre eigenen Prüfungen, Richtlinien und Aufgaben fest, ohne andere zu beeinträchtigen.
- Zugriffssteuerung: Die rollenbasierte Zugriffssteuerung (RBAC) schränkt den Zugriff der Benutzer auf Daten innerhalb ihrer Domäne ein. Beispielsweise kann die IT nur auf Infrastrukturdaten zugreifen, während die Finanzabteilung nur auf Finanztransaktionsdaten zugreifen kann.
- Erhöhte Sicherheit: Domain Separation stellt sicher, dass Benutzer in einer Abteilung nicht auf Daten aus anderen Abteilungen zugreifen können, wodurch das Risiko eines nicht autorisierten Zugriffs reduziert wird.

Ergebnis

- Verbesserte Datensicherheit: Sensible Daten werden geschützt, wodurch das Risiko nicht autorisierter Zugriffe reduziert wird.
- Operative Effizienz: Abteilungen arbeiten unabhängig voneinander und verwalten Konfigurationen und überwachen konfliktfrei.
- Regulatorische Compliance: Einfachere Einhaltung von Datenschutzbestimmungen (GDPR, SOX) durch sichere Datentrennung.
- Weniger Datenbeschädigung: Isolierte Umgebungen verhindern unbeabsichtigte abteilungsübergreifende Auswirkungen und verbessern die Systemstabilität.

Anwendungsfall: Regulatorische Compliance in einer Finanzdienstleistungslösung

Ein Finanzinstitut muss sicherstellen, dass auf seine Daten nur diejenigen Abteilungen zugreifen können, die für die angegebenen Daten autorisiert sind.

Herausforderung

Das Finanzinstitut muss Vorschriften einhalten, die eine strikte Datentrennung zwischen Abteilungen (z. B. HR, IT oder Finanzen) vorschreiben.

Lösung

1. Erstellen Sie separate Domänen für jede Abteilung (IT, Finanzen, HR, Compliance usw.) in der Konfiguration Agent Client Collector (ACC).
2. Wenden Sie Zugriffssteuerungen an, sodass vertrauliche Daten (z. B. Mitarbeiterdatensätze und Finanztransaktionen) nur für autorisierte Abteilungen zugänglich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Verwenden Sie ACC-Integritätsprüfungen, um sicherzustellen, dass die Datentrennung gewahrt wird, insbesondere beim Aktualisieren oder Behandeln von Systemen.
4. Überprüfen Sie die Einstellungen für Domain Separation regelmäßig, um die Compliance mit Datenschutzbestimmungen wie DSGVO, SOX oder PCI-DSS sicherzustellen.

Ergebnis

Die Einhaltung rechtlicher und behördlicher Anforderungen wird sichergestellt, und vertrauliche Daten werden vor nicht autorisiertem Zugriff geschützt.

Agent Client Collector Framework konfigurieren

Planen und konfigurieren Sie Ihre Agent Client Collector Framework-Implementierung.

Agent Client Collector Framework Die -Konfiguration folgt normalerweise den folgenden Schritten:

1. Konfigurieren Sie einen Agent-Registrierungsschlüssel.
2. Websocket-Server auf MID-Server installieren.
3. Websocket-Endpunkt konfigurieren.
4. Häufigkeit der Aktualisierung der Liste der MID-Server für Agents konfigurieren.
5. Agent Client Collector -Plugins erstellen und bearbeiten.
6. Agent Client Collector zur Massenbereitstellung in benutzerdefiniertes Basis-Image einbinden.
7. Installieren Sie Agent Client Collector.

   Das zu befolgende Installationsverfahren hängt vom Betriebssystem ab, unter dem Sie die Installation durchführen (Linux, Windowsoder macOS).
8. Agent Client Collector Monitoring auf dem MID-Server aktivieren.
9. Optimieren Sie die Verteilung von Service Desk-Mitarbeitern auf MID Servers.
10. Agent Client Collector-Konfigurationsdateien für Agents anzeigen.
11. Erstellen Sie eine Agent Client Collector Konfigurationsdatendatei.
12. Aktualisieren Sie Agent Client Collector Zertifikate manuell.
13. Aktivieren Sie die sichere OpenSSL-Signierung für -Plugins.
14. Führen Sie die Korrektur Zscaler durch.

Konfigurieren Sie einen Agent-Registrierungsschlüssel

Konfigurieren Sie einen Agent-Registrierungsschlüssel, damit Sie Agent Client Collector mithilfe von ITOM Cloud Services bereitstellen können. Mit ITOM Cloud Services können Sie Agent Client Collector ohne MID-Serverbereitstellen und so MID-Server für persistentere Ressourcen speichern.

Vorbereitungen
Installieren Sie die für ITOM Cloud Services erforderlichen Plugins wie in Installation von Agent Client Collectorbeschrieben.

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die geplante Aufgabe „Agent-Registrierungsschlüssel bereinigen“ wird täglich ausgeführt, wobei abgelaufene Registrierungsschlüssel gelöscht werden. Die Dauer, für die ein Registrierungsschlüssel gültig ist, wird durch die Eigenschaft *sn_agent.registration_key_validity.days* gesteuert, je nachdem, wann der Schlüssel erstellt wurde. Wie lange der Kunde vor dem bevorstehenden Ablauf des Schlüssels benachrichtigt wird, wird durch die Eigenschaft *sn_agent.registration_key_notification.days* gesteuert. Einzelheiten zu diesen Eigenschaften finden Sie unter Agent Client Collector Framework Konfigurationseigenschaften.

Wenn das Ablaufdatum eines Schlüssels näher rückt, erstellen Sie einen neuen Registrierungsschlüssel, und geben Sie ihn in vorhandene Automatisierungsaufgaben ein, um einen Registrierungsausfall zu verhindern.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agent-Registrierungsschlüssel**.
2. Wählen Sie **Neu**.
3. Geben Sie im Feld **Name** einen beschreibenden Namen für den Registrierungsschlüssel ein.
4. Wahlweise: Um Benachrichtigungen zu erhalten, wenn ein Registrierungsschlüssel bald abläuft, wählen Sie im Feld **Besitzgruppe** eine Gruppe mit einer gültigen E-Mail-Adresse aus.
5. Wählen Sie **Absenden**.

Ergebnisse

Der neue Agent-Registrierungsschlüssel kann jetzt für die Installation verwendet werden.

Websocket-Server auf MID-Server installieren

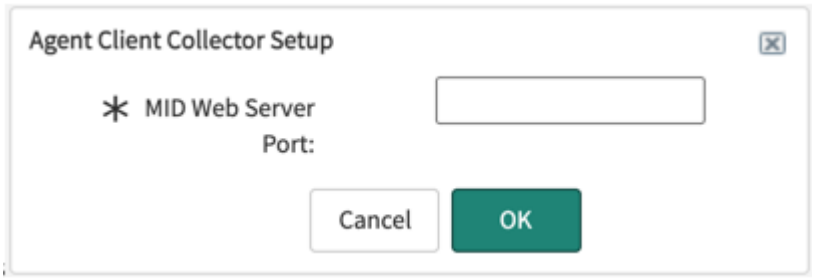
Konfigurieren Sie den Websocket-Server auf MID Servers, um Verbindungen von Agents mit MID-Serverzu ermöglichen. Sie können nur einen Websocket-Server pro MID-Serverkonfigurieren.

Vorbereitungen

- Stellen Sie sicher, dass Sie „curl“ (oder eine ähnliche Software) herunterladen und auf Ihrem Windows-Computer MID-Server installieren.
- Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Server**.
2. Wählen Sie den Namen des relevanten MID-Server aus.
3. Klicken Sie im Abschnitt **Zugehörige Links** auf **Setup ACC Listener** (ACC-Listener einrichten). Das Dialogfeld **Agent Client Collector Setup (Setup von Agent Client Collector)** wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Geben Sie den MID-Webserverport (**8800**) in das angezeigte Feld ein.

   Hinweis: Sie können den Standardport **8800**nach Bedarf ändern.

   - Um die sichere TLS-Konfiguration aufzurufen, führen Sie folgenden Befehl aus: `wss://<mid_ip>:<websocket_port>/ws/events`.
   - Um die TLS 1.3-Unterstützung für MID-Webserverzu aktivieren, legen Sie in der Datei `„wrapper-override.conf“` für MID-Serverden folgenden Parameter fest: `-Djdk.tls.server.protocols="TLSv1.3"`
   - In einer Linux -Umgebung können Portnummern unter 1024 nur mit Superuser-Rechten verwendet werden.

5. Klicken Sie auf **OK**.
   Eine Bestätigungsmeldung mit der URL für die Agent-Konfigurationsdatei wird angezeigt.

   Der Webserver und die Websocket-Erweiterung werden für MID-Serverkonfiguriert. Um die Konfiguration zu überprüfen, navigieren Sie zu den folgenden Menüoptionen:

   - **Agent Client Collector** > **MID-Webserver**. Wenn Sie die Felder im resultierenden Formular bearbeiten, müssen Sie die MID-Webservererweiterung neu starten, damit Ihre Änderungen gespeichert werden.
   - **Agent Client Collector** > **Websocket-Endpunkt**

6. Überprüfen Sie die Gültigkeit des Websocket mit curl:

   a. Geben Sie in ein cmd- oder Terminal-Fenster folgenden Befehl ein: *`curl -Lk -H "Authorization: Key <API_KEY>" https://<mid_server_address>:<port>/api/mid/mon`*.

   b. Stellen Sie sicher, dass Sie eine gültige JSON-Antwort (und keine Fehlermeldung) erhalten, z. B.:

JSON-Skript bei erfolgreicher Installation


```
{
  "uptime" : "53d 23h 50m 3s",
  "memory" : "used 127MB, total 503MB",
  "connectedAgentsNum" : 1,
  "interactiveResultQueueSize" : "0",
  "nonInteractiveResultQueueSize" : "0",
  "policiesNum" : 3,
  "allChecksNum" : 3,
  "eventsRate" : "MIN: 0.00(0), HOUR: 0.00(0), DAY: 0.00(0)",
  "metricRate" : "MIN: 0.00(0), HOUR: 0.00(0), DAY: 0.00(0)",
  "connectedAgents" : [ {
    "client" : {
      "name" : "10-196-39-193-new",
      "address" : "[redacted]",
      "agent_id" : "d56aa0470b49bfd6",
      "version" : "2.1.9",
      "timestamp" : 1602838990267,
      "isWindows" : false,
      "silent_mode" : false,
      "checkTimeout" : 120
    },
    "metricsRate" : "MIN: 0.00(0), HOUR: 0.00(0), DAY: 0.00(0)"
  } ]
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Websocket-Endpunkt konfigurieren

Konfigurieren Sie einen Websocket-Endpunkt, um Webzugriff von MID-Server auf Agent Client Collector (ACC) bereitzustellen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Stellen Sie für zusätzliche Sicherheit sicher, dass MID Servers, die für Agent Client Collector bereitgestellt werden, nicht für andere Komponenten bereitgestellt werden.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **MID-Server**.
2. Wählen Sie einen MID-Server.
3. Wählen Sie die Registerkarte **ACC-Websocket-Endpunkte** unten auf der Seite aus.
4. Wählen Sie **Neu**.
5. Konfigurieren Sie die Felder auf der Seite.

ACC-Websocket-Endpunktseite

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen für den Websocket-Endpunkt ein.
MID-Server	Der Name des ausgewählten MID-Server.
Kurzbeschreibung	Geben Sie optional eine Kurzbeschreibung für den Websocket-Endpunkt ein.
Zugängliche IP-Adresse	Wenden Sie eine externe/öffentliche IP an, wenn MID-Server über eine interne IP verfügt, auf die nicht von einem Agent aus zugegriffen werden kann. Wird für Cloud-Lösungen mit einem Agent verwendet, der nur Zugriff auf die öffentliche IP von MID-Serverhat. Wenn sich MID-Server und alle -Agents in derselben Virtual Private Cloud (VPC) befinden, kann dieses Feld leer gelassen werden.

6. Wählen Sie im Abschnitt „ **Zugehörige Links“Start**, um den Websocket-Endpunkt zu aktivieren.

Häufigkeit der Aktualisierung der Liste der MID-Server für Agents konfigurieren

Standardmäßig wird die Liste der mit Agents verbundenen MID Server einmal täglich aktualisiert. In einer dynamischen Umgebung, in der häufig MID Server hinzugefügt werden, empfiehlt es sich, häufigere Aktualisierungen zu planen oder den Aktualisierungsauftrag bei Bedarf auszuführen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

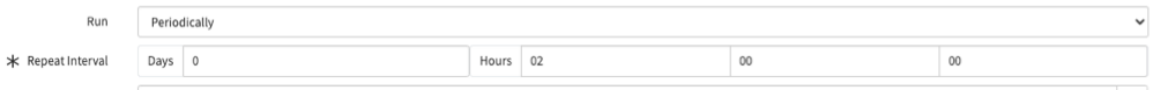
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Systemdefinition** > **Geplante Aufgaben**.
2. Suchen Sie den Auftrag **Update MID Server list for All Agents** (MID Server-Liste für alle Agents aktualisieren).
3. Um den Auftrag sofort auszuführen, klicken Sie auf **Jetzt ausführen**.
4. So bearbeiten Sie die Häufigkeit, mit der der Auftrag ausgeführt wird:

   a. Wählen Sie im Feld **Execute** (Ausführen) die Option **Periodically** (Regelmäßig) aus. Das Feld **Repeat Interval** (Wiederholungsintervall) wird angezeigt.

   Feld „Repeat interval“ (Wiederholungsintervall)

   b. Konfigurieren Sie die Häufigkeit, mit der der Auftrag ausgeführt werden soll. Die Zellen neben der Zelle **Hours** (Stunden) stellen Minuten bzw. Sekunden dar.

   c. Klicken Sie auf **Aktualisieren**, um die Auftragshäufigkeit zu aktualisieren.

Agent Client Collector wird mit ITOM Cloud Services installiert

Wenn Sie Agent Client Collector mit dem Cloud-Service (ICS) ITOM installieren, können Sie den Agent ohne MID-Serverausführen. Mit ICS können Sie MID-Server für persistentere Ressourcen verwenden.

Bevor Sie Agent Client Collector mit ICS verwenden, gehen Sie wie folgt vor:

1. Stellen Sie sicher, dass Ihre Instanz ServiceNow von einem F5-Lastenausgleichsmodul zu Application Delivery Controller, Version 2 (ADCv2) migriert wurde und mTLS-Unterstützung bietet.

   a. Navigieren Sie zu<instance_url> `/adcv2/server`

   - Wenn ein Servername angezeigt wird, befindet sich die Instanz auf ADCv2.
   - Wenn die Seite nicht gefunden oder umgeleitet wird, befindet sich die Instanz nicht unter ADCv2. Verwenden Sie das Automatisierungstool für die F5-zu-ADCv2-Migration, um zu ADCv2 zu migrieren. Weitere Informationen finden Sie im Artikel How to use F5 to ADCv2 Migration [KB0863990] (Verwendung der F5-zu-ADCv2-Migration) in der Now Support Knowledge Base.

   b. Navigieren Sie zu<instance_url> `/adcv2/supports_tls`

   Wenn die URL den Wert **true**zurückgibt, wird mTLS unterstützt.

2. Installieren Sie das Plugin für die bereichsbezogene App ITOM Cloud Services Core (sn_itom_cloud_svc).

   Vergewissern Sie sich, dass Sie über ein Abonnement ITOM für ITOM Operator Professional verfügen, um die Installation des bereichsbezogenen App-Plugins ITOM Cloud Services Core (sn_itom_cloud_svc) zu aktivieren.

   Wenn Sie Agent Client Collector Visibility – Inhaltverwenden, installieren Sie das Plugin Agent Client Collector Visibility – Inhalt (sn_acc_vis_content).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installieren Sie Agent Client Collector mit ITOM Cloud Services in einer Umgebung Windows von [].

Installieren Sie Agent Client Collector auf einem Computer Windows des Typs ohne MID-Server mithilfe von ITOM Cloud Services (ICS). Mit ICS können Sie MID-Server für persistentere Ressourcen verwenden.

Vorbereitungen
Installieren Sie das Plugin ITOM „ Cloud Services Core (sn_itom_cloud_svc).

Konfigurieren Sie einen Agent-Registrierungsschlüssel. Details finden Sie unter Konfigurieren Sie einen Agent-Registrierungsschlüssel.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zur Arbeit mit ICS finden Sie unter DEX-Architektur .

Prozedur
1. Rufen Sie die öffentlich zugängliche Gateway-URL basierend auf Ihrem Standort ab.
   - AMER (Amerika): `itomcnc-prod-gateway.amer.sncapps.service-now.com:443`
   - EMEA (Europa): `itomcnc-prod-gateway.emea.sncapps.service-now.com:443`
   - APAC (Asien-Pazifik): `itomcnc-prod-gateway.apac.sncapps.service-now.com:443`
2. Geben Sie auf dem Server Windows, auf dem der Agent installiert ist, den folgenden Befehl ein:

```
msiexec /i <msi_file_path> /quiet /qn /norestart
 CONNECT_WITHOUT_MID="true" ACC_CNC="<gateway_endpoint>"
 REGISTRATION_KEY="<registration_key>"
 INSTANCE_URL="https://<instance_url>"
```

   Einzelheiten zu den Parameterwerten im Befehl finden Sie unter Agent Client Collector Parameter des Installationsbefehls bei Verwendung von ITOM Cloud-Services.

Installieren Sie Agent Client Collector mit dem Cloud-Service ITOM in einer Umgebung Linux von [].

Installieren Sie Agent Client Collector auf einem Computer Linux des Typs ohne MID-Server mithilfe von ITOM Cloud Services (ICS). Mit ICS können Sie MID-Server für persistentere Ressourcen verwenden.

Vorbereitungen
Installieren Sie das Plugin ITOM „ Cloud Services Core (sn_itom_cloud_svc).

Konfigurieren Sie einen Agent-Registrierungsschlüssel. Details finden Sie unter Konfigurieren Sie einen Agent-Registrierungsschlüssel.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zur Arbeit mit ICS finden Sie unter DEX-Architektur .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Agent-Registrierungsschlüssel abrufen:
   a. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agent-Registrierungsschlüssel**.
   b. Wählen Sie den entsprechenden Agent-Registrierungsschlüssel aus.
   c. Kopieren Sie den Wert des Registrierungsschlüssels, und speichern Sie ihn an einem Ort, an dem Sie ihn bei Bedarf leicht abrufen können.
2. Rufen Sie die öffentlich zugängliche Gateway-URL basierend auf Ihrem Standort ab.
   - AMER (Amerika): `itomcnc-prod-gateway.amer.sncapps.service-now.com:443`
   - EMEA (Europa): `itomcnc-prod-gateway.emea.sncapps.service-now.com:443`
   - APAC (Asien-Pazifik): `itomcnc-prod-gateway.apac.sncapps.service-now.com:443`
3. Geben Sie auf dem Server Linux, auf dem der Agent installiert ist, den folgenden Befehl ein:

```
CONNECT_WITHOUT_MID="true" ACC_CNC="<gateway_endpoint>"
 REGISTRATION_KEY="<registration_key>"
 INSTANCE_URL="https://<instance_url>" bash -c "$(curl -L
 https://<instance_url>/api/sn_agent/agents/install_agent)"
```

Einzelheiten zu den Parameterwerten im Befehl finden Sie unter Agent Client Collector Parameter des Installationsbefehls bei Verwendung von ITOM Cloud-Services.

Installieren Sie Agent Client Collector mit dem Cloud-Service ITOM in einer Umgebung macOS von [].

Installieren Sie Agent Client Collector auf einem Computer macOS des Typs ohne MID-Server mithilfe von ITOM Cloud Services (ICS). Mit ICS können Sie MID-Server für persistentere Ressourcen verwenden.

Vorbereitungen

Installieren Sie das Plugin ITOM „ Cloud Services Core (sn_itom_cloud_svc).

Konfigurieren Sie einen Agent-Registrierungsschlüssel. Details finden Sie unter Konfigurieren Sie einen Agent-Registrierungsschlüssel.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zur Arbeit mit (ICS) finden Sie unter DEX-Architektur .

Prozedur

1. Agent-Registrierungsschlüssel abrufen:
   a. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agent-Registrierungsschlüssel**.
   b. Wählen Sie den entsprechenden Agent-Registrierungsschlüssel aus.
   c. Kopieren Sie den Wert des Registrierungsschlüssels, und speichern Sie ihn an einem Ort, an dem Sie ihn bei Bedarf leicht abrufen können.
2. Rufen Sie die öffentlich zugängliche Gateway-URL basierend auf Ihrem Standort ab.
   - AMER (Amerika): `itomcnc-prod-gateway.amer.sncapps.service-now.com:443`
   - EMEA (Europa): `itomcnc-prod-gateway.emea.sncapps.service-now.com:443`
   - APAC (Asien-Pazifik): `itomcnc-prod-gateway.apac.sncapps.service-now.com:443`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Geben Sie auf dem Server macOS, auf dem der Agent installiert ist, den folgenden Befehl ein:

```
CONNECT_WITHOUT_MID="true" ACC_CNC="<gateway_endpoint>"
 REGISTRATION_KEY="<registration_key>"
 INSTANCE_URL="https://<instance_url>" bash -c "$(curl -L
 https://<instance_url>/api/sn_agent/agents/install_agent)"
```

Einzelheiten zu den Parameterwerten im Befehl finden Sie unter Agent Client Collector Parameter des Installationsbefehls bei Verwendung von ITOM Cloud-Services.

Agent Client Collector -Plugins erstellen und bearbeiten

Je nach Bedarf können Sie die Standard-Plugins bearbeiten oder neue Plugins hinzufügen. Durch das Erstellen und Bearbeiten von Plugins werden die Überwachungsfunktionen von Agent Client Collector angepasst.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **ACC-Plugins**.
2. Klicken Sie auf **Neu**.
   Die Seite **Agent Client Collector Plugin - New record** (Agent Client Collector-Plugin - Neuer Datensatz) wird angezeigt.
3. Geben Sie Werte in die Felder auf der Seite ein, wie in der folgenden Tabelle beschrieben.

Plugin-Felder für Agent Client Collector

Feld	Beschreibung
Name	Name des Plugin. Dieses Feld wird automatisch mit dem Namen der an das Plugin angehängten tar.gz-Datei gefüllt und wird nur angezeigt, wenn ein vorhandener Datensatz ausgewählt wird.
Beschreibung	Beschreibung des Plugin
Betriebssystem	Wählen Sie das Betriebssystem aus, das vom Plugin überwacht werden soll.
Plattform	Wählen Sie die Plattform aus, die vom Plugin überwacht werden soll.
Aktiv	Hierüber aktivieren Sie das Plugin und laden es auf den MID Server herunter.
Erweitert	Duch Aktivierung dieses Kontrollkästchens ermöglichen Sie die Auswahl der vom Plugin zu überwachenden Version des Betriebssystems.
BS-Version	Wählen Sie die Betriebssystemversion aus, die mit dem Plugin überwacht werden soll. Dieses Feld ist nur verfügbar, wenn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	das Kontrollkästchen **Advanced** (Erweitert) aktiviert ist.

4. Folgen Sie den Anweisungen auf der UI-Seite, um eine `tar.gz`-Datei an den Plugin-Datensatz anzuhängen.

Benutzerdefiniertes Plugin mit Zertifikat schützen

Wenn Sie ein Agent Client Collector -Plugin anpassen oder erstellen, können Sie das Plugin entweder mit einem Zertifikat einer Drittpartei oder einem internen sicheren Zertifikat im Skript des Plugins sichern. Offizielle Plugins werden von einer externen Zertifizierungsstelle signiert.

Standardmäßig ist die Verwendung eines selbstsignierten Zertifikats aktiviert. Um diese Funktion zu deaktivieren, legen Sie die Eigenschaft *`verify-plugin-signature`* auf **False** fest. Wenn Sie ein selbstsigniertes Zertifikat deaktivieren, verwenden Ihre konfigurierten Plugins kein Zertifikat.

Einzelheiten zur Konfiguration eines selbstsignierten Zertifikats mit OpenSSL finden Sie unter Aktivieren Sie die sichere OpenSSL-Signierung für -Plugins. Einzelheiten zur Konfiguration von Drittparteizertifikaten finden Sie in der Dokumentation des Drittanbieters.

Wenn die aktuellen Zertifikate des -Agents ein Plugin nicht validieren können, fordert Agent Client Collector die aktualisierten Zertifikate von seinem synchronisierten MID-Serveran. Sie können den Agent manuell aktualisieren, um diese Zertifikate vor der geplanten Synchronisierung zu erhalten. Details finden Sie unter Aktualisieren Sie Agent Client Collector Zertifikate manuell.

Sie können die Zertifikate manuell in einem Verzeichnis auf dem MID-Server speichern, das mit den installierten Agents verbunden ist. Jeder -Agent, der in Ihrer -Umgebung installiert ist, kann dann über MID-Serverauf die Zertifikate zugreifen.

Einzelheiten zur Konfiguration der Eigenschaften für die Zertifikatsynchronisierung finden Sie unter Synchronisierungseigenschaften zum Validieren von Agent Client Collector -Plugins.

Installation von Agent Client Collector

Sie können Agent Client Collector auf jedem unterstützten Hostcomputer installieren. Der Agent Client Collector stellt über das HTTP/S-Protokoll eine Verbindung zum MID-Server her, und die Verbindung bleibt aktiv, nachdem sie hergestellt wurde. Ein MID-Server kann mehrere Agents gleichzeitig bearbeiten, während ein einzelner Agent jeweils nur mit einem MID-Server gleichzeitig arbeitet und bei Bedarf zu einem anderen MID-Server wechselt, um Failover-Schutz zu bieten.

Wenn sich die IP-Adresse eines Agent ändert, wird basierend auf der MID-Server-Liste des Agent ein MID-Server ausgewählt, zu dem eine Verbindung hergestellt wird.

Die maximale Anzahl von Agents, die mit einem einzigen MID-Server verbunden sein können, kann in der Eigenschaft *`sn_agent.mid.max_allowed_agents`* MID-Server konfiguriert werden. Der Standardwert ist 4.000.

Führen Sie unter Windowsden Agent-Service als gMSA-, LocalService- oder lokaler Systemaccount aus.

Führen Sie unter Linux und macOSden -Agent als Systemkonto aus.

Für ACC-VC kann standardmäßig 1 GiB MID-Server 700 Agents gleichzeitig unterstützen. Eine 8-GiB-Konfiguration für MID-Server kann 8.000 Agents gleichzeitig unterstützen. Sie können

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auch horizontal skalieren. Zum Beispiel können 5 MID Servers mit 8 GiB Heap-Größe bis zu 40.000 Agents verarbeiten.

Wenn Sie den Agent auf einem einzelnen Hostserver vollständig neu installieren, wird ein zweiter Agent-Datensatz in der Instanz registriert. Löschen Sie den ursprünglichen Agent auf der Seite **„Agent Client Collectors** “ (**Alle** > **Agent Client Collector** > **Agents**) an.

Agents mit **dem Status „Ausgefallen“** oder **„Verbindung getrennt“**, die nicht gelöscht wurden, werden nach 30 Tagen automatisch gelöscht. Sie können diese Einstellung auf der Seite „Formular automatisch entleeren“ ändern (siehe Formulare automatisch entleeren).

Vor der Installation von Agent Client Collector müssen Sie folgende Schritte ausführen:

- Stellen Sie sicher, dass bei Ihrer Instanz mindestens ein MID Servers ordnungsgemäß registriert und validiert wurde, sodass dieser für eine Agent-Verbindungsanforderung verfügbar ist. Einzelheiten hierzu finden Sie unter MID-Server konfigurieren . In einer Bereitstellungsumgebung benötigen Sie nur einen MID-Server. Konfigurieren Sie jedoch in einer Produktionsumgebung mindestens zwei MID Servers, um die Zero Touch-Konfiguration zu unterstützen und sicherzustellen, dass ein MID-Server immer verfügbar ist, wenn einer ausfällt.
- Stellen Sie sicher, dass eine validierte Verbindung zwischen dem festgelegten Server, auf dem Sie den Agent installieren, und MID-Serverbesteht.
- Stellen Sie sicher, dass der Port MID-Server, auf dem der Listener Agent Client Collector ausgeführt wird, zugänglich ist.
- Stellen Sie sicher, dass in Ihrer Instanz die folgenden Plugins installiert sind.

  Für ACC-VC:

  - Agent Client Collector Visibility – Inhalt
  - Agent Client Collector Framework
  - Plugin Discovery [com.snc.discovery]

  Für ACC-M:

  - Agent Client Collector Framework
  - Agent Client Collector Monitoring
  - Ereignismanagement and Service-Mapping Core
  - Metrikdaten Plugin „com.snc.sa.metric“.

  Für ACC-L:

  - Agent Client Collector Log Analytics
  - Health Log Analytics

  Für DEX: ITOM Cloud-Services

  Sie können überprüfen, ob diese Plugins auf installiert sind **Systemdefinitionen** > **Plugins** Seite.

- Alle Plugins, die zum Lieferumfang des Basissystems gehören, sind mit dem ServiceNow-Zertifikat signiert. Optional können Sie anwenderdefinierte Plugins verwenden und mit Ihrem eigenen Zertifikat signieren, wie in Aktivieren Sie die sichere OpenSSL-Signierung für -Pluginsbeschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass Ihr System die Mindestanforderungen für die Installation des Agent erfüllt.

Mindestanforderungen für die Installation

Komponente „Agent Client Collector“.	Anforderungen
Agent Client Collector Framework	◦ 1 GB RAM ◦ 300 MB freier Speicherplatz ◦ 1 CPU-Core
Agent Client Collector-Überwachung	◦ 1 GB RAM ◦ 1 GB freier Speicherplatz ◦ 1 CPU-Core
Agent Client Collector Visibility – Inhalt	◦ 1 GB RAM ◦ 1 GB freier Speicherplatz ◦ 1 CPU-Core

- Stellen Sie sicher, dass Sie Agent Client Collector unter einer der unterstützten Betriebssystem-Distributionen installieren:

Unterstützte Betriebssystemverteilungen

Betriebssystem	Verteilung
Linux	◦ Red Hat Enterprise Linux RHEL und Oracle Linux – OL 7, 8, 9 ◦ CentOS 7, CentOS Stream 8 und 9 ◦ SLES 12, 15 ◦ Ubuntu 18.04, 22.04 LTS ◦ Amazon Linux 2 AMIs
Windows (ACC-M und ACC-L werden nur auf Servern unterstützt, nicht auf Endpunkten)	◦ Windows Server 2012, 2012r2, 2016, 2019, 2022 ◦ Windows 10 Enterprise Edition ◦ Windows 11 Professional und Enterprise ◦ Windows 11 Surface auf ARM64
macOS (sowohl auf x86_64- als auch auf ARM64-Architekturen (Apple Silicon). ACC-M und ACC-L werden nur auf Servern unterstützt, nicht auf Endpunkten.)	◦ Catalina ◦ Big Sur ◦ Monterey ◦ Ventura

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Alle unterstützten Betriebssysteme nur funktionieren mit dem x86-64-CPU-Architekturtyp. ACC-F v3.1.1 bietet außerdem native Unterstützung für ARM64 für Apple Silicon-Architekturen. Die neuesten Informationen finden Sie im Artikel „ Agent Client Collection on Non-x86-64 Computers and Incident Boards“ [KB1172387] in der Knowledge Base Now Support.

Bei Verwendung von ACC-L: Agent Client Collector wird mit dem standardmäßigen *servicenow*-Benutzer bereitgestellt. Vergewissern Sie sich, dass dieser Benutzer Lesezugriff hat, damit von Agent Client Collector alle konfigurierten Protokollpfade angezeigt werden können. Beispielsweise verfügt der Agent Client Collector *servicenow*-Benutzer, der zusammen mit dem Basissystem installiert wird, nicht über Berechtigungen zum Anzeigen des Pfads zu `/var/log/` unter Linux und des Pfads zu `C:\Windows\System32` unter Windows. Informationen zum Konfigurieren von Berechtigungen für den *servicenow*-Benutzer finden Sie in der Now Support-Knowledge Base im Artikel ACC-L Permission Denied issues [KB1117271] (Probleme verweigerter ACC-L-Berechtigungen).

Bei der Bestimmung der Anzahl der Computer und Server, die zur Unterstützung Ihrer Agents erforderlich sind (z. B. die Anzahl der Computer, die Proxy-Agents erfordern), müssen Sie die Leistungs-KPIs der Agents berücksichtigen. Weitere Informationen zu KPIs für die Leistung von Service Desk-Mitarbeitern finden Sie unter Agent Client Collector Leistung und Platzbedarf für URL-Überwachung.

Weitere Informationen zur Verwendung von Agent Client Collector in einer Umgebung mit Luftspalten finden Sie im Artikel Agent Client Collector Framework Air Gapped Configuration Item Management Solution [KB1585753] in der Knowledge Base Now Support.

Agent Client Collector unterstützt Domänentrennung. Die Domäne des Agent und der von ihm erstellten CIs ist abhängig von der MID-Server-Domäne, mit der der Agent verbunden ist. Die Domäne des Benutzers muss sich auf der niedrigsten Domänenebene befinden (wird als untergeordnete Domäne bezeichnet), um die Erstellung einer Websocket-Endpunkterweiterung für MID-Serverzu ermöglichen.

Zugehörige Informationen

- Agent Client Collector-Installation unter einem Linux-Betriebssystem
- Installieren Sie Agent Client Collector manuell auf einem Computer Windows .

Automatische MID-Server-Auswahl

Die automatische Auswahl von MID Servers stellt sicher, dass jeder Service Desk-Mitarbeiter den effizientesten verfügbaren MID-Serververwendet.

Die automatische Auswahlfunktion MID-Server von Agent Client Collector ist standardmäßig deaktiviert. Bevor Sie bestimmen, ob die automatische MID-Server -Auswahl für Ihre Anwendungsfälle geeignet ist, sind mehrere Faktoren zu berücksichtigen.

Überlegungen zu Anwendungsfällen

Die automatische Auswahl MID-Server von bietet mehrere Vorteile. MID-Server-Fähigkeiten kann die Liste der MID Servers eingrenzen, zu denen ein Service Desk-Mitarbeiter eine potenzielle Verbindung herstellen kann. Durch die automatische Auswahl MID-Server wird die Liste der Back-End-URL-Konfigurationen auf dem Agent-Host ohne zusätzliche Workflows auf dem neuesten Stand gehalten.

Wenn die automatische Auswahl für MID-Server aktiviert ist, führt der Service Desk-Mitarbeiter einen Konnektivitätstest anhand der Liste der verfügbaren MID Servers durch und ermittelt die beste Verbindung basierend auf der Latenz und der Anzahl der derzeit verbundenen Service Desk-Mitarbeiter.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Es gibt jedoch mehrere zusätzliche Überlegungen, die die automatische Auswahl MID-Server von für Ihren Anwendungsfall falsch machen können.

Die automatische ACC-Auswahl MID-Server ist kein echtes Lastenausgleichsmodul und sollte als Failover-Mechanismus betrachtet werden. Die Auswahl einer Back-End-URL ist komplexer, da sie aus mehreren Eingabequellen abgeleitet wird. Wenn stattdessen ein Anwendungslastenausgleichsmodul verwendet wird, muss nur eine Back-End-URL angegeben werden. Weitere Informationen finden Sie unter Lastenausgleichsmodul von Agent Client Collector aktivieren.

Standardmäßig wird jedem Service Desk-Mitarbeiter die Liste aller MID Servers gesendet, die auf ACC-Verbindungen lauschen. Da diese Liste MID Servers enthält, das in eingeschränkten Bereichen ausgeführt wird, können die Service Desk-Mitarbeiter versuchen, eine Verbindung zu ihnen herzustellen, was Sicherheitswarnungen generieren kann.

Ihre DNS-Konfiguration sollte vor der Verwendung der automatischen MID-Server -Auswahl berücksichtigt werden, da die Lösung zu unerwarteten Ergebnissen führen kann. Die DNS-Auflösung wird regelmäßig durchgeführt. Computersysteme von Endanwendern, die zwischen internen Unternehmens-, WLAN-, VPN- oder externen Netzwerken wechseln, können möglicherweise nicht erneut eine Verbindung herstellen, wenn sich der Netzwerkkontext geändert hat.

Automatischer Auswahlprozess

Wenn die automatische Auswahl aktiviert ist, sendet die ServiceNow-Instanz periodisch MID-Server-Aktualisierungen an bestehende Agents. Der Agent wählt einen MID-Server basierend auf Informationen aus, die er von der ServiceNow-Instanz erhält.

Bei der automatischen Auswahl MID-Server wählt der Service Desk-Mitarbeiter eine primäre und eine sekundäre MID-Liste aus und schreibt sie in die Konfigurationsdatei des Service Desk-Mitarbeiters. Der Agent verwendet diese Liste für Failover-Schutz, wenn der primäre MID/ sekundäre MID in der Liste die Verbindung verliert.

Wenn ein Agent erkennt, dass sich seine IP-Adresse geändert hat, stellt er automatisch eine Verbindung zum effizientesten MID-Server her, der in der Liste des Agent MID Serversverfügbar ist.

Um die Kommunikation zwischen MID-Server und Agent zu sichern, verwenden Sie den einheitlichen Schlüsselspeicher des MID-Servers. Weitere Informationen zur Verwendung des einheitlichen Schlüsselspeichers MID-Server finden Sie unter MID-Server Schlüsselspeicher .

Zugehörige Informationen

Automatische Auswahl der MID-Server aktivieren

Automatische Auswahl der MID-Server aktivieren

Wenn Sie die automatische Auswahl MID-Server aktivieren, kann der Service Desk-Mitarbeiter einen Konnektivitätstest anhand der Liste der verfügbaren MID Servers durchführen und die beste Verbindung basierend auf der Latenz und der Anzahl der derzeit verbundenen Service Desk-Mitarbeiter ermitteln. Die automatische MID-Server Auswahl ist standardmäßig deaktiviert.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

- Um das Senden regelmäßiger MID-Server -Updates von der Instanz ServiceNow an vorhandene Agents zu ermöglichen, legen Sie die Systemeigenschaft *sn_agent.enable_auto_mid_selection* auf **true**fest.
- So aktivieren Sie die automatische Auswahl MID-Server für einzelne Service Desk-Mitarbeiter:
  1. Legen Sie die Eigenschaft *enable-auto-mid-selection* in der Datei `acc.yml` des Agents auf **true**fest.
  2. Aktivieren und führen Sie die geplanten Aufgaben „MID-Liste für alle Service Desk-Mitarbeiter aktualisieren“ und „MID-Liste für alle neuen Service Desk-Mitarbeiter aktualisieren“ aus.

Nächste Maßnahme
Um die automatische Auswahl MID-Server wieder zu deaktivieren, setzen Sie alle Eigenschaften wieder auf **false**.

Fähigkeiten Agent Client Collector für MID Serverskonfigurieren

Konfigurieren Sie MID Servers mit den Fähigkeiten Agent Client Collector, damit MID Servers mit Service Desk-Mitarbeitern zusammenarbeiten kann. Service Desk-Mitarbeiter mit identischen Fähigkeiten MID-Server sind für die automatische Auswahl MID-Server berechtigt.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Eine Fähigkeit definiert MID-Server -Funktionen. Jedes MID-Server, dem eine Fähigkeit mit der Eigenschaft **„Is ACC Capability=true“** zugewiesen ist, kann mit einem Service Desk-Mitarbeiter zusammenarbeiten. Einzelheiten zu den Fähigkeiten MID-Server finden Sie unter MID-Server-Fähigkeiten .

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Fähigkeiten**.
2. Wählen Sie eine Fähigkeit aus, damit MID-Server mit dem Service Desk-Mitarbeiter zusammenarbeiten kann.
   a. Wählen Sie die Spalte ACC-Fähigkeit neben dem Eintrag AgentClientCollector aus.
   b. Legen Sie den Wert auf **true**fest.
3. Aktivieren Sie andere Fähigkeiten für Agent Client Collector MID Servers, indem Sie die Spalte Ist ACC-Fähigkeit neben dem Eintrag AgentClientCollector auswählen und den Wert auf **true**festlegen.

Ergebnisse
MID Servers mit denselben Fähigkeiten können während der automatischen MID-Server -Auswahl verwendet werden.

Konfigurieren Sie die automatische MID-Server -Auswahl basierend auf den Agent Client Collector -Fähigkeiten

Konfigurieren Sie mit dem Service Desk-Mitarbeiter die MID Servers, die nicht für die automatische Auswahl MID-Server von berechtigt sind. Beispielsweise können Sie aufgrund von Firewall-Einschränkungen verhindern, dass ein MID-Server eine Verbindung zu Ihrem -Agent herstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Service Desk-Mitarbeiter mit unterschiedlichen ACC-Funktionen (Agent Client Collector) können für die automatische Auswahl MID-Server von nicht berücksichtigt werden. Wenn Sie verhindern möchten, dass ein MID-Server automatisch MID-Server ausgewählt wird, können Sie die MID-Server verschiedenen ACC-Fähigkeiten von allen MID Serversin Ihrer Umgebung zuweisen, aber nicht vom primären MID-Server.

Prozedur
1. Konfigurieren Sie die Fähigkeiten Agent Client Collector für MID Serverswie in Fähigkeiten Agent Client Collector für MID Serverskonfigurierenbeschrieben.
2. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Server**.
3. Wählen Sie MID-Server aus, die für die automatische Auswahl MID-Server nicht berechtigt sein sollen.
4. Wählen Sie das Symbol für zusätzliche Aktionen und wählen Sie **Ansicht** > **Standardansicht**.
5. Wählen Sie die Registerkarte **Funktionen**.
6. Stellen Sie sicher, dass MID-Server nicht mit den Fähigkeiten zugewiesen ist, für die auf der Registerkarte **FähigkeitenIs ACC Capability=true (Is ACC-Fähigkeit = true)** festgelegt ist.

Example: MID Servers wird so konfiguriert, dass er für die automatische Auswahl MID-Server von nicht berechtigt ist
1. Weisen Sie die **AgentClientCollector** -Fähigkeit MID-Server A und MID-Server C zu, aber nicht MID-Server B.
2. Auf der Seite „MID-Server-Fähigkeiten“:
   a. Weisen Sie MID-Server A und MID-Server C eine Fähigkeit zu.
   b. Weisen Sie MID-Server B eine andere Fähigkeit zu.
3. Installieren Sie Agent Client Collector Framework, und geben Sie während der Installation MID-Server A als MID-Server an.

   Nach der Installation hat der Agent **den Status = In Betrieb**, und sein MID-Server lautet MID-Server A.
4. Führen Sie die geplante Aufgabe für die MID-Server -Auswahl aus, um zu bestimmen, welche MID Servers für die automatische MID-Server -Auswahl berechtigt sind.

   MID-Server B ist für die automatische Auswahl nicht berechtigt, da es nicht über die gleiche ACC-Fähigkeit wie MID-Server A verfügt. MID-Server C ist berechtigt, da es über die gleiche ACC-Fähigkeit wie MID-Server A verfügt.

Agent Client Collector zur Massenbereitstellung in benutzerdefiniertes Basis-Image einbinden
Stellen Sie Agent Client Collector auf einem virtuellen Computer während einer Massenbereitstellung mithilfe des Basis-Image bereit. Bei der Massenbereitstellung findet eine automatische Installation statt, bei der der Installationsstatus nicht transparent ist.

Vorbereitungen
Verwenden Sie MicrosoftMicrosoft Azure Event Hubs SCCM, um die Bereitstellung und Sicherheit Ihrer Geräte zu verwalten, wie im KB-Artikel Create a Windows service account

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

with Log on as a Service (Windows-Servicekonto mit Anmeldung als Service erstellen) beschrieben.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agent-Downloads**.
2. Laden Sie die Installationsdatei des entsprechenden Betriebssystems herunter.
3. Installieren Sie den Agent gemäß den entsprechenden Betriebssystemanweisungen.
4. Führen Sie den folgenden Befehl aus, um den Agent-Service zu stoppen:
   - In einer Windows -Umgebung: Führen Sie den Befehl `sc stop AgentClientCollector`aus
   - In einer Linux -Umgebung: Führen Sie den Befehl `sudo systemctl stop acc`aus
5. Stellen Sie sicher, dass die Datei `acc.yml` keinen verschlüsselten API-Schlüssel enthält. Beispiel: `api-key: "`<insert plain text API key here> “
6. Löschen Sie den Inhalt des Cache-Verzeichnisses des Agent, wobei die Verzeichnisstruktur intakt bleibt:
   - In einer Windows -Umgebung: `C:\ProgramData\ServiceNow\agent-client-collector\cache`
   - In einer Linux -Umgebung: `/var/cache/servicenow/agent-client-collector`
7. Stellen Sie bei der Installation auf dem Computer Windows sicher, dass die Installation erfolgreich war, indem Sie einen der folgenden Schritte ausführen:
   - Aktivieren Sie die Protokollierung in der automatischen Installation, und stellen Sie sicher, dass die Protokolldatei mit der Zeichenfolge `Windows Installer installed the product` endet.
   - Stellen Sie sicher, dass der Service **AgentClientCollector** den Status `Running` (Wird ausgeführt) aufweist.
8. Greifen Sie bei der Installation auf einem Computer Linux auf den Computer zu, auf dem der Agent installiert ist, und ändern Sie die Datei `/usr/share/servicenow/agent-client-collector/serial_number.txt` auf eine der folgenden Arten:
   - Ändern Sie deren Inhalt mit der Seriennummer des Hosts, indem Sie den folgenden Befehl ausführen: `sudo -n dmidecode -s system-serial-number`
   - Weisen Sie dem Benutzer servicenow sudo-Berechtigungen zu, um die Ausführung des folgenden `osqueryi`-Befehls zu ermöglichen: `sudo -E env "PATH=$PATH" osqueryi --logger_min_status=3 --line "select hardware_serial from system_info"`

   Hinweis: Sie müssen den Hostnamen der virtuellen Maschine nach der Bereitstellung in einen eindeutigen Wert ändern, um eine Beschädigung des CI des Hosts zu vermeiden.

9. Starten Sie als Schritt nach der Bereitstellung den Agent-Service neu.
   - In einer Windows -Umgebung: Führen Sie den Befehl `sc start AgentClientCollector`aus
   - In einer Linux -Umgebung: Führen Sie den Befehl `sudo systemctl start acc`aus

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Lastenausgleichsmodul von Agent Client Collector aktivieren

Aktivieren Sie ein Lastenausgleichsmodul, um sicherzustellen, dass MID Serversfunktionsfähig ist. Ein Lastenausgleichsmodul verteilt Ressourcen über mehrere MID Servers, um sicherzustellen, dass kein einzelner MID-Server überlastet wird.

Vorbereitungen

1. Installieren Sie Agent Client Collector Framework.
2. Konfigurieren Sie den Webserver Agent Client Collector.
3. Stellen Sie sicher, dass Sie Zugriff auf die Konfiguration des Lastenausgleichsmoduls der internen Anwendung haben.
4. Stellen Sie sicher, dass die Datei<mid_server_install_path> „`/static/hello.txt`“ wurde während des Setups MID-Server von erstellt.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Lastenausgleichsmodule sind standardmäßig nicht konfiguriert. Befolgen Sie dieses Verfahren, um ein Lastenausgleichsmodul in Ihrer Umgebung zu konfigurieren.

Prozedur

1. Konfigurieren Sie das Lastenausgleichsmodul so, dass es im Parameter *`backend-url`* in der `acc.yml`- Konfigurationsdatei verwendet werden kann.
2. Führen Sie die folgenden Setup-Aktionen für das Lastenausgleichsmodul aus:

   a. Erhöhen Sie die Zeitüberschreitung bei Leerlauf auf 300 Sekunden.

   b. Konfigurieren Sie die Zielgruppe des Lastenausgleichsmoduls mit *`https`* und Port 443. Konfigurieren Sie alle MID Servers hinter dem Lastenausgleichsmodul als Ziele.

   c. Konfigurieren Sie die Integritätsprüfung des Lastenausgleichsmoduls, um das zu überwachen<mid_server_install_path> Während des Setups von MID-Server erstellte Datei „`/static/hello.txt`“.
   Die Integritätsprüfung stellt sicher, dass es keine Kommunikationsunterbrechungen zwischen dem Lastenausgleichsmodul und MID-Servergibt.

3. Fügen Sie hinzu<mid_server_install_path> Datei `/static/hello.txt` im statischen Ordner für jedes MID-Server.
   Sie können die Datei an einem anderen Speicherort platzieren, für den keine Anmeldeinformationen erforderlich sind, um das Setup zu vereinfachen.
4. Aktualisieren Sie die Konfigurationsdatei acc.yml mit dem entsprechenden FQDN (Wert*`backend-url`*) und der Portnummer, und deaktivieren Sie die automatische Auswahl MID-Server.

```
backend-url:
 - wss://<fqdn>:<port>/ws/events
enable_auto_mid_selection: false
```

5. Starten Sie Agent Client Collectorneu.

Ergebnisse

Der Daten-Flow Agent Client Collector wird wie in Agent Client Collector-Architekturbeschrieben fortgesetzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Informationen zur Verbesserung der Sicherheit durch SSL/TLS-Konfiguration finden Sie im Artikel mit Dokumentationsmaterial zu ITOM Agent Client Collector in der Now Support Knowledge Base.

Upgrade eines Agent in einer Instanz

Führen Sie ein selektives Selbst-Upgrade anstelle eines Massen-Upgrades durch, um die Effizienz bei der Arbeit mit Agents zu erhöhen, auf die schwer zugegriffen werden kann, z. B. in der Cloud bereitgestellte Agents. Sie können ein selektives Upgrade für bis zu 20 Agents gleichzeitig durchführen.

Vorbereitungen

Unterstützte Betriebssysteme: Windows und Linux.

Wenn Sie in einer Linux -Umgebung arbeiten, vergewissern Sie sich, dass Sie über sudo-Berechtigungen verfügen und dass die folgenden Konfigurationen festgelegt sind:

Linux-Betriebssysteme

BS	BS-Version	Befehle	Agent-Version
CentOS,Red Hat	7, 8	• `/usr/bin/ systemctl ACC starten` • `/usr/bin/ systemctl stop acc` • <systemctl location`daemon-reload` (Standardspeicherort ist `/usr/bin`) • `/usr/bin/rpm -Uv<cache dir location> / upgrade/ agent-client-collector-upgrade.rpm` Standardspeicherort für Cache-Verzeichnis: `/var/ cache/servicenow/ agent-client-collector` • `unzip -o`: Entpackt die Signaturdatei, um die Installation zu validieren. • `openedsl dgst -sha256 -verify`: Verifiziert die	2.7

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Betriebssysteme (Fortsetzung)

BS	BS-Version	Befehle	Agent-Version
		Verwendung einer Signatur aus einer ServiceNow-Installationsdatei.	
Debian, Ubuntu		• `/usr/bin/ systemctl ACC starten` • `/usr/bin/ systemctl stop acc` • <systemctl location`daemon-reload` (Standardspeicherort ist `/usr/bin`) • `/usr/bin/dpkg --installation --verweigern-downgrade -- überspringen-same-version<cache dir location> / upgrade/ agent-client-collector-upgrade.rpm` Standardspeicherort für Cache-Verzeichnis: `/var/ cache/servicenow/ agent-client-collector` • `unzip -o:` Entpackt die Signaturdatei, um die Installation zu validieren • `gpg -import und gpg --verify:` Verifiziert die Verwendung einer Signatur	2.7

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Betriebssysteme (Fortsetzung)

BS	BS-Version	Befehle	Agent-Version
		`aus einer ServiceNow-Installationsdatei.`	

Erforderliche Rolle:

- Linux: Sudo-RPM/Dpkg
- Windows: Lokales SYSTEM-Konto

Warum und wann dieser Vorgang ausgeführt wird

Agent Client Collector unterstützt selektive Selbst-Upgrades in den folgenden Betriebssystemen:

- Windows: Aufgrund von Windows UAC-Einschränkungen muss der Agent als lokales SYSTEM-Konto ausgeführt werden, um das Upgrade über *msiexec*durchzuführen.
- Linux: RPM und DEB

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
2. Wählen Sie den Agent aus, den Sie aktualisieren möchten.
3. Wählen Sie im Abschnitt **„Zugehörige Links “ Upgrade-Agent**.
4. Wählen Sie im Bestätigungsdialogfeld **Upgrade**aus.
   Die Seite **„Verläufe des Agent-Upgrades“** wird angezeigt, in der Sie den Upgrade-Fortschritt anhand der Spalte **„Status“** überwachen können, die entweder **Erfolg** oder **Fehlgeschlagen**anzeigt.
5. Zeigen Sie das Protokoll für das Agent-Upgrade in der Spalte **Nachricht** an.
   Navigieren Sie bei einem fehlgeschlagenen Upgrade auf einem Computer Linux zu<cache directory location> `/upgrade/agent-client-collector-upgrade.rpm`, und stellen Sie sicher, dass die Konfigurationen für das entsprechende Betriebssystem gemäß der Tabelle Linux Betriebssysteme oben festgelegt sind.

   Überprüfen Sie bei einem Upgrade auf einem Computer Windows die entsprechende Protokolldatei unter<user folder> `\AppData\Lokal\Temp\ACC_Logs`:

   - ACC-Protokolle: `ACC_Upgrade.log`
   - MSI-Protokolle: `MSI_ACC_Upgrade.log`

Upgrade mehrerer Agents in einer Instanz

Wenn Sie ein selektives Upgrade eines Agents in einer Instanz durchführen, können Sie mehrere Instanzen auswählen, die gleichzeitig aktualisiert werden sollen.

Vorbereitungen

Unterstützte Betriebssysteme: Windows und Linux.

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können bis zu 20 Agents gleichzeitig für das Upgrade auswählen. Um eine große Anzahl von Agents zu aktualisieren, integrieren Sie Agent Client Collector in Ihre Tools zur Softwarebereitstellung.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
2. Aktivieren Sie die Kontrollkästchen neben den Agents, für die Sie ein Upgrade durchführen möchten.
   Sie können bis zu 20 Mitarbeiter auswählen.
3. Wählen Sie im Feld **Aktionen für ausgewählte Zeilen...** die Option **Upgrade-Agent**aus.
4. Wählen Sie im Bestätigungsdialogfeld **Upgrade**aus.

Zugehörige Informationen

Upgrade eines Agent in einer Instanz

Agents manuell neu starten

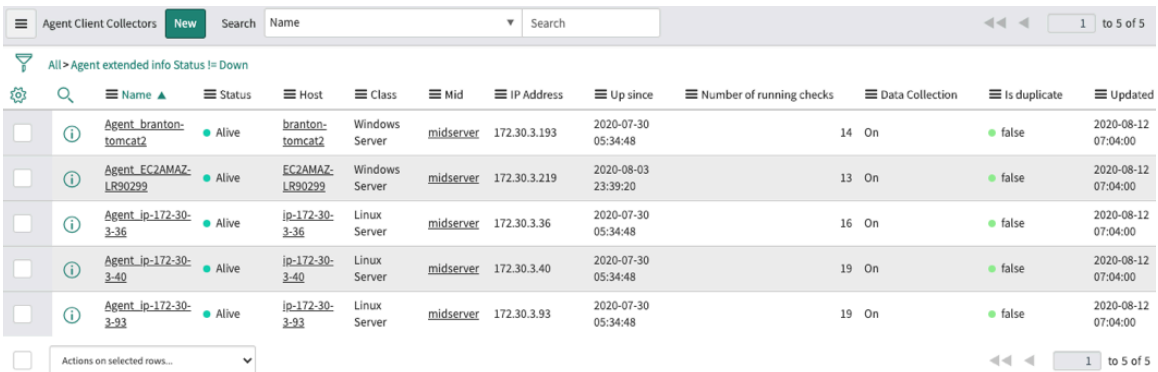
Führen Sie einen manuellen Neustart eines Agent durch, wenn die Agent-Konfigurationsdatei aktualisiert wurde oder wenn der Agent instabil ist. Ein manueller Neustart ist nur für Agents möglich, die entweder in einer Windows-Umgebung installiert sind oder als Linux-basierte Agents `systemd` verwenden.

Vorbereitungen

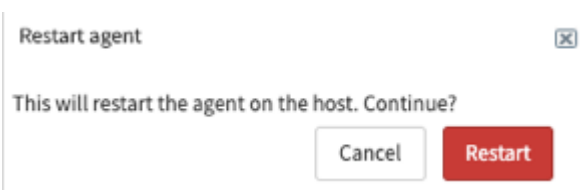
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
   Die Seite **Agent Client Collectors** wird mit der Liste der Agents angezeigt.



2. Aktivieren Sie das Kontrollkästchen des Agent, den Sie neu starten möchten.
   Sie können mehrere Agents auswählen.
3. Wählen Sie in der Liste **Actions on selected rows...** (Aktionen für ausgewählte Zeilen...) unter der Liste der Agents die Option **Restart Agent** (Agent neu starten) aus.
   Ein Bestätigungsdialogfeld wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie **Neustart**.
   Alternativ können Sie den Agent aus dem Agent-Datensatz neu starten, indem Sie den Namen des Agent auswählen und im Abschnitt **„Zugehörige Links“Agent neu starten**auswählen.

Agent Client Collector-Installation unter einem Linux-Betriebssystem

Installieren Sie Agent Client Collector auf einem System, das ein Linux-Betriebssystem verwendet, indem Sie entweder ein einzeiliges Befehlsskript verwenden oder das Installationsverfahren zur Einbettung in Ihren eigenen Paketverteilungsmechanismus befolgen. Das Installationsverfahren sorgt bei der Verwendung von Paketverteilungslösungen für Konsistenz.

Installieren Sie Agent Client Collector auf einem Linux -System

Installieren Sie Agent Client Collector mit einem Paketverteilungstool. Vor der Installation können Sie Agent Client Collector manuell auf einigen Computern installieren, um sicherzustellen, dass Ihre Agents die richtigen Richtlinien und Prüfungen enthalten, bevor Sie eine große Anzahl von Agents installieren.

Vorbereitungen

- Stellen Sie sicher, dass der Agent Client Collector -Listener auf Ihrem MID Serverskonfiguriert ist und dass der Service auf Ihren Zielhosts verfügbar ist.
- Stellen Sie sicher, dass das Betriebssystem und die Version Ihres Servers unterstützt werden. Eine Liste der unterstützten Betriebssysteme und Versionen finden Sie unter Installation von Agent Client Collector.
- Überprüfen Sie, ob während der Bereitstellung Einschränkungen oder Anforderungen zu beachten sind, z. B. die Angabe eines anderen Accounts als des standardmäßigen servicenow-Accounts. Weitere Informationen zum Einbetten des Agent in Ihr eigenes automatisiertes System finden Sie im Dokumentationsmaterial zu ITOM Agent Client Collector [KB1122613] .
- Stellen Sie sicher, dass MID-Server und die zugehörigen Erweiterungen MID-Webserver und ACC-Websocket-Endpunkte aktiv sind.
- Rufen Sie die Informationen zum MID-Server ACC-Listener ab, die im Parameter *backend-url* des Agents angegeben werden sollen.
  1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **MID-Server**.
  2. Wählen Sie einen MID-Server.
  3. Wählen Sie die Registerkarte **ACC-Websocket-Endpunkte**.
  4. Wählen Sie einen Websocket-Endpunkt aus.
  5. Kopieren Sie den Wert im Feld **Endpunkt-URL**.
- Rufen Sie den API-Schlüssel MID-Server ab, der im Parameter *api-key* des Agent angegeben ist.
  1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **MID-Webserver API-Schlüssel**.
  2. Wählen Sie den API-Schlüssel aus, den Sie verwenden möchten.
  3. Wählen Sie im Abschnitt **„Zugehörige Links“ API-Schlüssel anzeigen aus**.
  4. Kopieren Sie den API-Schlüsselwert, und schließen Sie das Popup-Fenster.

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Während der Installation (und des Upgrades) Linux von wird die ausführbare Datei des Agent standardmäßig mit Linux -Fähigkeiten (CAP_SETFCAP, CAP_SETPCAP) aktiviert. Store-Apps wie Agent Client Collector Log Analytics (ACC-L) können hiermit Funktionen zum Lesen des gesamten Dateisystems (CAP_DAC_READ_SEARCH) gewähren. Das System durchläuft verschiedene Sicherheitsmaßnahmen, z. B. die doppelte Überprüfung der Ursprungs des Inhalts, die Nutzung des Plugin-Überprüfungsprozesses und vieles mehr, um sicherzustellen, dass die Gewährung von Funktionen kein Sicherheitsrisiko darstellt. Dieses Verfahren setzt voraus, dass Sie mit den Befehlen für die Fähigkeiten Linux vertraut sind.

Um diese erweiterten Funktionen zu deaktivieren, führen Sie je nach Betriebssystem/ Paketsystem von Linux die folgenden Befehle aus:

Befehle zum Deaktivieren der erweiterten Linux-Fähigkeit

BS/Verpackungssystem	Befehle

U/min	`ACC_SKIP_CAPS=true yum / dnf localinstall`
	
	`ACC_SKIP_CAPS=wahre U/min -vi agent-client-collector-<version number> -x86_64.rpm`

Debian	`ACC_SKIP_CAPS=true apt-get install`
	
	`ACC_SKIP_CAPS=true dpkg -i agent-client-collector-<version number> -<distro> _amd64.deb`

SLES	`ACC_SKIP_CAPS=true zypper-Installation`

Prozedur

1. Laden Sie die relevanten Installationspakete herunter.
   - Für die manuelle Installation:
     a. Navigieren zu > **Agent Client Collector** > **Bereitstellung** > **Agent-Downloads**.
     b. Laden Sie die entsprechende .rpm- oder .deb-Installationsdatei herunter.
     c. Laden Sie die relevanten Signaturdateien herunter, um die Installationsdateien zu validieren.
   - Führen Sie für die Installation über die Befehlszeile die folgenden Befehle aus, um die Signatur- und Installationsdateien auf Ihren lokalen Computer herunterzuladen:

```
curl -LO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-client-collector-<version_number>-x86_64.rpm
curl -LO
 https://install.service-now.com/glide/distribution/builds/package/app-signed/agent-client-collector-<version_number>-x86_64-rpm-rpm.zip
```

Hinweis: Jeder „curl“-Befehl muss in einer einzigen Zeile stehen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Wahlweise: Verifizieren Sie die Paketsignatur.

a. Extrahieren Sie die Installationsdatei (wenn sie komprimiert ist), indem Sie den folgenden Befehl ausführen:
`unzip agent_client-collector-<version_number>-x86_64-rpm-rpm.zip`

b. Validieren Sie die Signatur der Installationsdatei, indem Sie die angegebenen Befehle ausführen.

- In einem RPM-basierten System:

```
openssl dgst -sha256 -verify {<ServiceNow DGST pem key>}
 -signature {<signature file>} agent-client-collector-<version
 number>-x86_64.rpm
```

Wo<ServiceNow DGST pem key> ist die `PEM-` Datei, die aus der `ZIP-` Datei extrahiert wird, und<signature file> ist die `.bin` -Datei, die aus der `.zip-` Datei extrahiert wird.

Zum Beispiel:

```
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/a
pp-signed/agent-client-collector-3.0.0-x86_64.rpm
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/a
pp-signed/agent-client-collector-3.0.0-x86_64-rpm-rpm.zip
$ unzip agent-client-collector-3.0.0-x86_64-rpm-rpm.zip
Archive: agent-client-collector-3.0.0-x86_64-rpm-rpm.zip
inflating: ServiceNow_Digicert_DGST.pem
extracting: agent-client-collector-3.0.0-x86_64.bin
$ openssl dgst -sha256 -verify ServiceNow_Digicert_DGST.pem
 -signature agent-client-collector-3.0.0-x86_64.bin
 agent-client-collector-3.0.0-x86_64.rpm
Verified OK
```

Hinweis: Jeder Befehl muss in einer einzelnen Zeile stehen.

- Auf einem Debian-basierten System:

(Optional) `gpg --import ServiceNow_Digicert_Public.gpg`

- Auf Debian 12-Computern: `dpkg-sig --verify agent-client-collector-`<version number> -<distro> _amd64.deb
- Auf anderen Debian-Computern: `sudo gpg --verify agent-client-collector-`<version number> -<distro> _amd64.deb

Zum Beispiel:

```
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/a
pp-signed/agent-client-collector-3.0.0-debian-9_amd64.deb
$ curl -sLO
 https://install.service-now.com/glide/distribution/builds/package/a
pp-signed/agent-client-collector-3.0.0-debian-9_amd64-deb-deb.zip
$ unzip agent-client-collector-3.0.0-debian-9_amd64-deb-deb.zip
Archive: agent-client-collector-3.0.0-debian-9_amd64-deb-deb.zip
extracting: ServiceNow_Digicert_Public.gpg
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
$ gpg --import ServiceNow_Digicert_Public.gpg
gpg: /home/admin/.gnupg/trustdb.gpg: trustdb created
gpg: key 985DD52C6A0ABB45: public key "ServiceNow, Inc. (Signing)
 <seceng@servicenow.com>"
imported
gpg: Total number processed: 1
gpg: imported: 1
$ dpkg-sig --verify agent-client-collector-3.0.0-debian-9_amd64.deb
Processing agent-client-collector-3.0.0-debian-9_amd64.deb...
GOODSIG _gpgbuilder 9B928FB49771DF6C047430DD985DD52C6A0ABB45
 1665054068
```

Hinweis: Jeder Befehl muss in einer einzelnen Zeile stehen.

3. Installieren Sie das Paket Agent Client Collector mit dem Paketmanager, der der Linux-Distribution zugeordnet ist.

BS	Befehl
RHEL-basiert	`yum / dnf localinstall`
SLES	`Zypper-Installation`
Debian-basiert	`apt-get installieren`

Wenn diese Befehle nicht ordnungsgemäß konfiguriert sind, können Sie alternativ die Kernbefehle verwenden, die für die Ausführung mit den Paketmanager-Befehlen konfiguriert sind.

- RPM-basiertes System: `#rpm -vi agent-client-collector-`<version number> -x86_64.rpm
- Debian-basiertes System: `# dpkg -i agent-client-collector-`<version number> -<distro> _amd64.deb

Überprüfen Sie mit Ihrem Systemadministrator, ob die Paketbefehle richtig konfiguriert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Für einige Dateisysteme sind möglicherweise Einschränkungen aktiviert. Beispielsweise kann `/var/` mit der Kennzeichnung *noexec* bereitgestellt werden. Da der Agent Agent Client Collector Plugins ausführen muss, die normalerweise im Verzeichnis „`/var/cache`" gespeichert sind, müssen Sie die Anwendung in bestimmten Ordnern bereitstellen, indem Sie die Installationspfade mit der Option `--relocate` als `.rpm`- Parameter anpassen.

Beispiel: `rpm -i --relocate /var/cache=/opt/cache agent-client-collector-`<version_number> -x86_64.rpm

Die folgenden Pfade können verschoben werden:

Pfad	Notizen
`/etc`	Bei der Aktualisierung müssen Sie auch den Parameter *allow-list* in der Datei `acc.yml` mit dem neuen Pfad aktualisieren.
`/usr/share`	N/V
`/var/cache`	Wenn Sie das Verzeichnis „`/var`" aktualisieren, werden alle Unterverzeichnisse „`/var`", die unter dem neuen Verzeichnis geschachtelt sind, beibehalten.
`/var/log`	
`/var/run`	
`/var`	

Überprüfen Sie die Pfade in `/usr/lib/systemd/system/acc.service`, um sicherzustellen, dass sie wie erwartet angezeigt werden.

4. Konfigurieren Sie bei der Installation eines DEB-Pakets die `acc.yml` -Konfigurationsdatei des Agent.

   a. Kopieren Sie die Beispielkonfigurationsdatei, indem Sie den folgenden Befehl ausführen.

   ```
   # cp -p /etc/servicenow/agent-client-collector/acc.yml.example /etc/servicenow/agent-client-collector/acc.yml
   ```

   b. Benennen Sie die Allow-Listendatei um.

   ```
   # cp -p /etc/servicenow/agent-client-collector/check-allow-list.json.default /etc/servicenow/agent-client-collector/check-allow-list.json
   ```

   Hinweis: Dieser Schritt ist nicht relevant für RPM-Pakete, die mit den Dateien `acc.yml` und `check-allow-list.json` im Basissystem enthalten sind.

5. Wenn Sie ein .deb- oder ein .rpm-Paket installieren, aktualisieren Sie die Konfigurationsdatei, indem Sie *check-allow-list.json* zu „`/etc/servicenow/agent-client-collector`" hinzufügen und die `Back-End-URL` und `den API-Schlüssel` aus der Instanz kopieren.
   Zum Beispiel:

```
---
# Agent Client Collector configuration
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
backend-url:
 - "wss://YOUR_MID_ENDPOINT_HERE:YOUR_MID_PORT_HERE/ws/events"
api-key: "YOUR_API_KEY_HERE"
log-level: "info"
insecure-skip-tls-verify: false
allow-list: /
etc/servicenow/agent-client-collector/check-allow-list.json
verify-plugin-signature: true
max-running-checks: 10
disable-sockets: true
disable-api: true
statsd-disable: true
enable-auto-mid-selection: false
agent_cpu_threshold:
 cpu_percentage_limit: 25
 repeated_high_cpu_num: 3
 monitor_interval_sec: 60
 agent_cpu_threshold_disabled: false
```

Die Funktion *allow-list*, die angibt, welche Befehle der Agent ausführen darf, ist aktiviert.

6. sudoers konfigurieren.

Die Konfiguration wird normalerweise von Ihrem Linux -Systemadministrator automatisiert. Um die Richtigkeit vor der vollständigen Konfiguration manuell zu konfigurieren, führen Sie den folgenden aus.

```
# visudo -f /etc/sudoers.d/01_servicenow
User_Alias ACC_USERS = servicenow
Cmnd_Alias ACC_CMD = /usr/sbin/dmidecode -s
 baseboard-serial-number,/usr/sbin/dmidecode -s
 chassis-serial-number,/usr/sbin/dmidecode -s
 system-serial-number,/usr/sbin/dmidecode -s system-uuid,/usr/sbin/ss
 -tanp
ACC_USERS ALL = (root) NOPASSWD:ACC_CMD
Defaults:ACC_USERS !requiretty
```

7. Konfigurieren Sie den Agent so, dass er als Dienst ausgeführt wird.

a. Schützen Sie den Ressourcenverbrauch, indem Sie die angegebenen Werte der Datei `/usr/lib/systemd/system/acc.service` hinzufügen.

- CPUShares = 128
- CPU-Kontingent = 10 %
- Arbeitsspeichergrenze = 192 MB
- BlockIOWeight = 10
- LimitNICE=15

Zum Beispiel:

```
# vi /usr/lib/systemd/system/acc.service
[Unit]
Description=Agent-Now acc
After=network-online.target
[Service]
Environment=AGENT_ROOT=/usr/share
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
Environment=AGENT_CACHE_ROOT=/var/cache
Environment=AGENT_CONFIG_ROOT=/etc
Environment=AGENT_LOG_ROOT=/var/log
Environment=AGENT_RUN_ROOT=/var/run
Environment=RUBYOPT=-Eutf-8
User=servicenow
Group=servicenow
ExecStart=/usr/share/servicenow/agent-client-collector/bin/acc-service
 start acc
KillMode=process
Restart=on-failure
RestartSec=1min
CPUShares=128
CPUQuota=10%
MemoryLimit=192M
BlockIOWeight=10
LimitNICE=+15
[Install]
WantedBy=network-online.target
```

b. Führen Sie den Befehl „reload daemon“ aus, wenn Sie die Servicedatei nach dem Aktivieren des acc-Service geändert haben.

```
# systemctl daemon-reload
```

c. Aktivieren und starten Sie den Service, indem Sie die folgenden Befehle ausführen.

```
# systemctl aktivieren acc
```

```
# systemctl start acc
```

Führen Sie eine einzeilige Agent Client Collector -Installation auf Linux mit ITOM Cloud Services durch

Installieren Sie Agent Client Collector auf einem Computer vom Typ Linux ohne MID-Server mithilfe von ITOM Cloud Services. Wenn Sie Informationen über die Cloud senden, aktivieren Sie die MID-Server für persistentere Ressourcen.

Vorbereitungen

Installieren Sie das Plugin ITOM „ Cloud Services.

Erstellen Sie einen Agent-Registrierungsschlüssel, wie in Konfigurieren Sie einen Agent-Registrierungsschlüsselbeschrieben.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zur Arbeit mit Cloud-Services finden Sie unter DEX-Architektur .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Agent-Registrierungsschlüssel abrufen:
   a. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agent-Registrierungsschlüssel**.
   b. Wählen Sie den entsprechenden Agent-Registrierungsschlüssel aus.
   c. Kopieren Sie den Wert des Registrierungsschlüssels, und speichern Sie ihn an einem Ort, an dem Sie ihn bei Bedarf problemlos abrufen können.
2. Rufen Sie die relevante öffentlich zugängliche Gateway-URL basierend auf Ihrem Standort ab:
   - AMER (Amerika): `itomcnc-prod-gateway.amer.sncapps.service-now.com:443`
   - EMEA (Europa): `itomcnc-prod-gateway.emea.sncapps.service-now.com:443`
   - APAC (Asien-Pazifik): `itomcnc-prod-gateway.apac.sncapps.service-now.com:443`
3. Geben Sie auf dem Server, auf dem Sie Agent Client Collectorinstallieren, den folgenden Befehl ein:

```
CONNECT_WITHOut_MID="wahr" ACC_CNC="wahr"<gateway_endpoint>
„ REGISTRATION_KEY = “<registration_key> „ INSTANCE_URL =
„https://“<instance_url> " bash -c "$(curl -L https:// /api/sn_agent/
agents/install_agent)“
```

Die folgende Tabelle zeigt die Parameterwerte im Befehl.

Befehlszeilenparameterwerte

Parameter	Wert
VERBINDEN_OHNE_MID	Geben Sie **„wahr“** an, um ITOM Cloud-Services zu aktivieren. Wenn kein Wert angegeben ist, wird die reguläre Websocket-Installation MID-Server aufgerufen. Einzelheiten zur Konfiguration eines Websocket auf dem MID-Serverfinden Sie unter Websocket-Server auf MID-Server installieren.
ACC_CNC	Öffentlicher Gateway-Endpunkt für Agent Client Collector, den Sie angeben können.
REGISTRATION_KEY	Aktiver und gültiger Agent-Registrierungsschlüssel, mit dem der Agent kommunizieren soll.
INSTANCE_URL	ServiceNow Instanz, bei der sich der Service Desk-Mitarbeiter registriert
ACC_ALLOW_LIST	Optionale Zeichenfolge *ACC_ALLOW_LIST=0*, die Sie hinzufügen können, um die Allow-Liste zu deaktivieren. Standard: Die Allow-Liste ist aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert
	Hinweis: Wenn Sie die Allow-Liste deaktivieren, gefährden Sie die Sicherheit Ihres Systems. Diese Aktion ist als temporäre Maßnahme gedacht, während Sie die Allow-Liste aktualisieren. Entfernen Sie nach Abschluss des Updates *ACC_ALLOW_LIST=0* aus der Befehlszeile.
ACC_VALIDATE_SIG	Optionale Zeichenfolge *ACC_VALIDATE_SIG=0*, die Sie hinzufügen können, um die Überprüfung der Validierung der Zertifizierung durch das Installationsprogramm zu deaktivieren. Standard: Validierung ist aktiviert. **Hinweis:** Deaktivieren Sie die Zertifizierungsvalidierung nur, wenn Sie nicht standardmäßige Signaturvalidierungstools verwenden.

Validieren Sie die Installation Linux.

Nach der Installation von Agent Client Collector auf einem Linux -System validieren Sie die Installation, indem Sie sich vergewissern, dass sie ordnungsgemäß durchgeführt wurde.

Vorbereitungen

Installieren Sie Agent Client Collector auf einem Linux -System (siehe Installieren Sie Agent Client Collector auf einem Linux -System).

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Führen Sie den Befehl `# systemctl status acc` aus.
   Der Indikator *active (running)* wird angezeigt, wenn der Service ordnungsgemäß ausgeführt wird.

```
# systemctl status acc
● acc.service - Agent-Now ACC
Loaded: loaded (/usr/lib/systemd/system/acc.service; enabled; vendor
 preset: disabled)
Active: active (running) since Mon 2022-04-25 14:10:24 UTC; 6 months 23
 days ago
Main PID: 2693 (acc)
Tasks: 10 (limit: 512)
Memory: 143.4M (limit: 192.0M)
CPU: 12h 57min 50.442s
CGroup: /system.slice/acc.service
└─2693 /usr/share/servicenow/agent-client-collector/bin/acc start
 --config-file
/etc/servicenow/agent-client-collect...
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Zeigen Sie das verschlüsselte *api-key* und das verwendete *agent-key-id* an, indem Sie den Befehl `grep -E '^api-key|agent-key-id' /etc/servicenow/agent-client-collector/acc.yml` ausführen.

```
# grep -E
 '^api-key|agent-key-id' /etc/servicenow/agent-client-collector/acc.yml
api-key:
 "encrypted:adskfjldfjlasd+ajflksadjmoreunreadablestringasdfdfkdjksdjaa
sdfas"
agent-key-id:
 b4ac2ab4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4ac2b4a
```

Hinweis: Der Befehl *grep* muss in einer einzelnen Zeile stehen.

3. Zeigen Sie die Verbindung des Service Desk-Mitarbeiters mit der Back-End-URL an, indem Sie den Befehl `grep 'successful Connected' /var/log/servicenow/agent-client-collector/acc.log` ausführen.

```
# grep 'successfully
 connected' /var/log/servicenow/agent-client-collector/acc.log
2022-11-17T19:03:17.94 [INFO] [agent] successfully connected to the
 url:
wss://MY_BACKEND_FQDN:MY_BACKEND_PORT/ws/events
```

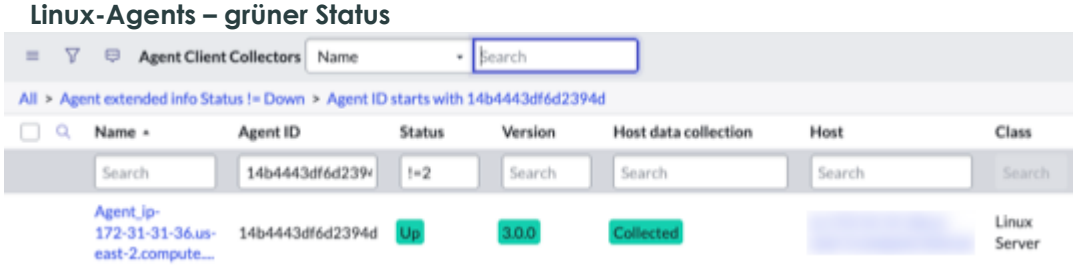
Hinweis: Der Befehl *grep* muss in einer einzelnen Zeile stehen.

4. Überprüfen Sie die eindeutige Agent-ID, indem Sie den Befehl `# reflekt $(hexdump -e '/1 "%02x"'/var/cache/servicenow/agent-client-collector/agent_now_id)` ausführen.

```
# echo $(hexdump -e '/1
 "%02x"' /var/cache/servicenow/agent-client-collector/agent_now_id)
14b4443df6d2394d
```

Die angegebene Agent-ID wird auf der Seite „Service Desk-Mitarbeiter“ in einer Instanz () angezeigt.**Alle** > **Agent Client Collector** > **Agents**) mit **Status = In Betrieb** und **Hostdatensammlung = Gesammelt** (beide grün angezeigt).

Linux-Agents – grüner Status



Führen Sie ein Upgrade Agent Client Collector von auf einem Linux -System durch

Aktualisieren Sie Ihre vorhandene Version Agent Client Collector auf einem System mit einem Linux-Betriebssystem, wenn das einzeilige Befehlsskript nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen verwenden möchten.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wahlweise: Sichern Sie vertrauliche Dateien, indem Sie den folgenden Befehl ausführen.

```
tar
 -cvzf /root/acc_backup.tar.gz /etc/servicenow/agent-client-collector \
/var/cache/servicenow/agent-client-collector/agent_now_id \
/usr/lib/systemd/system/acc.service
```

2. Laden Sie das .rpm/.deb-Agent-Paket und die Signaturdateien wie in Installieren Sie Agent Client Collector auf einem Linux -Systembeschrieben herunter.
3. Aktualisieren Sie das Paket.
   - In einem RPM-basierten System:

     ```
     U/min – Uv agent-client-sammler-<version number> -x86_64.rpm
     ```

   - In einem DEB-basierten System:

     ```
     dpkg -i agent-client-collector-<version number> -<distro> _amd64.deb
     ```

4. Stellen Sie die Systemd-Servicedatei wieder her (wenn Sie die Datei angepasst haben), indem Sie entweder ein Automatisierungstool verwenden oder die Systemd-Konfiguration neu laden.

```
tar -C / -xvzf /root/acc_backup.tar.gz
 usr/lib/systemd/system/acc.service \
/usr/lib/systemd/system/acc.servicesystemctl daemon-reload
```

5. Ändern Sie die Einstellung *owner:group* in die richtige Einstellung, indem Sie den folgenden Befehl ausführen.

```
chown -R
 sn_acc:sn_acc /
{etc,var/cache,var/log,usr/share}/servicenow/agent-client-collector
```

6. Starten Sie den Service neu, und vergewissern Sie sich, dass eine Verbindung zu seiner Back-End-URL hergestellt wird.

```
systemctl restart acc
grep -i successfully /var/log/servicenow/agent-client-collector/acc.log
2022-11-17T19:32:24.25 [INFO] [agent] successfully connected to the
 url: wss://YOUR_BACKEND_FQDN:YOUR_BACKEND_PORT/ws/events
```

Deinstallieren Sie Agent Client Collector aus einem Linux -System

Deinstallieren Sie Agent Client Collector manuell von einem Linux-Computer, wenn das Befehlsskript nicht verfügbar ist, weil der bestimmte Agent nicht mit der Instanz verbunden ist.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig wird ein deinstallierter Agent nach 30 Tagen aus dem System entfernt. Um diese Zeitspanne zu ändern, aktualisieren Sie die Tabelle *sn_agent_ci_extended_info*, auf die über die Seite Automatisch entleeren zugegriffen werden kann (geben Sie in das Suchfilterfeld der Instanz *sys_auto_flush.LIST* ein).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Halten Sie den Service an.
   `sudo systemctl stop acc`
2. Verwenden Sie das entsprechende Paketverwaltungstool, um den Service zu entfernen.
   - yum „agent-client-collector“ entfernen
   - apt-get zum Entfernen von „agent-client-collector“.
   - Zypper-Entferner „agent-client-collector“.

   Alternativ können Sie je nach verwendetem Betriebssystem einen der folgenden Befehle ausführen.

   - `U/min -e agent-client-collector`
   - `dpkg -r agent-client-collector`
3. Wenn Sie entweder den Befehl `„rpm“` oder `„dpkg“` ausgeführt haben, entfernen Sie alle verbleibenden Dateien aus Ihrem System.

```
# userdel -r servicenow
# groupdel servicenow
# rm
 -R /
{etc,var/cache,var/log,usr/share}/servicenow/agent-client-collector
```

Warnung: Verwenden Sie nicht den Befehl rm -Rf, da dies zu Datenverlust führen kann.

Einzeilige Agent Client Collector-Installation unter Linux

Verwenden Sie ein effizientes einzeiliges Befehlsskript, um Agent Client Collector auf einem Computer mit Linux-Betriebssystem zu installieren. Wenn ein Skript nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen verwenden möchten, müssen Sie Agent Client Collector möglicherweise manuell installieren.

Vorbereitungen

- Stellen Sie sicher, dass Sie den Agent Client Collector-Webserver konfiguriert haben.
- Vergewissern Sie sich, dass Betriebssystem und Version Ihres Servers mit der Liste der unterstützten Betriebssystemversionen in Installation von Agent Client Collector übereinstimmen.
- Bestimmen Sie die Ressourcengrenzen für den Agent, der nach der Installation in der Datei `/usr/lib/systemd/system/acc.service` konfiguriert werden soll.
- Stellen Sie sicher, dass Ihnen die Pakete `openssl` und `dgst` (für eine RHEL-/CentOS-/SUSE-Installation) sowie `dpkg-sig` und `dgst` (für Ubuntu-/Debian-Installationen) zur Verfügung stehen, die vom Installationsskript verwendet werden.
- Wenn Sie eine einzeilige Installation für mehr als einen Agent durchführen, laden Sie das Agent-Paket auf Ihren lokalen Computer herunter. Platzieren Sie das Paket mit einem Ansible-Skript auf Ihrem *FTP*-Server. Weitere Informationen zur Massenbereitstellung von Agents finden Sie unter Agent Client Collector zur Massenbereitstellung in benutzerdefiniertes Basis-Image einbinden.
- Damit der Agent die Betriebssystem-Seriennummern und TCP-Verbindungen mit zugehörigen laufenden Prozessen abrufen kann, ist auf Linux-Systemen sudo-Zugriff für „dmidecode“ und „ss“ erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Rufen Sie die Websocket-URL-Parameter des MID-Servers ab.
   a. Navigieren zu **Agent Client Collector** > **Websocket-Endpunkt** und wählen Sie den entsprechenden Websocket-Endpunkt aus.
   b. Kopieren Sie den Wert des Felds **Endpunkt-URL**, der im Installationsbefehl verwendet werden soll.
2. Kopieren und bearbeiten Sie die folgende Befehlszeile, und ersetzen Sie die Befehlsparameter durch Ihre eigenen Informationen.

```
ACC_API_KEY=<api_key> ACC_MID=wss://<mid_ip>:<websocket_port>/
ws/events bash -c "$(curl -L https://<instance URL>/api/sn_agent/agents/
install_agent)"
```

Befehlsparameter

Parameter	Wert
ACC_API_KEY	API-Schlüssel, der für den Zugriff auf den MID-Server-Websocket verwendet wird Wenn kein ACC_API_KEY-Wert angegeben ist, werden Sie während der Ausführung des Skripts aufgefordert, den API-Schlüsselwert einzugeben.
ACC_MID	URL des MID-Server-Websocket Wenn Sie mehrere MID Serversangeben, geben Sie für jedes MID-Servereine durch Kommas getrennte Zeichenfolge ein.

3. Wahlweise: Wenn Sie neue Prüfdefinitionen erstellen müssen, die in die Allow-Liste aufgenommen werden sollen, die angibt, welche Prüfungen für den Agent aktiviert sind, deaktivieren Sie die Allow-Liste, indem Sie *ACC_ALLOW_LIST=0* zur einzeiligen Befehlszeichenfolge hinzufügen.

   Hinweis: Diese Aktion beeinträchtigt die Sicherheit Ihres Systems und wird nur als vorübergehende Maßnahme empfohlen, bis Sie die Aktualisierung der Allow-Liste abgeschlossen haben. Nach der Aktualisierung aktivieren Sie die Allow-Liste erneut, indem Sie *ACC_ALLOW_LIST=0* aus der einzeiligen Befehlszeichenfolge entfernen.

4. Wahlweise: Wenn der Zertifikatvalidierungsprozess zu zeitaufwendig ist oder Sie den Agent für Entwicklungszwecke verwenden, können Sie die Zertifikatvalidierung umgehen, indem Sie der einzeiligen Befehlszeichenfolge *ACC_VALIDATE_SIG=0* hinzufügen.
5. Führen Sie den einzeiligen Befehl (oben in Schritt 2angegeben) auf dem Server aus, auf dem Agent Client Collector installiert ist.
6. Wahlweise: Konfigurieren Sie Ressourcengrenzen für den Agent in der Datei `/usr/lib/systemd/system/acc.service` entsprechend Ihren Geschäftsanforderungen.

   (Optional) Die Standardwerte in der Datei sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *CPUShares*: 128
- *CPUQuota*: 10 %
- *MemoryLimit*: 192M
- *BlockIOWeight*: 10
- *LimitNICE*: +15

Manuelles Upgrade von Agent Client Collector unter Linux

Führen Sie auf einem System mit Linux-Betriebssystem ein manuelles Upgrade Ihrer vorhandenen Agent Client Collector-Version durch, wenn das einzeilige Skript nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen verwenden möchten.

Vorbereitungen

- Stellen Sie sicher, dass Sie den Agent Client Collector-Webserver konfiguriert haben. Weitere Informationen finden Sie unter Websocket-Server auf MID-Server installieren.
- Stellen Sie sicher, dass Sie eine Linux-Version von Agent Client Collector installiert haben. Weitere Informationen finden Sie unter Agent Client Collector-Installation unter einem Linux-Betriebssystem.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Sichern Sie die `Agent-ID` und die Konfigurationsdateien.

```
mkdir -p /tmp/acc-upgrade-backup
sudo cp
 -rp /etc/servicenow/agent-client-collector/acc.yml /
tmp/acc-upgrade-backup
sudo cp
 -rp /etc/servicenow/agent-client-collector/check-allow-list.json /
tmp/acc-upgrade-backup
sudo cp
 -rp /var/cache/servicenow/agent-client-collector/agent_now_id /
tmp/acc-upgrade-backup
```

2. Deinstallieren Sie das Paket.

   a. Halten Sie den Service an.
   `sudo systemctl stop acc`

   b. Deaktivieren Sie den Service.
   `sudo systemctl disable acc`

   c. Deinstallieren Sie das Paket:
   - Für RHEL/CentOS/SUSE: `ssudo rpm -e agent-client-collector`
   - Für Ubuntu/Debian: `sudo dpkg -r agent-client-collector`

3. Laden Sie die Installationsdatei herunter.
   Wenn Sie beispielsweise mit einem Ubuntu-/Debian-Betriebssystem arbeiten, verwenden Sie die beiden folgenden Befehle:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
curl -L -O https://install.service-now.com/glide/distribution/builds/
package/app-signed/agent-client-collector-<version number>-<Ubuntu/Debian
version>_amd64-deb-deb.zip -O

https:/install.service-now.com/glide/distribution/builds/package/app-
signed/agent-client-collector/agent-client-collector-<version number>-
<Ubuntu/Debian version>_amd64.deb
```

4. Verifizieren und installieren Sie das Paket.
   a. Extrahieren Sie die komprimierte Datei.

   ```
   unzip agent-client-collector-2.3.0-debian-9_amd64-deb-deb.zip
   ```

   b. Validieren Sie die Signatur der Installationsdatei.
      - RHEL/CentOS/SUSE:

      ```
      openedsl dgst -sha256 -verify {<ServiceNow DGST pem key> } -Signatur
      {<signature file> } agent-client-sammler-<version number> -x86_64.rpm
      ```

      - Ubuntu/Debian:

      ```
      gpg --import ServiceNow_Digicert_Public.gpg
      dpkg-sig --verify agent-client_collector-<version
       number>-<Ubuntu/Debian version>_amd64.deb
      ```

   c. Installieren Sie das Paket.
      - RHEL/CentOS/SUSE: `sudo-rpm -vi --force agent-client-collector-`<version number> -x86_64.rpm
      - Ubuntu/Debian: `sudo dpkg -1 agent-client-collector-<version number>-<Ubuntu/Debian version>_amd64.deb`
5. Stellen Sie `Agent-ID` und Konfigurationsdateien wieder her.

```
sudo -u servicenow cp
 -rp /tmp/acc-upgrade-backup/acc.yml /
etc/servicenow/agent-client-collector/acc.yml
sudo -u servicenow cp
 -rp /tmp/acc-upgrade-backup/check-allow-list.json /
etc/servicenow/agent-client-collector/check-allow-list.json
sudo -u servicenow cp
 -rp /tmp/acc-upgrade-backup/agent_now_id /
var/cache/servicenow/agent-client-collector/agent_now_id
```

6. Konfigurieren Sie den Agent so, dass er als Dienst ausgeführt wird.
   `sudo systemctl enable acc`
7. Starten Sie den Dienst.
   `sudo systemctl start acc`
8. Zeigen Sie die Protokolle an, um zu überprüfen, ob der Start erfolgreich war.
   `sudo tail -f /var/log/servicenow/agent-client-collector/acc.log`

Agent Client Collector unter Linux mit einzeiligem Befehl deinstallieren

Deinstallieren Sie Agent Client Collector auf einem Linux-Computer, indem Sie einen effizienten einzeiligen Befehl ausführen. Wenn das Skript nicht mit der Instanz verbunden ist, müssen Sie Agent Client Collector möglicherweise manuell deinstallieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur

Deinstallieren Sie Agent Client Collector, indem Sie den folgenden Befehl in einem Befehlsfenster ausführen, wobei `<agent url>` die URL der ServiceNow-Instanz ist.
`bash -c "$(curl -L https://<agent url>/api/sn_agent/agents/install_agent)" -s "--remove"` .

Hinweis: Bei der Deinstallation von Agent Client Collector werden die Datei `acc.yml` und das zugehörige Verzeichnis von Ihrem Computer entfernt.

Agent Client Collector -Installation auf einem Windows -Computer

Wenn Sie Agent Client Collector auf einem Computer Windows vom Typ installieren, laden Sie entweder eine Installationsdatei herunter, und verwenden Sie einen Assistenten, um den Agent manuell zu installieren, oder verwenden Sie eine unbeaufsichtigte Installation, um die Installation und Konfiguration des Agent zu automatisieren. Mithilfe der manuellen Installation können Sie den Agent auf einem einzelnen System testen, während Sie mit der unbeaufsichtigten Installation den Agent bedarfsgerecht bereitstellen können.

Installieren Sie Agent Client Collector manuell auf einem Computer Windows .

Installieren Sie Agent Client Collector manuell auf einem Computer Windows, wenn Sie den Agent auf einem einzelnen System testen möchten.

Vorbereitungen

1. Vergewissern Sie sich, dass der Webserver Agent Client Collector konfiguriert wurde. Details finden Sie unter Websocket-Server auf MID-Server installieren.
2. Überprüfen Sie Betriebssystem und Version Ihres Servers.
3. Wenn Sie MicrosoftMicrosoft Azure Event Hubs Internet Explorer verwenden, gehen Sie wie folgt vor, um die Agent Client Collector-Installationsdatei vorzubereiten:
   a. Navigieren zu **Servermanager** > **Lokaler Server**.
   b. Deaktivieren Sie **Verstärkte Sicherheitskonfiguration für IE**.
   c. Laden Sie die Installationsdatei herunter.
   d. Ändern Sie die Erweiterung der Installationsdatei von `.man` in `.msi`.

Erforderliche Rolle: agent_client_collector_admin

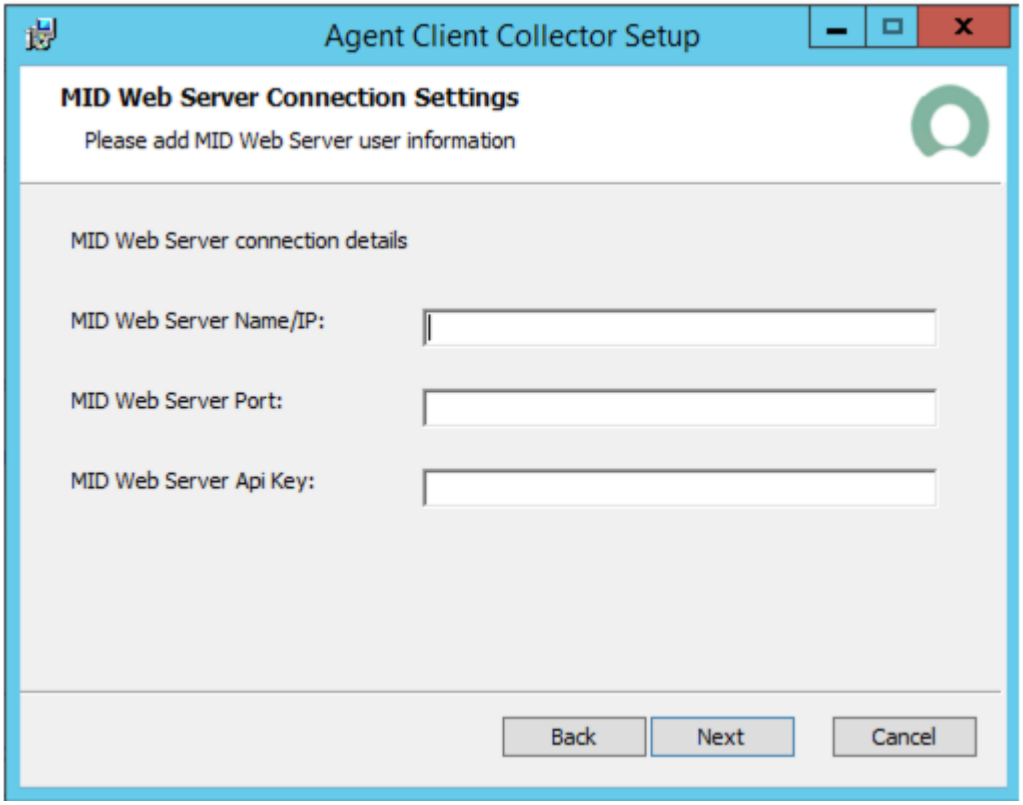
Prozedur

1. Navigieren zu **Agent Client Collector** > **Agent-Downloads**.
2. So führen Sie die Installation mit dem Assistenten durch:

   a. Laden Sie die .msi-Datei herunter, auf die über den Link in der Benutzeroberfläche zugegriffen werden kann.
   Der Installationsassistent wird geöffnet.

   b. Wählen Sie **Weiter** aus, bis Sie die Seite **MID-Webserver-Verbindungseinstellungen** erreichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Geben Sie in die Felder des Dialogfelds die relevanten Parameter ein:

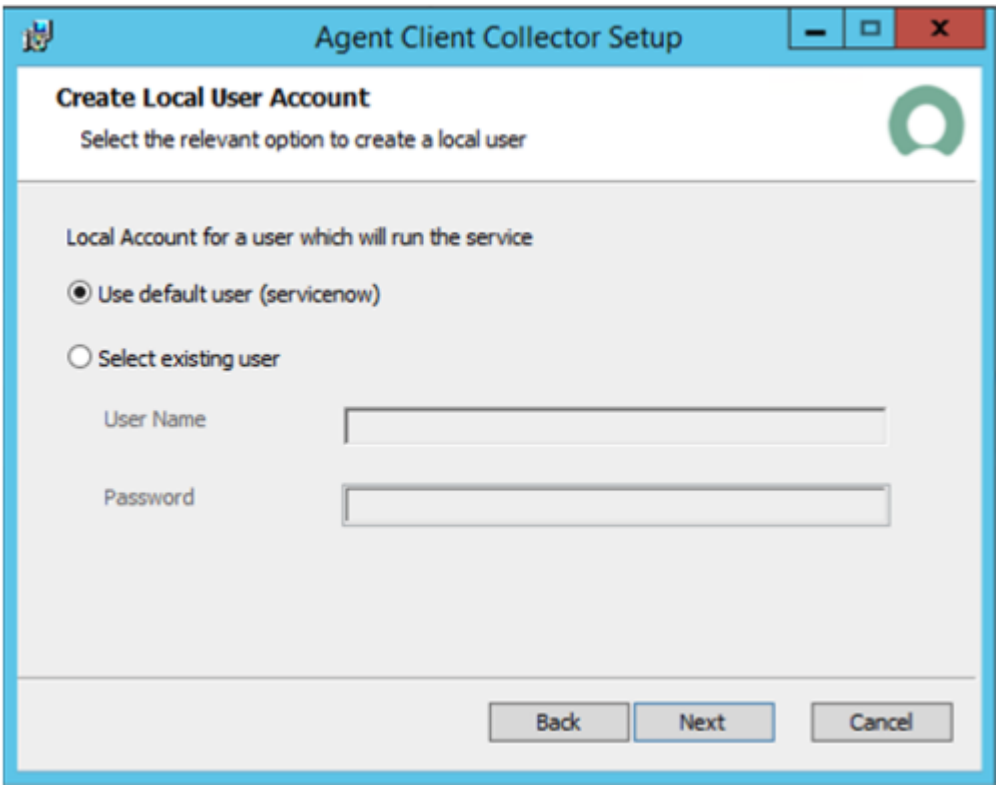
Felder für MID-Webserver-Verbindungseinstellungen

Feldname	Beschreibung
MID Web Server Name/IP (Name/IP des MID-Webservers)	IP-Adresse des MID-Webservers
MID Web Server Port (Port des MID-Webservers)	Portnummer des MID-Webservers. Verwenden Sie eine Zahl zwischen 1024 und 49151.
MID Web Server API Key (API-Schlüssel des MID-Webservers)	API-Schlüssel für den Zugriff auf den MID-Webserver

d. Wählen Sie **Weiter**.
Die Seite **Create Local User Account** (Lokales Benutzerkonto erstellen) wird angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Wählen Sie im Dialogfeld die relevante Option aus.

Dialogfeld „Create Local User Account“ (Lokales Benutzerkonto erstellen)

Optionen	Beschreibung
Use default user (servicenow) (Standardbenutzer (servicenow) verwenden)	Standardbenutzer, mit dem Agent Client Collector auf einem Windows-Computer ausgeführt werden soll Wenn Sie diese Option auswählen, wird ein lokaler Anwender namens **„servicenow“** als Teil der Installation erstellt. Das ServiceNow-Anwenderpasswort wird nach dem Zufallsprinzip generiert und nicht im System gespeichert. Auf dem Hostcomputer wird ein Sicherheitsereignis erstellt, das bei Wiederholung das Öffnen eines Supportfalls erfordert. Weitere Informationen finden Sie im Artikel KB1649116 in der HI Knowledge Base.
Select existing user (Vorhandenen Benutzer auswählen)	Wenn Sie diese Option auswählen, konfigurieren Sie die folgenden Unterfelder: ▪ **User Name** (Benutzername): Benutzername zum Anmelden bei der Windows-Umgebung ▪ **Password**: (Passwort) Kennwort des ausgewählten Benutzers

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionen	Beschreibung
	Der Benutzer kann einer der folgenden sein: ▪ Lokaler Anwender (vom Besitzer der VM erstellt; bietet zusätzliche Resilienz). ▪ Domänenbenutzer (von IT-Mitarbeitern erstellt). ▪ Von der Gruppe verwalteter Serviceaccount (gMSA): Geben Sie den Namen des von der Gruppe verwalteten Serviceaccounts in das Feld **Anwendername** ein, und lassen Sie das Feld **Passwort** leer. ▪ Lokaler Serviceaccount: Geben Sie *LOCALSERVICE* im Feld **Anwendername** ein, und lassen Sie das Feld **Passwort** leer. ▪ Lokales Systemkonto: Geben Sie *SYSTEM* im Feld **Anwendername** ein, und lassen Sie das Feld **Passwort** leer.

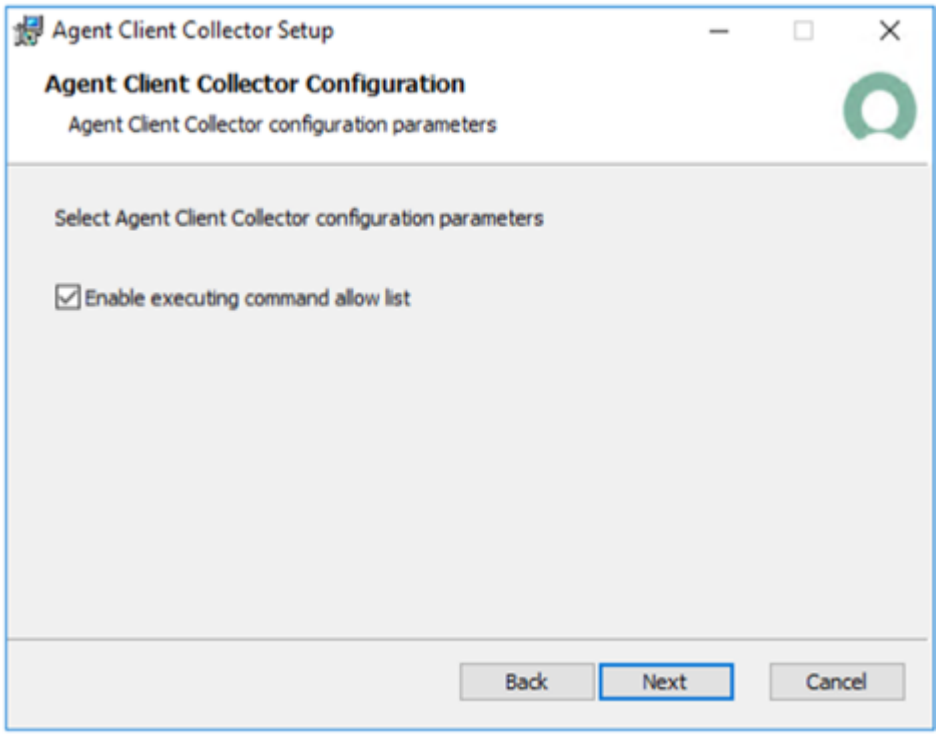
Hinweis: Wenn Sie ein lokales Systemkonto verwenden, wird die lokale Gruppe *ServiceNow Users* erstellt und der erstellte Benutzer wird der Gruppe hinzugefügt. Die ServiceNow-Anwendergruppe hat Zugriff auf die Verzeichnisse Agent Client Collector und verfügt über die folgenden Berechtigungen:

- **Performance Monitor**: Gehört zum Lieferumfang des Basissystems; ermöglicht die Anzeige aller Leistungszähler im System
- **Als Service anmelden**: Ermöglicht das Starten von Netzwerkservices und Services, die kontinuierlich ausgeführt werden, auch wenn niemand bei der Konsole angemeldet ist.
- **Programme debuggen**: Aktiviert Debugging-Prozesse und das Lesen von Prozessdetails für Benutzer außerhalb der Benutzergruppe ServiceNow.

f. Wählen Sie **Anwender erstellen aus**.
Im System wird ein Windows-Benutzer mit den angegebenen Anmeldeinformationen erstellt, und die Seite „Agent Client Collector Configuration“ (Agent Client Collector – Konfiguration) wird angezeigt.

g. Um die **Allow-Liste** mit den aktivierten Prüfungen zur Ausführung nach der Einrichtung zu aktivieren, aktivieren Sie auf der daraufhin angezeigten Seite das Kontrollkästchen **Enable executing command allow list** (Ausführungsbefehl für Allow-Liste aktivieren).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



h. Wählen Sie **Weiter** aus, um die Installationsseite zu öffnen.

Wenn die Installation abgeschlossen ist, klicken Sie auf **Weiter**, um den Assistenten zu beenden und zu schließen.

Nach einer erfolgreichen Installation startet der Service automatisch und generiert Folgendes:

- Benutzer: Standard = servicenow (Zur Verwaltung des Service kann auch ein vorhandener Benutzer konfiguriert werden.) Der Benutzer servicenow gehört zur lokalen Benutzergruppe der **ServiceNow-Benutzer**.
- Service: AgentClientCollector
- Dateispeicherort:
  - Standard für Installation = `C:\Programme\ServiceNow\agent-client-collector`
  - Standard für Servicedateien = `C:\ProgramData\ServiceNow\agent-client-collector`, enthält die Ordner „`cache`", „`config`"und „`log`".

3. Wenn Sie die automatische Installation ausführen möchten, um Installationsberichte zu deaktivieren, führen Sie die Befehlszeile im Abschnitt **Silent installation** (Automatische Installation) des Verfahrens wie folgt aus:

```
msiexec /i <msi_file_path> /quiet /qn /norestart ACC_API_KEY=<key_value>
ACC_MID=wss://<mid_ip>:<websocket_port>/ws/events ACC_ALLOW_LIST=False
```

Um die Allow-Liste der angegebenen Prüfungen beim Ausführen der automatische Installation zuzulassen, setzen Sie den Parameter *`ACC_ALLOW_LIST`* auf **True**.

4. Um mehrere MID Servers mit der unbeaufsichtigten Installation zu konfigurieren, führen Sie die Befehlszeile, die im Abschnitt **Unbeaufsichtigte Installation** des Verfahrens angezeigt wird, mit durch Kommas getrennten Werten wie folgt aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
msiexec /i <msi_file_path> /quiet /qn /norestart ACC_API_KEY=<key_value>
ACC_MID="wss://<mid1_ip>:<websocket1_port>/ws/events,wss://
<mid2_ip>:<websocket2_port>/ws/events"
```

Fügen Sie die folgenden Parameterwerte in den Befehl ein:

Befehlsparameter

Parameter	Wert
ACC_API_KEY	API-Schlüssel, der für den Zugriff auf den MID-Server-Websocket verwendet wird
ACC_MID	URL des MID-Server-Websocket
DENY_LOCAL_LOGON	Wenn dies auf *True* festgelegt ist, wird verhindert, dass sich andere Anwender als der standardmäßige ServiceNow-Anwender beim Service anmelden. Standardwert: False
PASSWORD_NEVER_expires	Wenn es auf *True* festgelegt ist, läuft das Passwort für den ServiceNow-Standardanwender nie ab. Standardwert: False
START_SERVICE	Wenn dies auf *True* festgelegt ist, wird der Service Agent Client Collector nach der Installation automatisch gestartet. Standardwert: True
LOKALER ANWENDERNAME	Account, der Agent Client Collector als Service Windows ausführt. Mögliche Werte: ◦ SYSTEM ◦ LOCAL SERVICE ◦ DOMÄNE\gMSA$ ◦ Zeichenfolge (lokaler Anwendername) Standard = `servicenow` Wenn Sie die Konten SYSTEM, LOCALSERVICE oder DOMAIN\gMSA $verwenden, müssen Sie kein Passwort konfigurieren.
LOCALPASSWORD	Passwort für den im Parameter LOCALUSERNAME angegebenen Anwender.

Die konfigurierten MID-Server-Werte werden automatisch der Datei `acc.yml` hinzugefügt. Der Agent stellt eine Verbindung zum ersten verfügbaren MID-Server in der Liste her.

Um einen sekundären MID Server zu konfigurieren, geben Sie im Abschnitt `backend-url` der Datei `acc.yml` die folgende Syntax gemäß `.yml`-Standard ein: – `"wss://<MID IP>:<Web socket port>/ws/events"` (mit Anführungszeichen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Manuelles Upgrade von Agent Client Collector auf einem Windows-System

Führen Sie ein manuelles Upgrade Ihrer vorhandenen Agent Client Collector-Version auf einem Windows-Betriebssystem durch.

Vorbereitungen

Sichern Sie die Konfigurationsdateien Agent Client Collector, z. B. `acc.yml`, `check-allow-list.json`, `agent_now_id` und `agent_now_keystore`. `agent_now_id` befindet sich im Cache-Verzeichnis: `C:\ProgramData\Servicenow\agent-client-collector\cache`

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Drücken Sie die Windows-Taste auf Ihrer Tastatur, und geben Sie **Dienste** ein, um die Services-Seite zu öffnen.
2. Suchen Sie den Agent Client Collector-Dienst.
3. Klicken Sie mit der rechten Maustaste auf den Agent Client Collector-Dienst und wählen Sie **Anhalten** aus.
4. Wählen Sie in der Windows-Systemsteuerung die Option **Programm deinstallieren** aus.
5. Wählen Sie das Agent Client Collector-Programm und anschließend **Deinstallieren** aus.
6. Navigieren zu **Agent Client Collector** > **Agent-Downloads** und laden Sie das MSI-Installationsprogramm im **Windows-Downloadbereich** herunter.
7. Installieren Sie den neuen Agent, wie in Installieren Sie Agent Client Collector manuell auf einem Computer Windows . beschrieben.
   Sie können entweder das manuelle oder das einzeilige Verfahren verwenden.
   Beim Wiederherstellen von Sicherungsdateien ersetzt das System die Werte der Konfigurationsdatei.
8. Halten Sie den Dienst nach Abschluss der Installation an.
9. Stellen Sie die `agent_now_id`- und `agent_now_keystore`-Konfigurationsdateien wieder her.
10. Starten Sie den Agent Client Collector-Dienst neu.

Agent Client Collector manuell von einem Windows-Computer deinstallieren

Anstatt mit dem einzeiligen Befehl können Sie Agent Client Collector auf einem Windows-Computer auch manuell deinstallieren. Nutzen Sie das manuelle Verfahren, wenn das Befehlsskript nicht verfügbar ist, weil der entsprechende Agent nicht mit der Instanz verbunden ist.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

Deinstallieren Sie Agent Client Collector in der Systemsteuerung Windows.

Installieren Sie Agent Client Collector auf Windows mithilfe von ITOM Cloud Services

Installieren Sie Agent Client Collector auf einem Computer vom Typ Windows ohne MID-Server mithilfe von ITOM Cloud Services. Wenn Sie Informationen über die Cloud senden, aktivieren Sie die MID-Server für persistentere Ressourcen.

Vorbereitungen

Installieren Sie das Plugin ITOM „ Cloud Services.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Agent-Registrierungsschlüssel, wie in Konfigurieren Sie einen Agent-Registrierungsschlüsselbeschrieben.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zur Arbeit mit Cloud-Services finden Sie unter DEX-Architektur .

Prozedur

1. Rufen Sie die öffentlich zugängliche Gateway-URL basierend auf Ihrem Standort ab:
   - AMER (Amerika): `itomcnc-prod-gateway.amer.sncapps.service-now.com:443`
   - EMEA (Europa): `itomcnc-prod-gateway.emea.sncapps.service-now.com:443`
   - APAC (Asien-Pazifik): `itomcnc-prod-gateway.apac.sncapps.service-now.com:443`
2. Geben Sie auf dem Server Windows, auf dem der Agent installiert ist, den folgenden Befehl ein:

```
msiexec /i <msi_file_path> /quiet /qn /norestart
 CONNECT_WITHOUT_MID="true" ACC_CNC="<gateway_endpoint>"
 REGISTRATION_KEY="<registration_key>"
 INSTANCE_URL="https://<instance_url>"
```

3. Die folgende Tabelle zeigt die Parameterwerte im Befehl.

Befehlszeilenparameterwerte

Parameter	Wert
VERBINDEN_OHNE_MID	Geben Sie **„wahr“** an, um ITOM Cloud-Services (**wahr**) zu aktivieren. Wenn Sie keinen Wert angeben, wird die reguläre Websocket-Installation MID-Server aufgerufen. Einzelheiten zur Konfiguration eines Websocket auf dem MID-Serverfinden Sie unter Websocket-Server auf MID-Server installieren.
ACC_CNC	Öffentlicher Gateway-Endpunkt für Agent Client Collector, den Sie angeben können.
REGISTRATION_KEY	Aktiver und gültiger Agent-Registrierungsschlüssel, mit dem der Agent kommunizieren soll.
INSTANCE_URL	ServiceNow Instanz, bei der sich der Service Desk-Mitarbeiter registriert

Installieren Sie Agent Client Collector auf einem Computer Windows mithilfe der unbeaufsichtigten Installation

Installieren Sie Agent Client Collector auf einem Computer Windows, indem Sie eine unbeaufsichtigte Installation verwenden, wenn Sie den Agenten bedarfsgerecht bereitstellen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Die unbeaufsichtigte Installation erstellt automatisch einen lokalen Anwender namens **servicenow** (es sei denn, ein anderer vorhandener Anwender wird mit dem Parameter *LOCALUSERNAME* aufgerufen, wie in der Tabelle mit den Befehlsparametern im folgenden Verfahren beschrieben). Das ServiceNow-Anwenderpasswort wird nach dem Zufallsprinzip generiert und nicht im System gespeichert. Auf dem Hostcomputer wird ein Sicherheitsereignis erstellt, das bei Wiederholung das Öffnen eines Supportfalls erfordert. Weitere Informationen finden Sie im Artikel KB1649116 in der HI Knowledge Base.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Um eine unbeaufsichtigte Installation zum Deaktivieren von Installationsberichten auszuführen, führen Sie die Befehlszeile aus, die im Abschnitt **„Beaufsichtigte Installation“** des Verfahrens angezeigt wird, wie folgt:

   ```
   msiexec /i <msi_file_path> /quiet /qn /norestart ACC_API_KEY=<key_value>
   ACC_MID=wss://<mid_ip>:<websocket_port>/ws/events ACC_ALLOW_LIST=False
   ```

   Um die Allow-Liste der angegebenen Prüfungen bei der Ausführung der unbeaufsichtigten Installation zu aktivieren, legen Sie den Parameter *ACC_ALLOW_LIST* auf den **Wert true** fest.

2. Um mit der automatische Installation mehrere MID Servers zu konfigurieren, führen Sie die Befehlszeile im Abschnitt **Silent installation** (Automatische Installation) des Verfahrens wie folgt mit kommagetrennten Werten aus:

   ```
   msiexec /i <msi_file_path> /quiet /qn /norestart ACC_API_KEY=<key_value>
   ACC_MID="wss://<mid1_ip>:<websocket1_port>/ws/events,wss://
   <mid2_ip>:<websocket2_port>/ws/events"
   ```

   Fügen Sie die folgenden Parameterwerte in den Befehl ein:

Befehlsparameter

Parameter	Typ	Wert
ACC_API_KEY	Zeichenfolge	API-Schlüssel, der für den Zugriff auf den MID-Server-Websocket verwendet wird
ACC_MID	Zeichenfolge	URL des MID-Server-Websocket
ACC_ALLOW_LIST	Boolean	Gibt an, ob die Allow-Liste aktiviert (wahr) oder deaktiviert (falsch) ist. Standard = Wahr
START_SERVICE	Boolean	Gibt an, ob der Agent bei der Installation automatisch gestartet wird (wahr) oder manuell gestartet werden muss (falsch). Standard = Wahr
LOKALER ANWENDERNAME	Zeichenfolge	Account, der Agent Client Collector als Service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Typ	Wert
		Windows ausführt. Mögliche Werte: ◦ SYSTEM ◦ LOCAL SERVICE ◦ DOMÄNE\gMSA$ ◦ Zeichenfolge (lokaler Anwendername) Standard = `servicenow` Bei Verwendung der Konten SYSTEM, LOCALSERVICE oder DOMAIN\gMSA$: ◦ Sie müssen kein Passwort konfigurieren. ◦ Sie müssen den entsprechenden .msi-Befehl ausführen (siehe Account-Befehle für LocalService, LocalSystem und gMSA während der Installation Windows von [].) .
LOKALES ANWENDERPASSWORT	Zeichenfolge	Passwort, das für den Zugriff auf den Agent verwendet wird. Standard =<randomly generated password>
ISDOMAIN	Boolean	Weist dem Service Windows ein Domänen-Benutzerkonto zu. Mögliche Werte: ◦ 0: DOMÄNE wird ignoriert ◦ 1: DOMÄNE wird verwendet
DOMAIN	Zeichenfolge	Gibt die Benutzerdomäne an. Gilt nur für Domänen-Anwenderaccounts (nicht gMSA)
PASSWORD_NEVER_expires	Boolean	Gibt an, ob das Anwenderpasswort abläuft (falsch) oder nie abläuft (wahr). Standard = falsch

Die konfigurierten MID-Server-Werte werden automatisch der Datei `acc.yml` hinzugefügt. Der Agent stellt eine Verbindung zum ersten verfügbaren MID-Server in der Liste her.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um einen sekundären MID Server zu konfigurieren, geben Sie im Abschnitt `backend-url` der Datei `acc.yml` die folgende Syntax gemäß `.yml`-Standard ein: – `"wss://<MID IP>:<Web socket port>/ws/events"` (mit Anführungszeichen).

Für<MID IP> Wert festgelegt ist, können Sie entweder den MID-FQDN oder den CNAME zuweisen. Um Hochverfügbarkeit zu ermöglichen, verwenden Sie entweder den Algorithmus für die automatische MID-Auswahl, oder verwalten Sie eine virtuelle IP mit einem Lastenausgleichsmodul. Weitere Informationen finden Sie im Artikel mit der Dokumentation zu ITOM Agent Client Collector [KB1122613] in der HI Knowledge Base.

Agent Client Collector unter einem Windows-System mit einzeiligem Befehl deinstallieren

Deinstallieren Sie Agent Client Collector auf einem Windows-Computer, indem Sie einen effizienten einzeiligen Befehl ausführen. Wenn das Skript nicht mit der Instanz verbunden ist, müssen Sie Agent Client Collector möglicherweise manuell deinstallieren.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

Deinstallieren Sie Agent Client Collector, indem Sie den folgenden Befehl in einem Befehlsfenster ausführen.
`msiexec /quiet /x <path_to_acc_msi_file>`.

Hinweis: Bei der Deinstallation von Agent Client Collector werden die Datei `acc.yml` und das zugehörige Verzeichnis von Ihrem Computer entfernt.

Agent Client Collector-Installation unter einem macOS-Betriebssystem

Installieren Sie Agent Client Collector auf einem System, auf dem macOS verwendet wird. Sie können entweder ein einzeiliges Befehlsskript verwenden oder eine manuelle Installation durchführen, wenn der Agent nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen wünschen.

Um privilegierten Zugriff auf Informationen im System macOS zu ermöglichen, fügen Sie der Administratorgruppe (oder einem entsprechenden System) das Benutzerkonto *_servcienow* hinzu.

Die Einbindung von Agent Client Collector in ein benutzerdefiniertes Basis-Image zur Massenbereitstellung wird unter macOS nicht unterstützt.

Einzeilige Agent Client Collector-Installation unter macOS durchführen

Verwenden Sie ein effizientes einzeiliges Befehlsskript, um Agent Client Collector auf einem Computer mit macOS-Betriebssystem zu installieren. Nehmen Sie eine manuelle Installation vor, wenn der Agent nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen wünschen.

Vorbereitungen

- Stellen Sie sicher, dass Sie den Agent Client Collector-Webserver konfiguriert haben.
- Vergewissern Sie sich, dass Betriebssystem und Version Ihres Servers mit der Liste der unterstützten Betriebssystemversionen in Installation von Agent Client Collector übereinstimmen.
- Stellen Sie sicher, dass Sie die *pkgutil*-Pakete zur Verfügung haben, die vom Installationsskript verwendet werden.
- Stellen Sie sicher, dass die Ziel-Agents über Folgendes verfügen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ServiceNow-Installationsserver [install.service-now.com]
- ServiceNow instance
- MID-Server, mit dem der Agent eine Verbindung herstellt

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Rufen Sie die Websocket-URL-Parameter des MID-Server ab.
   a. Navigieren zu **Agent Client Collector** > **Websocket-Endpunkt**.
   b. Wählen Sie den relevanten Websocket-Endpunkt aus.
   c. Kopieren Sie den Wert des Felds **Endpunkt-URL**, der im Installationsbefehl verwendet werden soll.
2. Rufen Sie den API-Schlüssel ab.
   a. Navigieren zu **Agent Client Collector** > **Bereitstellung** > **MID-Webserver API-Schlüssel**.
   b. Kopieren Sie den **API-Schlüssel**-Wert, der im Installationsbefehl verwendet werden soll.
3. Führen Sie den folgenden Befehl auf dem Server aus, auf dem Agent Client Collector installiert wird.

```
ACC_API_KEY=<api_key> ACC_MID=wss://<mid_ip>:<websocket_port>/ws/events
 bash -c "$(curl -L https://<instance
 URL>/api/sn_agent/agents/install_agent)"
```

Geben Sie die folgenden Werte in die Befehlszeile ein:

Befehlszeilenparameter

Parameter	Wert
ACC_API_KEY	Ersetzen Sie die *<api_key>*-Zeichenfolge durch den API-Schlüssel, der für den Zugriff auf den MID-Server-Websocket verwendet wird. Wenn kein Wert angegeben ist, werden Sie während der Ausführung des Skripts aufgefordert, den API-Schlüsselwert einzugeben.
ACC_MID	Ersetzen Sie die *<mid_ip>*-Zeichenfolge durch die URL des MID-Server-Websockets. Wenn Sie mehrere MID Servers angeben, geben Sie die MID-Server als kommagetrennte Zeichenfolge ein.
ACC_ALLOW_LIST	(Optional) Fügen Sie die Zeichenfolge *ACC_ALLOW_LIST=0* hinzu, um die Allow-Liste zu deaktivieren. Die Allow-Liste ist standardmäßig aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert
	Hinweis: Wenn die Allow-Liste deaktiviert ist, beeinträchtigt dies die Sicherheit Ihres Systems und es wird nur als vorübergehende Maßnahme empfohlen, bis Sie die Aktualisierung der Allow-Liste abgeschlossen haben. Nach der Aktualisierung aktivieren Sie die Allow-Liste erneut, indem Sie *ACC_ALLOW_LIST=0* aus der einzeiligen Befehlszeichenfolge entfernen.
ACC_VALIDATE_SIG	(Optional) Fügen Sie die Zeichenfolge *ACC_VALIDATE_SIG=0* hinzu, um die Überprüfung der Validierung des Installationszertifikats zu deaktivieren. Die Validierung ist standardmäßig aktiviert. Standard: Validierung ist aktiviert. **Hinweis:** Deaktivieren Sie die Zertifizierungsvalidierung nur, wenn Sie nicht standardmäßige Signaturvalidierungstools verwenden.

Führen Sie eine einzeilige Agent Client Collector -Installation unter macOS mithilfe von ITOM Cloud Services durch

Installieren Sie Agent Client Collector auf einem Computer macOS vom Typ ohne MID-Server mithilfe der Anwendung ITOM Cloud Services. Wenn Sie Informationen über die Cloud senden, aktivieren Sie die MID-Server für persistentere Ressourcen.

Vorbereitungen
Installieren Sie das Plugin ITOM „ Cloud Services.

Erstellen Sie einen Agent-Registrierungsschlüssel, wie in Konfigurieren Sie einen Agent-Registrierungsschlüsselbeschrieben.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zur Arbeit mit Cloud-Services finden Sie unter DEX-Architektur .

Prozedur

1. Agent-Registrierungsschlüssel abrufen:
   a. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agent-Registrierungsschlüssel**.
   b. Wählen Sie den entsprechenden Agent-Registrierungsschlüssel aus.
   c. Kopieren Sie den Wert des Registrierungsschlüssels, und speichern Sie ihn an einem Ort, an dem Sie ihn bei Bedarf problemlos abrufen können.
2. Rufen Sie die öffentlich zugängliche Gateway-URL basierend auf Ihrem Standort ab:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- AMER (Amerika): `itomcnc-prod-gateway.amer.sncapps.service-now.com:443`
- EMEA (Europa): `itomcnc-prod-gateway.emea.sncapps.service-now.com:443`
- APAC (Asien-Pazifik): `itomcnc-prod-gateway.apac.sncapps.service-now.com:443`

3. Geben Sie auf dem Server, auf dem Sie Agent Client Collectorinstallieren, den folgenden Befehl ein:

```
CONNECT_WITHOUT_MID="true" ACC_CNC="<gateway_endpoint>"
 REGISTRATION_KEY="<registration_key>"
 INSTANCE_URL="https://<instance_url>" bash -c "$(curl -L
 https://<instance_url>/api/sn_agent/agents/install_agent)"
```

Die folgende Tabelle zeigt die Parameterwerte im Befehl.

Befehlszeilenparameterwerte

Parameter	Wert
VERBINDEN_OHNE_MID	Geben Sie **„wahr“** an, um ITOM Cloud-Services zu aktivieren. Wenn Sie keinen Wert angeben, wird die reguläre Websocket-Installation MID-Server aufgerufen. Einzelheiten zur Konfiguration eines Websocket auf dem MID-Serverfinden Sie unter Websocket-Server auf MID-Server installieren.
ACC_CNC	Öffentlicher Gateway-Endpunkt für Agent Client Collector, den Sie angeben können.
REGISTRATION_KEY	Aktiver und gültiger Agent-Registrierungsschlüssel, mit dem der Agent kommunizieren soll.
INSTANCE_URL	ServiceNow Instanz, bei der sich der Service Desk-Mitarbeiter registriert
ACC_ALLOW_LIST	Optionale Zeichenfolge *ACC_ALLOW_LIST=0*, die Sie hinzufügen können, um die Allow-Liste zu deaktivieren. Standard: Die Allow-Liste ist aktiviert. **Hinweis:** Wenn Sie die Allow-Liste deaktivieren, gefährden Sie die Sicherheit Ihres Systems. Diese Aktion ist als temporäre Maßnahme gedacht, während Sie die Allow-Liste aktualisieren. Nachdem Sie das Update abgeschlossen haben, entfernen Sie *ACC_ALLOW_LIST=0* aus der Befehlszeile.
ACC_VALIDATE_SIG	Optionale Zeichenfolge *ACC_VALIDATE_SIG=0*, die Sie hinzufügen können, um die Verifizierung der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Wert
	Validierung der Zertifizierung des Installationsprogramms zu deaktivieren. Standard: Validierung ist aktiviert. **Hinweis:** Deaktivieren Sie die Zertifizierungsvalidierung nur, wenn Sie nicht standardmäßige Signaturvalidierungstools verwenden.

Agent Client Collector manuell unter macOS installieren

Installieren Sie Agent Client Collector manuell auf einem Computer, auf dem macOS verwendet wird, wenn der Agent nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen wünschen.

Vorbereitungen

- Stellen Sie sicher, dass Sie den Agent Client Collector-Webserver konfiguriert haben.
- Vergewissern Sie sich, dass Betriebssystem und Version Ihres Servers mit der Liste der unterstützten Betriebssystemversionen in Installation von Agent Client Collector übereinstimmen.
- Navigieren zu **Agent Client Collector** > **Bereitstellung** > **Agent-Downloads** und laden Sie die signierte `Paketdatei` herunter, die für Ihr Betriebssystem relevant ist.
- Speichern Sie das `.pkg`-Installationspaket auf einem Ihrer installierten Agents.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Laden Sie die Installationsdateien auf Ihren lokalen Computer herunter.

```
curl -L <download link from the Agent Downloads page on the instance>
```

2. Validieren Sie die Signatur der Installationsdatei.

```
pkgutil --check-signature agent-client-collector-<version
 number>-macos-catalina_x64.pkg
```

Hinweis: Stellen Sie sicher, dass die `.pkg`-Zertifikatkette über das Installationszertifikat der ServiceNow-Entwickler-ID verfügt.

3. Installieren Sie das Agent Client Collector-Paket.

```
sudo installer -pkg agent-client-collector-<version
 number>-macos-catalina_x64.pkg -target /
```

4. Kopieren Sie die Installationsdateien.

   a. Beispiel-Konfigurationsdatei:

```
sudo cp -p /Library/Application\ Support/servicenow/agent-client-
collector/acc.yml.example /Library/Application\ Support/servicenow/
agent-client-collector/acc.yml
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Beispiel für eine Allow-Listen-Datei:
```
sudo cp -p /Library/Application\ Support/servicenow/agent-client-collector/check-allow-list.json.default /Library/Application\ Support/servicenow/agent-client-collector/check-allow-list.json
```

5. Wahlweise: Um neue Prüfdefinitionen für die Allow-Liste zu erstellen, deaktivieren Sie zuerst die Allow-Liste, indem Sie den *allow-list*-Parameter in der Datei `acc.yml` auskommentieren.

(Optional) `sudo -H -u _servicenow vi /Library/Application\ Support/servicenow/agent-client-collector/acc.yml`

Hinweis: Diese Aktion beeinträchtigt die Sicherheit Ihres Systems und wird nur als vorübergehende Maßnahme empfohlen, bis Sie die Aktualisierung der Allow-Liste abgeschlossen haben. Sobald das Update abgeschlossen ist, aktivieren Sie die Allow-Liste wieder, indem Sie den Kommentar des Allow-Listen-Parameters in der Konfigurationsdatei entfernen.

Weitere Informationen zum Hinzufügen benutzerdefinierter Prüfungen zu einer Allow-Liste finden Sie unter Agent Client Collector-Zulassungsliste generieren.

6. Speichern Sie die Konfigurationsdatei.

7. Verbinden Sie in der Konfigurationsdatei den Agent mit dem MID-Server.

a. Legen Sie die MID-Server-Verbindung fest.
```
"wss://<MID Server IP>:<Web Socket Port>/ws/events"
```
Der Websocket-Port wurde auf dem MID-Server konfiguriert, als er als Agent Client Collector-Listener festgelegt wurde.

b. Suchen Sie den *api-key*-Parameter und geben Sie den API-Schlüsselwert in doppelten Anführungszeichen wie folgt an:
api-key:"11111111"
Der angegebene API-Schlüssel wird bei der ersten Ausführung des Agent verschlüsselt.

8. Um sicherzustellen, dass die Konfigurationsdatei auf einen gültigen Endpunkt verweist, führen Sie die folgenden Befehle aus, um Agent Client Collectorneu zu starten:
```
sudo launchctl unload -w /Library/LaunchDaemons/com.sn.acc.plist
sudo launchctl load -w /Library/LaunchDaemons/com.sn.acc.plist
```

Hinweis: Standardmäßig führt das Beenden des Installationsprogramms dazu, dass das Programm sofort neu gestartet wird. Damit das Programm nach dem Beenden im angehaltenen Zustand bleibt, legen Sie die Keep Alive-Eigenschaft in der Datei `/Library/LaunchDaemons/com.sn.acc.plist` auf **false** fest.

Führen Sie ein manuelles Upgrade Agent Client Collector von auf dem System macOS durch

Führen Sie ein manuelles Upgrade Ihrer vorhandenen Version Agent Client Collector auf einem System durch, auf dem macOSausgeführt wird. Ein manuelles Upgrade ist nützlich, wenn das einzeilige Befehlsskript nicht mit der Instanz verbunden ist oder Sie erweiterte Anpassungsoptionen verwenden möchten.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wahlweise: Sichern Sie die Konfigurationsdateien `agent-id` und `acc.yml` manuell, indem Sie die folgenden Befehle ausführen.

```
mkdir -p /tmp/acc-upgrade-backup
cp -rp /Library/Application
 Support/servicenow/agent-client-collector/acc.yml /
tmp/acc-upgrade-backup
cp -rp /Library/Application
 Support/servicenow/agent-client-collector/check-allow-list.json /
tmp/acc-upgrade-backup
cp -rp /Library/Application
 Support/servicenow/agent-client-collector/agent_now_id /
tmp/acc-upgrade-backupmkdir -p /tmp/acc-upgrade-backup
```

   Das manuelle Sichern der Konfigurationsdateien bietet eine zusätzliche Sicherheitsebene, indem sichergestellt wird, dass Ihre Dateien vor Beginn des Upgrade-Prozesses gesichert werden.

2. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agent-Downloads**.
3. Laden Sie im Abschnitt **„MacOS-Downloads“** das entsprechende Agent-Paket und die Signatur – Paketdateien herunter.
4. Führen Sie ein Paket-Upgrade durch.

```
sudo installer -pkg agent-client-collector-<version
 number>-macos-catalina_x64.pkg -target /
```

   Dieser Befehl sichert auch die agent-id- und Konfigurationsdateien vor dem Upgrade und stellt sie wieder her.

5. Vergewissern Sie sich, dass das Upgrade erfolgreich war.

   a. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.

   b. Überprüfen Sie die folgenden Werte für Ihren Agent:

   - **Hostdatensammlung** = Gesammelt
   - **Version** =<Relevant version number>

Agent Client Collector unter macOS mit einem einzeiligem Befehl deinstallieren

Deinstallieren Sie Agent Client Collector auf einem macOS-Computer, indem Sie einen effizienten einzeiligen Befehl ausführen. Wenn der Agent mit der Instanz verbunden ist, deinstallieren Sie Agent Client Collector manuell.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

Führen Sie den folgenden Befehl aus.

```
bash -c "$(curl -L https://<Instance
 URL>/api/sn_agent/agents/install_agent)" -s "--remove"
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Bei der Deinstallation von Agent Client Collector werden die Datei `acc.yml` und das zugehörige Verzeichnis von Ihrem Computer entfernt. Der Benutzer und die Gruppe **_servicenow**, die als Teil des Installationsprozesses erstellt wurden, werden ebenfalls entfernt.

Agent Client Collector auf einem macOS-Computer manuell deinstallieren

Deinstallieren Sie Agent Client Collector unter macOS manuell, anstatt das Verfahren mit einzeiligem Befehl zu verwenden, wenn der betreffende Agent nicht mit der Instanz verbunden ist.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Deaktivieren und beenden Sie den Dienst in einem Befehlsfenster:
   sudo launchctl unload -w /Library/LaunchDaemons/com.sn.acc.plist
2. Löschen Sie die folgenden Dateien/Verzeichnisse:

```
sudo rm /Library/LaunchDaemons/com.sn.acc.plist
sudo rm -rf /opt/servicenow/agent-client-collector
sudo rm -rf /var/run/servicenow/agent-client-collector
sudo rm -rf /Library/Application\
 Support/servicenow/agent-client-collector
```

3. Entfernen Sie den **_servicenow**-Benutzer und die Gruppe.

```
sudo /usr/bin/dscl . -delete /Users/_servicenow
sudo /usr/bin/dscl . -delete /Groups/_servicenow
```

4. Entfernen Sie das **Paket** aus der Liste der installierten Pakete.

```
sudo pkgutil --forget com.servicenow.agent-client-collector
```

Agent Client Collector Monitoring auf dem MID-Server aktivieren

Aktivieren Sie Agent Client Collector Monitoring auf dem MID-Server, indem Sie in einem einzigen Vorgang das Agent Client Collector-Framework (ACC-F) und die Metrikdaten-Erweiterungen konfigurieren. Durch Aktivieren der Agent Client Collector-Überwachung wird auch die Überwachung von Agents ermöglicht, die mit dem MID-Server verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Server**.
2. Wählen Sie auf der MID-Server-Seite einen MID-Server, um die Details des MID-Servers anzuzeigen.
3. Klicken Sie im Abschnitt **Zugehörige Links** auf **Setup ACC Monitoring** (ACC-Monitoring einrichten) und geben Sie die entsprechende Portnummer in das Feld **Port des MID Web Server** des Dialogfelds ein.

Ergebnisse
Der MID-Server ist so konfiguriert, dass er sowohl Agent Client Collector als auch Metrikdaten unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Sie werden nur bei der Ersteinrichtung der ACC-Überwachung zur Eingabe einer Portnummer aufgefordert.

Optimieren Sie die Verteilung von Service Desk-Mitarbeitern auf MID Servers

Optimieren Sie die Verteilung von Agents, indem Sie die Weitergabe von einem MID-Server zum anderen zulassen. Agents werden immer mit dem MID-Server mit der schnellsten Antwortzeit verbunden.

Vorbereitungen

Stellen Sie sicher, dass die folgenden Einstellungen konfiguriert sind:

- Die Systemeigenschaft *sn_agent.enable_auto_mid_selection* ist auf „True“ festgelegt. Bei Verwendung der Datei `acc.yml` heißt die Eigenschaft *enable_auto_mid_selection*.
- Auf der MID Server-Seite (**Agent Client Collector** > **MID-Server**):
  - Status: In Betrieb
  - Validiert: Ja

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Nur validierte MID Servers können Verbindungen von Service Desk-Mitarbeitern akzeptieren.

Prozedur

1. Navigieren zu **Agent Client Collector** > **Bereitstellung** > **MID-Server**.
2. Aktivieren Sie auf der Seite **MID Server [Ansicht „Agent Client Collector“]** das Kontrollkästchen neben dem MID-Server, über den Sie Agents neu verteilen möchten.
3. Wählen Sie in der Liste **Aktionen für ausgewählte Zeilen** die Option **Try redistributing connected agents** (Neuverteilung verbundener Agents versuchen) aus.
   Beachten Sie die Anzahl der Mitarbeiter, die MID Serverszugewiesen sind.
4. Aktualisieren Sie die Seite, um die Ergebnisse des Neuverteilungsversuchs anzuzeigen. Die Werte in der Spalte **Anzahl der Agents** für alle betroffenen MID-Server ändern sich, wenn Agents neu verteilt wurden.

Agent Client Collector-Konfigurationsdateien für Agents anzeigen

Zeigen Sie die `acc.yml` Agent Client Collector-Konfigurationsdatei an, ohne auf den Hostserver zugreifen zu müssen, indem Sie die Datei von einem Agent abrufen.

Vorbereitungen

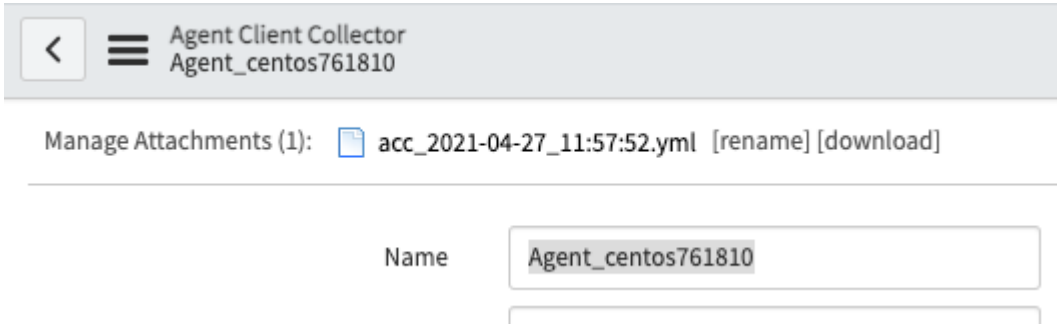
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
2. Wählen Sie auf der Seite „Agent Client Collector“ einen Agent aus.
3. Klicken Sie im Abschnitt **Zugehörige Links** auf **Grab agent config (acc.yml)** (Agent-Konfiguration abrufen (acc.yml)).
   Auf der Seite wird eine Meldung angezeigt, die angibt, dass die Datei angehängt wird.
4. Warten Sie einige Sekunden, und aktualisieren Sie die Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die `acc.yml`-Konfigurationsdatei wird als Anhang auf dem Agent angezeigt.



Zugehörige Informationen

Konfigurationsdateioptionen

Erstellen Sie eine Agent Client Collector Konfigurationsdatendatei

Erstellen Sie eine Konfigurationsdatendatei Agent Client Collector, und ordnen Sie sie Prüfungsdefinitionen zu, um die Informationen zu Ihrer Instanz anzuzeigen. Sie können den Konfigurationsdatendateien, die von Prüfungsdefinitionen während Prüfungsausführungen verwendet werden, auch einen Anhang hinzufügen oder löschen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Eine Prüfungsdefinition ist ein einzelner Prüfungseintrag im System. Details finden Sie unter Agent Client Collector Konfigurationsdatendateien.

Dateianhänge mit Konfigurationsdaten enthalten Instanzdaten, z. B. Informationen zu Configuration Item (CI), die beim Ausführen einer Prüfung verwendet werden.

Domänentrennung wird in den Konfigurationsdatendateien Agent Client Collector unterstützt.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Konfigurationsdateien**.
2. Wählen Sie **Neu**.
3. Fügen Sie einen Anhang hinzu, oder entfernen Sie ihn.

Aktion	Beschreibung
Fügen Sie eine Datei hinzu	Synchronisieren Sie den -Datensatz und das relevante MID Servers. **a.** Wählen Sie das Büroklammer-Symbol . Das Dialogfeld „Anhänge“ wird geöffnet. **b.** Wählen Sie **Datei auswählen** und anschließend eine anzuhängende Datei aus. **c.** Schließen Sie das Dialogfeld Anhänge.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion	Beschreibung
Löschen Sie eine Datei	Löschen Sie optional einen Anhang, der dem Datensatz nicht zugeordnet werden soll. **a.** Wählen Sie **Anhänge verwalten**. Das Dialogfeld „Anhänge“ wird geöffnet. **b.** Aktivieren Sie das Kontrollkästchen neben dem Anhang, den Sie entfernen möchten. **c.** Wählen Sie **Entfernen**.

Der Anhangname muss für jede Domäne eindeutig sein und darf nur aus alphanumerischen Zeichen bestehen.

Wenn der Anhang ungültige Zeichen enthält oder ein Duplikat eines anderen Anhangs ist, treten die folgenden Situationen auf:

- Die Konfigurationsdatei wird automatisch auf **Aktiv = False**festgelegt.
- In der Spalte „Fehler“ wird eine Meldung angezeigt, die auf ein Problem mit dem Anhang hinweist.

Jeder Datensatz kann nur einen Anhang enthalten.

4. Wahlweise: Geben Sie im Feld **Beschreibung** eine Beschreibung für die Konfigurationsdatendatei ein.
5. Wählen Sie **Absenden**.

Ergebnisse

- Die Konfigurationsdatendatei wird auf der Seite „Konfigurationsdatei von Agent Client Collector“ aufgeführt.
- Der Wert **Name** wird automatisch auf den Namen des Anhangs festgelegt.

Bei Prüfungen wird die Konfigurationsdatendatei mit Instanzdaten während der Prüfungsausführung verwendet.

Aktualisieren Sie Agent Client Collector Zertifikate manuell

Aktualisieren Sie selbstsignierte Agent Client Collector Zertifikate manuell, um Agent Client Collector Plugins zu validieren, anstatt auf die geplante Synchronisierung zu warten. Sie können diese Funktion beispielsweise verwenden, wenn der Agent ein Plugin nicht validieren kann und Sie nicht auf die geplante Synchronisierung warten möchten.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Server**.
2. Wählen Sie einen MID-Server.
3. Wählen Sie im Abschnitt „Zugehörige Links“ **Synchronisierung des ACC-Zertifikats auslösen**aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Selbstsignierte Zertifikate werden von MID-Server an Agent Client Collector gesendet, um die Plugins des -Agents zu validieren.

Aktivieren Sie die sichere OpenSSL-Signierung für -Plugins

Erstellen Sie ein selbstsigniertes Zertifikat für ein Agent Client Collector-Plugin. Das folgende Verfahren zeigt ein Beispiel für die Erstellung eines x509-Zertifikats mit OpenSSL. Informationen zu anderen Zertifikatstypen können Sie der OpenSSL-Dokumentation entnehmen.

Vorbereitungen
- Vergewissern Sie sich zum Prüfen der Signatur des Plugin, dass die Eigenschaft *verify-plugin-signature* in der Datei `acc.yml` des Agent auf **True** festgelegt ist.
- Stellen Sie sicher, dass **OpenSSL** auf Ihrem System installiert ist.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Das Aktivieren eines sicheren OpenSSL-Signiermechanismus für -Plugins funktioniert, wenn Agent Client Collector auf einem Linux -System installiert ist.

Prozedur
1. Erstellen Sie eine Plugin-Datei mit der Erweiterung `tar.gz`.
   Weitere Informationen finden Sie unter Agent Client Collector -Plugins erstellen und bearbeiten.
2. Generieren Sie Ihr eigenes sicheres Selbstzertifikat für die Plugin-Datei.

   a. Erstellen Sie ein x509-Zertifikat.

   ```
   openssl req -nodes -x509 -sha256 -newkey rsa:2048 -keyout "sign.key"
    -out "sign.crt" -days 365 -subj

    "/C=<CountryName>/ST=<StateOrProvinceName>/L=<Locality>/O=<Organizati
   on>/OU=<OrganizationalUnit>/CN=sign"
   ```

   b. Signieren Sie die Plugin-Datei.

   ```
   openssl dgst -sha256 -sign "sign.key" -out sign.txt.sha256
    <plugin-name>.tar.gz
   ```

   Alternativ können Sie Plugins mit einer Zertifizierungsstelle signieren. Weisen Sie dabei das PEM-Format des Zertifikats zu, und platzieren Sie es im Verzeichnis `cert` des Agent.

   c. Vergewissern Sie sich, dass die Signatur richtig konfiguriert ist.

   ```
   openssl dgst -sha256 -verify  <(openssl x509 -in "sign.crt" -pubkey
    -noout) -signature sign.txt.sha256 <plugin-name>.tar.gz
   ```

   Wenn die Datei gültig ist, lautet die Ausgabe `Verified OK`.

   d. Codieren Sie das Zertifikat der Signatur mit base64-Codierung.

   ```
   base64 sign.txt.sha256 > sign.txt.sha256_encode64.sig
   ```

   Eine `sign.txt.sha256_encode64.sig`-Datei wird erstellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Führen Sie die folgenden Befehle aus, um ein neues Verzeichnis zu erstellen und die Dateien „`tar.gz`" und „`sign.txt.sha256_encode64.sig`" einzufügen.
   a. `mkdir-Signed-Plugin`
   b. `mv<plugin-name> .tar.gz signiertes Plugin`
   c. `mv sign.txt.sha256_encode64.sig Signiertes Plugin`
   d. `cd signiertes Plugin`
4. Erstellen Sie eine weitere „`tar.gz`" -Datei, indem Sie dieselben Befehle wie für die erste „`tar.gz`" -Datei ausführen.
   a. `tar -C . -zcvf ../<plugin-name> .tar.gz *`
   b. `CD…`

   Hinweis: Neue Datei speichern als `../` <plugin-name> .tar.gz, um Namenskollisionen mit dem Original zu vermeiden `.tar.gz`– Datei, die im aktuellen Verzeichnis vorhanden ist.
5. Laden Sie die neue `tar.gz`-Plugin-Datei in die Instanz hoch.
6. Legen Sie die Plugin-Datei als *`active=true`*fest.
7. Platzieren Sie die Datei `sign.crt` im `Zertifikatverzeichnis` des Agent, das sich im `Konfigurationsordner` befindet.
8. Legen Sie in der Datei `acc.yml` den `Wert „verify-plugin-signature"` auf **true**fest.

Fügen Sie dem Truststore Ihres Betriebssystems ein selbstsigniertes Zertifikat hinzu

Fügen Sie dem Truststore Ihres Betriebssystems ein selbstsigniertes Zertifikat hinzu. Durch Hinzufügen eines Zertifikats zum Truststore können Sie überprüfen, ob das Zertifikat Authentizität und die Verbindungen sicher sind.

Warum und wann dieser Vorgang ausgeführt wird

Das Verfahren zum Hinzufügen eines Zertifikats zu einem Truststore hängt vom Betriebssystem des Hosts ab.

Durch Hinzufügen eines selbstsignierten Zertifikats zum Truststore wird das Betriebssystem angewiesen, dem Zertifikat zu vertrauen, wenn sichere Verbindungen hergestellt werden. Auf diese Weise können die Anwendungen sicher mit Services kommunizieren, die das selbstsignierte Zertifikat verwenden. Wenn Sie ein nicht vertrauenswürdiges Zertifikat hinzufügen, gefährden Sie möglicherweise die Sicherheit Ihres Systems.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Unter einem Windows -BS:
   a. Drücken Sie die Taste Windows + `R` auf Ihrer Tastatur.
      Das Feld **Ausführen** wird geöffnet.
   b. Geben Sie die Zeichenfolge `certmgr.msc` ein, und drücken Sie **die Eingabetaste**.
      Der Zertifikatmanager wird geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Erweitern Sie das Verzeichnis Vertrauenswürdige Stammzertifizierungsstellen.

d. Wählen und halten Sie **Zertifikate** (oder klicken Sie mit der rechten Maustaste darauf).

e. Auswahlvorgang **Alle Aufgaben** > **Importieren**.
Der Zertifikatimport-Assistent wird geöffnet.

f. Befolgen Sie die Schritte im Zertifikatimport-Assistenten.
Details finden Sie unter Importieren Sie ein selbstsigniertes Zertifikat.

Alternativ können Sie ein Windows -Zertifikat mit PowerShell hinzufügen, indem Sie den folgenden Befehl als Administrator ausführen:

```
Import-Certificate -FilePath <path to your certificate file>
 -CertStoreLocation Cert:\LocalMachine\Root
```

2. Auf einem macOS:

a. Importieren Sie das Zertifikat in einen Schlüsselbund, indem Sie in einem Terminalfenster den folgenden Befehl ausführen:

```
bash

code:
sudo security add-trusted-cert -d -r trustRoot -k
 "/Library/Keychains/System.keychain" <path to your certificate file>
```

b. Geben Sie das Administratorpasswort ein, wenn Sie dazu aufgefordert werden.

c. Öffnen Sie die Anwendung „Schlüsselbundzugriff“, um zu überprüfen, ob das Zertifikat hinzugefügt wurde.
Ein erfolgreich hinzugefügtes Zertifikat wird als gekennzeichnet. **Dieses Zertifikat wird für ... als vertrauenswürdig markiert. Plugin-Überprüfung.**

3. Unter einem Linux -BS:

a. Bereiten Sie die selbstsignierte Zertifikatdatei als PEM-Datei (Privacy Enhanced Mail) vor.

b. Kopieren Sie das Zertifikat in das Verzeichnis der Zertifizierungsstelle (Certificate Authority, CA), in dem die Zertifikate gespeichert werden.

- Führen Sie auf einem Debian/Ubundu-basierten System den folgenden Befehl aus:

```
sudo cp <path to certificate
 file> /etc/pki/ca-trust/source/anchors/do
```

- Führen Sie auf einem Red Hat/Fedora-basierten System den folgenden Befehl aus:

```
sudo cp <path to certificate file> /etc/pki/ca-trust/source/anchors
```

c. CA-Zertifikate aktualisieren:

- Führen Sie auf einem Debian/Ubundu-basierten System den folgenden Befehl aus:

```
update-ca-certificates
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Befehl liest das Zertifikatpaket im Verzeichnis `/usr/local/share/ca-certificates`, aktualisiert das Zertifikatpaket und speichert es unter `/ext/ssl/certs/ca-certificates.crt`.

- Führen Sie auf einem Red Hat/Fedora-basierten System den folgenden Befehl aus:

```
sudo update-ca-trust extract
```

Ergebnisse
Ihr selbstsigniertes Zertifikat befindet sich in dem Betriebssystem, mit dem Sie arbeiten.

Importieren Sie ein selbstsigniertes Zertifikat

Importieren Sie mit dem Zertifikatimport-Assistenten ein selbstsigniertes Zertifikat in ein Windows -System. Der Zertifikatimport-Assistent ist erforderlich, um den Importvorgang für selbstsignierte Zertifikate unter Windows dem Betriebssystem abzuschließen.

Vorbereitungen
Stellen Sie sicher, dass Sie das unter Fügen Sie dem Truststore Ihres Betriebssystems ein selbstsigniertes Zertifikat hinzubeschriebene Verfahren zum Importieren eines selbstsignierten Zertifikats in ein Windows -System befolgt haben.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Wählen Sie auf der ersten Seite des Assistenten **Weiter**aus.
   Der Truststore befindet sich normalerweise im Verzeichnis der vertrauenswürdigen Stammzertifizierungsstellen des Zertifikatmanagers.
2. Navigieren Sie zu dem Speicherort, an dem sich die selbstsignierte Zertifikatdatei befindet. Die Datei befindet sich normalerweise im Verzeichnis „`config/cert`“ des Agent.
3. Wählen und halten Sie die Zertifikatdatei (oder klicken Sie mit der rechten Maustaste darauf), und wählen Sie **Zertifikat installieren**aus.
4. Wählen Sie **Weiter**.
5. Wählen Sie die Option aus, um das Zertifikat im Truststore der vertrauenswürdigen Stammzertifizierungsstellen zu platzieren.
6. Wählen Sie **Weiter** und **Beenden aus**, um den Assistenten zu schließen.

Ergebnisse
Das Zertifikat wird in den Truststore importiert.

Nächste Maßnahme
Wenn eine Sicherheitswarnung angezeigt wird, wählen Sie **Bestätigen,** um den Import zu bestätigen.

Führen Sie die Korrektur Zscaler durch

Wenn die auf dem Windows- oder macOS-Agent installierte Zscaler-Anwendung nicht ordnungsgemäß ausgeführt wird, können Sie die App anhalten und neu starten. Dieser Prozess wird als *`remediation`* (Fehlerkorrektur) bezeichnet. Durch Ausführung der Fehlerkorrektur wird automatisch ein Incident auf dem Agent erstellt. Die Zscaler-Status können Sie auch im Zscaler-Dashboard als Diagramm anzeigen.

Standardmäßig wird die Überwachungsprüfung gemäß **Zscaler-Überwachungsrichtlinie** alle 30 Minuten ausgeführt, um den Status der Zscaler-App zu überprüfen, die auf dem Agent ausgeführt wird. Die Zscaler-Überwachungsrichtlinie beinhaltet die folgenden Prüfungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *zscaler-monitoring-check*: Überprüft den Status der auf dem Agent ausgeführten Zscaler-App.
- *zscaler-remediation-check*: Wird nur aufgerufen, wenn die Zscaler-App nicht effizient ausgeführt wird. Diese Prüfung fährt die App herunter, startet sie neu und erstellt automatisch einen Incident.

  Für eine Zscaler-App, bei der die Fehlerkorrektur nicht ordnungsgemäß verläuft, wird alle 24 Stunden nur ein Incident erstellt. Wenn die Fehlerkorrekturprüfung beispielsweise mehrmals auf einem Agent ausgeführt wird, werden neue Fehlerkorrektureinträge erstellt, die bis nach Ablauf von 24 Stunden demselben Incident zugeordnet werden. Anschließend wird ein zweiter Incident erstellt. Wenn die App Zscaler erfolgreich neu gestartet wird, wird der Incident geschlossen.

  Ausgabe der Zscaler-Fehlerkorrektur:

  - Pro Fehlerkorrektur erzeugte Datenmenge: 2 KB
  - Maximale Anzahl von Fehlerkorrekturen, die an einem Tag ausgeführt werden können: 48 (eine alle 30 Minuten)
  - Maximale Datenmenge, die von einem einzelnen Agent pro Tag erzeugt wird: 96 KB
  - Maximale Datenmenge, die von 20.000 Agents pro Tag erzeugt wird: 1,92 GB

Überprüfen Sie die Überwachung von Zscaler .

Überprüfen Sie den Überwachungsstatus Ihrer App Zscaler, um sicherzustellen, dass sie ordnungsgemäß ausgeführt wird.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die Überwachungs-App inaktiv ist, lautet der Zscaler-Tunnelstatus entweder *51 (SERVICE_DOWN_ERROR)* oder *56 (SYSTEM_SOCKETS_EXHAUSTED_ERROR)*. In diesem Fall wird eine Fehlerkorrekturprüfung ausgeführt, bei der die Zscaler-App heruntergefahren und neu gestartet wird.

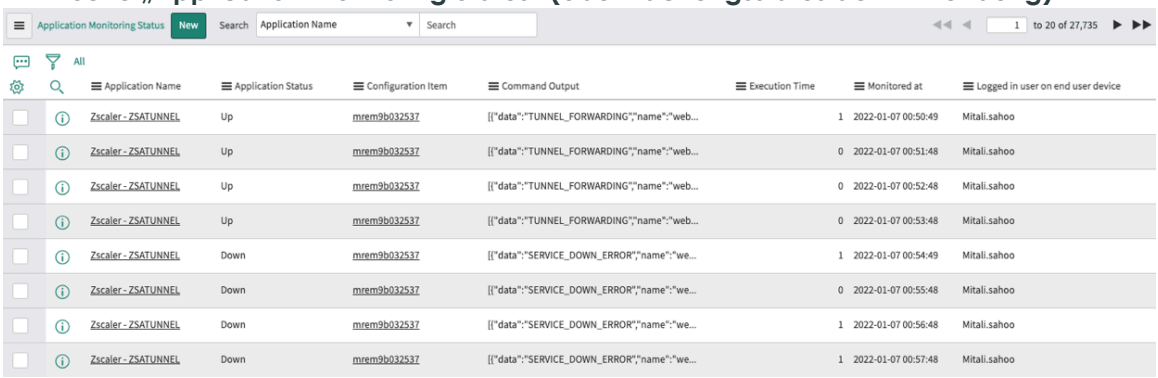
Standardmäßig findet die Zscaler-Überwachungsprüfung (*zscaler-monitoring-check*) automatisch alle 30 Minuten statt. Wenn bei der App Zscaler Probleme auftreten, sollten Sie die Prüfung häufiger oder sofort ausführen. Details finden Sie unter Zscaler-Überwachungsprüfung anpassen.

Prozedur

1. Navigieren zu **Alle** > **Zscaler-VPN nachbessern** > **Überwachungsstatus**.
   Die Seite **Application Monitoring Status** (Überwachungsstatus der Anwendung) wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „Application Monitoring Status“ (Überwachungsstatus der Anwendung)



- Wenn die App Zscaler ordnungsgemäß ausgeführt wird, wird in der Spalte **Anwendungsstatus** der Wert **In Betrieb** angezeigt.
- Wenn die App Zscaler nicht ordnungsgemäß ausgeführt wird, zeigt die Spalte **Anwendungsstatus** den Wert **Ausgeschaltet** an.

2. Wenn in der Spalte **Anwendungsstatus** der Wert **Ausgeschaltet** angezeigt wird, wird die Fehlerkorrekturprüfung (*`zscaler-remediation-check`*) ausgeführt.
   - Weitere Informationen zum Anpassen des Zeitraums, nach dem der Zscaler-Status vom System überprüft wird, finden Sie unter Wartezeit der Zscaler-Fehlerkorrektur anpassen.
   - Weitere Informationen zur Überwachung von Zscaler-Fehlerkorrekturprüfungen finden Sie unter Zscaler-Fehlerkorrektur überprüfen.

Wartezeit der Zscaler-Fehlerkorrektur anpassen

Konfigurieren Sie den Zeitraum (in Sekunden), nach dem der Zscaler-Status von der Zscaler-Fehlerkorrekturprüfung geprüft wird. Dieser Zeitraum gibt an, wie oft der Zscaler-Status vom System überprüft wird, nachdem die Fehlerkorrekturprüfung ausgeführt wurde.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Agent Client Collector** > **Agents** > **Konfiguration** > **Prüfungsdefinition**.
2. Wählen Sie *`zscaler-remediation-check`*.
3. Ändern Sie im Feld **Befehl** den Wert in: `zscaler_app_remediator.rb --wait_time=<time_in_sec>`. Dabei entspricht `<time_in_sec>` der Anzahl der Sekunden, die vom System vor Prüfung des Zscaler-Status gewartet wird.
   Standardmäßig beträgt die Wartezeit des Systems 30 Sekunden.
4. Wählen Sie **Speichern**.
   - Wenn die Zscaler-App innerhalb der konfigurierten `wait_time` (Wartezeit) ausgeführt wird, lautet das Fehlerkorrekturergebnis **Erfolg**.
   - Wenn die Zscaler-App nicht innerhalb der konfigurierten `wait_time` (Wartezeit) ausgeführt wird, lautet das Fehlerkorrekturergebnis **Fehlgeschlagen**.

Zscaler-Überwachungsprüfung anpassen

Passen Sie die Häufigkeit an, mit der die Zscaler-Überwachungsprüfung ausgeführt wird. Standardmäßig wird die Zscaler-Überwachungsprüfung alle 30 Minuten ausgeführt. Wenn die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

App Zscaler nicht effizient funktioniert, können Sie die Prüfung so einstellen, dass sie häufiger ausgeführt wird.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zum Anpassen der Zscaler-Überwachungsprüfung finden Sie unter Führen Sie die Korrektur Zscaler durch.

Prozedur
1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Richtlinien**.
2. Wählen Sie den Eintrag **Zscaler Monitoring Policy** (Zscaler-Überwachungsrichtlinie) aus.
3. Wählen Sie die Registerkarte **Zeitplanung** aus.
4. Ändern Sie im Feld **Intervall (Sek.)** den Wert in die Sekundenanzahl der Wartezeit, die zwischen den Ausführungen der Überwachungsprüfung eingelegt werden soll.
   Der Standardwert lautet 1800.

   Um die Überwachungsprüfung sofort auszuführen, geben Sie den Wert **1** ein.

Ergebnisse
Zscaler-Überwachungsprüfungen werden gemäß der im Feld **Intervall (Sek.)** angegebenen Häufigkeit ausgeführt.

Zscaler-Fehlerkorrektur überprüfen

Vergewissern Sie sich, dass die Zscaler-App durch die Zscaler-Fehlerkorrektur heruntergefahren und neu gestartet wird, nachdem die Überwachungsprüfung fehlgeschlagen ist.

Vorbereitungen
Stellen Sie sicher, dass die Überwachungsprüfung Zscaler den **Anwendungsstatus-** Wert **Inaktiv**zurückgibt, was darauf hinweist, dass die App Zscaler nicht ordnungsgemäß funktioniert.

Erforderliche Rolle: agent_client_collector_admin

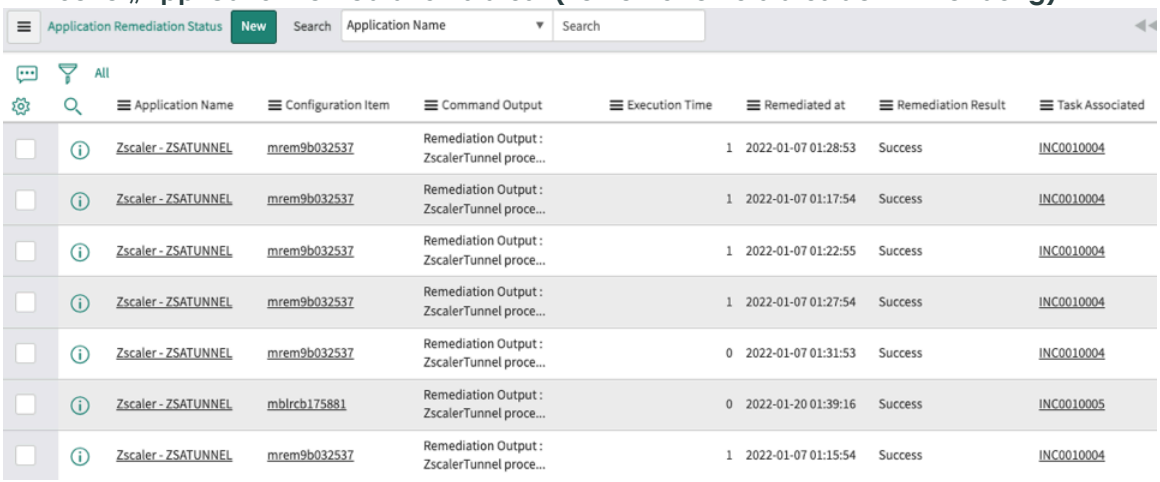
Prozedur

Navigieren zu **Alle** > **Zscaler-VPN nachbessern** > **Ergebnis der Fehlerkorrektur**.

Die Seite **Application Remediation Status** (Fehlerkorrekturstatus der Anwendung) wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „Application remediation status“ (Fehlerkorrekturstatus der Anwendung)



Application Name	Configuration Item	Command Output	Execution Time	Remediated at	Remediation Result	Task Associated
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	1	2022-01-07 01:28:53	Success	INC0010004
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	1	2022-01-07 01:17:54	Success	INC0010004
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	1	2022-01-07 01:22:55	Success	INC0010004
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	1	2022-01-07 01:27:54	Success	INC0010004
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	0	2022-01-07 01:31:53	Success	INC0010004
Zscaler - ZSATUNNEL	mblrcb175881	Remediation Output : ZscalerTunnel proce...	0	2022-01-20 01:39:16	Success	INC0010005
Zscaler - ZSATUNNEL	mrem9b032537	Remediation Output : ZscalerTunnel proce...	1	2022-01-07 01:15:54	Success	INC0010004

Wenn die Fehlerkorrektur Zscaler erfolgreich herunterfährt und neu startet, enthält die Spalte **Remediation Result** (Ergebnis der Fehlerkorrektur) den Wert **Erfolg**. In der Spalte **„Zugeordnete Aufgabe“** wird ein Link zu dem bei der Korrektur erstellten Incident angezeigt. Wenn die Fehlerkorrektur erfolgreich ist, wird der Incident automatisch geschlossen.

Zscaler-Dashboard verwenden

Verwenden Sie das Zscaler-Dashboard, um die Status der Zscaler-Überwachung und -Fehlerkorrektur im Diagrammformat anzuzeigen.

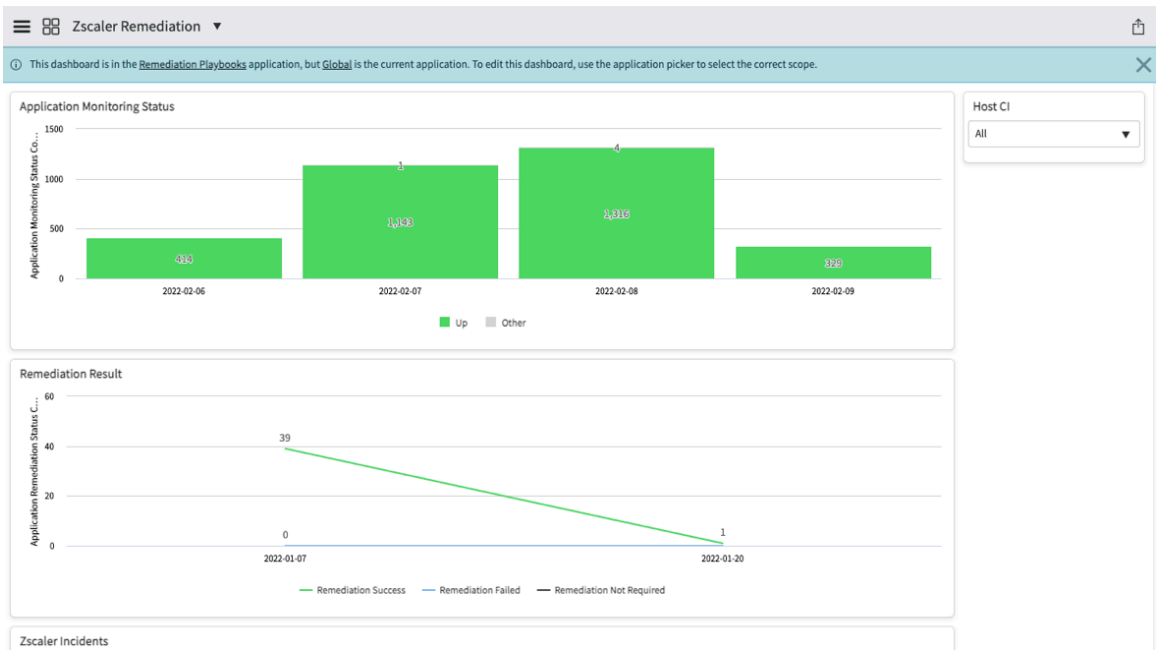
Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Zscaler-VPN nachbessern** > **Dashboard**.
   Das Dasbhoard „Zscaler Remediation“ (Zscaler-Fehlerkorrektur) wird angezeigt.

Zscaler-Dashboard



Das Dashboard zeigt Diagramme an, die in die folgenden Abschnitte unterteilt sind:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitte im Dashboard „Zscaler Remediation“ (Zscaler-Fehlerkorrektur)

Abschnitt	Beschreibung
Application Monitoring Status (Überwachungsstatus der Anwendung)	Zeigt ein Balkendiagramm der Anzahl der Zscaler-Apps nach Datum und deren Status (In Betrieb, Ausgeschaltet, Unbekannt, Sonstige) an.
Remediation Result (Ergebnis der Fehlerkorrektur)	Zeigt ein Liniendiagramm der Anzahl der Zscaler-Fehlerkorrekturen und deren Status (Erfolg, Fehlgeschlagen, Nicht erforderlich) an.
Zscaler Incidents (Zscaler-Incidents)	Zeigt ein Liniendiagramm der Anzahl der erstellten Zscaler-Incidents und deren Status (Geöffnet, Geschlossen) an.

2. Wahlweise: Wählen Sie im Fenster **Host-CI** oben rechts auf der Seite das CI aus, dessen Daten Sie anzeigen möchten.
   Der Standardwert ist Alle. Damit wird angegeben, dass das Dashboard Daten von allen CIs auf dem Host anzeigt.

Arbeiten mit Prüfungen und Richtlinien

Sie können Aktionen für Prüfungen und Richtlinien ausführen, um die Überwachung der Geräte Ihres Systems zu verbessern.

Prüfungen erstellen und bearbeiten

Sie können eine Prüfung abhängig vom Typ der Entität (z. B. einem Server oder einer Anwendung) auswählen, die Sie überwachen möchten. Nach Bedarf können Sie die Standardprüfungen anzeigen und bearbeiten oder neue Prüfungen erstellen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Prüfungsdefinitionen**.
2. Klicken Sie auf **Neu**.
   Die Seite **Check Definition** (Prüfungsdefinition) wird angezeigt.

   Hinweis: Die Verwendung von Ruby-Skripts in einer Windows-Umgebung verursacht einen hohen CPU-Verbrauch.

3. Geben Sie Werte in die Felder auf der Seite ein, wie in Agent Client Collector Prüfungsdefinitionsseitebeschrieben.
4. Geben Sie auf der Registerkarte **Parameter** nach Bedarf Parameterdefinitionen ein. Parameter werden für das Feld **Befehl** verwendet, wenn die Vorlage Simple verwendet wird (siehe Agent Client Collector Prüfungsdefinitionsseite) .

   Die Informationen, die Sie für Parameter hinzufügen können, sind unter Registerkarte „Prüfungsdefinition“-Formularparameterbeschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prüfungsdefinitionen oder Prüfungsinstanz testen

Wenn Sie mit einer Prüfungsdefinition oder Prüfungsinstanz arbeiten, können Sie die Prüfung mit dem zugewiesenen Agent testen, um sicherzustellen, dass die Prüfung ordnungsgemäß konfiguriert ist.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Prüfungsdefinitionen**.
2. Wählen Sie in der Liste eine Prüfungsdefinition aus.

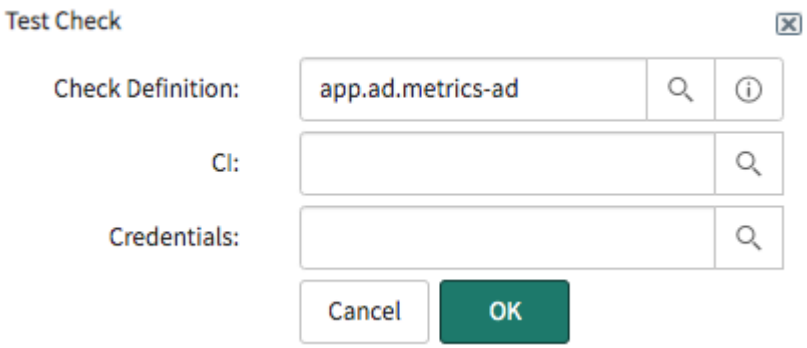
   Hinweis: Bei Prüfungstest in Prüfungsinstanz:

   a. Navigieren zu **Agent Client Collector** > **Richtlinien**.

   b. Wählen Sie eine Richtlinie aus.

   c. Wählen Sie in der Richtlinie eine Prüfungsinstanz aus.
   Fahren Sie mit den folgenden Schritten in diesem Verfahren fort.

3. Klicken Sie im Abschnitt **Related Links** (Zugehörige Links) auf **Test Check** (Testüberprüfung).
   Das Dialogfeld **Test Check** (Testüberprüfung) wird angezeigt.



4. Konfigurieren Sie die Felder im Dialogfeld.

Felder im Dialogfeld „Testüberprüfung“

Feld	Beschreibung
Prüfungsdefinition	Zeigt den Namen der ausgewählten Prüfungsdefinition an
CI	Wählen Sie das CI aus, für das die Prüfung ausgeführt werden soll. Zur Auswahl verfügbar sind diejenigen CIs, die die beiden folgenden Kriterien erfüllen: ◦ Gehören zu der im Feld **Check group** (Überprüfungsgruppe) angegebenen Gruppe ◦ Gehört zu einem Service Desk-Mitarbeiter mit dem Status **„In Betrieb“**. Wenn das Feld **Check group** (Überprüfungsgruppe) leer ist, wird

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	der Standardwert **cmdb_ci_computer** eingetragen.
Berechtigungen	Wählen Sie die Anmeldeinformationen des Benutzers aus, mit dem der Agent eine Verbindung herstellen soll. Dieses Feld wird nur angezeigt, wenn Sie auf der Registerkarte **Check Secure Parameter Definitions** (Sichere Parameterdefinitionen überprüfen) in der Prüfungsdefinition sichere Prüfungsparameter konfiguriert haben.
Proxy-Agent	Wählen Sie den Proxy-Agent aus, der der Prüfung zugeordnet werden soll. Dieses Feld wird nur angezeigt, wenn Sie mit einer Prüfungsinstanz arbeiten und eine der Optionen auf der Registerkarte **Proxy Settings** (Proxy-Einstellungen) in der Richtlinie der Instanz ausgewählt wurde.

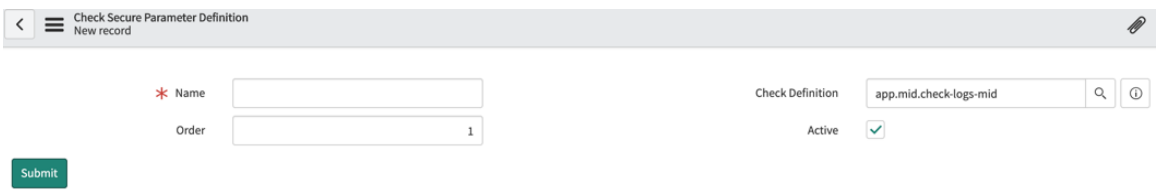
Sichere Parameter für Prüfungen erstellen

Beim Erstellen einer Prüfungsdefinition oder einer Prüfungsinstanz können Sie die Parameter konfigurieren, die gesichert werden sollen, wenn der Agent die Prüfung ausführt. Während der Prüfungsausführung werden die gesicherten Parameter verschleiert, wodurch ihre Informationen gesichert werden. Nur Anmeldeinformationen werden verschleiert.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Prüfungsdefinitionen**.
2. Wählen Sie in der angezeigten Liste eine Prüfungsdefinition aus.
   Die Seite **Check Definition** (Prüfungsdefinition) wird angezeigt.
3. Scrollen Sie zum Ende der Seite, und wechseln Sie zur Registerkarte **Check Secure Parameter Definitions** (Sichere Parameterdefinitionen überprüfen).
4. Klicken Sie auf **Neu**.
   Die Seite **Check Secure Parameter Definition New Record** (Sichere Parameterdefinitionen überprüfen: Neuer Datensatz) wird angezeigt.



5. Konfigurieren Sie die Felder auf der Seite.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feldname	Beschreibung
Name	Name des Parameters, formatiert als Referenzpräfix. So ist beispielsweise `cred_` ein Referenzpräfix für die Tabelle mit den Anmeldeinformationen.
Prüfungsdefinition	Name der mit dem Parameter verbundenen Prüfungsdefinition
Reihenfolge	Zahl, die die Reihenfolge angibt, in der der Parameter an den Prüfungsbefehl/das Prüfungsskript gesendet wird. Wenn Sie beispielsweise die folgenden Parameter konfigurieren: ◦ Name=**cred_user_name**, Reihenfolge=**1** ◦ Name=**cred_password**, Reihenfolge=**2** Dann wird der Parameter *username* an erster und der Parameter *password* an zweiter Stelle an die Standardeingabe gesendet. Der Befehl *READ* wird zuerst für den Parameter *username* und dann für den Parameter *password* ausgeführt. In Ihrem *Bash*-Skript können Sie dann *$username* und *$password* verwenden.
Aktiv	Aktivieren Sie dieses Kontrollkästchen, um den sicheren Parameter zu aktivieren.

6. Klicken Sie auf **Absenden**.
   Der konfigurierte Parameter wird in der Tabelle auf der Registerkarte **Check Secure Parameter Definitions** (Sichere Parameterdefinitionen überprüfen) angezeigt.

   Wiederholen Sie diesen Vorgang, um mehrere sichere Parameter einzugeben.

7. Geben Sie die sicheren Parameter in das Feld **Command prefix** (Befehlspräfix) der Prüfungsdefinition ein.

Neue Agent Client Collector-Richtlinie erstellen

Richtlinien bestehen aus den von Agent Client Collector überwachten CIs und den Prüfungen, die für diese CIs ausgeführt werden. Beim Erstellen einer Richtlinie konfigurieren Sie einen Filter, der die CIs bestimmt, für die die Prüfungen ausgeführt werden sollen. Beispielsweise eine Richtlinie zum Ausführen von Prüfungen auf allen Apache-Webservern. Sie können neue Richtlinien erstellen oder die Standardrichtlinien bearbeiten.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn Sie eine Prüfungsdefinition einer Richtlinie zuordnen, wird eine Kopie der Definition als Prüfungsinstanz erstellt. Diese Werte werden auf der Registerkarte **Prüfungsinstanzen** unten im Formular **Richtlinie** angezeigt. Alle Änderungen, die Sie an einer Prüfungsinstanz vornehmen, wirken sich nur auf die Instanz in der Richtlinie aus. Die ursprüngliche Prüfungsdefinition

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

bleibt unverändert. Wenn Sie die ursprüngliche Prüfungsdefinition ändern, gelten die Änderungen nicht für bereits erstellte Prüfungsinstanzen. Es wird empfohlen, eine Kopie einer Prüfungsdefinition zu erstellen, wenn Sie deren Standardparameter ändern, nachdem Sie eine oder mehrere Prüfungsdefinitionen in einer Richtlinie initiiert haben.

Einige Richtlinienprüfungen erfordern Anmeldeinformationen, andere nicht. Beispiel:

- Für Agent Client Collector sind keine Anmeldeinformationen für Prüfungen erforderlich, wenn diese auf demselben Server ausgeführt werden. Beim Zugriff auf Software, die Root-Zugriff oder Administratorzugriff erfordert (wie MySQL), sind hingegen Anmeldeinformationen erforderlich.
- Wenn Agent Client Collector als Proxy verwendet wird:
  - Anmeldeinformationen müssen aufgerufen werden, damit der Agent über SNMP oder andere Protokolle eine Verbindung zum Remote-Gerät herstellen kann.
  - Erhöhen Sie in der Datei `acc.yml` den im blauen Feld der Registerkarte **Proxy Settings** (Proxy-Einstellungen) angegebenen Wert *`cpu_percentage_limit`* des Agent.
- Wenn Agent Client Collector den HTTP-Endpunkt verwendet:
  - Wenn für die URL keine Anmeldung erforderlich ist (wie bei einer öffentlichen Website), werden keine Anmeldeinformationen benötigt.
  - Wenn für die URL eine Anmeldung erforderlich ist (wie bei einem API-Endpunkt), werden Anmeldeinformationen benötigt.

Auf der Registerkarte **Credentials** (Anmeldeinformationen) weisen Sie der Richtlinie wie folgt einen Anmeldeinformationsalias zu.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**.
2. Klicken Sie auf **Neu**.
   Die Seite **Policy** (Richtlinie) wird angezeigt.
3. Geben Sie in die Felder auf der Seite die in der folgenden Tabelle beschriebenen Werte ein:

Formular „Policy Definition“ (Richtliniendefinition)

Feld	Beschreibung
Name	Beschreibender Name für die Richtlinie
Beschreibung	Beschreibung der Richtlinie
Veröffentlichungsstatus	Hartcodiert als **Draft** (Entwurf), was bedeutet, dass die Richtlinie noch nicht veröffentlicht wurde. Dieses Feld können Sie nicht bearbeiten.
Hierarchie	Hartcodiert als **Keine**. Wenn der Richtlinie eine untergeordnete Richtlinie hinzugefügt wird, ändert sich der Wert in **Übergeordnet**. Untergeordnete Richtlinien haben den Wert **Untergeordnetes Element**.

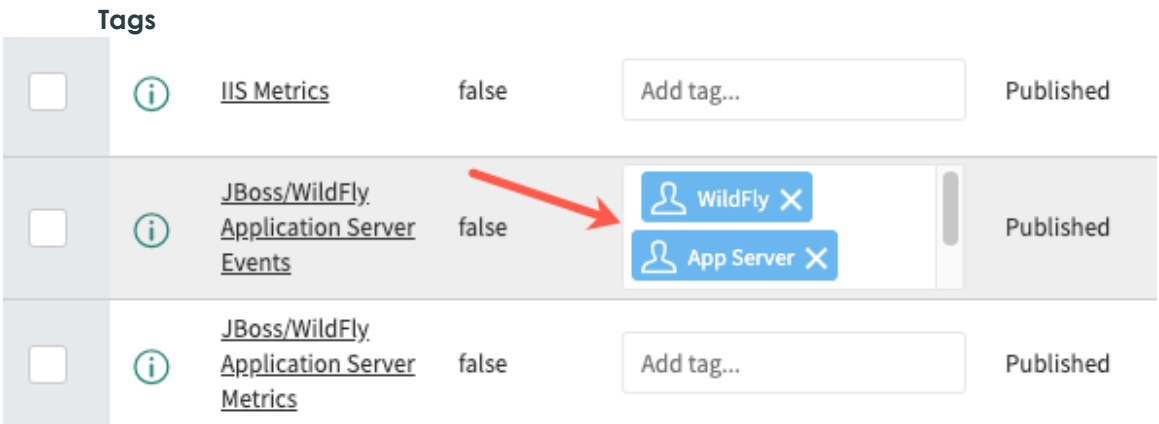
4. Wählen Sie auf der Registerkarte **Monitored CIs** (Überwachte CIs) eine der folgenden Optionen aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Manuelle Berechnung**: Wählen Sie diese Option aus, um die Richtlinie von der geplanten Richtlinienberechnung auszuschließen und Änderungen an den betroffenen CIs der Richtlinie zu ignorieren.

  Wählen Sie diese Option aus, wenn die Richtlinie ein einzelnes CI überwacht. Andernfalls dauert die Ausführung der geplanten Aufgabe „Überwachungsrichtlinien neu laden und veröffentlichen“ ungewöhnlich lange.

- **Monitored CI type by filter** (Überwachter CI-Typ durch Filter): Konfigurieren Sie die folgenden Unterfelder:
  - **Monitored CI type** (Überwachter CI-Typ): Wählen Sie den CI-Typ aus, der mithilfe der Richtlinienprüfungen überwacht werden soll.
  - **Filter**: Konfigurieren Sie einen Filter, sodass mit den Richtlinienprüfungen nur CI-Typen überwacht werden, die die angegebenen Kriterien erfüllen. In den verfügbaren Kriterien sind die **Tags** eines CI enthalten.



- **Monitored CI type by script** (Überwachter CI-Typ durch Skript): Ermöglicht die Angabe der überwachten CIs mithilfe eines Skripts. Mit einem Skript können Sie einen CI-Filter nicht nur für eine einzelne Tabelle, sondern für miteinander verknüpfte Tabellen erstellen. Bei der Suche nach einem CI können Sie beispielsweise einen Filter sowohl in einer Linux-Servertabelle als auch in einer Oracle-Tabelle festlegen. Am Ende des Skripts wird ein Objekt zurückgegeben, das die Tabelle und den Filter enthält.

  Beispiel für ein Skript, das im Feld **Monitored CI Script** (Überwachtes CI-Skript) angezeigt wird:

- **Monitored CI type by CMDB Group** (Überwachter CI-Typ nach CMDB-Gruppe): Ermöglicht die Angabe der überwachten CIs mithilfe eines Skripts. Wenn Sie diese Option auswählen, wird das Feld **Monitored CMDB group** (Überwachte CMDB-Gruppe)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

eingeblendet, in dem Sie eine CMDB-Gruppe auswählen, die der Richtlinie zugeordnet werden soll.

- Einzelheiten zu CMDB-Gruppen finden Sie unter CMDB-Gruppen .
- Weitere Informationen zum Erstellen einer CMDB-Abfrage mit dem CMDB-Abfragegenerator finden Sie unter CMDB-Abfrage mit dem CMDB-Abfragegenerator erstellen .

5. Wählen Sie Schecks in der Zelle **Verfügbar** auf der **Registerkarte Schecks** aus, und verschieben Sie sie in die Zelle **Ausgewählt**, damit sie in die Richtlinie aufgenommen werden.
   Prüfungen können mehrmals ausgewählt werden, wenn Sie mehrere Prozesse überwachen. Sie können auch im Feld **Filter checks by groups** (Prüfungen nach Gruppen filtern) eine Gruppe von Prüfungen auswählen, die Prüfungen der ausgewählten Gruppe in der Zelle **Available** (Verfügbar) anzeigt.
6. Wahlweise: Konfigurieren Sie einen Proxy-Server auf der Registerkarte **„Proxy-Einstellungen“**.

   (Optional) Konfigurieren Sie einen Proxy-Server nur dann, wenn Sie den Agent als Proxy zum Melden von Daten auf Remote-Computern verwenden. Details finden Sie unter Agent auf einem Proxy-Server konfigurieren.
7. Wählen Sie auf der Registerkarte **Zeitplanung** eine der folgenden Optionen aus:
   - **Interval-based scheduling** (Intervallbasierte Zeitplanung): Konfigurieren Sie das Zeitintervall (in Sekunden), um die Häufigkeit anzugeben, mit der die Prüfungen der Richtlinie ausgeführt werden.
   - **Cron-based scheduling** (Cron-basierte Zeitplanung): Ermöglicht die Konfiguration der Richtlinie so, dass sie nur während eines bestimmten Zeitraums oder bestimmter Zeitrahmen aktiv ist.

     a. Wählen Sie das Entsperren-Symbol ( ), um die Auswahl von Cron-Ausdrücken zu aktivieren.

     b. Wählen Sie das Suchsymbol ( ), um einen Cron-Ausdruck auszuwählen. Wählen Sie **Neu**, um einen neuen Cron-Ausdruck zu erstellen, oder wählen Sie einen der im Basissystem enthaltenen Cron-Ausdrücke aus:
     - Stündlich jede Nacht von 17:00 bis 7:00 Uhr
     - Minütlich jeden Tag von 8:00 bis 16:59 Uhr
     - Minütlich von Mo bis Fr von 8:00 bis 16:59 Uhr

     Wenn Sie einen neuen Cron-Ausdruck erstellen, müssen Sie ihn im gültigen Cron-Format eingeben.

     Der angegebene Cron-Ausdruck übernimmt die Zeitzone des Computers, auf dem der Agent gehostet wird.

   Hinweis: Wenn für die Prüfungsdefinition ein Wert für **Intervall** oder **Cron** angegeben wurde, überschreibt dieser Wert den in diesen Feldern konfigurierten Wert.
8. Wählen Sie im Feld **So senden Sie die Prüfergebnisse aus**, wie häufig Prüfergebnisse gesendet werden sollen.
   - Wenn sich der Ereignisschweregrad ändert (Standard für Ereignisprüfungen)
   - Prüfergebnisse immer senden (Standard für Nicht-Ereignisprüfungen)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Keine Prüfergebnisse senden
- Wenn sich die Prüfergebnisse ändern
- (Erweitert) Basierend auf Exit-Codes der Prüfung: Ergebnisse nur senden, wenn der Exit-Code 240 (OK), 241 (Warnung) oder 242 (Kritisch) lautet. Wenn die Befehlsausgabe jedoch leer ist, werden die Prüfergebnisse nicht gesendet, selbst wenn einer dieser Codes Teil des Exit-Codes ist.

9. Wählen Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) eine der folgenden Optionen aus:
   - **Credential name** (Anmeldeinformationsname): Wählen Sie Anmeldeinformationen aus, die der Richtlinie zugewiesen werden sollen. Die Parameter für Anmeldeinformationen werden auf Registerkarte **Check Secure Parameter Definitions** (Sichere Parameterdefinitionen überprüfen) der zugehörigen Prüfungsdefinition angezeigt.
   - **Credential alias** (Anmeldeinformationsalias): Klicken Sie auf das Suchsymbol, um einen Alias für die Anmeldeinformationen auszuwählen, mit dem bei den Prüfungen der Richtlinie eine Verbindung mit dem überwachten CI hergestellt wird. Die auf der Seite **Connection & Credential Aliases** (Aliasse für Verbindungen und Anmeldeinformationen) erstellten Optionen sind verfügbar. Einzelheiten zu Aliassen für Anmeldeinformationen finden Sie unter Aliasse für Anmeldeinformationen für Discovery .
10. Klicken Sie auf **Speichern**.
    Die folgenden Schaltflächen werden angezeigt:
    - **Veröffentlichen**: Veröffentlicht den Richtlinienentwurf und verschiebt seinen **Veröffentlichungsstatus** in **die Warteschlange**. Eine Richtlinie in der Warteschlange wird vom Richtlinienveröffentlichungsauftrag verarbeitet. Die Aufgabe berechnet, welche Agents die Richtlinie ausführen, und sendet die Richtlinie dann an den entsprechenden MID Servers. Die Aufgabe ändert dann den **Veröffentlichungsstatus** der Richtlinie in **Veröffentlicht**. Eine veröffentlichte Richtlinie ist für den Agent aktiv.
    - **Delete** (Löschen): Löscht die Richtlinie

Zugehörige Informationen

Richtlinienhierarchie erstellen

Richtlinienhierarchie erstellen

Richtlinien werden an Gruppen von zugehörigen CIs angehängt. Mit einer Untergruppe zugehöriger CIs können Sie mithilfe einer Richtlinienhierarchie eine neue Richtlinie an die Untergruppe anhängen, ohne die neue Richtlinie von Grund auf neu zu erstellen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Mit einer Richtlinienhierarchie können Sie eine Richtlinie als Vorlage zum Erstellen einer neuen Richtlinie verwenden, die dann an eine Untergruppe der CIs der ursprünglichen Richtlinie angehängt wird. Die ursprüngliche Richtlinie ist die **übergeordnete** Richtlinie, und die neue Richtlinie ist die **untergeordnete** Richtlinie.

Hinweis: Sie können keine untergeordnete Richtlinie erstellen, wenn ein Proxy-Agent für die übergeordnete Richtlinie vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**.
2. Wählen Sie auf der Seite **Policies** (Richtlinien) eine veröffentlichte Richtlinie mit dem Hierarchiewert **None** (Keine) oder **Parent** (Übergeordnet) aus.
3. Klicken Sie auf die Schaltfläche **Create Child** (Untergeordnet erstellen) oben auf der Seite oder unterhalb der Registerkarte **Monitored CIs** (Überwachte CIs).
   Eine neue (untergeordnete) Richtlinie mit denselben Parametern wie die ursprüngliche Richtlinie wird geöffnet. Der Name der Richtlinie lautet *<Policy name><date and time created>*.

   Hinweis: Die untergeordnete Richtlinie erbt die Parameter der übergeordneten Richtlinie nur bei der Erstellung. Es findet keine kontinuierliche Vererbung von der übergeordneten zur untergeordneten Richtlinie statt.

   Die folgenden Felder werden mit den angegebenen Werten hartcodiert angezeigt:

   Felder für untergeordnete Richtlinie

Feld	Wert
Veröffentlichungsstatus	Entwurf
Hierarchie	Untergeordnetes Element
Übergeordnet	<Name der übergeordneten Richtlinie>

   Der Wert im Feld **Order** (Reihenfolge) gibt die Priorität an, mit der der Agent an die Richtlinie angehängt wird. Je niedriger die Zahl, desto höher die Priorität, wobei jede erstellte untergeordnete Richtlinie jeweils einen höheren Wert als die vorhergehende Richtlinie annimmt. Diesen Wert können Sie bei Bedarf ändern.

4. Ändern Sie die Parameter der Richtlinie nach Bedarf.
   Die folgenden Schaltflächen werden auf der Seite der untergeordneten Richtlinie angezeigt:

Schaltfläche	Beschreibung
Compare to Parent (Mit übergeordneter vergleichen)	Klicken Sie auf diese Schaltfläche, um die Unterschiede zwischen der untergeordneten und der übergeordneten Richtlinie anzuzeigen.
Return to Parent (Zurück zu übergeordneter)	Klicken Sie auf diese Schaltfläche, um die Seite der untergeordneten Richtlinie zu verlassen (ohne zu speichern) und zur übergeordneten Richtlinie zurückzukehren.

   Die folgenden Schaltflächen werden auf der Seite der übergeordneten Richtlinie angezeigt:

Schaltfläche	Beschreibung
Deaktivieren	Wird für eine aktive Richtlinie angezeigt. Ermöglicht die Auswahl aus folgenden Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schaltfläche	Beschreibung
	◦ Übergeordnete Richtlinie und alle untergeordneten Richtlinien deaktivieren ◦ Nur die übergeordnete Richtlinie deaktivieren
Aktivieren	Wird für eine inaktive Richtlinie angezeigt. Ermöglicht die Auswahl aus folgenden Optionen: ◦ Übergeordnete Richtlinie und alle untergeordneten Richtlinien aktivieren ◦ Nur die übergeordnete Richtlinie aktivieren
Löschen	Ermöglicht die Auswahl aus folgenden Optionen: ◦ Übergeordnete Richtlinie und alle untergeordneten Richtlinien löschen ◦ Nur die übergeordnete Richtlinie löschen

5. Wählen Sie **Speichern**.
   Untergeordnete Richtlinien werden auf der Registerkarte **Child Policies** (Untergeordnete Richtlinien) der übergeordneten Richtlinie angezeigt.

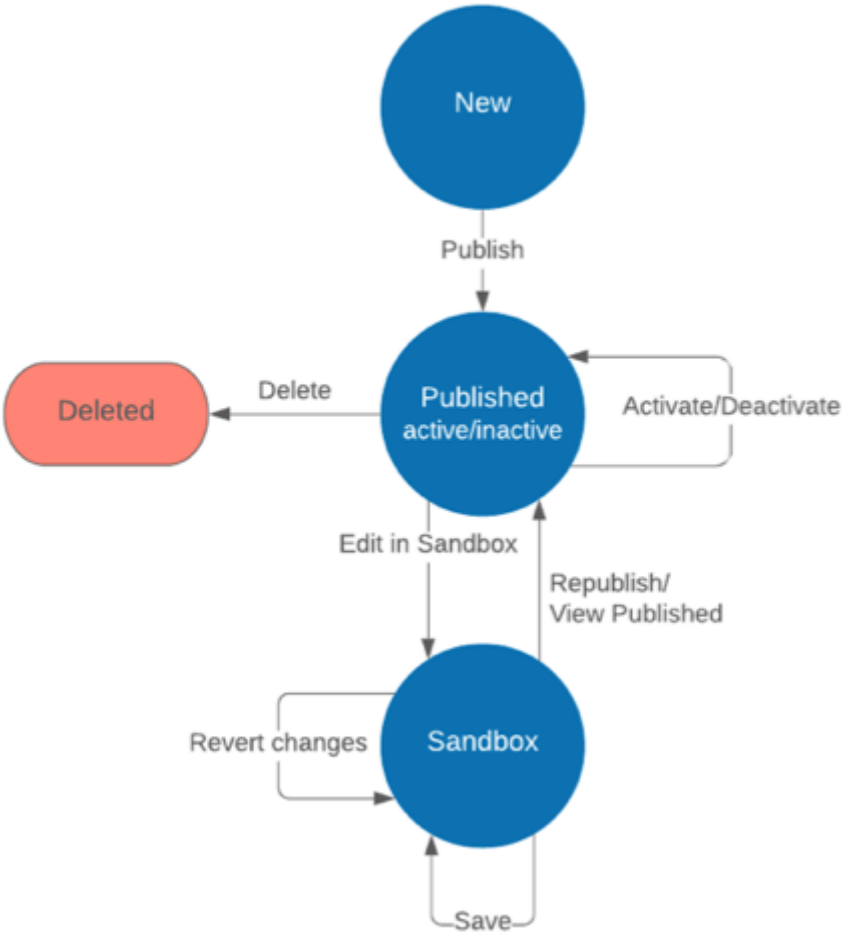
Veröffentlichte Richtlinien bearbeiten

Eine Richtlinie mit dem Status **Published** (Veröffentlicht) wurde über den MID-Server an den Agent übermittelt. Um eine veröffentlichte Richtlinie zu bearbeiten, müssen Sie die Bearbeitung aktivieren.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Um die Bearbeitung der Richtlinie zu aktivieren, wählen Sie eine veröffentlichte Richtlinie und dann die Option **Edit in Sandbox** (In Sandbox bearbeiten) aus. Sie bearbeiten die Richtlinie in der Sandbox und speichern, veröffentlichen oder löschen die Richtlinie nach Bedarf.
Das folgende Diagramm veranschaulicht den Bearbeitungsablauf einer veröffentlichten Richtlinie:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



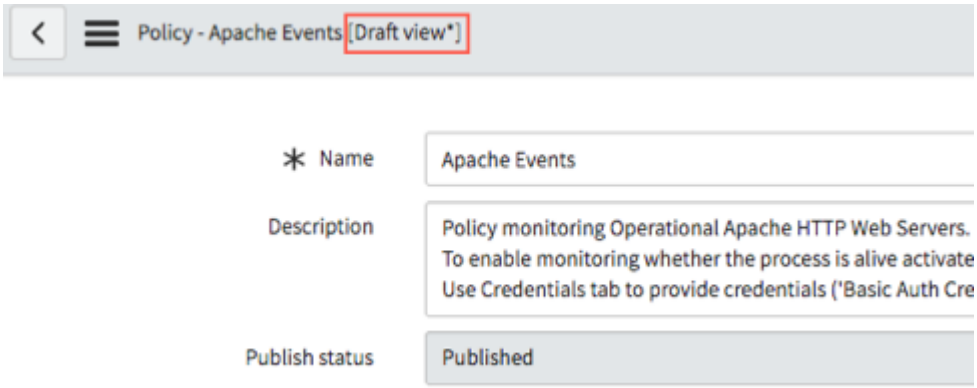
Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**.
2. Klicken Sie auf eine Richtlinie mit **Publish status** = **Published** (Veröffentlichungsstatus = Veröffentlicht).
3. Aktivieren oder deaktivieren Sie die Richtlinie nach Bedarf, indem Sie auf die Schaltfläche **Activate** (Aktivieren) oder **Deactivate** (Deaktivieren) klicken.
4. Klicken Sie auf die Schaltfläche **Edit in Sandbox** (In Sandbox bearbeiten).
   Daraufhin wird die Richtlinie in der **Draft view** (Entwurfsansicht) angezeigt, und Sie können ihre Felder bearbeiten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn Sie diese Option auswählen, können auch die Prüfungsinstanzen der Richtlinie bearbeitet werden.
- Auch in der **Draft view** (Entwurfsansicht) bleibt der **Publish status** (Veröffentlichungsstatus) der Richtlinie **Published** (Veröffentlicht).



Bei der Bearbeitung einer Richtlinie können Sie die folgenden Optionen auswählen:

Schaltflächen zum Bearbeiten von Richtlinien

Schaltfläche	Beschreibung
Alle Änderungen rückgängig machen	Setzt alle Bearbeitungen, die Sie an den Richtlinienfeldern in der Sandbox vorgenommen haben, auf die zuletzt veröffentlichten Werte zurück. Die Richtlinie wird in den **Publish status** (Veröffentlichungsstatus) **Published** (Veröffentlicht) zurückgesetzt und bleibt zur Bearbeitung in der **Draft view** (Entwurfsansicht). Diese Schaltfläche wird nur angezeigt, wenn Sie in den Richtlinienfeldern in der Sandbox Werte geändert haben.
Veröffentlichte anzeigen	Kehrt zur zuletzt veröffentlichten Richtlinie zurück. Die Richtlinie wird in den Status **Published** (Veröffentlicht) zurückgesetzt.
Speichern	Hiermit werden Ihre Bearbeitungen an den Richtlinienfeldern in der Sandbox gespeichert. Die Richtlinie bleibt in der **Draft view** (Entwurfsansicht), der **Publish status** (Veröffentlichungsstatus) lautet **Published*** (Veröffentlicht*). Das Sternchen zeigt an, dass die aktuell veröffentlichte Version nicht die aktuelle ist, da es unveröffentlichte Bearbeitungen gibt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schaltfläche	Beschreibung
Erneut veröffentlichen	Veröffentlicht Ihre Bearbeitungen an den Richtlinienfeldern in der Sandbox. Die Richtlinie wird mit Ihren Aktualisierungen gespeichert und als veröffentlichte Richtlinie geöffnet. ◦ Der **Veröffentlichungsstatus** der veröffentlichten Richtlinie wird auf „In **der Warteschlange“** gesetzt, wenn die Richtlinienänderungen Folgendes ergeben: ▪ Ein Change, in dem die Richtlinie von Agents ausgeführt wird (d. h. ein Change am überwachten CI-Filter). ▪ Eine Änderung der Prüfungsinstanzen der Richtlinie Der Veröffentlichungsauftrag der Richtlinie berechnet Richtlinien in der Warteschlange neu und sendet sie an die entsprechenden MID Servers. ◦ Der **Veröffentlichungsstatus** der veröffentlichten Richtlinie wird auf **Bereit zur Veröffentlichung** festgelegt, wenn die Änderungen an der Richtlinie keine Neuberechnung des Service Desk-Mitarbeiters erfordern (d. h. eine Änderung des Richtlinienintervalls). Der Veröffentlichungsauftrag der Richtlinie sendet Bereit zur Veröffentlichung von Richtlinien an die entsprechenden MID Servers, ohne diese Richtlinien neu zu berechnen. Nachdem der Richtlinienveröffentlichungsauftrag eine Richtlinie verarbeitet hat, wird der **Veröffentlichungsstatus** der Richtlinie in **Veröffentlicht**geändert. Diese Schaltfläche wird nur nach der Bearbeitung von Richtlinienfeldern einer Richtlinie angezeigt, deren **Publish status** somit gleich **Published*** (Veröffentlichungsstatus = Veröffentlicht*) ist.
Löschen	Löscht die Richtlinie Über diese Schaltfläche, die nur verfügbar ist, wenn die veröffentlichte Richtlinie angezeigt wird, wird sowohl die veröffentlichte Richtlinien als auch die die Richtlinie in der Sandbox gelöscht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie Schecks in der Zelle **Verfügbar** der Registerkarte Schecks aus, und verschieben Sie sie in die Zelle **Ausgewählt**, damit sie in die Richtlinie aufgenommen werden. Prüfungen können mehrmals ausgewählt werden, wenn Sie mehrere Prozesse überwachen. Sie können auch im Feld **Filter checks by groups** (Prüfungen nach Gruppen filtern) eine Gruppe von Prüfungen auswählen, die Prüfungen der ausgewählten Gruppe in der Zelle **Available** (Verfügbar) anzeigt.
6. Zeigen Sie in der Tabelle **Check Instances** (Prüfungsinstanzen) die für die Richtlinie konfigurierten Prüfungsinstanzen an, oder wählen Sie eine Prüfungsinstanz zur Bearbeitung aus.
7. Zeigen Sie auf der Registerkarte **Agents** die Agents an, von denen die Richtlinie ausgeführt wird.

   Die Liste der Agents wird basierend auf den überwachten CIs berechnet.

   Diese Registerkarte ist nur für veröffentlichte Richtlinien verfügbar.

Servicefilter für eine Richtlinie erstellen

Konfigurieren Sie einen Servicefilter, sodass mit der Richtlinie nur die Services überwacht werden, die dem Filter entsprechen.

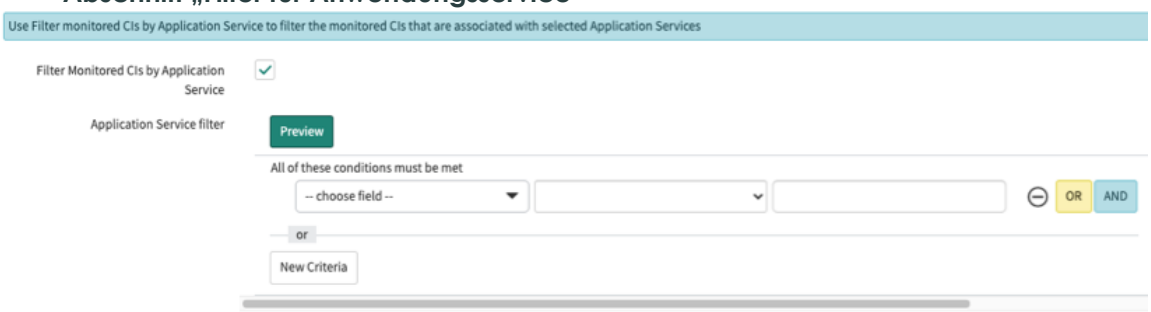
Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**.
   Die Seite **Richtlinien** wird angezeigt.
2. Wählen Sie eine Richtlinie aus.
   Die Detailseite der Richtlinie wird angezeigt.
3. Wählen Sie die Schaltfläche **In Sandbox bearbeiten** aus, um die Bearbeitung des Formulars zu aktivieren.
4. Aktivieren Sie auf der Registerkarte „Überwachte CIs“ das Kontrollkästchen **Filter Monitored CIs by service** (Überwachte CIs nach Service filtern).
   Der Abschnitt **Filter für Anwendungsservice** wird angezeigt.

Abschnitt „Filter für Anwendungsservice“



5. Konfigurieren Sie Bedingungen in den Feldern und wählen Sie unten auf der Seite **Speichern** aus.
   Die Richtlinie wird mit dem angegebenen Servicefilter konfiguriert. Nur CIs, die dem Servicefilter entsprechen, werden in die Protokolle der Richtlinie aufgenommen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector-Richtlinien exportieren und importieren

Sie können eine oder mehrere Agent Client Collector-Richtlinien aus einer ServiceNow-Instanz in eine andere verschieben, indem Sie die Richtlinien exportieren und dann in der Zielinstanz importieren. Nur veröffentlichte Richtlinien können exportiert werden.

Vorbereitungen

Vergewissern Sie sich, dass Sie die Richtlinien, die Sie exportieren möchten, in der Quellinstanz veröffentlicht haben.

Hinweis: Wenn Sie in einer domänengetrennten Umgebung arbeiten, werden importierte Richtlinien von der Quellinstanzdomäne zur identischen Domäne in der Zielinstanz verschoben. Daher müssen Sie sicherstellen, dass Sie in der Zielinstanz dieselben Domänen definiert haben wie in der Quellinstanz, indem Sie entweder die Quellinstanz klonen oder Domänen aus der Quellinstanz exportieren und in die Zielinstanz importieren.

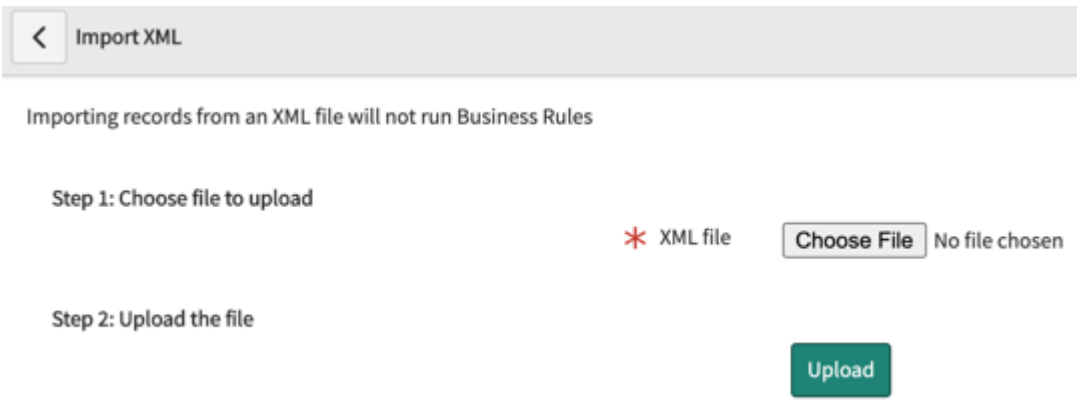
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**.
2. Aktivieren Sie die Kontrollkästchen der veröffentlichten Richtlinien, die Sie exportieren möchten.
3. Wählen Sie in der Liste **Actions on selected rows...** (Aktionen für ausgewählte Zeilen...) unter der Liste der Richtlinien die Option **Export policies** (Richtlinien exportieren) aus.
   Ein Bestätigungsdialogfeld wird angezeigt.
4. Klicken Sie auf **Ja**.
   Die ausgewählten Richtlinien werden als Update Set-Datei im XML-Format exportiert und in Ihrem Browser heruntergeladen. Das generierte Update Set weist die folgende Namenskonvention auf: `AccPolicyExport <Aktuelles Datum und aktuelle Uhrzeit>`. Beispiel: `AccPolicyExport 2020-08-11 15:35:05`.
5. Importieren Sie die Richtlinie in die Zielinstanz.

   a. Navigieren zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.
   Die Seite **Retrieved Update Sets** (Abgerufene Update Sets) wird angezeigt.

   b. Klicken Sie mit der rechten Maustaste auf einen der Tabellenheader, und wählen Sie **Import XML** (XML importieren) aus.
   Die Seite **Import XML** (XML importieren) wird angezeigt.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Klicken Sie auf die Schaltfläche **Choose File** (Datei wählen), und wählen Sie das zuvor heruntergeladene Update Set für den Import aus.

d. Klicken Sie auf **Hochladen**.

> **Hinweis:** Wenn sich der exportierte Inhalt in einem Bereich befindet, wird das importierte Update Set auf der Seite **Retrieved Update Sets** (Abgerufene Update Sets) in Form von mehreren Datensätzen angezeigt. Der Datensatz mit dem Bereich **Global** ist das übergeordnete Element, die anderen Datensätze werden mit dem Global-Datensatz als übergeordnetes Update Set angezeigt. Der Importvorgang lässt sich nur mit dem Global-Datensatz des Update Set initiieren.

e. Wählen Sie das Update Set **Global** aus.

f. Klicken Sie auf der Seite **Retrieved Update Sets** (Abgerufene Update Sets) auf **Preview Update Set Batch** (Vorschau auf Update Set-Batch), um zu überprüfen, ob Konflikte mit vorhandenen Richtlinien in der Zielinstanz bestehen.
Lösen Sie Konflikte gegebenenfalls.

g. Wenn keine Konflikte bestehen, klicken Sie auf **Commit Update Set Batch** (Commit für Update Set-Batch ausführen), um das Update Set zu validieren und zu bestätigen.

h. Navigieren zu **Agent Client Collector** > **Richtlinien** und überprüfen Sie, ob die importierten Richtlinien in der Liste Richtlinien angezeigt werden.
Die importierten Richtlinien werden mit den entsprechenden MID Serversn in der Zielinstanz synchronisiert und können sofort verwendet werden.

> **Hinweis:** Beim Importprozess werden alle vorhandenen Richtlinien in der Zielinstanz überschrieben, und die importierten Richtlinien werden auf **Published** (Veröffentlicht) gesetzt. Entwurfskopien von Richtlinien, die in der Zielinstanz erstellt wurden, werden jedoch nicht geändert. Löschen Sie daher nach Abschluss des Importvorgangs Entwurfsdatensätze der importierten Richtlinien, da diese Datensätze nicht mit den veröffentlichten Richtlinien in der Zielinstanz synchronisiert werden.

Prüfungstyp erstellen

Erstellen Sie einen Prüfungstyp, um den Befehl `osquery` für den Agent auszuführen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_integration oder agent_client_collector_admin

Prozedur

1. Geben Sie in einer Ereignismanagement-Instanz in der Navigationsleiste `sn_agent_check_type.list` ein.
   Die Seite **Check Types** (Prüfungstypen) wird angezeigt.
2. Klicken Sie auf **Neu**.
   Die Seite `Check Type - New Record` (Prüfungstyp – Neuer Datensatz) wird angezeigt.
3. Geben Sie im Feld **Name** den Namen `osquery` ein.
4. Geben Sie in das Feld **Instance Script** (Instanzskript) das folgende Skript ein:

```
for (var index = 0; index < checkResults.length; index++) {
var check = checkResults[index].check;
gs.info('result ' +
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
index + ': requestId: ' +
check.requestId + ' agent_name: ' +
checkResults[index].agent_id +
' ci_id: ' + check.ci_id +
' status: ' + check.status +
' output: ' + check.output);

}
```

Sie können dieses Skript nach Bedarf ändern. Mit diesem Ausgangsskript können Sie jedoch überprüfen, ob die Einrichtung erfolgreich war.

5. Klicken Sie auf **Absenden**.

Prüfungsdefinitionen erstellen

Erstellen Sie eine Prüfungsdefinition, um den Befehl `osquery` für den Agent auszuführen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_integration oder agent_client_collector_admin

Prozedur

1. Navigieren Sie in einer Instanz Ereignismanagement zu **Agent Client Collector** > **Prüfungsdefinitionen**.
2. Klicken Sie auf **Neu**.
3. Geben Sie im Feld **Name** den Namen `util.osquery` ein.
4. Geben Sie im Feld **Check type** (Prüfungstyp) den Namen `osquery` ein.
5. Geben Sie im Feld **Command** (Befehl) das folgende Skript ein:

```
osqueryi  --logger_min_status 1 --json "{{.labels.params_query}} "
```

6. Geben Sie im Abschnitt **Parameter** die folgenden Werte für eine Prüfungsparameterdefinition ein.

Spalte	Wert
Name	query
Standardwert	* aus logged_in_users auswählen
Obligatorisch	Wahr

7. Klicken Sie auf **Test check** (Testüberprüfung), und wählen Sie einen der verfügbaren Agents aus.
   Das angezeigte Testergebnis gibt an, ob die Überprüfung erfolgreich war oder fehlgeschlagen ist.

Prüfungen aus Agent Client Collector-Community aktivieren

Sie können Prüfungen aus der GitHub-Community abrufen und zur Verwendung in Agent Client Collector (ACC) anpassen oder eigene Skripts erstellen. Erstellen Sie ein Plugin mit der benutzerdefinierten Sensu-Prüfung, und installieren Sie es für eine ServiceNow-Instanz.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Kopieren Sie eine Prüfung aus der GitHub-Community auf Ihren lokalen Computer.
2. Erstellen Sie eine `tar.gz`-Datei, die an Ihr Plugin angehängt werden soll:

   a. Erstellen Sie einen Ordner auf Ihrem lokalen Computer.

   b. Erstellen Sie einen Unterordner mit der Bezeichnung `bin`.

   c. Legen Sie die Prüfungen im Ordner `bin` ab, die Sie ausführen möchten (Skripts und ausführbare Dateien).

   d. Erteilen Sie in einer Linux-Umgebung den Prüfungen Ausführungsberechtigungen, indem Sie für jede Prüfung *`chmod + x filename`* ausführen.

   e. Navigieren Sie zum übergeordneten Ordner (über dem bin-Ordner).

   f. Führen Sie in einer Linux-Umgebung den Befehl *`tar -C <parent_folder_name> --zcvf <my_plugin_name>.tar.gz *`* aus.
   Verwenden Sie in einer Windows-Umgebung ein Archivierungsdienstprogramm, das das Format `tar.gz` unterstützt.

   g. Achten Sie in einer Windows-Umgebung darauf, dass in den Ordner `bin` die folgenden Skripts eingefügt werden:

   - Batch-Skript, das für die Ausführung des Prüfbefehls und zur Initiierung der Ausführung konfiguriert ist. Beispiel:*`powershell <%~dp0>|test.ps1`*.

     Die Variable *`<%~dp0>`* verweist auf das Laufwerk (*`d`*) und den Pfad (*`p`*) der Batch-Datei.

   - Das relevante Skript (z. B. `test.ps1`), das im Batch-Skript ausgeführt werden soll

3. Erstellen Sie ein neues ACC-Plugin (siehe Agent Client Collector -Plugins erstellen und bearbeiten).
4. Testen Sie das neue Plugin.

   a. Erstellen Sie eine neue Prüfungsdefinition für die angepasste Sensu-Prüfung.
   Details finden Sie unter Prüfungen erstellen und bearbeiten.

   b. Navigieren Sie auf der Seite **Check Definition** (Prüfungsdefinition) zum Abschnitt **Related Links** (Zugehörige Links), und klicken Sie auf **Generate allow list content** (Inhalte für Allow-Liste generieren).

   c. Kopieren Sie die Einträge, die Sie in die Allow-Liste aufnehmen möchten, und fügen Sie sie der Datei `check-allow-list.json` des Agent entweder manuell oder mit einem Automatisierungs-Tool hinzu.
   Der Speicherort dieser Datei ist im Parameter `allow-list` der Datei `acc.yml` des Agent angegeben.

   d. Erstellen Sie eine neue Richtlinie, und fügen Sie die neu erstellte Prüfungsdefinition hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Details zum Erstellen einer Richtlinie finden Sie unter Neue Agent Client Collector-Richtlinie erstellen.

e. Wählen Sie die Prüfungsdefinition aus, und klicken Sie im Abschnitt **Related Links** (Zugehörige Links) auf **Test check** (Testüberprüfung).

5. Aktivieren Sie Anmeldeinformationen beim Testen einer Prüfung:

a. Navigieren zu **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.

b. Klicken Sie auf **Neu**.

c. Wählen Sie den Typ der Anmeldeinformationen aus, die Sie erstellen möchten. Weitere Informationen zum Erstellen von Anmeldeinformationen finden Sie unter Alias für Verbindungen und Anmeldeinformationen erstellen .

d. Geben Sie Werte in die Felder auf der Seite ein, um dem ausgewählten Anmeldeinformationstyp Anmeldeinformationen zuzuweisen.

e. Klicken Sie auf **Absenden**.

6. Erstellen Sie für Ihre Prüfung sichere Parameter (siehe Sichere Parameter für Prüfungen erstellen).

Agent Client Collector Datensammlung wird aktiviert

Sie können Aktionen ausführen, um die Datenerfassung von den Hosts zu verbessern, auf denen Agent Client Collector ausgeführt wird.

Aufruf-API zum Senden einer osquery-Anforderung erstellen

Erstellen Sie ein Hintergrundskript, um eine `osquery`-Anforderung zu senden. Die `osquery`-Anforderung ermöglicht die Datenerfassung im Betriebssystem Ihres Hosts.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Erstellen Sie das folgende Hintergrundskript:
   - `"MTLV9DE22016"` ist der Name des Servers, auf dem ein Agent ausgeführt wird.
   - `"c8bf9072539333003e76ddeeff7b12c5"` ist die sys_id der zuvor erstellten Prüfungsdefinition.

```
cis = new GlideRecord("cmdb_ci_server");
    cis.addQuery("name", "MTLV9DE22016");
    cis.query();
    check = {
        "checkDefId": "c8bf9072539333003e76ddeeff7b12c5",
        "params": {
            "query": "select pid,cmdLine from processes limit 4"
        }
    };
    var agentNow = new sn_agent.AgentNowHandler();
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    gs.info('request_id: ' +
agentNow.runCheckForCis(cis,check,'1',60000));
```

2. Führen Sie das Skript zur Ausgabe der Anforderungs-ID aus:
   request_id: `eefbff7ab75733003e766068de11a981`
3. Überprüfen Sie die Systemprotokolle auf Nachrichten vom Instanzskript.

```
result 0 requestId: 06c6c887b79733003e766068de11a912 agent_name:
 MTLV9DE22016 ci_id:
00726c36539333003e76ddeeff7b12db status: 0 output: [
{"cmdline":"","pid":"0"},
{"cmdline":"","pid":"1"},
{"cmdline":"","pid":"45"},
{"cmdline":"","pid":"46"}
]
```

Zeigen Sie die Hostdatensammlung für einen Agent an

Führen Sie eine Datensammlung auf dem Host eines Agent durch, um die auf dem Host ausgeführten Komponenten zu erkennen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Die regelmäßige Aufgabe „Hostdaten für Service Desk-Mitarbeiter neu laden“ sammelt Hostdaten und wird stündlich für Folgendes ausgeführt:

- Hosts, die in den letzten 12 Stunden nicht erkannt wurden.
- Host, bei dem Discovery fehlgeschlagen ist.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
   Zeigen Sie in der Spalte **Datensammlung des Hosts** den Status der Datensammlung auf dem Host des Agent an. Mögliche Status:

Status der Hostdatensammlung

Status	Beschreibung
<empty>	Gibt an, dass der Agent innerhalb der letzten Minute hinzugefügt wurde und die geplante Aufgabe „Überwachungsrichtlinien aktualisieren und veröffentlichen“ noch nicht ausgeführt wurde, um die Datenerfassung zu initiieren. Die Aufgabe wird jede Minute ausgeführt.
Gesammelt (grün)	Die Erfassung der Hostdaten ist abgeschlossen.
Wird gesammelt (gelb)	Hostdatenerfassung wird ausgeführt.
Sammlung fehlgeschlagen (rot)	Hostdatenerfassung fehlgeschlagen.

2. Wahlweise: Suchen Sie die Spalte **Zuletzt gesammelte Hostdaten,** um anzuzeigen, wann die Datenerfassung zuletzt auf dem Host durchgeführt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector-Zulassungsliste generieren

Geben Sie die Prüfungen an, die in die Liste der Prüfungen aufgenommen werden sollen, die für den Agent ausgeführt werden können.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Die standardmäßige Allow-Liste enthält alle validierten Prüfungen und ist in den Richtlinien des Basissystems enthalten. Wenn die Allow-Liste nicht richtig gelesen werden kann, werden keine Prüfungen für den Agent ausgeführt.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Prüfungsdefinitionen**.
   Die Seite **Check Definitions** (Prüfungsdefinitionen) wird angezeigt.
2. Klicken Sie im Abschnitt **Related Links** (Zugehörige Links) unten auf der Seite auf **Generate allow list** (Allow-Liste generieren).

   Hinweis: Alternativ können Sie eine Prüfungsdefinition oder den Datensatz einer Prüfungsinstanz auswählen und auf **Generate allow list** (Allow-Liste generieren) klicken, um eine vollständige Allow-Liste zu generieren.

   Die Seite **Agent Client Collector Command Allow-list Generator** (Agent Client Collector: Befehls-Allow-Listen-Generator) wird mit einer Liste der Prüfungen aus dem Feld **Befehl** der Prüfungsinstanzdatensätze angezeigt.

   Die Werte werden mit den folgenden Attributen angezeigt:

   Befehlsattribute

Attribut	Beschreibung
exec	Befehl, der ausgeführt wird
args	Mögliche Argumentzeichenfolgen
skip_arguments	Boolescher Wert. Legt fest, ob geprüft werden soll, ob das Argument der Allow-Liste hinzugefügt wurde ◦ **true**: Überspringt die Argumentvalidierung und prüft nur auf ungültige Zeichen, insbesondere |;\<>&'$() ◦ **false**: Führt eine Argumentvalidierung durch, um sicherzustellen, dass das Argument in der Allow-Liste enthalten ist. Wenn es nicht enthalten ist, kann der Befehl nicht ausgeführt werden.

3. Kopieren Sie die Einträge, die Sie in die Allow-Liste aufnehmen möchten, und fügen Sie sie der Datei `check-allow-list.json` des Agent entweder manuell oder mit einem Automatisierungs-Tool hinzu.
   Der Speicherort dieser Datei wird im Parameter *`allow-list`* der Datei `acc.yml` des Agent angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hostdatensammlung bei Bedarf ausführen

Sie können die Hostdatensammlung bei Bedarf durchführen, wenn Sie eine Datensammlung durchführen müssen, bevor die Ausführung der Aufgabe geplant ist.

Vorbereitungen

Stellen Sie sicher, dass Sie über ausreichende Berechtigungen zum Erstellen von CIs verfügen.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
   Die Seite **Agent Client Collectors** wird angezeigt.
2. Wählen Sie einen Agent mit **Status = Alive** aus.
3. Klicken Sie im Agent-Formular auf die Schaltfläche **Hostdaten erfassen**.

Agent Client Collector-Datensammlung anhalten

Wenn der CPU-Verbrauch auf Ihrem Server zu hoch wird, können Sie die Agent Client Collector-Datensammlung manuell deaktivieren, um alle vom Agent durchgeführten Prüfungen mit Ausnahme der Keep-Alive-Nachrichten des Agent anzuhalten.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
   Die Seite **Agent Client Collectors** wird mit einer Liste der konfigurierten Agents angezeigt.
2. Aktivieren Sie die Kontrollkästchen neben den relevanten Agents.
3. Wählen Sie in der Dropdown-Liste **Actions on selected rows...** (Aktionen für ausgewählte Zeilen...) die Option **Pause data collection** (Datensammlung anhalten) aus, um die Datensammlung auf den Agents anzuhalten (**Data Collection = Off (manual)** (Datensammlung = Aus (manuell))).

   Wählen Sie **Resume data collection** (Datensammlung fortsetzen) aus, um die Datensammlung auf den Agents fortzusetzen.

   Alternativ können Sie den Status eines Agent festlegen, indem Sie den Agent auswählen und im Abschnitt **Related Links** (Zugehörige Links) auf den Link **Pause data collection** (Datensammlung anhalten) klicken, um die Datensammlung für den Agent anzuhalten. Um die Datensammlung für den Agent wieder aufzunehmen, klicken Sie auf den Link **Resume data collection** (Datensammlung fortsetzen).

Validieren Sie Assets auf der MID-Server

Validieren Sie Assets in Ihrer Instanz von MID-Server, um sicherzustellen, dass sie mit den Assets in Ihrer Instanz von ServiceNow übereinstimmen. Durch das Validieren von Assets wird sichergestellt, dass die -Instanz genaue Daten für alle Ihre MID-Server -Assets bereitstellt.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **MID-Server**.
2. Wählen Sie einen MID-Server -Eintrag auf der Seite MID Servers aus.
3. Wählen Sie den Link **Assets validieren** aus.
   Die Seite „ **Warteschlangen**“ wird mit der ECC-Warteschlange angezeigt.
4. Aktualisieren Sie die Warteschlange, um den neuen Eingabedatensatz anzuzeigen.
5. Wählen Sie den Datensatz aus, um die Ergebnisse anzuzeigen.

   Der Validierungsstatus wird im Abschnitt **„Nutzlast“** des Formulars angezeigt.

   Wenn Assets nicht validiert werden, starten Sie MID-Serverneu. Assets werden automatisch synchronisiert, wenn MID-Server neu gestartet wird.

Validiert Assets auf Agents

Validieren Sie Assets auf Ihren Agents, um sicherzustellen, dass sie mit den Assets in Ihrer Instanz ServiceNow übereinstimmen. Durch das Validieren von Assets wird sichergestellt, dass die Instanz genaue Daten zu den Assets aller Service Desk-Mitarbeiter bereitstellt.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Nur Assets, die ausgeführt werden können, werden validiert. Wenn Sie beispielsweise einen -Agent auf einem macOSausführen, werden nur macOS -Assets in Ihrer Instanz validiert.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
2. Wählen Sie auf der Seite **„Agent Client Collectors“** einen Agent aus.
3. Wählen Sie den Link **Assets validieren** aus.
   Die Seite „ **Warteschlangen**“ wird mit der ECC-Warteschlange angezeigt.
4. Aktualisieren Sie die Warteschlange, um den neuen Eingabedatensatz anzuzeigen.
5. Wählen Sie den Datensatz aus, um die Ergebnisse anzuzeigen.

   Der Validierungsstatus wird im Abschnitt **„Nutzlast“** des Formulars angezeigt.

   Wenn Assets nicht validiert werden, navigieren Sie zurück zur Seite **„Agent Client Collectors“**, und wählen Sie den Link **Assets löschen** aus.

   Die Assets werden automatisch neu synchronisiert, wenn das nächste Mal ein Befehl ausgeführt wird, der das Asset erfordert.

Agent Client Collector -Protokolle werden verwendet

Verwenden Sie Protokolle Agent Client Collector, um Ereignisse in Ihrem System nachzuverfolgen. Protokollebenen geben den Schweregrad jedes Ereignisses an.

Agent Client Collector-Protokollebenen konfigurieren

Sie konfigurieren die Protokollebenen, die die Agent Client Collector-Protokolle einhalten sollen. Alle Events, die die angegebene Protokollebene erreichen oder sie überschreiten, werden in den Agent Client Collector-Protokollen verzeichnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Geben Sie die gewünschte Protokollebene in der Konfigurationsdatei `acc.yml` an. Alternativ können Sie die Protokollebene wie folgt als Argument in der Kennzeichnung der Befehlszeile `--loglevel` angeben:

```
acc start --log level debug
```

2. Starten Sie den Agent mit dem Servicemanager neu:
   - **Linux**:

```
sudo service acc restart
```

   - **Windows**:

```
sc.exe stop AgentClientCollector
sc.exe start AgentClientCollector
```

   - **macOS**:

```
sudo launchctl load -w /Library/LaunchDaemons/com.sn.acc.plist
```

Hinweis: Sie müssen den Service neu starten, nachdem Sie die Protokollebene geändert haben.

Agent Client Collector-Protokolle anzeigen

Sie können die Aktivitätsprotokolle für Agent Client Collector anzeigen.

Warum und wann dieser Vorgang ausgeführt wird
Agent Client Collector Protokolle sind zugänglich von:

- **Linux**: `/var/log/servicenow/agent-client-collector/acc.log`
- **Windows**: Durch die Konfigurationskennzeichnung `log-file` angegebener Speicherort. Der Standardspeicherort lautet: `C:/ProgramData/ServiceNow/agent-client-collector/log/acc.log`.

  Wenn das Verzeichnis `C:/ProgramData` ausgeblendet ist (z. B. bei älteren Windows-Versionen), ändern Sie den Explorer-Filter, um ausgeblendete Elemente anzuzeigen.
- **macOS**: Der Standardspeicherort lautet: `/Library/Application\ Support/servicenow/agent-client-collector`

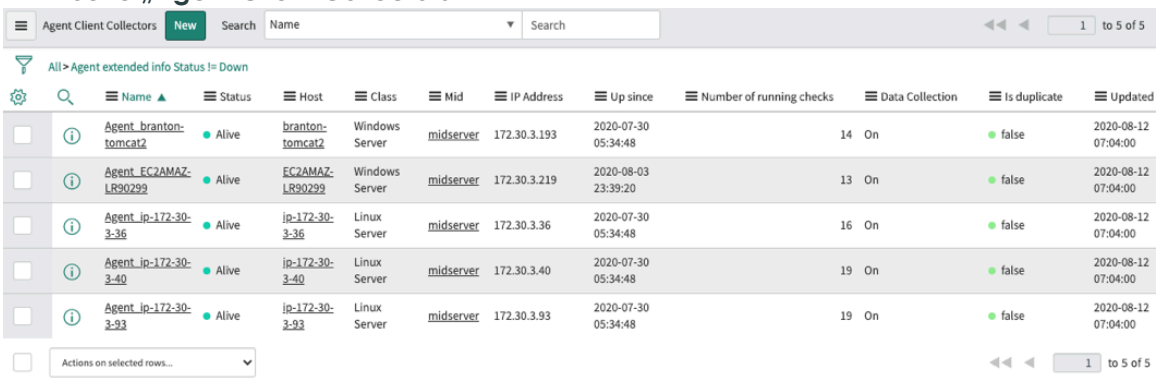
Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
   Die Seite **Agent Client Collectors** wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite „Agent Client Collectors“



Die angezeigten Spalten sind diejenigen, die ausgewählt werden, wenn Sie auf das Einstellungssymbol klicken.

Die Spalte **Host** gibt den Hostnamen des Agent an.

Die Spalte **Class** (Klasse) gibt den CI-Typ des Agent an.

2. Wählen Sie einen HR-Mitarbeiter aus.
   Die Seite **Agent Client Collector** wird angezeigt.
3. Klicken Sie im Abschnitt **Related Links (Zugehörige Links)** auf **Grab Agent Log (Agent-Protokoll abrufen)**.
   Die Seite **Queues** (Warteschlangen) wird für den ausgewählten Agent geöffnet.
4. Aktualisieren Sie die Seite, und klicken Sie auf den entsprechenden Eintrag mit dem Wert **Queue = input** (Warteschlange = Eingabe).
   Im Abschnitt **„Nutzlast“** des Formulars **„Warteschlange“** wird das Protokoll für Agent Client Collectorangezeigt.

Protokollüberwachung in einer Linux-Umgebung aktivieren

Um Überwachungsprotokolle in einer Linux-Umgebung zu aktivieren, wählen Sie die relevante Richtlinie aus, und weisen Sie ihr spezifische Prüfungsparameter zu. Wenn die Protokollüberwachung aktiviert ist und eine angegebene Zeichenfolge im überwachten Protokoll erkannt wird, wird ein Event erstellt.

Vorbereitungen

Stellen Sie sicher, dass der Benutzer servicenow Zugriff auf die überwachte Protokolldatei hat oder dass der angegebene Benutzer den `sudo`-Befehl ausführen kann.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**.
2. Wählen Sie die Richtlinie zur **Linux-Protokollüberwachung** aus.
3. Wählen Sie **util.check-logs** auf der Registerkarte **Check Instances (Prüfungsinstanzen)** aus, um die Überwachung von Protokolldateien zu aktivieren, die nicht dem *root*-Benutzer gehören.
   Stellen Sie sicher, dass der Agent Client Collector *servicenow*-Benutzer über Leseberechtigungen für die überwachte Protokolldatei verfügt.
4. Geben Sie die Protokolldatei an, die bei der Prüfung durchsucht werden soll:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie auf der Registerkarte **Check Parameter Definitions** (Definition von Prüfungsparametern) am unteren Seitenrand in der Spalte **Name** den Eintrag **file** (Datei) aus.

b. Geben Sie im Feld **Default value** (Standardwert) den Pfad zu der Protokolldatei ein, die Sie durchsuchen möchten.

5. Geben Sie die Zeichenfolge an, die Sie im Protokoll suchen möchten:

a. Wählen Sie auf der Registerkarte **Check Parameter Definitions** (Definition von Prüfungsparametern) am unteren Seitenrand in der Spalte **Name** den Eintrag **pattern** (Muster) aus.

b. Geben Sie im Feld **Default value** (Standardwert) die Suchmuster-Zeichenfolgen ein, nach denen Sie in der Protokolldatei suchen möchten, z. B. `404` und `Error`. Die Standardwerte lauten `SEVERE` (Schwerwiegend) und `Exception`(Ausnahme).

Stellen Sie sicher, dass Sie mehrere Muster durch eine Pipe (|) trennen und als Parameter in Anführungszeichen weitergeben. Zum Beispiel: `"SEVERE|404"`.

6. Klicken Sie auf **Update** (Aktualisieren), um Ihre Prüfungsinstanz zu speichern und zur Seite **Policy - Linux Log Monitoring** (Richtlinie - Linux-Protokollüberwachung) zurückkehren.

7. Wählen Sie die Prüfung **util.check-logs-sudo** aus, um Protokolle zu überwachen, die dem Root-Benutzer gehören.

8. Wiederholen Sie die Schritte 4 und 5, um Protokolle zu überwachen, die dem Root-Benutzer gehören.

9. Ändern Sie für die Prüfung **util.check-logs-sudo** wie folgt die Datei `etc/sudoers` auf dem Host oder virtuellen Linux-Computer:
Wenn der Agent am Standardspeicherort des Hosts (`/usr/share/servicenow/agent-client-collector`) oder auf einem virtuellen Linux-Computer installiert ist, fügen Sie der Datei `/etc/sudoers` die folgende Zeichenfolge hinzu:

```
servicenow ALL=
 SETENV: /
var/cache/servicenow/agent-client-collector/monitoring-plugin-linux/b
in/check-log.rb *
Defaults:servicenow !requiretty
Defaults exempt_group += servicenow
```

10. Klicken Sie auf der Seite **Policy** (Richtlinie) auf **Save** (Speichern) und dann auf **Publish** (Veröffentlichen), um die Richtlinie zum Überwachen der Protokolldatei zu aktivieren.

Protokollüberwachung in einer Windows-Umgebung aktivieren

Um Überwachungsprotokolle in einer Windows-Umgebung zu aktivieren, wählen Sie die relevante Richtlinie aus, und weisen Sie ihr spezifische Prüfungsparameter zu. Wenn die Protokollüberwachung aktiviert ist und eine angegebene Zeichenfolge im überwachten Protokoll erkannt wird, wird ein Event erstellt.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**.

2. Wählen Sie die Richtlinie zur **Windows-Protokollüberwachung** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **os.windows.check-log** auf der Registerkarte **Check Instances** (Prüfungsinstanzen) aus, um die Überwachung von Windows-Protokolldateien zu aktivieren.
4. Geben Sie auf der Registerkarte **Check Parameters** (Prüfungsparameter) die in der folgenden Tabelle beschriebenen Protokollparameter an, die durch die Prüfung überwacht werden sollen:

Parameter überprüfen

Name	Wert
warning	Häufigkeit des Auftretens der angegebenen Musterzeichenfolgen im Protokoll, durch die ein *warning*-Event generiert wird. Standard = 1. Beispiel: Wenn der Wert für *pattern* gleich **Exception** (Ausnahme) ist und das Protokoll ein Ausnahme-Event enthält, wird ein *warning*-Event generiert.
critical	Häufigkeit des Auftretens der angegebenen Musterzeichenfolgen im Protokoll, durch die ein *critical*-Event generiert wird. Standard = 2. Beispiel: Wenn der Wert für *pattern* gleich **Exception** (Ausnahme) ist und das Protokoll zwei Ausnahme-Events enthält, wird ein *critical* -Event generiert.
file	Speicherort der Protokolldatei
pattern	Zeichenfolgen, nach denen im Protokoll gesucht wird. Standardwerte: **Severe** (Schwerwiegend) und **Exception** (Ausnahme). Andere mögliche Werte: **404** und **Error** (Fehler) Stellen Sie sicher, dass Sie mehrere Muster durch eine Pipe (|) trennen und als Parameter in Anführungszeichen weitergeben. Zum Beispiel: `"SEVERE|404"`.

Legen Sie die Protokollebene für den Agent fest

Konfigurieren Sie die Agent-Protokollebene direkt in Ihrer Instanz ServiceNow®, ohne auf die Konfigurationsdatei `acc.yml` zugreifen zu müssen.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie die Protokollebene des Agent über die Instanz konfigurieren, wird die Protokollebene vorübergehend geändert. Die Protokollebene in der Konfigurationsdatei `acc.yml` wird nicht aktualisiert. Beim Neustart des Agent wird die Protokollebene auf den in der Konfigurationsdatei `acc.yml` festgelegten Status zurückgesetzt.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
2. Wählen Sie einen HR-Mitarbeiter aus.
3. Wählen Sie in den zugehörigen Links **Protokollebene festlegen**aus.
4. Wählen Sie im Dialogfeld „Protokollebene festlegen“ die Protokollebene aus, die für den Agent aufgerufen werden soll, und wählen Sie **OK**.
5. Setzen Sie die Protokollebene auf die ursprünglich konfigurierte Ebene zurück, indem Sie eine der folgenden Aktionen ausführen:
   - Wählen Sie in den zugehörigen Links **Protokollebene zurücksetzen aus**.
   - Starten Sie den Agent neu.

Löschen Sie Agent Client Collector Assets

Leeren Sie den Cache-Ordner für Asset- und Konfigurationsdateien und steuern Sie die Plugin-Downloads. Durch das Leeren des Cache-Ordners werden unerwünschte Plugins entfernt, die mit dem Agent synchronisiert wurden.

Vorbereitungen

Stellen Sie sicher, dass Folgendes auf Ihrem System installiert ist:

- Agent Client Collector Framework (ACC-F) ab Version 3.5.5
- MID-Server
- CMDB
- Agent Client Collector Agent, ab Version 3.5.5
- ACC Global Utilities

Stellen Sie sicher, dass die Systemeigenschaft **disable_assets** in der Konfigurationsdatei `acc.yml` auf **false**festgelegt ist.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents**.
2. Wählen Sie einen HR-Mitarbeiter aus.
3. Wählen Sie im Abschnitt **„Zugehörige Links“Assets löschen aus**.
4. Wählen Sie im Bestätigungsdialogfeld **Agent-Assets löschen aus**.
5. Wahlweise: Wählen Sie **Hostdaten sammeln** aus, um Ihre Plugins erneut aus der Instanz herunterzuladen.
   Plugins werden automatisch heruntergeladen, wenn sie von ihren jeweiligen Prüfungen/ Richtlinien verwendet werden.

Integritäts-Dashboard von Agent Client Collector

Im Agent Health-Dashboard können Sie den Status der Agents in Ihrem System überwachen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agent Health-Dashboard**.
   Die Seite **Agent Health Dashboard** (Agent-Integritäts-Dasbhoard) wird angezeigt. Sie enthält Informationen zu den konfigurierten Agents in den Dashboard-Widgets.

   Im Widget **Agents by Data Collection Status** (Agents nach Datenerfassungsstatus) gibt **Aus (manuell)** an, dass Agents manuell deaktiviert wurden (für Wartungsarbeiten oder zur Problembehandlung), und **Aus (automatisch)** bedeutet, dass Agents automatisch deaktiviert wurden (nachdem sie den Schwellenwert für die CPU-Auslastung überschritten hatten).

2. Klicken Sie auf das Pfeilsymbol zum Aktualisieren in der rechten oberen Ecke eines Widgets, um dessen Daten nach Bedarf zu aktualisieren.
   Sie können alle Widgets im Dashboard aktualisieren, indem Sie auf dieses Symbol im Formularheader klicken und dann **Aktualisieren** auswählen.

Agent-Funktionsmatrix anzeigen

Die Agent-Funktionsmatrix von Agent Client Collector zeigt die Verfügbarkeit von Agent Client Collector-Funktionen an. Die Matrix zeigt Daten in einem Diagramm und einer Tabelle an.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

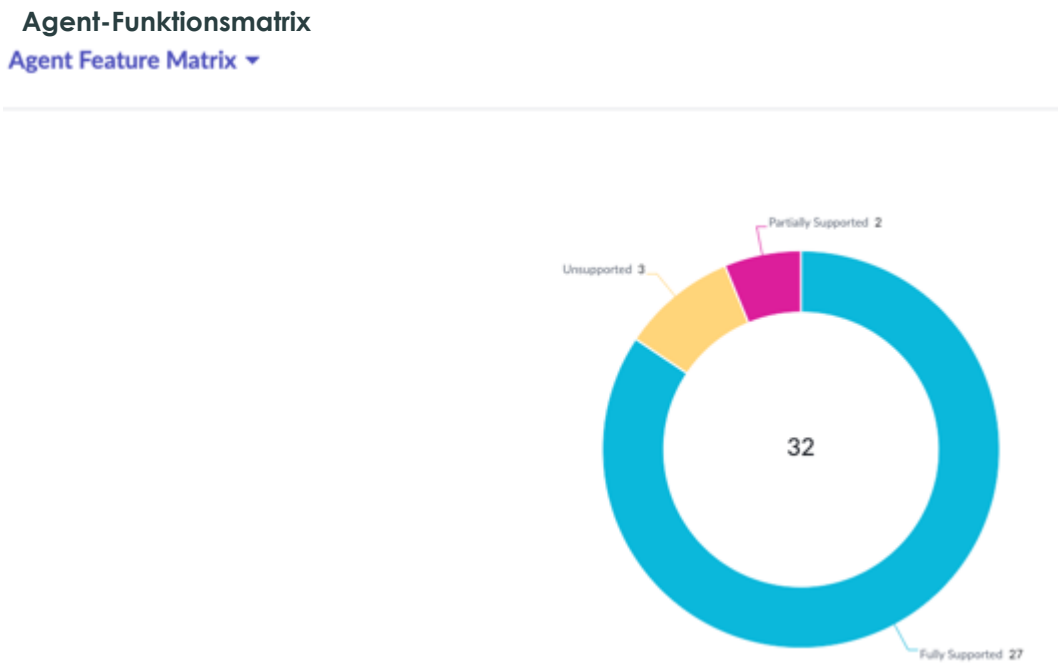
Warum und wann dieser Vorgang ausgeführt wird

Die Agent-Funktionsmatrix zeigt die Granularität der Agent Client Collector-Funktionen an, die vollständig, teilweise und nicht unterstützt werden. Für ein teilweise unterstützte Funktion können Instanz- und Framework-Anforderungen erfüllt sein, sie wird jedoch unter mindestens einer Agent-Version ausgeführt, die die Funktionsanforderungen nicht erfüllt.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agent-Funktionsmatrix**.
   Die **Agent-Funktionsmatrix** wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die Matrix zeigt den Unterstützungsstatus der Agent Client Collector -Funktionen „vollständig unterstützt“, „teilweise unterstützt“ und „nicht unterstützt“ (Nicht unterstützt).

2. Wählen Sie im Diagramm eine der Kategorien aus.
   Eine Liste aller Funktionen in der Kategorie wird auf der Seite **Agent Feature Support Status** (Status der Unterstützung von Agent-Funktionen) angezeigt.

Seite „Agent Feature Support Status“ (Status der Unterstützung von Agent-Funktionen)

sn_agent_feature_support_status 27

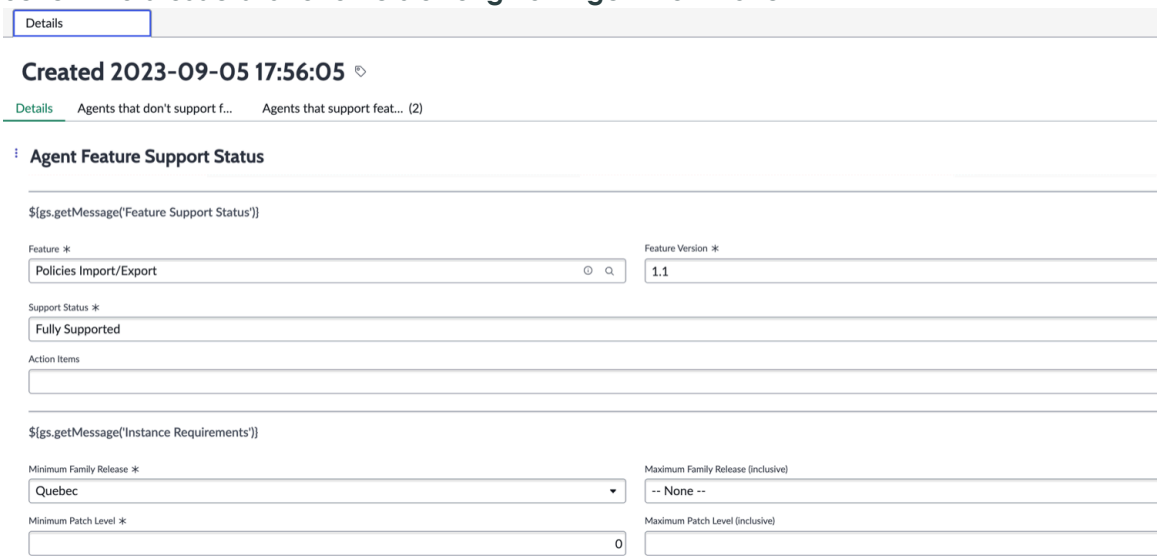
Last refreshed just now.

Feature	Feature Version	Support Status
OSQuery	5.7.0	Fully Supported
API Key	1.0	Fully Supported
Auto syncing certifications to agent	1.0	Fully Supported
Trigger MID selection when IP changes	1.0	Fully Supported
Policies Import/Export	1.1	Fully Supported
Allow List support per plugin	1.0	Fully Supported
Allow List	1.0	Fully Supported

3. Wählen Sie eine der Funktionen aus.
   Die Seite **Agent Feature Support Status** (Status der Unterstützung von Agent-Funktionen) wird für die spezifische Funktion angezeigt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Seite mit Statusdetails zur Unterstützung von Agent-Funktionen



Auf der Seite wird Folgendes angezeigt:

- Abschnitte, die den Unterstützungsstatus der Funktion und die verschiedenen Instanzanforderungen der Funktion angeben. Das Feld **Action Items** (Aktionselemente) zeigt die Aktionen an, die Sie ausführen müssen, um eine Funktion, die entweder teilweise oder nicht unterstützt wird, vollständig zu unterstützen.
- Anforderungen an die Instanz und die Version des Agent-Frameworks, die von der Agent-Funktion erfüllt wurden.

Agent Client Collector Framework-Referenz

Referenzthemen enthalten zusätzliche Informationen zum Zuordnen und Optimieren von Anwendungsservices mithilfe von Agent Client Collector Framework-Listen und -Formularen.

Agent Client Collector -Benutzerrollen

Administratoren können Benutzerrollen zuweisen, um Zugriff auf Agent Client Collector zu gewähren. Die folgenden Standardrollen für das Agent Client Collector-Framework (ACC-F) sind in dem ServiceNow-System enthalten, auf dem Agent Client Collector installiert ist.

Agent Client Collector – Benutzerrollen

Rolle	Beschreibung
agent_client_collector_admin	Alle Berechtigungen für Agent Client Collector, einschließlich: • Zugriff auf REST-API • Richtlinien, Prüfungen, Agents und Websockets hinzufügen, bearbeiten und löschen • MID-Server-Verwaltung
agent_client_collector_integration	Zugriff auf REST-API

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector – Benutzerrollen (Fortsetzung)

Rolle	Beschreibung
agent_client_collector_user	• Prüfungen und Richtlinien anzeigen • Zugriff auf einige REST APIs
evt_mgmt_admin	Startet den ACC-Listener

Standardprüfungen des Agent Client Collector-Framework

Das Agent Client Collector-Framework stellt mit dem Basissystem Standardprüfungen bereit.

Prüfungen

In der folgenden Tabelle sind die Standardprüfungen aufgeführt, die im Lieferumfang des Basissystem des Agent Client Collector-Framework vorhanden sind.

Typ	Name	Beschreibung	Befehl
Neu starten	restart	Startet den Agent neu. Die Prüfung ist standardmäßig aktiviert.	Agent neu starten
Discovery	check-discovery-basic	Führt eine Basiserkennung des Hosts des Agent durch, um Folgendes zu erkennen: • Host-CI, einschließlich IP-Adresse, Seriennummer und Hostname. • Laufende Prozesse (cmdb_running_process) des Hosts • TCP-Ports (cmdb_tcp) Die Überprüfung wird standardmäßig alle 12 Stunden (43.200 Sekunden) durchgeführt und läuft nach 600 Sekunden Inaktivität ab.	endpoint_discovery.rb

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Name	Beschreibung	Befehl
		Plugins: osquery, acc-f-commons, acc-f-modules	

Hinweis: Die Prüfungen *check-read-log* und *config-file-reader* sind nur für den internen Gebrauch bestimmt.

Agent Client Collector Leistung und Platzbedarf für URL-Überwachung

Die folgenden Tabellen zeigen die Leistungs-KPIs des Agent und seinen Platzbedarf auf dem Host während der Ausführung der URL-Überwachungsdatensammlung in verschiedenen Betriebssystemen.

URL-Überwachungsprüfungen in einem Linux -System

Linux Cent OS 8, 2 CPUs, 4 GB RAM					
Überprüfungen pro Minute	100	250	500	1000	1500
Metriken (erwartet/ tatsächlich)	700/700	1750/1750	3500/3500	7000/7000	10500/10500
Netzwerkauslastung – Tx (MID > Agent)	35 KB/s	78 KB/s	146 KB/s	286 KB/s	430 KB/s
Netzwerkauslastung – Rx (MID < Agent)	15 KB/s	27 KB/s	51 KB/s	107 KB/s	116 KB/s
Netzwerkauslastung – Tx (Agent > MID)	8 KB/s	23 KB/s	37 KB/s	89 KB/s	113 KB/s
Netzwerkauslastung – Rx (Agent < MID)	28 KB/s	72 KB/s	142 KB/s	285 KB/s	426 KB/s
Speicherverbrauch	22 MB	25 MB	26 MB	34 MB	39 MB
CPU aller Prüfungen	ca. 3 %	ca. 7 %	ca. 11 %	ca. 21 %	ca. 24 %
CPU-Auslastung des Prozesses	1% - 1.5%	1.5% - 2.5%	5% - 6%	6% - 7%	12% - 13%
CPU-Auslastung des Hosts	ca. 10 %	ca. 19 %	ca. 23 %	ca. 45 %	ca. 53 %

Agent Client Collector Prüfungsdefinitionsseite

Die Felder, die beim Erstellen einer Prüfungsdefinition auf der Seite Prüfungsdefinition konfiguriert werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Check Definition“ (Prüfungsdefinition)

Feld	Beschreibung
Name	Beschreibender Name der Prüfung
Check Type (Prüfungstyp)	Wählen Sie den Typ der Prüfung aus. Die verfügbaren Überwachungsoptionen lauten wie folgt: • Events • Metriken
Aktiv	Aktivieren Sie diese Option, um die Prüfung zu aktivieren.
Is Proxy Valid (Ist Proxy-fähig)	Aktivieren Sie dies, um anzugeben, dass die Richtlinie der Prüfung so eingerichtet ist, dass diese als Proxy fungiert. Wenn diese Option in der Prüfinstanz angezeigt wird, ist sie schreibgeschützt.
Command Auto Generation (Befehl automatisch erstellen)	Wählen Sie diese Option aus, um den Befehl automatisch mit dem Wert **Command Prefix** (Befehlspräfix) und den Werten der Registerkarte **Parameter** zu generieren.
Command Prefix (Befehlspräfix)	Der Befehl, der für die automatische Generierung verwendet wird, wenn **Command Auto Generation (Befehl automatisch erstellen)** aktiviert ist. Das Präfix besteht aus einem beliebigen Teil des Befehls, der statisch ist (sich nicht ändert), z. B. der Skriptname.
Befehl	• Geben Sie den Befehl ein, den Agent Client Collector ausführt. **Hinweis:** Wenn das Kontrollkästchen **Command Auto Generation** (Befehl automatisch erstellen) aktiviert ist, wird dieses Feld mit dem Präfix und den Flags der aktiven Parameter ausgefüllt, die auf der Registerkarte **Parameter** angegeben sind. • Das Feld enthält Parameter aus einem oder mehreren der folgenden Elemente: ◦ Simple template (Einfache Vorlage): `{{.labels.params_field_name}}`: Übernimmt Werte aus Einträgen auf der Registerkarte **Parameter**. Beispielsweise bedeutet die Zeichenfolge `{{.labels.params_warning}}`, dass der Wert des Parameters *`warning`* verwendet wird (sofern er auf der Registerkarte **Parameter** konfiguriert wurde). ◦ Monitored CI (Überwachtes CI): `{{.labels.params_ci_field_name}}`: Übernimmt

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Check Definition“ (Prüfungsdefinition) (Fortsetzung)

Feld	Beschreibung
	Werte automatisch aus dem überwachten CI, wobei `field_name` durch den exakten Namen des obligatorischen Felds in der CI-Tabelle ersetzt wird.
Konfigurationsdatendateien	Wählen Sie die Konfigurationsdatendateien aus, die heruntergeladen werden sollen, wenn die Prüfung ausgeführt wird.
Beschreibung	Beschreibung der Prüfung
Ausführungsmodus	Der Ausführungsmodus des Schecks. Verfügbare Optionen sind: • *shell*: Zur Verwendung für Prüfungen, die *execv* nicht unterstützen. • *execv*: Bietet mehr Sicherheit während der Ausführung von Prüfungen. Die standardmäßigen Ausführungsmodi sind: • Vorhandene Prüfungsdefinitionen: *shell* • Neue Prüfungsdefinitionen: *execv* • Wenn in das Feld kein Wert eingegeben wird: *shell* Wenn dieses Feld beim Upgrade auf Version 2.9.0 schreibgeschützt ist, müssen Sie den schreibgeschützten Status deaktivieren, wie im Artikel (KB1122498) in Now Support Knowledge Basebeschrieben.
Intervall	Zeit in Sekunden, die zwischen Prüfungsausführungen gewartet wird. Ein Wert von 60 bedeutet beispielsweise, dass die Prüfung alle 60 Sekunden ausgeführt wird. Der angegebene Wert muss eine ganze Zahl sein.
Zeitüberschreitung	Die Zeit in Sekunden, nach der die Prüfungsausführung angehalten wird, wenn keine Ausgabe zurückgegeben wird. Ein Wert von 60 bedeutet beispielsweise, dass die Ausführung angehalten wird, wenn die Prüfungsausführung 60 Sekunden lang keinen Wert zurückgibt.
Schwellenwert für Event-Statusänderung	Anzahl der aufeinanderfolgenden Male, die der Antwortstatus einer Prüfung auftreten muss, bevor ein neues Event gesendet wird. Wenn dieser Wert beispielsweise auf 5 festgelegt ist, generiert ein Scheck, dessen Antwortstatus von **OK** in **Fehler** wechselt, erst nach dem fünften Auftreten der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Check Definition“ (Prüfungsdefinition) (Fortsetzung)

Feld	Beschreibung
	Statusänderung in Folge ein neues Ereignis mit dem Status **Fehler**. Standardwert: 5 (außer AWS Ereignisrichtlinien)
Schwellenwert für Reparatur des Ereignisstatus	Anzahl der aufeinanderfolgenden Male, die sich der Antwortstatus einer Prüfung verbessern muss, bevor ein neues Event gesendet wird. Wenn dieser Wert beispielsweise auf 3 festgelegt ist, generiert eine Prüfung, deren Antwortstatus sich von **Fehler** in **OK** ändert, ein neues Event mit dem Status **OK** erst nach dem dritten Auftreten des Statuswechsels in Folge. Standardwert: 1 (außer AWS Ereignisrichtlinien)
Regulärer Ausdruck für Anmeldeinformationsfehler	Zeichenfolge in der Ausgabe der Prüfung, die angibt, dass die Prüfung aufgrund eines Fehlers in den Anmeldeinformationen fehlgeschlagen ist. Der Agent sucht dann weiter nach Anmeldeinformationen, die Teil des Anmeldeinformationsalias sind, bis die richtigen gefunden werden. Dieses Feld ist relevant (und obligatorisch), wenn die Richtlinie der Prüfung einen Anmeldeinformationsalias verwendet. Geben Sie die Zeichenfolge beim Erstellen einer neuen Prüfung manuell ein.
Plugins	Wählen Sie die Plugins aus, die mit der Prüfung verknüpft sein sollen. Anschließend werden die Plugins heruntergeladen, bevor die Prüfung ausgeführt wird.

Registerkarte „Prüfungsdefinition“-Formularparameter

Definitionen der Registerkarte „Parameter“ für das Feld **Befehl** im Prüfungsdefinitionsformular.

Registerkarte „Parameter“

Feld	Beschreibung
Name	Beschreibender Name für den Parameter
Default value / value (Standardwert/Wert)	Standardwert/Wert des Parameters
Aktiv	Boolescher Wert. Wenn der Parameter auf **true** gesetzt ist, wird er im Feld **Command** (Befehl) übernommen, sofern das Kontrollkästchen **Command Auto Generation (Befehl automatisch erstellen)** aktiviert ist.
Obligatorisch	Boolescher Wert. Bei Festlegung auf **true** muss ein Parameterwert angegeben werden, damit der Befehl ausgeführt werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Parameter“ (Fortsetzung)

Feld	Beschreibung
Flagge	Zeichenfolge. Dieses Präfix wird im Feld **Command** (Befehl) vor dem Parameterwert eingefügt, wenn das Kontrollkästchen **Command Auto Generation (Befehl automatisch erstellen)** aktiviert ist.
Wert erforderlich	Boolescher Wert. Wenn der Parameter auf **true** gesetzt und das Kontrollkästchen **Command Auto Generation (Befehl automatisch erstellen)** aktiviert ist, wird der Wert dieses Parameters dem Feld **Command** (Befehl) hinter dem Wert im Feld **Flag** (Kennzeichnung) hinzugefügt.

Testen Sie die Dialogfeldfelder zum Überprüfen

Das Dialogfeld Felder beim Testen einer Prüfungsdefinition.

Felder im Dialogfeld „Testüberprüfung“

Feld	Beschreibung
Prüfungsdefinition	Zeigt den Namen der ausgewählten Prüfungsdefinition an
CI	Wählen Sie das CI aus, für das die Prüfung ausgeführt werden soll. Zur Auswahl verfügbar sind diejenigen CIs, die die beiden folgenden Kriterien erfüllen: • Gehören zu der im Feld **Check group** (Überprüfungsgruppe) angegebenen Gruppe • Gehört zu einem Service Desk-Mitarbeiter mit dem Status **„In Betrieb“**. Wenn das Feld **Check group** (Überprüfungsgruppe) leer ist, wird der Standardwert **cmdb_ci_computer** eingetragen.
Berechtigungen	Wählen Sie die Anmeldeinformationen des Benutzers aus, mit dem der Agent eine Verbindung herstellen soll. Dieses Feld wird nur angezeigt, wenn Sie auf der Registerkarte **Check Secure Parameter Definitions** (Sichere Parameterdefinitionen überprüfen) in der Prüfungsdefinition sichere Prüfungsparameter konfiguriert haben.
Proxy Agent	Wählen Sie den Proxy-Agent aus, der der Prüfung zugeordnet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder im Dialogfeld „Testüberprüfung“ (Fortsetzung)

Feld	Beschreibung
	Dieses Feld wird nur angezeigt, wenn Sie mit einer Prüfungsinstanz arbeiten und eine der Optionen auf der Registerkarte **Proxy Settings** (Proxy-Einstellungen) in der Richtlinie der Instanz ausgewählt wurde.

Agent Client Collector Datensammlungseigenschaften

Beschreibung der Eigenschaften, die das Verhalten der Agent Client Collector -Datenerfassung bestimmen.

Datensammlungseigenschaften

Eigenschaft	Beschreibung
sn_agent.host-data_collection_refresh_duration_seconds	Die Zeit (in Sekunden) zwischen den Agent-Datenerfassungen auf dem Host. Gilt nur, wenn dem Agent kein Host-CI zugewiesen ist. Standard: 43200 (12 Stunden)
sn_agent.disco_minimum_threshold_for_endpoint_discovery_minutes	Die Mindestanzahl von Minuten, seit die letzte Endpunkt-Discovery auf einer bestimmten IP vor Discovery erneut ausgelöst werden kann. Diese Eigenschaft verhindert, dass die Endpunkt-Discovery zu oft ausgeführt wird, z. B. in Fällen, in denen ein Netzwerk zeitweise unterbrochen wird oder ein Laptop wiederholt neu gestartet wird. Standardwert: 60
sn_agent.disco_disable_ci_clobber_of_agentless_discovery	Die Einstellung gibt an, dass von den Quellen ServiceWatch oder ServiceNow Discovery erfasste Daten Vorrang vor Agent Client Collector haben, wenn der Schwellenwert in der Eigenschaft *sn_agent.disco_ci_clobber_of_agentless_disco_thre* nicht überschritten wurde. Standardwert: wahr
sn_agent.disco_ci_clobber_of_agentless_maximum_threshold_in_days	Maximale Anzahl von Tagen seit der Erkennung eines vorhandenen CI mit Discovery ohne Agent, bei der das vorhandene CI verknüpft wird, anstatt vom Agent erneut erkannt zu werden. Wird wirksam, wenn *endpoint_disco_disable_ci_clobber_of_agentless_di* = **wahr** und mehr als 14 Tage (standardmäßig) vergangen sind, seit

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datensammlungseigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
	eine Nicht-ACC-Discovery-Quelle (z. B. ServiceWatch oder ServiceNow) das CI erkannt hat. Nachdem dieser Schwellenwert überschritten wurde, kann der Agent Discovery ein vorhandenes CI unabhängig davon ausführen und überschreiben, ob das CI zuvor von einer Nicht-ACC-Discovery-Quelle erkannt wurde. Dieser Prozess stellt die zuletzt erkannten Daten in der CMDB bereit. Standard: 14
sn_agent.ci_prefers_ip_version	Gibt an, ob IPv4 oder IPv6 die bevorzugte Version ist, wenn ein IP-Adresswert im Feld „IP-Adresse“ des CI-Datensatzes gespeichert wird. Standard: 4
sn_agent.ci_serial_number.pref_order	Geben Sie die Reihenfolge der Felder an, um einen Seriennummernwert zu finden, der während der Agent-Datenerfassung im Feld *serial_number* des Host-CI gespeichert werden soll. Werte müssen durch Kommas getrennt, ohne Leerzeichen und in Kleinbuchstaben angegeben werden. Standard: bios,system,uuid,baseboard,chassis
sn_agent.mac_ci_name_pref_order	Geben Sie die Reihenfolge der Werte an, mit denen das Feld *Name* des CI-Datensatzes während der macOS-Datenerfassung gefüllt wird. Werte müssen durch Kommas getrennt, ohne Leerzeichen und in Kleinbuchstaben angegeben werden. Standard: name,hostname,computer_name,local_hostname
sn_agent.host_data_collection.disable_linux_containers	Die Einstellung gibt an, dass die Datenerfassung für containerisierte Agents deaktiviert ist. Standardwert: wahr

Agent Client Collector Eigenschaften der Richtliniensammlung

Beschreibung der Eigenschaften, die das Verhalten der Richtliniensammlung Agent Client Collector bestimmen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften der Richtliniensammlung

Eigenschaft	Beschreibung
sn_agent.full_policy_calculation_cycle_days	Die Anzahl der Tage, nach der eine Richtlinie einen vollständigen Berechnungszyklus erreichen muss. Wenn der letzte vollständige Berechnungszyklus der Richtlinie mehr als 7 Tage zurückliegt, wird die Richtlinie abgefragt, um ihren Berechnungszyklus vollständig zu berechnen. Standard: 7
sn_agent.max_number_of_monitored_cis_per_policy	Die maximale Anzahl der überwachten CIs, die pro Richtlinie verarbeitet werden können. Standard: 400000
sn_agent.max_num_of_monitored_ci_to_process_without_agent	Die maximale Anzahl von überwachten CIs, die nicht mit Agents verknüpft sind und pro Richtlinie verarbeitet werden können. Standardwert: 1000
sn_agent.policy_force_recalc_interval_limit	Die Intervallgrenze in Minuten, anhand der bestimmt wird, ob eine erzwungene Neuberechnung für Richtlinien erforderlich ist. Bei der erzwungenen Neuberechnung werden die überwachten CIs einer Richtlinie und der entsprechende Agent neu verteilt. Standard: 10
sn_agent.policy_force_recalc_required	Bei Festlegung auf *true* wird überprüft, ob eine erzwungene Neuberechnung für Richtlinien erforderlich ist. Durch die erzwungene Neuberechnung werden die überwachten CIs einer Richtlinie und der entsprechende Agent neu verteilt. Standardwert: wahr
sn_agent.populate_proxy_agent_monitored_ci_attribute	Wenn auf *true* festgelegt, werden die überwachten CIs für bestimmte Richtlinien neu gefüllt, um die Verteilung der CIs auf Proxy-Agents anzuzeigen. Standardwert: false

Agent Client Collector Framework Konfigurationseigenschaften

Beschreibung der Eigenschaften, die das Verhalten der Konfiguration Agent Client Collector Framework bestimmen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationseigenschaften des Frameworks

Eigenschaft	Beschreibung
sn_agent.agent_static_import_char_read_limit	Der Lesegrenzwert für Zeichen für ein bestimmtes Nutzlastelement. Bezieht sich nur auf das verarbeitete Konfigurationselement und nicht auf die Gesamtgröße des Anhangs. Standard: 1000000
sn_agent.agent_upgrade_wait_time	Maximale Anzahl von Minuten, die ein Agent erfolgreich aktualisiert werden muss, bevor er in den Status *Warning* wechselt. Standard: 30
sn_agent.agent_version	Die aktuell in der Instanz installierte ACC-F-Release-Version.
sn_agent.appl_classification_behavior	Merkmale und Verhalten von Anwendungen während der Agent-Discovery. Wenn dies auf *simple* festgelegt ist, wird ein Shell-CI erstellt. Standard: einfach
sn_agent.config_publish.max_payload_size	Die Größe in Byte, die „config_publish_payload“ im ECC-Warteschlangenthema „MonitoringProbe“ erreichen kann, bevor ein Fehler protokolliert und die Nutzlast übersprungen wird. Standard: 15000000
sn_agent.ecc_queue.max_payload_size	Die maximal zulässige Nutzlastgröße für einen vom Agent zu verarbeitenden ECC-Warteschlangendatensatz. Standard: 5000000
sn_agent.enable_auto_mid_selection	Bei Festlegung auf **true** sendet die Instanz eine Liste von MID Servers an die Service Desk-Mitarbeiter. Um die automatische Auswahl von MID-Server aus der Liste zu aktivieren, legen Sie die Eigenschaft *auto-mid-selection* in der Datei acc.yml des Agents auf true fest. Die automatische Auswahl von MID Servers stellt sicher, dass jeder Service Desk-Mitarbeiter den effizientesten verfügbaren MID-Serververwendet. Standardwert: false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationseigenschaften des Frameworks (Fortsetzung)

Eigenschaft	Beschreibung
	Hinweis: Diese Eigenschaft bestimmt nur, ob eine Liste von MID-Servern an den Agent gesendet wird. • Wenn diese Eigenschaft zuvor auf **„wahr“** festgelegt wurde und dann auf **„falsch“**festgelegt wird, wird die automatische MID-Auswahl für die zuvor gesendete Liste MID-Server durchgeführt, wenn die Eigenschaft *auto-mid-selection* in der Datei acc.yml auf **„wahr“** festgelegt ist. • Wenn diese Eigenschaft auf **„wahr“** und die Eigenschaft *auto-mid-selection* in der Datei acc.yml auf **„falsch“**festgelegt ist, wird keine automatische MID-Server -Auswahl durchgeführt.
sn_agent.installer_max_endpoints	Maximale Anzahl von MID-Webserver Endpunkt-URLs, die während der einzeiligen Installation des Agent ausgewählt werden sollen. Standard: 3
sn_agent.keep_alive.alive_duration	Der Zeitraum in Sekunden, innerhalb dessen der Zeitstempel „last_refreshed“ des Agent aktualisiert werden muss. Nach diesem Zeitraum ändert sich der Status des Service Desk-Mitarbeiters von *Up* in *Warning*. Wenn der angegebene Zeitraum erneut vergeht, ändert sich der Status von *Warning* in *Down*. Standard: 120
sn_agent.keep_alive.disconnected_duration	Die Zeit in Sekunden, innerhalb derer der Zeitstempel „last_keepalive“ aktualisiert werden muss. Nach diesem Zeitraum ändert sich der Status des Service Desk-Mitarbeiters von *Up* in *Disconnected*. Standard: 600
sn_agent.logging.verbosity	Die Mindestebene von Nachrichten, die für Agent Client Collector Frameworkprotokolliert werden. Nachrichten mit dem angegebenen Status und schwerwiegendere Status werden protokolliert. Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationseigenschaften des Frameworks (Fortsetzung)

Eigenschaft	Beschreibung
	• Fehler • warnen • Info • debuggen Standard: info
sn_agent.max_sys_ids_in_query	Die maximale Anzahl von Sys-IDs, die bei GlideRecord-Abfragen zurückgegeben werden sollen. Standard: 400000
sn_agent.maximum_mids_to_select	Die maximale Anzahl von MID Servers, die für das Agent-Setup ausgewählt werden kann. Standard: 20
sn_agent.min_upgrade_history_per_agent	Die Mindestanzahl der pro Agent gespeicherten Upgrades. Standardwert: 2
sn_agent.registration_key_validity.days	Die Anzahl der Tage nach der Erstellung eines Registrierungsschlüssels, in denen der Schlüssel gültig ist, bevor er gelöscht wird. Standard: 90
sn_agent.registration_key_notification.days	Die Anzahl der Tage vor dem Löschen des Registrierungsschlüssels, in der eine E-Mail-Benachrichtigung an die Besitzgruppe des Schlüssels gesendet wird, um sie über die ausstehende Löschung zu informieren. Standard: 14
sn_agent.sync_filters_interval_min	Die Anzahl der Minuten, nach der CMDB-Änderungen erkannt und dann mit MID-Serversynchronisiert werden. Standard: 10
sn_agent.time_ago_in_seconds_to_query_ecc_queues	Bei der Verarbeitung von ecc_queues nur diejenigen abfragen, die innerhalb der angegebenen Zeit (in Sekunden) erstellt wurden. Standard: 43200 (12 Stunden)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Datensammlungstabellen

Agent Client Collector führt eine Datensammlung basierend auf den von Ihnen installierten bereichsbezogenen Apps durch. Agent Client Collector Framework führt eine grundlegende Datensammlung durch, und Agent Client Collector Visibility – Inhalt führt eine erweiterte Datensammlung durch.

Die regelmäßige Aufgabe „Hostdaten für Service Desk-Mitarbeiter neu laden“ sammelt stündlich Hostdaten von Hosts, auf denen in den letzten 12 Stunden keine Daten erfasst wurden. Die Aufgabe sammelt die in den folgenden Tabellen beschriebenen Daten.

Agent Client Collector Framework-Datensammlung

Daten	CMDB-Feld
hostname	CI.Name
physischen Arbeitsspeicher	CI.RAM
Hardware-Lieferant	CI.Hersteller
Hardwaremodell	ci.model_id
CPU-Name	ci.cpu_type
BS-Domäne	ci.os_domain
BS-Name	CI.OS
BS-Version	ci.ip_address
IPv4-Adresse	ci.ip_address
Standard-Gateway	ci.default_gateway
Seriennummer	ci.serial_number
DNS-Name	CI.Name
FQDN	ci.fqdn
TCP-Verbindungen	cmdb_tcp
Laufende Prozesse	cmdb_running_process
Seriennummern **Hinweis:** Beim Sammeln von Daten von Linux-Hosts muss `dmidecode` mit `sudo`- Berechtigungen konfiguriert werden, um alle Seriennummern zu erfassen.	cmdb_serial_number

Agent Client Collector Visibility – Inhalt-Datensammlung

Daten	CMDB-Feld
CPU-Hersteller	ci.cpu_manufacturer
CPU-Geschwindigkeit	ci.cpu_speed
BS-Arch	ci.os_address_width
CPU-Anzahl	ci.cpu_count

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector Visibility – Inhalt-Datensammlung (Fortsetzung)

Daten	CMDB-Feld
Anzahl der CPU-Cores	ci.cpu_core_count
CPU-Kern-Thread	ci.cpu_core_thread
Ist virtuell	CI.virtual
Startdatum (Betriebszeit)	ci.start_date
Objekt-ID	ci.object_id
TCP-Verbindungen	cmdb_tcp
Laufende Prozesse	cmdb_running_process

Account-Befehle für LocalService, LocalSystem und gMSA während der Installation Windows von [].

Wenn Sie einen Agent auf einem Host Windows mit einem LocalService-, LocalSystem- oder gMSA-Account installieren, müssen Sie msi-Befehle ausführen, um die Accounts zu aktivieren.

Kontotypbefehle

Kontotyp	Befehl
Lokales System	`msiexec /i C:\acc-installer.msi /qn /norestart ACC_API_KEY=<API key code> ACC_MID=<MID Server URL>/ws/events ACC_ALLOW_LIST=False LOCALUSERNAME="SYSTEM"`
LocalService	`msiexec /i C:\acc-installer.msi /qn /norestart ACC_API_KEY=<API key code> ACC_MID=<MID Server URL>/ws/events ACC_ALLOW_LIST=False LOCALUSERNAME="LOCALSERVICE"`
gMSA	`msiexec /i C:\acc-installer.msi /qn /norestart ACC_API_KEY=<API key code> ACC_MID=<MID Server URL>/ws/events ACC_ALLOW_LIST=False LOCALUSERNAME="DOMAIN\gMSA$"`

Sicherstellen, dass die API mit einem Mitarbeiter verknüpft ist

Rufen Sie die API *`AgentNowHandler.hasAgent`* auf, um zu bestimmen, ob das CI einem Mitarbeiter zugeordnet ist. Die API ruft eine sys_id des CI ab und gibt ein true/false-Ergebnis zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Methode *hasAgent()* wird eine sys_id des CI als Zeichenfolgenparameter verwendet. Sie gibt **true** zurück, wenn das CI eine der folgenden Bedingungen erfüllt:

- Das CI ist `sn_agent_cmdb_ci_agent`, und dieser Agent ist aktiv.
- Das CI ist ein Host (der `cmdb_ci_hardware` erweitert), und es ist einem Mitarbeiter zugeordnet.
- Das CI ist eine Anwendung (die `cmdb_ci_appl` erweitert), und es besitzt eine Beziehung vom Typ „Wird-ausgeführt“ zu einem mit einem Mitarbeiter verknüpften Host.

Beispiel:

```
var agentNow = new sn_agent.AgentNowHandler();
gs.info('Agent assocation with CI? ' +
agentNow.hasAgent('158279505372b30034b8ddeeff7b1270'); // sys_id of agent
```

Konfigurationsdateioptionen

Verfügbare Optionen in der `acc.yml`- Konfigurationsdatei.

Grundlegende Konfigurationsoptionen für die acc.yml-Konfigurationsdatei

Option	Typ	Standard	Beschreibung	Beispiel
name	Zeichenfolge	Agent_ <value of the <a id="x1">[] Befehl>*hostname*	Der Name des in der SN-Instanz registrierten Agents kann vom Anwender angegeben werden. Das Ergebnis des Befehls „hostname“ wird als Standard verwendet.	`Name:<name of agent>`
Back-End-URL	Liste	`wss://127.0.0.1:8800/ws/events`	Liste der MID Webserver-Endpunkt-URLs für die Kommunikation mit. Wenn die Kommunikation mit der ersten URL nicht konfiguriert werden kann, wechselt das System zu den nachfolgenden URLs, bis eine Verbindung hergestellt wird. Funktioniert, wenn `enable-auto-mid-selection=wahr`	`Back-End-URL:<mid server ip> :<websocket port>`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Grundlegende Konfigurationsoptionen für die acc.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
API-Schlüssel	Zeichenfolge	<None>	API-Schlüssel, der von MID-Server zum Authentifizieren eingehender Agent-Verbindungen verwendet wird. Der Wert wird beim ersten Start des Agent verschlüsselt.	`API-Schlüssel:<mid web server api key>`
user	Zeichenfolge	Administrator	Anwendername, der für die Standardauthentifizierung verwendet wird. Wenn dieser Parameter leer ist, wird der Agent nicht gestartet.	`Anwender: „agent-01“`
Passwort	Zeichenfolge	Administrator	Für die Standardauthentifi verwendetes Passwort. Der Wert wird beim ersten Start des Agent verschlüsselt. Wenn dieser Parameter leer ist, wird der Agent nicht gestartet.	`Passwort:<secure-password>`
log-level	Zeichenfolge	Information	Protokollierungsum der in der Datei acc.log angezeigt werden soll. Werte: • Panic (Kritisch) • Schwerwiegend • Fehler • Warnen	`Protokollebene: Debuggen`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Grundlegende Konfigurationsoptionen für die acc.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
			• Information • Debuggen	
allow-list	Zeichenfolge	/etc/servicenow/agent-client-collector/check-allow-list.json	Pfad zur JSON-Datei, die die Liste der Prüfbefehle enthält, die der Agent ausführen kann. Kommentieren Sie diesen Parameter aus, um die Allow-Liste zu deaktivieren. Wenn dieser Parameter leer ist, ist die Allow-Liste deaktiviert.	`Allow-Liste: /etc/agent/check-allow-list.json`
appl_classification_behavior	Liste	Einfach	Gibt an, ob die Shell-CI-Erstellung auf dem Agent aktiviert werden soll. Mögliche Werte: • simple: Gibt an, dass die Shell-CI-Erstellung aktiviert ist. • off: Gibt an, dass keine Shell-CIs für die Anwendung erstellt werden. • full: Gibt an, dass Discovery der Anwendungs-CIs anhand von Mustern ausgeführt werden.	`appl_classification_behavio aus`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfigurationsoptionen für die acc.yml-Konfigurationsdatei

Option	Typ	Standard	Beschreibung	Beispiel
Verify-Plugin-Signatur	Boolean	wahr	Überprüft die Signatur des Plugins vor der Ausführung. Deaktivieren Sie diese Option, wenn selbstsignierte oder in der Entwicklung befindliche Plugins verwendet werden.	`Verify-Plugin-Signature: true`
unsecure-skip-tls-verify	Boolean	falsch	Bestimmt, ob das Zertifikat beim Herstellen einer Verbindung mit MID-Serverüberprüft wird.	`insecure-skip-tls-verify: false`
enable-auto-mid-selection	Boolean	wahr	Steuert die Funktion „Automatische MID-Auswahl“, um eine Verbindung zum optimalen, von der Instanz bereitgestellten MID-Webserver herzustellen.	`enable-auto-mid-selection: true`
„check-command-prefer-installed“	Boolean	falsch	Gibt die Einstellung von ausführbaren Dateien an, die in ACC-Plugins bereitgestellt werden, oder von ausführbaren Dateien, die in der PATH-Variablen des Hostsystems verfügbar sind. • false = ACC-Plugins • wahr = Ausführbare	`check-command-prefer-installed: falsch`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfigurationsoptionen für die acc.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
			Dateien in der PATH-Variablen des Hostsystems	
„powershell_installed“	Boolean	falsch	Deaktiviert die Ausführung von PowerShell-Befehlen auf Agents.	`PowerShell-Installiert: Wahr`
Allow-Liste-Global-nur	Boolean	falsch	Setzen Sie den Wert auf **„true“**, um die Sicherheit zu erhöhen, indem Sie sich nur auf die Allow-Liste verlassen, die im Parameter *`allow-list`* definiert ist, den Sie während der Konfiguration angeben, und die mit ACC-Plugins gebündelten Allow-Listen ignorieren.	`Allow-Liste nur global: falsch`
disable-assets	Boolean	falsch	Gibt an, ob eine Prüfung, die mit einer Asset-Abhängigkeit (Plugin) ausgeführt wird, ACC-Plugins aus der Instanz ServiceNow® abruft oder eine Kopie der Plugins in ihrem Cache-Ordner verwendet. Bei Festlegung auf **false**können zusätzliche Assets während der Ausführung der Prüfung	`disable-assets: falsch`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfigurationsoptionen für die acc.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
			heruntergeladen werden. Setzen Sie den Wert auf **„true“**, um die Sicherheit zu erhöhen und sicherzustellen, dass während der Ausführung der Prüfung keine neuen Plugins heruntergeladen werden.	
agent-upgrade-url-path	Zeichenfolge	`https://install.servicenow.com/glide/distribution/builds/package/app-signed/`	Gibt einen alternativen Webserver-URL-Endpunkt zum Herunterladen von ACC-Installationspaketen bei einem selektiven Upgrade an.	`Agent-Upgrade-URL-Pfad: https://<ip address> :<port> /acc_installers`
enable-patterns-on-agent	Boolean	falsch	Aktiviert das Sammeln von Details zu den Anwendungen, die unter Agent Client Collectorausgeführt werden. Dieser Parameter ist nur erforderlich, wenn Agent Client Collector für die Musterausführung verwendet wird.	`enable-patterns-on-agent: wahr`
-Keepalive-Filter-NICs	Boolean	wahr	Gibt an, ob Netzwerkschnittste Controller (NICs) während der Keepalive-Aktion nach dem Agent (**wahr**) oder MID-Server	`Keepalive-Filter-NICs: wahr`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfigurationsoptionen für die acc.yml-Konfigurationsdatei (Fortsetzung)

Option	Typ	Standard	Beschreibung	Beispiel
			(**falsch**) gefiltert werden.	
Keepalive-number_nics_per_ip_type	Ganzzahl	1	Gibt die maximale Anzahl von Netzwerkschnittstellen-Controllern (NICs) pro IP-Typ (IP4, IP6) an, die mit einer Keepalive-Aktion gesendet werden. Die angegebene Anzahl wird für jeden IP-Typ gesendet. Wenn der Wert beispielsweise 1 ist, werden maximal 2 NICs gesendet (jeweils 0–1 für IP4 und IP6). Wenn der Wert 4 ist, werden maximal 8 NICs gesendet (jeweils 0–4 für IP4 und IP6).	`Keepalive-number_nics_per_ip_type: 4`

Synchronisierungseigenschaften zum Validieren von Agent Client Collector -Plugins

Verwenden Sie die folgenden Eigenschaften, wenn Sie öffentliche Zertifikate von MID-Server mit Agent Client Collectorsynchronisieren.

Zertifikatsynchronisierung – MID-Eigenschaften

Eigenschaft	Beschreibung
mid.acc.cert_monitor_disable	Möglichkeit, die Synchronisierung öffentlicher Zertifikate durch den Monitor zu deaktivieren. Standardwert: False
mid.acc.cert_monitor_interval	Intervall (in Sekunden), in dem der Monitor öffentliche Zertifikate von einer konfigurierten Endpunkt-URL synchronisiert. Standardwert: 86.400

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zertifikatsynchronisierung – MID-Eigenschaften (Fortsetzung)

Eigenschaft	Beschreibung
mid.acc.cert_monitor_target_url	Präfix der Endpunkt-URL (ohne Dateiname), mit dem der Monitor öffentliche Zertifikate synchronisiert. Standardwert: ServiceNow Installationsserver
mid.acc.cert_monitor_target_filename	Name der Endpunkt-URL-Zieldatei, aus der der Monitor öffentliche Zertifikate synchronisiert. Standardwert: SNCertificates.zip

Zertifikatsynchronisierung – Agent-Eigenschaften

Eigenschaft	Beschreibung
fetch-certificates-from-mid	Status, ob die öffentlichen Zertifikate von MID-Server für die Validierung des Plugin-Assets abgerufen werden. Standardwert: True

Agent Client Collector Status

In der folgenden Tabelle werden die Status Agent Client Collector aufgelistet und beschrieben.

Agent Client Collector-Status

Status	Beschreibung
In Betrieb	Der Agent ist verbunden und funktioniert ordnungsgemäß.
Warnung	Agent wurde seit mehr als 2 Minuten nicht aktualisiert (basierend auf dem Wert der Eigenschaft „sn_agent.keep_alive.alive_duration“).
Ausgeschaltet	Agent wurde heruntergefahren.
Wird neu gestartet...	Agent-Neustart wird ausgeführt.
Wird aktualisiert…	Agent-Upgrade wird durchgeführt.
Verbindung getrennt	MID-Server des Agent ist ausgefallen.
Unbekannt	MID-Server des Service Desk-Mitarbeiters hat seit mehr als 10 Minuten keine Keepalive-Kommunikation gesendet (basierend auf dem Wert der Systemeigenschaft „sn_agent.keep_alive.disconnected_duration“).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector-Protokollebenen

Die folgende Tabelle zeigt die verfügbaren Protokollebenen, die den Schweregrad von Agent Client Collector-Events angeben.

Protokollebene	Beschreibung
Panic (Kritisch)	Kritische Fehler, die dazu führen, dass der Service unerwartet beendet wird
Fatal (Schwerwiegend)	Schwerwiegende Fehler, die dazu führen, dass der Service heruntergefahren wird (Status 0)
Fehler	Nicht schwerwiegende Servicefehlermeldungen
Warnung	Warnmeldungen, die auf potenzielle Probleme hinweisen
Info	Informationsmeldungen, die Serviceaktionen darstellen
Debuggen	Detaillierte Meldungen zum Servicebetrieb, die bei der Problembehandlung helfen

Parameter für Agent Client Collector-Protokollrotation

Wenn Agent Client Collector-Protokolle zu groß werden, können sie Systemressourcen beanspruchen. Um die Systemeffizienz sicherzustellen, konfigurieren Sie Parameter in der Datei `acc.yml`, nach der Protokolle aus dem Speicher des Systems rotiert werden sollen (Windows-Standardspeicherort = `C:\ProgramData\ServiceNow\agent-client-collector\config\acc.yml`). Linux-Standardspeicherort = `/etc/servicenow/agent-client-collector/acc.yml`).

Parameter für Protokollrotation

Parameter	Definition
log-file-and-stdout	Protokolle werden in die `stdout`-Datei geschrieben. Standardwert: **false**
Protokollaufbewahrungsdauer	Maximales Alter der Protokolldatei in Tagen, bevor sie aus dem Systemspeicher rotiert wird. Standard: **3**
Protokollaufbewahrungsdateien	Maximale Anzahl von Protokolldateien, die gespeichert werden können, bevor sie aus dem System rotiert werden. Standard: **3**
Protokoll-Maximale-Größe	Maximale Größe (in MB) der Protokolldatei, bevor sie aus dem Systemspeicher rotiert wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter für Protokollrotation (Fortsetzung)

Parameter	Definition
	Standard: **10**.
log-level	Protokollebene, die von den Protokollen gemessen werden soll. Available options are: **Panic**, **Fatal**, **Error**, **Warn**, **Info**, **Debug** (Kritisch, Schwerwiegend, Fehler, Warnung, Info, Debug). Standard: **Info** Die angegebene Protokollebene stellt die niedrigste Ebene der im Protokoll angezeigten Events dar. Beispiel: Einem Benutzer, der **Error** angibt, werden alle Events der Stufe „Error“ (Fehler) sowie schwerwiegende und kritische Events angezeigt.

Agent Client Collector-CPU-Schutzschwellenwerte

Wenn Prüfungen für Agent Client Collector zu viel CPU verbrauchen, unterbricht Agent Client Collector die Datenerfassung und wechselt in den CPU-Schutzmodus. Der Agent wechselt in den CPU-Schutzmodus, wenn er alle konfigurierten Schwellenwerte erreicht, die in der Datei `acc.yml` des Agent angegeben sind. Sie können die Parameterschwellenwerte nach Bedarf ändern. Agents im CPU-Schutzmodus werden in den Agent-Protokollen mit der Syntax `Agent Protection`angezeigt.

Parameter	Beschreibung
agent_cpu_threshold_disabled	Um zu verhindern, dass der Agent heruntergefahren wird, wenn der CPU-Speicher einen bestimmten Schwellenwert erreicht, setzen Sie den Wert auf **true**. Standard = False
cpu_percentage_limit	Prozentsatz der CPU-Nutzung durch den Agent, der den Agent in den CPU-Schutzmodus versetzt Standard = 5%
repeated_high_cpu_num	Anzahl der aufeinanderfolgenden Male, die der CPU-Verbrauch *cpu_percentage_limit* überschreiten muss, damit der Agent in den CPU-Schutzmodus wechselt Standard = 3
monitor_interval_sec	Gibt die Häufigkeit in Sekunden an, mit der die Agent-Überwachung ausgeführt wird, um zu überprüfen, ob *cpu_percentage_limit* überschritten wird

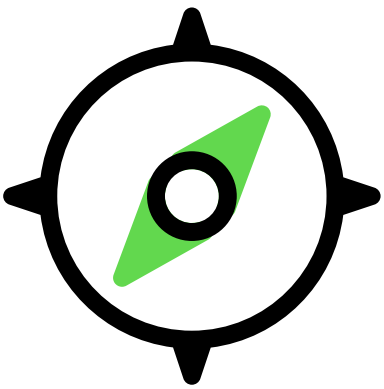
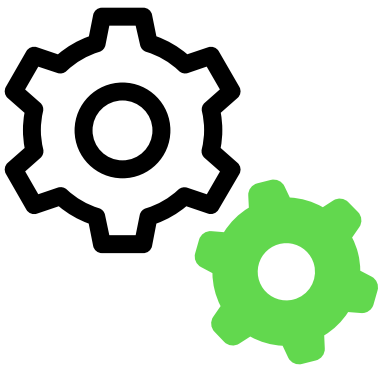
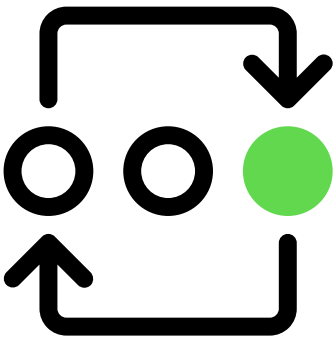
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
	Standard = 60

Agent Client Collector-Überwachung

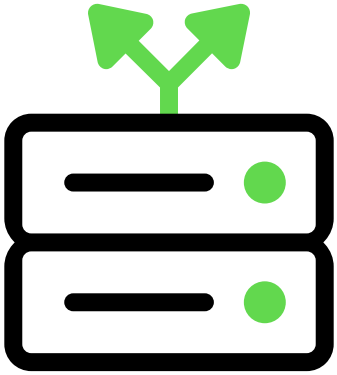
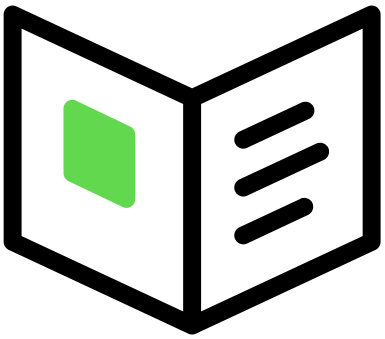
Agent Client Collector-Überwachung Mit können Sie Ihre Serviceverfügbarkeit überwachen, den Zustand und die Leistung Ihrer Umgebung überprüfen und sicherstellen, dass Ihre Infrastruktur und ihre Anwendungen ordnungsgemäß ausgeführt werden.

Erste Schritte

Untersuchen	Konfigurieren	Metrikdaten
		
Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen der Anwendung Agent Client Collector-Überwachung kennen.	Konfigurieren Sie die Funktionen und Komponenten, um Agent Client Collector-Überwachungzu aktivieren.	Verwenden Sie Metrikdaten, um Metrikdaten zu untersuchen und Anomalien zu identifizieren.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arbeiten Sie mit Monitoring Technology Dashboard	Verwenden Sie Proxy-Agents	Referenz
		
Überwachen Sie Serverressourcen nach Plattform.	Überwachen Sie den Zustand und die Leistung Ihrer Configuration Items (CIs), wenn der Agent außerhalb Ihres Hostservers bereitgestellt wird.	Erhalten Sie zusätzliche Details zu Prüfungen und Richtlinien sowie zur Metrikensammlung.

Problembehandlung und Hilfe

- Stellen oder beantworten Sie Fragen im Community-Forum von Agent Client Collector.
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Agent Client Collector-Überwachung erkunden

Agent Client Collector-Überwachung basiert auf einem Sensu-Framework, mit dem Sie Überwachungsprüfungen aus der Community übernehmen und erweitern können. Agent Client Collector-Überwachung sammelt Daten zur -Infrastruktur und zu den installierten Anwendungen Ihres Unternehmens.

Agent Client Collector-Überwachung – Übersicht

Prüfungen und Richtlinien werden auf dem Client des Agent ausgeführt, um die relevanten Daten abzurufen, die gegebenenfalls in Events oder Metriken umgewandelt werden. Events und Metriken werden vom Agent über einen Metrikdaten MID-Server zur ServiceNow-Instanz gesendet und in der entsprechenden Datenbank gespeichert. Ein einzelner MID-Server kann mehrere Agents unterstützen (z. B. ACC-M und ACC-L). Wie Sie den MID-Server für Metrikdaten konfigurieren, erfahren Sie unter MID Server und verteilter MID Server-Cluster für Metric Intelligence.

Agent Client Collector-Überwachung wird mit dem Plugin Ereignismanagement „ geliefert und erfordert auch die Installation der Anforderung Metricbase (Clotho DB), wie unter So fordern Sie die Konfiguration von Metricbase (Clotho DB) an (KB0816088) beschrieben an.

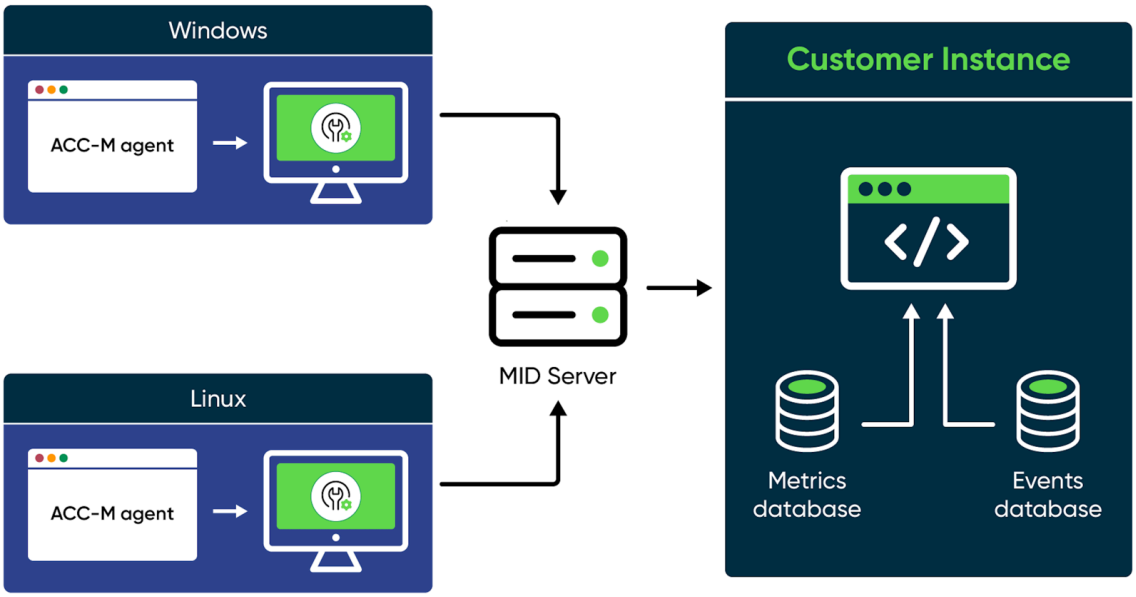
Einzelheiten zu den mit Agent Client Collector-Überwachunginstallierten Plugins finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Integrität.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector-Überwachung – Workflow

In der folgenden Abbildung werden das Layout und der Datenfluss in der Anwendung Agent Client Collector-Überwachung beschrieben.

Überwachung der Integrität und Verfügbarkeit von Services mit ACC-M



Agent Client Collector-Überwachung – Vorteile

Vorteil	Funktion	Anwender
Überwachungsprotokolle, die Ereignisse nachverfolgen, die in einer Windows -Umgebung auftreten	Windows Ereignisprotokollüberwachung	Agent Client Collector-Administrator
Überwachen Sie Betriebssysteme und Anwendungen	Betriebssystem- und Anwendungsüberwachung mit Agent Client Collector	Agent Client Collector-Administrator
Metriken zu Hostdaten sammeln	Metrikdaten	Agent Client Collector-Administrator

Agentbasierter Datenfluss

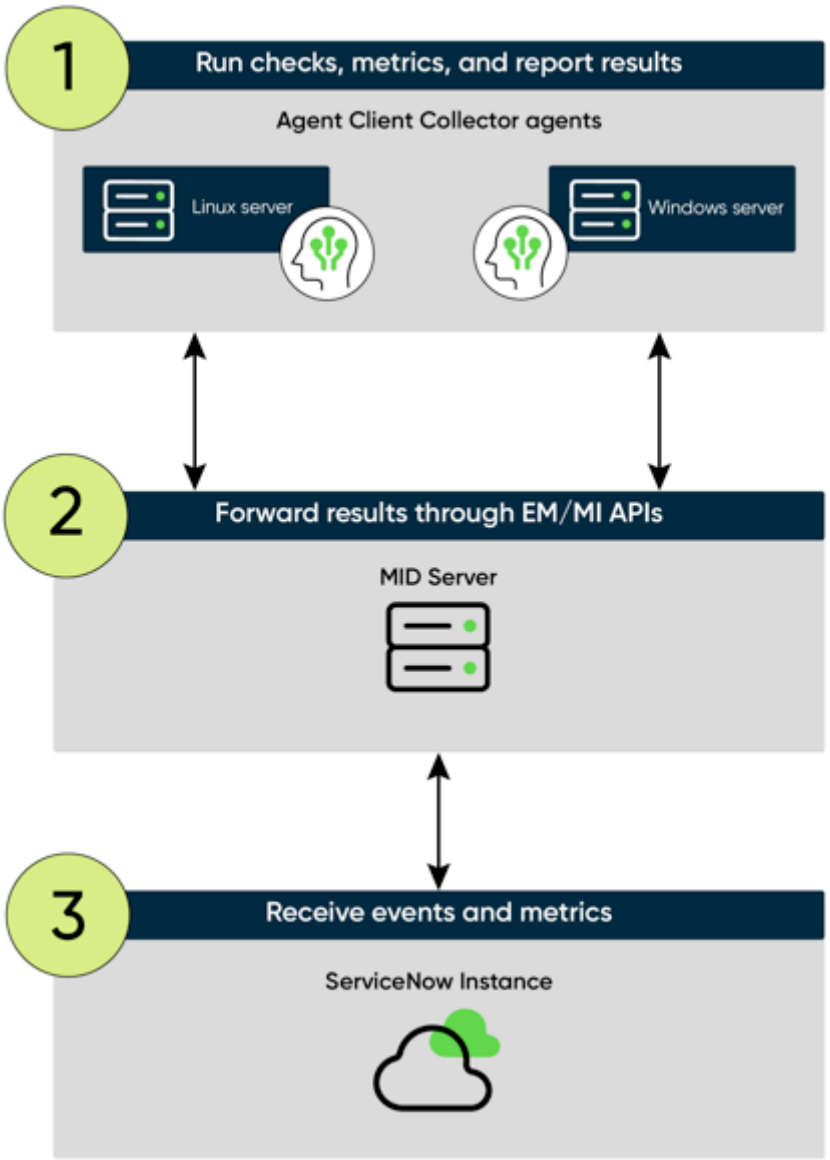
Agent Client Collector sammelt Informationen zum Zustand des CI, für den der Agent installiert ist, und zu den Anwendungen, die auf den Hosts ausgeführt werden. Der Agent führt mehrere Prüfungen durch und übermittelt die Ergebnisse der Prüfungen an den MID-Server, wo sie in Events oder Metriken umgewandelt werden.

Events werden in der Events-Datenbank der Instanz und Metriken in der Metrikdatenbank gespeichert.

Die folgende Abbildung zeigt den Datenfluss von Agent Client Collector zur Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die nummerierten Einträge im Flow stellen Folgendes dar:

1. Die angegebenen Prüfungen werden für den Agent ausgeführt. Daten, einschließlich Metriken, werden an den MID-Server übermittelt.
2. Der MID-Server analysiert die Daten und klassifiziert die Ergebnisse als Events oder Metriken. Der MID-Server verwendet die REST API, um die Ergebnisse an die Instanz zu senden.
3. Die Instanz empfängt die Daten und speichert sie in der entsprechenden Datenbank.

Agent Client Collector-Überwachung – Anwendungsfall

Der Anwendungsfall Agent Client Collector-Überwachung zeigt, wie Organisationen eine einheitliche Überwachung über hybride IT-Umgebungen hinweg erreichen können.

Übersicht über Anwendungsfälle

Viele Unternehmen arbeiten heute in einer hybriden IT-Umgebung, in der einige Ressourcen lokal gehostet werden, während sich andere in der Cloud befinden. Diese Komplexität führt häufig zu einer Fragmentierung der Überwachung, was es schwierig macht, einen einheitlichen Überblick über die Integrität von IT-Services zu erhalten. Agent Client Collector-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachung (ACC-M) schließt diese Lücke, indem ein umfassendes und konvergiertes Bild der Services eines Unternehmens vermittelt wird, unabhängig davon, wo sie gehostet werden. ACC-M ist eine schlanke Überwachungslösung, die sich nahtlos in die vorhandene Plattform ServiceNow integrieren lässt.

Herausforderung

Ein IT-Betriebsteam hatte aufgrund der unterschiedlichen Infrastruktur Probleme, die Serviceintegrität zusammenhängend zu überwachen. Lokale Ressourcen wie Datenbanken und ERP-Systeme wurden mit herkömmlichen Methoden überwacht, während Cloud-Services über separate Überwachungstools verfügten. Das Ergebnis dieser Fragmentierung:

- Es fehlt an Echtzeittransparenz in Bezug auf die allgemeine Serviceintegrität.
- Verzögerung bei der Identifizierung und Fehlerbehebung.
- Mehrere Überwachungsdashboards, erhöhen die Komplexität für das IT-Team.
- Schwierigkeiten bei der Korrelation von lokalen und Cloud-Warnungen, was zu Ineffizienzen führt.

Lösung

ACC-M ermöglicht eine einheitliche Echtzeittransparenz in einer hybriden IT-Umgebung. Sie verbessert die betriebliche Effizienz, reduziert Ausfallzeiten und sorgt für eine robustere IT-Infrastruktur, die sowohl lokale als auch cloudbasierte Services unterstützt.

ACC-M rationalisiert die Überwachung von lokalen und Cloud-Ressourcen in einer einzigen, einheitlichen Anzeige, indem die folgenden Lösungen angeboten werden:

Von ACC-M implementierte Lösungen

Lösung	Beschreibung	Ergebnis
Einheitliche Überwachung für alle Umgebungen	ACC-M erfasst Integritätsmetriken, Leistungsdaten und Warnungsstatus sowohl von lokalen als auch von cloudbasierten Infrastrukturkomponenten. ACC-M verwendet schlanke Agents, die auf Servern, VMs und Cloud-Ressourcen installiert sind, um relevante Daten zu sammeln. Sie bieten: • CPU-Auslastung und Arbeitsspeicher-Auslastung für lokale Server. • Netzwerkleistungsmetriken. • Verfügbarkeits- und Leistungsmetriken für Cloud-Services wie Datenbanken und Speicher.	Verbesserte Antwort: Mit einer einheitlichen Ansicht aller Ressourcen kann das IT-Betriebsteam schnell erkennen, wo Probleme auftreten, und sie basierend auf der Gesamtauswirkung auf den Service priorisieren. Dadurch wird die durchschnittliche Zeit bis zur Lösung (Mean Time-to-Resolution, MTTR) verkürzt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von ACC-M implementierte Lösungen (Fortsetzung)

Lösung	Beschreibung	Ergebnis
Ansicht der konvergierten Integrität	ACC-M stellt dem IT-Team eines Unternehmens ein konvergiertes Integritätsdashboard innerhalb der Plattform ServiceNow zur Verfügung, das: • Einheitliche Ansicht von lokalen und cloudbasierten Ressourcen. • Echtzeit-Updates zur Serviceintegrität, um sicherzustellen, dass Hybridservices gemeinsam und nicht isoliert überwacht werden. • Integrierte Einblicke in Serviceabhängigkeiten, die Incidents korrelieren, die sich sowohl auf lokale als auch auf cloudbasierte Systeme auswirken.	Proaktive Überwachung und Wartung: Die Echtzeit-Integritätsmetriken von ACC-M ermöglichen eine proaktive Überwachung von Services und vermeiden Ausfälle, indem Probleme erkannt und gelöst werden, bevor sie eskalieren.
Hybridwarnungen und -automatisierung	ACC-M ermöglicht die Einrichtung automatisierter Warnungen für lokale und cloudbasierte Umgebungen und optimiert so die Prozesse zur Reaktion auf Incidents. Wenn bei einem Service in der Hybridumgebung ein Problem auftritt, führt ACC-M Folgendes aus: • Generiert automatisch Warnungen mit erweitertem Kontext, die angeben, ob das Problem von der lokalen Infrastruktur oder von Cloud-Services verursacht wurde. • Löst automatisierte Workflows für die Behebung basierend auf dem Warnungstyp aus, wodurch manuelle Eingriffe reduziert werden.	Betriebliche Effizienz: Durch die Konvergenz von lokaler und cloudbasierter Überwachung auf einer einzigen Plattform sind mehrere Überwachungstools nicht mehr erforderlich. Dadurch wird die Komplexität reduziert, und die IT-Ressourcen können sich auf strategischere Aufgaben konzentrieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von ACC-M implementierte Lösungen (Fortsetzung)

Lösung	Beschreibung	Ergebnis
Serviceintegritätsvisualisierung	Die Verwendung der Servicezuordnung ServiceNow ermöglicht die Visualisierung der Leistung von Services in der gesamten Hybridinfrastruktur. ACC-M füttert sie mit kontinuierlichen Echtzeitdaten, die das IT-Team bei folgenden Aufgaben unterstützen: • Verfolgen Sie Abhängigkeiten zwischen lokalen und Cloud-Services nach. • Identifizieren Sie potenzielle Fehlerquellen, bevor sie sich auf das Geschäft auswirken. • Erkennen Sie auf einen Blick, welche Services fehlerfrei, beeinträchtigt oder gefährdet sind, unabhängig davon, wo sie gehostet werden.	Erweiterte Geschäftskontinuität: Mit einem vollständigen Überblick über die Integrität hybrider Infrastrukturen kann die IT sicherstellen, dass kritische Business Services betriebsbereit sind, und so die allgemeine Geschäftskontinuität verbessern.

Windows Ereignisprotokollüberwachung

Windows Die Ereignisprotokollüberwachung verfolgt, analysiert und verwaltet Ereignisprotokolle, die von verschiedenen Windows Betriebssystemkomponenten generiert wurden.

Die Richtlinie Windows „ BS-Ereignisse enthält die Prüfung os.windows.check-event-log, die das Ereignisprotokoll Windows anhand der in den Parametern der Prüfung angegebenen Schwellenwerte misst. Einzelheiten zu den konfigurierbaren Prüfungsparametern finden Sie unter Windows Ereignisprotokoll-Filterparameter.

Betriebssystem- und Anwendungsüberwachung mit Agent Client Collector

Die Überwachung von IT Operations Management (ITOM) für Agent Client Collector ist in der ServiceNow®-Instanz installiert. Dadurch werden das spezifische Betriebssystem und die Anwendungen überwacht, die auf dem Host-Computer installiert sind.

Agent Client Collector überwacht die folgenden Anwendungen.

ACC-Anwendungen

Betriebssystem/Anwendung	Konfigurationsbeschreibung
Windows	Keine spezielle Konfiguration erforderlich.
Linux	Keine spezielle Konfiguration erforderlich.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC-Anwendungen (Fortsetzung)

Betriebssystem/Anwendung	Konfigurationsbeschreibung
Apache HTTP Server	Weitere Informationen finden Sie unter Apache HTTP-Serverüberwachung mit Agent Client Collector konfigurieren.
Apache Tomcat	Weitere Informationen finden Sie unter Apache Tomcat-Überwachung mit Agent Client Collector konfigurieren.
IBM WebSphere	Keine spezielle Konfiguration erforderlich. Der Zugriff erfolgt über JMX. Standardverwaltungsport: **9100**.
IIS	Keine spezielle Konfiguration erforderlich.
JBoss/WildFly	Keine spezielle Konfiguration erforderlich. Standardport: **9990**. Informationen zur Fehlerbehebung finden Sie unter Leistungsüberwachung im Red Hat-Kundenportal.
Microsoft SQL Server	Keine spezielle Konfiguration erforderlich. Stellen Sie sicher, dass der Instanzname im CI-Datensatz eingetragen ist, indem Sie entweder Discovery ausführen oder den Datensatz manuell eintragen.
My SQL	Keine spezielle Konfiguration erforderlich. Standardport: **3306**.
Oracle-Datenbank	Keine spezielle Konfiguration erforderlich. Stellen Sie sicher, dass der SID- und Oracle-Basispfad im CI-Datensatz eingetragen ist, indem Sie entweder Discovery ausführen oder den Datensatz manuell eintragen. Standardport: **1521**.
Oracle WebLogic	Keine spezielle Konfiguration erforderlich. Der Zugriff erfolgt über einen JMX-Port. Standardport: **7001**. Stellen Sie sicher, dass der WebLogic-Basisparameter (wls_home) im CI-Datensatz eingetragen ist, indem Sie entweder Discovery ausführen oder den Datensatz manuell eintragen. Stellen Sie sicher, dass der Benutzer, der den Agent ausführt, über ausreichende Berechtigungen für den Zugriff auf die erforderlichen Dateien in den **WebLogic**-Installationsverzeichnissen verfügt.

Wenn Sie die Anwendungen **Microsoft SQL Server**, **Oracle Database** und **Oracle WebLogic** verwenden, müssen Sie Discovery ausführen, um CI-Felder in der Instanz zu konfigurieren. Stellen Sie sicher, dass das Plugin Discovery (com.snc.discovery) installiert ist, um die Ausführung von Discovery zu ermöglichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn die Anwendung auf einem anderen Port als dem Standardport ausgeführt wird, stellen Sie sicher, dass Sie die Portnummer in den Parametern der Prüfungsinstanz aktualisieren.

Apache HTTP-Serverüberwachung mit Agent Client Collector konfigurieren

Um Agent Client Collector für die Apache HTTP-Serverüberwachung zu konfigurieren, nehmen Sie in der Apache HTTP-Serveranwendung die folgenden Konfigurationen vor.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren Sie auf dem Host des Apache HTTP-Servers zu einem der folgenden Speicherorte:
   - In einer Linux-Umgebung:
     - `/etc/httpd`
     - `/etc/httpd/conf`
     - `/etc/apache2`
     - `/etc/apache2/conf`
   - In einer Windows-Umgebung: `conf`-Verzeichnis im Apache-Installationsverzeichnis
2. Suchen Sie entweder die Datei `httpd.conf` oder die Datei `apache2.conf`.
3. Stellen Sie sicher, dass die folgende Zeile keinen Kommentar enthält:
   `LoadModule status_module modules/mod_status.so`
4. Konfigurieren Sie den Port der Prüfungsinstanz so, dass er mit dem Port identisch ist, an dem Apache lauscht. (Der Standardport ist für beide **80**.)
5. Um eine sichere Verbindung zu gewährleisten, konfigurieren Sie SSL wie folgt:
   a. Stellen Sie sicher, dass die folgende Zeile keinen Kommentar enthält:
      `LoadModule ssl_module modules/mod_ssl.so`
   b. Aktivieren Sie den Parameter *ssl_secure_connection* in der Prüfungsinstanz.
   c. Konfigurieren Sie den Port der Prüfungsinstanz für sichere Verbindungen so, dass er mit dem Port identisch ist, an dem Apache lauscht. (Der Standardport ist **443**.)

Zugehörige Informationen

Apache-Modul

Apache SLL/TLS, starke Verschlüsselung: Vorgehensweise

Apache Tomcat-Überwachung mit Agent Client Collector konfigurieren

Um Agent Client Collector für die Apache-Tomcat-Überwachung zu konfigurieren, nehmen Sie in der Apache Tomcat-Anwendung die folgenden Konfigurationen vor.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie einen JMX-Verwaltungsport, wenn Sie den Server starten:

   a. In einer Linux-Umgebung:

      i. Erstellen Sie im Verzeichnis `bin` im Tomcat-Stammverzeichnis die Datei `setenv.sh`.

      ii. Stellen Sie sicher, dass die Datei Folgendes enthält:

```
export CATALINA_OPTS=$CATALINA_OPTS"
-Dcom.sun.management.jmxremote=true
-Dcom.sun.management.jmxremote.port={PORT NUMBER}
-Dcom.sun.management.jmxremote.rmi.port={PORT NUMBER}
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.authenticate=false
-Djava.rmi.server.hostname=127.0.0.1"
```

      iii. Führen Sie `chmod 755 setenv.sh` aus, um der Datei `setenv.sh` Ausführungsberechtigungen zuzuweisen.

   b. In einer Windows-Umgebung:

      i. Erstellen Sie im Verzeichnis `bin` im Tomcat-Stammverzeichnis die Datei `setenv.bat`.

      ii. Stellen Sie sicher, dass die Datei Folgendes enthält:

```
@echo=off
if defined CATALINA_OPTS (
set CATALINA_OPTS=%CATALINA_OPTS% -
Dcom.sun.management.jmxremote=true
) else (
set CATALINA_OPTS=-
Dcom.sun.management.jmxremote=true
)
set CATALINA_OPTS=%CATALINA_OPTS% -
Dcom.sun.management.jmxremote.port={PORT NUMBER}
set CATALINA_OPTS=%CATALINA_OPTS% -
Dcom.sun.management.jmxremote.rmi.port={PORT NUMBER}
set CATALINA_OPTS=%CATALINA_OPTS% -
Dcom.sun.management.jmxremote.authenticate=false
set CATALINA_OPTS=%CATALINA_OPTS% -
Dcom.sun.management.jmxremote.ssl=false
set CATALINA_OPTS=%CATALINA_OPTS% -
Djava.rmi.server.hostname=127.0.0.1
```

      {PORT NUMBER} entspricht der Nummer des Ports, den Sie für die JMX RMI-Überwachung öffnen. Der von der Prüfungsdefinition erstellte Standardwert lautet **9000**.

2. Starten Sie Tomcat neu.

   a. In einer Linux-Umgebung: Führen Sie zunächst das Skript `shutdown.sh` und dann das Skript `startup.sh` aus.

   b. In einer Windows-Umgebung: Führen Sie zunächst das Skript `shutdown.bat` und dann das Skript `startup.bat` aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Überwachen Sie HTTP-Punkte

Verwenden Sie die Richtlinien **„Überwachung von HTTP-Einstiegspunkten“** und **„Überwachung von HTTP-Einstiegspunktmetriken“**, die im Lieferumfang der bereichsbezogenen ITOM Überwachungs-App enthalten sind, um `http-` und `https-` Einstiegspunkte und Einstiegspunktmetriken zu überwachen. Sie können diese Richtlinien nach Bedarf anpassen oder eine neue Richtlinie für die Überwachung von Serviceeinstiegspunkten konfigurieren.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Einstiegspunkt ist der Zugangspunkt für einen Service. In einer Agent Client Collector-Richtlinie geben Sie den zu überwachenden Service an. Die Einstiegspunkte des Service werden dann mithilfe der Richtlinie überwacht.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**.
2. Wählen Sie eine der Richtlinien **Monitoring HTTP Entry Points** bzw. **Monitoring HTTP Entry Points Metrics** aus.
   Die entsprechende Seite **Policy - Monitoring HTTP Entry Points** wird geöffnet.
3. Auf der Registerkarte **Monitored CIs** (Überwachte CIs):
   a. Stellen Sie im Feld **Table** (Tabelle) sicher, dass die Datenbankansichts-Tabelle **sn_itmon_http_entrypoint** ausgewählt ist, damit Agent Client Collector HTTP- und HTTPS-Einstiegspunkte zur Überwachung abruft.
   b. Konfigurieren Sie im Abschnitt **Filter** einen Filter für die Services und Einstiegspunkte, die aus der Datenbankansichts-Tabelle **sn_itmon_http_entrypoint** übernommen werden sollen.
4. Klicken Sie auf die Registerkarte **Proxy Settings** (Proxy-Einstellungen), und wählen Sie den Proxy-Typ aus, den Sie für die Einstiegspunktüberwachung aktivieren möchten.
   - **Single proxy agent** (Einzelner Proxy-Agent): Wählen Sie diese Option aus, um die Überwachung eines einzelnen Agent zu aktivieren, den Sie im Feld **Proxy agent** auswählen, das nach Auswahl dieser Option eingeblendet wird.
   - **Multi-proxy agents by filter** (Mehrere Proxy-Agents durch Filter): Wählen Sie diese Option aus, um die Überwachung mehrerer Agents zu aktivieren. Konfigurieren Sie einen Filter im Abschnitt **Proxy Filter**, der nach Auswahl dieser Option eingeblendet wird, um nur die Agents zu überwachen, die mit den Filterbedingungen übereinstimmen.
   - **Script based proxy** (Skriptbasierter Proxy): Wählen Sie diese Option aus, um die Überwachung eines Agent basierend auf einem Skript zu aktivieren.

   Sie müssen einen Proxy zum Ausführen einer HTTP-Richtlinie konfigurieren.
5. Klicken Sie auf die Registerkarte **Checks** (Prüfungen), und wählen Sie im Feld **Filter checks by groups** (Prüfungen nach Gruppen filtern) die Option **HTTP** aus, um alle HTTP-Prüfungen in der Zelle **Available** (Verfügbar) anzuzeigen.
6. Wählen Sie die relevanten Prüfungen aus, und klicken Sie auf die Schaltfläche mit dem Rechtspfeil, um sie in die Zelle **Selected** (Ausgewählt) zu verschieben.
7. Aktivieren Sie das Kontrollkästchen **Active** (Aktiv) oben auf der Seite, um die Richtlinie zu aktivieren.
8. Klicken Sie auf **Aktualisieren**.
   Die Richtlinie überwacht die in den Konfigurationen der Richtlinie angegebenen Einstiegspunkte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector-Überwachung konfigurieren

Planen und konfigurieren Sie Ihre Agent Client Collector-Überwachung-Implementierung.

Um Agent Client Collector-Überwachungzu konfigurieren, gehen Sie wie folgt vor:

1. Ein MID-Server für die Verwendung mit Agent Client Collector-Überwachungkonfigurieren.
2. Zu überwachende Metriken auswählen und konfigurieren.
3. Konfigurieren Sie die Aktionsebene für die Anomalie-Erkennung.
4. Regel für Konfigurationseinstellungen erstellen.
5. Erfassung und Auswertung von Metriken aktivieren.

Führen Sie je nach zu überwachenden Prüfungen und Metriken die folgenden Aktionen aus, um die vollständige Aktivierung der Prüfung und die Erfassung von Metriken zu ermöglichen:

1. Anzeige von HAProxy-Metriken aktivieren.
2. Aktiviert die Ausführung von Varnish-Prüfungen.
3. Wählen Sie die Richtlinien Azure aus, die für die Metriksammlung aktiviert werden sollen.
4. Erstellen Sie Azure -Richtlinien für die Metrikensammlung.

Ein MID-Server für die Verwendung mit Agent Client Collector-Überwachungkonfigurieren

Verbinden Sie Service Desk-Mitarbeiter mit einem MID-Server, um die Funktion Agent Client Collector-Überwachung zu aktivieren.

Vorbereitungen

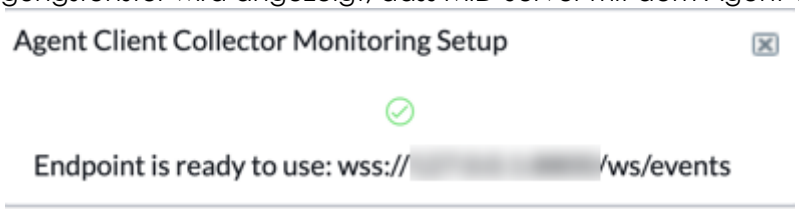
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Server**.
2. Wählen Sie MID-Server aus, die Sie mit dem Service Desk-Mitarbeiter verbinden möchten.
3. Wählen Sie im Abschnitt **„Zugehörige Links“ ACC-Überwachung einrichten**.

Ergebnisse

In einem Bestätigungsfenster wird angezeigt, dass MID-Server mit dem Agent verbunden ist.



Mehrere MID Servers für die Verwendung mit Agent Client Collector-Überwachungkonfigurieren

Verbinden Sie Service Desk-Mitarbeiter mit mehreren MID Servers, um die Funktion Agent Client Collector-Überwachung zu aktivieren. Mehrere MID Servers können sich gegenseitig beim Lastenausgleich und bei der Domänentrennung unterstützen.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie mehrere MID Serverskonfigurieren, verwenden Sie denselben Port für alle MID Servers. Wenn Sie verschiedene Ports verwenden, müssen Sie jeden MID-Server einzeln hinzufügen, wie in Ein MID-Server für die Verwendung mit Agent Client Collector-Überwachungkonfigurierenbeschrieben.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Server**.
2. Aktivieren Sie die Kontrollkästchen für MID Servers, die Sie mit Ihrem Service Desk-Mitarbeiter verbinden möchten.
3. Wählen Sie im Fenster **Aktionen für ausgewählte Zeilen...die Option ACC-Überwachung**einrichten aus.
   Die Option enthält die Anzahl von MID Servers, die aus der Anzahl der verfügbaren MID Serversausgewählt wurden. Beispiel: **Setup ACC Monitoring (7 of 8)** gibt an, dass 7 MID Servers von 8 verfügbaren MID Serversausgewählt wurden.

Ergebnisse

Ein Bestätigungsfenster zeigt an, dass die ausgewählten MID Servers mit dem Agent verbunden sind.

Zu überwachende Metriken auswählen und konfigurieren

Metric Intelligence verwendet Datenquellen, die Hunderte von Metriken für alle CIs überwachen können. Wählen Sie für jeden Datenquelltyp aus, welche Details für welche CIs wichtig sind, und aktivieren oder deaktivieren Sie dann den entsprechenden Überwachungstyp, um die Menge der verarbeiteten Daten zu steuern.

Vorbereitungen

Unter Erste Schritte mit Metrikdaten finden Sie allgemeine Schritte zum Setup von Metrikdaten.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Die SCOM-Datenquelle (standardmäßig verfügbar) erfasst etwa 400 Metriktypen von erkannten Geräten, z. B. „% verfügbarer Arbeitsspeicher“ und „% des freien Speicherplatzes“. Die Verarbeitung von Daten aus allen Metriktypen kann das System überlasten und die Leistung beeinträchtigen. Es kann erforderlich sein, ausgewählte Metriktypen für bestimmte CIs zu deaktivieren, um diese Last zu reduzieren.

Die Gesamtanzahl der Metriken, die verarbeitet werden können, hängt von der Anzahl der MID Server und deren Hardwarekonfiguration ab. Weitere Informationen zu Hardwareanforderungen und Skalierbarkeit von Metriken finden Sie unter MID Server und verteilter MID Server-Cluster für Metric Intelligence.

Hinweis: Die Einstellung *Active* („true“ oder „false“) für eine Metrik in der Tabelle „Überwachungssystemmetriken“ [sa_source_metric_type] hat Vorrang vor der Einstellung für die entsprechende Metrik in der Tabelle „Metrik-Zuordnung an CIs“ [sa_metric_map]. Wenn ein Metriktyp in der Tabelle „Überwachungssystemmetriken“ [sa_source_metric_type] deaktiviert ist, werden alle Datensätze, die sich auf die entsprechenden Metriken beziehen, aus der Tabelle „Metrik-Zuordnung an CIs“ [sa_metric_map] entfernt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Metriktypen**.
   In der Liste **Überwachungssystemmetriken** werden die Metriktypen angezeigt, die pro Datenquelle und CI-Typ erfasst werden.
2. Prüfen Sie die Liste **Typen der Überwachungssystemmetrik**, und legen Sie den Wert in der Spalte **Aktiv** je nach Bedarf auf **false** oder **true** fest.

Spalte	Beschreibung
Quelle	Datenquelle, die den Metriktyp überwacht.
Typ der Quellmetrik	Metriken wie „% freier Speicherplatz“, die für den CI-Typ überwacht werden
Aktionsebene der Anomalie-Erkennung	Die Ebene der Verarbeitung und Analyse der Erkennung von Anomalien, die auf CIs und Metriken angewendet wird. Verfügbare Optionen: ◦ **Nur Metriken**: Die Metriken aus der Datenquelle werden nur erfasst, ohne sie weiter zu verarbeiten. ◦ **Grenzen**: Beinhaltet die Verarbeitungsebene „Nur Metriken“. Zusätzlich werden statistische Modelle erzeugt und Grenzen im Explorer für Einblicke angezeigt. ◦ **Anomaliepunktzahlen**: Beinhaltet die Verarbeitungsebene „Grenzen“. Zusätzlich werden Anomaliepunktzahlen berechnet und angezeigt. ◦ **Anomaliewarnungen**: Beinhaltet die Verarbeitungsebene „Anomaliepunktzahlen“. Zusätzlich werden gegebenenfalls Anomaliewarnungen erzeugt. ◦ **IT-Warnungen**: Beinhaltet die Verarbeitungsebene „Anomaliewarnungen“. Zusätzlich werden gegebenenfalls IT-Warnungen auf Grundlage der Anomaliewarnungen erzeugt.
Typ des überwachten Objekts	CI-Typ, der überwacht wird.
Aktiv	Bestimmt, ob die Metrikdaten von Warnungszusammenfassungs- und RCA-Metriken von Ereignismanagement verarbeitet werden.
Einheit	Einheitentyp, der dem Quellmetriktyp zugeordnet ist und in den Berichten von Metric Intelligence angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurieren Sie die Aktionsebene für die Anomalie-Erkennung

Mit einer Regel für Konfigurationseinstellungen können Sie die Ebene der Anomalie-Erkennungs-Verarbeitung und -analyse präzisieren, die für bestimmte CIs und Metriken angewendet wird. Legen Sie eine Verarbeitungsebene fest, die die Bedeutung der Metriken in den verschiedenen Phasen der Implementierung widerspiegelt, um bei Bedarf die Datenlast zu reduzieren.

Die Anomalie-Erkennung umfasst mehrere Verarbeitungsebenen. Auf der untersten Ebene werden Metrikdaten aus Datenquellen gesammelt. Auf der höchsten Ebene werden statistische Modelle erzeugt, Anomaliepunktzahlen berechnet sowie Anomalie- und IT-Alarme erstellt. Sie können den vollständigen Anomalie-Erkennungs-Prozess oder eine reduzierte Verarbeitungsebene für bestimmte Datenreihen anwenden.

Verwenden Sie die Konfigurationseinstellung von *anomaly_detection_action_level* in einer Regel für Konfigurationseinstellungen, um die Verarbeitungsebene für bestimmte CIs und Metriken festzulegen. Beispielsweise können Sie zunächst nur einen kleinen Prozentsatz von CIs und Metriken festlegen, um Anomaliewarnungen zu generieren, und diesen Prozentsatz später erhöhen.

Aktionsebenen

Die Konfigurationseinstellung für *anomaly_detection_action_level* bietet Aktionsebenen, die bei „Nur Metriken“ für die grundlegende Anomalieverarbeitung beginnen und bei „IT-Warnungen“ für die vollständige Verarbeitung und Analyse enden.

Aktionsebenen von der niedrigsten bis zur höchsten:

Nur Metriken

Es werden nur Metriken aus der Datenquelle ohne weitere Verarbeitung erfasst.

Grenzen

Die Verarbeitungsebene „Nur Metriken“ und zusätzlich werden statistische Modelle erzeugt und Grenzen im Explorer für Einblicke angezeigt.

Anomaliepunktzahlen

Die Verarbeitungsebene „Grenzen“ und zusätzlich werden die Anomaliepunktzahlen berechnet und angezeigt.

Anomaliewarnungen

Die Verarbeitungsebene „Anomaliepunktzahlen“ und zusätzlich werden ggf. Anomaliewarnungen erzeugt.

IT-Warnungen

Die Verarbeitungsebene „Anomaliewarnungen“ und zusätzlich werden ggf. IT-Warnungen auf Grundlage der Anomaliewarnungen erzeugt.

Zugehörige Informationen

Regel für Konfigurationseinstellungen erstellen

Regel für Konfigurationseinstellungen erstellen

Konfigurationseinstellungen wirken sich darauf aus, wie Metrikdaten verarbeitet werden. Konfigurationseinstellungsregeln überschreiben das Standardverhalten bei der Metrikverarbeitung, um die Systemaktionen festzulegen, wenn eine Anomalie erkannt wird.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Eine Reihe von Konfigurationseinstellungen bestimmen das Verhalten von Metrikdaten MID Servers. Im Basissystem werden diese Konfigurationseinstellungen mit Standardwerten, Datentypen und gültigen Wertebereichen konfiguriert. Sie können diese Konfigurationseinstellungen nicht direkt ändern oder neue hinzufügen. Sie können jedoch eine Metrikkonfigurationsregel mit neuen Konfigurationseinstellungen erstellen, die die Standardwerte auf den MID Servern überschreiben.

Wenden Sie diese Regeln dann manuell auf alle Metrikdaten MID Servers in einem einzigen Synchronisierungsvorgang an, oder verlassen Sie sich auf eine stündliche Systemaufgabe, um die Synchronisierung durchzuführen.

Damit wirksam wird, muss Metrikdaten MID Servers mit den Aktualisierungen der Konfigurationseinstellungsregeln synchronisiert werden.

Es ist zulässig, über mehrere Regeln für eine Einstellung zu verfügen, die sich auf dieselben CIs auswirken. In diesem Fall gilt Folgendes:

- Regeln, in denen ein Filter definiert ist, haben Vorrang vor einer globalen Regel, in der kein Filter definiert wurde.
- Wenn mehrere Regeln, die sich auf denselben CI-Satz auswirken, dieselbe Priorität haben, wird nur die zuletzt zu definierende Regel angewendet.
- Wenn mehrere Regeln mit unterschiedlichen Prioritäten denselben CI-Satz betreffen, werden Regeln mit der höchsten Priorität angewendet.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Konfig.-Regeln für Metrik**.
2. Klicken Sie im Bereich „Metrikkonfigurationsregeln“ auf **Neu**, und füllen Sie das Formular aus.

Formular „Metrikkonfigurationsregeln“

Feld	Beschreibung
Name	Regelname
Reihenfolge	Regelpriorität in allen anderen Regeln. Höhere Zahlen stehen für höhere Prioritäten.
Filtern nach	Kontrollkästchen zum Anzeigen des Felds **Regel**, in dem Sie Bedingungen angeben können, die CIs erfüllen müssen, damit die Regel angewendet wird. Beispiel: Wählen Sie in der Liste **Feld auswählen** den Eintrag **Add Related Fields (Zugehörige Felder hinzufügen)** aus, und fügen Sie dann den Filter **[Klasse][ist][Linux-Server]** hinzu. Wenn diese Option deaktiviert ist, gilt die Regel global für alle CIs in der Tabelle „Metrik-Zuordnung an CI“ [sa_metric_map].

3. Klicken Sie mit der rechten Maustaste auf den Formulartitel, und wählen Sie **Speichern** aus.
4. Klicken Sie im Formularabschnitt „Überschriebene Konfigurationen der Metrik“ auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Überschriebene Konfigurationen der Metrik“

Feld	Beschreibung
Name	Konfigurationseinstellung, für die der Wert überschrieben werden soll. Klicken Sie auf das Symbol , um die Liste aller Konfigurationseinstellungen anzuzeigen. Klicken Sie auf das Symbol , um das Dialogfeld **Metrikeinstellungen** mit Details wie dem Bereich möglicher Werte anzuzeigen. Weitere Informationen zu Konfigurationseinstellungen finden Sie in den folgenden Tabellen („Konfigurationseinstellungen“ und „Interne Konfigurationseinstellungen“).
Regel	Regel, für die die erstellte Konfigurationseinstellung gilt
Wert	Neuer Wert, der den Standardwert für die angegebene Konfigurationseinstellung überschreibt.

Sie können die folgenden Konfigurationseinstellungen im Feld **Name** ändern.

Hinweis: Der in der Metrikkonfigurationsregel angegebene Filter gilt nicht für Einstellungen mit einem globalen Bereich.

Konfigurationseinstellungen

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
anomaly_detection_enabled Anomalie-Erkennung aktivieren/deaktivieren. **Hinweis:** Wenn anomaly_detection_action_level festgelegt ist, wird anomaly_detection_enabled ignoriert.	N/V	wahr	Boolean	CI/Metrik
anomaly_detection_action_level Aktionsebene der Anomalieanalyse und -verarbeitung. Weitere Informationen finden Sie unter Konfigurieren Sie die Aktionsebene für die Anomalie-Erkennung.	Auswahlmöglichkeiten: ◦ Nur Metriken ◦ Grenzwerte ◦ Anomaliepunktzahlen ◦ Anomaliewarnungen ◦ IT-Warnungen	◦ Neue Datensätze: Grenzen ◦ Aktualisierte Datensätze: Anomaliewarnungen	Auswahl	CI/Metrik
buffer_anomaly_eviction_size	60–1440	60	ganze Zahl	Global

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Maximale Anzahl von Anomalien auf individueller Metrikebene, die im internen Puffer gespeichert werden können, bevor sie für jedes CI/Metrik-Paar an die Instanz gesendet werden				
buffer_ci_score_eviction_size Maximale Anzahl von Anomalien auf CI-Ebene, die im internen Puffer gespeichert werden können, bevor sie an die Instanz gesendet werden (aktuell nicht verwendet)	60–1440	60	ganze Zahl	Global
buffer_metric_eviction_size Maximale Anzahl von Metriken, die im internen Puffer gespeichert werden können, bevor sie für jedes CI/Metrik-Paar an die Instanz gesendet werden	60–1440	60	ganze Zahl	Global
connection_login_timeout_secs Maximale Zeit in Sekunden für die Anmeldung bei der lokalen Datenbank auf dem MID Server	30–60	30	ganze Zahl	Global
corrupt_data_count_threshold Mindestanzahl von Schulungspunkten (Durchschnitt: 15 Minuten), die für statistische Analysen erforderlich ist	10–100	30	ganze Zahl	Global
deprioritize_early_batching_of_anomalous_ci Senden Sie anomale CI-Informationen sofort oder in regelmäßigen Abständen.	N/V	falsch	Boolean	Global
mad_model_min_days Anzahl der Tage, für die Daten verfügbar sein müssen, damit ein Modell auf Basis	10–120	10	ganze Zahl	CI/Metrik

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
der mittleren absoluten Abweichung vom Median (Median Absolute Deviation, MAD) in Erwägung gezogen werden kann.				
max_pool_connections_size Maximale Anzahl von Verbindungen für lokalen Datenbankpool	10–50	25	ganze Zahl	Global
observation_time_min Erwartetes minimales Beobachtungsintervall für Metrik	1–1440	1	ganze Zahl	CI/Metrik
robust_central_percentage Prozentsatz der Restdaten zur Berechnung der Reststandardabweichung für die Ausreißererkennung. Wenn auf 100 festgelegt, wird die Standardabweichung der regulären Stichprobe verwendet.	50–100	90	doppelt	Global
sparse_gap_fraction_threshold Wenn mehr als dieser Prozentsatz der Daten fehlt und keine andere Klasse identifiziert wurde, klassifizieren Sie sie als SPARSE. Versuchen Sie nicht, ein WEEKLY-Modell anzupassen.	0–100	50	doppelt	Global
weekly_model_min_days Anzahl der Tage, für die Daten verfügbar sein müssen, um nur eine WÖCHENTLICHE saisonabhängige Zerlegung zu berücksichtigen	14–90	15	ganze Zahl	CI/Metrik
daily_model_min_days Anzahl der Tage, für die Daten verfügbar sein müssen, um nur eine TÄGLICHE saisonabhängige Zerlegung zu berücksichtigen	2–90	3	ganze Zahl	CI/Metrik

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
build_snpm_model Erstellung eines SNPM-Datenmodells aktivieren/deaktivieren	N/V	wahr	Boolean	CI/Metrik
snpm_minimum_data_count Mindestanzahl der Datenpunkte, die für die Erstellung eines stationären, nicht-parametrischen Modells erforderlich sind	0 – 1e9	5.000	ganze Zahl	CI/Metrik

Die folgenden Konfigurationseinstellungen sind für die interne Verwendung bestimmt.

Interne Konfigurationseinstellungen

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
anomaly_memory_time_min Anomaliepunktzahl-Rechnerparameter: Speicherzeit für anormale Situation	1–600	45	doppelt	CI/Metrik
excess_z_score Anomaliepunktzahl-Rechnerparameter: Minimale Anomalie für Ausreißer akkumuliert	0–3	0,8	doppelt	CI/Metrik
linear_accumulator_threshold Schwellenwert der Entscheidungsstruktur: ACCUMULATOR-Analyse	0,5–5	1	doppelt	Global
low_freq_power_threshold Schwellenwert der Entscheidungsstruktur: WEEKLY-Analyse	0–100	50	doppelt	Global
low_variability_threshold Schwellenwert der Entscheidungsstruktur: TRENDY-Analyse	0,0000000001–0,001	0,0001	doppelt	Global
mid_freq_power_threshold	0–100	33	doppelt	Global

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Schwellenwert der Entscheidungsstruktur: WEEKLY-Analyse				
multinomial_count_threshold Schwellenwert der Entscheidungsstruktur: MULTINOMIAL-Analyse	1–1000	40	ganze Zahl	Global
non_zero_diff_threshold Schwellenwert der Entscheidungsstruktur: NEAR_CONSTANT-Analyse	0–100	5	doppelt	Global
normal_memory_time_min Anomaliepunktzahl-Rechnerparameter: Speicherzeit für normale Situation	1–600	1	doppelt	CI/Metrik
normal_probability_ewma_timescale_min Anomaliepunktzahl-Rechnerparameter: Normale Bewertungszeitskala	1–600	15	doppelt	CI/Metrik
normal_probability_weight Anomaliepunktzahl-Rechnerparameter: Anpassungsfaktor normale Bewertung	0–1	1	doppelt	CI/Metrik
sigmoid_offset Anomaliepunktzahl-Rechnerparameter: Konvertierung der Anomalie zu Punktzahl	0–5	2,1	doppelt	CI/Metrik
sigmoid_weight Anomaliepunktzahl-Rechnerparameter: Konvertierung der Anomalie zu Punktzahl	0–5	1,2	doppelt	CI/Metrik
tiny_variability_threshold	0–0,001	0,0000000001	doppelt	Global

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Schwellenwert der Entscheidungsstruktur: NEAR_CONSTANT-Analyse				
weekly_peak_hi_limit Schwellenwert der Entscheidungsstruktur: WEEKLY-Analyse	7–14	10	doppelt	Global
weekly_peak_lo_limit Schwellenwert der Entscheidungsstruktur: WEEKLY-Analyse	0,5–7	0,7	doppelt	Global
weekly_vs_daily_log_likelihood_threshold Um wie viel die Protokollwahrscheinlichkeit von WEEKLY größer als von DAILY sein muss, um das bevorzugte statistische Modell zu sein	100–1000	200	doppelt	CI/Metrik
daily_vs_noisy_log_likelihood_threshold Um wie viel die Protokollwahrscheinlichkeit von DAILY größer als von NOISY sein muss, um das bevorzugte statistische Modell zu sein	20–1000	200	doppelt	CI/Metrik
weekly_vs_noisy_log_likelihood_treshold Um wie viel die Protokollwahrscheinlichkeit von WEEKLY größer als von NOISY sein muss, um das bevorzugte statistische Modell zu sein	100–1000	200	doppelt	CI/Metrik
trendy_vs_noisy_log_likelihood_threshold Um wie viel die Protokollwahrscheinlichkeit von TRENDY größer als von NOISY sein muss, um das bevorzugte statistische Modell zu sein	10–1000	50	doppelt	CI/Metrik
seasonal_loess_width_in_hours	6–24	12	doppelt	CI/Metrik

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Wird auf die saisonale Komponente eines WEEKLY- oder DAILY-Modells angewendet, bevor eine Prognose für das zukünftige Verhalten erstellt wird. Wenn auf 0 festgelegt, wird jeder Datenpunkt im Saisonmodell unabhängig vom Rest der Datenpunkte.				
robustness Beeinflusst, wie Ausreißer zu saisonabhängigen und Trendberechnungen beitragen	N/V	wahr	Boolean	CI/Metrik
snpm_min_value_threshold Mindestwert der Daten, die zum Erstellen eines SNPM-Modells erforderlich sind	-1e9 – 1e9	0	doppelt	CI/Metrik
snpm_max_observation_interval_in_sec Maximales erwartetes Beobachtungsintervall, das zum Erstellen eines SNPM-Modells erforderlich ist	60–600000	120	ganze Zahl	CI/Metrik
min_std_jump_fraction Mindestverhältnis des lokal berechneten Beobachtungsrauschpegels zur typischen Sprunggröße, das die Neuberechnung einer größeren Abweichung des Beobachtungsrauschens rechtfertigt	0,0–1,0	0,2	doppelt	CI/Metrik
dynamic_threshold_error_smoothing Ob der exponentiell gewichtete gleitende Durchschnitt verwendet werden soll, um die Reste in der dynamischen Schwellenwertanalyse zu glätten	N/V	wahr	Boolean	CI/Metrik
ewma_alpha Der Alpha-Wert des exponentiell gewichteten gleitenden	1e-15–1,0	0,02739726027	doppelt	CI/Metrik

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Durchschnitts in der dynamischen Schwellenwertanalyse				
dynamic_threshold_beginning_smoothing_length Anzahl der geglätteten Datenpunkte, die auf den Mittelwert der doppelten Glättungslänge festgelegt werden soll	0–10.000	250	ganze Zahl	CI/Metrik
dynamic_threshold_error_buffer_minutes Anzahl der Datenpunkte um jeden Ausreißer, die gruppiert werden sollen	1–1000	30	ganze Zahl	CI/Metrik
dynamic_threshold_search_start Startwert, bei dem nach dem optimalen Steuerungsfaktor gesucht wird	0,5–20,0	3,0	doppelt	CI/Metrik
dynamic_threshold_search_interval Intervall zwischen Suchwerten des optimalen Kontrollfaktors	0,1–5,0	0,5	doppelt	CI/Metrik
dynamic_threshold_search_count Anzahl der Werte, die für die Suche nach dem optimalen Steuerungsfaktor erforderlich sind	1–50	19	ganze Zahl	CI/Metrik
dynamic_threshold_error_sequence_limit Maximale Anzahl von Fehlergruppen für einen bestimmten Steuerungsfaktorwert bei der Suche	1–20	5	ganze Zahl	CI/Metrik
dynamic_threshold_minimum_data_count Mindestanzahl der erforderlichen Rohdatenpunkte vor dem Versuch der dynamischen Schwellenwertbestimmung	1–10.000	5.000	ganze Zahl	CI/Metrik
linear_seasonal_log_likelihood_threshold	10–5.000	1.000	ganze Zahl	CI/Metrik

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name und Beschreibung	Werte	Standard	Datentyp	Bereich
Schwellenwert, der bei der Entscheidung verwendet wird, ob ein angepasstes Modell mit linearer Saisonalität einem Modell mit einer periodischen Komponente vorgezogen wird				

Regeln für Konfigurationseinstellungen synchronisieren

Die Konfigurationseinstellungsregeln für Metric Intelligence enthalten benutzerdefinierte Werte, die Standardwerte überschreiben, die derzeit auf MID Servern für Metric Intelligence vorhanden sind. Um wirksam zu werden, müssen die Metric Intelligence-MID Server mit dem Update Set der Konfigurationseinstellungsregeln synchronisiert werden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Synchronisierung manuell initiieren, um die Aktualisierungen sofort auf alle Metric Intelligence-MID Server anzuwenden. Oder Sie verlassen sich auf einen Systemauftrag, der nach einem stündlich wiederkehrenden Zeitplan ausgeführt wird und nach Updates für die Metrikkonfigurationsregeln sucht. Wenn festgestellt wird, dass Aktualisierungen vorhanden sind, sendet der Systemauftrag diese Aktualisierungen an die Metric Intelligence-MID Server.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement-Regeln** > **Anomalie-Erkennung** > **Konfig.-Regeln für Metrik**.
2. Klicken Sie im Bereich „Metrikkonfigurationsregeln“ auf **Mit MID synchronisieren**.

Nächste Maßnahme
Stellen Sie sicher, dass alle Metric Intelligence-MID Server mit dem aktualisierten Satz der Konfigurationseinstellungsregeln synchronisiert wurden:

1. Navigieren zu **Ausgabe und Artefakte** > **ECC-Warteschlange**.
2. Suchen Sie im Bereich **Warteschlangen** in der Spalte **Themen** nach `MetricConfigProbe`.
3. Überprüfen Sie die Spalte **Agent** und stellen Sie sicher, dass alle MID Server aktualisiert wurden.

Erfassung und Auswertung von Metriken aktivieren

Damit eine ServiceNow -Instanz Metriken sammeln und auswerten kann, müssen Sie einen verteilten MID-Server -Cluster erstellen, MID Servers dem -Cluster zuordnen und Metrikdaten für MID-Serveraktivieren.

Vorbereitungen
Stellen Sie sicher, dass in Ihrer Instanz die folgenden Plugins installiert sind:

- Ereignismanagement (com.glideapp.itom.snac)
- Metrikdaten Plugin „com.snc.sa.metric“.
- MetricBase

So überprüfen Sie, dass das Plugin MetricBase ordnungsgemäß installiert wurde:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Geben Sie im Instanznavigationsbereich `stats.do` ein.
2. Suchen Sie nach dem Abschnitt mit den **MetricBase-Statistiken**, und stellen Sie sicher, dass Folgendes angezeigt wird:
   - Status: ONLINE
   - Name: clotho

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Erstellen Sie einen verteilten Cluster MID-Server in Ihrer Instanz:

   a. Navigieren zu **MID-Server** > **Cluster**.
   Die Seite MID-Server -Cluster wird geöffnet und zeigt die Liste der konfigurierten MID-Server -Cluster an.

   b. Klicken Sie auf **Neu**.
   Die Seite **MID Server-Cluster – Neuer Datensatz** wird geöffnet.

   c. Weisen Sie im Feld **Name** einen beschreibenden Namen für das Cluster zu.

   d. Wählen Sie im Feld **Typ** die Option **Verteilt** aus.

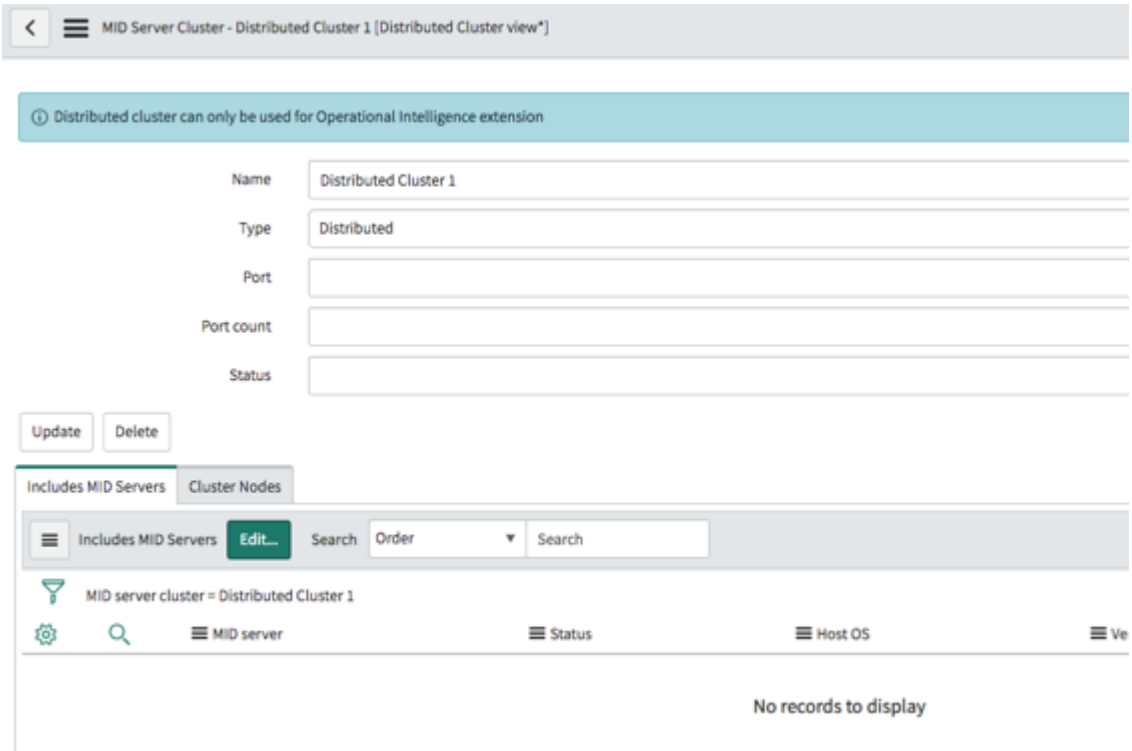
   e. Klicken Sie auf **Absenden**.
   Der verteilte MID-Server wird auf der Seite MID-Server -Cluster angezeigt.

2. Weisen Sie MID Servers dem verteilten Cluster MID-Server zu:

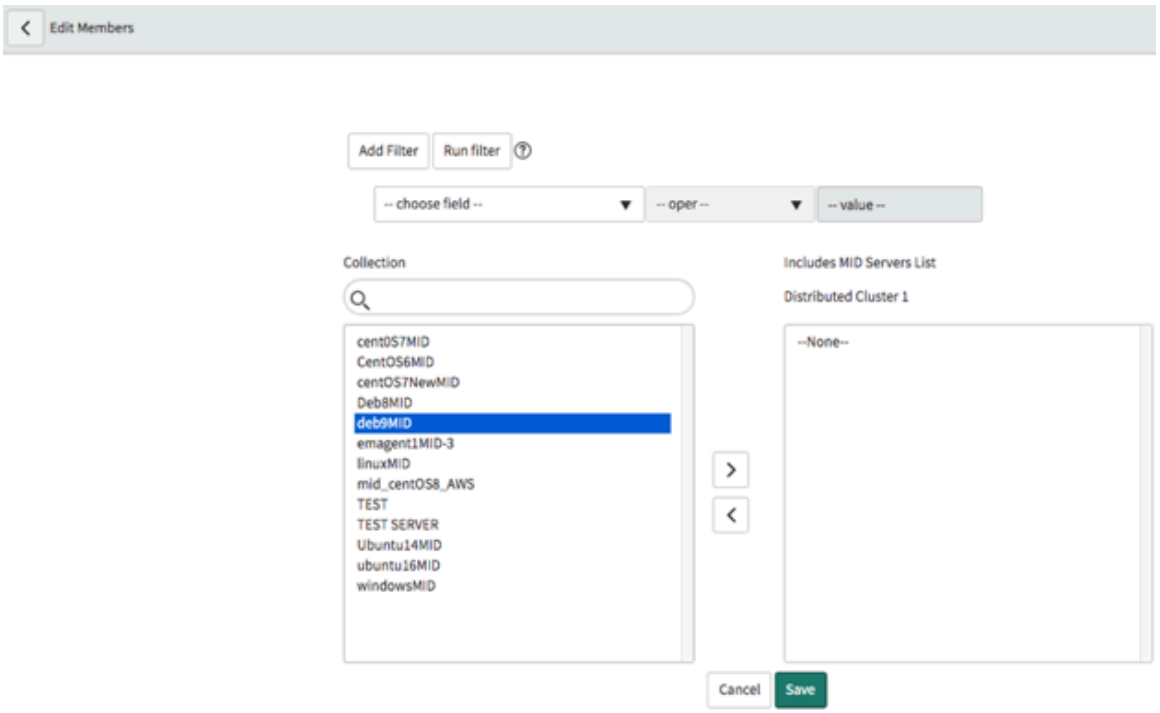
   a. Wählen Sie auf der Seite MID-Server -Cluster das verteilte Cluster MID-Server aus.
   Die folgende Seite wird angezeigt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



b. Klicken Sie auf der Registerkarte **Enthält MID Server** auf **Bearbeiten**.
Die Seite **Mitglieder bearbeiten** wird angezeigt.

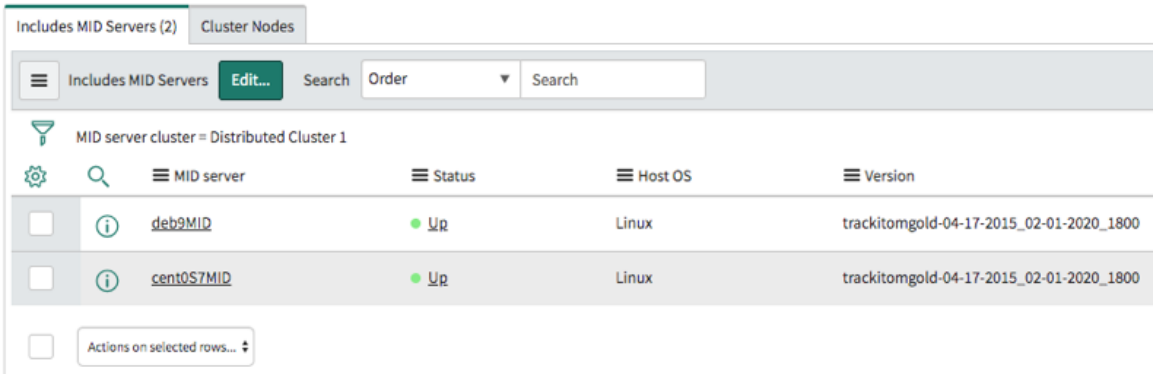


c. Wählen Sie das relevante MID Servers aus der linken Zelle aus, und klicken Sie auf die rechte Pfeilschaltfläche [>] um sie in die rechte Zelle zu verschieben.
In einer Staging-Umgebung ist es akzeptabel, mit nur einem MID-Server im Cluster zu arbeiten.

d. Klicken Sie auf **Speichern**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

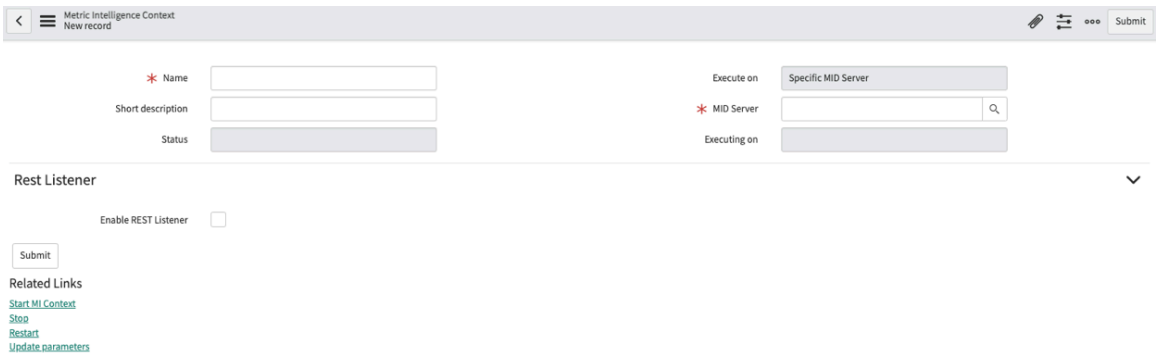
Auf der Registerkarte **Enthält MID-Server** werden die MID Servers angezeigt, die Teil des Clusters sind.



3. Metrikdaten für MID-Serveraktivieren:

a. Navigieren zu **MID-Server** > **Erweiterungen** > **Metrikdaten**.
Die Seite **Metric Intelligence Metrics Contexts** (Metric Intelligence-Metrikkontexte) wird angezeigt.

b. Klicken Sie auf **Neu**.
Die Seite **Metric Intelligence Contexts - New record** (Metric Intelligence-Kontexte – Neuer Datensatz) wird angezeigt.



c. Geben Sie im Feld **Name** einen beschreibenden Namen für die Metrikdaten-Metrikerweiterung ein.

d. Wählen Sie im Feld **MID-Server** den MID-Server aus, dem Sie die Metrikenerweiterung Metrikdaten zuordnen möchten.

e. Aktivieren Sie das Kontrollkästchen **ACC Dedicated MID**, um den angegebenen MID-Server als einzigen MID-Server im verteilten Cluster zuzuweisen.
Durch Auswahl dieser Option sparen Sie Systemressourcen und -speicher.

f. Klicken Sie im Abschnitt **„Zugehörige Links“** unten auf der Seite auf **Starten**.
Eine Meldung mit dem Status der Erweiterung wird angezeigt.

g. Klicken Sie auf **Absenden**.

h. Klicken Sie auf **Start**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfassung und Auswertung von Metriken beschränken

Sie können die Metriken beschränken, die der MID-Server an die Instanz sendet, indem Sie entweder ein bestimmtes CI oder einen kompletten CI-Typ deaktivieren.

Vorbereitungen

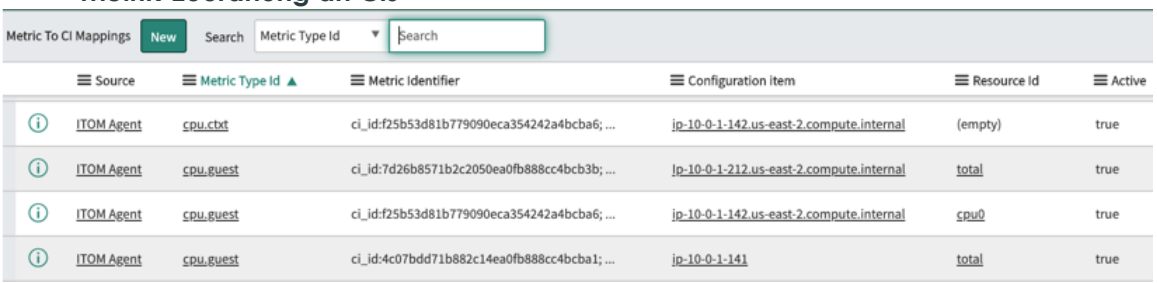
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. So beschränken Sie die Sammlung und Auswertung von Metriken für bestimmte CIs:

   a. Navigieren zu **Ereignismanagement** > **Anomalie-Erkennung** > **Metrik an CI**.
   Die Seite **Metrik-Zuordnung an CIs** wird angezeigt.

Metrik-Zuordnung an CIs



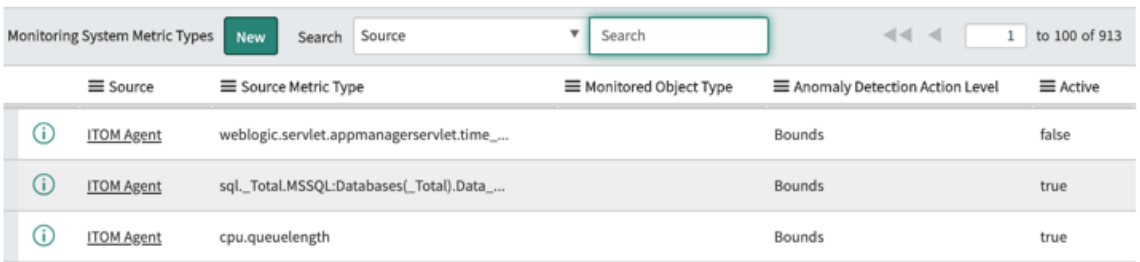
> **Hinweis:** Die Zuordnung der Metrik zum CI wird sowohl anhand der Metrik-ID als auch durch das Konfigurationselement identifiziert.

   b. Um zu verhindern, dass Metriken für eine bestimmte Metrik und ein bestimmtes CI gesendet werden, legen Sie den Wert der Spalte **Aktiv** auf **false** fest.

2. So beschränken Sie die Sammlung und Auswertung von Metriken für einen kompletten CI-Typ:

   a. Navigieren zu **Ereignismanagement** > **Anomalie-Erkennung** > **Metriktypen**.
   Die Seite **Typen der Überwachungssystemmetrik** wird angezeigt.

Typen der Überwachungssystemmetrik



   b. Um zu verhindern, dass Metriken für einen Metriktyp gesendet werden, legen Sie den Wert der Spalte **Aktiv** auf **false** fest.

Ereigniserstellung für nicht vorhandene Entitäten blockieren

Rufen Sie den Parameter *skip_events_for_nonexistent* auf, um die Ereigniserstellung zu blockieren, wenn ein bestimmter Prozess, Service oder Protokoll nicht vorhanden ist. Rufen Sie diesen Parameter auf, wenn Sie nicht über diese nicht vorhandenen Entitäten benachrichtigt werden möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Ein Prozess, Service oder Protokoll ist nicht vorhanden, wenn die folgenden Prüfungen keine gültigen Werte für die angegebenen Parameter enthalten:

Parameter überprüfen

Überprüfen	Parameter
os.linux.check-process	*file_pid*, *daemon_name*
util.check-windows-service	*service*
os.windows-check-log	*file*
util.checks-logs	*file*
util.checks-logs-sudo	*file*

Prozedur
1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Prüfungsdefinitionen**.
2. Suchen Sie die Prüfungsdefinition, für die Sie Ereignisse blockieren möchten.
3. Wählen Sie auf der Registerkarte **Parameterdefinitionen überprüfen** die Option *skip_events_for_nonexistent*aus.
4. Aktivieren Sie das Kontrollkästchen **Aktiv**, um den Parameter zu aktivieren und die Erstellung von Warnungen zu verhindern, wenn der Prozess, Service oder Protokoll für die angegebene Prüfung nicht gefunden wird.
   Wenn Sie eine Benachrichtigung über den fehlenden Prozess oder Service erhalten möchten, belassen Sie den Parameter *skip_events_for_nonexistent* auf dem Standardwert **false**.

Anzeige von HAProxy-Metriken aktivieren

Konfigurieren Sie die Statistikseite für HAProxy-Metriken, um die Überwachung Ihrer Systemgeräte durch Anzeige von HAProxy-Metriken zu ermöglichen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
HAProxy bietet Lastenausgleichs- und Reverse-Proxy-Funktionen für HTTP- und TCP-Anforderungen. Durch HAProxy-Prüfungen werden Back-End-Server entfernt, die mehrere Integritätsprüfungen hintereinander nicht bestehen. Außerdem wird eingehender Datenverkehr im Rahmen des Lastenausgleichs an Back-End-Server übertragen.

Prozedur
1. Greifen Sie auf die HAProxy-Konfigurationsdatei zu, die unter `/etc/haproxy/haproxy.cfg` gespeichert ist.
2. Fügen Sie den folgenden Code am Ende der Datei hinzu:

```
listen frontend *:8080       #Haproxy
Monitoring run on port 8080
mode http
option forwardfor
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
option httpclose
stats enable
stats show-legends
stats refresh 5s
stats uri /stats        #URL for HAProxy monitoring
stats realm Haproxy\Statistics.   #Title for pop up window
stats auth admin:admin     #User and Password for login to the
 monitoring dashboard
stats admin if TRUE
default_backend backend       #This is optional for monitoring backend
```

3. Führen Sie den folgenden Befehl aus, um HAProxy neu zu starten:
   `sudo service haproxy restart`
4. Zeigen Sie die HAProxy-Metriken auf dem System an, indem Sie die Statistikseite für HAProxy-Metriken aufrufen, auf die Sie über die folgende URL zugreifen können:
   `http://<HAProxyServer> :8080/stats`

Zugehörige Informationen

HAProxy – Standardprüfungen und Richtlinien

Aktiviert die Ausführung von Varnish-Prüfungen

Verwenden Sie Anwendungsfingerabdrücke, um das Varnish-CI (Configuration Item) zu erkennen und so die Ausführung von Varnish-Prüfungen zu ermöglichen.

Vorbereitungen

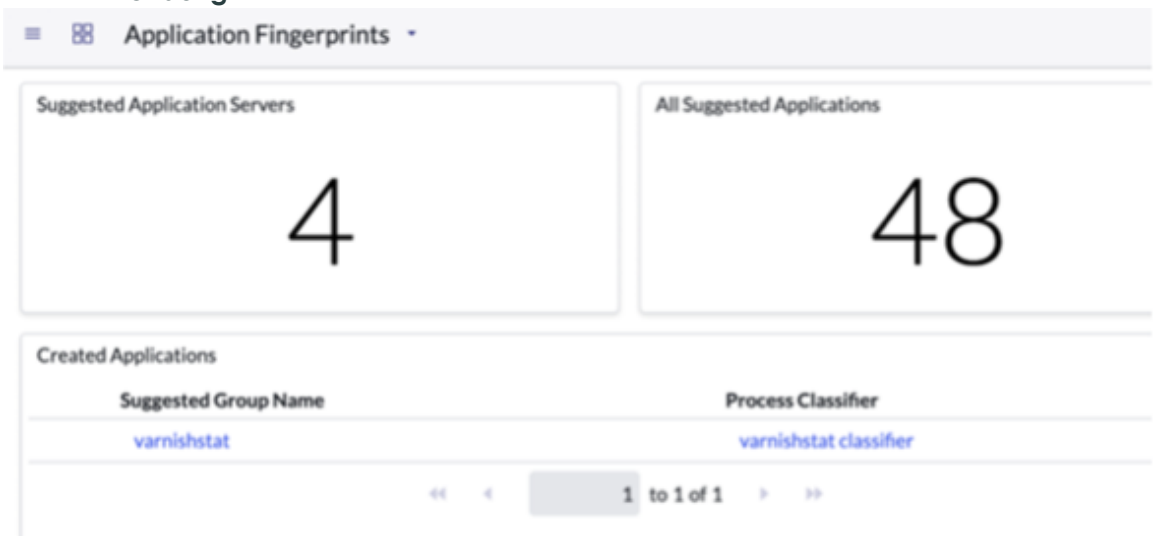
Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Discovery** > **Startseite**.
2. Wählen Sie die Kachel **Fingerabdrücke der Anwendung** aus.
   Das Dashboard **Fingerabdrücke der Anwendung** wird geöffnet.
3. Wählen Sie die Kachel **Alle vorgeschlagenen Anwendungen** aus.
4. Wählen Sie auf der Seite „Anwendungsvorschläge“ in der Spalte **Vorgeschlagener Gruppenname** den Eintrag **varnishstat** aus.
   Die varnishstat-Details werden auf der Seite „Anwendungsvorschläge“ angezeigt.
5. Wählen Sie „Anwendung erkennen“ aus.
   Von Discovery wird nach einem Anwendungs-CI für den varnishstat-Eintrag gesucht. Das CI wird im Dashboard „Fingerabdrücke der Anwendung“ im Abschnitt **Erstellte Anwendungen** angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abschnitt „Erstellte Anwendungen“ des Dashboards „Fingerabdrücke der Anwendung“



6. Führen Sie auf dem Hostcomputer „grundlegende Discovery“ aus.

Ergebnisse

Das varnishstat-CI wird erkannt, und in der Tabelle u_cmdb_ci_varnishstat wird ein Datensatz erstellt.

Die Varnish-Richtlinien und -Prüfungen können ausgeführt werden.

Wählen Sie die Richtlinien Azure aus, die für die Metriksammlung aktiviert werden sollen

Aktivieren Sie die mit dem Basissystem Agent Client Collector gelieferten Richtlinien Azure, damit die virtuellen Computer Azure Metriken erfassen können. Diese Metriken helfen Ihnen bei der Überwachung der Konfigurationselemente (CIs) in CMDB.

Vorbereitungen

- Bereiten Sie eine Instanz mit einer aktiven MID-Server - und Metrikbasis vor.
- Installieren Sie Agent Client Collector Framework und Agent Client Collector-Überwachung.
- Führen Sie Discovery im Cloud-Account Azure aus, um CMDB mit zu überwachenden CIs zu füllen.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Bereiten Sie den Proxy-Agent vor, der von der Richtlinie verwendet werden soll, und konfigurieren Sie ihn.
   Weitere Informationen zur Konfiguration eines Proxy-Agenten finden Sie unter Verwenden von Proxy-Agents in Agent Client Collector.
2. Weisen Sie die Anmeldeinformationen der Richtlinie Azure zu.

   a. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**.

   b. Wählen Sie die relevante Richtlinie aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einzelheiten zu den mit dem Basissystem verfügbaren Richtlinien finden Sie unter Azure Cloud-Metriken.

c. Wählen Sie die Registerkarte **Anmeldeinformationen**.

d. Wählen Sie im Feld **Anmeldeinformationsname** die Anmeldeinformationen aus, die für die Richtlinie aufgerufen werden sollen.
Um die verfügbaren Anmeldeinformationen anzuzeigen, wechseln Sie zur Seite „Anmeldeinformationen“, indem Sie zu navigieren **Alle** > **Discovery** > **Anmeldeinformationen**.

Stellen Sie sicher, dass Sie als **Typ = Azure-** Anmeldeinformationen auswählen. Wenn Sie Anmeldeinformationen erstellen müssen, wählen Sie **Neu** und anschließend Anmeldeinformationen **für Azure-Dienstprinzipal**.

e. Weisen Sie den **Anmeldeinformationen im Feld Alias** für Anmeldeinformationen einen Alias zu.

3. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Richtlinien** und wählen Sie die entsprechende zu aktivierende Richtlinie aus.
4. Wählen Sie das Anwendungsbereich-Symbol und vergewissern Sie sich, dass Sie sich im Bereich Agent Client Collector-Überwachung befinden, um die Richtlinie zu bearbeiten.
5. Aktivieren Sie die Richtlinie im Bearbeitungsmodus, indem Sie **In Sandbox bearbeiten**auswählen.
6. Aktivieren Sie den Proxy-Agent, der zur Ausführung der Prüfung verwendet werden soll.
   a. Wählen Sie die Registerkarte **Proxy-Einstellungen** aus.
   b. Wählen Sie **Einzel-Proxy-Agent** und anschließend den Proxy-Agent aus, der zur Ausführung der Prüfung im Feld **Proxy-Agent** verwendet werden soll.
7. Wählen Sie **Speichern**.
8. Veröffentlichen Sie die Richtlinie erneut, indem Sie **Erneut veröffentlichen**wählen.

Erstellen Sie Azure -Richtlinien für die Metrikensammlung

Erstellen Sie Ihre eigenen Richtlinien, damit Azure die Metriken für die Ressourcen sammeln kann, deren Richtlinien nicht im Basissystem enthalten sind. Die Prüfung Azure „ Metrikensammler“ übermittelt dem Agent die Metriken über die Azure Metriken-Batch-API.

Vorbereitungen

- Stellen Sie sicher, dass die Configuration Items (CIs), für die Sie die Metriken erfassen möchten, in CMDBenthalten sind. CIs werden normalerweise während Discoverygefüllt.
- Stellen Sie sicher, dass die Eigenschaft *sn_agent.multi_ci_dev_mode* auf der Seite **„Systemeigenschaften** “ () auf **„true“** festgelegt ist.**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**) an.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Richtlinien**.
2. Wählen Sie **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie das Anwendungsbereich-Symbol und vergewissern Sie sich, dass Sie sich im Bereich Agent Client Collector-Überwachung befinden.
4. Geben Sie im Feld **Name** einen Namen für die Richtlinie ein.
5. Konfigurieren Sie einen Filter, der bestimmt, welche CIs von der Richtlinie überwacht werden sollen, indem Sie die Registerkarte **Überwachte CIs** und das **Kontrollkästchen Überwachter CI-Typ nach Filter** aktivieren, wie in der folgenden Tabelle beschrieben.

Filter für überwachte CIs

Option	Aktion
Überwachter CI-Typ	Wählen Sie den zu überwachenden CI-Typ aus. Der CI-Typ muss mit der Ressource übereinstimmen, die Sie in der JSON-Skriptdatei eingegeben haben, die die zu überwachenden Metriken enthält.
<Filter fields>	Konfigurieren Sie die Bedingungen, die erfüllt werden müssen, damit die Ressourcen im angegebenen überwachten CI-Typ überwacht werden. Stellen Sie sicher, dass Sie die folgenden Bedingungen festlegen: ◦ **Objekt-ID** =<name of the resource entered in the .json script file that contains the metrics to be monitored> ◦ **Status** = Verfügbar Der Status „Verfügbar“ gibt an, dass Ressourcen zur Überwachung verfügbar sein müssen.
Vorschau	Wählen Sie diese Option aus, um die Anzahl der Ressourcen anzuzeigen, die der angegebenen Bedingung entsprechen. Die Anzahl der übereinstimmenden Ergebnisse wird neben der Schaltfläche **Vorschau** angezeigt. Wählen Sie das Ergebnis aus, um alle CI-Datensätze anzuzeigen, die der Bedingung entsprechen.

6. Fügen Sie der Richtlinie den Scheck Azure Metriksammler hinzu.
   a. Suchen Sie auf der **Registerkarte** Überprüfungen in der Zelle **Verfügbar** nach der Überprüfung **Azure-Metriksammler**.
   b. Wählen Sie die Nach-rechts-Taste, um das Häkchen in die Zelle **Ausgewählt** zu verschieben.
7. Konfigurieren Sie einen Proxy-Server für den Zugriff auf die Azure -Metriken.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie auf der Registerkarte **Proxy-Einstellungen** die **Option Einzel-Proxy-Agent**aus.

b. Wählen Sie im Feld **Proxy-Agent** den Proxy-Agent aus, um die Richtlinie auszuführen und die Metriken Azure abzurufen.

8. Konfigurieren Sie die Anmeldeinformationen für die Richtlinie.

a. Wählen Sie die Registerkarte **Anmeldeinformationen**.

b. Wählen Sie im Feld **Anmeldeinformationsname** die **Option azure_metrics_collector**aus.

9. Wählen Sie **Speichern**.

10. Fügen Sie der Prüfinstanz sichere Parameter hinzu.

a. Wählen Sie im Abschnitt **„Instanzen überprüfen“** der Richtlinie die Prüfinstanz **„Azure Metrics Collector“** aus.

b. Wählen Sie auf der Registerkarte **Sichere Parameter** überprüfen die **Option Neu**aus.

c. Fügen Sie die Sicherheitsprüfungsparameter hinzu, die in der folgenden Tabelle beschrieben werden.

Sichere Überprüfungsparameter

Name	Bestellwert
CRED_TENANT_ID	1
CRED_client_id	2
CRED_secret_key	3

Stellen Sie sicher, dass für jeden Parameter das Kontrollkästchen **Aktiv** aktiviert ist.

d. Wählen Sie **Aktualisieren**.

11. Fügen Sie der Überprüfungsinstanz die `JSON` -Konfigurationsdatei hinzu.
Die Datei sendet die Liste der Ressourcen Azure an den Service Desk-Mitarbeiter.

a. Wählen Sie die Prüfinstanz Azure Metrikensammler aus.

b. Wählen Sie die Unterregisterkarte **Prüfparameter** aus.

c. Wählen Sie **Neu**.

d. Füllen Sie die Felder des Formulars aus.

Formular „Parameter überprüfen“.

Feld	Beschreibung
Name	Beschreibender Name für die `JSON`– Datei, die den Konfigurationsdateien der Instanz hinzugefügt werden soll (**Agent Client Collector** > **Konfigurationsdateien**) an.
Wert	Zeichenfolge, die den Namen der `JSON`–Datei angibt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Beispiel: `acc_azure_vm_metrics_config.json`
Kennzeichnung	Wert, den Sie eingeben (**-c**), um anzugeben, dass die Prüfung den Namen der Konfigurationsdatei abruft. Die Konfigurationsdatei enthält einen Namespace und eine Liste von Metriken. Der Wert muss den Namen der Datei angeben, die in die Liste der Konfigurationsdateien hochgeladen wurde (**Agent Client Collector** > **Konfigurationsdateien**), im `JSON` -Format. Beispiel: `acc_azure_vm_metrics_config.json`.

Stellen Sie sicher, dass die Checkboxen **Aktiv**, **Obligatorisch**und **Wert erforderlich sind**.

e. Wählen Sie **Absenden**.

12. Erstellen Sie eine `JSON`– Datei, die die Metriken angibt, die Ihre Richtlinie überwachen soll.

Im folgenden Beispiel wird eine `JSON`– Datei zum Abrufen von Metriken für Lastenausgleichsmodule angezeigt.

acc_azure_static_ms_lb_config.json

```
{
  "namespace": "Microsoft.Network/loadBalancers",
  "metrics": [
        "AllocatedSnatPorts",
        "ByteCount",
        "DipAvailability",
        "PacketCount",
        "SnatConnectionCount",
        "SYNCount",
        "UsedSnatPorts",
        "VipAvailability"
  ],
  "time_grain": "PT1M"
}
```

Fügen Sie die `JSON`– Datei der Liste der Konfigurationsdateien unter hinzu **Agent Client Collector** > **Konfigurationsdateien**.

13. Erstellen Sie eine JSON-Datei, um die Ressourcen anzugeben, die Ihre Richtlinie überwachen soll.

a. Wählen Sie auf der Registerkarte **Proxy-Einstellungen** die **Option Multi-CI-Modus**aus.

b. Kopieren Sie ein Skript aus einer der Cloud-Richtlinien Azure, die im Basissystem enthalten sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Cloud-Richtlinien, die zum Lieferumfang des -Basissystems gehören, sind unter Erstellen Sie Azure -Richtlinien für die Metrikensammlungbeschrieben.
- Das Skript befindet sich im Feld **Erstellungsskript für Konfigurationsdatei** auf der Registerkarte **Proxy-Einstellungen** der Richtlinie.

c. Fügen Sie das Skript in das Feld **Erstellungsskript für Konfigurationsdatei** Ihrer Richtlinie ein.

d. Konfigurieren Sie am Ende des Skripts die Parameter *resource_id*, *region*und *sys_id* mit den Werten des CI, das die Richtlinie überwachen soll.

14. Wählen Sie **Speichern**, und veröffentlichen Sie die Richtlinie, indem Sie **Veröffentlichen**wählen.

Ergebnisse

Die konfigurierte Richtlinie ruft die Ressourcen und ihre Metriken aus dem angegebenen CI Azure ab und sendet sie an den -Agent.

Monitoring Technology Dashboard verstehen

Mit Monitoring Technology Dashboard können Sie Serverressourcen für die von Ihnen ausgewählte Plattform überwachen. Mit dem -Dashboard können Sie die CIs und Server in Ihrem System mit dem höchsten Ressourcenverbrauch und den neuesten aktiven Warnungen identifizieren.

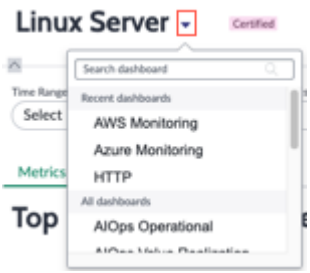
Sie können die Darstellung einzelner Widgets im Monitoring Technology Dashboardanpassen. Sie können beispielsweise die Datenparameter ändern, die für die Metrik „CPU-Auslastung (Linux)“ angezeigt werden, z. B. den Datumsbereich. Sie können die anwenderdefinierten Widgets einbeziehen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Dashboard für Überwachungstechnologie an.

Monitoring Technology Dashboard zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen während der letzten sechs Stunden und die 50 letzten aktiven Warnungen auf den Servern Ihres Betriebssystems.

Um die Anzeige von Monitoring Technology Dashboardzu aktivieren, vergewissern Sie sich, dass Sie Clotho-Version 23.1.0 installiert haben.

Um das Dashboard anzuzeigen, navigieren Sie zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** und wählen Sie das Betriebssystem aus, dessen Metriken Sie anzeigen möchten.

Wählen Sie den Pfeil neben dem Dashboard-Namen, um die Auswahl eines anderen anzuzeigenden Dashboards zu aktivieren:



Monitoring Technology Dashboard für Linux

Mit Linux Monitoring Technology Dashboardkönnen Sie den Zustand und die Leistung Ihrer Linux -Infrastruktur überwachen. Mit dem -Dashboard können Sie die CIs und Server in Ihrem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

System mit dem höchsten Ressourcenverbrauch und den neuesten aktiven Warnungen identifizieren.

Übersicht über das Dashboard

Monitoring Technology Dashboard zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden. Das Dashboard zeigt auch die 50 letzten aktiven Warnungen für die Server Ihres Betriebssystems an.

Um das Dashboard anzuzeigen, navigieren Sie zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** und wählen Sie **Linux Server**aus.

Verwenden des Dashboards für Überwachungstechnologie für Linux

Vor der Verwendung von Monitoring Technology Dashboard für Linux:

- Stellen Sie sicher, dass Sie im Überwachungsbereich Agent Client Collector in Ihrer Instanz ServiceNow arbeiten.
- Stellen Sie sicher, dass die Rollen „agent_client_collector_admin“ und „dashboard_admin“ aktiviert sind.
- Aktivieren Sie Metrikdaten auf dem MID-Server.
- Stellen Sie sicher, dass die Richtlinien **„Linux OS Events“** und **„Linux OS Metrics“** aktiviert sind.

  Durch Aktivieren dieser Richtlinien wird die Zuordnung von Metriken zu CI aktiviert.
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.
- Befolgen Sie nach dem Upgrade von einer früheren Version das Verfahren, das im Artikel ACC-M-Dashboard-Filter funktionieren bei einem Upgrade von Tokyo/Utah auf Vancouver nicht funktioniert [KB1438042] in der NOW Support-Knowledge Base beschrieben wird.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen. Wählen Sie die Registerkarte Warnungen, um die 50 letzten aktiven Warnungen für CIs anzuzeigen.

Sie können die Dashboard-Daten anhand der folgenden Filter filtern:

Dashboard-Filter

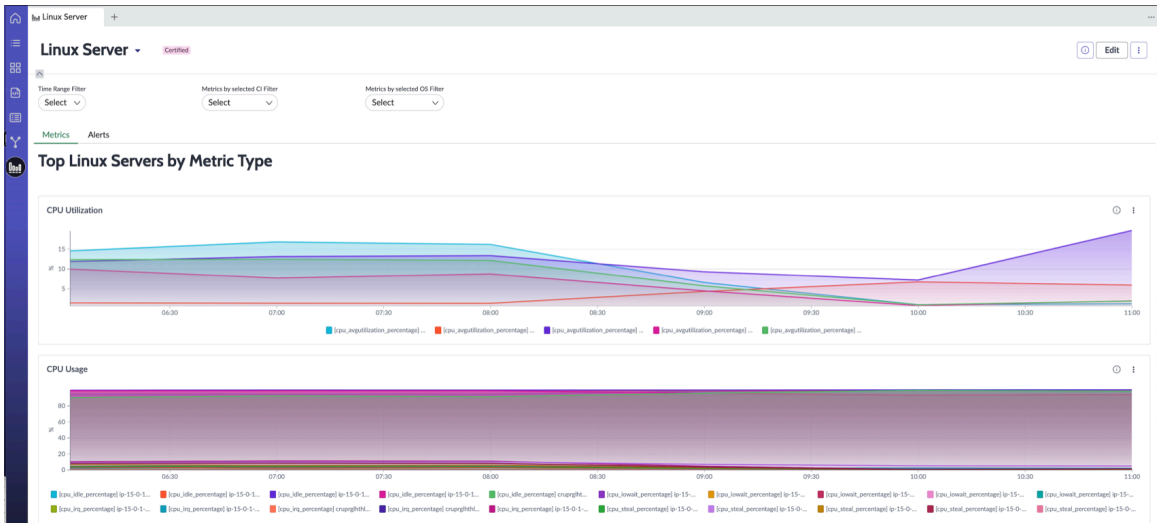
Filtername	Beschreibung
Filter für Zeitbereich	Der Zeitraum, für den Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem CI-Filter	Die CIs, für die Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem Betriebssystemfilter	Das Betriebssystem, für das Metrikdaten im Dashboard angezeigt werden sollen.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „Weitere Optionen“ (⋮) und **dann Gruppe ändern nach**auswählen. Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder BS-Version.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux Server-Dashboard



Auf der Unterregisterkarte Metriken werden die fünf leistungsstarken CIs und Server der letzten sechs Stunden gemäß den folgenden Metriken angezeigt.

- CPU-Auslastung
- Betriebszeit des Systems
- CPU-Auslastung
- Lastdurchschnitt
- Arbeitsspeicher
- Speicherverteilung
- Prozesse
- Netzwerkauslastung
- Vertauschen
- Festplattenauslastung

Sie können die Darstellung der einzelnen Widgets im Linux Monitoring Technology Dashboardanpassen. Sie können beispielsweise den Zeitrahmen ändern, für den die Warnungen angezeigt werden. Sie können auch anwenderdefinierte Widgets einbeziehen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Dashboard für Überwachungstechnologie an.

Monitoring Technology Dashboard für Windows

Mit Windows Monitoring Technology Dashboardkönnen Sie den Zustand und die Leistung Ihrer Windows -Infrastruktur überwachen. Mit dem -Dashboard können Sie die CIs und Server in Ihrem System mit dem höchsten Ressourcenverbrauch und den neuesten aktiven Warnungen identifizieren.

Übersicht über das Dashboard

Monitoring Technology Dashboard für Windows zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden. Das Dashboard zeigt auch die 50 letzten aktiven Warnungen für die Server Ihres Betriebssystems an.

Um das Dashboard anzuzeigen, navigieren Sie zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** und wählen Sie **Windows Server**aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden des Dashboards für Überwachungstechnologie für Windows

Vor der Verwendung von Monitoring Technology Dashboard für Windows:

- Stellen Sie sicher, dass Sie im Überwachungsbereich Agent Client Collector in Ihrer Instanz ServiceNow arbeiten.
- Stellen Sie sicher, dass die Rollen „agent_client_collector_admin“ und „dashboard_admin“ aktiviert sind.
- Aktivieren Sie Metrikdaten auf dem MID-Server.
- Stellen Sie sicher, dass die Richtlinien **„Windows-Betriebssystemereignisse“** und **„Windows-Betriebssystemmetriken“** aktiviert sind:

  Durch Aktivieren dieser Richtlinien wird die Zuordnung von Metriken zu CI aktiviert.
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.
- Befolgen Sie nach dem Upgrade von einer früheren Version das Verfahren, das im Artikel ACC-M-Dashboard-Filter funktionieren bei einem Upgrade von Tokyo/Utah auf Vancouver nicht funktioniert [KB1438042] in der NOW Support-Knowledge Base beschrieben wird.

Um das Dashboard anzuzeigen, navigieren Sie zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** und wählen Sie **Windows Server**aus.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen. Wählen Sie die Registerkarte Warnungen, um die 50 letzten aktiven Warnungen für CIs anzuzeigen.

Sie können die Dashboard-Daten anhand der folgenden Filter filtern:

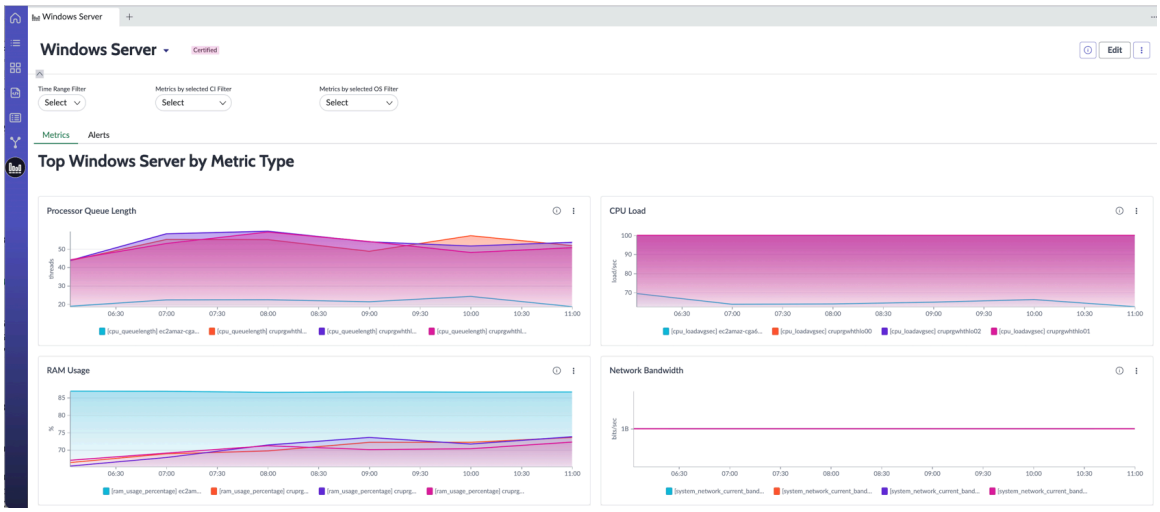
Dashboard-Filter

Filtername	Beschreibung
Filter für Zeitbereich	Der Zeitraum, für den Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem CI-Filter	Die CIs, für die Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem Betriebssystemfilter	Das Betriebssystem, für das Metrikdaten im Dashboard angezeigt werden sollen.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „Weitere Optionen“ (⋮) und **dann Gruppe ändern nach**auswählen. Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder BS-Version.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows Server-Dashboard



Auf der Unterregisterkarte Metriken werden die fünf leistungsstarken CIs und Server der letzten sechs Stunden gemäß den folgenden Metriken angezeigt.

- Länge der Prozessorwarteschlange
- CPU-Auslastung
- Betriebszeit des Systems
- CPU-Core
- RAM-Auslastung
- Netzwerkbandbreite
- Speicherverteilung
- Netzwerk-Flow
- Festplattenauslastung
- Datenträger – Lesen/Schreiben
- Datenträgerverteilung

Sie können die Darstellung der einzelnen Widgets im Windows Monitoring Technology Dashboardanpassen. Sie können beispielsweise den Zeitrahmen ändern, für den die Warnungen angezeigt werden. Sie können auch anwenderdefinierte Widgets einbeziehen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Dashboard für Überwachungstechnologie an.

Monitoring Technology Dashboard für HTTP

Mit HTTP Monitoring Technology Dashboard können Sie die Antwortzeit Ihrer `HTTP`– und `HTTPS` -URLs überwachen. Mithilfe des -Dashboards können Sie die URLs mit den höchsten Metrikauslesungen in der Infrastruktur Ihres Systems identifizieren und die neuesten aktiven Warnungen für diese URLs anzeigen.

Übersicht über das Dashboard

HTTP Monitoring Technology Dashboard zeigt die fünf URLs mit den höchsten Metrikauslesungen in den letzten sechs Stunden. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen für diese URLs an.

Um das Dashboard anzuzeigen, navigieren Sie zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** und wählen Sie **HTTP**aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwendung von Monitoring Technology Dashboard für HTTP

Vor der Verwendung von Monitoring Technology Dashboard für HTTP:

- Stellen Sie sicher, dass Sie im Überwachungsbereich Agent Client Collector in Ihrer Instanz ServiceNow arbeiten.
- Stellen Sie sicher, dass die Rollen „agent_client_collector_admin“ und „dashboard_admin“ aktiviert sind.
- Aktivieren Sie Metrikdaten auf dem MID-Server.
- Stellen Sie sicher, dass die Richtlinien **„HTTP-Einstiegspunkt-Ereignisse“** und **„HTTP-Einstiegspunktmetriken“** aktiviert sind.

  Durch Aktivieren dieser Richtlinien wird die Zuordnung von Metriken zu CI aktiviert.
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.
- Befolgen Sie nach dem Upgrade von einer früheren Version das Verfahren, das im Artikel ACC-M-Dashboard-Filter funktionieren bei einem Upgrade von Tokyo/Utah auf Vancouver nicht funktioniert [KB1438042] in der NOW Support-Knowledge Base beschrieben wird.

Azure Monitoring Technology Dashboard enthält die Registerkarten, die in der folgenden Tabelle aufgeführt sind.

HTTP-Registerkarten Monitoring Technology Dashboard

Tab-Taste	Beschreibung
Metriken	Zeigt die 5 besten Metriken an, die den URLs in Ihrem System zugeordnet sind.
Warnungen	Zeigt die 50 neuesten Warnungen an, die den URLs in Ihrem System zugeordnet sind. Warnungen helfen Ihnen, Ihr System zu korrigieren, indem sie Informationen zu problematischem Verhalten bereitstellen.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „Weitere Optionen“ (⋮) und **dann Gruppe ändern nach**auswählen. Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder BS-Version.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen.

Verwenden Sie den **Filter Zeitbereich,** um den Zeitbereich zu filtern, für den Metrikdaten im Dashboard angezeigt werden sollen.

Sie können die Darstellung der einzelnen Widgets auf HTTP Monitoring Technology Dashboardanpassen. Sie können beispielsweise die Datenparameter ändern, die für die Metrik „Antwortzeit“ angezeigt werden, z. B. den Zeitbereich, in dem die Antwortzeit angezeigt wird. Sie können auch die anwenderdefinierten Widgets einbeziehen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Dashboard für Überwachungstechnologie an.

Monitoring Technology Dashboard für Azure

Mit Azure Monitoring Technology Dashboardkönnen Sie den Zustand und die Leistung Ihrer Azure -Infrastruktur überwachen. Mithilfe des Dashboards können Sie die Configuration Items

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(CIs) und Server mit den höchsten Metrikauslesungen identifizieren und die neuesten aktiven Warnungen zu diesen CIs anzeigen.

Übersicht über das Dashboard

Azure Monitoring Technology Dashboard zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen in Ihrer Azure -Umgebung an. Basierend auf den Dashboard-Metriken möchten Sie möglicherweise die Größe Ihrer CIs und Server ändern, um die Leistung und Effizienz Ihres Systems zu verbessern.

Um das Dashboard anzuzeigen, navigieren Sie zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** und wählen Sie **Azure-Überwachung**aus.

Monitoring Technology Dashboard für Azureverwenden

Vor der Verwendung von Monitoring Technology Dashboard für Azure:

- Erstellen Sie Azure -Anmeldeinformationen. Einzelheiten zum Erstellen von Azure -Anmeldeinformationen finden Sie unter Anmeldeinformationen für Azure-Cloud erstellen.
- Erstellen Sie mit den im vorherigen Schritt erstellten Anmeldeinformationen einen Zeitplan Discovery. Einzelheiten zum Erstellen eines Discovery -Zeitplans finden Sie unter Erkennung von Azure-Clouds.
- Stellen Sie sicher, dass Sie im Überwachungsbereich Agent Client Collector in Ihrer Instanz ServiceNow arbeiten.
- Stellen Sie sicher, dass die Rollen „agent_client_collector_admin“ und „dashboard_admin“ aktiviert sind.
- Aktivieren Sie Metrikdaten auf dem MID-Server.
- Stellen Sie sicher, dass die Richtlinien **Azure-VM-Metriken**, **Azure Storage-Account-Metriken**, **Azure Load Balancer-Metriken**, **Azure Gateway-Metriken**und **Azure Redis-Cache-Metriken** aktiviert sind
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.

Azure Monitoring Technology Dashboard enthält die Registerkarten, die in der folgenden Tabelle aufgeführt sind.

Azure Monitoring Technology Dashboard Registerkarten

Tab-Taste	Beschreibung
Virtuelle Maschinen	Zeigt die Metrikdaten der virtuellen Computer in der Umgebung Azure an.
Speicherkonten	Zeigt die Metrikdaten aus den Speicherkonten in der Umgebung Azure an.
Load Balancer	Zeigt die Metrikdaten aus den Lastenausgleichsmodulen in der Umgebung Azure an.
Application Gateway	Zeigt die Metrikdaten aus dem Anwendungs-Gateway in der Umgebung Azure an.
Redis	Zeigt die Metrikdaten aus dem Redis-Cache in der Umgebung Azure an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen.

Sie können die Dashboard-Daten anhand der folgenden Filter filtern:

Dashboard-Filter

Filtername	Beschreibung
Filter für Zeitbereich	Der Zeitraum, für den Metrikdaten im Dashboard angezeigt werden sollen.
Metriken nach ausgewähltem CI-Filter	Die CIs, für die Metrikdaten im Dashboard angezeigt werden sollen.

Sie können die Darstellung der einzelnen Widgets im Azure Monitoring Technology Dashboardanpassen. Sie können beispielsweise ändern, wann die CPU-Auslastung auf virtuellen Computern angezeigt wird. Sie können auch die anwenderdefinierten Widgets einbeziehen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Dashboard für Überwachungstechnologie an.

Monitoring Technology Dashboard für AWS

Mit AWS Monitoring Technology Dashboardkönnen Sie den Zustand und die Leistung Ihrer AWS -Infrastruktur überwachen. Mithilfe des -Dashboards können Sie die Configuration Items (CIs) und Server mit den höchsten Metrikauslesungen identifizieren und die neuesten aktiven Warnungen zu diesen CIs und Servern anzeigen.

Übersicht über das Dashboard

AWS Monitoring Technology Dashboard zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen in Ihrer AWS -Umgebung an.

Um das Dashboard anzuzeigen, navigieren Sie zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** und wählen Sie **AWS Monitoring (Überwachung)**aus.

Monitoring Technology Dashboard für AWSverwenden

Vor der Verwendung von Monitoring Technology Dashboard für AWS:

- Erstellen Sie AWS -Anmeldeinformationen. Einzelheiten zum Erstellen von AWS -Anmeldeinformationen finden Sie unter AWS-Servicekonten einrichten.
- Erstellen Sie mit den im vorherigen Schritt erstellten Anmeldeinformationen einen Zeitplan Discovery. Einzelheiten zum Erstellen eines Discovery -Zeitplans finden Sie unter Amazon AWS Cloud Discovery.
- Stellen Sie sicher, dass Sie im Überwachungsbereich Agent Client Collector in Ihrer Instanz ServiceNow arbeiten.
- Stellen Sie sicher, dass die Rollen „agent_client_collector_admin“ und „dashboard_admin“ aktiviert sind.
- Aktivieren Sie Metrikdaten auf dem MID-Server.
- Stellen Sie sicher, dass die Richtlinien **AWS-Metriken**, **AWS EC2-Metriken**und **AWS DynamoDB-Metriken** aktiviert sind.

  Durch Aktivieren dieser Richtlinien wird die Zuordnung von Metriken zu CI aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.
- Befolgen Sie nach dem Upgrade von einer früheren Version das Verfahren, das im Artikel ACC-M-Dashboard-Filter funktionieren bei einem Upgrade von Tokyo/Utah auf Vancouver nicht funktioniert [KB1438042] in der NOW Support-Knowledge Base beschrieben wird.

AWS Monitoring Technology Dashboard enthält die Registerkarten, die in der folgenden Tabelle aufgeführt sind.

AWS Monitoring Technology Dashboard Registerkarten

Tab-Taste	Beschreibung
EC2	Zeigt die Metrikdaten von EC2 (virtuelle Maschinen) in der Umgebung AWS an.
EC2-Warnungen	Zeigt die aktiven EC2-Warnungen (virtueller Computer) in der Umgebung AWS an.
EBS-Inklusionsmodule	Zeigt die Metrikdaten aus dem EBS (Speichervolume) in der Umgebung AWS an.
S3	Zeigt die Metrikdaten aus S3 (Cloud-Objektspeicher) in der Umgebung AWS an.
RDS	Zeigt die Metrikdaten aus dem RDS (Cloud Database) in der Umgebung AWS an.
ELB	Zeigt die Metrikdaten aus dem ELB (Cloud-Lastenausgleich) in der Umgebung AWS an.
Dynamo-DB	Zeigt die Metrikdaten aus Dynamo DB (Cloud-Datenbank) in der Umgebung AWS an.
ECS-Cluster	Zeigt die Metrikdaten aus dem ECS-Cluster in der Umgebung AWS an.
ECS-Service	Zeigt die Metrikdaten aus dem ECS-Service in der Umgebung AWS an.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „Weitere Optionen“ (⋮) und **dann Gruppe ändern nach**auswählen. Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder BS-Version.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen. Wählen Sie die Registerkarte **Warnungen**, um die 50 neuesten aktiven Warnungen in Ihrer Umgebung anzuzeigen. Warnungen helfen Ihnen, Ihr System zu korrigieren, indem sie Informationen zu problematischem Verhalten bereitstellen.

Verwenden Sie den **Filter Zeitbereich,** um den Zeitbereich zu filtern, für den Metrikdaten im Dashboard angezeigt werden sollen.

Verwenden Sie den **Filter Metriken nach ausgewähltem CI,** um die CIs auszuwählen, für die Sie Metriken anzeigen möchten.

Sie können die Darstellung der einzelnen Widgets im AWS Monitoring Technology Dashboardanpassen. Sie können beispielsweise die Zeit ändern, zu der die EC2-Metriken angezeigt werden. Sie können auch die anwenderdefinierten Widgets einbeziehen, wenn Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Dashboard für Überwachungstechnologie an.

Monitoring Technology Dashboard für GCP

Mit GCP Monitoring Technology Dashboardkönnen Sie den Zustand und die Leistung Ihrer GCP -Infrastruktur überwachen. Mithilfe des -Dashboards können Sie die Configuration Items (CIs) und Server mit den höchsten Metrikauslesungen identifizieren und die neuesten aktiven Warnungen zu diesen CIs und Servern anzeigen.

Übersicht über das Dashboard

GCP Monitoring Technology Dashboard zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen in Ihrer GCP -Umgebung an.

Um das Dashboard anzuzeigen, navigieren Sie zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** und wählen Sie **GCP Monitoring**aus.

Monitoring Technology Dashboard für GCPverwenden

Vor der Verwendung von Monitoring Technology Dashboard für GCP:

- Erstellen Sie GCP -Anmeldeinformationen, und verwenden Sie sie, um einen Discovery -Zeitplan zu erstellen. Einzelheiten zum Erstellen von GCP -Anmeldeinformationen finden Sie unter Erkennung von Google Cloud Platform.
- Erstellen Sie mit den im vorherigen Schritt erstellten Anmeldeinformationen einen Zeitplan Discovery. Einzelheiten zum Erstellen eines Discovery -Zeitplans finden Sie unter Erkennung von Google Cloud Platform.
- Stellen Sie sicher, dass Sie im Überwachungsbereich Agent Client Collector in Ihrer Instanz ServiceNow arbeiten.
- Stellen Sie sicher, dass die Rollen „agent_client_collector_admin“ und „dashboard_admin“ aktiviert sind.
- Aktivieren Sie Metrikdaten auf dem MID-Server.
- Stellen Sie sicher, dass die Richtlinie **„GCP GCE Metrics“** aktiviert ist.

  Durch Aktivieren dieser Richtlinie wird die Zuordnung von Metriken zu CI aktiviert.
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.19.0.10 oder höher aktiviert ist.
- Befolgen Sie nach dem Upgrade von einer früheren Version das Verfahren, das im Artikel ACC-M-Dashboard-Filter funktionieren bei einem Upgrade von Tokyo/Utah auf Vancouver nicht funktioniert [KB1438042] in der NOW Support-Knowledge Base beschrieben wird.

GCP Monitoring Technology Dashboard enthält die in der folgenden Tabelle aufgeführten Registerkarten.

Registerkarten des GCP-Überwachungs-Dashboards

Tab-Taste	Beschreibung
GCP	Zeigt Diagramme der 14 Betriebssystemressourcen mit der besten Leistung an, z. B. CPU, Arbeitsspeicher, Datenträgervorgänge und Netzwerk.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarten des GCP-Überwachungs-Dashboards (Fortsetzung)

Tab-Taste	Beschreibung
Warnungen	Zeigt die 50 neuesten Warnungen an, die den URLs in Ihrem System zugeordnet sind. Warnungen helfen Ihnen, Ihr System zu korrigieren, indem sie Informationen zu problematischem Verhalten bereitstellen.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „Weitere Optionen“ (⋮) und **dann Gruppe ändern nach**auswählen. Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder BS-Version.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen.

Verwenden Sie den **Filter Zeitbereich,** um den Zeitbereich zu filtern, für den Metrikdaten im Dashboard angezeigt werden sollen.

Verwenden Sie den **Filter Metriken nach ausgewähltem CI,** um die CIs auszuwählen, für die Sie Metriken anzeigen möchten.

Sie können die Darstellung der einzelnen Widgets im GCP Monitoring Technology Dashboardanpassen. Sie können beispielsweise den Zeitrahmen ändern, für den die Warnungen angezeigt werden. Sie können auch anwenderdefinierte Widgets einbeziehen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Dashboard für Überwachungstechnologie an.

Monitoring Technology Dashboard für VMware vSphere

Mit VMware vSphere Monitoring Technology Dashboardkönnen Sie den Zustand und die Leistung Ihrer VMware vSphere -Infrastruktur überwachen. Mithilfe des -Dashboards können Sie die Configuration Items (CIs) und Server mit den höchsten Metrikauslesungen identifizieren und die neuesten aktiven Warnungen zu diesen CIs und Servern anzeigen.

Übersicht über das Dashboard

VMware vSphere Monitoring Technology Dashboard zeigt die fünf CIs und Server mit den höchsten Metrikauslesungen in den letzten sechs Stunden. Das Dashboard zeigt auch die 50 neuesten aktiven Warnungen in Ihrer VMware vSphere -Umgebung an.

Um das Dashboard anzuzeigen, navigieren Sie zu **Alle** > **AIOps – Dashboards** > **Überwachungstechnologie-Dashboards** und wählen Sie **VMware vSphere Monitoring**aus.

Monitoring Technology Dashboard für VMware vSphereverwenden

Vor der Verwendung von Monitoring Technology Dashboard für VMware vSphere:

- Erstellen Sie VMware vSphere -Anmeldeinformationen, und verwenden Sie sie, um einen Discovery -Zeitplan zu erstellen. Einzelheiten zum Erstellen von VMware vSphere -Anmeldeinformationen finden Sie unter Erkennung von VMware-Clouds.
- Erstellen Sie mit den im vorherigen Schritt erstellten Anmeldeinformationen einen Zeitplan Discovery. Einzelheiten zum Erstellen eines Discovery -Zeitplans finden Sie unter VMware-Erkennung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass Sie im Überwachungsbereich Agent Client Collector in Ihrer Instanz ServiceNow arbeiten.
- Stellen Sie sicher, dass die Rollen „agent_client_collector_admin“ und „dashboard_admin“ aktiviert sind.
- Aktivieren Sie Metrikdaten auf dem MID-Server.
- Stellen Sie sicher, dass die Richtlinien **„VSphere Datacenter-Metriken“**, **„VSphere Datastore Metrics“**, **„VSphere ESX Server-Metriken“** und **„VSphere VirtualMachine-Metriken“** aktiviert sind.

  Durch Aktivieren dieser Richtlinien wird die Zuordnung von Metriken zu CI aktiviert.
- Stellen Sie sicher, dass das Clotho-Plugin Version 1.1.0 oder höher aktiviert ist.
- Befolgen Sie nach dem Upgrade von einer früheren Version das Verfahren, das im Artikel ACC-M-Dashboard-Filter funktionieren bei einem Upgrade von Tokyo/Utah auf Vancouver nicht funktioniert [KB1438042] in der NOW Support-Knowledge Base beschrieben wird.

VMware vSphere Monitoring Technology Dashboard enthält die in der folgenden Tabelle aufgeführten Registerkarten.

VMware vSphere Registerkarten für das Überwachungs-Dashboard

Tab-Taste	Beschreibung
VirtualMachine	Zeigt Diagramme der wichtigsten VMware vSphere VMs nach Metriktyp an.
ESX-Server	Zeigt Diagramme der VMware vSphere wichtigsten ESX-Server nach Metriktyp an.
Rechenzentrum	Zeigt Diagramme der Top-Rechenzentren VMware vSphere nach Metriktyp an.
Datenspeicher	Zeigt Diagramme der Top-Datenspeicher VMware vSphere nach Metriktyp an.
Warnungen	Zeigt die 50 neuesten Warnungen an, die den URLs in Ihrem System zugeordnet sind. Warnungen helfen Ihnen, Ihr System zu korrigieren, indem sie Informationen zu problematischem Verhalten bereitstellen.

Auf der rechten Seite von Widgets, die eine einzelne Metrik anzeigen, können Sie das Symbol „Weitere Optionen“ (⋮) und **dann Gruppe ändern nach**auswählen. Wählen Sie die Kategorie aus, nach der Sie die Metrik anzeigen möchten: Hostname, Klasse, Betriebssystem oder BS-Version.

Zeigen Sie auf das entsprechende Widget, um einen bestimmten Datenpunkt und alle zugehörigen Details in einem Popup-Fenster anzuzeigen.

Sie können die Dashboard-Daten anhand der folgenden Filter filtern:

Dashboard-Filter

Filter für Zeitbereich	Der Zeitraum, für den Metrikdaten im Dashboard angezeigt werden sollen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dashboard-Filter (Fortsetzung)

Metriken nach ausgewähltem CI-Filter	Die CIs, für die Metrikdaten im Dashboard angezeigt werden sollen.

Sie können die Darstellung der einzelnen Widgets im VMware vSphere Monitoring Technology Dashboardanpassen. Sie können beispielsweise den Zeitrahmen ändern, für den die Warnungen angezeigt werden. Sie können auch anwenderdefinierte Widgets einbeziehen, wenn Sie ein anwenderdefiniertes Dashboard erstellen. Weitere Informationen finden Sie unter Passen Sie das Dashboard für Überwachungstechnologie an.

Passen Sie das Dashboard für Überwachungstechnologie an

CPassen Sie die Widgets des Überwachungstechnologie-Dashboards in der Datenvisualisierungsbibliothek so an, dass Ihr Dashboard Informationen genau so anzeigt, wie Sie sie sehen möchten.

Vorbereitungen

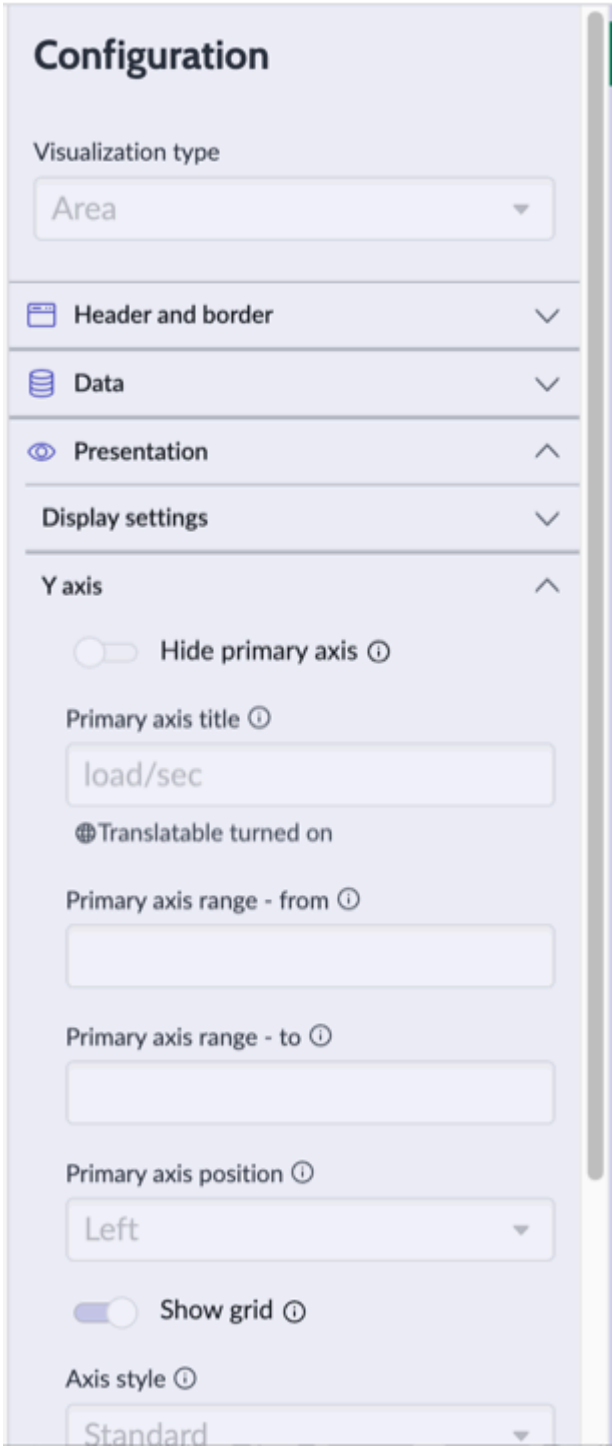
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren Sie zum BS-Dashboard, dessen Widgets Sie anpassen möchten.
   - Um auf das Windows Server-Dashboard zuzugreifen, navigieren Sie zu **Alle** > **AIOps** > **Dashboard für Überwachungstechnologie** > **Windows-Server**.
   - Um auf das Linux-Server-Dashboard zuzugreifen, navigieren Sie zu **Alle** > **AIOps** > **Dashboard für Überwachungstechnologie** > **Linux-Server**.
2. Auswahlvorgang **Analytics Center** > **Datenvisualisierungen**.
3. Zeigen Sie alle verfügbaren Widgets an, indem Sie die Registerkarte **Alle** auswählen.
4. Wählen Sie das Widget aus, das Sie ändern möchten.
5. Wählen Sie das Symbol ( ) und anschließend **Duplikat**aus.
6. Geben Sie im Feld **Neuer Name** des Dialogfelds einen Namen für Ihr dupliziertes Widget ein, und wählen Sie **Duplizieren**aus.
7. Erweitern Sie auf der Registerkarte **Konfiguration** auf der rechten Seite des Widgets die relevanten Optionen, und passen Sie die Informationen für das Widget an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsregisterkarte



Einzelheiten zum Arbeiten mit Datenvisualisierungen finden Sie unter Datenvisualisierungen im Analytics Center Datenvisualisierungen im Analytics Center .

8. Wählen Sie **Speichern und schließen aus**.

Ergebnisse
Ihre anwenderdefinierten Widgets werden in der Datenvisualisierungsbibliothek gespeichert und können zum Konfigurieren eines anwenderdefinierten Dashboards verwendet werden (siehe Dashboard mit dem Inline-Editor erstellen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden von Proxy-Agents in Agent Client Collector

Sie können einen Proxy-Agent verwenden, um den Zustand und die Leistung Ihrer Konfigurationselemente (CIs) zu überwachen, selbst wenn sich der Agent in der Cloud oder an einem anderen Ort außerhalb Ihres Host-Servers befindet.

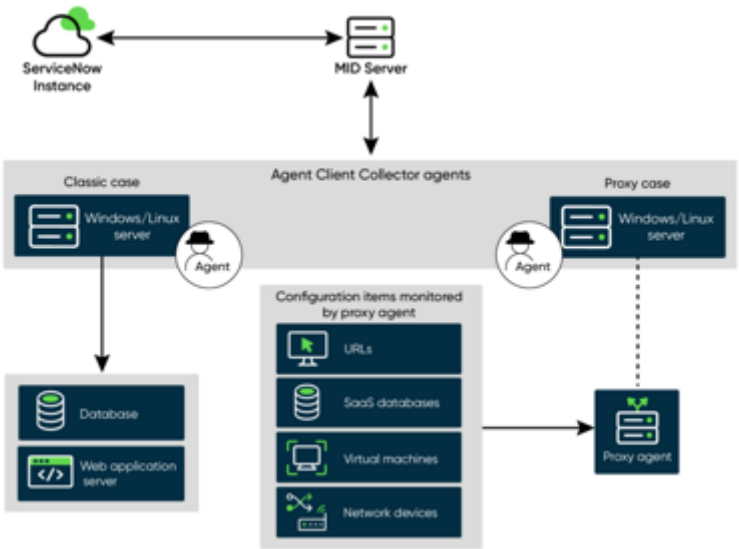
Proxy-Agents dienen zur Überwachung von:

- URLs (um sicherzustellen, dass die URLs verfügbar und zugänglich sind)
- Services, die keinen Hostserver haben
- Geschlossene Services, für die Sie keinen Agent konfigurieren können
- Externe Datenbanken in der Cloud

Ein Service Desk-Mitarbeiter kann mehrere Entitäten und ihre CIs überwachen.

Das folgende Diagramm zeigt die Verbindung zwischen einer Instanz ServiceNow, den Agents MID-Serverund Agent Client Collector sowie Proxy-Agents, die CIs überwachen, die sich außerhalb des Agents befinden.

Proxy-Agent-Konfiguration



Sie können den Proxy-Agent so konfigurieren, dass bei der Überwachung externer Entitäten eine anwenderdefinierte Prüfung durchgeführt wird. Informationen zum Erstellen anwenderdefinierter Schecks finden Sie unter Prüfungen erstellen und bearbeiten.

Sie können einen Cluster von Proxy-Agents auf mehreren Proxy-Servern erstellen, um die Services zu überwachen, die sich außerhalb des Host-Servers befinden. Informationen zum Erstellen eines Proxy-Agent-Clusters finden Sie unter Erstellen Sie ein Proxy-Agent-Cluster.

Zugehörige Informationen

Prüfungen und Richtlinien

Agent Client Collector-Überwachung – Standardprüfungen und Richtlinien

Agent auf einem Proxy-Server konfigurieren

Konfigurieren Sie Agent Client Collector auf einem Proxy-Server, wenn Sie Services außerhalb des Hostservers überwachen, z. B. URLs oder externe Datenbanken in der Cloud.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Proxy-Agents sollten dedizierte Agents sein, da die Ausführung anderer Apps auf einem Proxy-Agent wahrscheinlich zu einer Verschlechterung der Leistung führt.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents** > **Richtlinien**.
2. Wählen Sie die Richtlinie aus, die die Prüfungen enthält, die Sie auf einem Proxy-Server ausführen möchten.
   Sie müssen einen Proxy-Server für Prüfungen und Richtlinien konfigurieren, mit denen externe Services überwacht werden. Einzelheiten über diese Prüfungen und Richtlinien finden Sie unter Agent Client Collector-Überwachung – Standardprüfungen und Richtlinien.
3. Wählen Sie die Registerkarte **Proxy-Einstellungen** aus.
4. Wählen Sie aus den folgenden Feldern aus.

Feld	Beschreibung
Einzelner Proxy-Agent	Bei Auswahl dieser Option wird das Feld **Proxy Agent** (Proxy-Agent) angezeigt, in dem Sie einen einzelnen Proxy-Agent auswählen.
Mehrere Proxy-Agents nach Cluster	Wählen Sie diese Option aus, um einer Gruppe von Proxy-Agents die Überwachung der Richtlinien-CIs zu ermöglichen. Wenn Sie dieses Kontrollkästchen aktivieren, wird das Feld **Name des Agent-Clusters** angezeigt.
Name des Agent-Clusters	Wählen Sie einen Agent-Cluster aus, um die Richtlinien-CIs zu überwachen.
Mehrere Proxy-Agents via Filter	Wählen Sie dieses Feld aus, um mehrere Proxy-Agents aus der Agent-Liste zu filtern. Wenn Sie diese Option auswählen, werden von allen Proxy-Agents dieselben Services überwacht. Beispielsweise empfiehlt es sich, diese Option für mehrere Proxy-Server an verschiedenen geografischen Standorten zu verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ◦ Dieses Feld wird nur angezeigt, wenn der **Filter „Multi-Proxy-Agent ausblenden nach“, wenn seine nicht ausgewählte** Eigenschaft (*sys_ui_policy*) auf **active=false**festgelegt ist. ◦ Dieses Feld wird nur für vorhandene Richtlinien angezeigt, bei denen diese Option zuvor ausgewählt wurde. Wenn Sie den Filter in einer vorhandenen Richtlinie entfernen, wird die Option ausgeblendet.
Mehrere Proxy-Agents via Skript	Wählen Sie dieses Feld aus, um ein Java-Skript für die Auswahl von Proxy-Agents zu konfigurieren. Wenn Sie diese Option auswählen, können Sie Services verschiedenen Proxy-Agents zuweisen. Dies kann als eine Form des Lastenausgleichs dienen.
Prüfungen für alle Proxy-Agents ausführen (kein Lastenausgleich)	Deaktivieren Sie diese Option, um einen Lastenausgleich für die ausgewählten Multi-Proxy-Agents herzustellen, die die übereinstimmenden CIs auf der Registerkarte **„Überwachte CIs“** der Richtlinie überwachen. Wählen Sie diese Option für jeden Agent aus, um alle übereinstimmenden CIs auf der Registerkarte **Überwachte CIs** der Richtlinie zu überwachen. Wenn Sie beispielsweise fünf Agents in einem Cluster haben oder fünf Agents, die die Filter-/Skriptoption und 10 übereinstimmende CIs in der Richtlinie verwenden, überwacht jeder Agent zwei CIs, wenn Sie diese Option deaktivieren. Wenn Sie diese Option auswählen, überwacht jeder Agent alle 10 übereinstimmenden CIs in der Richtlinie. Für vorhandene oder aktive Richtlinien ist diese Option standardmäßig aktiviert. Für neue und inaktive Richtlinien ist diese Option standardmäßig deaktiviert. Wählen Sie diese Option nur aus, wenn Sie einen externen Endpunkt haben, für den Sie messen möchten, wie schnell

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	von verschiedenen Standorten auf ihn zugegriffen wird.

5. Wählen Sie **Aktivieren**.

Erstellen Sie ein Proxy-Agent-Cluster

Erstellen Sie ein Agent-Cluster auf mehreren Proxy-Servern, um Services außerhalb des Host-Servers zu überwachen. Durch das Erstellen eines Clusters von Agents können Sie dieses Cluster mehreren Richtlinien zuweisen, anstatt die Agents jeder Richtlinie einzeln zuweisen zu müssen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Ein Proxy-Agent-Cluster überwacht die CIs, die dem auf der Registerkarte **Überwachte CIs** der Richtlinie angegebenen Filter entsprechen.

Ein Proxy-Agent-Cluster muss mindestens einen Agent enthalten. Alle Agents des Clusters überwachen die in der zugewiesenen Richtlinie angegebenen CIs. Zum Aktivieren der Proxy-Clusterüberwachung ist keine spezielle Konfiguration auf Richtlinienebene erforderlich.

Der standardmäßige CPU-Schwellenwert bei der Arbeit mit Proxy-Agent-Clustern beträgt 80 %. Sie können diesen Wert in der Eigenschaft *proxy_cpu_percentage_limit* ändern.

Prozedur
1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Proxy-Agent-Cluster**.
2. Wählen Sie **Neu**.
3. Geben Sie im Feld **Name** einen beschreibenden Namen für den Cluster ein.
4. Fügen Sie dem Cluster einen Agent hinzu.
   a. Suchen Sie im Abschnitt **„Service Desk-Mitarbeiter im Cluster“** nach der Spalte **Agent**, und wählen Sie **Neue Zeile einfügen aus**.
   b. Wählen Sie das Suchsymbol ( ) und anschließend einen Agent aus, der dem Cluster hinzugefügt werden soll.
   c. Wählen Sie das Häkchen-Symbol ( ), um den Agent dem Cluster hinzuzufügen. Wiederholen Sie diesen Schritt für jeden Agent, den Sie dem Cluster hinzufügen möchten.
5. Wählen Sie **Absenden**.

Ergebnisse
Die Seite **„Proxy Agent-Cluster“** wird angezeigt und zeigt den dem Cluster hinzugefügten Agent an.

Nächste Maßnahme
Wählen Sie diesen Proxy-Cluster aus, um CIs zu überwachen, die in einer Agent-Richtlinie angegeben sind. Details finden Sie unter Agent auf einem Proxy-Server konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weisen Sie einer Richtlinie einen Proxy-Agent-Cluster zu

Weisen Sie einer Richtlinie einen Proxy-Agent-Cluster zu, wenn Sie Services außerhalb des Hostservers überwachen, z. B. URLs oder externe Datenbanken in der Cloud. Die Agents im Cluster überwachen alle CIs der Richtlinie.

Vorbereitungen

Stellen Sie sicher, dass Sie eine Richtlinie haben, die die Prüfungen zur Überwachung externer Services enthält. Einzelheiten über diese Prüfungen und Richtlinien finden Sie unter Agent Client Collector-Überwachung – Standardprüfungen und Richtlinien.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Auf einem bestimmten Proxy-Agent sollte nur eine App ausgeführt werden, da das Ausführen mehrerer Apps wahrscheinlich zu einer Verschlechterung der Leistung führt.

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Agents** > **Richtlinien**.
2. Wählen Sie die Richtlinie aus, die die Prüfungen enthält, die Sie auf einem Proxy-Server ausführen möchten.
3. Wählen Sie die Registerkarte **Proxy-Einstellungen** aus.
4. Wählen Sie **In Sandbox bearbeiten** aus, um das Ändern von Feldern im Formular zu aktivieren.
5. Geben Sie an, ob Sie einen einzelnen Proxy-Agent oder einen Proxy-Agent-Cluster zur Überwachung der Richtlinien-CIs zuweisen.
   - Weisen Sie einen einzelnen Proxy-Agent zu, indem Sie **Einzelner Proxy-Agent** und dann einen Agent auswählen.
   - Aktivieren Sie einen Proxy-Agent-Cluster, indem Sie **Mehrere Proxy-Agents nach Cluster**auswählen. Geben Sie den Namen des Clusters in das angezeigte Feld ein.
6. Bestimmt, ob mehrere Proxy-Agents über einen Filter oder ein Skript aus der Liste der Agents ausgewählt werden sollen.
   - Um Agents über einen Filter auszuwählen, konfigurieren Sie einen Filter oder behalten oder ändern Sie einen vorhandenen Filter, wenn die Option **Mehrere Proxy-Agents nach Filter** auswählen.

     Hinweis:

     - Dieses Feld wird nur angezeigt, wenn der **Filter „Multi-Proxy-Agent ausblenden nach“ , wenn seine nicht ausgewählte** Eigenschaft (*sys_ui_policy*) auf **active=false**festgelegt wurde.
     - Wenn Sie den Filter in einer vorhandenen Richtlinie entfernen, wird die Option ausgeblendet.

   - So wählen Sie Agents über ein Skript aus:
     a. Wählen Sie **In Sandbox bearbeiten**.
     b. Löschen Sie alle ausgewählten Proxy-Optionen auf der Registerkarte **„Proxy-Einstellungen“**.
     c. Wählen Sie **Mehrere Proxy-Agents nach Skript**.
     d. Geben Sie im Feld **Proxy-Skript** ein Skript ein, um verschiedenen Proxy-Agents Services im Rahmen des Lastenausgleichs zuzuweisen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Legen Sie fest, ob ein Lastenausgleich für die ausgewählten Multi-Proxy-Agents erfolgen soll, die die übereinstimmenden CIs auf der Registerkarte **Überwachte CIs** der Richtlinie überwachen, oder ob jeder Agent die übereinstimmenden CIs überwachen soll.
   - Um einen Lastenausgleich für die ausgewählten Agents mit mehreren Proxys zu erreichen, die die übereinstimmenden CIs überwachen, deaktivieren Sie die Option **Prüfungen für alle Proxy-Agents ausführen (kein Lastenausgleich)**.

     Wenn Sie beispielsweise fünf Agents in einem Cluster haben oder fünf Agents, die die Filter-/Skriptoption und 10 übereinstimmende CIs in der Richtlinie verwenden, würde jeder Agent zwei CIs überwachen.

     Sie können den Lastenausgleich auch zu einem späteren Zeitpunkt aktivieren, wie in Lastenausgleich zwischen Proxy-Agents in einem Cluster aktivierenbeschrieben.

   - Damit jeder Agent alle übereinstimmenden CIs überwacht, wählen Sie die Option **Prüfungen für alle Proxy-Agents ausführen (kein Lastenausgleich)**.

     Wenn in der Richtlinie 10 übereinstimmende CIs vorhanden sind, überwacht jeder Agent alle 10 CIs. Beispielsweise können Sie diese Option für mehrere Proxy-Server an verschiedenen geografischen Standorten verwenden.

     Wenn ein Agent nicht ordnungsgemäß funktioniert, werden die überwachten CIs an einen anderen Agent neu verteilt.

   Hinweis: Für vorhandene oder aktive Richtlinien ist die Option **Prüfungen für alle Proxy-Agents ausführen (kein Lastenausgleich)** standardmäßig aktiviert. Für neue und inaktive Richtlinien ist diese Option standardmäßig deaktiviert.

8. Wählen Sie **Aktivieren**.

Lastenausgleich zwischen Proxy-Agents in einem Cluster aktivieren

Aktivieren Sie den Lastenausgleich zwischen Proxy-Agents in einem Cluster, sodass überwachte CIs an einen anderen Agent neu verteilt werden, wenn ein Agent nicht ordnungsgemäß funktioniert. Nach Aktivierung des Lastenausgleichs können Sie vdie von den einzelnen Proxy-Agents überwachten CIs in einer Richtlinieanzeigen.

Vorbereitungen

Stellen Sie sicher, dass Sie ein Upgrade auf Tokyo Patch 1 oder San Diego Patch 7 durchgeführt haben.

Erforderliche Rolle: agent_client_collector_user

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Konfiguration** > **Richtlinien**.
2. Wählen Sie die Richtlinie mit den CIs aus, die die Proxy-Agents überwachen sollen.
3. Wählen Sie die Registerkarte **Proxy-Einstellungen** aus.
4. Aktivieren Sie den Lastenausgleich für die Proxy-Agents, indem Sie das **Kontrollkästchen Prüfungen für alle Proxy-Agents ausführen (kein Lastenausgleich)** deaktivieren.
   Für die Proxy-Agents, die die CIs überwachen, ist ein Lastenausgleich aktiviert. Wenn Sie beispielsweise fünf Mitarbeiter und zehn übereinstimmende CIs in der Richtlinie haben, überwacht jeder Mitarbeiter zwei CIs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Abschnitt „ **Zugehörige Links“Verteilung der CIs des Proxy-Agents anzeigen aus**.
   In einem Popup-Fenster wird die Verteilung der überwachten CIs auf die Agents innerhalb der Richtlinie angezeigt.

Agent Client Collector-Überwachung – Referenz

Referenzthemen enthalten zusätzliche Informationen zu Prüfungen und Richtlinien Agent Client Collector-Überwachung von .

Footprint von Agent Client Collector Monitoring

In der folgenden Tabelle wird der Ressourcenverbrauch von Agent Client Collector beschrieben.

Parameter	Linux	Windows
Machine spec (Computerspezifikation)	Cent OS 8, 4 CPU-Kerne, 8 GB Arbeitsspeicher	Windows Server 2019, 2 CPUs, 4 GB Arbeitsspeicher
Network - (Agent > MID)	10,64 KB/s	350-400 Byte/s
Network - (MID > Agent)	48 Byte/s	5-15 Byte/s
Average CPU Utilization (Durchschnittliche CPU-Auslastung)	~1%	~3.89%
Max CPU per check (Max. CPU pro Prüfung)	10 bis 15 %	15 bis 20 %
Memory overhead (avg) (Arbeitsspeicher-Overhead (Durchschnitt))	~ 13,88 MB	~ 31,15 MB

Agent Client Collector-Überwachung – Standardprüfungen und Richtlinien

Agent Client Collector-Überwachung bietet verschiedene Standardprüfungen und -richtlinien.

Bereitgestellte Prüfungen

In den folgenden Tabellen sind die Standardprüfungen aufgelistet. Sie können diese Prüfungen nach Bedarf bearbeiten. Weitere Informationen zu einer bestimmten Prüfung finden Sie auf der Seite „Check Definitions“ (Prüfungsdefinitionen) (siehe Prüfungen und Richtlinien).

Linux

Typ	Name	Beschreibung
Event	os.linux.check-process	Zählt die Anzahl der laufenden Prozesse Sie können die Ereigniserstellung für diese Prüfung blockieren, wenn kein Prozess erkannt wird. Details finden Sie unter Ereigniserstellung für nicht vorhandene Entitäten blockieren.
Ereignis	os.linux.check-system-cpu	Prüft den Prozentsatz der CPU-Auslastung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux (Fortsetzung)

Typ	Name	Beschreibung
Event	os.linux.check-system-cpu-load	Prüft den Prozentsatz der CPU-Datenauslastung im Vergleich zu den konfigurierten Schwellenwerten
Event	os.linux.check-system-disk-usage	Prüft die Bereitstellungspunkte und Metriken des Dateisystems
Event	os.linux.check-system-memory-percentage	Prüft den Prozentsatz der Speicherauslastung
Event	os.linux.check-system-memory-swap	Prüft die Auslastung des Arbeitsspeicher-Austauschs
Event	os.linux.check-threads-count	Zählt die Anzahl der im System ausgeführten Threads. Sendet eine Warnung, wenn diese Zahl größer als die Schwellenwerte für Warnung oder Kritisch ist.
Metrik	os.linux.metrics-memory-vmstat	Sammelt vmstat-Speichermetriken
Metrik	os.linux.metrics-process-status	Sammelt Prozessstatusmetriken, die für den Metrikparameter bereitgestellt werden
Metrik	os.linux.metrics-system-cpu	Sammelt CPU-Metriken, einschließlich Kernen.
Metrik	os.linux.metrics-system-cpu-load	Nutzt die Betriebszeit, um CPU-Lastmetriken zu erfassen
Metrik	os.linux.metrics-system-cpu-percentage	Sammelt Metriken für die prozentuale CPU-Auslastung, einschließlich des durchschnittlichen Prozentsatzes der CPU-Auslastung.
Metrik	os.linux.metrics-system-disk	Sammelt Festplattenmetriken
Metrik	os.linux.metrics-system-disk-capacity	Sammelt Metriken zur Festplattenkapazität
Metrik	os.linux.metrics-system-disk-usage	Erfasst Metriken zur Datenträgerauslastung und liefert den gesamten, verwendeten und verfügbaren Arbeitsspeicher sowie den Prozentsatz des verwendeten Arbeitsspeichers des Datenträgers.
Metrik	os.linux.metrics-system-memory	Sammelt Speichermetriken und liefert Daten in KB.
Metrik	os.linux.metrics-system-memory-percent	Sammelt Metriken zur prozentuellen Speicherauslastung
Metrik	os.linux.metrics-system-uptime	Erfasst die Systembetriebszeit in Sekunden.
Metrik	os.linux.metrics-reboot-count-today	Erfasst die Anzahl der heute durchgeführten Neustarts

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Protokollüberwachung

Typ	Name	Beschreibung
Event	util.check-logs	Aktiviert die Überwachung von Protokolldateien, die einem normalen Benutzer gehören. Sie können die Ereigniserstellung für diese Prüfung blockieren, wenn kein Prozess erkannt wird. Details finden Sie unter Ereigniserstellung für nicht vorhandene Entitäten blockieren.
Ereignis	util.check-logs-sudo	Aktiviert die Überwachung von Protokolldateien, die einem Root-Benutzer gehören. Sie können die Ereigniserstellung für diese Prüfung blockieren, wenn kein Prozess erkannt wird. Details finden Sie unter Ereigniserstellung für nicht vorhandene Entitäten blockieren.

Linux-Netzwerküberwachung

Typ	Name	Beschreibung
Metrik	os.linux.metrics-network-interface	Ruft alle auf die Netzwerkschnittstelle bezogenen Metriken für Linux-Server ab.
Metrik	os.linux.metrics-netstat.tcp	Ruft Metriken zu TCP-Socket-Status von netstat ab. Nützlich bei Web- oder Proxy-Servern mit hohem Datenverkehr und einer großen Anzahl eingehender und ausgehender kurzzeitiger TCP-Verbindungen.

Windows-Protokollüberwachung

Typ	Name	Beschreibung
Event	os.windows.check-log	Aktiviert die Überwachung von Protokolldateien auf einem Windows-Server.

Windows

Typ	Name	Beschreibung
Ereignis	os.windows.check-disk-name	Verwendet den Namen des Speicherlaufwerks als Eingabe und überprüft, ob das Laufwerk vorhanden ist. Gibt basierend auf dem angegebenen Parameter einen Wert für KRITISCH\WARNUNG\OK zurück.
Ereignis	os.windows.check-event-log	Misst das Ereignisprotokoll Windows anhand von Parameterschwellenwerten und gibt ein Ereignis KRITISCH \WARNUNG\OK zurück.
Ereignis	os.windows.check-event-log-count	Misst das Ereignisprotokoll Windows anhand von Parameterschwellenwerten und gibt ein Ereignis KRITISCH \WARNUNG\OK zurück.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows (Fortsetzung)

Typ	Name	Beschreibung
		Stellt Informationen zur Anzahl der Ereignisse bereit, die innerhalb eines angegebenen Zeitraums für eine einzelne Protokolldatei und eine einzelne ID aufgetreten sind. Gibt auch die Filter an, die zum Abrufen von Ereignissen für eine bestimmte einwertige Windows-Ereignisebene und einen bestimmten Anbieternamen angewendet werden sollen. Das Abrufen von Ereignissen aus mehreren Protokolldateien wird nicht unterstützt. Die Anzahl der Ereignisse wird ohne Details zu den einzelnen Ereignissen angegeben.
Ereignis	os.windows.check-event-log-details	Sammelt und filtert Windows-Ereignisprotokolle basierend auf den Werten `„duration_hour“`, `„event_log_level“` und `„log_file“`. Ruft Windows-Ereignisprotokolle gemäß den angegebenen Parametern ab und filtert sie. Gibt basierend auf dem angegebenen Schweregrad Details zu den Ereignissen mit dem Status KRITISCH, WARNUNG oder OK zurück.
Ereignis	os.windows.check-env-variables	Überprüft die Umgebungsvariablen mit einem regulären Ausdruck und gibt entweder den Wert *WARNING* oder *OK* zurück. Wenn nach der Installation des Agent eine neue Systemvariable erstellt wird, müssen Sie den Agent neu starten. Diese Prüfung kann nur auf die Anwendervariablen zugreifen, die dem aktuellen Anwender zugeordnet sind (verwendet während der Agent-Installation).
Ereignis	os.windows.check-file-hashcode-update	Verwendet den Pfad und den MD5-Hashcode der Datei als Eingabe und überprüft, ob der Dateiinhalt geändert wurde. Gibt einen Wert *CRITICAL*, *WARNING* oder *OK* zurück. Für die überwachte Datei sind Leseberechtigungen erforderlich.
Ereignis	os.windows.check-file-update	Verwendet den Pfad und das Intervall der Datei als Eingabe und überprüft, ob der Dateiinhalt geändert wurde. Gibt einen Wert *CRITICAL*, *WARNING* oder *OK* zurück. Für die überwachte Datei sind Leseberechtigungen erforderlich.
Ereignis	os.windows.check-modules	Überprüft, ob die Liste der Module vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows (Fortsetzung)

Typ	Name	Beschreibung
Ereignis	os.windows.check-processor-queue-length	Prüft die Länge der Prozessorwarteschlange
Event	os.windows.check-system-cpu-load	Prüft die CPU-Last mit dem Befehl *typeperf*
Event	os.windows.check-system-disk	Prüft die Festplattenauslastung unter bestimmten Parametern
Event	os.windows.check-system-memory	Erfasst die RAM-Auslastung
Ereignis	os.windows.check-system-patch	Verifiziert die Installation des System-Patch. Gibt einen Wert *WARNING* oder *OK* zurück.
Ereignis	os.windows.check-system-process	Prüft die Aufgabenliste des Benutzers, um laufende Prozesse zu ermitteln
Ereignis	os.windows.check-user-account	Verwendet die Liste der Anwendernamen als Eingabe und überprüft, ob der Anwenderaccount aktiv ist. Gibt einen Wert *CRITICAL*, *WARNING* oder *OK* zurück.
Ereignis	os.windows.check-windows-directory	Prüft, ob ein Verzeichnis vorhanden ist
Event	os.windows.check-windows-pagefile	Erfasst die Auslastung der Auslagerungsdatei und vergleicht sie mit den Schwellenwerten für Warnung und Kritisch
Event	os.windows.check-windows-process	Prüft, ob ein Benutzereingabeprozess ausgeführt wird
Event	util.check-windows-service	Prüft, ob unter Windows ein vom Benutzer angegebener Service ausgeführt wird Sie können die Ereigniserstellung für diese Prüfung blockieren, wenn kein Prozess erkannt wird. Details finden Sie unter Ereigniserstellung für nicht vorhandene Entitäten blockieren.
Metrik	os.windows.metrics-process-status	Ruft die Anzahl der ausgeführten Instanzen, den Prozentsatz der CPU-Auslastung und die Auslastung des Arbeitsspeichers (in Kilobyte) des angegebenen Prozesses Windows ab.
Metrik	os.windows.metrics-processor-queue	Erfasst die Länge der Prozessorwarteschlange
Metrik	os.windows.metrics-system-cpu-load	Erfasst die durchschnittliche CPU-Last pro Sekunde
Metrik	os.windows.metrics-system-disk-usage	Sammelt Metriken zur Festplattenauslastung
Metrik	os.windows.metrics-system-memory-percent	Erfasst die RAM-Auslastung pro Sekunde und liefert den Prozentsatz des freien physischen, freien virtuellen, gesamten physischen und virtuellen Gesamtspeichers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows (Fortsetzung)

Typ	Name	Beschreibung
Metrik	os.windows.metrics-system-network	Sammelt Netzwerkmetriken
Metrik	os.windows.metrics-system-uptime	Erfasst die Systemverfügbarkeit
Metrik	util.metrics-windows-perf-counters	(Keine Beschreibung)

MID Server

Typ	Name	Beschreibung
Event	app.mid.check-active	Prüft anhand des Vorkommens von LogStatusMonitor im MID-Protokoll, ob der MID-Server aktiv ist
Events	app.mid.check-logs-mid	Prüft die MID-Protokolle auf Fehler
Metrik	app.mid.metrics-stats	Sammelt Informationen zum MID-Server aus dem Protokoll und gibt Metriken zurück

HAProxy-Überwachung

Typ	Name	Beschreibung
Ereignis	check-haproxy	Ruft die Details des Lastenausgleichsmoduls HAProxy ab, um zu bestimmen, ob es ausgeführt wird.
Metrik	metrics-check-haproxy	Ruft die Metriken des Lastenausgleichsmoduls HAProxy ab, um zu bestimmen, ob es ausgeführt wird.

HTTP (im Proxy-Modus auszuführen)

Typ	Name	Beschreibung
Event	util.check-http-response	Verwendet eine URL oder eine Kombination aus Host, Pfad, Port und SSL und sucht nach einer Antwort „200“, die einem Muster entspricht, sofern eines angegeben ist. Kann Client-Zertifikate nutzen
Event	util.check-http-follow-redirect	Stellt sicher, dass die URL die maximale Anzahl von Weiterleitungen nicht überschreitet
Metrik	util.metrics-http-curl	Ruft HTTP-Endpunktmetriken mit curl ab

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliche HTTP-Prüfungen (keine Richtlinie)

Typ	Name	Beschreibung
Ereignis	util.check-http-response-code	Löst ein kritisches Ereignis aus, wenn der URL-Antwortcode nicht mit dem regulären Ausdruck übereinstimmt.

Active Directory-Metriken

Typ	Prüfung	Beschreibung	Befehl
Metrik	metrics.windows.active-directory	Sammelt Active Directory-Metriken auf dem Windows-Host Verwendung: Winchecks Metric-Windows-Active-Dir -s Hostname	`Winchecks Metric-Windows-Active-Dir {{if .labels.params_scheme}} -S {{.labels.params_scheme}} {{end}}`

Apache

Typ	Event/Metrik	Beschreibung	Mindestversio
Metrik	app.apache.metrics-apache	Ruft Apache HTTP-Servermetriken ab	2.4.x

Apache Kafka

Typ	Event/Metrik	Beschreibung	Mindestversio
Ereignis	kafka.check-zookeeper-status	Löst ein kritisches Ereignis aus, wenn der gehostete ZooKeeper von Apache Kafka ausgefallen ist.	ZooKeeper 3.1.2
Ereignis	kafka.check-topic-replicas	Löst ein kritisches Ereignis aus, wenn ein Thema Partitionen mit unbekannten Replikaten aufweist.	ZooKeeper 3.1.2
Ereignis	kafka.check-topic-replication-factor	Löst ein kritisches Ereignis aus, wenn der Replikationsfaktor mindestens eines Themas über oder unter dem angegebenen Replikationsfaktorparameter liegt.	ZooKeeper 3.1.2
Ereignis	kafka.check-topic-leader	Löst ein kritisches Ereignis aus, wenn ein Thema Partitionen mit unbekannten Leitern oder einem nicht bevorzugten Replikat als Leiter aufweist.	ZooKeeper 3.1.2
Ereignis	kafka.check-topic-partitions	Löst ein kritisches Ereignis aus, wenn die Anzahl der Partitionen für ein Thema kleiner als der Parameter „min_partitions“ ist.	ZooKeeper 3.1.2
Ereignis	kafka.check-broker-status	Löst ein kritisches Ereignis aus, wenn der Kafka-Broker auf dem Host ausgefallen ist.	Kafka 0.10.1.0

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Mindestversio
Metrik	kafka.metrics.broker	Sammelt Kafka-Broker-Metriken vom Host.	Kafka 0.10.1.0
Metrik	kafka.metrics.zookeeper	Sammelt ZooKeeper-Metriken vom Host.	ZooKeeper 3.5.0-alpha

Azure Kubernetes (K8s) Service-Metriken

Typ	Event/Metrik	Beschreibung	Befehl
Metrik	azure.metrics-k8s-service	Stellt Metriken auf Pod-, -Knoten und Clusterebene aus allen Azure Kubernetes-Services im Metrikformat bereit. Verwendung: metrics-azure-k8s-service.rb Befehlsbeispiel: `metrics-azure-k8s-service.rb -S {{.labels.params_subscription_id}} -r westus2`	`metrics-azure-k8s-service.rb -r {{.labels.params_ci_region}} {{-s {{if.labels.params_subscriptio -S {{.labels.params_subscription_ {{end}}`

Azure VM-Metriken

Typ	Event/Metrik	Beschreibung	Befehl
Metrik	azure.metrics-vm-cpu	Stellt CPU-bezogene Metriken für jede VM-Instanz in der Azure-Region bereit. Befehlsbeispiel: `./metrics-azure-vm.rb -S {{.labels.params_subscription_id}} -T cpu`	`metrics-azure-vm.rb -r {{.labels.params_ci_region}} {{if .labels.params_subscriptio -S {{.labels.params_subscription_ {{end}} -T {{.labels.params_type}}`
Metrik	azure.metrics-vm-disk	Stellt laufwerksbezogene Metriken für jede VM-Instanz in der Azure-Region bereit. Befehlsbeispiel: `./metrics-azure-vm.rb -S`	`metrics-azure-vm.rb -r {{.labels.params_ci_region}} {{if .labels.params_subscriptio -S {{.labels.params_subscription_ {{end}} -T {{.labels.params_type}}`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure VM-Metriken (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Befehl
		`{{.labels.params_subscription_id}} -T disk`	
Metrik	azure.metrics-vm-memory	Stellt arbeitsspeicherbezogene Metriken für jede VM-Instanz in der Azure-Region bereit. Befehlsbeispiel: `./metrics-azure-vm.rb -S {{.labels.params_subscription_id}} -T memory`	`metrics-azure-vm.rb -r {{.labels.params_ci_region}} {{if .labels.params_subscriptio -S {{.labels.params_subscription_ {{end}} -T {{.labels.params_type}}`
Metrik	azure.metrics-vm-network	Stellt netzwerkbezogene Metriken für jede VM-Instanz in der Azure-Region bereit. Befehlsbeispiel: `./metrics-azure-vm.rb -S {{.labels.params_subscription_id}} -T network`	`metrics-azure-vm.rb -r {{.labels.params_ci_region}} {{if .labels.params_subscriptio -S {{.labels.params_subscription_ {{end}} -T {{.labels.params_type}}`
Metrik	azure.metrics-vm-flows	Stellt Flows-bezogene Metriken für jede VM-Instanz in der Azure-Region bereit. Befehlsbeispiel: `./metrics-azure-vm.rb -S {{.labels.params_subscription_id}} -T flows`	`metrics-azure-vm.rb -r {{.labels.params_ci_region}} {{if .labels.params_subscriptio -S {{.labels.params_subscription_ {{end}} -T {{.labels.params_type}}`

GCP GCE-Metriken

Typ	Event/Metrik	Beschreibung
Metrik	gcp.metrics.GCE	Ruft Metriken aus GCP für Google Compute Engine ab.
Metrik	glassfish.metric-server-requests	Macht HTTP-Anforderungsmetriken für alle auf dem GlassFish-Server bereitgestellten Anwendungen verfügbar.
Metrik	glassfish.metric-server-resources	Macht Metriken der auf dem GlassFish-Server bereitgestellten Ressourcen verfügbar.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

GCP GCE-Metriken (Fortsetzung)

Typ	Event/Metrik	Beschreibung
Metrik	glassfish.metric-transaction-service	Macht Metriken für alle Transaktionen in Anwendungen verfügbar, die auf dem GlassFish-Server bereitgestellt wurden.
Metrik	GlassFish.metric-deployed-apps	Stellt Metrikausgabe der auf dem GlassFish-Server bereitgestellten Anwendungen bereit.
Metrik	GlassFish.metric-Bereitstellung-Lebenszyklus	Stellt Lebenszyklusmetriken von Anwendungen bereit, die auf dem GlassFish-Server bereitgestellt werden.

Glasfisch

Typ	Name	Beschreibung
Metrik	glassfish.metric-jvm-level	Ruft JVM-Metriken auf dem GlassFish-Server ab.
Metrik	glassfish.metric-server-requests	Macht HTTP-Anforderungsmetriken für alle auf dem GlassFish-Server bereitgestellten Anwendungen verfügbar.
Metrik	glassfish.metric-server-resources	Macht Metriken der auf dem GlassFish-Server bereitgestellten Ressourcen verfügbar.
Metrik	glassfish.metric-transaction-service	Macht Metriken für alle Transaktionen in Anwendungen verfügbar, die auf dem GlassFish-Server bereitgestellt wurden.
Metrik	GlassFish.metric-deployed-apps	Stellt Metrikausgabe der auf dem GlassFish-Server bereitgestellten Anwendungen bereit.
Metrik	GlassFish.metric-Bereitstellung-Lebenszyklus	Stellt Lebenszyklusmetriken von Anwendungen bereit, die auf dem GlassFish-Server bereitgestellt werden.

IBM WebSphere AS

Typ	Event/Metrik	Beschreibung	Mindestversio
Metrik	app.websphere.metrics-websphere	Gibt IBM WebSphere-Anwendungsservermetriken zurück.	9

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IBM WebSphere AS (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Mindestversio
		Stellen Sie sicher, dass der Benutzer, der den Agent ausführt, über ausreichende Berechtigungen für den Zugriff auf die erforderlichen Dateien in den `IBM Websphere AS`-Installationsverzeichnissen verfügt.	

IIS

Typ	Event/Metrik	Beschreibung	Mindestversio
Event	app.iis.check-iis-alive	Prüft, ob IIS ausgeführt wird	-
Event	app.iis.check-iis-current-connections	Prüft die Anzahl der aktuellen Verbindungen zum IIS-Server und deren Status, abhängig von der Eingabe. Standardmäßig sind alle Sites mit dem IIS-Server verbunden.	-
Metrik	app.iis.metrics-iis	Gibt IIS-Metriken zurück	-

JBoss/WildFly

Typ	Event/Metrik	Beschreibung	Mindestversio
Metrik	app.jboss.metrics-jboss	Ruft JBoss- bzw. WildFly-Servermetriken ab Stellen Sie sicher, dass der Benutzer, der den Agent ausführt, über ausreichende Berechtigungen für den Zugriff auf die erforderlichen Dateien in den`JBoss-/ WildFly` -Installationsverzeichnissen verfügt.	16, 17

Kubernetes

Typ	Event/Metrik	Beschreibung	Befehl
Event	k8s.check-kube-apiserver-available	Überprüft, ob der Kubernetes-API-Server aktiv ist.	`check-kube-apiserver-available.rb {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}}`
Event	k8s.check-kube-nodes-ready	Überprüft, ob Kubernetes-Knoten betriebsbereit sind.	`check-kube-nodes-ready.rb {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}}`
Event	k8s.check-kube-pods-pending	Misst den Schwellenwert, bis zu dem sich Pods im Status „Ausstehend“ befinden. Bestimmen Sie den Schwellenwert, indem Sie den Wert des Prüfparameters	`check-kube-pods-pending.rb {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}}`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kubernetes (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Befehl
		pending_timeout festlegen (Standard = 300 Sekunden).	
Event	k8s.check-kube-pods-restarting	Überprüft die Pods, die neu gestartet werden. Bestimmen Sie den Schwellenwert, indem Sie den Wert des Prüfparameters festlegen (Standard = 10).	`check-kube-pods-restarting.rb {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}} {{if .labels.params_restart}} -r {{.labels.params_restart}} {{end}}`
Event	k8s.check-kube-pods-running	Überprüft die Pods, die sich im Status „Wird ausgeführt“ befinden. Konfigurieren Sie den Schwellenwert im Prüfparameter *not_ready_time* in Sekunden (Standard = 0).	`check-kube-pods-running.rb {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}} {{if .labels.params_not_ready_time}} -time {{.labels.params_not_ready_time}} {{end}}`
Event	k8s.check-kube-pods-runtime	Überprüft, ob Pods länger als erwartet ausgeführt werden. Konfigurieren Sie den Schwellenwert im Prüfparameter (in Sekunden). Sie können beide Schwellenwerte, WARNUNG und KRITISCH, konfigurieren.	check-kube-pods-runtime.rb {{if .labels.params_critical}} -c {{.labels.params_critical}} {{end}} {{if .labels.params_warning}} -w {{.labels.params_warning}} {{end}} {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}}
Event	k8s.check-kube-service-available	Überprüft, ob Kubernetes-Services ausgeführt werden. Fügen Sie die Liste der zu überwachenden Services dem Feld *check_param* des Service als kommagetrennte Werte (ohne Leerzeichen) hinzu. Wenn Sie ungültige Services eingeben, schlägt die Prüfung fehl.	`check-kube-pods-runtime.rb {{if .labels.params_critical}} -c {{.labels.params_critical}} {{end}} {{if .labels.params_warning}} -w {{.labels.params_warning}} {{end}} {{if .labels.params_api_server}} -s {{.labels.params_api_server}} {{end}}`
Metrik	k8s.metrics-pods	Stellt eine Pod-Anzahl für alle verfügbaren Services bereit.	`metrics-pods.rb {{if .labels.params_api_server}} -s {{.labels.params__api_server }} {{end}}`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MsSQL

Typ	Event/Metrik	Beschreibung	Mindestversio
Metrik	app.msssql.metrics-mssql	Ruft MSSQL-Datenbankmetriken ab	2016
Metrik	app.metrics-mssql-query	Generische MSSQL-Abfrageklasse, die eine Abfrage akzeptiert und Metriken ausgeben kann.	2016

MySQL

Typ	Event/Metrik	Beschreibung	Mindestversio
Event	app.mysql.check-mysql-alive	Prüft, ob die MySQL-Datenbank ausgeführt wird	5.7, 8
Event	app.mysql.check-mysql-threads	Prüft die Anzahl der laufenden Threads in der MySQL-Datenbank. Bestimmt den Status je nach Eingabe: OK, Warnung oder Kritisch.	5.7, 8
Event	util.check-mysql-query	Prüft die Länge des Ergebnissatzes einer MySQL-Abfrage Für diese Prüfung müssen Sie auf dem MySQL-Server die Authentifizierungsmethode native_password verwenden.	5.7, 8
Metrik	app.mysql.metrics-mysql	Gibt MySQL-Datenbankmetriken zurück	5.7, 8
Metrik	app.mysql.metrics-mysql-processes	Gibt Metriken für MySQL-Datenbankprozesse zurück	5.7, 8
Metrik	util.metrics-mysql-query	Erzeugt eine formatierte Metrik für die Länge des Ergebnissatzes einer MySQL-Abfrage	5.7, 8

MongoDB

Typ	Event/Metrik	Beschreibung	Mindestversion
Ereignis	app.mongodb.check-mongodb-alive	Überwacht, ob der MongoDB-Server aktiv ist, und erstellt Warnungen für den MongoDB-Server-Integritätsstatus.	
Ereignis	app.mongodb.check-mongodb-metrics	Erstellt Warnungen für eine der MongoDB-Metriken basierend auf dem Schwellenwert.	
Metrik	app.mongodb.metrics-mongodb	Gibt Metriken des MongoDB-Servers und aller Datenbanken zurück.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Oracle

Typ	Event/Metrik	Beschreibung	Mindestversio
Event	app.oracle.check-oracle-alive	Prüft, ob die Oracle-Datenbank ausgeführt wird	12c, 18c
Metrik	app.oracle.metrics-oracle	Gibt Oracle-Datenbankmetriken zurück	12c, 18c
Metrik	util.metrics-oracle-query	Generische Oracle-Abfrageklasse, die eine Abfrage akzeptiert und Metriken ausgeben kann	12c, 18c

Oracle WebLogic AS

Typ	Event/Metrik	Beschreibung	Mindestversio
Metrik	app.weblogic.metrics-weblogic	Gibt Metriken für Oracle WebLogic-Anwendungsserver zurück Stellen Sie sicher, dass der Benutzer, der den Agent ausführt, über ausreichende Berechtigungen für den Zugriff auf die erforderlichen Dateien in den `WebLogic`-Installationsverzeichnissen verfügt.	12cR2

Tomcat

Typ	Event/Metrik	Beschreibung	Mindestversio
Metrik	app.tomcat.metrics-tomcat	Gibt Metriken für den Apache Tomcat-Server zurück.	8.5.27, 9.x

App

Typ	Name	Beschreibung
Event	util.check-snmp	SNMP-Prüfung, die den Metrikwert mit dem Standardwert vergleicht. Erfordert Eingaben wie Server, Port, SNMP-Community und Grenzwerte
Metrik	util.metrics-snmp	Sammelt Metriken aus einem SNMP-OID-Wert
Metrik	util.metrics-snmp-bulk-sn	Sammelt Metriken aus einer SNMP-Tabellen-OID und gibt das Ergebnis als Tabelle zurück

Serviceverbesserungen (können jeder Richtlinie zugeordnet werden)

Typ	Event/Metrik	Beschreibung	Befehl
Metrik (Windows)	os.windows.metrics-service-status	Erfasst den Windows-Servicestatus und liefert Metriken zur Anzahl der ausgeführten Services.	`winchecks metric-windows-service-status -S Wcmsvc --scheme hostname.proc`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Varnish

Typ	Name	Beschreibung
Metrik	app.varnish.metrics-varnish	Sammelt Varnish-Metriken vom Host.

vSphere

Typ	Name	Beschreibung
Metrik	vsphere.metric-VirtualMachine	Ruft Metriken für die virtuelle vSphere-Maschine ab.
Metrik	vsphere.metric – Datenspeicher	Ruft Metriken für den vSphere Datastore ab.
Metrik	vsphere.metric-Datacenter	Ruft Metriken für das vSphere Datacenter ab.
Metrik	vsphere.metric-ESX_Server	Ruft Metriken für vSphere ESX Server oder HostSystem ab

Zscaler

Typ	Name	Beschreibung
Metrik	zscaler-monitoring-check	Überprüft, ob die App Zscaler ordnungsgemäß ausgeführt wird.
Metrik	zscaler-remediation-check	Fährt die App Zscaler herunter, startet sie neu und erstellt einen Incident. Wird nur ausgeführt, wenn bei zscaler-monitoring-check ein Fehler auftritt.

CPU-Verbesserungen

Typ	Event/Metrik	Beschreibung	Befehl
Metrik	os.windows.metrics-system-cpu	Sammelt CPU-Kernmetriken.	`winchecks metric-windows-cpu --scheme hostname.proc`

Datenträgerverbesserungen – Linux-Ereignisse (können jeder Richtlinie zugeordnet werden)

Event/Metrik	Beschreibung	Befehl
os.linux.check-disk-ioTimeWeighted	Misst den `ioTimeWeighted-Wert des Datenträgers` und gibt die Meldung **KRITISCH\WARNUNG\OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-disk-ioTimeWeighted.rb`
os.linux.check-disk-sectorsWritten	Misst die Gesamtzahl der erfolgreich geschriebenen	`check-disk-sectorsWritten.rb`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenträgerverbesserungen – Linux-Ereignisse (können jeder Richtlinie zugeordnet werden) (Fortsetzung)

Event/Metrik	Beschreibung	Befehl
	Sektoren und gibt die Meldung **KRITISCH/ WARNUNG/OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	
os.linux.check-disk-sectorsRead	Misst die Gesamtzahl der erfolgreich gelesenen Sektoren des Datenträgers und gibt die Meldung **KRITISCH\WARNUNG\OK** zurück, entsprechend den in den Parametern angegebenen Schwellenwerten.	`check-disk-sectorsRead.rb`
os.linux.check-disk-readTime	Misst die Gesamtzahl der Millisekunden, die von allen zum Lesen verwendeten Schwellenwerten verwendet wurden, und gibt die Meldung **KRITISCH \WARNUNG\OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-disk-readTime.rb`
os.linux.check-disk-writes	Misst die Gesamtzahl der erfolgreich abgeschlossenen Schreibvorgänge und gibt die Meldung **KRITISCH/ WARNUNG/OK** zurück, und zwar gemäß den in den Parametern angegebenen Schwellenwerten.	`check-disk-writes.rb`
os.linux.check-disk-reads	Misst die Gesamtzahl der erfolgreich abgeschlossenen Lesevorgänge und gibt die Meldung **KRITISCH/ WARNUNG/OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-disk-reads.rb`
os.linux.check-disk-writesMerged	Misst den Wert `des zusammengeführten Datenträgerschreibvorgangs` und gibt die Meldung **KRITISCH/WARNUNG/OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-disk-writesMerged.rb`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenträgerverbesserungen – Linux-Ereignisse (können jeder Richtlinie zugeordnet werden) (Fortsetzung)

Event/Metrik	Beschreibung	Befehl
os.linux.check-disk-readsMerged	Misst den `zusammengeführten Wert des Datenträgers` und gibt die Meldung **KRITISCH\WARNUNG\OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-disk-readsMerged.rb`
os.linux.check-disk-writeTime	Misst die Gesamtzahl der Millisekunden, die von allen Schreibvorgängen benötigt wurden, und gibt die Meldung **KRITISCH/WARNUNG/OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-disk-writeTime.rb`
os.linux.check-disk-ioInProgress	Misst den `ioInProgress-Wert des Datenträgers` und gibt die Meldung **KRITISCH/WARNUNG/OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-disk-ioInProgress.rb`
os.linux.check-disk-iotime	Misst den `ioTime-Wert des Datenträgers` und gibt die Meldung **KRITISCH/WARNUNG/OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-disk-ioTime.rb`

Datenträgerverbesserungen – Windows-Ereignisse (können jeder Richtlinie zugeordnet werden)

Event/Metrik	Beschreibung	Befehl
os.windows.check-disk-AvgSecWrite	Misst die durchschnittlichen Datenträgerschreibvorgänge pro Sekunde und gibt die Meldung **KRITISCH/WARNUNG/OK** zurück, wie in den Parametern angegeben.	`winchecks check-windows-AvgDisksec-write -w 1 -c 0`
os.windows.check-disk-ReadBytes-sec	Misst den `ReadBytes-Wert des Datenträgers` pro Sekunde und gibt die Meldung **KRITISCH/WARNUNG/**	`winchecks check-windows-DiskReadBytes-sec -w 1 -c 0`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Datenträgerverbesserungen – Windows-Ereignisse (können jeder Richtlinie zugeordnet werden) (Fortsetzung)

Event/Metrik	Beschreibung	Befehl
	OK gemäß den in den Parametern angegebenen Schwellenwerten zurück.	
os.windows.check-disk-WriteBytes-sec	Misst den `WriteBytes-Wert des Datenträgers` pro Sekunde und gibt die Meldung **KRITISCH/WARNUNG/OK** gemäß den in den Parametern angegebenen Schwellenwerten zurück.	`winchecks check-windows-DiskWriteBytes-sec -w 1 -c 0`
os.windows.check-disk-AvgSecRead	Misst die durchschnittlichen Datenträger-Lesevorgänge pro Sekunde und gibt die Meldung **KRITISCH/WARNUNG/OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`winchecks check-windows-AvgDisksec-read -w 1 -c 0`

Datenträgerverbesserungen – Windows-Metriken (kann jeder Richtlinie zugeordnet werden)

Event/Metrik	Beschreibung	Befehl
os.windows.metrics-system-disk	Erfasst die folgenden Datenträgermetriken: • AvgDiskSecPerRead • AvgDiskSecPerWrite • DiskReadBytesPerSec • DiskWriteBytesPerSec	`winchecks metric-windows-disk`

Erweiterungen des Arbeitsspeichers (können jeder Richtlinie zugeordnet werden)

Typ	Event/Metrik	Beschreibung	Befehl
Ereignis (Linux)	os.linux.check-free-physical-memory	Misst den Prozentsatz des freien physischen Arbeitsspeichers des Linux-Systems und gibt die Ereignismeldung **KRITISCH/WARNUNG/OK** gemäß den in den Parametern angegebenen	`check-free-physical-memory -w 10 -c 5`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterungen des Arbeitsspeichers (können jeder Richtlinie zugeordnet werden) (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Befehl
		Schwellenwerten zurück.	
Ereignis (Linux)	os.linux.check-free-virtual-memory	Misst den Prozentsatz des freien virtuellen Speichers des Linux-Systems und gibt die Ereignismeldung **KRITISCH/WARNUNG/OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-free-virtual-memory -w 10 -c 5`
Ereignis (Windows)	os.windows.check-free-physical-memory	Misst den Prozentsatz des freien physischen Arbeitsspeichers des Windows-Systems und gibt die Ereignismeldung **KRITISCH/WARNUNG/OK** gemäß den in den Parametern angegebenen Schwellenwerten zurück.	`Winchecks Check-Windows-Free-Physfical-Memory -w 10 -c 5`
Ereignis (Windows)	os.windows.check-free-virtual-memory	Misst den Prozentsatz des freien virtuellen Speichers des Windows-Systems und gibt die Ereignisnachricht **KRITISCH/WARNUNG/OK** zurück, und zwar gemäß den in den Parametern angegebenen Schwellenwerten.	`winchecks check-windows-free-physical-memory -w 10 -c 5`
Metrik (Windows)	os.windows.metrics-system-memory	Erfasst die folgenden Arbeitsspeichermetriken: • FreePhysicalMemory • TotalPhysicalMemory • FreeVirtualMemory • TotalVirtualMemorySize • AvailableMemory • TotalVisibleMemorySize	`winchecks metric-windows-memory --scheme hostname.proc`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozessverbesserungen (können mit jeder Richtlinie verknüpft werden)

Typ	Event/Metrik	Beschreibung	Befehl
Ereignis (Linux)	os.linux.check-process-cpu	Misst die CPU-Auslastung des Linux-Prozesses und gibt die Meldung **KRITISCH/ WARNUNG/OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-process-cpu.rb -p acc -c 95 -w 85`
Ereignis (Linux)	os.linux.check-process-memory	Misst die Auslastung des Linux-Prozessarbeitsspeichers und gibt die Meldung **KRITISCH/ WARNUNG/OK** zurück, gemäß den in den Parametern angegebenen Schwellenwerten.	`check-process-memory.rb -p acc -c 95 -w 85`
Metrik (Linux)	os.linux.metrics-process-usage	Erfasst den Linux-Prozessstatus, einschließlich der vom Prozess verwendeten CPU- und Arbeitsspeicherdaten.	`metrics-process-usage.rb -p acc -s hostname.proc`
Ereignis (Windows)	os.windows.check-process-cpu	Misst die CPU-Auslastung des Windows-Prozesses und gibt die Meldung **KRITISCH\WARNUNG \OK** gemäß den in den Parametern angegebenen Schwellenwerten zurück.	`winchecks check-windows-process-cpu-p acc -c 95 -w 85`
Ereignis (Windows)	os.windows.check-process-memory	Misst die Auslastung des Windows-Prozessarbeitsspeichers und gibt die Meldung **„KRITISCH\WARNUNG \OK“** gemäß den in den Parametern angegebenen Schwellenwerten zurück.	`winchecks check-windows-process-memory-p acc -c 95 -w 85`
Metrik (Windows)	os.windows.metrics-process-usage	Erfasst den Windows-Prozessstatus, einschließlich	`winchecks metric-windows-process-`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozessverbesserungen (können mit jeder Richtlinie verknüpft werden) (Fortsetzung)

Typ	Event/Metrik	Beschreibung	Befehl
		der vom Prozess verwendeten CPU- und Arbeitsspeicherdaten.	`status -n Svchost -s hostname.proc`

Unterstützte Agent-Richtlinien

In dieser Tabelle sind die unterstützten Richtlinien von Agent Client Collector for Monitoring aufgelistet, denen die Prüfungsdefinitionen zugeordnet sind. Richtlinien bestehen aus den überwachten CIs und den Prüfungen, die für sie ausgeführt werden.

Name	Beschreibung	Prüfungen
Apache Events	Überwacht laufende Apache HTTP-Webserver Um die Überwachung zu aktivieren, wenn der Prozess aktiv ist, aktivieren Sie die entsprechende Prüfung: • Für Linux: os.linux.check-process • Für Windows: os.windows.check-windows-process Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen für die Standardauthentifizierung an.	• os.linux.check-process • os.windows.check-windows-process
Apache Metrics	Überwacht laufende Apache HTTP-Webserver Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen für die Standardauthentifizierung an.	app.apache.metrics-apache
Apache Kafka Ereignisse	Überwacht den Status von Kafka-Broker, Kafka-Themen, Partitionen, Replikate und ZooKeeper.	
Apache Kafka Metriken	Überwacht und sammelt Metriken von Kafka Broker und Kafka ZooKeeper.	
Azure DB-Metriken	Überwacht Datenbanken von Azure in einem Rechenzentrum Azure. So aktivieren Sie die Prüfungen der Richtlinie: • Konfigurieren Sie einen Proxy-Agent. • Fügen Sie die folgenden Azure-Service-Prinzipal-Anmeldeinformationen hinzu:	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	◦ Mandanten-ID ◦ Client-ID ◦ Geheimer Schlüssel • Konfigurieren Sie die Authentifizierungsmethode als **Geheimer Clientschlüssel**. • Fügen Sie der Richtlinie Azure-Anmeldeinformationen hinzu. • Geben Sie den Wert *subscription_id* in jeder Prüfungsinstanz an. Der standardmäßige überwachte CI-Typ ist „cmdb_ci_azure_datacenter“, die Bindung erfolgt jedoch in der Cloud-Datenbank (cmdb_ci_cloud_database). Weitere Informationen zum Konfigurieren einer Richtlinie finden Sie unter Neue Agent Client Collector-Richtlinie erstellen.	
Azure Kubernetes (K8s) Service-Metriken	Überwacht das Azure-CI *cmdb_ci_azure_datacenter*. Wird mit dem Kubernetes-Datencluster *cmdb_ci_kubernetes_cluster* verbunden.	azure.metrics-k8s-service Details finden Sie unter Azure-Systemüberwachung – Standardprüfungen und Richtlinien.
Azure VM-Metriken	Überwacht das Azure-CI *cmdb_ci_azure_datacenter*. Wird mit der VM-Instanz *cmdb_ci_vm_instance* verbunden.	• azure.metrics-vm-cpu • azure.metrics-vm-disk • azure.metrics-vm-memory • azure.metrics-vm-network • azure.metrics-vm-flows Details finden Sie unter Azure-Systemüberwachung – Standardprüfungen und Richtlinien.
Basic Discovery	Führt alle 12 Stunden für alle Agents eine Basiserkennung mit ServiceNow Discovery aus. Diese Prüfung extrahiert Basisinformationen über den Host und seine laufenden Prozesse. Die Hostinformationen werden verwendet, um in der CMDB den entsprechenden Host zu erstellen. Anhand der laufenden Prozesse werden die klassifizierten Anwendungs-CIs erstellt.	check-discovery-basic

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	Sie benötigen erweiterte BS-Berechtigungen, um mit dem netstat-Befehl Ports zu erkennen. Der auszuführende Befehl ist von Ihrem Betriebssystem abhängig: • Linux: `sudo -n netstat -antp` • Windows: `netstat -anop TCP`	
Docker Container Metrics	Sammelt Leistungsmetriken für Docker-Container Geben Sie die Anmeldeinformationen von Benutzern an, die Mitglieder der Docker-Benutzergruppe sind oder die über sudo-Rechte verfügen. Geben Sie diese Anmeldeinformationen auf der Registerkarte **Credentials** (Anmeldeinformationen) des Richtlinienformulars an.	container.docker.metrics-docker
Docker Engine Metrics	Sammelt allgemeine Metriken für die Docker-Engine Stellt die Anmeldeinformationen eines Benutzers bereit, der entweder Mitglied der Docker-Benutzergruppe ist oder dem auf der Registerkarte **Anmeldeinformationen** sudo-Rechte zugewiesen wurden. Um laufende Prüfungen über diese Richtlinie zu aktivieren, fügen Sie der Docker-Benutzergruppe auf dem Computer, auf dem der Agent ausgeführt wird, den Benutzer servicenow hinzu.	container.docker.metrics-docker-info
F5 SNMP Events	Beispiel für die Verwendung von SNMP-Prüfungen Da der Agent nicht auf SNMP-Geräten ausgeführt wird, geben Sie Folgendes an, um diese Richtlinie durchzuführen: • Einen Proxy-Agent und Anmeldeinformationen. • Den Host des Proxy-Agent. Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der SNMP-Community für die Verbindung zum Server an.	util.check-snmp
F5 SNMP Metrics	Beispiel für die Verwendung von SNMP-Metriken	• util.metrics-snmp • util.metrics-snmp-bulk-sn

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	Da der Agent nicht auf SNMP-Geräten ausgeführt wird, geben Sie Folgendes an, um diese Richtlinie durchzuführen: • Einen Proxy-Agent und Anmeldeinformationen. • Den Host des Proxy-Agent. Geben Sie auf der Registerkarte **Anmeldeinformationen** die Anmeldeinformationen der SNMP-Community für die Verbindung zum Server an.	
GlassFish-Metriken	Führt Metrikprüfungen auf dem GlassFish-Server aus. GlassFish-Metriken werden in ITOM Agent Client Collector Version 2.3.0 – August 2022, unterstützt, die im ServiceNow Store verfügbar ist.	
HAProxy Ereignisse	Ruft die Details des Lastenausgleichsmoduls HAProxy ab, um zu bestimmen, ob es ausgeführt wird. HAProxy Ereignisse werden in ITOM Agent Client Collector Version 2.3.0 – August 2022, verfügbar im ServiceNow Store , unterstützt.	
HAProxy Metriken	Ruft die Metriken des Lastenausgleichsmoduls HAProxy ab, um zu bestimmen, ob es ausgeführt wird. HAProxy -Metriken werden in ITOM Agent Client Collector Version 2.3.0 – August 2022, unterstützt, die im ServiceNow Store verfügbar ist.	
HTTP Entry Points Events	Führt die Prüfung util.check-http-follow-redirect für alle HTTP-Einstiegspunkte aus, die zu den Business Services der Anwendung gehören. Die Services werden mittels Richtlinienfilter ausgewählt. Die Services definieren die Einstiegspunkte. • Zum Aktivieren dieser Prüfung ist eine neue Datenbankansicht verfügbar, die die Tabelle der Anwendungsservices mit der Tabelle der Einstiegspunkte kombiniert. • Sie können die Services filtern, um die Einstiegspunkte zu erhalten. • Warnungen, die Sie erhalten, sind automatisch an die Einstiegspunkte gebunden. Diese Warnungen wirken sich	util.check-http-follow-redirect

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	auf die Auswirkungsberechnung aus, da Einstiegspunkte berücksichtigt werden. • Für diese Richtlinie ist ein Proxy-Agent erforderlich.	
HTTP Entry Points Metrics	Wenn die Warnung beispielsweise an den Einstiegspunkt gebunden ist, identifiziert die Servicezuordnung ein Problem am Einstiegspunkt. • Die Metrik wird an das Einstiegspunkt-CI gebunden. In früheren Releases war die Metrik an den Service gebunden, und der Einstiegspunkt war die Ressource. • Für diese Richtlinie ist ein Proxy-Agent erforderlich.	util.metrics-http-curl
IIS Events	Überwacht laufende IIS-Server	• app.iis.check-iis-alive • app.iis.check-iis-current-connections
IIS Metrics	Überwacht laufende IIS-Server	app.iis.metrics-iis
JBoss/WildFly Application Server Events	Überwachung laufender JBoss/WildFly-Anwendungsserver Um die Überwachung zu aktivieren, wenn der JBoss-Prozess aktiv ist, aktivieren Sie os.linux.check-process. Der Parameter *jboss_home* in der Prüfungsinstanz wird als Speicherort für die JBoss-Installation angegeben.	os.linux.check-process
JBoss/WildFly Application Server Metrics	Überwacht laufende JBoss/WildFly-Anwendungsserver	app.jboss.metrics-jboss
Kubernetes	Überwacht den Zustand der Kubernetes-Infrastruktur, z. B. Cluster, Knoten, Pod-Status, API und Serviceverfügbarkeit. Bei der Ausführung von Kubernetes-Prüfungen: • Der Proxy-Agent muss aktiviert sein. • Geben Sie Kubernetes-Anmeldeinformationen ein, entweder eine Kombination aus Benutzername und Passwort oder ein Bearer-Token (aber nicht beides).	• k8s.check-kube-apiserver-available • k8s.check-kube-nodes-ready • k8s.check-kube-pods-pending • k8s.check-kube-pods-restarting • k8s.check-kube-pods-running

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	• Um die Richtlinie zu aktivieren und zu veröffentlichen, konfigurieren Sie den Wert *api_server* in den Prüfparameterdefinitionen jeder Prüfung mit einem der folgenden Werte: ◦ `https://127.0.0.1:<portnumber>/api` (wenn API-Server und Agent auf demselben Server ausgeführt werden) ◦ `https://<api_server_url>/api` (wenn API-Server und Agent auf demselben Server oder auf verschiedenen Servern ausgeführt werden) Um localhost als api_server zu verwenden, führen Sie den folgenden Befehl aus: `"kubectl proxy -port=8081 &"`. • Führen Sie Discovery aus , um alle Kubernetes-CIs zu erkennen. Einzelheiten hierzu finden Sie unter Kubernetes-Discovery.	• k8s.check-kube-pods-runtime • k8s.check-kube-service-available • k8s.metrics-pods
Linux log monitoring	Überwacht Protokolle auf laufenden Linux-Servern.	• util.check-logs • util.check-logs-sudo
Linux OS Events	Führt Linux-Prüfungen auf ausgeführten Linux-Servern aus.	• os.linux.check-process • os.linux.check-system-cpu • os.linux.check-system-cpu-load • os.linux.check-system-disk-usage • os.linux.check-system-memory-percentage • os.linux.check-system-memory-swap • os.linux.check-threads-count
Linux OS Metrics	Sammelt Linux-Metriken auf laufenden Linux-Servern	• os.linux.metrics-memory-vmstat • os.linux.metrics-process-status • os.linux.metrics-system-cpu • os.linux.metrics-system-cpu-load

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
		• os.linux.metrics-system-disk • os.linux.metrics-system-disk-capacity • os.linux.metrics-system-disk-usage • os.linux.metrics-system-memory • os.linux.metrics-system-memory-percentage • os.linux.metrics.reboot_count_today
MSSQL Events	Überwacht den Betriebsprozess von MSSQL-Servern. Führt os.windows.check-windows-process aus, um zu überwachen, wann der Serverprozess aktiv ist	os.windows.check-windows-process
MSSQL Metrics	Überwacht den Betriebsprozess von MSSQL-Servern. Führt app.mssql.metrics-mssql aus, um Metriken zu erfassen	app.mssql.metrics-mssql
MySQL DB Events	Überwacht laufende MySQL-Instanzen Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Datenbankserver an. **Hinweis:** Dienstprogrammprüfungen mit dem Präfix „util“ mit obligatorischen Parametern, für die Sie einen Wert angeben müssen. Für diese Parameter sind keine Standardwerte verfügbar.	• app.mysql.check-mysql-alive • app.mysql.check-mysql-threads • util.check-mysql-query
MySQL DB Metrics	Überwacht laufende MySQL-Instanzen Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Datenbankserver an. **Hinweis:** Dienstprogrammprüfungen mit dem Präfix „util“ mit obligatorischen Parametern, für die Sie einen Wert angeben müssen. Für diese Parameter sind keine Standardwerte verfügbar.	• app.mysql.metrics-mysql • app.mysql.metrics-mysql-processes • util.metrics-mysql-query
Ping-Metriken für das Netzwerk	Überwacht die in der Instanz ServiceNow erkannte IP-Adresse. Der überwachte CI-Typ cmdb_ci_hardware ist an den entsprechenden Server gebunden:	util.metrics-ping

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	Diese Richtlinie erfordert einen Proxy-Agent.	
Oracle DB Events	Überwacht laufende Oracle-Datenbankinstanzen Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Datenbankserver an. **Hinweis:** Dienstprogrammprüfungen mit dem Präfix „util“ mit obligatorischen Parametern, für die Sie einen Wert angeben müssen. Für diese Parameter sind keine Standardwerte verfügbar.	app.oracle.check-oracle-alive
Oracle DB Metrics	Überwacht laufende Oracle-Datenbankinstanzen Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Datenbankserver an. **Hinweis:** Dienstprogrammprüfungen mit dem Präfix „util“ mit obligatorischen Parametern, für die Sie einen Wert angeben müssen. Für diese Parameter sind keine Standardwerte verfügbar.	• app.oracle.metrics-oracle • util.metrics-oracle-query
Self-Healing Events	Führt einen Ping-Befehl zu einem anderen Host aus. Diese Prüfung muss im Proxy-Modus ausgeführt werden.	util.check-ping
Tomcat Events	Überwacht laufende Apache Tomcat-Server Um die Überwachung zu aktivieren, wenn der Tomcat-Prozess aktiv ist, aktivieren Sie die entsprechende Prüfung: • Für Linux: os.linux.check-process • Für Windows: util.check-windows-service Wenn der Tomcat-Service unter einem anderen Namen ausgeführt wird, aktualisieren Sie den Wert des Parameters *service* der Prüfungsinstanz auf den korrekten Wert.	• os.linux.check-process • util.check-windows-service
Tomcat Metrics	Überwacht laufende Apache Tomcat-Server	app.tomcat.metrics-tomcat

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
	Wenn Tomcat-Metriken an einem anderen Port als dem Standardport (9000) ausgeführt werden, aktualisieren Sie den Wert des Parameters *port* der Prüfungsinstanz auf den korrekten Portwert.	
Varnish-Metriken	Überwacht und sammelt Varnish-Metriken. Varnish-Metriken werden in ITOM Agent Client Collector Version 2.3.0 – August 2022, unterstützt, die im ServiceNow Store verfügbar ist. Sie müssen eine Erkennung mithilfe von Anwendungsfingerabdrücken durchführen, bevor Sie Varnish-Prüfungen ausführen. Details finden Sie unter Aktiviert die Ausführung von Varnish-Prüfungen.	
vSphere-Metriken	Überwacht und sammelt Metriken von vSphere. vSphere-Metriken werden in ITOM Agent Client Collector Version 2.3.0 – August 2022, unterstützt, die im ServiceNow Store verfügbar ist. Diese Richtlinie erfordert einen Proxy-Agent.	
WebLogic Application Server Events	Überwacht laufende Oracle WebLogic-Anwendungsserver. Diese Richtlinie überwacht, ob der unter Linux ausgeführte WebLogic-Prozess aktiv ist. Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Anwendungsserver an.	os.linux.check-process
WebLogic Application Server Metrics	Überwacht laufende Oracle WebLogic-Anwendungsserver. Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Anwendungsserver an. Stellen Sie sicher, dass der Benutzer, der den Agent ausführt, über ausreichende Berechtigungen für den Zugriff auf die erforderlichen Dateien in den `WebLogic`-Installationsverzeichnissen verfügt.	app.weblogic.metrics-weblogic

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
WebSphere Application Server Events	Überwacht laufende IBM WebSphere-Server. Diese Richtlinie überwacht, ob der unter Linux ausgeführte WebSphere-Prozess aktiv ist. Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Anwendungsserver an.	os.linux.check-process
WebSphere Application Server Metrics	Überwacht laufende IBM WebSphere-Server. Geben Sie auf der Registerkarte **Credentials** (Anmeldeinformationen) die Anmeldeinformationen der Standardauthentifizierung für die Verbindung zum Anwendungsserver an.	app.websphere.metrics-websphere
Windows Protokollüberwachung	Überwacht Protokolle auf laufenden Windows-Servern.	os.windows.check-log Sie können die Ereigniserstellung für diese Prüfung blockieren, wenn kein Prozess erkannt wird. Details finden Sie unter Ereigniserstellung für nicht vorhandene Entitäten blockieren.
Windows BS-Ereignisse	Führt Windows-Prüfungen auf ausgeführten Windows-Servern aus.	• os.windows.check-processor-queue-length • os.windows.check-system-cpu-load • os.windows.check-system-disk • os.windows.check-system-memory • os.windows.check-system-process • os.windows.check-windows-directory • os.windows.check-windows-directory • os.windows.check-windows-directory

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung	Prüfungen
		• os.windows.check-windows-pagefile • os.windows.check-windows-process
Windows BS-Ereignisse – Erweitert	Führt Windows Prüfungen durch, um Verzeichnisse und Dateien auf den Servern Windows zu überwachen.	• „check-directory-file-count“ • „check-directory-integrity“ • check-file-age • Überprüfe-Datei-Antwortzeit • überprüfe-Dateigröße • check-file-space • os.windows.check-directory-space
Windows BS-Metriken	Sammelt Windows-Metriken auf laufenden Windows-Servern	• os.windows.metrics-processor-queue-len • os.windows.metrics-system-cpu-load • os.windows.metrics-system-disk-usage • os.windows.metrics-system-memory-percent • os.windows.metrics-system-network • os.windows.metrics-system-uptime
Zscaler-Überwachungsrichtlinie	Führt die Zscaler-Überwachung für alle CIs eines Computers aus.	• zscaler-monitoring-check • zscaler-remediation-check

Active Directory-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Active Directory-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
active_dir.DRA_Inbound_Bytes_after_compressed/sec			Zeigt die komprimierte Größe der eingehenden komprimierten Replikationsdaten an (Größe nach der Komprimierung von DSAs in andere Standorte).
active_dir.DRA_Inbound_Bytes_before_compressed/sec			Zeigt die Originalgröße der eingehenden komprimierten Replikationsdaten an (Größe vor der Komprimierung von DSAs in andere Standorte).
active_dir.DRA_Inbound_Bytes_not_compressed/sec			Zeigt die Anzahl der eingehenden replizierten Bytes an, die nicht an der Quelle komprimiert wurden (d. h. von DSAs in den gleichen Standort).
active_dir.DRA_Inbound_Bytes_Total/sec (empfohlene Metrik)			Zeigt die Gesamtzahl der eingehenden replizierten Bytes an. Dieser Zähler ist die Summe der Anzahl unkomprimierter Bytes (nie komprimiert) und der Anzahl komprimierter Bytes (nach der Komprimierung).
active_dir.DRA_Inbound_Full_Sync_Objects_Remaining (empfohlene Metrik)			Zeigt die Anzahl der bis zum Abschluss der vollständigen Synchronisierung verbleibenden Objekte an (falls festgelegt).
active_dir.DRA_Inbound_Object_Updates_Remaining_in_Packet			Zeigt die Anzahl der empfangenen Objektaktualisierungen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			im aktuellen Verzeichnisreplikations-Aktualisierungspaket, die auf den lokalen Server nicht angewendet wurden.
active_dir.DRA_Inbound_Objects/sec			Zeigt die Rate an, zu der Replikationsaktualisierungen von Replikationspartnern vom lokalen Verzeichnisdienst angewendet werden. Bei diesem Zähler werden Änderungen ausgeschlossen, die empfangen, aber nicht angewendet wurden (z. B. weil die Änderung bereits vorgenommen wurde). Diese Metrik gibt an, wie viele Replikationsaktualisierungsaktivitäten auf dem Server aufgrund von Änderungen auftreten, die auf anderen Servern generiert wurden.
active_dir.DRA_Inbound_Objects_Applied/sec			Zeigt die Anzahl der Objekte an, die von eingehenden Replikationspartnern empfangen wurden, aber keine Aktualisierungen enthalten und daher nicht angewendet werden müssen.
active_dir.DRA_Inbound_Objects_Filtered/sec			Zeigt die Anzahl der durch eingehende Replikation von benachbarten Computern

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			empfangenen Objekte. Ein benachbarter Computer ist ein Domänen-Controller, von dem ausgehend der lokale Domänen-Controller eine lokale Replikation durchführt.
active_dir.DRA_Inbound_Properties_Applied/sec			Zeigt die Anzahl der Eigenschaften an, die aktualisiert werden, weil die eingehende Eigenschaft die Abgleichslogik, nach der der endgültige zu replizierende Wert bestimmt wird, erfolgreich durchlaufen hat.
active_dir.DRA_Inbound_Properties_Filtered/sec			Zeigt die Anzahl der während der Replikation empfangenen Eigenschaftsänderungen an, die bereits bekannt sind.
active_dir.DRA_Inbound_Properties_Total/sec			Zeigt die Gesamtanzahl der Objekteigenschaften an, die von eingehenden Replikationspartnern empfangen wurden.
active_dir.DRA_Inbound_Values_DNs/sec			Zeigt die Anzahl der von eingehenden Replikationspartnern empfangenen Objekteigenschaftswerte an, bei denen es sich um Distinguished Names (DNs) handelt, die auf andere Objekte verweisen. DN-Werte, z. B. Gruppen- oder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Verteilerlistenmitgliedschaften, sind meist aufwendiger anzuwenden als andere Werte.
active_dir.DRA_Inbound_Values_Total/sec			Zeigt die Gesamtanzahl der Objekteigenschaftenwerte an, die von eingehenden Replikationspartnern empfangen wurden. Jedes eingehende Objekt hat mindestens eine Eigenschaft, und jede Eigenschaft hat null oder mehr Werte. Der Wert null bedeutet, dass eine Eigenschaften entfernt wird.
active_dir.DRA_Outbound_Bytes_after_compressed/sec			Zeigt die komprimierte Größe der ausgehenden komprimierten Replikationsdaten an (Größe nach der Komprimierung von DSAs in andere Standorte).
active_dir.DRA_Outbound_Bytes_before_compressed/sec			Zeigt die ursprüngliche Größe der ausgehenden komprimierten Replikationsdaten an (Größe vor der Komprimierung von DSAs in andere Standorte).
active_dir.DRA_Outbound_Bytes_not_compressed/sec			Zeigt die Anzahl der ausgehend replizierten Bytes an, die nicht komprimiert wurden (z. B. von DSAs in den gleichen Standort).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
active_dir.DRA_Outbound_Bytes_Total/sec (empfohlene Metrik)			Zeigt die Gesamtanzahl der ausgehenden replizierten Bytes an. Dieser Zähler ist die Summe der Anzahl unkomprimierter Bytes (nie komprimiert) und der Anzahl komprimierter Bytes (nach der Komprimierung).
active_dir.DRA_Outbound_Objects/sec			Zeigt die Anzahl der Objekte an, bei denen durch die ausgehende Replikation ermittelt wurde, dass sie keine Aktualisierungen aufweisen, über die der ausgehende Partner nicht verfügt.
active_dir.DRA_Outbound_Objects_Filtered/sec			Zeigt die Anzahl der ausgehend replizierten Objekte an.
active_dir.DRA_Outbound_Properties/sec			Zeigt die Anzahl der ausgehend replizierten Eigenschaften an.
active_dir.DRA_Outbound_Values_DNs/sec			Zeigt die Anzahl der Objekteigenschaftenwerte an, die DNs enthalten und an ausgehende Replikationspartner gesendet werden. DN-Werte, z. B. Gruppen- oder Verteilerlistenmitgliedschaften, sind zeitaufwendiger zu lesen als andere Werte.
active_dir.DRA_Outbound_Values_Total/sec			Zeigt die Anzahl der Objekteigenschaftenwerte an, die an ausgehende

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Replikationspartner gesendet wurden.
active_dir.DRA_Pending_Replication_Synchronizations			Zeigt die Anzahl der Verzeichnissynchronisierungen an, die sich für diesen Server in der Warteschlange befinden, aber noch nicht verarbeitet wurden.
active_dir.DRA_Sync_Requests_Made			Zeigt die Anzahl der Synchronisierungsanforderungen an benachbarte Computer an.
active_dir.DS_Threads_in_Use (empfohlene Metrik)			Zeigt die aktuelle Anzahl derzeit vom Verzeichnisdienst verwendeter Threads an (dies unterscheidet sich von der Anzahl von Threads im Verzeichnisdienstprozess). Dies ist die Anzahl der Threads, die aktuell von Client-API-Aufrufen verwendet werden, und gibt Aufschluss darüber, ob zusätzliche Prozessoren verwendet werden sollten.
active_dir.LDAP_Bind_Time (empfohlene Metrik)			Zeigt die Dauer (in Millisekunden) der letzten erfolgreichen LDAP-Bindung.
active_dir.LDAP_Client_Sessions (empfohlene Metrik)			Zeigt die Anzahl der derzeit verbundenen LDAP-Client-Sitzungen an.
active_dir.LDAP_Searches/sec (empfohlene Metrik)			Zeigt die Rate der Suchzugriffe von LDAP-Clients an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Active Directory-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
active_dir.LDAP_Successful_Binds/sec (empfohlene Metrik)			Zeigt die Anzahl der LDAP-Bindungen pro Sekunde an.

Apache Kafka – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Richtlinien für die Apache Kafka-Systemüberwachung. Die Richtlinien beinhalten die in der angegebenen Tabelle ausgewiesenen Prüfungen. Richtlinien und Prüfungen sind für Windows und Linuxverfügbar.

Apache Kafka-Themenereignisse

Prüfung	Beschreibung	Verwendung	Ausgabe
kafka.check-zookeeper-status	Löst ein kritisches Ereignis aus, wenn der gehostete ZooKeeper von Apache Kafka ausgefallen ist.	`commonchecks check-kafka-zk-status` [Kennzeichnungen] Mit folgenden Kennzeichnungen: `-p, --port =` ZooKeeper-Port (Standardwert: „2181“). Verwendungsbeispiel: `commonchecks check-kafka-zk-status -p 2181`	Kafka Zookeeper Status OK: Kafka-Zookeeper is Up! (Kafka-ZooKeeper-Status OK: Kafka-ZooKeeper ist aktiv!)
kafka.check-topic-replicas	Löst ein kritisches Ereignis aus, wenn ein Thema Partitionen mit unbekannten Replikaten aufweist.	`commonchecks check-kafka-replicas` [Kennzeichnungen] Mit folgenden Kennzeichnungen: • `-p, --port =` ZooKeeper-Port (Standardwert: „2181“). • `-d, --detailed` = Listet unbekannte Replikate in jeder Partition eines Themas auf.	<topic> has partitions with unknown replicas (<Thema> hat Partitionen mit unbekannten Replikaten.) Unknown replicas are: {"0":["0"],"1":["0"],"2":["0"]} (Unbekannte Replikate sind: {"0":["0"],"1":["0"],"2":["0"]}). <topic> has partitions with unknown replicas (<Thema> hat Partitionen mit unbekannten Replikaten.) Unknown

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-Themenereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung	Ausgabe
		• `-i, --include_list` = Kommagetrennte Liste zum Einbeziehen von Themen („*“ als Platzhalterzeichen zulässig) • `-e, --exclude_list` = Kommagetrennte Liste zum Ausschließen von Themen („*“ als Platzhalterzeichen zulässig) Verwendungsbeispiel: commonchecks check-kafka-replicas -H localhost -p 2181 -i "test*" -e "accTopic,*offsets" -d	replicas are: {"0": ["0"]} (Unbekannte Replikate sind: {"0": ["0"]}).
kafka.check-topic-replication-factor	Löst ein kritisches Ereignis aus, wenn der Replikationsfaktor mindestens eines Themas über oder unter dem angegebenen Replikationsfaktorparame.t. liegt.	`commonchecks check-kafka-rf` [Kennzeichnungen] Mit folgenden Kennzeichnungen: • `-p, --port` = ZooKeeper-Port (Standardwert: „2181“). • `-d, --detailed` = Listet unbekannte Replikate in jeder Partition eines Themas auf. • `-i, --include_list` = Kommagetrennte Liste zum Einbeziehen von Themen („*“ als Platzhalterzeichen zulässig) • `-e, --exclude_list` = Kommagetrennte	TestTopic has replication factor 1, which is less than expected: 2. (TestTopic hat Replikationsfaktor 1, was kleiner ist als erwartet: 2). accMetrics has replication factor 1, which is less than expected: 2. (accMetrics hat Replikationsfaktor 1, was kleiner ist als erwartet: 2).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-Themenereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung	Ausgabe
		Liste zum Ausschließen von Themen („*“ als Platzhalterzeichen zulässig) • `-r, --replication factor` = Erwarteter Replikationsfaktor für ein Thema (Standardwert: 1) Beispiele: `commonchecks check-kafka-partitions -H localhost -p 2181 -r 2 -i "accMetrics,*Topic" -e "testTopic"`	
kafka.check-topic-leader	Löst ein kritisches Ereignis aus, wenn ein Thema Partitionen mit unbekannten führenden Komponenten (Leadern) oder nicht bevorzugten Replikaten als Leader aufweist.	`commonchecks check-kafka-leader` [Kennzeichnungen] Mit folgenden Kennzeichnungen: • `-p, --port` = ZooKeeper-Port (Standardwert: „2181“). • `-d, --detailed` = Eine Liste von Partitionen in jedem Thema mit unbekannten Leadern oder nicht bevorzugten Replikaten. • `-i, --include_list` = Kommagetrennte Liste zum Einbeziehen von Themen („*“ als Platzhalterzeichen zulässig)	<topic> contains, partitions with unpreferred replica as leader. (partitions with unpreferred replicas are [0]). (<Thema> enthält Partitionen mit nicht bevorzugten Replikaten als Leader. (Partitionen mit nicht bevorzugten Replikaten sind [0])). <topic> contains, partitions with unpreferred replica as leader. (partitions with unpreferred replicas are [0]). (<Thema> enthält Partitionen mit nicht bevorzugten Replikaten als Leader. (Partitionen mit nicht bevorzugten Replikaten sind [0])).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-Themenereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung	Ausgabe
		• `-e, --exclude_list` = Kommagetrennte Liste zum Ausschließen von Themen („*“ als Platzhalterzeichen zulässig) Beispiele: `commonchecks check-kafka-leader -H localhost -p 2181 -d -e "*offsets"`	
kafka.check-topic-partitions	Löst kritische Ereignisse aus, wenn die Anzahl der Partitionen für ein Thema kleiner ist als der Parameter min_partitions.	`commonchecks check-kafka-partitions [Kennzeichnungen]` Mit folgenden Kennzeichnungen: • `-p, --port` = ZooKeeper-Port (Standardwert: „2181“). • `-P, --min_partitions` = Mindestanzahl der Partitionen für ein Thema (Standardwert: 1). • `-i, --include_list` = Kommagetrennte Liste zum Einbeziehen von Themen („*“ als Platzhalterzeichen zulässig) • `-e, --exclude_list` = Kommagetrennte Liste zum Ausschließen von	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-Themenereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung	Ausgabe
		Themen („*“ als Platzhalterzeichen zulässig)	
		Verwendungsbeispiel 1: `commonchecks check-kafka-partitions -H localhost -p 2181 -P 3`	<topic> has 1 partitions, expected at least 3 (<Thema> hat 1 Partition, mindestens 3 erwartet). <topic> has 1 partitions, expected at least 3 (<Thema> hat 1 Partition, mindestens 3 erwartet). <topic> has 1 partitions, expected at least 3 (<Thema> hat 1 Partition, mindestens 3 erwartet).
		Verwendungsbeispiel 2: commonchecks check-kafka-partitions -H localhost -p 2181 -P 3 -i "accMetrics,*Topic" -e "testTopic"	<topic> has 1 partitions, expected at least 3 (<Thema> hat 1 Partition, mindestens 3 erwartet). <topic> has 1 partitions, expected at least 3 (<Thema> hat 1 Partition, mindestens 3 erwartet).

Hinweis: Werte für die Parameter include_list und exclude_list müssen in doppelte Anführungszeichen gesetzt werden. Beispiel: "test1,*topic".

Apache Kafka-Broker-Ereignisse

Prüfung	Beschreibung	Verwendung	Ausgabe
kafka.check-broker-status	Löst ein kritisches Ereignis aus, wenn der Kafka-Broker auf dem Host ausgefallen ist.	`commonchecks check-kafka-broker-status` [Kennzeichnungen]	Kafka Broker Status OK: Kafka Broker ubuntu20:9092 is Up! (Kafka-Broker-Status OK: Kafka-Broker

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-Broker-Ereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung	Ausgabe
		Mit folgenden Kennzeichnungen: `-p, --port` = Port des Kafka-Brokers (Standardwert: „9092“). Verwendungsbeispiel: `commonchecks check-kafka-broker-status -p 9092`	ubuntu20:9092 ist aktiv!)

Apache Kafka-Broker-Metriken

Prüfung	Beschreibung	Verwendung	Ausgabe
kafka.metrics.broker	Sammelt Kafka-Broker-Metriken vom Host.	`commonchecks metric-kafka-broker` [Kennzeichnungen] Mit folgenden Kennzeichnungen: • `-J, --javapath` = Pfad der ausführbaren Java-Datei (Standardwert: „java“). • `-j, --jmxport` = JMX-Port (Standardwert: „9999“) Verwendungsbeispiel: `commonchecks metric-kafka-broker -J "/usr/bin/java" -j 9999`	hostname.Kafka.Broker.ReplicaManag 0.000 hostname.Kafka.Broker.DelayedOper 627.000 hostname.Kafka.Broker.ControllerStats 0.000 hostname.Kafka.Broker.RequestMetric 0.000

Apache Kafka-ZooKeeper-Metriken

Prüfung	Beschreibung	Verwendung	Ausgabe
kafka.metrics.zookeeper	Sammelt ZooKeeper-Metriken vom Host.	`commonchecks metric-kafka-zookeeper` [Kennzeichnungen]	hostname.Kafka.Zookeeper.outstandi 2.000 1648183249 hostname.Kafka.Zookeeper.avg_later 1.05 1648183249

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Apache Kafka-ZooKeeper-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung	Ausgabe
		Mit folgender Kennzeichnung: `-p, --adminserverport` = Port des Verwaltungsservers (Standardwert: „8085“) Verwendungsbeispiel: `commonchecks metric-kafka-zookeeper -p 8085`	hostname.Kafka.Zookeeper.num_alive 1.000 1648183249 hostname.Kafka.Zookeeper.open_file 124.000 1648183249

Apache Kafka-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Kafka-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Broker-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
Kafka.Broker.RequestMetrics.TotalTimeMs.FetchConsumer.Mean (empfohlene Metrik)			Gesamtzeit (in ms) für die Verarbeitung der Consumer-Anforderung.
Kafka.Broker.RequestMetrics.TotalTimeMs.FetchFollower.Mean (empfohlene Metrik)			Gesamtzeit (in ms) für die Verarbeitung der Follower-Anforderung.
Kafka.Broker.RequestMetrics.TotalTimeMs.Produce.Mean (empfohlene Metrik)			Gesamtzeit (in ms) für die Verarbeitung der Producer-Anforderung.
Kafka.Broker.BrokerTopicMetrics.BytesOutPerSec.OneMinuteRate (empfohlene Metrik)			Zusammengefasste ausgehende Byterate.
Kafka.Broker.BrokerTopicMetrics.BytesInPerSec.OneMinuteRate (empfohlene Metrik)			Zusammengefasste eingehende Byterate.
Kafka.Broker.ReplicaManager.UnderReplicatedPartitions.Value			Anzahl der nicht replizierten Partitionen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Broker-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
Kafka.Broker.ReplicaManager.IsrExpandsPerSec.OneMinuteRate			Rate, mit der der Pool der synchronen Replikate (In-Sync Replicas, ISRs) kleiner wird.
Kafka.Broker.ReplicaManager.IsrShrinksPerSec.OneMinuteRate			Rate, mit der der Pool der synchronen Replikate (In-Sync Replicas, ISRs) kleiner wird.
Kafka.Broker.KafkaController.ActiveControllerCount.Value (empfohlene Metrik)			Anzahl der aktiven Controller im Cluster.
Kafka.Broker.KafkaController.OfflinePartitionsCount.Value			Anzahl der Offline-Partitionen.
Kafka.Broker.ControllerStats.LeaderElectionRateAndTimeMs.OneMinuteRate (empfohlene Metrik)			Leader-Wahlrate und -Latenz.
Kafka.Broker.ControllerStats.UncleanLeaderElectionsPerSec.OneMinuteRate			Anzahl der nicht bereinigten Auswahlen pro Sekunde.
Kafka.Broker.DelayedOperationPurgatory.PurgatorySize.Fetch.Value			Anzahl der Abrufanforderungen, die in der als „Purgatory“ (Fegefeuer) bezeichneten Datenstruktur von Kafka warten.
Kafka.Broker.DelayedOperationPurgatory.PurgatorySize.Produce.Value			Anzahl der Anforderungen, die in der als Producer-„Purgatory“ (Fegefeuer) bezeichneten Datenstruktur von Kafka warten.
Kafka.Broker.RequestMetrics.RequestsPerSec.Produce.OneMinuteRate (empfohlene Metrik)			Anzahl der Producer-Anforderungen pro Sekunde.
Kafka.Broker.RequestMetrics.RequestsPerSec.FetchConsumer.OneMinuteRate (empfohlene Metrik)			Anzahl der Consumer-Anforderungen pro Sekunde.
Kafka.Broker.RequestMetrics.RequestsPerSec.FetchFollower.OneMinuteRate (empfohlene Metrik)			Anzahl der Follower-Anforderungen pro Sekunde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ZooKeeper-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
Kafka.Zookeeper.outstanding_requests (empfohlene Metrik)			Anzahl der Anforderungen in der Warteschlange.
Kafka.Zookeeper.avg_latency (empfohlene Metrik)			Durchschnittliche Zeit (in ms), die für die Beantwortung einer Client-Anforderung benötigt wird.
Kafka.Zookeeper.num_alive_connections (empfohlene Metrik)			Anzahl der mit ZooKeeper verbundenen Clients.
Kafka.Zookeeper.open_file_descriptor_count			Anzahl der verwendeten Dateideskriptoren.
Kafka.Zookeeper.pending_syncs			Anzahl der ausstehenden Synchronisierungen von Followern.
Kafka.Zookeeper.followers			Anzahl der aktiven Follower.

AWS-Systemüberwachung – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für AWS-Monitoring.

AWS-Metrikenrichtlinie

Typ	Prüfung	Beschreibung	Verwendung	Verwendungsbeispi
Metrik	aws.metrics-ec2	Gibt Metriken aller EC2-Instanzen in einem AWS-Rechenzentrum zurück	metrics-ec2.rb (Optionen) -F, --filter FILTER Zeichenfolgendars' des Filters zum Filtern von EC2-Instanzen nach Tags. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Instanzen, von denen Metriken parallel	`./metrics-ec2.rb -F "{name:tag:environment,valu [ENV1,ENV2]} "{name:tag:Name,values: [Instance1,Instance2]}"` Geben Sie die Filterzeichenfolge mit doppelten Anführungszeichen ("") um den Filterparameter an. Legen Sie den Parameter

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Metrikenrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Verwendungsbeispi
			abgerufen werden. (Standardwert: 10)	*batch_size* entsprechend der Agent-Umgebung fest.
Metrik	aws.metrics-ebs	Gibt Metriken aller EBS-Volumes in einem AWS-Rechenzentrum zurück	metrics-ebs.rb (Optionen) -F, --filter FILTER Zeichenfolgendarstellung des Filters zum Filtern von EBS-Volumes nach Tags. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Volumes, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	`./metrics-ebs.rb -F "{name:tag:environment,valu [ENV1,ENV2]} {name:tag:Name,values: [Volume1,Volume2]}"` Geben Sie die Filterzeichenfolge mit doppelten Anführungszeichen ("") um den Filterparameter an. Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest.
Metrik	aws.metrics-s3	Gibt Metriken aller S3-Buckets in einem AWS-Rechenzentrum zurück	metrics-s3.rb (Optionen) -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der S3-Buckets, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	`./metrics-s3.rb -b 5` Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest.
Metrik	aws.metrics-rds	Gibt Metriken aller RDS-Buckets in einem AWS-Rechenzentrum zurück	metrics-rds.rb (Optionen) -F, --filter FILTER Zeichenfolgendarstellung des Filters zum Filtern von RDS-Instanzen nach Tags.	`./metrics-rds.rb -F "{name:tag:environment,valu [ENV1,ENV2]} {name:tag:engine,values: [MariaDB]}"` Geben Sie die Filterzeichenfolge mit doppelten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Metrikenrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Verwendungsbeispi
			-b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Datenbanken, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	Anführungszeichen ("") um den Filterparameter an. Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest.
Metrik	aws.metrics-classic-elb	Gibt Metriken aller klassischen elastischen Lastenausgleichsmodule in einem AWS-Rechenzentrum zurück	metrics-elb.rb (Optionen) -e, --exclude_lb EXCLUDE_LB Metriken von Lastenausgleichsmodulen ausschließen, deren Name eine der durch Kommas getrennten Zeichenfolgen enthält. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Datenbanken, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	`./metrics-elb.rb -t classic -e "classic,itom,ip" -b 10` Geben Sie kommagetrennte Zeichenfolgen in doppelten Anführungszeichen ("") für den Parameter *exclude_lb* an. Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest.
Metrik	aws.metrics-network-elb	Gibt Metriken aller elastischen Netzwerk-Lastenausgleichsmodule in einem AWS-Rechenzentrum zurück	metrics-elb.rb (Optionen) -e, --exclude_lb EXCLUDE_LB Metriken von Lastenausgleichsmodulen ausschließen, deren Name eine der durch Kommas getrennten	`./metrics-elb.rb -t network -e "vpc,itom,ip" -b 10` Geben Sie kommagetrennte Zeichenfolgen in doppelten Anführungszeichen ("") für den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Metrikenrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Verwendungsbeispi
			Zeichenfolgen enthält. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Datenbanken, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	Parameter *exclude_lb* an. Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest. Ändern Sie das Befehlspräfix nicht.
Metrik	aws.metrics-application-elb	Gibt Metriken aller elastischen Anwendungs-Lastenausgleichsmodule in einem AWS-Rechenzentrum zurück	metrics-elb.rb (Optionen) -e, --exclude_lb EXCLUDE_LB Metriken von Lastenausgleichsmodulen ausschließen, deren Name eine der durch Kommas getrennten Zeichenfolgen enthält. -b, --batch_size BATCH_SIZE Batch-Größe. Anzahl der Datenbanken, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	`./metrics-elb.rb -t application -e "classic,app,ip" -b 10` Geben Sie kommagetrennte Zeichenfolgen in doppelten Anführungszeichen ("") für den Parameter *exclude_lb* an. Legen Sie den Parameter *batch_size* entsprechend der Agent-Umgebung fest. Ändern Sie das Befehlspräfix nicht.

Metrik	aws.metrics-ec2-count	Gibt die Anzahl der EC2-Instanzen nach instance_type oder Status in einem AWS-Rechenzentrum zurück	metrics-ec2-count.rb (Optionen)
			
			-s, --scheme SCHEME Metrikbenennungs-Text, der der Metrik vorangestellt
				`./metrics-ec2-count.rb -t status`
				
				`./metrics-ec2-count.rb -t status -s metric.aws.ec2`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Metrikenrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Verwendungsbeispi
			werden soll. Standard: aws.ec2 -t, --typ METRIC-Typ Anzahl nach Typ: Status, Instanz. Standard: Instanz	

AWS DynamoDB-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Befehl
Metrik	aws.metrics-dynamodb	Überwacht die Integrität von DynamoDB-Tabellen in einem AWS-Rechenzentrum. Wird mit der DynamoDB-Tabelle (cmdb_ci_dynamodb_table) verbunden	e, --exclude_tb EXCLUDE_TB Schließen Sie Metriken aus Tabellen aus, deren Name eine der durch Kommas getrennten Zeichenfolgen enthält. b, --batch_size BATCH_SIZE Batchgröße. Anzahl der Tabellen, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	`metrics-dynamodb.rb -r {{.labels.params_ci_region}} {{.labels.params_exclude_tb -f {{.labels.params_exclude_tb {{end}} {{.labels.params_batch_size -b {{.labels.params_filter}} {{end}}`

AWS EC2-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Befehl
Metrik	aws.metrics-ecs-cluster	Überwacht ECS-Cluster in einem AWS-Rechenzentrum. Wird mit dem AWS ECS Cluster-CI-Typ	-F, --filter FILTER Zeichenfolgendarstellung des Filters zum Filtern von ECS-Clustern nach Tags.	`metrics-ecs-cluster.rb -r {{.labels.params_ci_region} {{.labels.params_filter}} -f {{.labels.params_filter}} {{end}} {{.labels.params_batch_size`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS EC2-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Befehl
		(cmdb_ci_cloud_ecs_cluster) verbunden	-b, --batch_size BATCH_SIZE Batchgröße. Anzahl der Cluster, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	`-b {{.labels.params_filter}} {{end}}`
Metrik	aws.metrics-ecs-service	Überwacht ECS-Services in einem AWS-Rechenzentrum. Wird mit dem AWS ECS Service-CI-Typ (cmdb_ci_cloud_ecs_service) verbunden	-F, --filter FILTER Zeichenfolgendarstellung des Filters zum Filtern von ECS-Clustern nach Tags. -b, --batch_size BATCH_SIZE Batchgröße. Anzahl der Cluster, von denen Metriken parallel abgerufen werden. (Standardwert: 10)	`metrics-ecs-service.rb -r {{.labels.params_ci_region}} {{.labels.params_filter}} -f {{.labels.params_filter}} {{end}} {{.labels.params_batch_size -b {{.labels.params_filter}} {{end}}`

Zugehörige Informationen

AWS-Metriken

AWS-Metriken

In den folgenden Tabellen werden die Metriken aufgelistet und beschrieben, die als Ausgabe von den angegebenen AWS-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

aws.metrics-ec2-Metriken

Metrikname	Beschreibung
aws.ec2.CPUCreditBalance.Average	Anzahl der verdienten CPU-Guthaben, die eine Instanz seit dem Start gesammelt hat

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ec2-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.ec2.CPUUtilization.Average	Durchschnittlicher Prozentsatz der zugewiesenen EC2-Recheneinheiten, die derzeit in der Instanz verwendet werden
aws.ec2.DiskReadOps.Average (Empfohlene Metrik)	Durchschnitt der abgeschlossenen Lesevorgänge aus allen Instanzspeicher-Volumes, die für die Instanz in einem angegebenen Zeitraum verfügbar sind
aws.ec2.DiskWriteOps.Average (Empfohlene Metrik)	Abgeschlossene Schreibvorgänge in allen Instanzspeicher-Volumes, die für die Instanz in einem angegebenen Zeitraum verfügbar sind
aws.ec2.DiskReadBytes.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der gelesenen Bytes aus allen für die Instanz verfügbaren Instanzspeicher-Volumes
aws.ec2.DiskWriteBytes.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der geschriebenen Bytes in allen für die Instanz verfügbaren Instanzspeicher-Volumes
aws.ec2.NetworkIn.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der über alle Netzwerkschnittstellen von der Instanz empfangenen Byte. Diese Metrik identifiziert das Volumen des eingehenden Netzwerkdatenverkehrs für eine einzelne Instanz.
aws.ec2.NetworkOut.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der über alle Netzwerkschnittstellen von der Instanz gesendeten Byte. Diese Metrik identifiziert das Volumen des ausgehenden Netzwerkdatenverkehrs einer einzelnen Instanz.
aws.ec2.NetworkPacketsIn.Average	Durchschnittliche Anzahl der über alle Netzwerkschnittstellen von der Instanz empfangenen Pakete. Diese Metrik identifiziert das Volumen des eingehenden Netzwerkdatenverkehrs als Anzahl der Pakete für eine einzelne Instanz.
aws.ec2.NetworkPacketsOut.Average	Durchschnittliche Anzahl der über alle Netzwerkschnittstellen von der Instanz gesendeten Pakete. Diese Metrik identifiziert das Volumen des ausgehenden Netzwerkdatenverkehrs als Anzahl der Pakete für eine einzelne Instanz.
aws.ec2.MetadataNoToken.Average	Durchschnittliche Anzahl der erfolgreichen Zugriffe auf den Instanzmetadatenservice mit einer Methode, die kein Token verwendet

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ec2-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.ec2.CPUCreditUsage.Average	Durchschnittliche Anzahl der von der Instanz für die CPU-Auslastung ausgegebenen CPU-Guthaben
aws.ec2.CPUSurplusCreditBalance.Average	Durchschnittliche Anzahl der überschüssigen Guthaben, die von einer unbegrenzten Instanz ausgegeben wurden, wenn ihr Wert für `CPUCreditBalance` null ist
aws.ec2.CPUSurplusCreditsCharged.Average	Durchschnittliche Anzahl der ausgegebenen überschüssigen Guthaben, die nicht durch verdiente CPU-Guthaben abgegolten werden und daher eine zusätzliche Gebühr verursachen
aws.ec2.StatusCheckFailed_Instance.Average	Meldet, ob die Instanz die Instanzstatusprüfung in der letzten Minute bestanden hat
aws.ec2.StatusCheckFailed_System.Average	Meldet, ob die Instanz die Systemstatusprüfung in der letzten Minute bestanden hat
aws.ec2.StatusCheckFailed.Average	Meldet, ob die Instanz die Instanzstatusprüfung und die Systemstatusprüfung in der letzten Minute bestanden hat

aws.metrics-ebs-Metriken

Metrikname	Beschreibung
aws.ebs.VolumeReadBytes.Average (Empfohlene Metrik)	Durchschnittliche Gesamtanzahl der während der Lesevorgänge im Zeitraum übertragenen Bytes
aws.ebs.VolumeWriteBytes.Average (Empfohlene Metrik)	Durchschnittliche Gesamtanzahl der während der Schreibvorgänge im Zeitraum übertragenen Bytes
aws.ebs.VolumeReadOps.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der Lesevorgänge in einem angegebenen Zeitraum
aws.ebs.VolumeWriteOps.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der Schreibvorgänge in einem angegebenen Zeitraum
aws.ebs.VolumeTotalReadTime.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der Sekunden, die alle Lesevorgänge in einem angegebenen Zeitraum benötigt haben
aws.ebs.VolumeTotalWriteTime.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der Sekunden, die alle Schreibvorgänge in einem angegebenen Zeitraum benötigt haben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ebs-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.ebs.VolumeIdleTime.Average	Durchschnittliche Gesamtzahl der Sekunden in einem angegebenen Zeitraum, in denen keine Lese- oder Schreibvorgänge übermittelt wurden
aws.ebs.VolumeQueueLength.Average	Durchschnittliche Anzahl von Lese- und Schreibvorgangsanforderungen, die in einem angegebenen Zeitraum auf den Abschluss warten
aws.ebs.VolumeThroughputPercentage.Average	Durchschnittlicher Prozentsatz der gelieferten E/A-Vorgänge pro Sekunde (IOPS) der gesamten für ein Amazon EBS-Volume bereitgestellten IOPS
aws.ebs.VolumeConsumedReadWriteOps.Average	Durchschnittliche Gesamtmenge der in einem angegebenen Zeitraum verbrauchten Lese- und Schreibvorgänge (normalisiert auf 256.000 Kapazitätseinheiten)
aws.ebs.BurstBalance.Average	Durchschnittlicher Prozentsatz der im Burst-Bucket verbleibenden E/A-Guthaben (für gp2) oder Durchsatz-Guthaben (für st1 und sc1)

aws.metrics-s3-Metriken

Metrikname	Beschreibung
aws.s3.NumberOfObjects.Average (Empfohlene Metrik)	Durchschnittliche Gesamtanzahl der in einem Bucket gespeicherten Objekte für alle Speicherklassen. Alle 12 Stunden erfasst
aws.s3.BucketSizeBytes.Average (Empfohlene Metrik)	Durchschnittliche Datenmenge in Byte, die in einem Bucket in der Speicherklasse STANDARD gespeichert ist. Alle 12 Stunden erfasst

aws.metrics-rds-Metriken

Metrikname	Beschreibung
aws.rds.BinLogDiskUsage.Average	Durchschnittliche Menge des von Protokollen von Binärdateien belegten Speicherplatzes auf dem primären Speicher. Gilt für MySQL-Lesereplikate
aws.rds.BurstBalance.Average	Durchschnittlicher Prozentsatz der verfügbaren Burst-Bucket-E/A-Guthaben für Allzweck-SSDs (gp2)
aws.rds.CPUUtilization.Average	Durchschnittliche CPU-Auslastung in Prozent

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-rds-Metriken (Fortsetzung)

Metrikname	Beschreibung
(Empfohlene Metrik)	
aws.rds.CPUCreditUsage.Average	Durchschnittliche Anzahl der von der Instanz für die CPU-Auslastung ausgegebenen CPU-Guthaben
aws.rds.CPUCreditBalance.Average	Durchschnittliche Anzahl der überschüssigen Guthaben, die von einer unbegrenzten Instanz ausgegeben wurden, wenn ihr Wert für *CPUCreditBalance* null ist
aws.rds.DatabaseConnections.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der verwendeten Datenbankverbindungen
aws.rds.DiskQueueDepth.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der ausstehenden E/A-Anforderungen (Lese-/Schreibanforderungen), die auf den Zugriff auf das Laufwerk warten
aws.rds.EBSByteBalance%.Average	Durchschnittlicher Prozentsatz der verbleibenden Durchsatzguthaben im Burst-Bucket Ihrer RDS-Datenbank
aws.rds.EBSIOBalance%.Average	Durchschnittlicher Prozentsatz der verbleibenden E/A-Guthaben im Burst-Bucket Ihrer RDS-Datenbank
aws.rds.FailedSQLServerAgentJobsCount.Average (Empfohlene Metrik)	Durchschnittliche Anzahl der fehlgeschlagenen Microsoft SQL Server Agent-Aufträge in der letzten Minute
aws.rds.FreeableMemory.Average (Empfohlene Metrik)	Durchschnittliche Menge des verfügbaren Arbeitsspeichers
aws.rds.FreeStorageSpace.Average	Durchschnittliche Menge des verfügbaren Speicherplatzes
aws.rds.MaximumUsedTransactionIDs.Average	Durchschnittliche Anzahl der verwendeten maximalen Transaktions-IDs. Gilt für PostgreSQL
aws.rds.NetworkReceiveThroughput.Average (Empfohlene Metrik)	Durchschnittlicher eingehender (empfangener) Netzwerkdatenverkehr in der DB-Instanz, einschließlich des Datenverkehrs der Kundendatenbank und des Amazon RDS-Datenverkehrs, der für Überwachung und Replikation verwendet wird
aws.rds.NetworkTransmitThroughput.Average (Empfohlene Metrik)	Durchschnittlicher ausgehender (gesendeter) Netzwerkdatenverkehr in der DB-Instanz, einschließlich des Datenverkehrs der Kundendatenbank und des Amazon RDS-Datenverkehrs, der für Überwachung und Replikation verwendet wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-rds-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.rds.OldestReplicationSlotLag.Average	Durchschnittliche Verzögerungsgröße des Replikats mit der größten Verzögerung hinsichtlich der empfangenen Write-Ahead-Protokolldaten (WAL-Daten) Gilt für PostgreSQL
aws.rds.ReadIOPS.Average	Durchschnittliche Anzahl der Laufwerks-E/A-Lesevorgänge pro Sekunde
aws.rds.ReadLatency.Average (Empfohlene Metrik)	Durchschnittliche Zeit, die pro Laufwerks-E/A-Vorgang benötigt wird
aws.rds.ReadThroughput.Average	Durchschnittliche Anzahl der pro Sekunde vom Laufwerk gelesenen Byte
aws.rds.ReplicaLag.Average	Durchschnittliche Zeit, die eine Lese-Replikat-DB-Instanz hinter der Quell-DB-Instanz zurückliegt. Gilt für Lesereplikate von MySQL, MariaDB, Oracle, PostgreSQL und SQL Server
aws.rds.ReplicationSlotDiskUsage.Average	Durchschnittliche Menge des von Replikations-Slot-Dateien verwendeten Speicherplatzes Gilt für PostgreSQL
aws.rds.SwapUsage.Average	Durchschnittliche Menge des in der DB-Instanz verwendeten Swap-Bereichs. Diese Metrik ist für SQL Server nicht verfügbar.
aws.rds.TransactionLogsDiskUsage.Average	Durchschnittlicher von Transaktionsprotokollen verwendeter Speicherplatz Gilt für PostgreSQL
aws.rds.TransactionLogsGeneration.Average	Durchschnittliche Größe der pro Sekunde generierten Transaktionsprotokolle. Gilt für PostgreSQL
aws.rds.WriteIOPS.Average	Durchschnittliche Anzahl der Laufwerks-E/A-Schreibvorgänge pro Sekunde
aws.rds.WriteLatency.Average (Empfohlene Metrik)	Durchschnittliche Zeit, die pro Laufwerks-E/A-Vorgang benötigt wird
aws.rds.WriteThroughput.Average	Durchschnittliche Anzahl der pro Sekunde auf das Laufwerk geschriebenen Byte
aws.rds.CPUSurplusCreditBalance.Average	Durchschnittliche Anzahl der überschüssigen Guthaben, die von einer unbegrenzten Instanz ausgegeben wurden, wenn ihr Wert für `CPUCreditBalance` null ist
aws.rds.CPUSurplusCreditsCharged.Average	Durchschnittliche Anzahl der ausgegebenen überschüssigen Guthaben, die nicht durch verdiente CPU-Guthaben abgegolten werden und daher eine zusätzliche Gebühr verursachen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-classic-elb-Metriken

Metrikname	Beschreibung
aws.classicElb.EstimatedALBActiveConnectionCount.Average (Empfohlene Metrik)	Durchschnittliche geschätzte Anzahl gleichzeitiger aktiver TCP-Verbindungen von Clients zum Lastenausgleichsmodul und vom Lastenausgleichsmodul zu Zielen
aws.classicElb.EstimatedALBConsumedLCUs.Average	Durchschnittliche geschätzte Anzahl der von einem Lastenausgleichsmodul für Anwendungen verwendeten Lastenausgleichsmodul-Kapazitätseinheiten (Load Balancer Capacity Units, LCU). Sie zahlen für die Anzahl der pro Stunde verwendeten LCUs.
aws.classicElb.EstimatedALBNewConnectionCount.Average (Empfohlene Metrik)	Durchschnittliche geschätzte Anzahl neuer TCP-Verbindungen die von Clients zum Lastenausgleichsmodul und vom Lastenausgleichsmodul zu Zielen hergestellt werden
aws.classicElb.EstimatedProcessedBytes.Average	Geschätzte Anzahl von Bytes, die von einem Lastenausgleichsmodul für Anwendungen verarbeitet werden
aws.classicElb.DesyncMitigationMode_NonCompliant_Request_Count.Sum	Anzahl der Anforderungen, die nicht RFC 7230 entsprechen
aws.classicElb.HTTPCode_ELB_5XX.Sum (Empfohlene Metrik)	Anzahl der vom Lastenausgleichsmodul generierten HTTP 4XX-Client-Fehlercodes
aws.classicElb.HTTPCode_ELB_4XX.Sum (Empfohlene Metrik)	Anzahl der vom Lastenausgleichsmodul generierten HTTP 5XX-Server-Fehlercodes
aws.classicElb.SurgeQueueLength.Maximum	Maximale Gesamtanzahl der Anforderungen (HTTP-Listener) oder Verbindungen (TCP-Listener), für die die Weiterleitung an eine fehlerfreie Instanz aussteht. Die maximale Größe der Warteschlange beträgt 1.024. Zusätzliche Anforderungen oder Verbindungen werden abgelehnt, wenn die Warteschlange voll ist.
aws.classicElb.SpilloverCount.Sum (Empfohlene Metrik)	Gesamtzahl der Anforderungen, die abgelehnt wurden, da die Warteschlange für Anforderungswellen (Surge Queue) voll ist
aws.classicElb.RequestCount.Sum	Gesamtzahl der während des angegebenen Intervalls abgeschlossenen Anforderungen oder hergestellten Verbindungen
aws.classicElb.Latency.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzeit in Sekunden seit dem Zeitpunkt, zu dem das Lastenausgleichsmodul die Anforderung an eine registrierte Instanz gesendet hat, bis die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-classic-elb-Metriken (Fortsetzung)

Metrikname	Beschreibung
	Instanz mit dem Senden der Antwortheader begonnen hat
aws.classicElb.BackendConnectionErrors.Sum (Empfohlene Metrik)	Gesamtzahl der Verbindungen, die zwischen dem Lastenausgleichsmodul und den registrierten Instanzen nicht erfolgreich hergestellt wurden
aws.classicElb.HealthyHostCount.Average	Durchschnittliche Anzahl der beim Lastenausgleichsmodul registrierten fehlerfreien Instanzen. Eine neu registrierte Instanz gilt als fehlerfrei, nachdem sie die erste Integritätsprüfung bestanden hat.
aws.classicElb.UnHealthyHostCount.Average	Durchschnittliche Anzahl der beim Lastenausgleichsmodul registrierten fehlerhaften Instanzen. Eine Instanz gilt als fehlerhaft, nachdem sie den für Integritätsprüfungen konfigurierten Schwellenwert für den Status „fehlerhaft“ überschritten hat.

aws.metrics-network-elb

Metrikname	Beschreibung
aws.networkElb.ActiveFlowCount.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der gleichzeitigen Flows (oder Verbindungen) von Clients zu Zielen. Diese Metrik schließt Verbindungen in den Status SYN_SENT und ESTABLISHED ein.
aws.networkElb.ActiveFlowCount_TCP.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der gleichzeitigen TCP-Flows (oder Verbindungen) von Clients zu Zielen. Diese Metrik enthält nur Verbindungen im Status ESTABLISHED.
aws.networkElb.ActiveFlowCount_TLS.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der gleichzeitigen TLS-Flows (oder Verbindungen) von Clients zu Zielen. Diese Metrik enthält nur Verbindungen im Status ESTABLISHED.
aws.networkElb.ActiveFlowCount_UDP.Average (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der gleichzeitigen UDP-Flows (oder Verbindungen) von Clients zu Zielen
aws.networkElb.ClientTLSNegotiationErrorCount.Sum (Empfohlene Metrik)	Durchschnittliche Gesamtzahl der TLS-Handshakes, die während der Aushandlung zwischen einem Client und einem TLS-Listener fehlgeschlagen sind
aws.networkElb.ConsumedLCUs.Average	Durchschnittliche Anzahl der vom Lastenausgleichsmodul verwendeten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-network-elb (Fortsetzung)

Metrikname	Beschreibung
	Lastenausgleichsmodul-Kapazitätseinheiten (LCU)
aws.networkElb.ConsumedLCUs_TCP.Average	Durchschnittliche Anzahl der vom Lastenausgleichsmodul für TCP verwendeten Lastenausgleichsmodul-Kapazitätseinheiten (LCU)
aws.networkElb.ConsumedLCUs_TLS.Average	Durchschnittliche Anzahl der vom Lastenausgleichsmodul für TLS verwendeten Lastenausgleichsmodul-Kapazitätseinheiten (LCU)
aws.networkElb.ConsumedLCUs_UDP.Average	Durchschnittliche Anzahl der vom Lastenausgleichsmodul für UDP verwendeten Lastenausgleichsmodul-Kapazitätseinheiten (LCU)
aws.networkElb.HealthyHostCount.Maximum (Empfohlene Metrik)	Die maximale Anzahl von Zielen, die als fehlerfrei gelten
aws.networkElb.NewFlowCount.Sum (Empfohlene Metrik)	Gesamtzahl der neuen Flows (oder Verbindungen), die von Clients zu Zielen im Zeitraum hergestellt wurden
aws.networkElb.NewFlowCount_TCP.Sum (Empfohlene Metrik)	Gesamtzahl der neuen TCP-Flows (oder Verbindungen), die von Clients zu Zielen im Zeitraum hergestellt wurden
aws.networkElb.NewFlowCount_TLS.Sum (Empfohlene Metrik)	Gesamtzahl der neuen TLS-Flows (oder Verbindungen), die von Clients zu Zielen im Zeitraum hergestellt wurden
aws.networkElb.NewFlowCount_UDP.Sum (Empfohlene Metrik)	Gesamtzahl der neuen UDP-Flows (oder Verbindungen), die von Clients zu Zielen im Zeitraum hergestellt wurden
aws.networkElb.PeakBytesPerSecond.Maximum (Empfohlene Metrik)	Maximaler durchschnittlicher Durchsatz (Byte pro Sekunde), berechnet während des Stichprobenfensters alle 10 Sekunden. Diese Metrik enthält Datenverkehr zur Integritätsprüfung.
aws.networkElb.PeakPacketsPerSecond.Maximum (Empfohlene Metrik)	Maximale durchschnittliche Paketrate (verarbeitete Pakete pro Sekunde), berechnet während des Stichprobenfensters alle 10 Sekunden. Diese Metrik enthält Datenverkehr zur Integritätsprüfung.
aws.networkElb.ProcessedBytes.Sum	Gesamtzahl der vom Lastenausgleichsmodul verarbeiteten Byte, einschließlich TCP/IP-Header. Diese Anzahl umfasst den Datenverkehr von und zu Zielen, abzüglich des Datenverkehrs der Integritätsprüfung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-network-elb (Fortsetzung)

Metrikname	Beschreibung
aws.networkElb.ProcessedBytes_TCP.Sum	Gesamtanzahl der von TCP-Listenern verarbeiteten Bytes
aws.networkElb.ProcessedBytes_TLS.Sum	Gesamtanzahl der von TLS-Listenern verarbeiteten Bytes
aws.networkElb.ProcessedBytes_UDP.Sum	Gesamtanzahl der von UDP-Listenern verarbeiteten Bytes
aws.networkElb.ProcessedPackets.Sum	Gesamtzahl der vom Lastenausgleichsmodul verarbeiteten Pakete. Diese Anzahl umfasst den Datenverkehr von und zu Zielen, einschließlich des Datenverkehrs der Integritätsprüfung.
aws.networkElb.TargetTLSNegotiationErrorCount.Sum (Empfohlene Metrik)	Gesamtzahl der TLS-Handshakes, die während der Aushandlung zwischen einem TLS-Listener und einem Ziel fehlgeschlagen sind
aws.networkElb.TCP_Client_Reset_Count.Sum	Gesamtzahl der Reset(RST)-Pakete, die von einem Client an ein Ziel gesendet wurden. Diese Zurücksetzungen werden vom Client generiert und vom Lastenausgleichsmodul weitergeleitet.
aws.networkElb.TCP_ELB_Reset_Count.Sum	Gesamtzahl der vom Lastenausgleichsmodul generierten Reset(RST)-Pakete
aws.networkElb.TCP_Target_Reset_Count.Sum	Gesamtzahl der Reset(RST)-Pakete, die von einem Ziel an einen Client gesendet wurden. Diese Zurücksetzungen werden vom Ziel generiert und vom Lastenausgleichsmodul weitergeleitet.
aws.networkElb.UnHealthyHostCount.Maximum (Empfohlene Metrik)	Die maximale Anzahl von Zielen, die als fehlerhaft gelten

aws.metrics-application-elb-Metriken

Metrikname	Beschreibung
aws.applicationElb.ActiveConnectionCount.Sum (Empfohlene Metrik)	Gesamtzahl gleichzeitiger aktiver TCP-Verbindungen von Clients zum Lastenausgleichsmodul und vom Lastenausgleichsmodul zu Zielen
aws.applicationElb.ClientTLSNegotiationErrorCount.Sum (Empfohlene Metrik)	Gesamtzahl der vom Client initiierten TLS-Verbindungen, von denen aufgrund eines TLS-Fehlers keine Sitzung mit dem Lastenausgleichsmodul hergestellt wurden
aws.applicationElb.ConsumedLCUs.Average	Durchschnittliche Anzahl der vom Lastenausgleichsmodul verwendeten Lastenausgleichsmodul-Kapazitätseinheiten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-application-elb-Metriken (Fortsetzung)

Metrikname	Beschreibung
	(LCU). Sie zahlen für die Anzahl der pro Stunde verwendeten LCUs. Weitere Informationen finden Sie unter „Preise für Elastic Load Balancing“.
aws.applicationElb.DesyncMitigationMode_NonCompliant_Request_Count.Sum (Empfohlene Metrik)	Gesamtzahl der Anforderungen, die nicht RFC 7230 entsprechen
aws.applicationElb.DroppedInvalidHeaderRequestCount.Average (Empfohlene Metrik)	Durchschnittliche Anzahl von Anforderungen, bei denen vom Lastenausgleichsmodul vor der Weiterleitung der Anforderung HTTP-Header mit ungültigen Headerfeldern entfernt wurden. Vom Lastenausgleichsmodul werden diese Header nur entfernt, wenn das Attribut routing.http.drop_invalid_header_fields.enabled auf „true“ festgelegt ist.
aws.applicationElb.ForwardedInvalidHeaderRequestCount.Average (Empfohlene Metrik)	Durchschnittliche Anzahl von Anforderungen, die vom Lastenausgleichsmodul weitergeleitet wurden und HTTP-Header mit ungültigen Headerfeldern aufwiesen. Vom Lastenausgleichsmodul werden Anforderungen mit solchen Headern nur weitergeleitet, wenn das Attribut routing.http.drop_invalid_header_fields.enabled auf „false“ festgelegt ist.
aws.applicationElb.GrpcRequestCount.Sum	Gesamtzahl der über IPv4 und IPv6 verarbeiteten gRPC-Anforderungen
aws.applicationElb.HTTP_Fixed_Response_Count.Sum	Gesamtzahl der erfolgreichen Fixed-Response-Aktionen
aws.applicationElb.HTTP_Redirect_Count.Sum	Gesamtzahl der erfolgreichen Weiterleitungsaktionen
aws.applicationElb.HTTP_Redirect_Url_Limit_Exceeded_Count.Sum (Empfohlene Metrik)	Gesamtzahl der Weiterleitungsaktionen, die nicht abgeschlossen werden konnten, da die URL im Adressheader der Antwort größer als 8 kB ist
aws.applicationElb.HTTPCode_ELB_3XX_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 3XX-Weiterleitungscodes, die vom Lastenausgleichsmodul stammen. Diese Anzahl enthält keine von Zielen generierten Antwortcodes.
aws.applicationElb.HTTPCode_ELB_4XX_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 4XX-Clientfehlercodes, die vom Lastenausgleichsmodul stammen. Diese Anzahl enthält keine von Zielen generierten Antwortcodes.
aws.applicationElb.HTTPCode_ELB_5XX_Count.Sum	Gesamtzahl der HTTP 5XX-Serverfehlercodes, die vom Lastenausgleichsmodul stammen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-application-elb-Metriken (Fortsetzung)

Metrikname	Beschreibung
(Empfohlene Metrik)	Diese Anzahl enthält keine von Zielen generierten Antwortcodes.
aws.applicationElb.HTTPCode_ELB_500_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 500-Fehlercodes, die vom Lastenausgleichsmodul stammen
aws.applicationElb.HTTPCode_ELB_502_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 502-Fehlercodes, die vom Lastenausgleichsmodul stammen
aws.applicationElb.HTTPCode_ELB_503_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 503-Fehlercodes, die vom Lastenausgleichsmodul stammen
aws.applicationElb.HTTPCode_ELB_504_Count.Sum (Empfohlene Metrik)	Gesamtzahl der HTTP 504-Fehlercodes, die vom Lastenausgleichsmodul stammen
aws.applicationElb.IPv6ProcessedBytes.Sum	Gesamtzahl der vom Lastenausgleichsmodul über IPv6 verarbeiteten Byte
aws.applicationElb.IPv6RequestCount.Sum	Gesamtzahl der vom Lastenausgleichsmodul empfangenen IPv6-Anforderungen
aws.applicationElb.NewConnectionCount.Sum	Gesamtzahl neuer TCP-Verbindungen, die von Clients zum Lastenausgleichsmodul und vom Lastenausgleichsmodul zu Zielen hergestellt werden
aws.applicationElb.NonStickyRequestCount.Sum	Gesamtanzahl der Anforderungen, bei denen vom Lastenausgleichsmodul ein neues Ziel ausgewählt wurde, da eine vorhandene dauerhafte Sitzung nicht verwendet werden konnte
aws.applicationElb.ProcessedBytes.Sum (Empfohlene Metrik)	Gesamtzahl der vom Lastenausgleichsmodul über IPv4 und IPv6 verarbeiteten Byte
aws.applicationElb.RejectedConnectionCount.Sum (Empfohlene Metrik)	Gesamtzahl der Verbindungen, die abgelehnt wurden, da das Lastenausgleichsmodul seine maximale Anzahl von Verbindungen erreicht hatte
aws.applicationElb.RequestCount.Sum	Gesamtzahl der über IPv4 und IPv6 verarbeiteten Anforderungen
aws.applicationElb.RuleEvaluations.Sum	Gesamtzahl der vom Lastenausgleichsmodul verarbeiteten Regeln bei einer pro Stunde gemittelten Anforderungsrate

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ec2-count-Metriken

Metrikname	Beschreibung
aws.ec2.types.<type_name>	Anzahl der EC2-Instanzen für den angegebenen Typ im AWS-Rechenzentrum
aws.ec2.status.running	Anzahl der EC2-Instanzen im Status „Aktiv“ in einem AWS-Rechenzentrum
aws.ec2.status.stopped	Anzahl der EC2-Instanzen im Status „Angehalten“ in einem AWS-Rechenzentrum
aws.ec2.status.total	Anzahl aller EC2-Instanzen in einem AWS-Rechenzentrum

aws.metrics-dynamodb-Metriken

Metrikname	Beschreibung
aws.dynamodb.ConsumedWriteCapacityUnits.Average (Empfohlene Metrik)	Anzahl der über den angegebenen Zeitraum verbrauchten Schreibkapazitätseinheiten, auf deren Basis nachverfolgt wird, wie viel bereitgestellter Durchsatz verwendet wird
aws.dynamodb.ConsumedReadCapacityUnits.Average (Empfohlene Metrik)	Anzahl der über den angegebenen Zeitraum verbrauchten Lesekapazitätseinheiten, auf deren Basis nachverfolgt wird, wie viel bereitgestellter Durchsatz verwendet wird
aws.dynamodb.ProvisionedWriteCapacityUnits.Average (Empfohlene Metrik)	Anzahl der bereitgestellten Schreibkapazitätseinheiten für eine Tabelle
aws.dynamodb.ProvisionedReadCapacityUnits.Average (Empfohlene Metrik)	Anzahl der bereitgestellten Lesekapazitätseinheiten für eine Tabelle
aws.dynamodb.SuccessfulRequestLatency.GetItem.Average (Empfohlene Metrik)	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem GetItem-Vorgang ausgeführt
aws.dynamodb.SuccessfulRequestLatency.BatchGetItem.Average	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem BatchGetItem-Vorgang ausgeführt
aws.dynamodb.SuccessfulRequestLatency.PutItem.Average (Empfohlene Metrik)	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem PutItem-Vorgang ausgeführt
aws.dynamodb.SuccessfulRequestLatency.BatchPutItem.Average	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem BatchPutItem-Vorgang ausgeführt
aws.dynamodb.SuccessfulRequestLatency.Query.Average	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-dynamodb-Metriken (Fortsetzung)

Metrikname	Beschreibung
	des angegebenen Zeitraums. Wird von einem Query-Vorgang ausgeführt
aws.dynamodb.SuccessfulRequestLatency.Scan.Average	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem Scan-Vorgang ausgeführt
aws.dynamodb.ReturnedItemCount.Scan.Average	Anzahl der von Scan-Vorgängen während des angegebenen Zeitraums zurückgegebenen Elemente
aws.dynamodb.ReturnedItemCount.Query.Average	Anzahl der von Query-Vorgängen während des angegebenen Zeitraums zurückgegebenen Elemente
aws.dynamodb.UserErrors.Average (Empfohlene Metrik)	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 400-Statuscode generiert wurde. Ein HTTP 400-Code zeigt normalerweise einen clientseitigen Fehler an, z. B. eine ungültige Kombination von Parametern, einen Versuch, eine nicht vorhandene Tabelle zu aktualisieren, oder eine falsche Anforderungssignatur.
aws.dynamodb.SystemErrors.GetItem.Average (Empfohlene Metrik)	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem GetItem-Vorgang ausgeführt
aws.dynamodb.SystemErrors.Scan.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem Scan-Vorgang ausgeführt
aws.dynamodb.SystemErrors.Query.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem Query-Vorgang ausgeführt
aws.dynamodb.SystemErrors.BatchGetItem.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-dynamodb-Metriken (Fortsetzung)

Metrikname	Beschreibung
	internen Servicefehler an. Wird von einem BatchGet-Vorgang ausgeführt
aws.dynamodb.SystemErrors.PutItem.Average (Empfohlene Metrik)	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem PutItem-Vorgang ausgeführt
aws.dynamodb.SystemErrors.UpdateItem.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem UpdateItem-Vorgang ausgeführt
aws.dynamodb.SystemErrors.DeleteItem.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem DeleteItem-Vorgang ausgeführt
aws.dynamodb.SystemErrors.BatchWriteItem.Average	Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums, von denen ein HTTP 500-Statuscode generiert wurde. Ein HTTP 500-Code zeigt normalerweise einen internen Servicefehler an. Wird von einem BatchWrite-Vorgang ausgeführt
aws.dynamodb.ConditionalCheckFailedRequests.Average (Empfohlene Metrik)	Anzahl der fehlgeschlagenen Versuche, bedingte Schreibvorgänge auszuführen
aws.dynamodb.TimeToLiveDeletedItemCount.Average	Anzahl der über die Gültigkeitsdauer (Time to Live, TTL) gelöschten Elemente während des angegebenen Zeitraums. Diese Metrik hilft Ihnen, die Rate der TTL-Löschungen in Ihrer Tabelle zu überwachen.
aws.dynamodb.TransactionConflict.Average	Aufgrund von Transaktionskonflikten zwischen gleichzeitigen Anforderungen für dieselben Elemente abgelehnte Anforderungen auf Elementebene
aws.dynamodb.ReadThrottleEvents.Average (Empfohlene Metrik)	Anforderungen an DynamoDB, die die bereitgestellten Lesekapazitätseinheiten für eine Tabelle überschreiten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-dynamodb-Metriken (Fortsetzung)

Metrikname	Beschreibung
aws.dynamodb.WriteThrottleEvents.Average (Empfohlene Metrik)	Anforderungen an DynamoDB, die die bereitgestellten Schreibkapazitätseinheiten für eine Tabelle überschreiten
aws.dynamodb.ThrottledRequests.GetItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen GetItem-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.PutItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen PutItem-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.DeleteItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen DeleteItem-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.UpdateItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen UpdateItem-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.BatchGetItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen BatchGetItem-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.Scan.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen Scan-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.Query.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen Query-Vorgang überschreiten
aws.dynamodb.ThrottledRequests.BatchWriteItem.Average	Anforderungen an DynamoDB, die die bereitgestellten Durchsatzgrenzen für eine Ressource für einen BatchWriteItem-Vorgang überschreiten
aws.dynamodb.SuccessfulRequestLatency.GetRecords.Average	Erfolgreiche Anforderungen an DynamoDB- oder Amazon DynamoDB-Streams während des angegebenen Zeitraums. Wird von einem GetRecords-Vorgang ausgeführt
aws.dynamodb.ReturnedBytes.GetRecords.Average	Die Anzahl der von GetRecords-Vorgängen (Amazon DynamoDB-Streams) während des angegebenen Zeitraums zurückgegebenen Byte
aws.dynamodb.ReturnedRecordsCount.GetRecords.Average	Die Anzahl der von GetRecords-Vorgängen (Amazon DynamoDB-Streams) während des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-dynamodb-Metriken (Fortsetzung)

Metrikname	Beschreibung
	angegebenen Zeitraums zurückgegebenen Stream-Datensätze

aws.metrics-ecs-cluster-Metriken

Metrik	Beschreibung
aws.ecs.cluster.CPUReservation.Average (Empfohlene Metrik)	Prozentsatz der CPU-Einheiten, die durch ausgeführte Aufgaben im Cluster reserviert wurden
aws.ecs.cluster.CPUUtilization.Average (Empfohlene Metrik)	Prozentsatz der CPU-Einheiten, die im Cluster verwendet werden
aws.ecs.cluster.MemoryReservation.Average (Empfohlene Metrik)	Prozentsatz des Arbeitsspeichers, der durch ausgeführte Aufgaben im Cluster reserviert wurde
aws.ecs.cluster.MemoryUtilization.Average (Empfohlene Metrik)	Prozentsatz des Arbeitsspeichers, der im Cluster verwendet wird
aws.ecs.cluster.CpuReserved.Average	CPU-Einheiten, die durch Aufgaben im Cluster reserviert wurden
aws.ecs.cluster.CpuUtilized.Average	CPU-Einheiten, die durch Aufgaben im Cluster verwendet wurden
aws.ecs.cluster.NetworkRxBytes.Average (Empfohlene Metrik)	Anzahl der vom Cluster empfangenen Byte
aws.ecs.cluster.NetworkTxBytes.Average (Empfohlene Metrik)	Anzahl der vom Cluster übertragenen Byte
aws.ecs.cluster.EphemeralStorageReserved.Average	Der flüchtige Speicher ist der flüchtige temporäre Speicher, der an Ihre Instanzen angehängt und nur während der Laufzeit der Instanz vorhanden ist.
aws.ecs.cluster.MemoryUtilized.Average (Empfohlene Metrik)	Arbeitsspeicher, der von Aufgaben im Cluster verwendet wird
aws.ecs.cluster.MemoryReserved.Average (Empfohlene Metrik)	Arbeitsspeicher, der von Aufgaben im Cluster reserviert wurde
aws.ecs.cluster.StorageReadBytes.Average (Empfohlene Metrik)	Anzahl der aus dem Speicher im Cluster gelesenen Byte
aws.ecs.cluster.StorageWriteBytes.Average	Anzahl der in den Speicher im Cluster geschriebenen Byte

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ecs-cluster-Metriken (Fortsetzung)

Metrik	Beschreibung
(Empfohlene Metrik)	
aws.ecs.cluster.ContainerInstanceCount.Average (Empfohlene Metrik)	Anzahl der EC2-Instanzen, die den Amazon ECS-Agent ausführen und bei einem Cluster registriert sind
aws.ecs.cluster.ServiceCount.Average (Empfohlene Metrik)	Anzahl der Services im Cluster
aws.ecs.cluster.TaskCount.Average	Anzahl der im Cluster ausgeführten Aufgaben

aws.metrics-ecs-service-Metriken

Metrik	Beschreibung
aws.ecs.service.CPUUtilization.Average (Empfohlene Metrik)	Prozentsatz der CPU-Einheiten, die im Service verwendet werden
aws.ecs.service.MemoryUtilization.Average (Empfohlene Metrik)	Prozentsatz des Arbeitsspeichers, der im Service verwendet wird
aws.ecs.service.CpuReserved.Average	CPU-Einheiten, die durch Aufgaben im Service reserviert wurden
aws.ecs.service.CpuUtilized.Average	CPU-Einheiten, die durch Aufgaben im Service verwendet wurden
aws.ecs.service.NetworkRxBytes.Average (Empfohlene Metrik)	Anzahl der vom Service empfangenen Byte
aws.ecs.service.NetworkTxBytes.Average (Empfohlene Metrik)	Anzahl der vom Service übertragenen Byte
aws.ecs.service.EphemeralStorageReserved.Average	Der flüchtige Speicher ist der flüchtige temporäre Speicher, der an Ihre Instanzen angehängt und nur während der Laufzeit der Instanz vorhanden ist.
aws.ecs.service.MemoryUtilized.Average	Arbeitsspeicher, der von Aufgaben im Service verwendet wird
aws.ecs.service.MemoryReserved.Average	Arbeitsspeicher, der von Aufgaben im Service reserviert wurde
aws.ecs.service.StorageReadBytes.Average (Empfohlene Metrik)	Anzahl der aus dem Speicher im Service gelesenen Byte
aws.ecs.service.StorageWriteBytes.Average	Anzahl der in den Speicher im Service geschriebenen Byte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aws.metrics-ecs-service-Metriken (Fortsetzung)

Metrik	Beschreibung
(Empfohlene Metrik)	
aws.ecs.service.RunningTaskCount.Average (Empfohlene Metrik)	Anzahl der Aufgaben, die sich derzeit im Status „WIRD AUSGEFÜHRT“ befinden
aws.ecs.service.DeploymentCount.Average	Anzahl der Bereitstellungen in einem Amazon ECS-Service
aws.ecs.service.DesiredTaskCount.Average (Empfohlene Metrik)	Gewünschte Anzahl von Aufgaben für einen Amazon ECS-Service
aws.ecs.service.TaskSetCount.Average (Empfohlene Metrik)	Anzahl der Aufgabensätze im Service
aws.ecs.service.PendingTaskCount.Average (Empfohlene Metrik)	Anzahl der Aufgaben, die sich derzeit im Status „AUSSTEHEND“ befinden

Azure-Systemüberwachung – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für Azure-Systemüberwachung.

Azure Kubernetes (K8s) Service-Metriken

Typ	Prüfung	Beschreibung	Befehl
Metrik	azure.metrics-k8s-service	Stellt Metriken auf Pod-, -Knoten und Clusterebene aus allen Azure Kubernetes-Services im Metrikformat bereit. Verwendung: metrics-azure-k8s-service.rb `-S, --subscription ID ARM Subscription ID -r, Region` Beispiel: `metrics-azure-k8s-service.rb -S`	`metrics-azure-k8s-service.rb -r {{.labels.params_ci_region}} {{-s {{if.labels.params_subscriptio -S {{.labels.params_subscription_ {{end}}`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Kubernetes (K8s) Service-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
		`{{.labels.params_subscription_id}} -r westus2`	

Azure-Metriken

In den folgenden Tabellen werden die Metriken aufgelistet und beschrieben, die als Ausgabe von Prüfungen Azure gesammelt werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Azure Kubernetes Service-Prüfmetriken

Metrikname	Beschreibung
apiserver_current_inflight_requests (Empfohlene Metrik)	Maximale Anzahl der derzeit auf dem API-Server verwendeten Anforderungen während der ausführung pro Anforderungsart in der letzten Sekunde.
cluster_autoscaler_cluster_safe_to_autoscale	Bestimmt, ob die automatische Clusterskalierung Aktionen für den Cluster durchführt.
cluster_autoscaler_scale_down_in_cooldown	Bestimmt, ob sich die Herunterskalierung in der Abklingzeit befindet; während dieses Zeitraums werden keine Knoten entfernt.
cluster_autoscaler_unschedulable_pods_count	Anzahl der Pods, die derzeit nicht im Cluster geplant werden können.
kube_node_status_allocatable_cpu_cores (Empfohlene Metrik)	Gesamtzahl der verfügbaren CPU-Kerne in einem verwalteten Cluster.
kube_node_status_allocatable_memory_bytes (Empfohlene Metrik)	Gesamtmenge des verfügbaren Arbeitsspeichers in einem verwalteten Cluster.
kube_node_status_condition (Empfohlene Metrik)	Status für verschiedene Knotenbedingungen.
kube_pod_status_phase (Empfohlene Metrik)	Anzahl der Pods nach Phase.
kube_pod_status_ready (Empfohlene Metrik)	Anzahl der Pods im Status „Bereit“.
node_cpu_usage_millicores (Empfohlene Metrik)	Aggregierte Messung der CPU-Auslastung in Millicore im gesamten Cluster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Kubernetes Service-Prüfmetriken (Fortsetzung)

Metrikname	Beschreibung
node_cpu_usage_percentage (Empfohlene Metrik)	Aggregierte durchschnittliche CPU-Auslastung in Prozent im gesamten Cluster.
node_disk_usage_bytes	Anzahl der vom Gerät verwendeten Festplattenspeicher-Bytes.
node_disk_usage_percentage (Empfohlene Metrik)	Prozentsatz des Speicherplatzes, der vom Gerät verwendet wird.
node_memory_rss_bytes	Anzahl der verwendeten Container-RSS-Speicherbytes.
node_memory_rss_percentage (Empfohlene Metrik)	Prozentsatz des verwendeten Container-RSS-Speichers.
node_memory_working_set_bytes	Anzahl der verwendeten Arbeitsspeicher-Bytes des Container-Arbeitssatzes.
node_memory_working_set_percentage (Empfohlene Metrik)	Prozentsatz des verwendeten Arbeitsspeichers des Containers.
node_network_in_bytes (Empfohlene Metrik)	Vom Netzwerk empfangene Bytes.
node_network_out_bytes (Empfohlene Metrik)	Vom Netzwerk übertragene Bytes.

Azure VM-CPU-Metriken

Metrikname	Beschreibung
Percentage CPU (CPU-Prozentsatz) (Empfohlene Metrik)	Der Prozentsatz der zugewiesenen Recheneinheiten , die derzeit von den virtuellen Computern verwendet werden.
CPU Credits Remaining (CPU-Guthaben verbleibend)	Gesamtanzahl des für Burst verfügbaren Guthabens. Nur auf platzfähigen VMs der B-Serie verfügbar.
CPU Credits Consumed (CPU-Guthaben verbraucht)	Gesamtanzahl des vom virtuellen Computer verbrauchten Guthabens. Nur auf VM-Modellen der B-Serie verfügbar

Azure VM-Netzwerk-Metriken

Metrikname	Beschreibung
Netzwerkeingang	Die Anzahl der abrechenbaren Bytes, die auf allen Netzwerkschnittstellen von den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure VM-Netzwerk-Metriken (Fortsetzung)

Metrikname	Beschreibung
(Empfohlene Metrik)	virtuellen Computern empfangen wurden (Eingehender Datenverkehr) (Veraltet).
Netzwerkausgang (Empfohlene Metrik)	Die Anzahl der abrechenbaren Bytes, die über alle Netzwerkschnittstellen von den virtuellen Computern gesendet wurden (Ausgehender Datenverkehr) (Veraltet).
Network In Total (Netzwerkeingang insgesamt) (Empfohlene Metrik)	Die Anzahl der über alle Netzwerkschnittstellen von virtuellen Computern empfangenen Bytes (Eingehender Datenverkehr).
Network Out Total (Netzwerkausgang insgesamt) (Empfohlene Metrik)	Die Anzahl der Bytes, die über alle Netzwerkschnittstellen von den virtuellen Computern gesendet werden (ausgehender Datenverkehr).

Azure VM-Laufwerksmetriken

Metrikname	Beschreibung
Disk Read Bytes (Laufwerk-Lesebytes) (Empfohlene Metrik)	Während des Überwachungszeitraums vom Datenträger gelesene Bytes.
Disk Write Bytes (Laufwerk-Schreibbytes) (Empfohlene Metrik)	Während des Überwachungszeitraums auf den Datenträger geschriebene Bytes.
Disk Read Operations/Sec (Laufwerk-Lesevorgänge/s) (Empfohlene Metrik)	Lese-IOPS des Datenträgers.
Disk Write Operations/Sec (Laufwerk-Schreibvorgänge/s) (Empfohlene Metrik)	Datenträger-Schreib-IOPS.
Data Disk Read Bytes/sec (Datenträger-Lesebytes/s) (Empfohlene Metrik)	Bytes pro Sekunde, die während des Überwachungszeitraums von einem einzelnen Datenträger gelesen wurden.
Data Disk Write Bytes/sec (Datenträger-Schreibbytes/s) (Empfohlene Metrik)	Bytes, die pro Sekunde auf einen einzelnen Datenträger während des Überwachungszeitraums geschrieben wurden.
Data Disk Read Operations/Sec (Datenträger-Lesevorgänge/s) (Empfohlene Metrik)	Lese IOPS von einem einzelnen Datenträger während des Überwachungszeitraums.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure VM-Laufwerksmetriken (Fortsetzung)

Metrikname	Beschreibung
Data Disk Write Operations/Sec (Datenträger-Schreibvorgänge/s) (Empfohlene Metrik)	Schreiben Sie während des Überwachungszeitraums IOPS von einem einzelnen Datenträger.
Data Disk Bandwidth Consumed Percentage (Datenträger – Prozentsatz verbrauchter Bandbreite) (Empfohlene Metrik)	Prozentsatz der verbrauchten Bandbreite des Datenträgers pro Minute
Data Disk IOPS Consumed Percentage (Datenträger – Prozentsatz verbrauchter IOPS) (Empfohlene Metrik)	Prozentsatz der verbrauchten E/As des Datenträgers pro Minute
Data Disk Target Bandwidth (Ziel-Bandbreite für Datenträger) (Empfohlene Metrik)	Baseline-Durchsatz in Byte pro Sekunde, den der Datenträger ohne Bursting erreichen kann
Data Disk Target IOPS (Datenträger-Ziel-IOPS) (Empfohlene Metrik)	Baseline-IOPS, die der Datenträger ohne Bursting erreichen kann
Data Disk Max Burst Bandwidth (Maximale Burst-Bandbreite für Datenträger) (Empfohlene Metrik)	Maximaler Durchsatz in Byte pro Sekunde, den der Datenträger mit Bursting erreichen kann
Data Disk Max Burst IOPS (Max. Burst-IOPS für Datenträger) (Empfohlene Metrik)	Maximale IOPS, die der Datenträger mit Bursting erreichen kann
Data Disk Used Burst BPS Credits Percentage (Prozentsatz des verwendeten Burst-BPS-Guthabens für Datenträger)	Prozentsatz des bisher verwendeten Datenträger-Guthabens für Burst-Bandbreite
Data Disk Used Burst IO Credits Percentage (Prozentsatz des verwendeten Burst-EA-Guthabens für Datenträger)	Prozentsatz des bisher verwendeten Datenträger-Guthabens für Burst-E/A
Premium Data Disk Cache Read Hit (Lese-Treffer für Premium-Datenträger-Cache) (Empfohlene Metrik)	Lese-Treffer für Premium-Datenträger-Cache
Premium Data Disk Cache Read Miss (Lese-Fehler für Premium-Datenträger-Cache) (Empfohlene Metrik)	Lese-Fehler für Premium-Datenträger-Cache
Premium OS Disk Cache Read Hit (Lese-Treffer für Premium-BS-Laufwerks-Cache)	Lese-Treffer für Premium-BS-Laufwerks-Cache

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure VM-Laufwerksmetriken (Fortsetzung)

Metrikname	Beschreibung
(Empfohlene Metrik)	
Premium OS Disk Cache Read Miss (Lese-Fehler für Premium-BS-Laufwerks-Cache) (Empfohlene Metrik)	Lese-Fehler für Premium-BS-Laufwerks-Cache

Azure VM-Flow-Metriken

Metrikname	Beschreibung
Eingehender Verkehr (Empfohlene Metrik)	Eingehende Flows sind die Anzahl der aktuellen Flows in eingehender Richtung (Datenverkehr, der in die VM eingeht).
Ausgehender Verkehr (Empfohlene Metrik)	Maximale Erstellungsrate ausgehender Flows (Datenverkehr, der die VM verlässt)
Inbound Flows Maximum Creation Rate (Maximale Erstellungsrate für eingehende Flows) (Empfohlene Metrik)	Maximale Erstellungsrate eingehender Flows (Datenverkehr, der in die VM eingeht)
Outbound Flows Maximum Creation Rate (Maximale Erstellungsrate für ausgehende Flows) (Empfohlene Metrik)	Maximale Erstellungsrate ausgehender Flows (Datenverkehr, der die VM verlässt)

Azure VM-Arbeitsspeichermetriken

Metrikname	Beschreibung
VM Cached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter gecachter Bandbreite) (Empfohlene Metrik)	Prozentsatz der zwischengespeicherten Laufwerks-Bandbreite, die von der VM verbraucht wurde
VM Cached IOPS Consumed Percentage (VM – Prozentsatz verbrauchter gecachter IOPS)	Prozentsatz der zwischengespeicherten Laufwerks-IOPS, die von der VM verbraucht wurden
VM Uncached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter ungecachter Bandbreite) (Empfohlene Metrik)	Prozentsatz der nicht zwischengespeicherten Laufwerks-Bandbreite, die von der VM verbraucht wurde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure VM-Arbeitsspeichermetriken (Fortsetzung)

Metrikname	Beschreibung
VM Uncached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter ungecachter Bandbreite)	Prozentsatz der nicht zwischengespeicherten Laufwerks-IOPS, die von der VM verbraucht wurden
Available Memory Byte (Verfügbarer Arbeitsspeicher (Byte)) (Empfohlene Metrik)	Menge des physischen Arbeitsspeichers in Byte, die sofort für die Zuordnung zu einem Prozess oder für die Systemnutzung in der virtuellen Maschine verfügbar ist.

Azure-VM-Metrikrichtlinie: Prüfmetriken des Azure-Metrikensammlers

Metrikname	Einheiten	Beschreibung
Prozentuale CPU (empfohlene Metrik)	%	Der Prozentsatz der zugewiesenen Recheneinheiten, die derzeit von der virtuellen Maschine verwendet werden.
CPU Credits Remaining (CPU-Guthaben verbleibend)		Anzahl der verdienten CPU-Punktzahlen, die von der virtuellen Maschine nicht verbraucht wurden.
CPU Credits Consumed (CPU-Guthaben verbraucht)		Gesamtzahl der CPU-Punktzahlen, die von der virtuellen Maschine verbraucht wurden.
Netzwerkeingang		Anzahl der über alle Netzwerkschnittstellen empfangenen Bytes.
Netzwerkausgang		Anzahl der Bytes, die über alle Netzwerkschnittstellen von der Instanz gesendet wurden.
Netzwerk insgesamt (empfohlene Metrik)	Byte	Die Anzahl der auf allen Netzwerkschnittstellen von den virtuellen Computern empfangenen Bytes (Eingehender Datenverkehr).
Netzwerkausgabe gesamt (empfohlene Metrik)	Byte	Die Anzahl der Bytes, die über alle Netzwerkschnittstellen von den virtuellen Computern gesendet werden (ausgehender Datenverkehr).
Verfügbarer Arbeitsspeicher in Byte (empfohlene Metrik)	Byte	Sofort verfügbare Menge des physischen Arbeitsspeichers in Byte für die Zuteilung an einen Prozess oder für die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-VM-Metrikrichtlinie: Prüfmetriken des Azure-Metrikensammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
		Systemverwendung in der virtuellen Maschine.
VM Cached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter gecachter Bandbreite)		Prozentsatz der zwischengespeicherten Laufwerks-Bandbreite, die von der VM verbraucht wurde
VM Cached IOPS Consumed Percentage (VM – Prozentsatz verbrauchter gecachter IOPS)		Prozentsatz der zwischengespeicherten Laufwerks-IOPS, die von der VM verbraucht wurden
VM Uncached Bandwidth Consumed Percentage (VM – Prozentsatz verbrauchter ungecachter Bandbreite)		Prozentsatz der nicht zwischengespeicherten Laufwerks-Bandbreite, die von der VM verbraucht wurde
Verbrauchter Prozentsatz der nicht zwischengespeicherten IOPS der VM		Prozentsatz der nicht zwischengespeicherten Laufwerks-IOPS, die von der VM verbraucht wurden
Bytes des Datenträger-Lesevorgangs (empfohlene Metrik)	Byte	Während des Überwachungszeitraums vom Datenträger gelesene Bytes.
Datenträger-Schreibbytes (empfohlene Metrik)	Byte	Während des Überwachungszeitraums auf den Datenträger geschriebene Bytes.
Datenträger-Lesevorgänge/Sek. (empfohlene Metrik)	AnzahlProSekunde	Lese-IOPS des Datenträgers.
Datenträger-Schreibvorgänge/Sek. (empfohlene Metrik)	AnzahlProSekunde	Datenträger-Schreib-IOPS.
BS-Datenträger – Lesebytes/Sek		Während des Überwachungszeitraums vom Datenträger gelesene Bytes/Sek.
BS-Datenträger – Schreibvorgänge in Byte/Sek		Während des Überwachungszeitraums auf den Datenträger geschriebene Bytes/Sek.
BS-Datenträger-Lesevorgänge/Sek		Liest IOPS während des Überwachungszeitraums vom Datenträger.
BS-Datenträger-Schreibvorgänge/Sek		Schreiben Sie IOPS während des Überwachungszeitraums vom Datenträger.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-VM-Metrikrichtlinie: Prüfmetriken des Azure-Metrikensammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
Tiefe der BS-Datenträgerwarteschlange		Durchschnittliche Anzahl der Lese- und Schreibanforderungen, die sich während des Stichprobenzeitraums für den ausgewählten Datenträger in der Warteschlange befanden.
Verbrauchter Prozentsatz der BS-Datenträger-Bandbreite		Prozentsatz der verbrauchten Bandbreite des Datenträgers pro Minute
Verbrauchter Prozentsatz der IOPS des BS-Datenträgers		Prozentsatz der verbrauchten E/As des Datenträgers pro Minute
Zielbandbreite des BS-Datenträgers		Baseline-Durchsatz in Byte pro Sekunde, den ein Datenträger ohne Bursting erreichen kann.
BS-Datenträger-Ziel-IOPS		Baseline-IOPS-Datenträger können ohne Bursting erreichen.
Max. Burst-Bandbreite des BS-Datenträgers		Maximaler Durchsatz in Byte pro Sekunde, den ein Datenträger beim Bursting erreichen kann.
Max. Burst-IOPS des BS-Datenträgers		Maximale IOPS, die der Datenträger beim Bursting erreichen kann.
Prozentsatz der verwendeten Burst-BPS-Gutschriften des BS-Datenträgers		Prozentsatz der bisher verwendeten Datenträger-Burst-Bandbreiten-Gutschriften.
Prozentsatz der verwendeten Burst-E/A-Gutschriften des BS-Datenträgers		Prozentsatz der bisher verwendeten Datenträger-Burst-E/A-Gutschriften.
Premium OS Disk Cache Read Hit (Lese-Treffer für Premium-BS-Laufwerks-Cache)		Lesetreffer für Premium-Betriebssystemdatenträger-Cache.
Premium OS Disk Cache Read Miss (Lese-Fehler für Premium-BS-Laufwerks-Cache)		Lesefehler im Premium-Betriebssystem-Datenträger-Cache.
Eingehende Flows		Anzahl der aktuellen Flows in eingehender Richtung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-VM-Metrikrichtlinie: Prüfmetriken des Azure-Metrikensammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
		(Datenverkehr, der in die VM eingeht).
Ausgehende Flows		Anzahl der aktuellen Flows in eingehender Richtung (von der VM ausgehender Datenverkehr).
Inbound Flows Maximum Creation Rate (Maximale Erstellungsrate für eingehende Flows)		Maximale Erstellungsrate eingehender Flows (Datenverkehr, der in die VM eingeht)
Outbound Flows Maximum Creation Rate (Maximale Erstellungsrate für ausgehende Flows)		Maximale Erstellungsrate ausgehender Flows (Datenverkehr, der die VM verlässt)

Metrikrichtlinie für Azure-Lastenausgleichsmodul – Prüfmetriken des Azure-Metrikensammlers

Metrikname	Einheiten	Beschreibung
AllocatedSnatPorts (empfohlene Metrik)		Gesamtzahl der SNAT-Ports, die innerhalb des Zeitraums zugeordnet sind, der durch den Wert *PT*(Zeitraum) der Metrikdefinition angegeben wird.
ByteCount (empfohlene Metrik)	Bytes	Gesamtzahl der Bytes, die innerhalb des Zeitraums übertragen wurden, der durch den Wert *PT*(Zeitraum) der Metrikdefinition angegeben wurde.
DIP-Verfügbarkeit (empfohlene Metrik)	count	Durchschnittlicher Status von Lastenausgleichsmodul-Integritätsprüfungen pro Zeitdauer.
BlockedCount (empfohlene Metrik)		Gesamtzahl der Pakete, die innerhalb des Zeitraums übertragen wurden, der durch den Wert *PT*(Zeitraum) der Metrikdefinition angegeben wird.
SnatConnectionCount (empfohlene Metrik)	count	Gesamtzahl der neuen SNAT-Verbindungen, die innerhalb des Zeitraums erstellt wurden, der durch den Wert *PT*(Zeitraum) der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikrichtlinie für Azure-Lastenausgleichsmodul – Prüfmetriken des Azure-Metrikensammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
		Metrikdefinition angegeben wurde.
SYNCount (empfohlene Metrik)		Gesamtzahl der SYN-Pakete, die innerhalb des Zeitraums übertragen wurden, der durch den Wert *PT* (Zeitraum) der Metrikdefinition angegeben wird.
UsedSnatPorts (empfohlene Metrik)		Gesamtzahl der SNAT-Ports, die innerhalb des Zeitraums verwendet werden, der durch den Wert *PT* (Zeitraum) der Metrikdefinition angegeben wird.
VipAvailability (empfohlene Metrik)	count	Durchschnittliche Datenpfadverfügbarkeit des Lastenausgleichsmoduls pro Zeitdauer.

Azure Redis Cache-Richtlinie – Prüfmetriken des Azure-Metrikensammlers

Metrikname	Einheiten	Beschreibung
verbundeneClients		Anzahl der Clientverbindungen mit dem Cache.
insgesamtBefehleverarbeitet		Gesamtzahl der vom Cache-Server verarbeiteten Befehle.
Cache-Hits (empfohlene Metrik)	count	Anzahl der erfolgreichen Schlüsselsuchen.
Cachemisses (empfohlene Metrik)	count	Anzahl der fehlgeschlagenen Schlüsselsuchen.
Cache-Fehlerrate		Rate der fehlgeschlagenen Schlüsselsuchen.
getcommands		Anzahl der Abrufvorgänge aus dem Cache.
setcommands (empfohlene Metrik)	count	Anzahl der festgelegten Vorgänge für den Cache.
„operationsProSecond“		Anzahl der unmittelbar im Cache ausgeführten Vorgänge pro Sekunde.
entfernteSchlüssel		Anzahl der aus dem Cache entfernten Elemente.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Redis Cache-Richtlinie – Prüfmetriken des Azure-Metrikensammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
Gesamtschlüssel		Anzahl der Schlüssel im Cache.
abgelaufeneSchlüssel		Anzahl der Elemente, die aus dem Cache abgelaufen sind.
VerwendeterArbeitsspeicher	Bytes	Menge des Cache-Speichers, die für Schlüssel-Wert-Paare im Cache verwendet wird.
verwendetarbeitsspeicherRss	Bytes	Menge des Cache-Speichers, die während des angegebenen Berichtsintervalls verwendet wurde, einschließlich Fragmentierung und Metadaten
serverLoad (empfohlene Metrik)	Prozent	Prozentsatz der Zyklen, in denen der Redis-Server mit der Verarbeitung ausgelastet ist und nicht im Leerlauf auf Nachrichten wartet
CacheWrite (empfohlene Metrik)	BytesPersSecond	Menge der in den Cache geschriebenen Daten.
CacheRead (empfohlene Metrik)	BytesProSekunde	Aus dem Cache gelesene Datenmenge.
allConnectionsCreatedProSecond		Anzahl der pro Sekunde im Cache erstellten sofortigen Verbindungen über Port 6379 oder 6380 (SSL).
allConnectionsClosedProSecond		Anzahl der sofort im Cache geschlossenen Verbindungen pro Sekunde über Port 6379 oder 6380 (SSL).
allconnectedclients (empfohlene Metrik)	count	Anzahl der derzeit mit dem System verbundenen Clients.
GesamtzahlVerarbeiteterBefehle		Die kumulative Anzahl aller vom System verarbeiteten Befehle.
AlleVorgängeProSekunde		Gesamtzahl der Vorgänge (z. B. Lese- oder Schreibbefehle) pro Sekunde für alle Instanzen.
GesamterVerwendeterArbeitsspeicher (empfohlene Metrik)	Bytes	Gesamtmenge an Arbeitsspeicher, die im

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Redis Cache-Richtlinie – Prüfmetriken des Azure-Metrikensammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
		gesamten System verwendet wird.
allusedmemoryRss (empfohlene Metrik)	Bytes	Die Gesamtgröße des Resident Set (RSS), die die Menge des physisch im RAM vorhandenen Arbeitsspeichers für alle Instanzen, einschließlich Swap, widerspiegelt.

Azure Gateway-Metrikrichtlinie: Prüfmetriken des Azure-Metrikensammlers

Metrikname	Einheiten	Beschreibung
ApplicationGatewayTotalTime (empfohlene Metrik)	Millisekunden	Zeit, die benötigt wird, um eine Anforderung zu verarbeiten und ihre Antwort zu senden.
Durchschn.AnforderungsanzahlProgesundeHost		Durchschnittliche Anzahl der Anforderungen pro Minute pro fehlerfreiem Back-End-Host in einem Pool.
AzwafBotProtectionMatches		Übereinstimmende Bot-Regeln
AzwafCustomRuleMatches		Übereinstimmende anwenderdefinierte Regeln.
AzwafSecRuleMatches		Übereinstimmende verwaltete Regeln.
AzwafTotalRequests		Gesamtzahl der von WAF ausgewerteten Anforderungen.
Back-EndConnectTime		Zeit, die für den Verbindungsaufbau mit einem Back-End-Server aufgewendet wurde.
BackEndFirstByteResponseTime		Zeitintervall zwischen dem Beginn des Herstellens einer Verbindung zum Back-End-Server und dem Empfang des ersten Bytes des Antwortheaders, ungefähre Verarbeitungszeit des Back-End-Servers.
Back-EndLastByteResponseTime		Zeitintervall zwischen dem Beginn des Verbindungsaufbaus mit dem Back-End-Server und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Gateway-Metrikrichtlinie: Prüfmetriken des Azure-Metrikensammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
		dem Empfang des letzten Bytes des Antworttexts.
BackendAntwortStatus		Anzahl der von den Back-End-Mitgliedern generierten HTTP-Antwortcodes. Dies umfasst keine Antwortcodes, die von Application Gateway generiert wurden.
BlockedCount		Gesamtzahl der blockierten Vorgänge oder Anforderungen
BytesReceived (empfohlene Metrik)	Bytes	Gesamtzahl der Bytes, die Application Gateway von Clients empfangen hat.
BytesSent (empfohlene Metrik)	Bytes	Gesamtzahl der von Application Gateway an Clients gesendeten Bytes.
Kapazitätseinheiten		Verbrauchte Kapazitätseinheiten.
ClientRtt		Roundtrip-Zeit zwischen Clients und Anwendungs-Gateway. Gibt an, wie lange es dauert, Verbindungen herzustellen und Bestätigungen zurückzugeben.
ComputeUnits		Verbrauchte Einheiten berechnen.
CPUUtilization		Aktuelle CPU-Auslastung von Application Gateway.
CurrentConnections (empfohlene Metrik)	count	Anzahl der aktuell mit Application Gateway hergestellten Verbindungen.
GeschätzteAbgerechnetKapazitätEinheiten		Geschätzte Kapazitätseinheiten, die berechnet werden.
FailedRequests (empfohlene Metrik)	count	Anzahl der fehlgeschlagenen Anforderungen, die von Application Gateway verarbeitet wurden.
FesteAbrechnungsfähigeKapazitätEinheiten		Einheiten für feste abrechenbare Kapazität.
HealthHostCount (empfohlene Metrik)	count	Anzahl der fehlerfreien Back-End-Hosts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Gateway-Metrikrichtlinie: Prüfmetriken des Azure-Metrikensammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
NeueVerbindungenProSekunde		Neue Verbindungen pro Sekunde, die mit Application Gateway hergestellt werden.
ResponseStatus		Von Application Gateway zurückgegebener HTTP-Antwortstatus.
Durchsatz (empfohlene Metrik)	BytesProSekunde	Anzahl der Bytes, die pro Sekunde von Application Gateway verarbeitet wurden.
TotalRequests (empfohlene Metrik)	count	Anzahl der erfolgreichen Anforderungen, die von Application Gateway verarbeitet wurden.
UnhealthyHostCount (empfohlene Metrik)	count	Anzahl der fehlerhaften Back-End-Hosts.

Azure Storage-Kontorichtlinie – Prüfmetriken des Azure-Metrikensammlers

Metrikname	Einheiten	Beschreibung
Transaktionen (empfohlene Metrik)	count	Gesamtzahl der an das Speicherkonto gestellten Anforderungen.
Eingehend (empfohlene Metrik)	Bytes	Menge der Eingangsdaten. Diese Zahl umfasst den Eingang von einem externen Client in den Speicher Azure sowie den Eingang innerhalb von Azure.
Ausgehend (empfohlene Metrik)	Bytes	Menge der Ausgangsdaten. Diese Zahl umfasst den Ausgang von einem externen Client in den Speicher Azure sowie den Ausgang innerhalb von Azure. Daher spiegelt diese Zahl nicht den abrechenbaren Ausgang wider.
SuccessServerLatency (empfohlene Metrik)	Millisekunden	Durchschnittliche Latenz, die von Azure Speicher zur Verarbeitung einer erfolgreichen Anforderung verwendet wird.
SuccessE2ELatency (empfohlene Metrik)	Millisekunden	Die durchschnittliche End-to-End-Latenz erfolgreicher Anforderungen an einen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Storage-Kontorichtlinie – Prüfmetriken des Azure-Metrikensammlers (Fortsetzung)

Metrikname	Einheiten	Beschreibung
		Speicherservice oder den angegebenen API-Vorgang.
Verfügbarkeit (empfohlene Metrik)	Prozent	Prozentsatz der Verfügbarkeit für den Speicherservice oder den angegebenen API-Vorgang.

Azure Blob Services-Metriken

Metrikname	Beschreibung
Verfügbarkeitsdiagramm	Prozentsatz der Verfügbarkeit für den Speicherservice oder den angegebenen API-Vorgang. Die Verfügbarkeit wird berechnet, indem der Wert TotalBillableRequests durch die Anzahl der zutreffenden Anforderungen geteilt wird, einschließlich derer, die unerwartete Fehler verursacht haben. Alle unerwarteten Fehler tragen zu verringerter Verfügbarkeit für den Speicherservice oder den angegebenen API-Vorgang bei.
BlobCapacity (Empfohlene Metrik)	Menge des vom Blob-Service des Speicherkontos verwendeten Speichers in Byte
BlobCount	Anzahl der Blobs im Blob-Service des Speicherkontos
Container Count (Containeranzahl)	Anzahl der Container im Blob-Service des Speicherkontos
Ausgehend (Empfohlene Metrik)	Menge der Ausgangsdaten in Byte. Schließt den ausgehenden Datenverkehr eines externen Clients in den Azure-Speicher sowie den ausgehenden Datenverkehr des Azure-Clients ein. Daher spiegelt diese Zahl nicht den abrechenbaren ausgehenden Datenverkehr wider.
Index Capacity (Indexkapazität) (Empfohlene Metrik)	Vom (hierarchischen) ADLS Gen2-Index genutzter Speicher in Byte
Eingehend (Empfohlene Metrik)	Menge der Eingangsdaten in Byte. Schließt den eingehenden Datenverkehr eines externen Clients in den Azure-Speicher sowie den eingehenden Datenverkehr des Azure-Clients ein.
SuccessE2ELatency (Empfohlene Metrik)	End-to-End-Latenzzeit erfolgreicher Anforderungen an einen Speicherservice oder den angegebenen API-Vorgang in Millisekunden. Schließt die erforderliche

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure Blob Services-Metriken (Fortsetzung)

Metrikname	Beschreibung
	Verarbeitungszeit im Azure-Speicher zum Lesen der Anforderung, zum Senden der Antwort und zum Empfangen einer Bestätigung der Antwort ein.
SuccessServerLatency (Empfohlene Metrik)	Latenz in Millisekunden, die vom Azure-Speicher zur Verarbeitung einer erfolgreichen Anforderung verwendet wird. Dieser Wert enthält nicht die in **SuccessE2ELatency** angegebene Netzwerklatenz.
Transactions	Anzahl der Anforderungen, die an einen Speicherservice oder den angegebenen API-Vorgang gesendet wurden. Enthält erfolgreiche und fehlgeschlagene Anforderungen sowie Anforderungen, die Fehler verursacht haben. Verwenden Sie die Dimension *ResponseType* für die Anzahl der verschiedenen Antworttypen.

Azure Cloud-Metriken

Cloud-MetrikenAzure für werden aus virtuellen Computern (VMs) von Azure und Speicherkontorichtlinien Azure von erfasst. Durch das Sammeln der Cloud-Metriken können Sie die Leistung Ihrer Azure -Ressourcen überwachen.

Azure Sammlung von Cloud-Metriken – Übersicht

Um mit der Erfassung von Cloud-Metriken Azure zu beginnen, müssen Sie die Metriken auswählen, die Sie zu CMDB hinzufügen möchten, und die relevanten Systemkonfigurationen festlegen. Sie können beispielsweise die Anzahl der von Azure -Ressourcen gesendeten und empfangenen Bytes überwachen. Details finden Sie unter Agent Client Collector Visibility – Inhalt – Referenz.

Azure -Richtlinien werden verwendet

Sie können vorkonfigurierte Richtlinien Azure für die Metriksammlung verwenden oder eigene Richtlinien Azure erstellen.

Bei Verwendung einer vorkonfigurierten Richtlinie führen Sie folgende Aufgaben aus:

- Bereiten Sie eine Instanz mit einer aktiven MID-Server - und Metrikbasis vor.
- Installieren Sie Agent Client Collector Framework und Agent Client Collector-Überwachung.
- Führen Sie Discovery im Cloud-Account Azure aus, um CMDB mit den zu überwachenden Konfigurationselementen (CIs) zu füllen.
- Konfigurieren Sie einen Proxy-Agent, und weisen Sie der Richtlinie Anmeldeinformationen zu. Proxy-Agents überwachen CIs für Agents in der Cloud. Mit Anmeldeinformationen kann der Service Desk-Mitarbeiter auf die Richtlinie Azure zugreifen.

In der folgenden Tabelle werden die mit dem Basissystem verfügbaren Richtlinien beschrieben, die Sie aktivieren und konfigurieren können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Azure-Richtlinien, die mit dem Basissystem verfügbar sind

Richtliniename	Beschreibung	Link zu unterstützten Metriken
Azure Metriken des Lastenausgleichsmoduls	Sammelt die Metriken für die Lastenausgleichsmodule Azure.	Unterstützte Metriken für Microsoft Load Balancers
Azure Gateway-Metriken	Sammelt die Metriken für das Netzwerkgateway Azure.	Unterstützte Metriken für Microsoft Network Gateways
Azure Redis-Cache-Metriken	Sammelt die Metriken für den Redis-Cache Azure.	Unterstützte Metriken für Microsoft Redis-Cache
Azure Speicherkontometriken	Sammelt die Metriken für die Speicher-Accounts Azure.	Unterstützte Metriken für Microsoft-Speicherkonten
Azure Metriken für virtuelle Computer (VM).	Sammelt die Metriken für die VMs, die Ihnen bei der Überwachung von Azure -VMs helfen.	Unterstützte Metriken für virtuelle Microsoft-Computer

CIs für die Metriksammlung angeben

Wenn Sie Richtlinien erstellen, müssen Sie die CIs, für die Sie die Metriken erfassen möchten, in CMDBangeben. Die CIs werden in der Regel während Discoveryausgefüllt. Dabei werden Anwendungen und Geräte in Ihrem Netzwerk gefunden und CMDB entsprechend aktualisiert.

Beim Erstellen einer Richtlinie müssen Sie entscheiden, welche CIs überwacht werden sollen. Um die Überwachung von CIs zu aktivieren, gehen Sie wie folgt vor:

1. Konfigurieren Sie das Kontrollkästchen Azure Metriksammler in der Richtlinie.
2. Legen Sie die Anmeldeinformationen für die Prüfung Azure „ Metrics Collector“ fest, um das Abrufen von Metriken von Azure für den Agent Client Collector -Agent zu ermöglichen.
3. Generieren Sie eine JSON-Datei, die die Liste der zu überwachenden Ressourcen angibt.
4. Generieren Sie eine JSON-Datei, die die Liste der Metriken angibt, die aus den überwachten Ressourcen abgerufen werden sollen.

Einzelheiten zu den Azure-Richtlinien finden Sie unter Erstellen Sie Azure -Richtlinien für die Metrikensammlung.

Weitere Informationen zur Azure Metriken-Batch-API finden Sie auf der Seite „Metriken-Batch-API“ .

Cassandra – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Richtlinien für die Cassandra-Systemüberwachung. Die Richtlinien beinhalten die in der angegebenen Tabelle ausgewiesenen Prüfungen. Richtlinien und Prüfungen sind nur für Linux verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cassandra Metriken

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
app.cassandra.metrics-cassandra	Gibt Metriken einer Datenbank Cassandra zurück.	`metrics-cassandra-graphite.rb` Optionen: -h host Hostname, auf dem die Datenbank Cassandra ausgeführt wird -P port Cassandra JMX-Port	`metrics-cassandra-graphite.rb --cfstats -P {{.labels.params_port}} -h {{.labels.params_host}}`	`<host>.cassandra.load 132270.08 1645107221`

Cassandra-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Cassandra-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Metriken – Cassandra-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.load (empfohlene Metrik)		Byte	Der von Live-Daten auf einem Knoten verwendete Speicherplatz.
cassandra.uptime (empfohlene Metrik)		seconds	
cassandra.heap.used (empfohlene Metrik)		Byte	
cassandra.heap.total (empfohlene Metrik)		Byte	
cassandra.exceptions		count	Anzahl der erfassten internen Ausnahmen. Unter normalen Ausnahmebedingungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			sollte dieser Wert null sein.
cassandra.key_cache.	size	Byte	Gesamtgröße des belegten Cache in Byte.
cassandra.key_cache.	capacity	Byte	Cache-Kapazität in Byte.
cassandra.key_cache.	hits	count	Gesamtzahl der Cache-Treffer.
cassandra.key_cache. (empfohlene Metrik)	requests	count	Gesamtzahl der Cache-Anforderungen.
cassandra.key_cache. (empfohlene Metrik)	hit_rate	count	Cache-Trefferquote (gesamte Zeitspanne).
cassandra.compaction	stats.pending_tasks	count	Anzahl der ausstehenden Komprimierungen.
cassandra.threadpool.	ReadStage.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Lokale Lesevorgänge, die für diesen Thread-Pool in dieser ReadStage ausgeführt werden.
cassandra.threadpool.	ReadStage.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	ReadStage.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	ReadStage.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	MiscStage.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verschiedene in dieser Phase

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			ausgeführte Aufgaben.
cassandra.threadpool.	MiscStage.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	MiscStage.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	MiscStage.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	CompactionExecutor.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Komprimierungen werden für diese Threads ausgeführt.
cassandra.threadpool.	CompactionExecutor.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	CompactionExecutor.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	CompactionExecutor.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	MutationStage.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich für alle anderen Schreibvorgänge.
cassandra.threadpool.	MutationStage.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	MutationStage.completed	count	Anzahl der abgeschlossenen Aufgaben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.threadpool.	MutationStage.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	MemtableReclaimMemory.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Memtable-Recycling.
cassandra.threadpool.	MemtableReclaimMemory.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	MemtableReclaimMemory.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	MemtableReclaimMemory.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	PendingRangeCalculator.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Berechnet den Tokenbereich.
cassandra.threadpool.	PendingRangeCalculator.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	PendingRangeCalculator.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	PendingRangeCalculator.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	GossipStage.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Behandelt Gossip-Anforderungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.threadpool.	GossipStage.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	GossipStage.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	GossipStage.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	SecondaryIndexManagement.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Führt Aktualisierungen von sekundären Indizes durch.
cassandra.threadpool.	SecondaryIndexManagement.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	SecondaryIndexManagement.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	SecondaryIndexManagement.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	HintsDispatcher.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Führt eine angedeutete Übergabe (hinted Handoff) durch.
cassandra.threadpool.	HintsDispatcher.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	HintsDispatcher.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	HintsDispatcher.blocked	count	Anzahl der Aufgaben, die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.RequestResponseStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Koordinatoranforderungen an den Cluster werden in diesem Thread-Pool ausgeführt.
cassandra.threadpool.RequestResponseStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.RequestResponseStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.RequestResponseStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.ReadRepairStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Die Lesereparatur (Read Repair) erfolgt in diesem Thread-Pool.
cassandra.threadpool.ReadRepairStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.ReadRepairStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.ReadRepairStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.CounterMutationStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Verantwortlich für Zählerschreibvorgänge.
cassandra.threadpool.CounterMutationStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.CounterMutationStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.CounterMutationStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.MigrationStage.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Führt Schemamigrationen aus.
cassandra.threadpool.MigrationStage.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.MigrationStage.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.MigrationStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.MemtablePostFlush.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Bereinigt das Commit-Protokoll, nachdem die Memtable auf den Datenträger geschrieben wurde.
cassandra.threadpool.MemtablePostFlush.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.threadpool.MemtablePostFlush.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.MemtablePostFlush.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.PerDiskMemtableFlushWriter_0.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich für das Schreiben einer Spezifikation (pro Datenträger (0–N) gibt es eine davon).
cassandra.threadpool.PerDiskMemtableFlushWriter_0.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.PerDiskMemtableFlushWriter_0.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.PerDiskMemtableFlushWriter_0.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.ValidationExecutor.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Führt eine Validierungskomprimierung oder -bereinigung durch.
cassandra.threadpool.ValidationExecutor.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.ValidationExecutor.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.ValidationExecutor.blocked		count	Anzahl der Aufgaben, die aufgrund von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	Sampler.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich für die Neufestlegung der Indexzusammenfassungen von *SStables*.
cassandra.threadpool.	Sampler.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	Sampler.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	Sampler.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	MemtableFlushWriter.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Schreibt Memtables auf den Datenträger.
cassandra.threadpool.	MemtableFlushWriter.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	MemtableFlushWriter.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	MemtableFlushWriter.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	InternalResponseStage.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			für clusterinterne Rückrufe.
cassandra.threadpool.	InternalResponseStage.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	InternalResponseStage.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	InternalResponseStage.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	ViewMutationStage.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Verantwortlich für Schreibvorgänge in der materialisierten Ansicht.
cassandra.threadpool.	ViewMutationStage.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	ViewMutationStage.completed	count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.	ViewMutationStage.blocked	count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.	AntiEntropyStage.active	count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Erstellt einen Hash-Baum für Reparaturen.
cassandra.threadpool.	AntiEntropyStage.pending	count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.	AntiEntropyStage.completed	count	Anzahl der abgeschlossenen Aufgaben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.threadpool.AntiEntropyStage.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.threadpool.CacheCleanupExecutor.active		count	Anzahl der Aufgaben, an denen dieser Pool aktiv arbeitet. Für diesen Thread-Pool durchgeführte Cache-Wartung.
cassandra.threadpool.CacheCleanupExecutor.pending		count	Anzahl der Aufgaben in der Warteschlange in diesem Pool.
cassandra.threadpool.CacheCleanupExecutor.completed		count	Anzahl der abgeschlossenen Aufgaben.
cassandra.threadpool.CacheCleanupExecutor.blocked		count	Anzahl der Aufgaben, die aufgrund von Warteschlangensättigung blockiert wurden.
cassandra.message_type.READ.dropped		count	Anzahl der gelöschten Nachrichten. Reguläre Lesevorgänge.
cassandra.message_type.RANGE_SLICE.dropped		count	Anzahl der gelöschten Nachrichten. Gelesener Tokenbereich.
cassandra.message_type._TRACE.dropped		count	Anzahl der gelöschten Nachrichten. Nachverfolgen von Schreibvorgängen.
cassandra.message_type.HINT.dropped		count	Anzahl der gelöschten Nachrichten. Erneute Wiedergabe von Hinweis.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.message_type.MUTATION.dropped		count	Anzahl der gelöschten Nachrichten. Reguläre Schreibvorgänge.
cassandra.message_type.COUNTER_MUTATION.dropped		count	Anzahl der gelöschten Nachrichten. Zählerschreibvorgänge.
cassandra.message_type.BATCH_STORE.dropped		count	Anzahl der gelöschten Nachrichten. Batchlog-Schreibvorgang.
cassandra.message_type.BATCH_REMOVE.dropped		count	Anzahl der gelöschten Nachrichten. Batchlog-Bereinigung (nach erfolgreicher Anwendung).
cassandra.message_type.REQUEST_RESPONSE.dropped		count	Anzahl der gelöschten Nachrichten. RPC-Rückrufe.
cassandra.message_type.PAGED_RANGE.dropped		count	Anzahl der gelöschten Nachrichten. Lesen als Seite.
cassandra.message_type.READ_REPAIR.dropped		count	Anzahl der gelöschten Nachrichten. Lesereparatur.
cassandra.system_traces.read_count		count	Anzahl der Lesevorgänge für diese Tabelle.
cassandra.system_traces.read_latency			Lokale Leselatenz für diese Tabelle.
cassandra.system_traces.write_count		count	Anzahl der Schreibvorgänge für diese Tabelle.
cassandra.system_traces.write_latency			Lokale Schreiblatenz für diese Tabelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriken – Cassandra-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cassandra.system_traces.pending_flushes		count	Geschätzte Anzahl der ausstehenden Löschaufgaben für diese Tabelle.
cassandra.system.read_count (empfohlene Metrik)		count	
cassandra.system.read_latency (empfohlene Metrik)		Mikrosekunden	
cassandra.system.write_count (empfohlene Metrik)		count	
cassandra.system.write_latency (empfohlene Metrik)		Mikrosekunden	
cassandra.system.pending_flushes		count	
cassandra.system_distributed.read_count		count	
cassandra.system_distributed.read_latency			
cassandra.system_distributed.write_count		count	
cassandra.system_distributed.write_latency			
cassandra.system_distributed.pending_flushes		count	
cassandra.system_schema.read_count		count	
cassandra.system_schema.read_latency			
cassandra.system_schema.write_count		count	
cassandra.system_schema.write_latency			
cassandra.system_schema.pending_flushes		count	
cassandra.system_auth.read_count		count	
cassandra.system_auth.read_latency			
cassandra.system_auth.write_count		count	
cassandra.system_auth.write_latency			
cassandra.system_auth.pending_flushes		count	

Standardprüfungen und -richtlinien für die Verzeichnisscan-Überwachung

Agent Client Collector stellt die folgenden Standardprüfungen und -richtlinien für die Verzeichnisscan-Überwachung bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Ereignis	„check-directory-file-count“	Prüft die Anzahl der Dateien in einem bestimmten Verzeichnis und vergleicht sie mit den angegebenen Schwellenwerten für Warnungen und kritische Werte. Gibt basierend auf den Schwellenwerten für „Kritisch“ und „Warnung“ ein Ereignis „KRITISCH“, „WARNUNG“ oder „OK“ zurück. **Hinweis:** • Zählt die Anzahl der Dateien im Verzeichnis (ohne Dateien in Unterverzeic • Der Agent benötigt Lese- und Ausführungs für das überwachte Verzeichnis.	check-directory-file-count.rb (Optionen) -d, --dir Absoluter Pfad zum Verzeichnis zum Zählen der Dateien (erforderlich) -w, --warning Warnungsschwellenwert (erforderlich) -c, --critical Kritischer Schwellenwert (erforderlich) -H, inklusive_hidden_files „aktiv“ auf **„wahr“** setzen, um ausgeblendete Dateien in die Zählung einzubeziehen (Standardwert ist **„falsch“**) **Anwendungsbeispiel:** `check-directory-file-count.rb -d /path/to/directory -w 50 -c 100` berechtigungen	DirectoryFileCount KRITISCH:<path to dir> hat 165 Dateien.
Ereignis	„check-directory-integrity“	Vergleicht den Zeitpunkt der letzten Änderung des Verzeichnisses mit dem	commonchecks check-directory-integrity (Optionen) -d, --dirpath DIRPATH:	Allgemeine Prüfungen KRITISCH: Verzeichnisintegrität: Changes erkannt für<path to file> innerhalb

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		aktuellen Zeitpunkt, um zu bestimmen, ob innerhalb eines definierten Zeitintervalls Aktualisierungen erfolgt sind. Basierend auf diesem Vergleich gibt die Prüfung ein Ereignis KRITISCH oder OK zurück. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für das überwachte Verzeichnis.	Absoluter Pfad zum zu überprüfenden Verzeichnis (erforderlich). -i, --interval INTERVAL: Zeitintervall in Sekunden, in dem nach aktuellen Updates gesucht wird (erforderlich). Der Standardwert kann auf 180 Sekunden festgelegt werden. **Anwendungsbeispiel:** `commonchecks check-directory-update -d /path/to/directory -i 180`	der letzten 180 Sekunden (zuletzt geändert: Mi, 04. Dez. 2024 12:18:55 EST).
Ereignis	check-file-age	Wertet das Alter einer angegebenen Datei aus, indem der Zeitpunkt der letzten Änderung mit dem aktuellen Zeitpunkt verglichen wird. Löst eine Warnung aus, wenn die Datei die definierten Schwellenwerte für das Alter von „Kritisch“ oder „Warnung“ überschreitet.	commonchecks check-file-age (Optionen) -f, --filepath FILEPATH: Absoluter Pfad zu der zu überprüfenden Datei (erforderlich). -c, --critical KRITISCH: Schwellenwert für kritisches Alter in Minuten für die Datei (erforderlich).	Allgemeine Prüfungen OK: Datei<path to file> Alter: 30 Minuten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Hinweis: Der Agent benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	-w, --warning WARNUNG: Altersschwellenwert für Warnung in Minuten für die Datei (erforderlich). **Anwendungsbeispiel:** `commonchecks check-file-age -f /path/to/file.txt -c 120 -w 60`	
Ereignis	Überprüfe-Datei-Antwortzeit	Vergleicht die Zeit, die zum Lesen einer angegebenen Datei benötigt wird, und vergleicht sie mit den Schwellenwerten für „Kritisch“ und „Warnung“. Basierend auf diesem Vergleich gibt die Prüfung ein Ereignis KRITISCH oder OK zurück. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	commonchecks check-file-response-time (Optionen) -f, --filepath FILEPATH: Absoluter Pfad zu der zu überprüfenden Datei (erforderlich). -c, --critical KRITISCH: Kritischer Schwellenwert in Sekunden für die Dateiantwortzeit (erforderlich). -w, --warning WARNUNG: Warnschwellenwert in Sekunden für Dateiantwortzeit (erforderlich). -t, --timeout TIMEout: Maximal zulässige Zeit zum Lesen des Dateiinhalts in Sekunden. Zeitüberschreitungswert muss größer als der kritische	Allgemeine Prüfungen OK: Antwortzeit beim Lesen der Datei: 0,0020 Sekunden für Dateiname: / var/log/ servicenow/ agent-client-collector/ acc.log.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Schwellenwert sein. **Anwendungsbeispiel:** `commonchecks check-file-response-time -f /var/log/servicenow/agent-client-collector/acc.log -c 10 -w 5 -t 20`	
Ereignis	überprüfe-Dateigröße	Misst die Größe einer Datei (die tatsächliche Menge der darin enthaltenen Daten) und vergleicht sie mit den angegebenen Schwellenwerten. Gibt basierend auf dem Vergleich von Dateigröße und Schwellenwerten ein Ereignis „KRITISCH“, „WARNUNG“ oder „OK“ zurück. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	commonchecks check-file-size (Optionen) -f, --filepath FILEPATH Absoluter Pfad zur erforderlichen Datei (erforderlich). -c, --critical KRITISCH. Kritischer Schwellenwert in Kilobyte. Als Zahl ohne Einheiten angeben (z. B. 1000 für 1000 KB) (erforderlich) -w, --warning WARNUNG. Warnungsschwellenwert in Kilobyte. Als Zahl ohne Einheiten angeben (z. B. 500 für 500 KB) (erforderlich) **Anwendungsbeispiel:** `commonchecks check-file-size -f C:\ProgramData\ServiceNow\agent-client-collector`	Allgemeine Prüfungen OK: Für Datei<path to file> Größe: 4,72 KB liegt innerhalb der Schwellenwerte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			`\config \acc.yml`	
Ereignis	check-file-space	Misst die Größe einer Datei auf einem Datenträger anhand der angegebenen Schwellenwerte und gibt basierend auf den Schwellenwerten ein Ereignis KRITISCH, WARNUNG oder OK zurück. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	commonchecks check-file-space (Optionen) -f, --filepath FILEPATH: Absoluter Pfad zur relevanten Datei (erforderlich). -c, --critical KRITISCH: Schwellenwert für „Kritisch“ in Kilobyte. Angegeben als Zahl ohne Einheiten (z. B. 1000 für 1000 KB) (erforderlich) -w, --warning WARNUNG: Warnungsschwellenwert in Kilobyte. Angegeben als Zahl ohne Einheiten (z. B. 500 für 500 KB) (erforderlich) -b, --blocksize BLOCKSIZE: Blockgröße in Byte (Standard = 4096) (erforderlich) **Anwendungsbeispiel:** `commonchecks check-file-space -f C:\ProgramData\ServiceNow\agent-client-collector`	Allgemeine Prüfungen OK: Datei<path to file> Speicherplatz: 8,00 KB liegen innerhalb des Schwellenwerts

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			`\config \acc.yml`	
Ereignis	os.windows.check-directory-space	Überprüft den Speicherplatz, der vom Inhalt eines Verzeichnisses belegt wird. Gibt ein Ereignis KRITISCH, WARNUNG oder OK zurück, basierend auf dem Vergleich mit den angegebenen Schwellenwerten für den Schweregrad von kritischen Ereignissen und Warnungsereignissen. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für das überwachte Verzeichnis.	Winchecks check-dir-space (Optionen) -d, --dirpath DIRPATH: Absoluter Pfad zum zu überprüfenden Verzeichnis (erforderlich). -c, --critical KRITISCH: Schwellenwert für kritischen Speicherplatz in Kilobyte (erforderlich). -w, --warning WARNUNG: Warnung: Speicherplatzschwellenwert in Kilobyte (erforderlich). -t, --timeout TIMEout: Maximal zulässige Zeit für die Berechnung der Verzeichnisgröße, angegeben in Sekunden (erforderlich). **Anwendungsbeispiel:** `Winchecks check-dir-space -d /path/to/directory -c 1000 -w 500 -t 120`	Windows-Prüfungen OK: Verzeichnis<path to file> Platz: 369,25 KB liegen innerhalb der Schwellenwerte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Ereignis	„check-directory-file-count“	Prüft die Anzahl der Dateien in einem bestimmten Verzeichnis und vergleicht sie mit den angegebenen Schwellenwerten für Warnungen und kritische Werte. Gibt basierend auf den Schwellenwerten für „Kritisch“ und „Warnung“ ein Ereignis „KRITISCH“, „WARNUNG“ oder „OK“ zurück. **Hinweis:** • Zählt die Anzahl der Dateien im Verzeichnis (ohne Dateien in Unterverzeic • Der Agent benötigt Lese- und Ausführungs für das überwachte Verzeichnis.	check-directory-file-count.rb (Optionen) -d, --dir Absoluter Pfad zum Verzeichnis zum Zählen der Dateien (erforderlich) -w, --warning Warnungsschwellenwert (erforderlich) -c, --critical Kritischer Schwellenwert (erforderlich) -H, inklusive_hidden_files „aktiv“ auf **„wahr“** setzen, um ausgeblendete Dateien in die Zählung einzubeziehen (Standardwert ist **„falsch“**) **Anwendungsbeispiel:** `check-directory-file-count.rb -d /path/to/directory -w 50 -c 100` berechtigungen	DirectoryFileCount KRITISCH:<path to dir> hat 165 Dateien.
Ereignis	„check-directory-integrity“	Vergleicht den Zeitpunkt der letzten Änderung des Verzeichnisses mit dem	commonchecks check-directory-integrity (Optionen) -d, --dirpath DIRPATH:	Allgemeine Prüfungen KRITISCH: Verzeichnisintegrität: Changes erkannt für<path to file> innerhalb

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		aktuellen Zeitpunkt, um zu bestimmen, ob innerhalb eines definierten Zeitintervalls Aktualisierungen erfolgt sind. Basierend auf diesem Vergleich gibt die Prüfung ein Ereignis KRITISCH oder OK zurück. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für das überwachte Verzeichnis.	Absoluter Pfad zum zu überprüfenden Verzeichnis (erforderlich). -i, --interval INTERVAL: Zeitintervall in Sekunden, in dem nach aktuellen Updates gesucht wird (erforderlich). Der Standardwert kann auf 180 Sekunden festgelegt werden. **Anwendungsbeispiel:** `commonchecks check-directory-update -d /path/to/directory -i 180`	der letzten 180 Sekunden (zuletzt geändert: Mi, 04. Dez. 2024 12:18:55 EST).
Ereignis	check-file-age	Wertet das Alter einer angegebenen Datei aus, indem der Zeitpunkt der letzten Änderung mit dem aktuellen Zeitpunkt verglichen wird. Löst eine Warnung aus, wenn die Datei die definierten Schwellenwerte für das Alter von „Kritisch“ oder „Warnung“ überschreitet.	commonchecks check-file-age (Optionen) -f, --filepath FILEPATH: Absoluter Pfad zu der zu überprüfenden Datei (erforderlich). -c, --critical KRITISCH: Schwellenwert für kritisches Alter in Minuten für die Datei (erforderlich).	Allgemeine Prüfungen OK: Datei<path to file> Alter: 30 Minuten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Hinweis: Der Agent benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	-w, --warning WARNUNG: Altersschwellenwert für Warnung in Minuten für die Datei (erforderlich). **Anwendungsbeispiel:** `commonchecks check-file-age -f /path/to/file.txt -c 120 -w 60`	
Ereignis	Überprüfe-Datei-Antwortzeit	Vergleicht die Zeit, die zum Lesen einer angegebenen Datei benötigt wird, und vergleicht sie mit den Schwellenwerten für „Kritisch“ und „Warnung“. Basierend auf diesem Vergleich gibt die Prüfung ein Ereignis KRITISCH oder OK zurück. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	commonchecks check-file-response-time (Optionen) -f, --filepath FILEPATH: Absoluter Pfad zu der zu überprüfenden Datei (erforderlich). -c, --critical KRITISCH: Kritischer Schwellenwert in Sekunden für die Dateiantwortzeit (erforderlich). -w, --warning WARNUNG: Warnschwellenwert in Sekunden für Dateiantwortzeit (erforderlich). -t, --timeout TIMEout: Maximal zulässige Zeit zum Lesen des Dateiinhalts in Sekunden. Zeitüberschreitungswert muss größer als der kritische	Allgemeine Prüfungen OK: Antwortzeit beim Lesen der Datei: 0,0020 Sekunden für Dateiname: / var/log/ servicenow/ agent-client-collector/ acc.log.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Schwellenwert sein. **Anwendungsbeispiel:** `commonchecks check-file-response-time -f /var/log/servicenow/agent-client-collector/acc.log -c 10 -w 5 -t 20`	
Ereignis	überprüfe-Dateigröße	Misst die Größe einer Datei (die tatsächliche Menge der darin enthaltenen Daten) und vergleicht sie mit den angegebenen Schwellenwerten. Gibt basierend auf dem Vergleich von Dateigröße und Schwellenwerten ein Ereignis „KRITISCH“, „WARNUNG“ oder „OK“ zurück. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	commonchecks check-file-size (Optionen) -f, --filepath FILEPATH Absoluter Pfad zur erforderlichen Datei (erforderlich). -c, --critical KRITISCH. Kritischer Schwellenwert in Kilobyte. Als Zahl ohne Einheiten angeben (z. B. 1000 für 1000 KB) (erforderlich) -w, --warning WARNUNG. Warnungsschwellenwert in Kilobyte. Als Zahl ohne Einheiten angeben (z. B. 500 für 500 KB) (erforderlich) **Anwendungsbeispiel:** `commonchecks check-file-size -f C:\ProgramData\ServiceNow\agent-client-collector`	Allgemeine Prüfungen OK: Für Datei<path to file> Größe: 4,72 KB liegt innerhalb der Schwellenwerte

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			`\config \acc.yml`	
Ereignis	check-file-space	Misst die Größe einer Datei auf einem Datenträger anhand der angegebenen Schwellenwerte und gibt basierend auf den Schwellenwerten ein Ereignis KRITISCH, WARNUNG oder OK zurück. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für die überwachte Datei.	commonchecks check-file-space (Optionen) -f, --filepath FILEPATH: Absoluter Pfad zur relevanten Datei (erforderlich). -c, --critical KRITISCH: Schwellenwert für „Kritisch“ in Kilobyte. Angegeben als Zahl ohne Einheiten (z. B. 1000 für 1000 KB) (erforderlich) -w, --warning WARNUNG: Warnungsschwellenwert in Kilobyte. Angegeben als Zahl ohne Einheiten (z. B. 500 für 500 KB) (erforderlich) -b, --blocksize BLOCKSIZE: Blockgröße in Byte (Standard = 4096) (erforderlich) **Anwendungsbeispiel:** `commonchecks check-file-space -f C:\ProgramData\ServiceNow\agent-client-collector`	Allgemeine Prüfungen OK: Datei<path to file> Speicherplatz: 8,00 KB liegen innerhalb des Schwellenwerts

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			`\config \acc.yml`	
Ereignis	os.linux.check-directory-size	Überprüft den im Verzeichnis eines Datenträgers zugewiesenen Speicherplatz und vergleicht ihn mit den angegebenen Schwellenwerten für „Kritisch“ und „Warnung“. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für das überwachte Verzeichnis.	linuxchecks check-directory-size (Optionen) -d, --dirpath DIRPATH: Absoluter Pfad zum zu überprüfenden Verzeichnis (erforderlich). -c, --critical KRITISCH: Schwellenwert für kritischen Speicherplatz in Kilobyte (erforderlich). -w, --warning WARNUNG: Warnung: Speicherplatzschwellenwert in Kilobyte (erforderlich). -t, --timeout TIMEout: Maximal zulässige Zeit für die Berechnung der Verzeichnisgröße, angegeben in Sekunden (erforderlich). **Anwendungsbeispiel:** `linuxchecks check-directory-size -d Pfad/zu/Verzeichnis -c 100 -w 50 -t 30`	Linux prüft KRITISCH: Verzeichnis<path to file> Größe: 500,00 KB überschreitet den kritischen Schwellenwert von 10,00 KB
Ereignis	os.linux.check-directory-space	Überprüft den Speicherplatz, der vom Verzeichnisinhalt	linuxchecks check-directory-space (Optionen)	Linux prüft KRITISCH: Verzeichnis<path to file>

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		belegt wird. Gibt basierend auf dem Vergleich mit den Schwellenwerten für „Kritisch“ und „Warnung“ ein Ereignis „KRITISCH“, „WARNUNG“ oder „OK“ zurück. **Hinweis:** Der Agent benötigt Lese- und Ausführungsberechtigungen für das überwachte Verzeichnis.	-d, --dirpath DIRPATH: Absoluter Pfad zum zu überprüfenden Verzeichnis (erforderlich). -c, --critical KRITISCH: Schwellenwert für kritischen Speicherplatz in Kilobyte (erforderlich). -w, --warning WARNUNG: Warnung: Speicherplatzschwellenwert in Kilobyte (erforderlich). -t, --timeout TIMEout: Maximal zulässige Zeit für die Berechnung der Verzeichnisgröße, angegeben in Sekunden (erforderlich). **Anwendungsbeispiel:** `linuxchecks check-directory-space -d /path/to/directory -c 10 -w 5 -t 30`	Speicherplatz: 374,00 KB überschreitet den kritischen Schwellenwert von 10,00 KB

Automatische Übersetzung

GlassFish – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für die GlassFish-Systemüberwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für GlassFish-Metriken

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe

Metrik	glassfish.metric-jvm-level	Ruft die JVM-Metriken des GlassFish-Servers ab.
		
		Erfordert Anmeldeinformatio für die Standardauthentifizi
			`-i, --instance Glassfish Monitoring Instance Name (required) -p, --password Glassfish password -P, --port Glassfish API port --ssl Enable secure connnection to Glassfish -u –username Glassfish username`
			
			Verwendungsbeispiel:
			`metric-glassfish-jvm-level.rb {{if .labels.params_port}} -P {{.labels.params_port}} {{end}} -i {{.labels.params_glassfish_server_instance`
				`glassfish.jvm.garbage-collectors.Scavenge.Collect 200 0 1652959788`

Metrik	glassfish.metric-server-requests	Macht HTTP-Anforderungsmetrik für alle auf dem GlassFish-Server bereitgestellten Anwendungen verfügbar. Erfordert Anmeldeinformatio für die Standardauthentifizi	`-i, --instance Glassfish Monitoring Instance Name (required) -p, --password Glassfish password -P, --port Glassfish API port --ssl Enable`	`glassfish.http-service.server.request.Cour 200 0 1652959788`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für GlassFish-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			secure connnection to Glassfish -u –username Glassfish username Verwendungsbeispiel: metric-glassfish-server-requests.rb -i {{.labels.params_glassfish_server_instance {{if .labels.params_port}} -P {{.labels.params_port}} {{end}}	
Metrik	glassfish.metric-server-resources	Macht Metriken der auf dem GlassFish-Server bereitgestellten Ressourcen verfügbar. Erfordert Anmeldeinformation für die Standardauthentifizi	-i, --instance Glassfish Monitoring Instance Name (required) -P, --port Glassfish API port -r --resource_pool Resource Pool Name --ssl Enable secure connnection to Glassfish -u –username Glassfish username -p --password Glassfish password	glassfish.resources.{{PoolName}}.AverageConnWai 0 1652959936

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für GlassFish-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Verwendungsbeispiel: `metric-glassfish-server-resources.rb {{if .labels.params_port}} -P {{.labels.params_port}} {{end}} {{if .labels.params_resource_pool}} -r {{.labels.params_resource_pool}} {{end}} -i {{.labels.params_glassfish_server_instance`	

Metrik	glassfish.metric-transaction-service	Macht Metriken für alle Transaktionen in Anwendungen verfügbar, die auf dem GlassFish-Server bereitgestellt wurden.
		
		Erfordert Anmeldeinformatio für die Standardauthentifizi
			`-i, --instance Glassfish Monitoring Instance Name (required) -P, --port Glassfish API port --ssl Enable secure connnection to Glassfish -u –username Glassfish username -p --password Glassfish password`
			
			Verwendungsbeispiel:
			`metric-glassfish-transaction-service.rb {{if .labels.params_port}} -P {{.labels.params_port}} {{end}} -i {{.labels.params_glassfish_server_instance`
				`Glassfish.transaction-service.ActiveCount 0 1652959977`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für GlassFish-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe

Metrik	glassfish.metrics-deployed-apps	Macht Metrikausgaben von Anwendungen verfügbar, die auf dem GlassFish-Server bereitgestellt wurden.
		
		Erfordert Anmeldeinformatio für die Standardauthentifizi
			`-a, --apps Application deployed on Glassfish server (required) -i, --instance Glassfish Monitoring Instance Name (required) -P, --port Glassfish API port --ssl Enable secure connnection to Glassfish -u –username Glassfish username -p --password Glassfish password`
			
			Verwendungsbeispiel:
			`metric-glassfish-deployed-applications.rb {{if .labels.params_port}} -P {{.labels.params_port}} {{end}} -a {{.labels.params_deployed_apps}} -i {{.labels.params_glassfish_server_instance`
				`glassfish.applications.{{Deployed Application}}.ActivatedSess 0 1652959665`

Metrik	glassfish.metrics-deployment-lifecycle	Stellt Lebenszyklusmetrike der GlassFish-Serveranwendunge bereit.	`metric-glassfish-deployment-lifecycle.rb (options) -i, --instance`	`glassfish.deployment.lifecy 2 1653022649`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für GlassFish-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Erfordert Anmeldeinformatio für die Standardauthentifizi	Glassfish Monitoring Instance Name (required) -p --password Glassfish password -P, --port Glassfish API port --ssl Enable secure connnection to Glassfish -u –username Glassfish username Verwendungsbeispiel: `metric-glassfish-deployment-lifecycle.rb {{if .labels.params_port}} -P {{.labels.params_port}} {{end}} -i {{.labels.params_glassfish_server_instance`	

GlassFish-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von GlassFish-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

glassfish.metrics-deployed-apps – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.applications.{Deployed Application}.TotalServletsLoaded	Deployed Application	count	Gesamtanzahl der bisher geladenen Servlets.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metrics-deployed-apps – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
	(Bereitgestellte Anwendung)		
glassfish.applications.{Deployed Application}.ServletProcessingTimes	Deployed Application (Bereitgestellte Anwendung)	ms	Kumulative Servlet-Verarbeitungszeiten.
glassfish.applications.{Deployed Application}.ActiveServlets	Deployed Application (Bereitgestellte Anwendung)	count	Anzahl der geladenen Servlets.
glassfish.applications.{Deployed Application}.ExpiredSessionsTotal (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher abgelaufenen Sitzungen.
glassfish.applications.{Deployed Application}.PassivatedSessionsTotal	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher passivierten Sitzungen.
glassfish.applications.{Deployed Application}.ActivatedSessionsTotal	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher aktivierten Sitzungen.
glassfish.applications.{Deployed Application}.SessionsTotal	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher erstellten Sitzungen.
glassfish.applications.{Deployed Application}.RejectedSessionsTotal (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher abgelehnten Sitzungen.
glassfish.applications.{Deployed Application}.PersistedSessionsTotal	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher bestehen bleibenden Sitzungen.
glassfish.applications.{Deployed Application}.ActiveSessions (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	count	Anzahl der aktiven Sitzungen.
glassfish.applications.{Deployed Application}.RequestCount	Deployed Application (Bereitgestellte Anwendung)	count	Kumulative Anzahl der bisher verarbeiteten Anforderungen
glassfish.applications.{Deployed	Deployed Application	ms	Längste Antwortzeit für eine Anforderung;

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metrics-deployed-apps – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
Application}.MaxTime (empfohlene Metrik)	(Bereitgestellte Anwendung)		kein kumulativer Wert, sondern die längste Antwortzeit unter den Antwortzeiten.
glassfish.applications.{Deployed Application}.ErrorCount (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	count	Kumulativer Wert der Fehleranzahl. Dabei stellt die Fehleranzahl die Anzahl der Fälle dar, in denen der Antwortcode größer oder gleich 400 war.
glassfish.applications.{Deployed Application}.ProcessingTime	Deployed Application (Bereitgestellte Anwendung)	ms	Durchschnittliche Anforderungsverarbeitungsdauer.
glassfish.applications.{Deployed Application}.TotalJspCount	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der bisher geladenen JSP-Seiten.
glassfish.applications.{Deployed Application}.JspCount	Deployed Application (Bereitgestellte Anwendung)	count	Anzahl der aktiven JSP-Seiten.
glassfish.applications.{Deployed Application}.JspErrorCount (empfohlene Metrik)	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der durch Aufrufe von JSP-Seiten ausgelösten Fehler.
glassfish.applications.{Deployed Application}.JspReloadedCount	Deployed Application (Bereitgestellte Anwendung)	count	Gesamtanzahl der neu geladenen JSP-Seiten.

glassfish.metrics-deployment-lifecycle – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.deployment.lifecycle.ActiveApplications (empfohlene Metrik)		count	Gesamtanzahl der bisher bereitgestellten Anwendungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metrics-deployment-lifecycle – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.deployment.lifecycle.TotalApplicationsDeployed (empfohlene Metrik)		Count	Anzahl der bereitgestellten Anwendungen.

glassfish.metric-server-requests – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.http-service.server.request.Count200		count	Anzahl der Antworten mit Statuscode 200.
glassfish.http-service.server.request.Count2xx		count	Anzahl der Antworten mit einem Statuscode im Bereich 2xx.
glassfish.http-service.server.request.Count302		count	Anzahl der Antworten mit Statuscode 302.
glassfish.http-service.server.request.Count304		count	Anzahl der Antworten mit Statuscode 304.
glassfish.http-service.server.request.Count3xx		count	Anzahl der Antworten mit einem Statuscode im Bereich 3xx.
glassfish.http-service.server.request.Count400		count	Anzahl der Antworten mit Statuscode 400.
glassfish.http-service.server.request.Count401		count	Anzahl der Antworten mit Statuscode 401.
glassfish.http-service.server.request.Count403		count	Anzahl der Antworten mit Statuscode 403.
glassfish.http-service.server.request.Count404		count	Anzahl der Antworten mit Statuscode 404.
glassfish.http-service.server.request.Count4xx		count	Anzahl der Antworten mit einem Statuscode im Bereich 4xx.
glassfish.http-service.server.request.Count503		count	Anzahl der Antworten mit Statuscode 503.
glassfish.http-service.server.request.Count5xx		count	Anzahl der Antworten mit einem Statuscode im Bereich 5xx.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metric-server-requests – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.http-service.server.request.MaxTime		ms	Längste Antwortzeit für eine Anforderung; kein kumulativer Wert, sondern die längste Antwortzeit unter den Antwortzeiten.
glassfish.http-service.server.request.CountBytesReceived (empfohlene Metrik)		count	Anzahl der empfangenen Bytes.
glassfish.http-service.server.request.CountBytesTransmitted (empfohlene Metrik)		count	Anzahl der übertragenen Bytes.
glassfish.http-service.server.request.RequestCount (empfohlene Metrik)		count	Kumulative Anzahl der bisher verarbeiteten Anforderungen.
glassfish.http-service.server.request.CountOpenConnections		count	Anzahl der offenen Verbindungen.
glassfish.http-service.server.request.ProcessingTime (empfohlene Metrik)		ms	Durchschnittliche Anforderungsverarbeitungsdauer.

glassfish.metric-jvm-level – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.jvm.garbage-collectors.Scavenge.CollectionCount		count	Gesamtanzahl der aufgetretenen Sammlungen.
glassfish.jvm.garbage-collectors.Scavenge.CollectionTime		ms	Ungefähre verstrichene Erfassungszeit in Millisekunden.
glassfish.jvm.garbage-collectors.MarkSweepCompact.CollectionCount		count	Gesamtanzahl der aufgetretenen Sammlungen.
glassfish.jvm.garbage-collectors.MarkSweepCompact.CollectionTime		ms	Ungefähre verstrichene Erfassungszeit in Millisekunden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metric-jvm-level – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.jvm.memory.CommittedHeapSize		Bytes	Menge an Arbeitsspeicher in Byte, die für die Verwendung durch die Java Virtual Machine festgeschrieben ist.
glassfish.jvm.memory.CommittedNonHeapSize		Bytes	Menge an Arbeitsspeicher in Byte, die für die Verwendung durch die Java Virtual Machine festgeschrieben ist.
glassfish.jvm.memory.InitHeapSize		Bytes	Menge an Arbeitsspeicher in Byte, die von der Java Virtual Machine anfänglich vom Betriebssystem für die Speicherverwaltung angefordert wird.
glassfish.jvm.memory.InitNonHeapSize		Bytes	Menge an Arbeitsspeicher in Byte, die von der Java Virtual Machine anfänglich vom Betriebssystem für die Speicherverwaltung angefordert wird.
glassfish.jvm.memory.MaxHeapSize (empfohlene Metrik)		Bytes	Maximale Arbeitsspeichermenge in Byte, die für die Speicherverwaltung verwendet werden kann.
glassfish.jvm.memory.MaxNonHeapSize		Bytes	Maximale Arbeitsspeichermenge in Byte, die für die Speicherverwaltung verwendet werden kann.
glassfish.jvm.memory.ObjectPendingFinalizationCount		Count	Ungefähre Anzahl von Objekten, für die die Finalisierung aussteht.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metric-jvm-level – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.jvm.memory.UsedHeapSize		Bytes	Menge des verwendeten Arbeitsspeichers in Byte.
glassfish.jvm.memory.UsedNonHeapSize		Bytes	Menge des verwendeten Arbeitsspeichers in Byte.

glassfish.metric-transaction-service – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfish.transaction-service.ActiveCount (empfohlene Metrik)		count	Gibt die Anzahl der derzeit aktiven Transaktionen an.
glassfish.transaction-service.CommittedCount (empfohlene Metrik)		count	Stellt die Anzahl der Transaktionen bereit, für die ein Commit ausgeführt wurde.
glassfish.transaction-service.RolledBackCount (empfohlene Metrik)		count	Stellt die Anzahl der Transaktionen bereit, für die ein Rollback ausgeführt wurde.

glassfish.metric-server-resources – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfis.resources.{PoolName}.AverageConnWaitTime	PoolName	ms	Durchschnittliche Dauer der Wartezeit pro erfolgreicher Verbindungsanforderung.
glassfis.resources.{PoolName}.ConnRequestWaitTime	PoolName	ms	Die längsten und kürzesten Wartezeiten von Verbindungsanforderungen. Der aktuelle Wert gibt die Wartezeit der letzten Anforderung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metric-server-resources – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			an, die vom Pool verarbeitet wurde.
glassfis.resources.{PoolName}.NumConn	PoolName Acquired	count	Anzahl der aus dem Pool abgerufenen logischen Verbindungen.
glassfis.resources.{PoolName}.NumConn	PoolName Created	count	Die Anzahl der physischen Verbindungen, die seit dem letzten Zurücksetzen erstellt wurden.
glassfis.resources.{PoolName}.NumConn	PoolName Destroyed	count	Anzahl der physischen Verbindungen, die seit dem letzten Zurücksetzen zerstört wurden.
glassfis.resources.{PoolName}.NumConn	PoolName failedValidation	count	Die Gesamtanzahl der Verbindungen im Verbindungspool, bei denen die Validierung von der Startzeit bis zum Zeitpunkt der letzten Abtastung fehlgeschlagen ist.
glassfis.resources.{PoolName}.NumConn	PoolName Free	count	Die Gesamtanzahl der freien Verbindungen im Pool zum Zeitpunkt der letzten Abtastung.
glassfis.resources.{PoolName}.NumConn	PoolName notSuccessfullyMatched	count	Anzahl der während des Abgleichs abgelehnten Verbindungen.
glassfis.resources.{PoolName}.NumConn	PoolName Released	count	Anzahl der für den Pool freigegebenen logischen Verbindungen.
glassfis.resources.{PoolName}.NumConn	PoolName SuccessfullyMatched	count	Anzahl der erfolgreich abgeglichenen Verbindungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

glassfish.metric-server-resources – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
glassfis.resources.{PoolName}.NumConnTimedOut	PoolName	count	Die Gesamtanzahl der Verbindungen im Pool, bei denen zwischen der Startzeit und dem Zeitpunkt der letzten Abtastung eine Zeitüberschreitung aufgetreten ist.
glassfis.resources.{PoolName}.NumConnUsed	PoolName	count	Stellt Statistiken zur Verbindungsnutzung bereit. Die Gesamtanzahl der derzeit verwendeten Verbindungen sowie Informationen zur maximalen Anzahl der Verbindungen, die verwendet wurden (die Obergrenzenmarkierung).
glassfis.resources.{PoolName}.NumPotentialConnLeak (empfohlene Metrik)	PoolName	count	Anzahl der potenziellen Verbindungsverluste.
glassfis.resources.{PoolName}.WaitQueueLength (empfohlene Metrik)	PoolName	count	Anzahl der Verbindungsanforderungen in der Warteschlange, die darauf warten, verarbeitet zu werden.

Automatische Übersetzung

HAProxy – Standardprüfungen und Richtlinien

Agent Client Collector stellt die folgenden Standardprüfungen und -richtlinien für die Überwachung HAProxy von bereit.

HAProxy Ereignisrichtlinie

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
Event	check-haproxy	Ruft die Details des Lastenausgleichsmo HAProxy ab, um zu bestimmen, ob es ausgeführt wird.	`commonchecks check-haproxy (options) -h host host`	`CheckHAProxy OK: UP: 50% of 4 // services, DOWN: backend/ nginx1[L4CON],`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HAProxy Ereignisrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe

			`-P port Port on which the HAProxy server is running`
			`-A all services all services`
			`-q Path on which HAProxy Stats URI is configured`
			`-use ssl ssl`
			
			Verwendungsbeispiel:
			`check-haproxy.rb -h localhost -P 8080 -A true -q stats -use_ssl false`
				`backend/ BACKEND`

HAProxy Metriken-Richtlinie

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe

Metrik	metrics-check-haproxy	Ruft die Metriken des Lastenausgleichsmo HAProxy ab, um zu bestimmen, ob es ausgeführt wird.	`commonchecks metrics-check-haproxy (options)`
			
			`-q host Path on which HAProxy Stats URI is configured`
			
			`-P port Port on which the HAProxy server is running`
				`<hostname>.haproxy.frontend.session_current 0 1652265603`
				`<hostname>.haproxy.frontend.session_total 0 1652265603`
				`<hostname>.haproxy.backend.session_current 0 1652265603`
				`<hostname>.haproxy.backend.session_t`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HAProxy Metriken-Richtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
			`-c host host name` Verwendungsbeispiel: `metrics-check-haproxy.rb -q stats -P 8080 -c localhost`	`otal 1 1652265603`

HAProxy-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von HAProxy-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Front-End-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
haproxy.frontend.session_current (empfohlene Metrik)		count	Die aktuelle Anzahl der Sitzungen, die zum Ausgeben von Anforderungen verwendet werden.
haproxy.frontend.session_total (empfohlene Metrik)		count	Gesamtanzahl der Sitzungen
haproxy.frontend.bytes_in (empfohlene Metrik)		count	Die Gesamtanzahl der Bytes, die der Server in der letzten Sekunde vom Client empfangen hat.
haproxy.frontend.bytes_out (empfohlene Metrik)		count	Die Gesamtanzahl der vom Server in der letzten Sekunde gesendeten Bytes.
haproxy.frontend.connection_errors (empfohlene Metrik)		count	Die Anzahl der Anforderungen, bei denen beim Versuch, eine Verbindung zu einem Server herzustellen, ein Fehler aufgetreten sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Front-End-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
haproxy.frontend.warning_retries		count	Die Anzahl der erneuten Versuche, eine Verbindung mit einem Server herzustellen.
haproxy.frontend.warning_redispatched		count	Die Häufigkeit, mit der eine Anforderung an einen anderen Server weitergeleitet wurde.
haproxy.frontend.response_1xx		count	HAProxy macht die Anzahl der Antworten nach HTTP-Statuscode - 1xx - verfügbar
haproxy.frontend.response_2xx		count	HAProxy macht die Anzahl der Antworten nach HTTP-Statuscode - 2xx - verfügbar
haproxy.frontend.response_3xx		count	HAProxy gibt die Anzahl der Antworten nach HTTP-Statuscode an – 3xx
haproxy.frontend.response_4xx		count	HAProxy macht die Anzahl der Antworten nach HTTP-Statuscode - 4xx - verfügbar
haproxy.frontend.response_5xx		count	HAProxy gibt die Anzahl der Antworten nach HTTP-Statuscode an – 5xx
haproxy.frontend.response_other		count	HAProxy macht die Anzahl der Antworten von Nicht-HTTP-Anwendungen verfügbar
haproxy.frontend.queue_time		count	Die durchschnittliche Warteschlangenzeit der letzten 1.024 Anforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Front-End-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
haproxy.frontend.connect_time		count	Die durchschnittliche Verbindungszeit der letzten 1.024 Anforderungen.
haproxy.frontend.response_time (empfohlene Metrik)		count	Die Zeit der Antwort an den Client
haproxy.frontend.average_time (empfohlene Metrik)		count	Die durchschnittliche Zeit für die Sitzungen.

Back-End-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
haproxy.backend.session_current (empfohlene Metrik)		count	Die aktuelle Anzahl der Sitzungen, die zum Ausgeben von Anforderungen verwendet werden.
haproxy.backend.session_total (empfohlene Metrik)		count	Gesamtanzahl der Sitzungen
haproxy.backend.bytes_in (empfohlene Metrik)		count	Die Gesamtanzahl der Bytes, die der Server in der letzten Sekunde vom Client empfangen hat.
haproxy.backend.bytes_out (empfohlene Metrik)		count	Die Gesamtanzahl der vom Server in der letzten Sekunde gesendeten Bytes.
haproxy.backend.connection_errors (empfohlene Metrik)		count	Die Anzahl der Anforderungen, bei denen beim Versuch, eine Verbindung zu einem Server herzustellen, ein Fehler aufgetreten sind.
haproxy.backend.warning_retries		count	Die Anzahl der erneuten Versuche, eine Verbindung mit einem Server herzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Back-End-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
haproxy.backend.warning_redispatched		count	Die Häufigkeit, mit der eine Anforderung an einen anderen Server weitergeleitet wurde.
haproxy.backend.response_1xx		count	HAProxy macht die Anzahl der Antworten nach HTTP-Statuscode - 1xx - verfügbar
haproxy.backend.response_2xx		count	HAProxy macht die Anzahl der Antworten nach HTTP-Statuscode - 2xx - verfügbar
haproxy.backend.response_3xx		count	HAProxy gibt die Anzahl der Antworten nach HTTP-Statuscode an – 3xx
haproxy.backend.response_4xx		count	HAProxy macht die Anzahl der Antworten nach HTTP-Statuscode - 4xx - verfügbar
haproxy.backend.response_5xx		count	HAProxy gibt die Anzahl der Antworten nach HTTP-Statuscode an – 5xx
haproxy.backend.response_other		count	HAProxy macht die Anzahl der Antworten von Nicht-HTTP-Anwendungen verfügbar
haproxy.backend.queue_time		count	Die durchschnittliche Warteschlangenzeit der letzten 1.024 Anforderungen.
haproxy.backend.connect_time		count	Die durchschnittliche Verbindungszeit der letzten 1.024 Anforderungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Back-End-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
haproxy.backend.response_time (empfohlene Metrik)		count	Die Zeit der Antwort an den Client
haproxy.backend.average_time (empfohlene Metrik)		count	Die durchschnittliche Zeit für die Sitzungen.
haproxy.backend.num_up		count	

HTTP – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Richtlinien für die HTTP-Systemüberwachung. Richtlinien werden mit den in den folgenden Tabellen angegebenen Prüfungen geliefert.

Richtlinie für HTTP-Einstiegspunktereignisse

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Event	util.check-http-follow-redirect	Überprüft, ob Umleitungslinks in einer festgelegten Anzahl von Anforderungen verfolgt werden können.	Verwendung von check-head-redirect.rb (Optionen): • -A, --auth-first-only: Standardauthentifizierung nur bei der ersten Anforderung verwenden. • -aws-access-key-id: AWS-Zugriffsschlüssel. Legen Sie entweder die Variable ENV["AWS_ACCESS_KEY_ID"] fest, oder geben Sie diese als Option für den Agent an. • -r -aws-region: AWS-Region (Standardwert: us-east-1). • --aws-secret-access-key: Geheimer	Check Head Redirect OK (Überprüfung Head Redirect OK)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für HTTP-Einstiegspunktereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			AWS-Zugriffsschlüssel. Legen Sie entweder die Variable ENV["AWS_SECRET_ACCESS_KEY"] fest, oder geben Sie diese als Option für den Agent an. • -R --redirect: Den ersten <N> Umleitungen folgen • -g --get-redirects: Den ersten <N> Umleitungen mit GET-Anforderungen folgen. • -s, --s3-config-bucket: S3-Konfigurations-Bucket zum Abrufen der Konfiguration. • -k, --s3-config-key: S3-Konfigurationsschlüssel zum Abrufen der Konfiguration. • -u, --url: Die URL muss in `Monitoring HTTP Entrypoint/ cmdb_ci_endpoint_http_list.do` für das CI aktualisiert werden. Die Parameter Aws-region, aws-secret-key, aws-access-key,	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für HTTP-Einstiegspunktereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			s3-config und s3-config-key sind nützlich, wenn Sie keine Verbindungsinformationen in anderen Prüfparametern konfigurieren möchten. Wenn über einen Bucket und einen Schlüssel auf die Umgebung zugegriffen wird, in der die Sensu-Prüfung ausgeführt wird, geben Sie einen AWS-Schlüssel und ein AWS-Token an. Von den Prüfungen wird dann die angegebene JSON-Datei aus S3 abgerufen und die JSON-Konfiguration mit der aktuellen Prüfungskonfiguration zusammengeführt. Verwendungsbeispiel: `command: check-head-redirect.rb -R 10 -u 'https://servicenow.com'`	
Event	util.check-http-response	Überprüft die URL-Antwortzeit und löst ein CRITICAL/ WARNING-Ereignis aus, wenn die verstrichene Zeit die angegebenen CRITICAL/	Verwendung: check-head-redirect.rb (Optionen) • -R, --redirect: Den ersten <N> Umleitungen folgen.	Check Head Redirect OK (Überprüfung Head Redirect OK)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für HTTP-Einstiegspunktereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		WARNING-Schwellenwerte überschreitet. Andernfalls wird ein Ereignis vom Typ OK ausgelöst.	• -w --timeout_warning: Den Schwellenwert für Zeitüberschreitung für „Warnung“ in Millisekunden festlegen. • -c --timeout_critical: Den Schwellenwert für Zeitüberschreitung für „kritisch“ in Millisekunden festlegen. • -u, --url: Die URL muss in `Monitoring HTTP Entrypoint/cmdb_ci_endpoint_http_list.do` für das CI aktualisiert werden. Verwendungsbeispiel: `command: check-head-redirect.rb -R 10 -u 'https://servicenow.com' -w 3000 -c 5000`	

Metrikrichtlinie für HTTP-Einstiegspunkt

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Metrik	util.metrics-http-curl	Ruft Metriken auf HTTP-Endpunkten mit curl ab. Für diese Prüfung ist ein	Verwendung: • -a, --curl_args "CURL ARGS": Zusätzliche	Prüfung erfolgreich ausgeführt. Ausgabe:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikrichtlinie für HTTP-Einstiegspunkt (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		Proxy-Agent erforderlich.	an curl zu übergebende Argumente. • s, --scheme SCHEME: Metrikbenennungsschema, Text, der der Metrik angefügt werden soll (Standardwert: hostname). • -u, --url: Die URL muss in `Monitoring HTTP Entrypoint/ cmdb_ci_endpoint_list.do` für das CI aktualisiert werden. Verwendungsbeispiel: `metrics-curl.rb -u myURL.com -a -Lk`	ws10.curl_timings.time_total 0.219622 1642749209 ws10.curl_timings.time_namelook 0.145474 1642749209 ws10.curl_timings.time_connect 0.151103 1642749209 ws10.curl_timings.time_pretransfe 0.168569 1642749209 ws10.curl_timings.time_redirect 0.095899 1642749209 ws10.curl_timings.time_starttransfe 0.219351 1642749209 ws10.curl_timings.http_code 200 1642749209

HTTP-Einstiegspunktmetriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von HTTP-Einstiegspunktprüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

HTTP-Einstiegspunktmetriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
http_code (empfohlene Metrik)			Statuscode der Anforderung.
time_total (empfohlene Metrik)		milliseconds	Gesamtdauer des Vorgangs.
time_namelookup (empfohlene Metrik)		seconds	Zeit zum Auflösen des Namens in der URL.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTTP-Einstiegspunktmetriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
time_connect (empfohlene Metrik)		seconds	Zeit zum Herstellen der Verbindung zum Remote-Host oder Proxy.
time_pretransfer (empfohlene Metrik)		seconds	Zeit zwischen Start und Beginn der Dateiübertragung. Enthält alle Befehle und Aushandlungen vor der Übertragung.
time_starttransfer (empfohlene Metrik)		seconds	Zeit zwischen Start und Übertragung des ersten Bytes. Enthält *time_pretransfer* und die Zeit, die der Server zur Berechnung des Ergebnisses verwendet hat.
time_redirect (empfohlene Metrik)		seconds	Zeit für alle Umleitungsschritte, einschließlich: • Namenssuche • connect • Vorabübertragung • Übertragung Zeigt die vollständige Ausführungszeit für mehrere Umleitungen an.

HTTP-Antwortcodeprüfung

Agent Client Collector bietet die folgende zusätzliche Prüfung für den HTTP-Antwortcode. Diese Prüfung ist keiner Richtlinie zugeordnet.

HTTP-Antwortcodeprüfung

Typ	Name	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Event	util.check-http-response-code	Löst ein kritisches Ereignis aus, wenn der URL-Antwortcode	`-u, --url URL needs to be updated`	`CheckResponseCode OK : URL is in OK state (CheckResponseCode`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

HTTP-Antwortcodeprüfung (Fortsetzung)

Typ	Name	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		nicht mit dem regulären Ausdruck übereinstimmt. Übergeben Sie die Anmeldeinformation (Benutzername und Passwort) mit sicheren Parametern.	in the Monitoring HTTP Entrypoint/cmdb_ci_endpoint_http_list.do for the CI -r, --response-code Regex string to match the response code. Otherwise, a critical event is raised. Default: 200 -f, --follow_redirects Follows redirect URLs Verwendungsbeispiel: command: check-response-code.rb -u 'https://servicenow.com' -r 2.. -f	OK: URL ist im Status OK). HTTP Response code is 200, matches regex (HTTP-Antwortcode ist 200, entspricht regulärem Ausdruck)

Internet Information Services (IIS) – Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von IIS-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
iis._Total.Web_Service(_Total).Current_Connections (empfohlene Metrik)		count	Gesamtanzahl der aktuellen Verbindungen mit IIS.
iis._Total.Web_Service(_Total).Total_Get_Requests (empfohlene Metrik)		count	Gesamtanzahl der vom IIS-Server empfangenen HTTP-GET-Anforderungen.
iis._Total.Web_Service(_Total).Total_Post_Requests (empfohlene Metrik)		count	Gesamtanzahl der vom IIS-Server empfangenen HTTP-POST-Anforderungen.
iis._Total.Web_Service(_Total).Get_Requests/sec (empfohlene Metrik)		Anzahl pro Sekunde	Rate aller vom IIS-Server empfangenen HTTP-GET-Anforderungen.
iis._Total.Web_Service(_Total).Post_Requests/sec (empfohlene Metrik)		Anzahl pro Sekunde	Rate aller vom IIS-Server empfangenen HTTP-POST-Anforderungen.

Linux – Standardprüfungen und Richtlinien

Agent Client Collector stellt die folgenden Standardprüfungen und -richtlinien für die Überwachung von Linux -Metriken bereit.

Prüfungen der Linux-Überwachungsmetriken

Linux-Metrikrichtlinie

Überprüfen	Metrikname	Ressource	Beschreibung	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
os.linux.metrics-process-usage	proc.acc.running	Prozessname	Anzahl der laufenden Prozesse mit diesem Namen (ACC)	count		
	proc.acc.cpuPercent	Prozessname	Prozentsatz der CPU, die vom Prozess beansprucht wird.	Prozent		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	proc.acc. memPercent	Prozessname	Prozentsatz des vom Prozess belegten Arbeitsspeichers.	Prozent		
os.linux.metrics-reboot-count-today	reboot.count.today	leer	Anzahl der heute durchgeführten Neustarts	count		
os.linux.metrics-system-cpu	cpu.total.user	gesamt	Normale Prozesse, die im Anwendermodus ausgeführt werden; „cpu.total.user“ ist die Summe der cpuN.user-Metriken.	count		
	cpu.total.nice	gesamt	Bearbeitete Prozesse, die im Anwendermodus ausgeführt werden; cpu.total.nice ist die Summe der cpuN.nice-Metriken.	count		
	cpu.total.system	gesamt	Zeit, die die CPU für die Ausführung des Kernels aufgewendet hat. cpu.total.system ist die Summe der cpuN.system-Metriken.	Sek		
	cpu.total.idle	gesamt	Gesamtzeit, die	Sek		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			sich die CPU im Leerlauf verbracht hat. „cpu.total.idle“ ist die Summe der cpuN.idle-Metriken.			
	cpu.total.iowait	gesamt	Gesamtzeit, die die CPU mit Warten auf den Abschluss von E/A-Vorgängen verbracht hat. cpu.total.iowait ist die Summe der cpuN.iowait-Metriken.	Sek		
	cpu.total.irq	gesamt	Gesamtzeit, die der Prozessor für die Verarbeitung von Unterbrechungen verbringt cpu.total.irq ist die Summe der cpuN.irq-Metriken.	Sek		
	cpu.total.softirq	gesamt	Für die Bearbeitung von Anforderungen weicher Unterbrechungen aufgewendete Zeit „cpu.total.softirq“	Sek		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			ist die Summe der cpuN.softirq-Metriken.			
	cpu.total.steal	gesamt	Gesamtzeit, die die virtuelle CPU damit verbracht hat, darauf zu warten, dass der Hypervisor eine andere virtuelle CPU bedient. Gilt nur für virtuelle Computer.	Sek		
	cpu.total.guest	gesamt	Gesamtzeit, die von der CPU für die Ausführung des virtuellen Prozessors aufgewendet wurde. Gilt nur für Hypervisoren.	Sek		
	cpu.total.guest_nice	gesamt	Gesamtzeit, die die CPU als Gast-Betriebssystem ausgeführt hat. cpu.total.guset_nice ist die Summe der cpuN.guest_nice-Metriken	Sek		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	cpu.<cpu-core>.user	cpu-core	Zeit, die für die Verarbeitung mit normaler Priorität im Benutzermodus aufgewendet wurde.	Sek		
	cpu.<cpu-core>.nice	cpu-core	Für verarbeitete Prozesse im Anwendermodus aufgewendete Zeit.	Sek		
	cpu.<cpu-core>.system	cpu-core	Zeitaufwand für die Ausführung im Kernel-Modus.	Sek		
	cpu.<cpu-core>.idle	cpu-core	Zeit, die im Urlaub mit Daumendrücken verbracht wird.	Sek		
	cpu.<cpu-core>.iowait	cpu-core	Zeit, die zum Warten auf den Abschluss von E/A aufgewendet wurde. Dies wird auch als Leerlaufzeit betrachtet.	Sek		
	cpu.<cpu-core>.irq	cpu-core	Zeit, die für die Verarbeitung von Hardware-Interrupts aufgewendet wurde.	Sek		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	cpu.<cpu-core>.softirq	cpu-core	Zeit, die für die Verarbeitung von Software-Interrupts aufgewendet wurde.	Sek		
	cpu.<cpu-core>.steal	cpu-core	Zeit, die von anderen Betriebssystemen vereinnahmt wurde, die in einer virtuellen Umgebung ausgeführt wurden.	Sek		
	cpu.<cpu-core>.guest	cpu-core	Zeit, die für die Ausführung einer virtuellen CPU oder eines Gastbetriebssystems unter der Kontrolle des Kernels aufgewendet wird.	Sek		
	cpu.<cpu-core>.guest_nice	cpu-core	Gesamtzeit, die von der CPU für die Ausführung als Gastbetriebssystem mit nice-Priorität aufgewendet wurde.	Sek		
	cpu.intr	leer	Seit Startzeit verarbeitete Interrupts.	Sek		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	cpu.ctxt	leer	Gesamtanzahl der Kontextwechsel über alle CPUs hinweg.	count		
	cpu.btime	leer	Die Uhrzeit des Systemstarts	Sek		
	cpu.processes	leer	Anzahl der erstellten Prozesse und Threads, einschließlich jener (aber nicht beschränkt auf jene), die durch Aufrufe der Systemaufrufe fork() und clone() erstellt wurden.	count		
	cpu.procs_running	leer	Gesamtanzahl der Prozesse, die auf allen CPUs ausgeführt werden.	count		
	cpu.procs_blocked	leer	Anzahl der derzeit blockierten Prozesse, die auf den Abschluss von E/A warten.	count		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	cpu.cpu_count	leer	Anzahl der CPUs im System	count		
	cpu.<cpu-core>.cores	cpu-core	Die Anzahl der CPU-Kerne	Anzahl der Kerne		
os.linux.metrics-system-cpu-load	load_avg.one	leer	Durchschnittliche Systemauslastung über eine Minute.	Thread-Anzahl	Ja	Ja
	Last_Durchschnitt.Fünf	leer	Durchschnittliche Systemauslastung über fünf Minuten.	Thread-Anzahl	Ja	Ja
	load_avg.fifteen	leer	Durchschnittliche Systemauslastung über 15 Minuten.	Thread-Anzahl	Ja	Ja
	load_avg.norm.one	leer	Durchschnittliche Systemauslastung über eine Minute, normalisiert durch die Anzahl der CPUs.	Thread-Anzahl		
	load_avg.norm.five	leer	Durchschnittliche Systemauslastung über fünf Minuten, normalisiert durch die Anzahl der CPUs.	Thread-Anzahl		
	load_avg.norm.fifteen	leer	Durchschnittliche Systemauslastung über 15 Minuten, normalisiert durch die Anzahl der CPUs.	Thread-Anzahl		
os.linux.metrics-system-cpu-percentage	cpu.avgutilization_percentage	leer	Prozentsatz der CPU wurde	Prozent		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			durchschnittlich verwendet			
	cpu.user_percentage	leer	Prozentsatz der Zeit, in der die CPU insgesamt von normalen Prozessen im Anwendermodus verwendet wurde	Prozent	Ja	Ja
	cpu.nice_ percentage	leer	Prozentsatz der Zeit, in der alle CPUs von bearbeiteten Prozessen im Anwendermodus verwendet werden	Prozent	Ja	Ja
	cpu.system_ percentage	leer	Prozentsatz der Zeit, die die CPU für die Ausführung des Kernels aufgewendet hat.	Prozent	Ja	Ja
	cpu.idle_percentage	leer	Prozentsatz der Zeit, in der sich alle CPUs im Leerlauf befanden	Prozent	Ja	Ja
	cpu.iowait_ percentage	leer	Prozentsatz der Zeit, in der alle CPUs auf den Abschluss von E/A warten	Prozent	Ja	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	cpu.irq_percentage	leer	Prozentsatz der Zeit, in der alle CPUs für Serviceunterbrechungen unterbrochen werden	Prozent	Ja	Ja
	cpu.softirq_ percentage	leer	Prozentsatz der Zeit, in der alle CPUs, die Software-Unterbrechungen durchführen, unterbrochen werden	Prozent	Ja	Ja
	cpu.steal_ percentage	leer	Prozentsatz der Zeit, in der alle CPUs die Betriebssysteme virtueller Hosts bedienen	Prozent	Ja	Ja
	cpu.guest_ percentage	leer	Prozentsatz der Zeit, in der alle CPUs das Gastbetriebssystem bedienen	Prozent	Ja	Ja
os.linux.metric-system-disk	Datenträger.<disk-name> .lesen	Datenträgername	Gesamtanzahl der erfolgreich abgeschlossenen Lesevorgänge.	Anzahl	Ja	Ja
	disk.<disk-name>.readsMerged	Datenträgername	Gesamtanzahl der zusammengeführten Lesevorgänge	Anzahl		
	disk.<disk-name>.sectorsRead	Datenträgername	Gesamtanzahl der erfolgreich gelesenen Sektoren.	Anzahl		
	disk.<disk-name>.readTime	Datenträgername	Gesamtanzahl an Millisekunden, die für	Millisek		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			alle Lesevorgänge aufgewendet wurden.			
	Datenträger.<disk-name> .schreibt	Datenträgername	Gesamtanzahl der erfolgreich abgeschlossenen Schreibvorgänge.	count	Ja	Ja
	disk.<disk-name>.writesMerged	Datenträgername	Gesamtzahl der zusammengeführten Schreibvorgänge	count		
	disk.<disk-name>.sectorsWritten	Datenträgername	Gesamtanzahl der erfolgreich geschriebenen Sektoren.	count		
	disk.<disk-name>.writeTime	Datenträgername	Gesamtanzahl an Millisekunden, die für alle Schreibvorgänge aufgewendet wurden.	millisec		
	disk.<disk-name>.ioInProgress	Datenträgername	Gesamtzahl der derzeit ausgeführten E/A-Vorgänge	count		
	Datenträger.<disk-name> .ioTime		Für E/A-Vorgänge aufgewendete Gesamtzeit	Millisek	Ja	Ja
	disk.<disk-name>.ioTimeWeighted	Datenträgername	Für E/A-Vorgänge aufgewendete Gesamtzeit. Dies kann ein einfaches Maß für die E/A-Abschlusszeit und den Backlog	Millisek		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			sein, der sich ansammeln kann.			
os.linux.metrics.system-disk-capacity	disk.<file-system-name>.total	Dateisystemname	Gesamtgröße des Dateisystems.	Byte		
	disk.<file-system-name>.used	Dateisystemname	Gesamtmenge des Speicherplatzes, der vorhandenen Dateien im Dateisystem zugewiesen ist.	Byte		
	disk.<file-system-name>.avail	Dateisystemname	Gesamtmenge des im Dateisystem verfügbaren Speicherplatzes.	Byte		
	disk.<file-system-name>.used_percentage	Dateisystemname	Der Prozentsatz des verfügbaren Speicherplatzes, der derzeit allen Dateien im Dateisystem zugewiesen ist.	Prozent		
	disk.<file-system-name>.itotal	Dateisystemname	Die Gesamtzahl der Inodes im Dateisystem.	count		
	disk.<file-system-name>.iused	Dateisystemname	Die Anzahl der verwendeten In-Knoten.	count		
	disk.<file-system-name>.iavail	Dateisystemname	Die Anzahl der freien	count		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			(nicht verwendeten) Inodes.			
	disk.<file-system-name>.iused_percentage	Dateisystemname	Der Prozentsatz der verwendeten Inodes.	Prozent		
os.linux.metrics-system-disk-usage	disk_usage.<disk>.total	Datenträgername	Gesamtmenge an verfügbarem Speicherplatz auf diesem Datenträger	Bytes		
	disk_usage.<disk>.used	Datenträgername	Gesamter Speicherplatz, der auf diesem Datenträger verwendet wird	Bytes		
	disk_usage.<disk>.avail	Datenträgername	Gesamtmenge an verfügbarem Speicherplatz auf diesem Datenträger	Bytes		
	disk_usage<disk> .verwendeter Prozentsatz	Datenträgername	Der Prozentsatz des Speicherplatzes, der auf diesem Datenträger verwendet wird	Prozent	Ja	Ja
os.linux.metrics-system-speicher os. linux.metrics-system-speicher-prozent	memory.total	leer	Insgesamt nutzbarer RAM.	KB		
	memory.free	leer	Insgesamt freier RAM.	KB		
	memory.available	leer	Eine Schätzung, wie viel	KB		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			Arbeitsspeicher zum Starten neuer Anwendungen ohne Austausch verfügbar ist.			
	memory.buffers	leer	Temporärer Speicher, der für Rohdatenträger-Blöcke verwendet wird.	KB		
	memory.cached	leer	In-Memory Cache für vom Datenträger gelesene Dateien (Seiten-Cache). Enthält nicht „mem_swapcached“.	KB		
	„memory.swapTotal“	leer	Insgesamt verfügbarer Auslagerungsbereich (Swap Space).	KB	Ja	Ja
	„memory.swapFree“	leer	Derzeit nicht genutzter Auslagerungsbereich.		Ja	Ja
	memory.dirty	leer	Arbeitsspeicher, der darauf wartet, auf den Datenträger zurückgeschrieben zu werden.	KB		
	„memory.swapUsed“	leer	Menge des	KB	Ja	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			verwendeten Auslagerungsbereichs.			
	memory.used	leer	Menge des verwendeten RAM.	KB		
	Arbeitsspeicher. verwendeteWOPufferCaches	leer	Menge des verwendeten Arbeitsspeichers.	KB		
	Arbeitsspeicher. FreeWOPufferCaches	leer	Wert von MemAvailable von / proc/ meminfo, falls vorhanden, greift aber auf das Hinzufügen von freiem + gepuffertem + zwischengespeichertem Arbeitsspeicher zurück, falls nicht.	KB		
	Speicher. swapUsedPercentage	leer	Prozentsatz des verwendeten Auslagerungsbereichs.	Prozent		
	„memory_percent. kostenlos“.	leer	Prozentsatz des freien RAM	Prozent	Ja	Ja
	„memory_percent“ verfügbar	leer	Prozentsatz von verfügbarem Mem	Prozent	Ja	Ja
	„memory_percent. buffers“	leer	Prozent des Arbeitsspeichers, der für Rohdatenträgerblöcke verwendet wird	Prozent	Ja	Ja

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	„memory_percent“ zwischengespeichert	leer	Prozentsatz des Arbeitsspeichers, der für den In-Memory-Cache für vom Datenträger gelesene Dateien verwendet wird	Prozent	Ja	Ja
	„memory_percent“. dirty	leer	Prozentsatz des Arbeitsspeichers, der darauf wartet, auf den Datenträger zurückgeschrieben zu werden.	Prozent	Ja	Ja
	„memory_percent“. swapUsed	leer	Prozentsatz des verwendeten Auslagerungsbereichs.	Prozent	Ja	Ja
	„memory_percent. usedWOBuffersCaches“.	leer	Prozentsatz des Arbeitsspeichers wird verwendet	Prozent	Ja	Ja
	„memory_percent. „freieWoPufferCaches“	leer	Prozentsatz des verfügbaren Arbeitsspeichers	Prozent	Ja	Ja
os.linux.metrics-system-uptime	system.uptime(sec)	leer	Zeit, während der das System funktioniert und verfügbar ist.	Sek		
os.linux.metrics-memory-vmstat	vmstat.nr_free_pages	leer	Seiten, die derzeit	Seiten		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			vom System nicht verwendet werden.			
	vmstat.nr_alloc_batch	leer	Seiten, die anderen Domänen aufgrund von unzureichendem Arbeitsspeicher in jeder Domäne jeder NUMA zugewiesen sind	Seiten		
	vmstat.nr_inactive_anon	leer	Speicherseiten in jeder Domäne jedes NUMA-Knotens, auf die längere Zeit nicht zugegriffen wurde	Seiten		
	vmstat.nr_active_anon	leer	Seiten des anonymen virtuellen Speichers, die kürzlich verwendet wurden	KB		
	Datei vmstat.nr_inactive_	leer	Die Speicherseite, die der Datei entspricht, auf die in jeder Domäne jeder NUMA längere	KB		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			Zeit nicht zugegriffen wurde.			
	Datei vmstat.nr_active_	leer	Die Speicherseite, die der Datei entspricht, auf die kürzlich zugegriffen wurde.	Seiten		
	vmstat.nr_ unevictable	leer	Die Anzahl der Seiten ist in der Liste der nicht ausführbaren (Nicht-)LRUs aufgeführt	count		
	vmstat.nr_mlock	leer	Seiten, die einer VM_LOCKED-VMA zugeordnet sind, sind eine Klasse von Seiten, die nicht entfernt werden können.	Seiten		
	vmstat.nr_anon_ pages	leer	Im Arbeitsspeicher zugeordnete Seiten, die nicht Teil einer Datei sind.	Seiten		
	vmstat.nr_zugeordnet	leer	Anzahl der zugeordneten Speicherseiten.	count		
	vmstat.nr_file_pages	leer				

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	vmstat.nr_dirty	leer	Seiten warten darauf, auf den Datenträger geschrieben zu werden	Seiten		
	vmstat.nr_writeback	leer	Seiten, die derzeit auf den Datenträger geschrieben werden	Seiten		
	vmstat.nr_slab_reclaimable	leer	Seiten aus der Nutzung des Kernel-Slab-Arbeitsspeichers, die zurückgefordert werden können	Seiten		
	vmstat.nr_slab_unreklamierbar	leer	Seiten aus der Nutzung des Kernel-Slab-Arbeitsspeichers, die nicht zurückgefordert werden können	Seiten		
	vmstat.nr_page_table_pages	leer	Seiten, die Seitentabellen zugeordnet sind	Seiten		
	vmstat.nr_kernel_stapel	leer	Arbeitsspeicher, die Kernel-Stapeln zugeteilt ist.	KB	ermenge,	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	vmstat.nr_unstable	leer	Die Anzahl der instabilen Seiten in jeder Domäne jedes NUMA-Knotens	count		
	vmstat.nr_bounce	leer				
	vmstat.nr_vmscan_write	leer	Die Anzahl der geänderten Seiten, die während eines Scans von LRU(s) zurückgeschrieben wurden	count		
	vmstat.nr_vmscan_immediate_reclaim	leer				
	vmstat.nr_writeback_temp	leer				
	vmstat.nr_isolated_anon	leer	Die Anzahl der anonymen Speicherseiten, die in jeder Domäne jedes NUMA-Knotens isoliert sind	count		
	vmstat.nr_isolierte_Datei	leer	Die Anzahl der Seiten von Dateispeicherseiten, die in jeder Domäne	count		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			jedes NUMA-Knotens isoliert sind			
	vmstat.nr_shmem	leer	Die Anzahl der Seiten des gemeinsam genutzten Speichers	count		
	vmstat.nr_dirtied	leer	Die Anzahl der geänderten Seiten in jeder Domäne jedes NUMA-Knotens	count		
	vmstat.nr_written	leer				
	vmstat.numa_hit	leer	Anzahl der Seiten, die diesem Knoten erfolgreich zugeordnet wurden.	count		
	vmstat.numa_miss	leer	Die Anzahl der Seiten, die auf diesem Knoten aufgrund von unzureichendem Arbeitsspeicher auf dem gewünschten Knoten zugeteilt wurden.	count		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	vmstat.numa_foreign	leer	Die Anzahl der Seiten, die ursprünglich für diesen Knoten vorgesehen waren und stattdessen einem anderen Knoten zugewiesen wurden	count		
	vmstat.numa_ interleave	leer	Anzahl der Seiten, die gemäß Interleave-Richtlinie erfolgreich diesem Knoten zugeordnet wurden.	count		
	vmstat.numa_local	leer	Die Anzahl der Seiten, die auf diesem Knoten durch einen Prozess auf diesem Knoten erfolgreich zugeordnet wurden	count		
	vmstat.numa_other	leer	Die Anzahl der Seiten, die auf			

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			diesem Knoten von einem Prozess auf einem anderen Knoten zugeordnet wurden.			
	vmstat.workset_refault	leer				
	vmstat.workset_activate	leer				
	vmstat.workset_nodereclaim	leer				
	vmstat.nr_anon_transparent_hugepages	leer				
	vmstat.nr_free_cma	leer	Freie kontinuierliche Speicherzuteilungsseiten in jeder Domäne jeder NUMA			
	vmstat.nr_dirty_schwellenwert	leer				
	vmstat.nr_dirty_background_threshold	leer				
	vmstat.pgpgin	leer	Die Anzahl der vom Datenträger importierten Seiten	count		
	vmstat.pgpgout	leer	Die Anzahl der auf den Datenträger geschriebenen Seiten	count		
	vmstat.pswpin	leer	Die Anzahl der Seiten,	count		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			die aus Swap Space importiert werden			
	vmstat.pswpout	leer	Die Anzahl der Seiten, die im Swap Space ausgelagert wurden	count		
	vmstat.pgalloc_dma	leer				
	vmstat.pvalloc_ dma32	leer				
	vmstat.pvalloc_ normal	leer				
	vmstat.pvalloc_ movable	leer				
	vmstat.pgfree	leer	Die Anzahl der Seiten, die seit dem letzten Start frei sind	count		
	vmstat.pgactivat	leer	Anzahl der Seitenaktivierungen seit dem letzten Start	count		
	vmstat.pgdeactivate	leer	Anzahl der Seitendeaktivierungen seit dem letzten Start	count		
	vmstat.pgfault	leer	Geringfügige Fehler seit dem letzten Start	Seiten		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	vmstat.pgmajfault	leer	Schwerwiegende Fehler seit dem letzten Start	Seiten		
	vmstat.pglazyfreed	leer				
	vmstat.pgrefill_dma	leer				
	vmstat.pgrefill_dma32	leer				
	vmstat.pgrefill_normal	leer	Anzahl der Seitenfüllungen seit dem letzten Start	count		
	vmstat.pgrefill_ movable	leer				
	vmstat.pgsteal_ kswapd_dma	leer				
	vmstat.pgsteal_ kswapd_dma32	leer				
	vmstat.pgsteal_ kswapd_normal	leer				
	vmstat.pgsteal_ kswapd_movable	leer				
	vmstat.pgsteal_ direct_dma	leer				
	vmstat.pgsteal_ direct_dma32	leer				
	vmstat.pgsteal_ direct_normal	leer				
	vmstat.pgsteal_ direct_movable	leer				
	vmstat.pgscan_ kswapd_dma	leer				
	vmstat.pgscan_ kswapd_dma32	leer				
	vmstat.pgscan_ kswapd_normal	leer	Anzahl der Seiten, die seit dem Start von kswapd	count		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			gescannt wurden			
	vmstat.pgscan_ kswapd_movable	leer				
	vmstat.pgscan_ direct_dma	leer				
	vmstat.pgscan_ direct_dma32	leer				
	vmstat.pgscan_ direct_normal	leer	Anzahl der seit dem Start zurückgeforderten Seiten	count		
	vmstat.pgscan_ direct_movable	leer				
	vmstat.pgscan_ direct_throttle	leer				
	vmstat.zone_ reclaim_failed	leer				
	vmstat.pginodesteal	leer				
	vmstat.slabs_scanned	leer				
	vmstat.kswapd_ inodesteal	leer				
	vmstat.kswapd_low_ wmark_hi_quickly	leer				
	vmstat.kswapd_high_ wmark_hi_quickly	leer				
	vmstat.pageoutrun	leer	Anzahl der Aufrufe der Seitenrückforderung durch kswapd	count		
	vmstat.allocstall	leer	Anzahl der direkten Aufrufe der Seitenrückforderung (wenig Arbeitsspeicher)	count		
	vmstat.pgrotated	leer				

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
	vmstat.drop_ pagecache	leer				
	vmstat.drop_slab	leer				
	vmstat.numa_pte_ updates	leer				
	vmstat.numa_huge_ pte_updates	leer				
	vmstat.numa_hint_ Fehler	leer				
	vmstat.numa_hint_ faults_local	leer				
	vmstat.numa_pages_ migriert	leer				
	vmstat.pgmigrate_ success	leer				
	vmstat.pgmigrate_fail	leer				
	vmstat.compact_ migrate_scanned	leer				
	vmstat.compact_ „Free_scanned“	leer				
	vmstat.compact_ isoliert	leer				
	vmstat.compact_stall	leer	Die Häufigkeit, mit der ein Prozess anhält, um eine Speicherkomprimierung auszuführen, sodass eine große Seite zur Verwendung frei wird.	count		
	vmstat.compact_fail	leer	Die Anzahl der Versuche des Systems, Arbeitsspeicher	count		

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			zu komprimieren, bei denen dies fehlgeschlagen ist.			
	vmstat.compact_Erfolg	leer	Häufigkeit, mit der vom System Arbeitsspeicher komprimiert und eine große Seite zur Verwendung freigegeben wurde.	count		
	vmstat.htlb_buddy_alloc_success	leer				
	vmstat.htlb_buddy_alloc_fail	leer				
	vmstat.unevictable_pgs_culted	leer				
	vmstat.unevictable_pgs_scanned	leer				
	vmstat.unevictable_pgs_rescued	leer				
	vmstat.unevictable_pgs_mlocked	leer				
	vmstat.unevictable_pgs_munlocked	leer				
	vmstat.unevictable_pgs_cleared	leer				
	vmstat.unevictable_pgs_Stranded	leer				
	vmstat.thp_fault_alloc	leer	Die Anzahl der großen Seiten wurde erfolgreich zugewiesen, um einen	count		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			Seitenfehler zu behandeln.			
	vmstat.thp_fault_fallback	leer	Durch die fehlerhafte Anzahl von Seiten kann keine große Seite zugeteilt werden, und stattdessen wird auf die Verwendung kleiner Seiten zurückgegriffen.	count		
	vmstat.thp_collapse_alloc	leer	Die Anzahl der Reduzierungen eines Seitenbereichs auf eine große Seite und die anschließende erfolgreiche Zuordnung einer neuen großen Seite zum Speichern der Daten.	count		
	vmstat.thp_collapse_alloc_failed	leer	Die Anzahl der reduzierten Elemente eines Seitenbereichs auf eine	count		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			große Seite, bei denen die Zuordnung jedoch fehlgeschlagen ist.			
	vmstat.thp_split	leer	Die Anzahl der Aufteilungen einer großen Seite in Basisseiten	count		
	vmstat.thp_zero_page_alloc	leer	Die Anzahl der erfolgreichen Zuteilungen der großen Nullseite	count		
	vmstat.thp_zero_page_alloc_failed	leer	Gibt an, wie oft der Kernel eine große Nullseite nicht zuordnen konnte und auf die Verwendung kleiner Seiten zurückgreift.	count		
	vmstat.balloon_inflate	leer				
	vmstat.Ballons_deflationieren	leer				
	vmstat.Ballons_migrate	leer				
os.linux.metrics-process-status	proc.<process>.VmSize	Prozessname	Die Gesamtmenge des vom Prozess	KB		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Überprüfen	Metrikname	Ressource	Beschreibun	Einheiten	Empfohlene Metrik	Anomalie-Erkennung
			verwendeten virtuellen Arbeitsspeichers			
	proc.<process>.VmRSS	Prozessname	Der physische Speicher (nicht Swap), den ein Prozess verwendet hat	KB		
	proc.<process>.VmSwap	Prozessname	Gesamtmenge des verwendeten Auslagerungsbereichs.	KB		

Prüfungen zur Linux-Netzwerküberwachung

Hinweis: Beim Upgrade von einer früheren Version fügen Sie die Prüfungen in dieser Tabelle manuell der Linux-Metrikenrichtlinie hinzu.

Linux-Metrikrichtlinie

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbe	Gesammelte Metriken	Empfohlene Metrik
Metrik	os.linux.metrics-network-interface	Ruft alle auf die Netzwerkschnittstelle bezogenen Metriken für Linux-Server ab.	Verwendung: -x,excludeinterface: Liste der auszuschließenden Schnittstellen (kommagetrennt) -i, Einbindungsschnittstelle: Liste der einzubeziehenden Schnittstellen (kommagetrennt) -I, insertinterfaceregex: Regulärer Ausdruck, der den einzubeziehende	• rxBytes (empfohlene Metrik) • rxPackets (empfohlene Metrik) • rxFehler • rxDrops (empfohlene Metrik) • rxFifo • rxFrame • rxkomprimiert • rxMulticast • rxBytes (empfohlene Metrik)	Ja

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbe	Gesammelte Metriken	Empfohlene Metrik
			Schnittstellen entspricht • -X,excludeinterfaceregex: Regulärer Ausdruck, der mit den auszuschließenden Schnittstellen übereinstimmt Anwendungsbeispiel: `Befehl: metrics-network-interface.rb`	• rxPackets (empfohlene Metrik) • rxFehler • rxDrops (empfohlene Metrik) • rxFifo • rxColls • rxCarrier • rxkomprimiert	
Metrik	os.linux.metrics-netstat-tcp	Ruft Metriken zu TCP-Socket-Status von netstat ab. Nützlich bei Web- oder Proxy-Servern mit hohem Datenverkehr und einer großen Anzahl eingehender und ausgehender kurzzeitiger TCP-Verbindungen.	Verwendung: • -p, port: Der Port, von dem Sie Metriken empfangen möchten. Wertebereich = 1–65535. • -t, Typ: Der Porttyp, von dem Metriken empfangen werden sollen. Werte=lokal oder remote. Standard = lokal • -d, disabletcp6: Deaktiviert die TCP6-Prüfung. Geben Sie einen Wert ein, um	• tcp.UNBEKANNT • tcp.HERGESTELLT • tcp.SYN_SENT • tcp.SYN_RECV • tcp.FIN_WAIT1 • tcp.FIN_WAIT2 • tcp.TIME_WAIT • tcp.SCHLIESSEN • tcp.CLOSE_WAIT • tcp.LAST_ack • tcp.HÖREN • tcp.SCHLIESSEN	nein

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Linux-Metrikrichtlinie (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbe	Gesammelte Metriken	Empfohlene Metrik
			disabletcp6 auf „wahr“ festzulegen. Anwendungsbeispiel: `metrics-netstat-tcp.rb`		

Linux-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Linux-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

os.linux.metrics-process-usage – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
proc.acc.running			Anzahl der Prozesse, die mit diesem Namen ausgeführt werden (acc).
proc.acc.cpuPercent			Prozentsatz der vom Prozess beanspruchten CPU.
proc.acc.memPercent			Prozentsatz des vom Prozess belegten Arbeitsspeichers.

os.linux.metrics-reboot-count-today – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
reboot.count.today			Anzahl der Neustarts heute.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.total.user			Prozesse mit normaler Priorität, die im Benutzermodus ausgeführt werden; *cpu.total.user* ist die Summe der *cpuN.user*-Metriken.
cpu.total.nice			Bearbeitete Prozesse, die im Anwendermodus ausgeführt werden; *cpu.total.nice* ist die Summe der *cpuN.nice* -Metriken.
cpu.total.system			Zeit, die die CPU für die Ausführung des Kernels aufgewendet hat; *cpu.total.system* ist die Summe der *cpuN.system*-Metriken.
cpu.total.idle			Gesamtzeit, die die CPU im Leerlauf verbracht hat; *cpu.total.idle* ist die Summe der *cpuN.idle*-Metriken.
cpu.total.iowait			Gesamtzeit, die die CPU auf den Abschluss von E/A-Vorgängen gewartet hat; *cpu.total.iowait* ist die Summe der *cpuN.iowait*-Metriken.
cpu.total.irq			Gesamtzeit, die der Prozessor für Interrupts aufwendet; *cpu.total.irq* ist die Summe der *cpuN.irq*-Metriken.
cpu.total.softirq			Zeitaufwand für die Verarbeitung von Soft Interrupt-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Anforderungen; *cpu.total.softirq* ist die Summe der *cpuN.softirq* Metriken.
cpu.total.steal			Gesamtzeit, die die virtuelle CPU darauf gewartet hat, dass der Hypervisor eine Verarbeitung für eine andere virtuelle CPU durchführt. Gilt nur für virtuelle Computer.
cpu.total.guest			Gesamtzeit, die von der CPU für die Ausführung des virtuellen Prozessors aufgewendet wurde. Gilt nur für Hypervisoren.
cpu.total.guest_nice			Gesamtzeit, die von der CPU für die Ausführung als Gastbetriebssystem mit nice-Priorität aufgewendet wurde; *cpu.total.guset_nice* ist die Summe der *cpuN.guest_nice* Metriken
cpu.<cpu-core>.user			Zeit, die für die Verarbeitung mit normaler Priorität im Benutzermodus aufgewendet wurde.
cpu.<cpu-core>.nice			Zeit, die für die mit nice-Prozesspriorität erfolgende Verarbeitung im Benutzermodus aufgewendet wurde.
cpu.<cpu-core>.system			Zeitaufwand für die Ausführung im Kernel-Modus.
cpu.<cpu-core>.idle			Im Leerlauf verbrachte Zeit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.<cpu-core>.iowait			Wartezeit auf Abschluss von E/A-Vorgängen. Wird auch als Leerlaufzeit betrachtet.
cpu.<cpu-core>.irq			Zeit, die für die Verarbeitung von Hardware-Interrupts aufgewendet wurde.
cpu.<cpu-core>.softirq			Zeit, die für die Verarbeitung von Software-Interrupts aufgewendet wurde.
cpu.<cpu-core>.steal			Zeit, die von anderen Betriebssystemen vereinnahmt wurde, die in einer virtuellen Umgebung ausgeführt wurden.
cpu.<cpu-core>.guest			Zeit, die für die Ausführung einer virtuellen CPU oder eines Gastbetriebssystems unter der Steuerung des Kernels aufgewendet wurde.
cpu.<cpu-core>.guest_nice			Gesamtzeit, die von der CPU für die Ausführung als Gastbetriebssystem mit nice-Priorität aufgewendet wurde.
cpu.intr			Seit Startzeit verarbeitete Interrupts.
cpu.ctxt			Gesamtanzahl der Kontextwechsel über alle CPUs hinweg.
cpu.btime			Startzeit.
cpu.processes			Anzahl der erstellten Prozesse und Threads, einschließlich jener (aber nicht

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			beschränkt auf jene), die durch Aufrufe der Systemaufrufe fork() und clone() erstellt wurden.
cpu.procs_running			Gesamtanzahl der Prozesse, die auf allen CPUs ausgeführt werden.
cpu.procs_blocked			Anzahl der derzeit blockierten Prozesse, die auf den Abschluss von E/A-Vorgängen warten.
cpu.cpu_count			Die Anzahl der CPUs im System.
cpu.<cpu-core>.cores			Anzahl der CPU-Kerne.

os.linux.metrics-system-cpu-load – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
load_avg.one (empfohlene Metrik)			Durchschnittliche Systemauslastung über eine Minute.
load_avg.five (empfohlene Metrik)			Durchschnittliche Systemauslastung über fünf Minuten.
load_avg.fifteen (empfohlene Metrik)			Durchschnittliche Systemauslastung über 15 Minuten.
load_avg.norm.one			Durchschnittliche Systemauslastung über eine Minute, normalisiert durch die Anzahl der CPUs.
load_avg.norm.five			Durchschnittliche Systemauslastung über fünf Minuten, normalisiert durch die Anzahl der CPUs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu-load – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
load_avg.norm.fifteen			Durchschnittliche Systemauslastung über 15 Minuten, normalisiert durch die Anzahl der CPUs.

os.linux.metrics-system-cpu-percentage – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.avgutilization_percentage			Durchschnittlicher Prozentsatz der verwendeten CPU.
cpu.user_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der die gesamte CPU von Prozessen mit normaler Priorität im Benutzermodus verwendet wurde.
cpu.nice_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der alle CPUs von Prozessen mit nice-Priorität im Benutzermodus verwendet wurden.
cpu.system_percentage (empfohlene Metrik)			Prozentsatz der Zeit, die von der CPU für die Ausführung des Kernels aufgewendet wurde.
cpu.idle_percentage (empfohlene Metrik)			Prozentsatz der Zeit, in der sich alle CPUs im Leerlauf befanden.
cpu.iowait_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der von allen CPUs auf den Abschluss von E/A-Vorgängen gewartet wurde.
cpu.irq_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-cpu-percentage – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			allen CPUs Interrupts verarbeitet wurden.
cpu.softirq_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der von allen CPUs Software-Interrupts verarbeitet wurden.
cpu.steal_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der alle CPUs virtuelle Hostbetriebssysteme bedient haben.
cpu.guest_percentage (empfohlene Metrik)			Prozentsatz der Zeit, während der alle CPUs Gastbetriebssysteme bedient haben.

os.linux.metrics-system-disk – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
disk.<disk-name>.reads (empfohlene Metrik)			Gesamtanzahl der erfolgreich abgeschlossenen Lesevorgänge.
disk.<disk-name>.readsMerged			Gesamtanzahl der zusammengeführten Lesevorgänge.
disk.<disk-name>.sectorsRead			Gesamtanzahl der erfolgreich gelesenen Sektoren.
disk.<disk-name>.readTime		milliseconds	Gesamtanzahl an Millisekunden, die für alle Lesevorgänge aufgewendet wurden.
disk.<disk-name>.writes (empfohlene Metrik)			Gesamtanzahl der erfolgreich abgeschlossenen Schreibvorgänge.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-disk – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
disk.<disk-name>.writesMerged			Gesamtanzahl der zusammengeführten Schreibvorgänge.
disk.<disk-name>.sectorsWritten			Gesamtanzahl der erfolgreich geschriebenen Sektoren.
disk.<disk-name>.writeTime		milliseconds	Gesamtanzahl an Millisekunden, die für alle Schreibvorgänge aufgewendet wurden.
disk.<disk-name>.ioInProgress			Gesamtanzahl der derzeit ausgeführten E/A-Vorgänge.
disk.<disk-name>.ioTime (empfohlene Metrik)			Insgesamt für E/A-Vorgänge aufgewendete Zeit.
disk.<disk-name>.ioTimeWeighted			Insgesamt für E/A-Vorgänge aufgewendete Zeit. Dies kann ein Maß für die E/A-Abschlusszeit und den Rückstand sein, der sich möglicherweise ansammelt.

os.linux.metrics-system-disk-capacity – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
disk.<file-system-name>.total			Gesamtgröße des Dateisystems.
disk.<file-system-name>.used			Gesamtmenge des Speicherplatzes, der vorhandenen Dateien im Dateisystem zugewiesen ist.
disk.<file-system-name>.avail			Gesamtmenge des im Dateisystem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-disk-capacity – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			verfügbaren Speicherplatzes.
disk.<file-system-name>.used_percentage			Prozentsatz des verfügbaren Speicherplatzes, der derzeit allen Dateien im Dateisystem zugeordnet ist.
disk.<file-system-name>.itotal			Gesamtanzahl von *inodes* im Dateisystem.
disk.<file-system-name>.iused			Anzahl der verwendeten *inodes*.
disk.<file-system-name>.iavail			Anzahl der freien (nicht verwendeten) *inodes*.
disk.<file-system-name>.iused_percentage			Prozentsatz der verwendeten *inodes*.

os.linux.metrics-system-disk-usage – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
disk_usage.<disk>.total			Insgesamt verfügbarer Speicherplatz auf dem Datenträger.
disk_usage.<disk>.used			Gesamtmenge des auf dem Datenträger verwendeten Speicherplatzes.
disk_usage.<disk>.avail			Insgesamt verfügbarer Speicherplatz auf dem Datenträger.
disk_usage.<disk>.used_percentage (empfohlene Metrik)			Prozentsatz des verwendeten Speicherplatzes auf dem Datenträger.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-memory – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
memory.total			Insgesamt nutzbarer RAM.
memory.free			Insgesamt freier RAM.
memory.available			Eine Schätzung, wie viel Arbeitsspeicher zum Starten neuer Anwendungen verfügbar ist, ohne dass eine Auslagerung (Swapping) durchgeführt wird.
memory.buffers			Temporärer Speicher, der für Rohdatenträger-Blöcke verwendet wird.
memory.cached			In-Memory Cache für vom Datenträger gelesene Dateien (Seiten-Cache). *mem_swapcached* ist nicht enthalten.
memory.swapTotal (empfohlene Metrik)			Insgesamt verfügbarer Auslagerungsbereich (Swap Space).
memory.swapFree (empfohlene Metrik)			Derzeit nicht genutzter Auslagerungsbereich.
memory.dirty			Arbeitsspeicher, der darauf wartet, auf den Datenträger zurückgeschrieben zu werden.
memory.swapUsed (empfohlene Metrik)			Menge des verwendeten Auslagerungsbereichs.
memory.used			Menge des verwendeten RAM.
memory.usedWOBuffersCaches			Menge des verwendeten Arbeitsspeichers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-memory – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
memory.freeWOBuffersCaches			Wert *MemAvailable* von */proc/meminfo* , falls vorhanden; falls nicht vorhanden erfolgt Rückgriff auf freien + gepufferten + zwischengespeicherten Speicher.
memory.swapUsedPercentage			Prozentsatz des verwendeten Auslagerungsbereichs.

os.linux.metrics-system-memory-percent – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
memory_percent.free (empfohlene Metrik)			Prozentsatz des freien RAM.
memory_percent.available (empfohlene Metrik)			Prozentsatz des verfügbaren Arbeitsspeichers
memory_percent.buffers (empfohlene Metrik)			Prozentsatz des Arbeitsspeichers, der für Rohdatenträger-Blöcke verwendet wird.
memory_percent.cached (empfohlene Metrik)			Prozentsatz des Arbeitsspeichers, der mit In-Memory Cache für vom Datenträger gelesene Dateien verwendet wird.
memory_percent.dirty (empfohlene Metrik)			Prozentsatz des Arbeitsspeichers, der darauf wartet, auf den Datenträger zurückgeschrieben zu werden.
memory_percent.swapUsed (empfohlene Metrik)			Prozentsatz des verwendeten Auslagerungsbereichs.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-system-memory-percent – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
memory_percent.used (empfohlene Metrik)	WOBuffersCaches		Prozentsatz des verwendeten Arbeitsspeichers.
memory_percent.free (empfohlene Metrik)	WOBuffersCaches		Prozentsatz des verfügbaren Arbeitsspeichers.

os.linux.metrics-system-uptime – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
system.uptime(sec)			Zeit, während der das System funktioniert und verfügbar ist.

os.linux.metrics-memory-vmstat – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.nr_free_pages			Seiten, die derzeit vom System nicht verwendet werden.
vmstat.nr_alloc_batch			Seiten, die anderen Domänen aufgrund von unzureichendem Arbeitsspeicher in jeder Domäne jedes NUMA-Knotens (Non-Uniform Memory Access) zugewiesen sind.
vmstat.nr_inactive_anon			Speicherseiten in jeder Domäne jedes NUMA-Knotens, auf die nicht zugegriffen wurde.
vmstat.nr_active_anon			Seiten des anonymen virtuellen Arbeitsspeichers, die kürzlich verwendet wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.nr_inactive_file			Speicherseite, die der Datei entspricht, auf die in jeder Domäne jedes NUMA-Knotens nicht zugegriffen wurde.
vmstat.nr_active_file			Speicherseite, die der Datei entspricht, auf die kürzlich zugegriffen wurde.
vmstat.nr_unevictable			Anzahl der Seiten in der (Nicht-)LRU-Liste (Least Recently Used) des Arbeitsspeichers, der nicht freigegeben werden kann (unevictable Memory).
vmstat.nr_mlock			Seiten, die einem virtuellen Speicherbereich (Virtual Memory Area, VMA) mit dem VMA-Flag VM_Locked zugeordnet sind und eine Klasse von Seiten im nicht freigebbaren Arbeitsspeicher darstellen.
vmstat.nr_anon_pages			Speicherzuordnungsseiten, die nicht Teil einer Datei sind.
vmstat.nr_mapped			Anzahl der zugeordneten Speicherseiten.
vmstat.nr_file_pages			
vmstat.nr_dirtied			Seiten, die darauf warten, auf den Datenträger geschrieben zu werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.nr_writeback			Seiten, die derzeit auf den Datenträger geschrieben werden.
vmstat.nr_slab_reclaimable			Seiten aus der Kernel-Slab-Speichernutzung, die zurückgewonnen werden können.
vmstat.nr_slab_unreclaimable			Seiten aus der Kernel-Slab-Speichernutzung, die nicht zurückgewonnen werden können.
vmstat.nr_page_table_pages			Seiten, die Seitentabellen zugeordnet sind.
vmstat.nr_kernel_stack			Arbeitsspeichermenge, die Kernel-Stapeln zugeteilt ist.
vmstat.nr_unstable			Anzahl der instabilen Seiten in jeder Domäne jedes NUMA-Knotens.
vmstat.nr_bounce			
vmstat.nr_vmscan_write			Anzahl der modifizierten Seiten, die während eines LRU-Scans zurück auf den Datenträger geschrieben wurden.
vmstat.nr_vmscan_immediate_reclaim			
vmstat.nr_writeback_temp			
vmstat.nr_isolated_anon			Anzahl der anonymen Speicherseiten, die in jeder Domäne jedes NUMA-Knotens isoliert sind.
vmstat.nr_isolated_file			Anzahl der Dateispeicherseiten, die in jeder Domäne

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			jedes NUMA-Knotens isoliert sind.
vmstat.nr_shmem			Anzahl der gemeinsam genutzten Speicherseiten.
vmstat.nr_dirtied			Anzahl der modifizierten Seiten in jeder Domäne jedes NUMA Knotens.
vmstat.nr_written			
vmstat.numa_hit			Anzahl der Seiten, die diesem Knoten erfolgreich zugeordnet wurden.
vmstat.numa_miss			Anzahl der Seiten, die diesem Knoten aufgrund von wenig Arbeitsspeicher im vorgesehenen Knoten zugeordnet wurden.
vmstat.numa_foreign			Anzahl der ursprünglich für diesen Knoten bestimmten Seiten, die einem anderen Knoten zugeordnet wurden.
vmstat.numa_interleave			Anzahl der Seiten, die gemäß Interleave-Richtlinie erfolgreich diesem Knoten zugeordnet wurden.
vmstat.numa_local			Anzahl der Seiten, die in diesem Knoten durch einen Prozess in diesem Knoten erfolgreich zugeordnet wurden.
vmstat.numa_other			Anzahl der Seiten, die in diesem Knoten durch einen Prozess in einem anderen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Knoten zugeordnet wurden.
vmstat.workingset_refault			
vmstat.workingset_activate			
vmstat.workingset_nodereclaim			
vmstat.nr_anon_transparent_hugepages			
vmstat.nr_free_cma			Freie kontinuierliche Speicherzuordnungsseiten in jeder Domäne jedes NUMA-Knotens.
vmstat.nr_dirty_threshold			
vmstat.nr_dirty_background_threshold			
vmstat.pgpgin			Anzahl der vom Datenträger importierten Seiten.
vmstat.pgpgout			Anzahl der auf den Datenträger geschriebenen Seiten.
vmstat.pswpin			Anzahl der aus dem Auslagerungsbereich importierten Seiten.
vmstat.pswpout			Anzahl der in den Auslagerungsbereich ausgelagerten Seiten.
vmstat.pgalloc_dma			
vmstat.pgalloc_dma32			
vmstat.pgalloc_normal			
vmstat.pgalloc_movable			
vmstat.pgfree			Anzahl der seit dem letzten Start verfügbaren Seiten.
vmstat.pgactivate			Anzahl der Seitenaktivierungen seit dem letzten Start.
vmstat.pgdeactivate			Anzahl der Seitendeaktivierungen seit dem letzten Start.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.pgfault			Geringfügige Fehler seit dem letzten Start.
vmstat.pgmajfault			Schwerwiegende Fehler seit dem letzten Start.
vmstat.pglazyfreed			
vmstat.pgrefill_dma			
vmstat.pgrefill_dma32			
vmstat.pgrefill_normal			Anzahl der Seitenauffüllungen seit dem letzten Start.
vmstat.pgrefill_movable			
vmstat.pgsteal_kswapd_dma			
vmstat.pgsteal_kswapd_dma32			
vmstat.pgsteal_kswapd_normal			
vmstat.pgsteal_kswapd_movable			
vmstat.pgsteal_direct_dma			
vmstat.pgsteal_direct_dma32			
vmstat.pgsteal_direct_normal			
vmstat.pgsteal_direct_movable			
vmstat.pgscan_kswapd_dma			
vmstat.pgscan_kswapd_dma32			
vmstat.pgscan_kswapd_normal			Anzahl der von *kswapd* seit dem Start gescannten Seiten.
vmstat.pgscan_kswapd_movable			
vmstat.pgscan_direct_dma			
vmstat.pgscan_direct_dma32			
vmstat.pgscan_direct_normal			Anzahl der seit dem Start zurückgewonnenen Seiten.
vmstat.pgscan_direct_movable			
vmstat.pgscan_direct_throttle			
vmstat.zone_reclaim_failed			

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.pginodesteal			
vmstat.slabs_scanned			
vmstat.kswapd_inodesteal			
vmstat.kswapd_low_wmark_hit_quickly			
vmstat.kswapd_high_wmark_hit_quickly			
vmstat.pageoutrun			Anzahl der durch *kswapd* erfolgenden Aufrufe der Seitenrückgewinnung.
vmstat.allocstall			Anzahl der direkten Aufrufe der Seitenrückgewinnung (wenig Arbeitsspeicher).
vmstat.pgrotated			
vmstat.drop_pagecache			
vmstat.drop_slab			
vmstat.numa_pte_updates			
vmstat.numa_huge_pte_updates			
vmstat.numa_hint_faults			
vmstat.numa_hint_faults_local			
vmstat.numa_pages_migrated			
vmstat.pgmigrate_success			
vmstat.pgmigrate_fail			
vmstat.compact_migrate_scanned			
vmstat.compact_free_scanned			
vmstat.compact_isolated			
vmstat.compact_stall			Häufigkeit, mit der ein Prozess bei der Arbeitsspeicherkomprimierung verzögert wird, sodass eine große Seite zur Verfügung steht.
vmstat.compact_fail			Häufigkeit, mit der vom System versucht wurde, den Arbeitsspeicher

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			zu komprimieren, und mit der der betreffende Versuch fehlgeschlagen ist.
vmstat.compact_success			Häufigkeit, mit der vom System Arbeitsspeicher komprimiert und eine große Seite zur Verwendung freigegeben wurde.
vmstat.htlb_buddy_alloc_success			
vmstat.htlb_buddy_alloc_fail			
vmstat.unevictable_pgs_culled			
vmstat.unevictable_pgs_scanned			
vmstat.unevictable_pgs_rescued			
vmstat.unevictable_pgs_mlocked			
vmstat.unevictable_pgs_munlocked			
vmstat.unevictable_pgs_cleared			
vmstat.unevictable_pgs_stranded			
vmstat.thp_fault_alloc			Anzahl der großen Seiten, die erfolgreich zur Behandlung eines Seitenfehlers zugeordnet wurden.
vmstat.thp_fault_fallback			Anzahl der Seitenfehler, bei denen die Zuordnung einer großen Seite vor Rückgriff auf die Verwendung kleiner Seiten fehlgeschlagen ist.
vmstat.thp_collapse_alloc			Anzahl der Seiten, die mit der erfolgreichen Zuordnung einer neuen großen Seite zum Speichern der Daten zu einer großen Seite zusammengefasst wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-memory-vmstat – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmstat.thp_collapse_alloc_failed			Anzahl der Seiten, die zu einer großen Seite zusammengefasst wurden, bei denen die Zuordnung jedoch fehlgeschlagen ist.
vmstat.thp_split			Anzahl der Basisseiten, in die eine große Seite aufgeteilt werden soll.
vmstat.thp_zero_page_alloc			Anzahl der erfolgreichen Zuordnungen von großen „Zero Pages“ (Nullseiten).
vmstat.thp_zero_page_alloc_failed			Häufigkeit, mit der vom Kernel eine große Nullseite nicht zugeordnet werden konnte und auf die Verwendung kleiner Seiten zurückgegriffen wurde.
vmstat.balloon_inflate			
vmstat.balloon_deflate			
vmstat.balloon_migrate			

os.linux.metrics-process-status – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
proc.<process>.VmSize			Gesamtmenge des vom Prozess verwendeten virtuellen Arbeitsspeichers.
proc.<process>.VmRSS			Der nicht ausgelagerte physische

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

os.linux.metrics-process-status – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Arbeitsspeicher, der von einem Prozess verwendet wird.
proc.<process>.VmSwap			Gesamtmenge des verwendeten Auslagerungsbereichs.

MongoDB – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Richtlinien für die MongoDB-Systemüberwachung. Die Richtlinien beinhalten die in der angegebenen Tabelle ausgewiesenen Prüfungen. Richtlinien und Prüfungen sind für Windows und Linux verfügbar.

MongoDB-Ereignisse

Typ	Prüfung	Beschreibung	Verwendung	Befehl	Ausgabe

Event	app.mongodb.check-mongodb-alive	Überwacht, ob der MongoDB-Server aktiv ist, und erstellt Warnungen für den MongoDB-Server-Integritätsstatus.	`commonchecks check-mongodb-alive -H db_host -p db_port`
			
			Wobei:
			• `db_host` = Host, auf dem der Server ausgeführt wird.
			• `db_port` = Port für die Verbindung mit dem MongoDB-Server.
			
			Verwendungsbeispiel:
			`command: commonchecks check-mongodb-alive -H 10.***.***.*** -p 27017`
				`commonchecks check-mongodb -p {{.labels.parameter_port}} -H {{.labels.parameter_host}}`	`Check mongodb Alive OK:` Gibt an, dass der Integritätsstatus des Servers in Ordnung ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MongoDB-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Befehl	Ausgabe

Event	app.mongodb.check-mongodb-metrics	Erstellt Warnungen für eine der MongoDB-Metriken basierend auf dem Schwellenwert.
		
		Um die Warnungen für eine MongoDB-Servermetrik auszulösen, übergeben Sie den gesamten Metriknamen im Parameter.
			`commonchecks check-mongodb-metrics -H Hostname -p port -w warning -c critical -d database -m MetricName`
			
			Wobei:
			• `Hostname` = Host, auf dem der Server ausgeführt wird.
			• `port` = Port zum Herstellen der Verbindung mit dem MongoDB-Server.
			• `warning` = Warnungsschwellenwert.
			• `critical` = Kritischer Schwellenwert.
			• `database` = Datenbankname.
			• `MetricName` = Spezifische zu überwachende Metrik.
			
			Verwendungsbeispiel:
			`command: commonchecks check-mongodb-alive -H 10.***.***.*** -p 27017`
				`commonchecks check-mongodb-metrics -c {{.labels.params_critical}} -d {{.labels.params_database}} -w {{.labels.params_warning}} -H {{.labels.params_host}} -p {{.labels.params_port}} -m {{.labels.params_metric}}`	`Check mongodb Metrics OK`: Gibt an, dass der Wert von `mongodb.connection.curre` innerhalb des akzeptablen Schwellenwerts liegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MongoDB-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Befehl	Ausgabe
Metrik	app.mongodb.metrics-mongodb	Gibt Metriken des MongoDB-Servers und aller Datenbanken zurück. Beispielmetriken: • `mongodb.connections.totalCreated`: Eingehende Verbindungen • `mongodb.locks.Database.acquireCount_IX`: Sperrmodus „Intent Exclusive“ • `mongodb.locks.Database.acquireCount_X`: Sperrmodus „Exklusive“ • `mongodb.locks.Database.acquireCount_IS`: Sperrmodus „Intent Shared“	`commonchecks check-mongodb` Wobei: • `host` = Name des Hosts, auf dem der MongoDB-Server ausgeführt wird. • `port` = Port zum Herstellen der Verbindung mit dem MongoDB-Server. • `database` = Datenbankname.	`commonchecks metrics-mongodb -p {{.labels.params_port}} -H {{.labels.params_host}} -d {{.labels.params_database}}`	`<hostname>.mongodb.conne 20632 1639498004`

MongoDB-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von MongoDB-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

metrics-mongodb – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.asserts.msg (empfohlene Metrik)		count	Anzahl der seit Beginn des MongoDB-Prozesses ausgelösten Nachrichten-Assertionen. Untersuchen Sie

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			die Protokolldatei auf weitere Informationen zu diesen Nachrichten.
mongodb.asserts.regular (empfohlene Metrik)		count	Anzahl der regulären Assertionen, die seit Beginn des MongoDB-Prozesses ausgelöst wurden. Untersuchen Sie die Protokolldatei auf weitere Informationen zu diesen Nachrichten.
mongodb.asserts.rollovers		count	Anzahl, die angibt, wie oft bei den Rollover-Zählern seit dem letzten Start des MongoDB-Prozesses ein Rollover durchgeführt wurde.
mongodb.asserts.tripwire			Anzahl der seit Beginn des MongoDB-Prozesses ausgelösten Tripwire-Assertionen.
mongodb.asserts.user		count	Anzahl der „Benutzer-Asserts“, die seit dem letzten Start des MongoDB-Prozesses aufgetreten sind.
mongodb.asserts.warning (empfohlene Metrik)		count	Anzahl der Warnungen, die seit Beginn des MongoDB-Prozesses ausgelöst wurden.
mongodb.connections.available		count	Anzahl der nicht verwendeten eingehenden Verbindungen, die verfügbar sind.
mongodb.connections.current		count	Anzahl der eingehenden Verbindungen von Clients zum Datenbankserver.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.connections.totalCreated		count	Anzahl aller eingehenden Verbindungen, die mit dem Server hergestellt wurden.
mongodb.cursor.open.noTimeout		count	Anzahl der offenen Cursor, bei denen die Option *DBQuery.Option.noTimeout* festgelegt ist, damit eine Zeitüberschreitung nach einem Zeitraum der Inaktivität verhindert wird.
mongodb.cursor.open.pinned		count	Anzahl der „angehefteten“ offenen Cursor.
mongodb.cursor.open.total (empfohlene Metrik)		count	Anzahl der Cursor, die MongoDB für Clients verwaltet. Da MongoDB nicht verwendete Cursor aufbraucht, ist dieser Wert normalerweise klein oder null. Wenn jedoch eine Warteschlange, veraltete „Tailable Cursor“ (spezielle bei Abschluss einer Abfrage nicht geschlossene, sondern offen gehaltene Cursor) oder eine große Anzahl von Vorgängen vorhanden sind, kann dieser Wert steigen.
mongodb.cursor.timedOut		count	Gesamtanzahl der Cursor, bei denen seit dem Start des Serverprozesses eine Zeitüberschreitung aufgetreten ist.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.databaseSize.avgObjSize	admin	Bytes	Durchschnittliche Größe jedes Dokuments in Bytes.
mongodb.databaseSize.avgObjSize	config	Bytes	Durchschnittliche Größe jedes Dokuments in Bytes.
mongodb.databaseSize.avgObjSize	local	Bytes	Durchschnittliche Größe jedes Dokuments in Bytes.
mongodb.databaseSize.collections	admin	count	Anzahl der Sammlungen in der Datenbank.
mongodb.databaseSize.collections	config	count	Anzahl der Sammlungen in der Datenbank.
mongodb.databaseSize.collections	local	count	Anzahl der Sammlungen in der Datenbank.
mongodb.databaseSize.dataSize	admin	Bytes	Gesamtgröße der unkomprimierten Daten in der Datenbank. Der Wert *dataSize* wird kleiner, wenn Sie Dokumente entfernen. Für Datenbanken, bei denen die Speicher-Engine *WiredTiger* verwendet wird, kann *dataSize* größer sein als *storageSize*, wenn die Komprimierung aktiviert ist. Der Wert *dataSize* wird kleiner, wenn Dokumente kleiner werden.
mongodb.databaseSize.dataSize	config	Bytes	Gesamtgröße der unkomprimierten Daten in der Datenbank.
mongodb.databaseSize.dataSize	local	Bytes	Gesamtgröße der unkomprimierten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Daten in der Datenbank.
mongodb.databaseSizes.indexes	admin	count	Gesamtanzahl der Indizes für alle Sammlungen in der Datenbank.
mongodb.databaseSizes.indexes	config	count	Gesamtanzahl der Indizes für alle Sammlungen in der Datenbank.
mongodb.databaseSizes.indexes	local	count	Gesamtanzahl der Indizes für alle Sammlungen in der Datenbank.
mongodb.databaseSizes.indexSize	admin	Bytes	Summe des Speicherplatzes, der allen Indizes in der Datenbank zugeordnet ist, einschließlich des freien Indexspeichers.
mongodb.databaseSizes.indexSize	config	Bytes	Summe des Speicherplatzes, der allen Indizes in der Datenbank zugeordnet ist, einschließlich des freien Indexspeichers.
mongodb.databaseSizes.indexSize	local	Bytes	Summe des Speicherplatzes, der allen Indizes in der Datenbank zugeordnet ist, einschließlich des freien Indexspeichers.
mongodb.databaseSizes.objects	admin	count	Anzahl der Objekte (insbesondere Dokumente) in der Datenbank über alle Sammlungen hinweg.
mongodb.databaseSizes.objects	config	count	Anzahl der Objekte (insbesondere Dokumente) in der Datenbank über alle Sammlungen hinweg.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.databaseSize.objects	escdb	count	Anzahl der Objekte (insbesondere Dokumente) in der Datenbank über alle Sammlungen hinweg.
mongodb.databaseSize.storageSize	escdb	Bytes	Dieser Wert verringert sich nicht, wenn Sie Dokumente entfernen oder verkleinern. Dieser Wert kann für Datenbanken, bei denen die Speicher-Engine *WiredTiger* mit aktivierter Komprimierung verwendet wird, kleiner als *dataSize* sein. *storageSize* enthält keinen den Indizes zugeordneten Speicherplatz. Informationen zur Gesamtindexgröße finden Sie unter *indexSize*.
mongodb.databaseSize.totalSize	escdb	Bytes	Summe des Speicherplatzes, der allen Sammlungen in der Datenbank zum Speichern von Dokumenten zugeordnet ist, einschließlich des freien Speicherplatzes.
mongodb.databaseSize.totalSize	escdb	Bytes	Summe des Speicherplatzes, der allen Sammlungen in der Datenbank zum Speichern von Dokumenten zugeordnet ist, einschließlich des freien Speicherplatzes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.globalLock.activeClients.readers (empfohlene Metrik)		count	Anzahl der aktiven Clientverbindungen, von denen Lesevorgänge ausgeführt werden.
mongodb.globalLock.activeClients.total		count	Gesamtzahl der internen Clientverbindungen mit der Datenbank, einschließlich der System-Threads sowie der Reader und Writer in der Warteschlange. Diese Metrik ist aufgrund der Einbeziehung von System-Threads höher als die Summe von *activeClients.readers* und *activeClients.writers*.
mongodb.globalLock.activeClients.writers (empfohlene Metrik)		count	Anzahl der aktiven Clientverbindungen, von denen Schreibvorgänge ausgeführt werden.
mongodb.globalLock.currentQueue.readers (empfohlene Metrik)		count	Anzahl der Vorgänge, die sich derzeit in der Warteschlange befinden und auf die Lesesperre warten. Eine durchgängig kleine Lesewarteschlange, insbesondere von kürzeren Vorgängen, ist kein Grund zur Besorgnis.
mongodb.globalLock.currentQueue.total		count	Gesamtanzahl der Vorgänge in der Warteschlange, die auf die Sperre warten (d. h. die Summe von *globalLock.currentQueue.reader* und

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			globalLock.currentQueue.writer Eine durchgängig kleine Warteschlange, insbesondere von kürzeren Vorgängen, ist kein Grund zur Besorgnis. Die *globalLock.activeClients*-Reader- und -Writer-Informationen machen Kontext für diese Daten verfügbar.
mongodb.globalLock.currentQueue.writers (empfohlene Metrik)		count	Anzahl der Vorgänge, die sich derzeit in der Warteschlange befinden und auf die Schreibsperre warten. Eine durchgängig kleine Schreibwarteschlange, insbesondere von kürzeren Vorgängen, ist kein Grund zur Besorgnis.
mongodb.globalLock.totalTime		Mikrosekunden	Zeit in Mikrosekunden, seit die Datenbank zuletzt gestartet wurde und die *globalLock* erstellt hat. Dies entspricht in etwa der Gesamtbetriebszeit des Servers.
mongodb.locks.Collection.acquireCount_r		count	Anzahl, die angibt, wie oft die Sammlungssperre im Sperrmodus „Intent Shared“ (IS) erfasst wurde.
mongodb.locks.Collection.acquireCount_w		count	Anzahl, die angibt, wie oft die Sammlungssperre im Sperrmodus „Intent

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Exclusive“ (IX) erfasst wurde.
mongodb.locks.Collection.acquireCount_W		count	Anzahl, die angibt, wie oft die Sammlungssperre im Sperrmodus „Exclusive“ (X) erfasst wurde.
mongodb.locks.Database.acquireCount_r		count	Anzahl, die angibt, wie oft die Datenbanksperre im Sperrmodus „Intent Shared“ (IS) erfasst wurde.
mongodb.locks.Database.acquireCount_w		count	Anzahl, die angibt, wie oft die Datenbanksperre im Sperrmodus „Intent Exclusive“ (IX) erfasst wurde.
mongodb.locks.Database.acquireCount_W		count	Anzahl, die angibt, wie oft die Datenbanksperre im Sperrmodus „Exclusive“ (X) erfasst wurde.
mongodb.locks.Global.acquireCount_r		count	Anzahl, die angibt, wie oft die globale Sperre im Sperrmodus „Intent Shared“ (IS) erfasst wurde.
mongodb.locks.Global.acquireCount_w		count	Anzahl, die angibt, wie oft die globale Sperre im Sperrmodus „Intent Exclusive“ (IX) erfasst wurde.
mongodb.locks.Global.acquireCount_W		count	Anzahl, die angibt, wie oft die globale Sperre im Sperrmodus „Exclusive“ (X) erfasst wurde.
mongodb.mem.pageFaults		count	Gesamtanzahl der Seitenfehler. Der *extra_info.page_faults*-Zähler kann

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			in Momenten schlechter Leistung drastisch ansteigen und mit Umgebungen mit begrenztem Arbeitsspeicher und größeren Datensätzen korrelieren. Begrenzte und sporadische Seitenfehler weisen nicht unbedingt auf ein Problem hin.
mongodb.mem.resident (empfohlene Metrik)		Mebibyte	Dieser Wert entspricht in etwa der Größe des Arbeitsspeichers (in Mebibyte, MiB), der derzeit vom Datenbankprozess verwendet wird. Während des normalen Gebrauchs steigt dieser Wert tendenziell an. Bei dedizierten Datenbankservern nähert sich die Anzahl häufig der Gesamtmenge des Systemspeichers an.
mongodb.mem.virtual		Mebibyte	Menge des vom mongod-Prozess verwendeten virtuellen Arbeitsspeichers in Mebibyte (MiB).
mongodb.metrics.document.deleted		count	Gesamtanzahl der gelöschten Dokumente.
mongodb.metrics.document.inserted		count	Gesamtanzahl der eingefügten Dokumente.
mongodb.metrics.document.returned		count	Gesamtanzahl der von Abfragen zurückgegebenen Dokumente.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.metrics.document.updated		count	Gesamtanzahl der aktualisierten Dokumente.
mongodb.metrics.getLastError.wtime_num (empfohlene Metrik)		count	Gesamtanzahl der *getLastError*-Vorgänge, bei denen der „Write Concern“ (w) so festgelegt ist, dass von mindestens einem Mitglied eines Replikatsatzes die Bestätigung des Schreibvorgangs abgewartet wird (Einstellung: w-Wert größer als 1).
mongodb.metrics.getLastError.wtime_totalMillis (empfohlene Metrik)		Millisekunden	Gesamtzeit in Millisekunden, die vom mongod-Prozess darauf verwendet wurde, *getLastError*-Vorgänge auszuführen, bei denen der „Write Concern“ (w) so festgelegt ist, dass von mindestens einem Mitglied eines Replikatsatzes die Bestätigung des Schreibvorgangs abgewartet wird (Einstellung: w-Wert größer als 1).
mongodb.metrics.getLastError.wtimeouts (empfohlene Metrik)		count	Anzahl, die angibt, wie oft bei „Write Concern“-Vorgängen aufgrund des *wtimeout*-Schwellenwerts für *getLastError* eine Zeitüberschreitung aufgetreten ist. Diese Anzahl wird sowohl für standardmäßige als auch für nicht

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			dem Standard entsprechende „Write Concern"-Spezifikationen schrittweise erhöht.
mongodb.metrics.operation.scanAndOrder		count	Gesamtanzahl der Abfragen, von denen sortierte Zahlen zurückgegeben werden und bei denen der Sortiervorgang nicht mit einem Index ausgeführt werden kann.
mongodb.metrics.queryExecutor.scanned		count	Gesamtanzahl der während Abfragen und Abfrageplanauswertungen gescannten Indexelemente. Dieser Zähler ist derselbe wie *totalKeysExamined* in der Ausgabe von explain().
mongodb.metrics.queryExecutor.scannedObjects		count	Gesamtanzahl der Dokumente, die während Abfragen und Abfrageplanauswertungen gescannt wurden. Dieser Zähler ist derselbe wie *totalDocsExamined* in der Ausgabe von explain().
mongodb.metrics.record.moves			Ein Dokument, in dem über Daten im Zusammenhang mit der Datensatzzuordnung in den Speicherdateien auf dem Datenträger berichtet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.metrics.repl.	apply.batches_num	count	Gesamtanzahl der auf alle Datenbanken angewendeten Batches.
mongodb.metrics.repl.	apply.batches_totalMillis	count	Gesamtzeit in Millisekunden, die vom mongod-Prozess darauf verwendet wurde, Vorgänge aus der oplog-Sammlung (Operations Log) anzuwenden.
mongodb.metrics.repl.	apply.ops	count	Gesamtanzahl der angewendeten oplog-Vorgänge. Der *metrics.repl.apply.ops*-Wert wird nach jedem Vorgang erhöht.
mongodb.metrics.repl.	buffer.count	count	Aktuelle Anzahl der Vorgänge im oplog-Puffer.
mongodb.metrics.repl.	buffer.maxSizeBytes	Bytes	Maximale Größe des Puffers. Dieser Wert ist eine konstante Einstellung im mongod-Prozess und kann nicht konfiguriert werden.
mongodb.metrics.repl.	buffer.sizeBytes	Bytes	Aktuelle Größe des Inhalts des oplog-Puffers.
mongodb.metrics.repl.	network.bytes	count	Gesamtmenge der aus der Replikationssynchronisierungsquelle gelesenen Daten.
mongodb.metrics.repl.	network.getmores_num	count	Meldet die Gesamtanzahl der *getmore*-Vorgänge, bei denen es sich um Vorgänge handelt, mit denen ein zusätzlicher Satz von Vorgängen von der

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Replikationssynchronisierungsquelle angefordert wird.
mongodb.metrics.repl.network.getmores_totalMillis		Millisecond	Gesamtzeit, die zum Sammeln von Daten aus *getmore*-Vorgängen erforderlich ist.
mongodb.metrics.repl.network.ops		count	Gesamtanzahl der aus der Replikationsquelle gelesenen Vorgänge.
mongodb.metrics.repl.network.readersCreated		count	Gesamtanzahl der erstellten oplog-Abfrageprozesse. Von MongoDB wird jedes Mal eine neue oplog-Abfrage erstellt, wenn ein Fehler in der Verbindung auftritt, einschließlich einer Zeitüberschreitung oder eines Netzwerkvorgangs. Darüber hinaus wird der *metrics.repl.network.readersCr* Wert jedes Mal erhöht, wenn von MongoDB eine neue Quelle für die Replikation ausgewählt wird.
mongodb.metrics.ttl.deletedDocuments		count	Gesamtanzahl der Dokumente, die aus Sammlungen mit einem *ttl*-Index gelöscht wurden.
mongodb.metrics.ttl.passes		count	Gesamtanzahl der Dokumente, die aus Sammlungen mit einem *ttl*-Index gelöscht wurden.
mongodb.network.bytesIn		count	Gesamtanzahl der Bytes, die vom

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Server über von Clients initiierte Netzwerkverbindungen empfangen wurden.
mongodb.network.bytesOut		count	Gesamtanzahl der Bytes, die vom Server über von Clients initiierte Netzwerkverbindungen gesendet wurden.
mongodb.network.numRequests		count	Gesamtanzahl der eindeutigen Anforderungen, die der Server erhalten hat. Verwenden Sie diesen Wert, um Kontext für die Werte *network.bytesIn* und *network.bytesOut* bereitzustellen und dadurch sicherzustellen, dass die Netzwerkauslastung von MongoDB den Erwartungen und der Anwendungsnutzung entspricht.
mongodb.opcounters.	command	count	Gesamtanzahl der seit dem letzten Start der mongod-Instanz an die Datenbank ausgegebenen Befehle. Von *opcounters.command* werden alle Befehle mit Ausnahme der Schreibbefehle insert (einfügen), update (aktualisieren) und delete (löschen) gezählt.
mongodb.opcounters.	delete	count	Gesamtanzahl der Löschvorgänge seit dem letzten Start der mongod-Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.opcounters.	getmore	count	Gesamtanzahl der *getMore*-Vorgänge seit dem letzten Start der mongod-Instanz. Dieser Zähler kann hoch sein, auch wenn die Abfrageanzahl niedrig ist. Von sekundären Knoten werden *getMore*-Vorgänge als Teil des Replikationsprozesses gesendet.
mongodb.opcounters.	insert	count	Gesamtanzahl der Einfügevorgänge, die seit dem letzten Start der mongod-Instanz empfangen wurden.
mongodb.opcounters.	query	count	Gesamtanzahl der Abfragen, die seit dem letzten Start der mongod-Instanz empfangen wurden.
mongodb.opcounters.	update	count	Gesamtanzahl der Aktualisierungsvorgänge, die seit dem letzten Start der mongod-Instanz empfangen wurden.
mongodb.opcountersRepl.	command	count	Gesamtanzahl der seit dem letzten Start der mongod-Instanz an die Datenbank ausgegebenen replizierten Befehle.
mongodb.opcountersRepl.	delete	count	Gesamtanzahl der replizierten Löschvorgänge seit dem letzten Start der mongod-Instanz.
mongodb.opcountersRepl.	getmore	count	Gesamtanzahl der getMore-Vorgänge seit dem letzten Start der mongod-Instanz.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-mongodb – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mongodb.opcountersRepl.insert (empfohlene Metrik)		count	Gesamtanzahl der replizierten Einfügevorgänge seit dem letzten Start der mongod-Instanz.
mongodb.opcountersRepl.query (empfohlene Metrik)		count	Gesamtanzahl der seit dem letzten Start der mongod-Instanz replizierten Abfragen.
mongodb.opcountersRepl.update		count	Gesamtanzahl der replizierten Aktualisierungsvorgänge seit dem letzten Start der mongod-Instanz.

Standardprüfungen und -richtlinien für MS Exchange

Agent Client Collector stellt die folgenden Standardprüfungen und -richtlinien für die MS Exchange-Überwachung bereit.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe

Metrik	app.msexchange.metric-msexchange	Gibt Microsoft Exchange-Metriken zurück.	`winchecks metric-msexchange (options) -s scheme Replaces the host name with this parameter`
			
			Anwendungsbeispiel:
			`Winchecks Metric-msexchange {{if .labels.params_scheme}} -s {{if .labels.params_scheme}} {{end}}`
				Metriken von MS Exchange-Server

MSSQL – Standardprüfungen und Richtlinien

Agent Client Collector stellt die folgenden Standardprüfungen und -richtlinien für die Überwachung von MSSQL-Metriken bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MSSQL Metrics

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Metrik	app.metrics-mssql-query	Generische MSSQL-Abfrageklasse, die eine Abfrage akzeptiert und Metriken ausgeben kann.	winchecks metrics-mssql-query (Optionen) -d, --database DATABASE – Datenbankschema, mit dem eine Verbindung hergestellt werden soll (erforderlich) -q ,--query – Die auszuführende Abfrage; sollte einen Listenmetriknamen und -wert zurückgeben, z. B. SELECT METRIC_NAME, VALUE FROM GV $SYSMETRIC -h, --host HOST – Name des Hosts, mit dem eine Verbindung hergestellt werden soll; Standardwert: localhost -r, --port PORT – Port, mit dem eine Verbindung hergestellt werden soll; Standardwert: 1433 -s, --scheme SCHEME – Metrikbenennungsschema; Text, der . $parent.$child vorangestellt werden soll. **Verwendungsbeispiel**	In den Parametern definierte benutzerdefinierte Metriken, die auch Wert und Zeitstempel enthalten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MSSQL Metrics (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			`.winchecks metrics-mssql-query -d master -H localhost -p 1437 -q "select name,size from sys.database_files"`	

MySQL-Standardprüfungen und -richtlinien

Agent Client Collector stellt die folgenden Standardprüfungen und -richtlinien für die Überwachung von MySQL-Metriken bereit.

MySQL-Ereignisse

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Ereignis	app.mysql.check-mysql-alive	Überprüft die Länge eines Ergebnissatzes aus einer MySQL-Abfrage.	check-mysql-query-result-count.rb (Optionen) -c, --critical COUNT COUNT kritischer Schwellenwert für die Anzahl der von der Abfrage zurückgegebenen Elemente (erforderlich) -d, --database DATABASE MySQL-Datenbank (erforderlich) -h, --host HOST MySQL-Host, mit dem eine Verbindung hergestellt werden soll (erforderlich) -i, --ini VALUE My.cnf INI-Datei	MysqlQueryCountCheck OK/KRITISCH/ WARNUNG: Meldung zum Verhältnis zwischen Abfragelänge und Schwellenwerten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			--ini-section Abschnitt „WERT“ in INI-Datei „my.cnf“. Um die Verbindung mit MySQL über die INI-Datei zu aktivieren, geben Sie die Werte für die Eigenschaften „user“ und „password“ im **Client-** Abschnitt der INI-Datei an. -P, --port PORT-MySQL-Port, mit dem eine Verbindung hergestellt werden soll -q, --query QUERY Auszuführende Abfrage (erforderlich) -w, --warning COUNT Anzahlwarnungsschwellenwert für die Anzahl der von der Abfrage zurückgegebenen Elemente (erforderlich) -S, --socket UNIX-Socket für die Verbindung mit (erforderlich, wenn der angegebene Host „localhost“ unter UNIX-ähnlichen Systemen ist) **Verwendungsbeispiel**	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			`check-mysql-query-result-count.rb -h 127.0.0.1 -P 3306 -d mysql -q "* aus Anwender auswählen" -w 5 -c 8`	
Ereignis	app.mysql.check-mysql-threads	Überprüft die MySQL DB-Anzahl der laufenden Threads und weist abhängig von den Eingabewerten den Status OK/WARNUNG/ KRITISCH zu.	check-mysql-threads.rb (Optionen) -h, --hostname HOST Hostname für die Anmeldung -i, --ini VALUE My.cnf INI-Datei --ini-section Abschnitt „WERT“ in INI-Datei „my.cnf“ (Erforderlich, wenn INI-Pfad angegeben). Um die Verbindung mit MySQL über die INI-Datei zu aktivieren, geben Sie die Werte für die Eigenschaften „user“ und „password“ im **Client-** Abschnitt der INI-Datei an. -c, --critnum NUMBER Anzahl der laufenden Threads, für die eine Warnung ausgegeben wird -w, --warnnum NUMBER Anzahl der laufenden	CheckMySQLHealth OK/Kritisch/ Warnung und Anzahl der laufenden Threads

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Threads, für die eine Warnung ausgegeben wird -P, --port PORT-MySQL-Port, mit dem eine Verbindung hergestellt werden soll -S, --socket UNIX-Socket für die Verbindung mit (erforderlich, wenn der angegebene Host „localhost“ unter UNIX-ähnlichen Systemen ist) **Verwendungsbeispiel** `check-mysql-threads.rb -h 127.0.0.1 -P 3306 -l 0 -m 1 -c 25 -w 20`	
Ereignis	util.check-mysql-query	Überprüft, ob MySQL DB ausgeführt wird.	check-mysql-threads.rb (Optionen) -h, --hostname HOST Hostname für die Anmeldung -i, --ini VALUE My.cnf INI-Datei --ini-section Abschnitt „WERT“ in INI-Datei „my.cnf“ (Erforderlich, wenn INI-Pfad angegeben ist). Um die Verbindung mit MySQL über	CheckMySQLHealth OK/Kritisch/ Warnung und Anzahl der laufenden Threads

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			die INI-Datei zu aktivieren, geben Sie die Werte für die Eigenschaften „user“ und „password“ im **Client-** Abschnitt der INI-Datei an. -c, --critnum NUMBER Anzahl der laufenden Threads, für die eine Warnung ausgegeben wird -w, --warnnum NUMBER Anzahl der laufenden Threads, für die eine Warnung ausgegeben wird -l, --critlow NUMBER Anzahl der laufenden Threads, unter denen eine Warnung ausgegeben wird -m, --warnlow NUMBER Anzahl der laufenden Threads, unter denen eine Warnung ausgegeben wird -P, --port PORT-MySQL-Port, mit dem eine Verbindung hergestellt werden soll -s, --socket UNIX-Socket für die	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Verbindung mit (erforderlich, wenn der angegebene Host „localhost“ unter UNIX-ähnlichen Systemen ist) **Verwendungsbeispiel** `check-mysql-threads.rb -h 127.0.0.1 -P 3306 -l 0 -m 1 -c 25 -w 20`	

MySQL-Metriken

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Metrik	app.mysql.metrics-mysql	Gibt Metriken in der MySQL-DB zurück.	/usr/local/bin/metrics-mysql-graphite.rb (Optionen) -h, --host HOST MySQL-Host, mit dem eine Verbindung hergestellt werden soll (erforderlich) -i, --ini VALUE My.cnf INI-Datei --ini-section Abschnitt „WERT“ in INI-Datei „my.cnf“ (Erforderlich, wenn INI-Pfad angegeben ist). Um die Verbindung mit MySQL über die INI-Datei zu aktivieren, geben Sie die Werte für die	MysqlQueryCountCheck OK/KRITISCH/ WARNUNG: Meldung zum Verhältnis zwischen Abfragelänge und Schwellenwerten

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Eigenschaften „user“ und „password“ im **Client-** Abschnitt der INI-Datei an. -P, --port PORT MySQL-Port, mit dem eine Verbindung hergestellt werden soll. -s, --scheme SCHEME-Metrikbenennungsschema, Text, der an die Metrik angehängt werden soll -S, --socket UNIX-Socket für die Verbindung mit (erforderlich, wenn der angegebene Host „localhost“ unter UNIX-ähnlichen Systemen ist) -v, --verbose Zeigt Fehler (falls generiert) für sekundäre Statuskopien an. Fügen Sie dem Befehl zum Aktivieren -v hinzu. **Verwendungsbeispiel** `check-mysql-threads.rb -h 127.0.0.1 -P 3306 -l 0 -m 1 -c 25 -w 20`	
Metrik	app.mysql.check-mysql-threads	Überprüft die MySQL DB-Anzahl der	/usr/local/bin/metrics-mysql-	hostname.mysql.general.aborted 7600 1649630975

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
		laufenden Threads und weist abhängig von den Eingabewerten den Status OK/WARNUNG/ KRITISCH zu.	graphite.rb (Optionen) -h, --hostname HOST Hostname, mit dem eine Verbindung hergestellt werden soll (erforderlich) -i, --ini VALUE My.cnf INI-Datei --ini-section Abschnitt „WERT“ in INI-Datei „my.cnf“ (Erforderlich, wenn INI-Pfad angegeben ist). Um die Verbindung mit MySQL über die INI-Datei zu aktivieren, geben Sie die Werte für die Eigenschaften „user“ und „password“ im **Client-** Abschnitt der INI-Datei an. -c, --critnum NUMBER Anzahl der laufenden Threads, für die eine Warnung ausgegeben wird -w, --warnnum NUMBER Anzahl der laufenden Threads, für die eine Warnung ausgegeben wird -l, --critlow NUMBER Anzahl der laufenden	hostname.mysql.general.aborted 247 1649630975 hostname.mysql.allgemein.txByte 752733902 1649630975 hostname.mysql.commands.adm 1631 1649630975 hostname.mysql.commands.alter 0 1649630975

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			Threads, unter denen eine Warnung ausgegeben wird -m, --warnlow NUMBER Anzahl der laufenden Threads, unter denen eine Warnung ausgegeben wird -P, --port PORT-MySQL-Port, mit dem eine Verbindung hergestellt werden soll -s, --socket UNIX-Socket für die Verbindung mit (erforderlich, wenn der angegebene Host „localhost“ unter UNIX-ähnlichen Systemen ist) **Verwendungsbeispiel** `metrics-mysql-graphite.rb -h 127.0.0.1 -P 3306`	
Metrik	app.mysql.metrics-mysql-processes	Gibt verschiedene Metriken zu MySQL DB-Prozessen zurück	/usr/local/bin/metrics-mysql-processes.rb (Optionen) -h, --host MySQL-Host, zu dem eine Verbindung hergestellt werden soll	Prozesse, die von ihnen ausgeführten Befehle und die Datenbanken, in denen die Befehle ausgeführt werden **Beispiel:**

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			-i, --ini VALUE My.cnf INI-Datei --ini-section Abschnitt „WERT“ in INI-Datei „my.cnf“ (Erforderlich, wenn INI-Pfad angegeben ist). Um die Verbindung mit MySQL über die INI-Datei zu aktivieren, geben Sie die Werte für die Eigenschaften „user“ und „password“ im **Client-** Abschnitt der INI-Datei an. -P, --port PORT-MySQL-Port, mit dem eine Verbindung hergestellt werden soll -s --scheme SCHMEMetrikbenennungsschema, Text, der an die Metrik angehängt werden soll -s, --socket UNIX-Socket für die Verbindung mit (erforderlich, wenn der angegebene Host „localhost“ unter UNIX-ähnlichen Systemen ist) **Verwendungsbeispiel** `metrics-mysql-processes.rb`	• hostname.mysql.database.mys 1 1649631113 • hostname.mysql.command.Da 1 1649631113 • hostname.mysql.command.Sle 4 1649631113 • hostname.mysql.command.Qu 1 1649631113

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MySQL-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			`-h 127.0.0.1 -P 3306`	

Standardprüfungen und -richtlinien für Netzwerk-Ping

Agent Client Collector stellt die folgenden Standardprüfungen und -richtlinien für die Netzwerk-Ping-Überwachung bereit. Richtlinien und Prüfungen sind für Windows und Linuxverfügbar.

Richtlinie für Netzwerk-Ping-Metriken

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe

util.metrics-ping	Wird unter der in der Instanz ServiceNow erkannten IP-Adresse ausgeführt. Pingt den Host an und sammelt Metriken.
	
	Der überwachte CI-Typ ist *cmdb_ci_hardware* und ist an den entsprechenden Server gebunden.
	
	Ein Proxy-Agent ist erforderlich.
		metrics-ping.rb (Optionen)
		
		`c --count COUNT Ping-Anzahl`
		
		`-h Host zum Ping`
		
		`-t --timeout TIMEout (Zeitüberschreitung) Zeitüberschreitung`
		
		Beispiel: ./ metrics-ping.rb -h 10.196.121.11
				`c7inc0047383.ping.packets_transmitted 5 1675923886`
				
				`c7inc0047383.ping.packets_received 5 1675923886`
				
				`c7inc0047383.ping.packet_loss 0 1675923886`
				
				`c7inc0047383.ping.time 3999 1675923886`
				
				`c7inc0047383.ping.min 0.253 1675923886`
				
				`c7inc0047383.ping.avg 0.292 1675923886`
				
				`c7inc0047383.ping.max 0.318 1675923886`
				
				`c7inc004738`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Netzwerk-Ping-Metriken (Fortsetzung)

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
				`3.ping.mdev 0.032 1675923886` **Hinweis:** Windows unterstützt die Metriken *ping.time* und *ping.mdev* nicht.

Ping-Metriken für das Netzwerk

In der folgenden Tabelle sind die Metriken aufgeführt, die als Ausgabe von Netzwerk-Ping-Prüfungen gesammelt werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Netzwerk-Ping-Metriken

Metriktyp	Einheiten	Beschreibung des Metriktyps
ping.packets_transmitted	count	Anzahl der Datenpakete, die während des Ping-Tests an den Zielhost gesendet wurden.
ping.packets_received	count	Anzahl der Datenpakete, die erfolgreich vom Zielhost empfangen wurden.
ping.packet_loss	percentage	Prozentsatz der Datenpakete, die den Zielhost nicht erreicht haben.
ping.time	ms	Zeit, die Datenpakete zum Ziel und zurück benötigen.
ping.min	ms	Kürzeste Zeit für eine Reihe von Ping-Anforderungen für die Datenpakete.
ping.durchschn	ms	Durchschnittliche Zeit für eine Reihe von Ping-Anforderungen für die Datenpakete.
ping.max	ms	Längste Zeit für eine Reihe von Ping-Anforderungen für die Datenpakete.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerk-Ping-Metriken (Fortsetzung)

Metriktyp	Einheiten	Beschreibung des Metriktyps
ping.mdev	ms	Durchschnittliche Abweichung (Messung der Variabilität oder Streuung) der Umlaufzeit (Round-Trip Time, RTT) der während des Ping-Tests gesendeten Pakete.

Verfügbarkeitsprüfung des Netzwerkhosts

Agent Client Collector bietet die folgende Standardprüfung für die Netzwerk-Ping-Überwachung. Die Prüfung ist für Windows und Linux verfügbar.

util.check-ping check

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
util.check-ping	Überprüft die Verfügbarkeit des Netzwerkhosts über ICMP-(Ping-)Anforderungen. Generiert ein OK-Ereignis, wenn die Ping-Erfolgsquote den Warnungsschwellenwert (-W, Standard 50 %) überschreitet. Generiert ein Warnereignis, wenn die Ping-Erfolgsquote zwischen dem Warnungsschwellenwert (-W, Standard 50 %) und dem kritischen Schwellenwert (-C, Standard 20 %) liegt. Generiert ein kritisches Ereignis, wenn die Ping-Erfolgsquote unter den kritischen	`check-ping.rb -h` <ip-address> (Optionen) `-h host`: Host zu Ping (erforderlich). Standard =<localhost> `-c count`: Anzahl der an den Host gesendeten Ping-Anforderungen. Standard = 1 `-T-Zeitüberschreitung`: Die Zeitüberschreitung (in Sekunden) für jede Ping-Anforderung. Wenn die Zeitüberschreitung abläuft, bevor eine Antwort empfangen wird, gilt der Ping als fehlgeschlagen. Standard = 5 `-6 ipv6`: Aktiviert IPv6-		`ICMP ping unsuccessful for host: 192.168.1.1 (successful: 0/5)`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

util.check-ping check (Fortsetzung)

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
	Schwellenwert (-C, Standard 20 %) fällt. Ein Proxy-Agent ist erforderlich.	Ping. Ping verwendet IPv4, wenn diese Kennzeichnung nicht verwendet wird. Standard = False `-i-Intervall`: Intervall (in Sekunden) zwischen den einzelnen Ping-Anforderungen. Standard = 1 `-W-Verhältnis`: Der Schwellenwert für das Erfolgsverhältnis für den Status „Warnung“. Wenn die Anzahl der erfolgreichen Ping-Antworten unter diesem Verhältnis und über dem -C-Verhältnis liegt, gibt das Skript eine Warnung zurück. Standard = 0,5 `-C-Verhältnis`: Der Schwellenwert für das Erfolgsverhältnis für einen Status „Kritisch“. Wenn die Anzahl der erfolgreichen Ping-Antworten darunter liegt, gibt das Skript einen kritischen Fehler zurück. Standard = 0,2 `-r Bericht`: Kennzeichnung,		

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

util.check-ping check (Fortsetzung)

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
		die an die Fehlermeldung eines MTR-Berichts (My Trace Route) angehängt werden soll, wenn der Ping fehlschlägt. Wenn MTR ausgeführt wird, wird ein Netzwerkdiagnosebericht generiert. Standard = falsch		

Nginx – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Richtlinien für die Nginx-Systemüberwachung. Die Richtlinien beinhalten die in der angegebenen Tabelle ausgewiesenen Prüfungen. Richtlinien und Prüfungen sind für Windows und Linux verfügbar.

Richtlinie für Nginx-Ereignisse

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
nginx.check-nginx-alive	Überprüft, ob der Nginx-Server aktiv ist. **Hinweis:** Verwenden Sie für Ereignisse die Standardauthentifizierung.	`check-nginx-status.rb` -h, --host Nginx-Hostname -p, --port Nginx-Port **Hinweis:** Verwenden Sie für Ereignisse die Standardauthentifizierung.		Erfolgreich `CheckNginxStatus OK: Nginx is Alive and healthy` (CheckNginxStatus OK: Nginx ist aktiv und fehlerfrei) Fehler `CheckNginxStatus CRITICAL: Nginx is Down` (CheckNginxStatus KRITISCH: Nginx ist ausgefallen)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Nginx-Metriken

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe

nginx.metrics-nginx-server	Ruft die folgenden Informationen ab:
	nginx.active_connections
	Gesamtanzahl der aktiven Verbindungen auf dem Server.
	nginx.accepts
	Die akzeptierten Verbindungen.
	nginx.handled
	Behandelte Verbindungen, die normalerweise der Anzahl der akzeptierten Verbindungen entsprechen.
	nginx.requests
	Gesamtanzahl der vom Server verarbeiteten Anforderungen.
	nginx.read
	Zeigt an, ob vom Server Anforderungen gelesen werden.
	nginx.writing
	Zeigt an, ob
		`metrics-nginx.rb`
		Optionen:
		`-u --url` Vollständige URL zur Serverstatusseite. Beispiel: `https://yoursite.com/nginx_status`
				`ws19-INC0047517.nginx.active_connections 1 1640135552`
				`ws19-INC0047517.nginx.accepts 5746 1640135552`
				`ws19-INC0047517.nginx.handled 5746 1640135552`
				`ws19-INC0047517.nginx.requests 9603 1640135552`
				`ws19-INC0047517.nginx.reading 0 1640135552`
				`ws19-INC0047517.nginx.writing 1 1640135552`
				`ws19-INC0047517.nginx.waiting 0 1640135552`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Nginx-Metriken (Fortsetzung)

Überprüfen	Beschreibung	Verwendung	Befehl	Ausgabe
	vom Server Antworten an den Client geschrieben werden. nginx.waiting Inaktive Verbindungen, die auf eine Anforderung warten. **Hinweis:** Verwenden Sie für Metriken die Standardauthentifizierung.			

Nginx-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Nginx-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

metrics-nginx – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
nginx.active_connections (empfohlene Metrik)	admin	count	Gesamtanzahl der auf dem Server geöffneten Verbindungen, einschließlich wartender Verbindungen (*nginx.waiting*-Wert). Sie gibt die Anzahl der aktuellen Benutzer auf der Website

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-nginx – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			wieder. Für einen einzelnen Benutzer können mehrere Verbindungen geöffnet sein.
nginx.accepts (empfohlene Metrik)	admin	count	Stellt die Gesamtanzahl der hergestellten Verbindungen dar, wenn `https://yoursite.com/nginx_status` ausgelöst wird.
nginx.handled (empfohlene Metrik)	admin	count	Gesamtanzahl der vom Nginx-Server verarbeiteten Verbindungen.
nginx.requests (empfohlene Metrik)	admin	count	Gesamtanzahl der vom Nginx-Server verarbeiteten Anforderungen.
nginx.reading (empfohlene Metrik)	admin	count	Aktuelle Anzahl der Verbindungen, bei denen vom Nginx-Server der Anforderungsheader gelesen wird.
nginx.writing (empfohlene Metrik)	admin	count	Stellt die aktuelle Anzahl der Verbindungen dar, bei denen vom Nginx-Server die Antwort an den Client zurückgeschrieben wird.
nginx.waiting (empfohlene Metrik)	admin	count	Anzahl der im Leerlauf befindlichen Clientverbindungen, die auf eine Anforderung warten.

PostgreSQL – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für PostgreSQL-Systemüberwachung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PostgreSQL-Prüfungen

Typ	Prüfung	Beschreibung	Befehl
Event	postgresql.check-alive	Löst eine Warnung zum Status der PostgreSQL-Datenbank aus	`commonchecks check-postgres-alive -d {{.labels.params_database}} -p {{.labels.params_port}} -H {{.labels.params_host}}`
Event	postgresql.check-connections	Löst basierend auf dem konfigurierten Schwellenwert eine Warnung über die gesamte Verbindungslast in der PostgreSQL-Datenbank aus	`commonchecks check-postgres-connections -d {{.labels.params_database}} -c {{.labels.params_critical}} -p {{.labels.params_port}} -H {{.labels.params_host}} -w {{.labels.params_warning}} -a {{.labels.params_use_percentage`
Metrik	postgresql.metric-active-connections	Stellt Metriken für die gesamte aktive Verbindung in der PostgreSQL-Datenbank bereit	`commonchecks metric-postgres-connections -p {{.labels.params_port}} -d {{.labels.params_database}} -H {{.labels.params_host}}`
Metrik	postgresql.metric-dbsize	Stellt Metriken zur Gesamtgröße für jede PostgreSQL-Datenbank des Servers bereit	`commonchecks metric-postgres-dbsize -d {{.labels.params_database}} -H {{.labels.params_host}} -p {{.labels.params_port}}`
Metrik	postgresql.metric-locks	Stellt Metriken für die Sperren für die PostgreSQL-Datenbank/Tabellen bereit	`commonchecks metric-postgres-locks -p {{.labels.params_port}} -d {{.labels.params_database}} -H {{.labels.params_host}}`
Metrik	postgresql.metric-relation-size	Stellt Metriken zur Größe der Datenbanktabelle auf dem Server bereit	`commonchecks metric-postgres-relation-size -p {{.labels.params_port}}`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

PostgreSQL-Prüfungen (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
			`-l {{.labels.params_limit}} -H {{.labels.params_host}} -d {{.labels.params_database}}`
Metrik	postgresql.metric-statsbgwriter	Stellt Metriken im Zusammenhang mit Pufferzuordnungen bereit	`commonchecks metric-postgres-statsbgwriter -p {{.labels.params_port}} -d {{.labels.params_database}} -H {{.labels.params_host}}`
Metrik	postgresql.metric-statsdb	Stellt Metriken bereit, die sich auf Commits/ Rollbacks/Tupel-Transaktionen/ Deadlocks/ Abfragekonflikte beziehen	`commonchecks metric-postgres-statsdb -d {{.labels.params_database}} -H {{.labels.params_host}} -p {{.labels.params_port}}`
Metrik	postgresql.metric-statsio	Stellt tabellenbasierte Metriken hinsichtlich Indexlesevorgängen/ Gesamttreffer für einen Tabellenindex bereit	`commonchecks metric-postgres-statsio -s {{.labels.params_scope}} -H {{.labels.params_host}} -p {{.labels.params_port}} -d {{.labels.params_database}}`
Metrik	postgresql.metric-statstable	Stellt Metriken im Zusammenhang mit CRUD-Vorgängen bereit	`commonchecks metric-postgres-statstable -d {{.labels.params_database}} -H {{.labels.params_host}} -s {{.labels.params_scope}} -p {{.labels.params_port}}`

Automatische Übersetzung

PostgreSQL-Metriken

In den folgenden Tabellen werden die Metriken aufgelistet und beschrieben, die als Ausgabe von den angegebenen PostgreSQL-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

postgresql.check-connections-Metriken

Metrik	Beschreibung
pgsql.connections.active (Empfohlene Metrik)	Stellt Metriken für die gesamten aktiven Verbindungen in der PostgreSQL-Datenbank bereit
pgsql.connections.idle (Empfohlene Metrik)	Stellt Metriken für die gesamten inaktiven Verbindungen in der PostgreSQL-Datenbank bereit

postgresql.metric-dbsize-Metriken

Metrik	Beschreibung
pgsql.db.size (Empfohlene Metrik)	Stellt Metriken zur Gesamtauslastung der Laufwerksgröße für jede PostgreSQL-Datenbank auf dem Server bereit

postgresql.metric-locks-Metriken

Metrik	Beschreibung
pgsql.locks.AccessShareLock	Stellt Metriken für den Lesesperrmodus bereit, die automatisch aus abgefragten Tabellen abgerufen werden
pgsql.locks.ExclusiveLock	Stellt Metriken für den Lesesperrmodus bereit, die von der Tabelle LOCK TABLE für IN EXCLUSIVE MODE-Anweisungen abgerufen werden

postgresql.metric-relation-size-Metriken

Metrik	Beschreibung
pgsql.tables_size (Empfohlene Metrik)	Stellt Metriken zur Größe der Datenbanktabelle auf dem Server bereit

postgresql.metric-statsbgwriter-Metriken

Metrik	Beschreibung
pgsql.statsbgwriter.buffers_alloc	Stellt Metriken im Zusammenhang mit der Anzahl zugeordneter Puffer bereit
pgsql.statsbgwriter.buffers_backend	Stellt Metriken bereit, die sich auf die Anzahl der direkt von einem Back-End geschriebenen Puffer beziehen
pgsql.statsbgwriter.buffers_backend_fsync	Stellt Metriken bereit, die sich auf die Häufigkeit beziehen, mit der ein Back-End seinen eigenen fsync-Aufruf ausführen muss (normalerweise verarbeitet der Hintergrund-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

postgresql.metric-statsbgwriter-Metriken (Fortsetzung)

Metrik	Beschreibung
	Writer diese, auch wenn das Back-End seinen eigenen Schreibvorgang durchführt)
pgsql.statsbgwriter.buffers_checkpoint	Stellt Metriken bereit, die sich auf die Anzahl der während Prüfpunkten geschriebenen Puffer beziehen
pgsql.statsbgwriter.buffers_clean	Stellt Metriken bereit, die sich auf die Anzahl der vom Hintergrund-Writer geschriebenen Puffer beziehen
pgsql.statsbgwriter.checkpoint_sync_time	Stellt Metriken bereit, die sich auf die Gesamtzeit in Millisekunden beziehen, die für den Teil der Prüfpunktverarbeitung aufgewendet wurde, bei dem Dateien mit dem Laufwerk synchronisiert werden
pgsql.statsbgwriter.checkpoint_write_time	Stellt Metriken bereit, die sich auf die Gesamtzeit in Millisekunden beziehen, die für den Teil der Prüfpunktverarbeitung aufgewendet wurde, bei dem Dateien auf das Laufwerk geschrieben werden
pgsql.statsbgwriter.checkpoints_req (Empfohlene Metrik)	Stellt Metriken bereit, die sich auf die Anzahl der durchgeführten angeforderten Prüfpunkte beziehen
pgsql.statsbgwriter.checkpoints_timed (Empfohlene Metrik)	Stellt Metriken bereit, die sich auf die Anzahl der durchgeführten geplanten Prüfpunkte beziehen
pgsql.statsbgwriter.maxwritten_clean	Stellt Metriken bereit, die sich darauf beziehen, wie oft der Hintergrund-Writer einen Reinigungsscan angehalten hat, weil zu viele Puffer geschrieben wurden

postgresql.metric-statsdb-Metriken

Metrik	Beschreibung
pgsql.statsdb.blk_read_time (Empfohlene Metrik)	Stellt Metriken bereit, die sich auf die Zeit in Millisekunden beziehen, die für das Lesen von Datendateiblöcken durch Back-Ends in dieser Datenbank aufgewendet wurde
pgsql.statsdb.blk_write_time (Empfohlene Metrik)	Stellt Metriken bereit, die sich auf die Zeit in Millisekunden beziehen, die für das Schreiben von Datendateiblöcken durch Back-Ends in dieser Datenbank aufgewendet wurde
pgsql.statsdb.blks_hit (Empfohlene Metrik)	Stellt Metriken bereit, die sich darauf beziehen, wie oft Datenträgerblöcke im Puffer-Cache gefunden wurden, sodass kein Lesen erforderlich war. Dies umfasst nur

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

postgresql.metric-statsdb-Metriken (Fortsetzung)

Metrik	Beschreibung
	Treffer im PostgreSQL-Puffer-Cache, nicht den Dateisystem-Cache des Betriebssystems.
pgsql.statsdb.blks_read	Stellt Metriken bereit, die sich auf die Anzahl der in dieser Datenbank gelesenen Datenträgerblöcke beziehen
pgsql.statsdb.checksum_failures	Stellt Metriken bereit, die sich auf die Anzahl der in dieser Datenbank (oder in einem gemeinsam genutzten Objekt) erkannten Prüfsummenfehler für Datenseiten beziehen, oder 0, wenn Datenprüfsummen nicht aktiviert sind
pgsql.statsdb.conflicts	Stellt Metriken bereit, die sich auf die Anzahl der Abfragen beziehen, die aufgrund von Konflikten mit der Wiederherstellung in dieser Datenbank abgebrochen wurden. Konflikte treten nur auf Standby-Servern auf.
pgsql.statsdb.deadlocks (Empfohlene Metrik)	Stellt Metriken bereit, die sich auf die Anzahl der in dieser Datenbank erkannten Deadlocks beziehen
pgsql.statsdb.numbackends	Stellt Metriken bereit, die sich auf die Anzahl der aktuell mit dieser Datenbank verbundenen Back-Ends beziehen. Dies ist die einzige Spalte in dieser Ansicht, die einen Wert zurückgibt, der den aktuellen Status widerspiegelt. Alle anderen Spalten geben die kumulierten Werte seit dem letzten Zurücksetzen zurück.
pgsql.statsdb.temp_bytes	Stellt Metriken bereit, die sich auf die Gesamtmenge der Daten beziehen, die durch Abfragen in dieser Datenbank in temporäre Dateien geschrieben wurden. Alle temporären Dateien werden gezählt, unabhängig davon, warum die temporäre Datei erstellt wurde, und unabhängig von der Einstellung *log_temp_files*.
pgsql.statsdb.temp_files	Stellt Metriken bereit, die sich auf die Anzahl der temporären Dateien beziehen, die durch Abfragen in dieser Datenbank erstellt wurden. Alle temporären Dateien werden gezählt, unabhängig davon, warum die temporäre Datei erstellt wurde (wie zum Sortieren oder zur Hash-Generierung), und unabhängig von der Einstellung *log_temp_files*.
pgsql.statsdb.tup_deleted	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die durch Abfragen in dieser Datenbank gelöscht wurden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

postgresql.metric-statsdb-Metriken (Fortsetzung)

Metrik	Beschreibung
pgsql.statsdb.tup_fetched	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die durch Abfragen in dieser Datenbank abgerufen wurden
pgsql.statsdb.tup_inserted	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die durch Abfragen in dieser Datenbank eingefügt wurden
pgsql.statsdb.tup_returned	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die durch Abfragen in dieser Datenbank zurückgegeben wurden
pgsql.statsdb.tup_updated	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die durch Abfragen in dieser Datenbank aktualisiert wurden
pgsql.statsdb.xact_commit	Stellt Metriken bereit, die sich auf die Anzahl der Transaktionen in dieser Datenbank beziehen, für die ein Commit ausgeführt wurde
pgsql.statsdb.xact_rollback	Stellt Metriken bereit, die sich auf die Anzahl der Transaktionen in dieser Datenbank beziehen, für die ein Rollback ausgeführt wurde.

postgresql.metric-statsio-Metriken

Metrik	Beschreibung
pgsql.statsio.heap_blks_hit (Empfohlene Metrik)	Stellt Metriken im Zusammenhang mit der Anzahl von Puffertreffern in dieser Tabelle bereit
pgsql.statsio.heap_blks_read	Stellt Metriken bereit, die sich auf die Anzahl der in dieser Tabelle gelesenen Datenträgerblöcke beziehen
pgsql.statsio.idx_blks_hit	Stellt Metriken im Zusammenhang mit der Anzahl von Puffertreffern in allen Indizes dieser Tabelle bereit
pgsql.statsio.idx_blks_read	Stellt Metriken bereit, die sich auf die Anzahl der in allen Indizes dieser Tabelle gelesenen Datenträgerblöcke beziehen
pgsql.statsio.tidx_blks_hit	Stellt Metriken im Zusammenhang mit der Anzahl von Puffertreffern im TOAST-Tabellenindex (sofern vorhanden) dieser Tabelle bereit
pgsql.statsio.tidx_blks_read	Stellt Metriken bereit, die sich auf die Anzahl der im TOAST-Tabellenindex dieser Tabelle gelesenen Datenträgerblöcke beziehen
pgsql.statsio.toast_blks_hit	Stellt Metriken im Zusammenhang mit der Anzahl von Puffertreffern in der TOAST-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

postgresql.metric-statsio-Metriken (Fortsetzung)

Metrik	Beschreibung
	Tabelle (sofern vorhanden) dieser Tabelle bereit
pgsql.statsio.toast_blks_read	Stellt Metriken bereit, die sich auf die Anzahl der in der TOAST-Tabelle (falls vorhanden) dieser Tabelle gelesenen Datenträgerblöcke beziehen

postgresql.metric-statsio-Metriken

Metrik	Beschreibung
pgsql.statstable.idx_scan	Stellt Metriken im Zusammenhang mit der Anzahl von Index-Scans bereit, die für diese Tabelle initiiert wurden
pgsql.statstable.idx_tup_fetch	Stellt Metriken bereit, die sich auf die Anzahl der aktiven Zeilen beziehen, die durch Index-Scans abgerufen wurden
pgsql.statstable.n_dead_tup	Stellt Metriken im Zusammenhang mit der geschätzten Anzahl inaktiver Zeilen bereit
pgsql.statstable.n_live_tup	Stellt Metriken im Zusammenhang mit der geschätzten Anzahl aktiver Zeilen bereit
pgsql.statstable.n_tup_del	Stellt Metriken im Zusammenhang mit der Anzahl gelöschter Zeilen bereit
pgsql.statstable.n_tup_hot_upd	Stellt Metriken bereit, die sich auf die Anzahl der Zeilen beziehen, die im laufenden Betrieb aktualisiert wurden (wobei keine separate Indexaktualisierung erforderlich war)
pgsql.statstable.n_tup_ins	Stellt Metriken im Zusammenhang mit der Anzahl eingefügter Zeilen bereit
pgsql.statstable.n_tup_upd	Stellt Metriken im Zusammenhang mit der Anzahl aktualisierter Zeilen bereit
pgsql.statstable.seq_scan	Stellt Metriken im Zusammenhang mit der Anzahl von sequenziellen Scans bereit, die für diese Tabelle initiiert wurden
pgsql.statstable.seq_tup_read	Stellt Metriken bereit, die sich auf die Anzahl der aktiven Zeilen beziehen, die durch sequenzielle Scans abgerufen wurden

RabbitMQ – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für die RabbitMQ-Systemüberwachung. Sie müssen die RabbitMQ-Erkennung durchführen, bevor Sie die Prüfungen ausführen. RabbitMQ-Prüfungen sind nur in einer Windows-Umgebung verfügbar.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für RabbitMQ-Ereignisse

Typ	Prüfung	Beschreibung	Befehl
Event	check-rabbitmq-alive	Überprüft mithilfe der REST-API, ob der RabbitMQ-Server aktiv ist. Wenn der Server inaktiv ist, wird eine Warnung ausgelöst.	`check-rabbitmq-alive.rb --host {{.labels.params_host}} --port {{.labels.params_port}} -v {{.labels.params_vhost}}`
Event	check-rabbitmq-cluster-health	Überprüft, ob die Clusterknoten des RabbitMQ-Servers ausgeführt werden. Wenn die Knoten inaktiv sind, wird eine Warnung ausgelöst.	`check-rabbitmq-cluster-health.rb --host {{.labels.params_host}} --port {{.labels.params_port}}`
Event	check-rabbitmq-consumers	Überprüft die Anzahl der Verbraucher auf dem RabbitMQ-Server und löst eine Warnung basierend auf dem konfigurierten Schwellenwert aus.	`check-rabbitmq-consumers.rb {{if .labels.params_warn}} --warn {{.labels.params_warn}} {{end}} {{if .labels.params_critical}} --critical {{.labels.params_critical}} {{end}} --host {{.labels.params_host}} --port {{.labels.params_port}}`
Event	check-rabbitmq-messages	Überprüft die Gesamtanzahl der Nachrichten in der Warteschlange auf dem RabbitMQ-Server und löst eine Warnung basierend auf dem Schwellenwert aus.	`check-rabbitmq-messages.rb --critical {{.labels.params_critical}} --port {{.labels.params_port}} --warn {{.labels.params_warn}} --host {{.labels.params_host}}`
Event	check-rabbitmq-network-partitions	Überprüft, ob die RabbitMQ-Netzwerkpartitionierung aufgetreten ist, und löst eine Warnung basierend auf dem Schwellenwert aus.	check-rabbitmq-network-partitions.rb --host {{.labels.params_host}} --port {{.labels.params_port}}
Event	check-rabbitmq-node-health	Überprüft, ob der RabbitMQ-Serverknoten den Status der Ausführung aufweist.	`check-rabbitmq-node-health.rb --host {{.labels.params_host}}`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für RabbitMQ-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
			{{if .labels.params_watchalarms}} --alarms {{.labels.params_watchalarms}} {{end}} {{if .labels.params_socketwarn}} --swarn {{.labels.params_socketwarn}} {{end}} {{if .labels.params_memcrit}} --mcrit {{.labels.params_memcrit}} {{end}} {{if .labels.params_fdcrit}} --fcrit {{.labels.params_fdcrit}} {{end}} {{if .labels.params_socketcrit}} --scrit {{.labels.params_socketcrit}} {{end}} --port {{.labels.params_port}} {{if .labels.params_memwarn}} --mwarn {{.labels.params_memwarn}} {{end}} {{if .labels.params_fdwarn}} --fwarn {{.labels.params_fdwarn}} {{end}}
Event	check-rabbitmq-node-usage	Überprüft die Nutzung des RabbitMQ-Serverknotens und zeigt sie an.	check-rabbitmq-node-usage.rb {{if .labels.params_procwarn}} --pwarn {{.labels.params_procwarn}}

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für RabbitMQ-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
			{{end}} --port {{.labels.params_port}} {{if .labels.params_socketwarn}} --swarn {{.labels.params_socketwarn}} {{end}} --type {{.labels.params_type}} {{if .labels.params_diskcrit}} --dcrit {{.labels.params_diskcrit}} {{end}} {{if .labels.params_fdcrit}} --fcrit {{.labels.params_fdcrit}} {{end}} {{if .labels.params_proccrit}} --pcrit {{.labels.params_proccrit}} {{end}} {{if .labels.params_diskwarn}} --dwarn {{.labels.params_diskwarn}} {{end}} {{if .labels.params_socketcrit}} --scrit {{.labels.params_socketcrit}} {{end}} --host {{.labels.params_host}} {{if .labels.params_memcrit}} --mcrit {{.labels.params_memcrit}} {{end}} {{if .labels.params_fdwarn}} --fwarn {{.labels.param

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für RabbitMQ-Ereignisse (Fortsetzung)

Typ	Prüfung	Beschreibung	Befehl
			`s_fdwarn}} {{end}} {{if .labels.params_memwarn}} mwarn {{.labels.params_memwarn}} {{end}}`
Event	check-rabbitmq-queue-drain-time	Überprüft die Zeit, die jede Warteschlange auf dem RabbitMQ-Server zum Leeren benötigt, basierend auf der aktuellen Nachrichtenausgangsr Wenn eine Warteschlange beispielsweise 1.000 Nachrichten enthält, aber nur 1 Nachricht pro Sekunde die Warteschlange verlässt, wird eine Warnung generiert, da die standardmäßig auf 360 Sekunden festgelegte Warnstufe „kritisch“ überschritten wurde.	`check-rabbitmq-queue-drain-time.rb --host {{.labels.params_host}} --port {{.labels.params_port}} --warn {{.labels.params_warn}} --critical {{.labels.params_critical}}`
Event	check-rabbitmq-queues-synchronised	Überprüft, ob alle gespiegelten Warteschlangen mit sekundären Warteschlangen synchronisiert sind.	`check-rabbitmq-queues-synchronised.rb --host {{.labels.params_host}} --port {{.labels.params_port}}`
Event	check-rabbitmq-stomp-alive	Überprüft, ob der RabbitMQ-Server aktiv ist und auf STOMP reagiert.	`check-rabbitmq-stomp-alive.rb --host {{.labels.params_host}} --queue {{.labels.params_queue}} --port {{.labels.params_port}}`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für RabbitMQ-Metriken

Typ	Prüfung	Beschreibung	Befehl
Metrik	metrics-rabbitmq-overview	Stellt RabbitMQ-Übersichtsstatistiken bereit.	`metrics-rabbitmq-overview.rb --port {{.labels.params_port}} --host {{.labels.params_host}}`
Metrik	metrics-rabbitmq-queue	Stellt RabbitMQ-Metriken pro Warteschlange bereit.	`metrics-rabbitmq-queue.rb --port {{.labels.params_port}} --host {{.labels.params_host}} {{if .labels.params_vhost}} --vhost {{.labels.params_vhost}} {{end}}`

RabbitMQ-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von RabbitMQ-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

metrics-rabbitmq-overview – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
rabbitmq.queue_totals.messages.count		count	Stellt Metriken zur Gesamtanzahl der Nachrichten bereit (bereit und nicht bestätigt).
rabbitmq.queue_totals.messages.rate (empfohlene Metrik)		Rate/Sek.	Stellt Metriken zur Gesamtanzahl der Nachrichten bereit (bereit und nicht bestätigt)
rabbitmq.queue_totals.messages_ready.count		count	Stellt Metriken zur Anzahl der zur Zustellung bereiten Nachrichten bereit.
rabbitmq.queue_totals.messages_ready.rate		Rate/Sek.	Stellt Metriken zur Anzahl der zur Zustellung bereiten Nachrichten bereit.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-rabbitmq-overview – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
rabbitmq.queue_totals.messages_unacknowledged.count		count	Stellt Metriken zur Anzahl der nicht bestätigten Nachrichten bereit.
rabbitmq.queue_totals.messages_unacknowledged.rate		Rate/Sek.	Stellt Metriken zur Anzahl der nicht bestätigten Nachrichten bereit.
rabbitmq.message_stats.deliver_get.count		count	Stellt Metriken zu Nachrichten bereit, die kürzlich an Verbraucher gesendet wurden.
rabbitmq.message_stats.deliver_get.rate (empfohlene Metrik)		Rate/Sek.	Stellt Metriken zu Nachrichten bereit, die kürzlich an Verbraucher gesendet wurden.
rabbitmq.message_stats.deliver_no_ack.count		count	Stellt Metriken zu nicht bestätigten Nachrichten bereit, die kürzlich an Verbraucher gesendet wurden.
rabbitmq.message_stats.deliver_no_ack.rate		Rate/Sek.	Stellt Metriken zu nicht bestätigten Nachrichten bereit, die kürzlich an Verbraucher gesendet wurden.
rabbitmq.message_stats.publish.count		count	Stellt Metriken zu kürzlich veröffentlichten Nachrichten bereit.
rabbitmq.message_stats.publish.rate		Rate/Sek.	Stellt Metriken zu den kürzlich veröffentlichten Nachrichten bereit.
rabbitmq.object_totals.channels.count		count	Stellt Metriken zur Gesamtanzahl der Kanäle bereit.
rabbitmq.object_totals.connections.count (empfohlene Metrik)		count	Stellt Metriken zur Gesamtanzahl der Verbindungen bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-rabbitmq-overview – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
rabbitmq.object_totals.consumers.count (empfohlene Metrik)		count	Stellt Metriken zur Gesamtanzahl der Verbraucher bereit.
rabbitmq.object_totals.exchanges.count		count	Stellt Metriken zur Gesamtanzahl der Austauschvorgänge bereit.
rabbitmq.object_totals.queues.count (empfohlene Metrik)		count	Stellt Metriken zur Gesamtanzahl der Warteschlangen bereit.

metrics-rabbitmq-queue – Metriken

rabbitmq.queue.{{QueueName}}.avg_egress_rate (empfohlene Metrik)	Abfragename	count	Stellt warteschlangenspezifische Metriken zur Rate bereit, mit der nicht bestätigte Nachrichtendatensätze in den Arbeitsspeicher für die angegebene Warteschlange gelangen.
rabbitmq.queue.{{QueueName}}.consumers	Abfragename	count	Stellt warteschlangenspezifische Metriken zur Gesamtanzahl der Verbraucher für die angegebene Warteschlange bereit.
rabbitmq.queue.{{QueueName}}.messages	Abfragename	count	Stellt warteschlangenspezifische Metriken zur Gesamtanzahl der Nachrichten in der angegebenen Warteschlange bereit.
rabbitmq.queue.{{QueueName}}.drain_time	Abfragename	count	Stellt warteschlangenspezifische Metriken zur Nachrichtenabflusszeit

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

metrics-rabbitmq-queue – Metriken (Fortsetzung)

			für die angegebene Warteschlange bereit.

Standardprüfungen und -richtlinien für die URL-Überwachung

Agent Client Collector stellt Richtlinien für die URL-Überwachung bereit. Policen enthalten eingebettete Prüfungen.

Die URL-Überwachung verwendet die Standardrichtlinien für HTTP-Einstiegspunkte. Details finden Sie unter HTTP – Standardprüfungen und Richtlinien.

Varnish – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für die Varnish-Systemüberwachung.

Richtlinie für Varnish-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe

Metrik	app.varnish.metrics-varnish	Sammelt Varnish-Metriken vom Host.	`linuxchecks metrics-varnish (Optionen)`
			wobei:
			• -t = fields – Liste der erforderlichen Metriken, durch Kommas getrennt, zwischen ""
			• -v = varnishname – Die Varnish-Instanz, aus der Daten abgerufen werden sollen.
				`hostname.MAIN_sess_conn 175 1649420020`
				`hostname.MAIN_sess_drop 0 1649420020`
				`hostname.MAIN_client_req 173 1649420020`
				`hostname.MAIN_cache_hit 0 1649420020`
				`hostname.MAIN_cache_hitpass 0 1649420020`
				`hostname.MAIN_cache_miss 167 1649420020`
				`hostname.MAIN_backend_conn 0 1649420020`
				`hostname.MAIN_backend_unhealthy 0 1649420020`
				`hostname.MAIN_backend_b`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Varnish-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
				usy 0 1649420020 hostname.MAIN_backend_fail 171 1649420020 hostname.MAIN_backend_reuse 0 1649420020 hostname.MAIN_backend_recycle 0 1649420020 hostname.MAIN_threads 200 1649420020 hostname.MAIN_threads_limited 0 1649420020 hostname.MAIN_threads_created 200 1649420020 hostname.MAIN_threads_failed 0 1649420020 hostname.MAIN_thread_queue_len 0 1649420020 hostname.MAIN_sess_queued 0 1649420020 hostname.MAIN_n_expired 167 1649420020 hostname.MAIN_n_lru_nuked 0 1649420020 hostname.MAIN_backend_req 0 1649420020

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Varnish-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Varnish-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Varnish-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
MAIN_sess_conn (empfohlene Metrik)		count	Kumulative Anzahl der akzeptierten Clientverbindungen nach Varnish-Cache.
MAIN_sess_drop (empfohlene Metrik)		count	Anzahl der Verbindungen, die aufgrund einer vollen Warteschlange getrennt wurden.
MAIN_client_req (empfohlene Metrik)		count	Kumulative Anzahl der empfangenen Clientanforderungen. Wird schrittweise erhöht, nachdem eine Anforderung empfangen wurde, aber bevor eine Antwort von Varnish erfolgt.
MAIN_cache_hit		count	Kumulative Anzahl, die angibt, wie oft eine Datei aus dem Cache von Varnish bereitgestellt wurde.
MAIN_cache_hitpass		count	Kumulative Anzahl von Treffern für eine Datei vom Typ „pass“.
MAIN_cache_miss		count	Kumulative Anzahl, die angibt, wie oft eine Datei angefordert wurde, sich aber nicht im Cache befand und daher vom Back-End angefordert wurde.
MAIN_backend_conn		count	Kumulative Anzahl erfolgreicher TCP-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Varnish-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Verbindungen mit dem Back-End.
MAIN_backend_unhealthy (empfohlene Metrik)		count	Kumulative Anzahl der Back-End-Verbindungen, bei denen nicht versucht wurde, sie herzustellen, da das Back-End als fehlerhaft markiert wurde.
MAIN_backend_busy		count	Kumulative Anzahl der Fälle, in denen die maximale Anzahl von Verbindungen mit dem Back-End erreicht wurde.
MAIN_backend_fail (empfohlene Metrik)		count	Kumulative Anzahl der fehlgeschlagenen Verbindungen mit dem Back-End.
MAIN_backend_reuse (empfohlene Metrik)		count	Kumulative Anzahl der Verbindungen, die aus dem Keep Alive-Pool wiederverwendet wurden.
MAIN_backend_recycle		count	Kumulative Anzahl der aktuellen Back-End-Verbindungen, die in einen Pool von Keep Alive-Verbindungen zurückversetzt und noch nicht verwendet wurden.
MAIN_threads (empfohlene Metrik)		count	Anzahl der Threads in allen Pools.
MAIN_threads_limited		count	Anzahl, die angibt, wie oft ein Thread erstellt werden musste, aber nicht konnte, weil die für varnishd konfigurierte Kapazität für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Varnish-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			neue Threads ausgeschöpft wurde.
MAIN_threads_created		count	Anzahl der Erstellungen eines Threads.
MAIN_threads_failed (empfohlene Metrik)		count	Anzahl der erfolglosen Versuche von Varnish, einen Thread zu erstellen.
MAIN_thread_queue_len		count	Aktuelle Warteschlangenlänge: Anzahl der Anforderungen, die im Worker Thread darauf warten, verfügbar zu werden.
MAIN_sess_queued		count	Anzahl, die angibt, wie oft in Varnish keine Threads mehr vorhanden waren und eine Anforderung in die Warteschlange gestellt werden musste.
MAIN_n_expired (empfohlene Metrik)		count	Kumulative Anzahl abgelaufener Objekte, z. B. aufgrund von TTL.
MAIN_n_lru_nuked (empfohlene Metrik)		count	Least Recently Used Nuked Objects (Am längsten nicht verwendete entfernte Objekte): Kumulative Anzahl der zwischengespeicherten Objekte, die von Varnish aufgrund von Platzmangel aus dem Cache entfernt wurden.
MAIN_backend_req (empfohlene Metrik)		count	Anzahl der Anforderungen an das Back-End.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vSphere – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für die vSphere-Systemüberwachung.

Richtlinie für Metriken für virtuelle vSphere-Maschinen

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
Metrik	vsphere.metric-VirtualMachine	Ruft Metriken für eine virtuelle vSphere-Maschine ab. Muss einen Proxy-Agent verwenden.	`commonchecks metric-vsphere -H hostname -R VirtualMachine -v vm_id -r true -i 20` wobei: • -H = hostname – Instanz-Hostname • -i = intervalId – 20 für Echtzeitmetriken; 300 für 5 Minuten ältere zusammengefasste Metriken (Standardwert: 300) • -r = resourceLevelMetric – Zum Aktivieren von Metriken auf Ressourcenebene (Standardwert = false)	`vsphere.VirtualMachine.disk 8 1654755994`

Richtlinie für vSphere-Datastore-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
Metrik	vSphere.metric-Datastore	Ruft Metriken für vSphere-Datastore ab. Muss einen Proxy-Agent verwenden.	`commonchecks metric-vsphere -H hostname -R Datastore -v vm_id -r` wobei:	`vsphere.Datastore.disk.capa 21474836480 1655182836`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für vSphere-Datastore-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
			• -H = hostname – Instanz-Hostname • -r = resourceLevelMetric – Zum Aktivieren von Metriken auf Ressourcenebene (Standardwert = false)	

Richtlinie für vSphere-Datencenter-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe

Metrik	vsphere.metric-Datacenter	Ruft Metriken für das vSphere-Datencenter ab.	`commonchecks metric-vsphere -H hostname -R Datacenter -v vm_id -r`
			wobei:
			• -H = hostname – Instanz-Hostname
			• -r = resourceLevelMet Zum Aktivieren von Metriken auf Ressourcenebene (Standardwert = false)
				`vsphere.Datacenter.vmop.numChangeDS.latest.total 217 1655194924`
				`vsphere.Datacenter.vmop.numChangeHost.latest.total 1373 1655194924`
				`vsphere.Datacenter.vmop.numChangeHostDS.latest.total 9 1655194924`
				`vsphere.Datacenter.vmop.numClone.latest.total 192 1655194924`

Richtlinie für vSphere ESX-Server-Metriken

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
Metrik	vsphere.metric-ESX_Server	Ruft Metriken für vSphere ESX-Server oder -Hostsystem	`commonchecks metric-vsphere -H hostname -R`	`vsphere.HostSystem.net.broadcastRx.summation.to`

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für vSphere ESX-Server-Metriken (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung	Ausgabe
		ab. Muss einen Proxy-Agent verwenden.	`HostSystem -v vm_id -r` wobei: • -H = hostname – Instanz-Hostname • -r = resourceLevelMet Zum Aktivieren von Metriken auf Ressourcenebene (Standardwert = false)	`tal 63885 1655198166 vsphere.HostSystem.net.broadcastTx.summation.total 196 1655198166 vsphere.HostSystem.net.bytesRx.average.total 5924 1655198166`

vSphere-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von vSphere-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

vsphere.metric-VirtualMachine – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
net.broadcastRx.summation	Netzwerkadapter	Pakete	Anzahl der empfangenen Broadcast-Pakete.
net.broadcastTx.summation	Netzwerkadapter	Pakete	Anzahl der übertragenen Broadcast-Pakete.
net.bytesRx.average	Netzwerkadapter	KiB	Durchschnittliche Menge der pro Sekunde empfangenen Daten.
net.bytesTx.average	Netzwerkadapter	KiB	Durchschnittliche Menge der pro Sekunde übertragenen Daten.
net.droppedRx.summation	Netzwerkadapter	Pakete	Anzahl der verworfenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			empfangenen Pakete.
net.droppedTx.summation	Netzwerkadapter	Pakete	Anzahl der verworfenen übertragenen Pakete.
net.multicastRx.summation	Netzwerkadapter	Pakete	Anzahl der empfangenen Multicast-Pakete.
net.multicastTx.summation	Netzwerkadapter	Pakete	Anzahl der übertragenen Multicast-Pakete.
net.packetsRx.summation	Netzwerkadapter	Pakete	Anzahl der empfangenen Pakete.
net.packetsTx.summation	Netzwerkadapter	Pakete	Anzahl der übertragenen Pakete.
net.received.average	Netzwerkadapter	KiB	Durchschnittliche Rate, mit der Daten während des Intervalls empfangen wurden. Dies stellt die Bandbreite des Netzwerks dar.
net.transmitted.average	Netzwerkadapter	KiB	Durchschnittliche Rate, mit der Daten während des Intervalls übertragen wurden. Dies stellt die Bandbreite des Netzwerks dar.
net.usage.average (empfohlene Metrik)	Netzwerkadapter	KiB	Netzwerkauslastung (kombinierte Übertragungs- und Empfangsraten).
disk.maxTotalLatency.latest (empfohlene Metrik)	Laufwerk	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Festplatten.
disk.read.average	Laufwerk	KiB	Durchschnittliche Anzahl der pro Sekunde von der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Festplatte gelesenen Kilobytes.
disk.usage.average (empfohlene Metrik)	Laufwerk	KiB	Aggregierte Festplatten-E/A-Rate.
disk.usage.maximum	Laufwerk	KiB	Maximale Festplatten-E/A-Rate.
disk.usage.minimum	Laufwerk	KiB	Minimale Festplatten-E/A-Rate.
disk.write.average	Laufwerk	KiB	Durchschnittliche Anzahl der pro Sekunde auf die Festplatte geschriebenen Kilobytes.
cpu.costop.summation	cpu-core	Millisekunde	Zeit, zu der die virtuelle Maschine zur Ausführung bereit ist, aber aufgrund von Co-Scheduling-Einschränkungen nicht ausgeführt werden kann.
cpu.demand.average	cpu-core	Megahertz	Menge der CPU-Ressourcen, die von einer virtuellen Maschine verwendet würde, wenn es keinen CPU-Konflikt oder kein CPU-Limit gäbe.
cpu.demandEntitlementRatio.latest	cpu-core	Prozent	Verhältnis von CPU-Ressourcenberechtigung zu CPU-Bedarf.
cpu.entitlement.latest	cpu-core	Megahertz	Vom ESXi-Planer bereitgestellte CPU-Ressourcen.
cpu.idle.summation	cpu-core	Millisekunde	Gesamtzeit, die die CPU im Leerlauf verbracht hat.
cpu.latency.average	cpu-core	Prozent	Prozentsatz der Zeit, während der die virtuelle Maschine nicht ausgeführt werden kann, da sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			um Zugriff auf die physische(n) CPU(s) konkurriert.
cpu.maxlimited.summation	cpu-core	Millisekunde	Zeit, zu der die virtuelle Maschine zur Ausführung bereit ist, aber nicht ausgeführt wird, da der festgelegte Höchstwert des CPU-Limits erreicht ist.
cpu.overlap.summation	cpu-core	Millisekunde	Zeit, zu der die virtuelle Maschine unterbrochen wurde, damit von ihr Systemservices für sich selbst oder für andere virtuelle Maschinen ausgeführt werden konnten.
cpu.readiness.average	cpu-core	Prozent	Prozentsatz der Zeit, während der die virtuelle Maschine bereit war, die Ausführung auf der physischen CPU jedoch nicht geplant werden konnte.
cpu.ready.summation	cpu-core	Millisekunde	CPU-Zeit (in Millisekunden) im Status „Bereit“.
cpu.run.summation	cpu-core	Millisekunde	Zeit, zu der die Ausführung der virtuellen Maschine geplant ist.
cpu.swapwait.summation	cpu-core	Millisekunde	CPU-Zeit, während der darauf gewartet wird, dass auf die Festplatte ausgelagerte Prozesse zur Ausführung in den Arbeitsspeicher abgerufen werden (Swap-in).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.system.summation	cpu-core	Millisekunde	Zeit, die für Systemprozesse auf jeder virtuellen CPU in der virtuellen Maschine aufgewendet wird.
cpu.usage.average (empfohlene Metrik)	cpu-core	Prozent	Prozentsatz der verwendeten CPU-Kapazität.
cpu.usagemhz.average	cpu-core	Megahertz	CPU-Auslastung, gemessen in Megahertz.
cpu.used.summation	cpu-core	Millisekunde	Zeit, die der virtuellen Maschine zugerechnet wird. Wenn ein Systemservice für diese virtuelle Maschine ausgeführt wird, sollte die von diesem Service aufgewendete Zeit (abgebildet durch cpu.system) dieser virtuellen Maschine in Rechnung gestellt werden. Wenn nicht, sollte die aufgewendete Zeit (abgebildet durch cpu.overlap) nicht dieser virtuellen Maschine berechnet werden.
cpu.wait.summation (empfohlene Metrik)	cpu-core	Millisekunde	Gesamte CPU-Zeit im Wartestatus. Die Gesamtwartezeit umfasst die Zeit, die in den Status „CPU-Leerlauf“, „CPU-Swap-Wartezeit“ und „CPU-E/A-Wartezeit“ verbracht wurde.
cpu.usage.vcpus.average	cpu-core	Prozent	Prozentsatz der verwendeten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Kapazität virtueller CPUs.
cpu.utilization.average	cpu-core	Prozent	Prozentsatz der verwendeten CPU-Kapazität.
mem.active.average	memory	KiB	Aktiv genutzte Arbeitsspeichermenge, die von VMkernel basierend auf kürzlich bearbeiteten Arbeitsspeicherseiten geschätzt wird.
mem.activewrite.average	memory	KiB	Geschätzte Menge des Arbeitsspeichers, in den von der virtuellen Maschine aktiv geschrieben wird.
mem.compressed.average	memory	KiB	Arbeitsspeichermenge (in Kilobyte), die komprimiert wurde.
mem.compressionRate.average	memory	KiB	Rate der Arbeitsspeicherkomprimierung für die virtuelle Maschine.
mem.consumed.average	memory	KiB	Menge des physischen Hostarbeitsspeichers, der von einer virtuellen Maschine, einem Host oder einem Cluster verbraucht wird.
mem.decompressionRate.average	memory	KiB	Rate der Arbeitsspeicherdekomprimierung für die virtuelle Maschine.
mem.entitlement.average	memory	KiB	Menge des physischen Hostarbeitsspeichers, die die virtuelle Maschine beanspruchen kann, wie vom ESX Scheduler festgelegt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mem.granted.average	memory	KiB	Menge des physischen Hostarbeitsspeichers oder des physischen Arbeitsspeichers, die einer virtuellen Maschine oder einem Host zugeordnet ist.
mem.latency.average	memory	KiB	Prozentsatz der Zeit, während der die virtuelle Maschine auf den Zugriff auf den ausgelagerten oder komprimierten Arbeitsspeicher wartet.
mem.llSwapInRate.average	memory	KiB	Rate, mit der Arbeitsspeicher vom Host-Cache in den aktiven Arbeitsspeicher ausgelagert wird.
mem.llSwapOutRate.average	memory	KiB	Rate, mit der Arbeitsspeicher vom aktiven Arbeitsspeicher in den Host-Cache ausgelagert wird.
mem.llSwapUsed.average	memory	KiB	Platz, der zum Zwischenspeichern ausgelagerter Seiten im Host-Cache verwendet wird.
mem.overhead.average	memory	KiB	Physischer Hostarbeitsspeicher, der von der Virtualisierungsinfrastruktur für die Ausführung der virtuellen Maschine verbraucht wird.
mem.overheadMax.average	memory	KiB	Physischer Hostarbeitsspeicher, der für die Verwendung als

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Virtualisierungs-Overhead für die virtuelle Maschine reserviert ist.
mem.overheadTouched.average	memory	KiB	Aktiv belegter Overhead des physischen Hostarbeitsspeichers (KB), der für die Verwendung als Virtualisierungs-Overhead für die virtuelle Maschine reserviert ist.
mem.shared.average	memory	KiB	Menge des physischen Gastarbeitsspeichers, der mit anderen virtuellen Maschinen gemeinsam genutzt wird, bezogen auf eine einzelne virtuelle Maschine oder auf alle eingeschalteten virtuellen Maschinen auf einem Host.
mem.usage.average (empfohlene Metrik)	memory	Prozent	Arbeitsspeichernutzung als Prozentsatz des insgesamt konfigurierten oder verfügbaren Arbeitsspeichers.
mem.vmmemctl.average	memory	KiB	Menge des Arbeitsspeichers, die vom Treiber für die Arbeitsspeichersteuerung der virtuellen Maschine zugeordnet wird.
mem.vmmemctltarget.average	memory	KiB	Von VMkernel festgelegter Zielwert für die Arbeitsspeicher-Balloon-Größe der virtuellen Maschine. In Verbindung mit der Metrik vmmemctl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			wird diese Metrik von VMkernel dazu verwendet, die Balloon-Größe für eine virtuelle Maschine zu erhöhen oder zu verringern.
mem.zero.average	memory	KiB	Arbeitsspeicher, der nur Nullen enthält. In der gemeinsamen Menge enthalten. Durch die transparente gemeinsame Seitennutzung (Transparent Page Sharing, TPS) können Speicherseiten, die nur Nullen enthalten, von virtuellen Maschinen, auf denen dasselbe Betriebssystem ausgeführt wird, gemeinsam genutzt werden.
power.energy.summation	Strom	Joule	Gesamte Energie (in Joule), die seit dem letzten Zurücksetzen der Statistik verbraucht wurde.
power.power.average	Strom	Watt	Aktueller Stromverbrauch.
sys.heartbeat.latest	System	Nummer	Anzahl der pro virtueller Maschine ausgegebenen Taktsignale (Heartbeats).
sys.osUptime.latest	System	seconds	Gesamtzeit (in Sekunden) seit dem letzten Start des Betriebssystems.
sys.uptime.latest	System	seconds	Insgesamt verstrichene Zeit

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			seit dem letzten Systemstart.
virtualDisk.read.average	virtuelle Festplatte	KiB	Durchschnittliche Anzahl der pro Sekunde von der virtuellen Festplatte gelesenen Kilobytes.
virtualDisk.write.average	virtuelle Festplatte	KiB	Durchschnittliche Anzahl der pro Sekunde auf die virtuelle Festplatte geschriebenen Kilobytes.
rescpu.actav1.latest	rescpu	Prozent	Durchschnittliche aktive Zeit der CPU während 1 Minute.
rescpu.actav15.latest	rescpu	Prozent	Durchschnittliche aktive Zeit der CPU während 15 Minuten.
rescpu.actav5.latest	rescpu	Prozent	Durchschnittliche aktive Zeit der CPU während 5 Minuten.
escpu.actpk1.latest	rescpu	Prozent	Aktive Spitzenzeit der CPU während 1 Minute.
rescpu.actpk15.latest	rescpu	Prozent	Aktive Spitzenzeit der CPU während 15 Minuten.
rescpu.actpk5.latest	rescpu	Prozent	Aktive Spitzenzeit der CPU während 5 Minuten.
rescpu.runav1.latest	rescpu	Prozent	Durchschnittliche Laufzeit der CPU während 1 Minute.
rescpu.runav15.latest	rescpu	Prozent	Durchschnittliche Laufzeit der CPU während 15 Minuten.
rescpu.runav5.latest	rescpu	Prozent	Durchschnittliche Laufzeit der CPU während 5 Minuten.
rescpu.runpk1.latest	rescpu	Prozent	Spitzenlaufzeit der CPU während 1 Minute.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-VirtualMachine – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
rescpu.runpk15.latest	rescpu	Prozent	Spitzenlaufzeit der CPU während 15 Minuten.
rescpu.runpk5.latest	rescpu	Prozent	Spitzenlaufzeit der CPU während 5 Minuten.
rescpu.sampleCount.latest	rescpu	Millisekunde	CPU-Abtastrate für Gruppe.
rescpu.samplePeriod.latest	rescpu	Millisekunde	CPU-Abtastzeitraum für Gruppe.

vsphere.metric-Datacenter – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmop.numChangeDS.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Datenspeicher-Änderungsvorgänge für ausgeschaltete und angehaltene virtuelle Maschinen.
vmop.numChangeHost.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Hoständerungsvorgänge für ausgeschaltete und angehaltene virtuelle Maschinen.
vmop.numChangeHostDS.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Host- und Datenspeicher-Änderungsvorgänge für ausgeschaltete und angehaltene virtuelle Maschinen.
vmop.numClone.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Klonvorgänge für die virtuelle Maschine.
vmop.numCreate.latest (empfohlene Metrik)	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Erstellungsvorgänge für die virtuelle Maschine.
vmop.numDeploy.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Vorlagenbereitstellungsvorgänge

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datacenter – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			für die virtuelle Maschine.
vmop.numDestroy.latest (empfohlene Metrik)	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Löschvorgänge für die virtuelle Maschine.
vmop.numPoweroff.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Ausschaltvorgänge für die virtuelle Maschine.
vmop.numPoweron.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Einschaltvorgänge für die virtuelle Maschine.
vmop.numRebootGuest.latest (empfohlene Metrik)	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Neustartvorgänge für den VM-Gast.
vmop.numReconfigure.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Neukonfigurationsvorgänge für die virtuelle Maschine.
vmop.numRegister.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Registrierungsvorgänge für die virtuelle Maschine.
vmop.numReset.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Vorgänge zum Zurücksetzen für die virtuelle Maschine.
vmop.numSVMotion.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Migrationen mit Storage vMotion (Datenspeicher-Änderungsvorgänge für eingeschaltete virtuelle Maschinen).
vmop.numShutdownGuest.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Vorgänge zum Herunterfahren für den VM-Gast.
vmop.numStandbyGuest.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Standby-Vorgänge für den VM-Gast.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datacenter – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
vmop.numSuspend.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Vorgänge zum Anhalten für die virtuelle Maschine.
vmop.numUnregister.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Vorgänge zur Aufhebung der Registrierung für die virtuelle Maschine.
vmop.numVMotion.latest (empfohlene Metrik)	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Migrationen mit vMotion (Hoständerungsvorgänge für eingeschaltete virtuelle Maschinen).
vmop.numXVMotion.latest	Leistungsindikatoren für VM-Vorgänge	Nummer	Anzahl der Host- und Datenspeicher-Änderungsvorgänge für eingeschaltete und angehaltene virtuelle Maschinen.

vsphere.metric-Datastore – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
datastore.busResets.summation	Datenspeicher	Nummer	Anzahl der ausgegebenen Befehle zum Zurücksetzen des SCSI-Busses.
datastore.commandsAborted.summation	Datenspeicher	Nummer	Anzahl der abgebrochenen SCSI-Befehle.
datastore.datastoreIops.average	Datenspeicher	Nummer	Aggregierte IOPS für Datenspeicher-E/A-Ressourcenverwaltung (Storage I/O Control).
datastore.datastoreMaxQueueDepth.latest	Datenspeicher	Nummer	Maximale Datenspeicher-Warteschlangentiefe für Datenspeicher-E/A-Ressourcenverwaltung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
datastore.datastoreNormalReadLatency.latest	Datenspeicher	Millisekunde	Normalisierte Leselatenz des Storage DRS-Datenspeichers.
datastore.datastoreNormalWriteLatency.latest	Datenspeicher	Millisekunde	Normalisierte Schreiblatenz des Storage DRS-Datenspeichers.
datastore.datastoreReadBytes.latest	Datenspeicher	Millisekunde	Gelesene Bytes des Storage DRS-Datenspeichers.
datastore.datastoreReadIops.latest	Datenspeicher	Nummer	Rate gelesener E/A-Vorgänge des Storage DRS-Datenspeichers.
datastore.datastoreReadMetric.latest	Datenspeicher	Nummer	Storage DRS-Datenspeichermetrik für das Lese-Workload-Modell.
datastore.datastoreReadOIO.latest	Datenspeicher	Nummer	Ausstehende Leseanforderungen des Storage DRS-Datenspeichers.
datastore.datastoreVMObservedLatency.latest	Datenspeicher	Mikrosekunden	Die durchschnittliche Latenz des Datenspeichers aus der Sicht von virtuellen Maschinen.
datastore.datastoreWriteBytes.latest	Datenspeicher	Millisekunde	Geschriebene Bytes des Storage DRS-Datenspeichers.
datastore.datastoreWriteIops.latest	Datenspeicher	Nummer	Rate geschriebener E/A-Vorgänge des Storage DRS-Datenspeichers.
datastore.datastoreWriteMetric.latest	Datenspeicher	Nummer	Storage DRS-Datenspeichermetrik für das Schreib-Workload-Modell.
datastore.datastoreWriteOIO.latest	Datenspeicher	Nummer	Ausstehende Schreibanforderungen des Storage DRS-Datenspeichers.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
datastore.maxTotalLatency.latest	Datenspeicher	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Datenspeicher.
datastore.numberReadAveraged.average	Datenspeicher	Nummer	Durchschnittliche Anzahl der pro Sekunde an den Datenspeicher ausgegebenen Lesebefehle.
datastore.numberWriteAveraged.average	Datenspeicher	Nummer	Durchschnittliche Anzahl der während des Erfassungsintervalls pro Sekunde an den Datenspeicher ausgegebenen Schreibbefehle.
datastore.read.average (empfohlene Metrik)	Datenspeicher	KiB	Rate des Lesens von Daten aus dem Datenspeicher.
datastore.siocActiveTimePercentage.average (empfohlene Metrik)	Datenspeicher	Prozent	Prozentsatz der Zeit, während der die Latenz des Datenspeichers aktiv von der Datenspeicher-E/A-Ressourcenverwaltung gesteuert wurde.
datastore.sizeNormalizedDatastoreLatency.average	Datenspeicher	Mikrosekunden	Größennormalisierte E/A-Latenz der Datenspeicher-E/A-Ressourcenverwaltung.
datastore.throughput.contention.average	Datenspeicher	Millisekunde	Durchschnittliche Zeit für einen E/A-Vorgang für den Datenspeicher oder die LUN für alle ESX-Hosts, die darauf zugreifen.
datastore.throughput.usage.average	Datenspeicher	KiB	Aktuelle Bandbreitennutzung für den Datenspeicher oder die LUN.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
datastore.totalReadLatency.average	Datenspeicher	Millisekunde	Durchschnittliche Zeitdauer für einen Lesevorgang aus dem Datenspeicher.
datastore.totalWriteLatency.average	Datenspeicher	Millisekunde	Durchschnittliche Zeitdauer für einen Schreibvorgang aus dem Datenspeicher.
datastore.unmapIOs.summation	Datenspeicher	Nummer	Anzahl der Vorgänge zum Aufheben von Zuordnungen.
datastore.unmapSize.summation	Datenspeicher	Nummer	Gesamtgröße des Aufhebens der Zuordnung.
datastore.write.average (empfohlene Metrik)	Datenspeicher	KiB	Rate des Schreibens von Daten in den Datenspeicher.
disk.busResets.summation	disk	Nummer	Anzahl der ausgegebenen Befehle zum Zurücksetzen des SCSI-Busses.
disk.capacity.latest	disk	KiB	Konfigurierte Größe des Datenspeichers.
disk.capacity.contention.average	disk	KiB	Ausmaß der Überbelegung der Speicherkapazität für die Entität, gemessen in Prozent.
disk.capacity.provisioned.average	disk	KiB	Bereitgestellte Größe der Entität.
disk.capacity.usage.average	disk	KiB	Menge der Speicherkapazität, die derzeit von oder in der Entität verbraucht wird.
disk.commands.summation	disk	Nummer	Anzahl der ausgegebenen SCSI-Befehle.
disk.commandsAborted.summation	disk	Nummer	Anzahl der abgebrochenen SCSI-Befehle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
disk.commandsAveraged.latest	disk	Nummer	Durchschnittliche Anzahl der pro Sekunde ausgegebenen SCSI-Befehle.
disk.deltaused.latest	disk	KiB	Speicher-Overhead einer virtuellen Maschine oder eines Datenspeichers aufgrund von Delta-Festplattensicherungen.
disk.deviceLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die zum vollständigen Ausführen eines SCSI-Befehls von einem physischen Gerät benötigt wird.
disk.deviceReadLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die es dauert, bis der Vorgang des Lesens von einem physischen Gerät abgeschlossen ist.
disk.deviceWriteLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die es dauert, bis der Vorgang des Schreibens von einem physischen Gerät abgeschlossen ist.
disk.kernelLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die von VMkernel für die Verarbeitung jedes SCSI-Befehls aufgewendet wird.
disk.kernelReadLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die von VMkernel für die Verarbeitung jedes SCSI-Lesebefehls aufgewendet wird.
disk.kernelWriteLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die von VMkernel für die Verarbeitung jedes

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			SCSI-Schreibbefehls aufgewendet wird.
disk.maxQueueDepth.average (empfohlene Metrik)	disk	Nummer	Maximale Warteschlangentiefe.
disk.maxTotalLatency.latest	disk	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Festplatten.
disk.numberRead.summation	disk	Nummer	Anzahl der Festplatten-Lesevorgänge während des Erfassungsintervalls.
disk.numberReadAveraged	disk.average	Nummer	Durchschnittliche Anzahl der pro Sekunde an den Datenspeicher ausgegebenen Lesebefehle.
disk.numberWrite.summation	disk	Nummer	Anzahl der Festplatten-Schreibvorgänge während der Erfassung.
disk.numberWriteAveraged	disk.average	Nummer	Durchschnittliche Anzahl der pro Sekunde an den Datenspeicher ausgegebenen Schreibbefehle.
disk.provisioned.latest	disk	KiB	Speichermenge, die für die Verwendung durch einen Datenspeicher oder eine virtuelle Maschine reserviert ist. Dateien im Datenspeicher und auf der virtuellen Maschine können auf diese Größe erweitert werden, jedoch nicht darüber hinaus.
disk.queueLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die in der VMkernel-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			Warteschlange (pro SCSI-Befehl) verbracht wird.
disk.queueReadLatency.average (empfohlene Metrik)	disk	Millisekunde	Durchschnittliche Zeit, die in der VMkernel-Warteschlange (pro SCSI-Lesebefehl) verbracht wird.
disk.queueWriteLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die in der VMkernel-Warteschlange (pro SCSI-Schreibbefehl) verbracht wird.
disk.read.average	disk	KiB	Durchschnittliche Anzahl der pro Sekunde von der Festplatte gelesenen Kilobytes.
disk.scsiReservationCnflctPct.average	disk	Nummer	Anzahl der SCSI-Reservierungskonflikte für die LUN als Prozentsatz der gesamten Befehle während des Erfassungsintervalls.
disk.scsiReservationConflicts.summation	disk	Nummer	Anzahl der SCSI-Reservierungskonflikte für die LUN während des Erfassungsintervalls.
disk.throughput.contention.average	disk	Millisekunde	Durchschnittliche Zeit für einen E/A-Vorgang für den Datenspeicher oder die LUN für alle ESX-Hosts, die darauf zugreifen.
disk.throughput.usage.average	disk	KiB	Aktuelle Bandbreitennutzung für den Datenspeicher oder die LUN.
disk.totalLatency.average (empfohlene Metrik)	disk	Millisekunde	Durchschnittliche Zeit, die während des Erfassungsintervalls

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			dafür benötigt wird, einen vom Gastbetriebssystem an die virtuelle Maschine ausgegebenen SCSI-Befehl zu verarbeiten.
disk.totalReadLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die dafür benötigt wird, einen vom Gastbetriebssystem an die virtuelle Maschine ausgegebenen SCSI-Lesebefehl zu verarbeiten.
disk.totalWriteLatency.average	disk	Millisekunde	Durchschnittliche Zeit, die dafür benötigt wird, einen vom Gastbetriebssystem an die virtuelle Maschine ausgegebenen SCSI-Schreibbefehl zu verarbeiten.
disk.unshared.latest	disk	KiB	Größe des Speicherplatzes, der ausschließlich einer virtuellen Maschine zugeordnet ist.
disk.usage.average (empfohlene Metrik)	disk	KiB	Aggregierte Festplatten-E/A-Rate.
disk.used.latest	disk	KiB	Tatsächlich von der virtuellen Maschine oder dem Datenspeicher verwendeter Speicherplatz. Kann kleiner sein als die zu einem bestimmten Zeitpunkt bereitgestellte Menge, je nachdem, ob die virtuelle Maschine ausgeschaltet ist, ob Snapshots

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-Datastore – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			erstellt wurden oder nicht, sowie in Abhängigkeit von anderen derartigen Faktoren.
disk.write.average	disk	KiB	Durchschnittliche Anzahl der pro Sekunde auf die Festplatte geschriebenen Kilobytes.

vsphere.metric-ESX_Server – Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
cpu.coreUtilization.average (empfohlene Metrik)	cpu-core	Prozent	CPU-Auslastung des entsprechenden Kerns (wenn Hyper-Threading aktiviert ist) als Prozentsatz.
cpu.reservedCapacity.average	cpu-core	Megahertz	CPU-Gesamtkapazität, die von virtuellen Maschinen reserviert wurde.
cpu.totalCapacity.average	cpu-core	Megahertz	CPU-Gesamtkapazität, die von virtuellen Maschinen reserviert wurde und für diese verfügbar ist.
datastore.maxTotalLatency.latest	datastore	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Datenspeicher.
hbr.hbrDiskReadLatency.average	hostbasierte Replikation	Millisekunde	Durchschnittliche Festplatten-Leselatenz.
hbr.hbrDiskStallLatency.average	hostbasierte Replikation	Millisekunde	Durchschnittliche Verzögerungslatenz der Festplatte.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-ESX_Server – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
hbr.hbrNetRx.average	hostbasierte Replikation	KiB	Durchschnittliche Menge der pro Sekunde empfangenen Daten.
hbr.hbrNetTx.average	hostbasierte Replikation	KiB	Durchschnittliche Menge der pro Sekunde übertragenen Daten.
hbr.hbrNumVms.average	hostbasierte Replikation	Nummer	Anzahl der eingeschalteten virtuellen Maschinen, die auf diesem Host ausgeführt werden und für die derzeit der hostbasierte Replikationsschutz aktiviert ist.
mem.heap.average	memory	KiB	Virtueller VMkernel-Adressraum für den VMkernel-Haupt-Heap und zugehörige Daten.
mem.heapfree.average	memory	KiB	Freier Adressraum im VMkernel-Haupt-Heap. Variiert je nach Anzahl der physischen Geräte und Konfigurationsoptionen.
mem.llSwapIn.average	memory	KiB	Menge des per Swap-in geladenen Arbeitsspeichers aus dem Host-Cache.
mem.llSwapOut.average	memory	KiB	Menge des per Swap-out in den Host-Cache ausgelagerten Arbeitsspeichers.
mem.lowfreethreshold.average	memory	KiB	Schwellenwert für den freien physischen Hostarbeitsspeicher. Unterhalb dieses Schwellenwerts wird von ESX/ESXi mittels Ballooning

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-ESX_Server – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			(Zurückgewinnung und Wiederverwendung von ungenutztem Arbeitsspeicher) und Swapping (Auslagerung von Arbeitsspeicher) damit begonnen, Arbeitsspeicher von virtuellen Maschinen zurückzugewinnen.
mem.reservedCapacity.average	memory	MiB	Gesamtmenge der Arbeitsspeicherreservierung, die von eingeschalteten virtuellen Maschinen und vSphere-Diensten auf dem Host verwendet wird.
mem.sharedcommon.average	memory	KiB	Menge des VM-Arbeitsspeichers, der von allen eingeschalteten virtuellen Maschinen und vSphere-Diensten auf dem Host gemeinsam genutzt wird.
mem.state.latest	memory	KiB	Eine von vier Schwellenwertstufen, die den Prozentsatz des freien Arbeitsspeichers auf dem Host darstellen.
mem.swapin.average	memory	KiB	Menge des per Swap-in von der Festplatte geladenen Arbeitsspeichers.
mem.swapinRate.average	memory	KiB	Rate, mit der Arbeitsspeicher von der Festplatte in den aktiven Arbeitsspeicher geladen wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-ESX_Server – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mem.swapout.average	memory	KiB	Menge des per Swap-out auf die Festplatte ausgelagerten Arbeitsspeichers.
mem.swapoutRate.average	memory	KiB	Rate, mit der Arbeitsspeicher vom aktiven Arbeitsspeicher auf die Festplatte ausgelagert wird.
mem.swapused.average	memory	KiB	Für den Auslagerungsvorgang verwendete Arbeitsspeichermenge. Summe des ausgelagerten Arbeitsspeichers aller eingeschalteten virtuellen Maschinen und vSphere-Dienste auf dem Host.
mem.sysUsage.average	memory	KiB	Menge des physischen Hostarbeitsspeichers, der von VMkernel für Kernfunktionen verwendet wird, z. B. für Gerätetreiber und andere interne Zwecke. Enthält keinen Arbeitsspeicher, der von virtuellen Maschinen oder vSphere-Diensten verwendet wird.
mem.totalCapacity.average	memory	KiB	Gesamtmenge der Arbeitsspeicherreservierung, die von eingeschalteten virtuellen Maschinen und vSphere-Diensten auf dem Host verwendet wird und für diese verfügbar ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-ESX_Server – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mem.unreserved.average	memory	KiB	Menge des nicht reservierten Arbeitsspeichers. Arbeitsspeicherreservierung, die nicht von der Servicekonsole, von VMkernel, vSphere-Diensten und anderen eingeschalteten virtuellen Maschinen verwendet wird, benutzerdefinierte Arbeitsspeicherreservierungen und Overhead-Arbeitsspeicher.
mem.vmfs.pbc.capMissRatio.latest (empfohlene Metrik)	Memory	Prozent	Nachfolgender Durchschnitt des Verhältnisses von „Capacity Misses“ zu „Compulsory Misses“ für den VMFS-PB-Cache.
mem.vmfs.pbc.overhead.latest	memory	KiB	Menge des VMFS-Heaps, der vom VMFS-PB-Cache verwendet wird.
mem.vmfs.pbc.size.latest	memory	MiB	Platz, der zum Halten von VMFS-Zeigerblöcken im Arbeitsspeicher verwendet wird.
mem.vmfs.pbc.sizeMax.latest	memory	MiB	Maximale Größe, auf die der VMFS-Zeigerblock-Cache anwachsen kann.
mem.vmfs.pbc.workingSet.latest	Memory	TiB	Anzahl der Dateiblöcke, deren Adressen im VMFS-PB-Cache zwischengespeichert werden.
mem.vmfs.pbc.workingSetMax.latest	Memory	TiB	Maximale Anzahl der Dateiblöcke, deren Adressen im VMFS-PB-Cache

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vsphere.metric-ESX_Server – Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			zwischengespeichert werden.
net.errorsRx.summation (empfohlene Metrik)	Netzwerkadapter	Nummer	Anzahl der empfangenen Pakete mit Fehlern.
net.errorsTx.summation (empfohlene Metrik)	Netzwerkadapter	Nummer	Anzahl der übertragenen Pakete mit Fehlern.
net.unknownProtos.summation	Netzwerkadapter	KiB	Anzahl der empfangenen Frames mit unbekanntem Protokoll.
power.powerCap.average	System	Watt	Maximal zulässiger Stromverbrauch.
rescpu.maxLimited1.latest	rescpu	Prozent	Menge an CPU-Ressourcen über dem Grenzwert, die verweigert wurden; Durchschnitt über 1 Minute.
rescpu.maxLimited15.latest	rescpu	Prozent	Menge an CPU-Ressourcen über dem Grenzwert, die verweigert wurden; Durchschnitt über 15 Minuten.
rescpu.maxLimited5.latest	rescpu	Prozent	Menge an CPU-Ressourcen über dem Grenzwert, die verweigert wurden; Durchschnitt über 5 Minuten.
storageAdapter.maxTotalLatency (empfohlene Metrik)	Speicheradapter	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Speicheradapter.
storagePath.maxTotalLatency (empfohlene Metrik)	Speicherpfad	Millisekunde	Höchster Latenzwert für alle vom Host verwendeten Speicherpfade.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgenden Standardprüfungen und Richtlinien für Windows-Systemüberwachung.

Windows Ereignisüberwachungsprüfungen

Richtlinie für Windows-Betriebssystemereignisse

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
os.windows.check-event-log	Misst das Ereignisprotokoll Windows anhand von Parameterschwellenwerten und gibt ein Ereignis *CRITICAL|WARNING|OK* zurück.	Verwendung: • -w Warnung – Löst ein WARNUNGS-Ereignis aus, wenn die Anzahl der Ereignisprotokolle, die dem Muster entsprechen, über dem WARNUNGS-Parameterwert liegt, der im Prüfparameter angegeben ist. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn die dem Muster entsprechende Ereignisprotokollanzahl über dem im Prüfparameter angegebenen Parameterwert KRITISCH liegt. • -e Ereignisebene: Gibt den Schweregrad des Ereignisses an. Mögliche Werte: Information, Verbose, Kritisch, Warnung, Fehler. • -i: Eindeutige Ereignis-ID • -d – Die Dauer in Stunden, in der Ereignisse aus dem Ereignisprotokoll Windows abgerufen werden sollen.	Ereignisprotokoll prüfen OK: Das Ereignisprotokoll, das dem Muster entspricht, lautet<matched count>

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Anwendungsbeispiel: `Winchecks check-windows-event-log -w 5 -c 10 -e "Information" -l "Application" -d 24`	
os.windows.check-event-log-count	Misst das Ereignisprotokoll Windows anhand von Parameterschwellenwerten und gibt ein Ereignis KRITISCH\WARNUNG \OK zurück. Stellt Informationen zur Anzahl der Ereignisse bereit, die innerhalb eines angegebenen Zeitraums für eine einzelne Protokolldatei und eine einzelne ID aufgetreten sind. Gibt auch die Filter an, die zum Abrufen von Ereignissen für eine bestimmte einwertige Windows-Ereignisebene und einen bestimmten Anbieternamen angewendet werden sollen. Das Abrufen von Ereignissen aus mehreren Protokolldateien wird nicht unterstützt. Die Anzahl der Ereignisse wird ohne Details zu den einzelnen Ereignissen angegeben.	Verwendung: • -w Warnung – Löst ein WARNUNGS-Ereignis aus, wenn die Anzahl der Ereignisprotokolle, die dem Muster entsprechen, über dem WARNUNGS-Parameterwert liegt, der im Prüfparameter angegeben ist. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn die dem Muster entsprechende Ereignisprotokollanzahl über dem im Prüfparameter angegebenen Parameterwert KRITISCH liegt. • -l log_file – Die zu überwachende Protokolldatei. Der Name der Datei ist in doppelten Anführungszeichen angegeben. • -r regex_pattern: Das Muster des regulären Ausdrucks, das die Beschreibung im Ereignisprotokoll herausfiltert. In doppelten Anführungszeichen geschrieben.	Ereignisprotokoll prüfen OK: Das Ereignisprotokoll, das dem Muster entspricht, lautet<matched count>

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		• -e Ereignisebene: Gibt den Schweregrad des Ereignisses an. Mögliche Werte: Information, Verbose, Kritisch, Warnung, Fehler. • -i id: Eindeutige Ereignis-ID • -d duration_hour: Die Dauer in Stunden, in der Sie Ereignisse aus dem Ereignisprotokoll Windows abrufen möchten. Es können Dezimalstellen verwendet werden. beispielsweise 30 Minuten – 0,5. • -p provider_name: Quelle des Ereignisses, in doppelten Anführungszeichen angegeben. Anwendungsbeispiel: `Winchecks check-windows-event-log -w 5 -c 10 -e "Information" -l "Application" -d 24`	
os.windows.check-event-log-details	Sammelt und filtert Windows-Ereignisprotokolle basierend auf den Werten „duration_hour“, „event_log_level“ und „log_file“. Ruft Windows-Ereignisprotokolle gemäß den	Verwendung: • -d duration_hour: Dauer (in Stunden) ab dem aktuellen Zeitpunkt zum Filtern von Ereignissen (Standard: 24). • -e event_log_level: Filtert die Ereignisse basierend auf der	Ereignisprotokolldetails prüfen WARNUNG: Typ: Informationen, Kategorie: Anwendung, Computer: ws19-inc0061393.LOCAL.LAB, Event_ID: 1704, Nachricht: Sicherheitsrichtlinie in den

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	angegebenen Parametern ab und filtert sie. Gibt basierend auf dem angegebenen Schweregrad Details zu den Ereignissen mit dem Status KRITISCH, WARNUNG oder OK zurück.	Ereignisebene. Mögliche Werte: Information, Verbose, Kritisch, Warnung, Fehler. Mehrere Werte werden durch Kommas getrennt (Standard: Informationen). Beispiel: Information, Warnung • -i ID – Filtert Ereignisse basierend auf den angegebenen Ereignis-IDs. Bei mehreren IDs werden die Werte durch Kommas getrennt und in doppelte Anführungszeichen eingeschlossen. Beispiel: „1257, 1001“ • -l log_file: Gibt den Namen der Protokolldatei zum Filtern von Ereignissen an. Der Name der Datei ist in doppelten Anführungszeichen angegeben. Unterstützt das Erstellen von anwenderdefinierten Dateien, und mehrere Werte werden durch Kommas getrennt. (Standard: Anwendung). Beispiel: „Anwendung, System“ • -p provider_name: Der Name des	Gruppenrichtlinienobjekten wurde erfolgreich angewendet., Erstellt am: 14.10.2024 00:09:35 . Typ: Informationen, Kategorie: Anwendung, Computer: ws19-inc0061393.LOCAL.LAB, Event_ID: 16384, Nachricht: Neustart des Softwareschutzservice um 2124-09-20T06:25:44Z erfolgreich geplant. Grund: Regel-Engine, Erstellungszeit: 13.10.2024 23:25:44. Typ: Informationen, Kategorie: Anwendung, Computer: ws19-inc0061393.LOCAL.LAB, Event_ID: 16394, Nachricht: Offline-Migration auf niedrigerer Ebene erfolgreich., TimeCreated: 13.10.2024 11:24:19. Typ: Informationen, Kategorie: Anwendung, Computer: ws19-inc0061393.LOCAL.LAB, Event_ID: 8224, Nachricht: Der VSS-Service wird aufgrund einer Leerlauf-Zeitüberschreitung heruntergefahren., Erstellt: 13.10.2024 11:51:36.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Ereignisanbieters in doppelten Anführungszeichen. • -r regex_pattern: Filtert Ereignisse, indem die Ereignisnachricht mit dem angegebenen Muster abgeglichen wird. Wert muss in doppelte Anführungszeichen eingeschlossen werden. • -s servicenow_event_severity – Erstellt ein ServiceNow-Ereignis mit dem in diesem Parameter angegebenen Wert. Mögliche Werte: „Kritisch“, „Warnung“ und „OK“. Anwendungsbeispiel: `Winchecks check-windows-event-log-details -d 24 -l Anwendung -e Warnung -r "*" -s Warnung`	
os.windows.check-disk-name	Verwendet den Namen des Speicherlaufwerks als Eingabe und überprüft, ob das Laufwerk vorhanden ist. Gibt einen *CRITICAL|WARNING|OK*-Wert basierend auf dem angegebenen Parameter zurück.	Winchecks check-windows-disk-name<options> -d: Datenträgername (Standard = C) Anwendungsbeispiel: `Winchecks check-windows-disk-name -d C`	Windows-Prüfungen OK: Datenträgerspeicher C ist vorhanden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
os.windows.check-processor-queue-length	Misst die Länge der Prozessorwarteschlange anhand von Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -w Warnung – Löst ein WARNUNGS-Ereignis aus, wenn die Anzahl der Prozessorwarteschlangenlängen, die dem Muster entsprechen, über dem WARNUNGS-Parameterwert liegt, der im Prüfparameter angegeben ist. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn die Anzahl der Prozessorwarteschlangen, die dem Muster entsprechen, über dem im Prüfparameter angegebenen Parameterwert KRITISCH liegt. Verwendungsbeispiel: `winchecks check-windows-processor-queue-length -w 5 -c 10`	Processor Queue Length OK: The Processor Queue length is 0.00 (Länge der Prozessorwarteschlange OK: Die Länge der Prozessorwarteschlange beträgt 0,00.)
os.windows.check-system-cpu-load	Prüft die CPU-Last mithilfe von typeperf. Misst die CPU-Last anhand von konfigurierten Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -w Warnung – Löst ein WARNUNGS-Ereignis aus, wenn die Anzahl der CPU-Auslastungen, die dem Muster entspricht, über dem WARNUNGS-Parameterwert liegt, der im Prüfparameter angegeben ist. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn	CPU Load OK: The total CPU utilization is 26.92% (CPU-Last OK: Die CPU-Gesamtlast beträgt 26,92 %.)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		die Anzahl der CPU-Auslastungen, die dem Muster entspricht, über dem im Prüfparameter angegebenen Parameterwert KRITISCH liegt. Verwendungsbeispiel: `winchecks check-windows-cpu-load -w 85 -c 95`	
os.windows.check-system-disk	Misst den freien physischen Arbeitsspeicher anhand von Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -w Warnung – Löst ein WARNUNGS-Ereignis aus, wenn der Prozentsatz des Ereignisprotokolls, der dem Muster entspricht, über dem WARNUNGS-Parameterwert liegt, der im Prüfparameter angegeben ist. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn der Prozentsatz des Ereignisprotokolls, der dem Muster entspricht, über dem im Prüfparameter angegebenen Parameterwert KRITISCH liegt. Verwendungsbeispiel: `winchecks check-windows-disk -w 85 -c 95`	Disk Usage Check OK: The disk usage is % (Datenträgerverwendungsprüfung OK: Die Datenträgerverwendung beträgt %.)
os.windows.check-system-memory-percent	Erfasst die RAM-Auslastung. Misst die Arbeitsspeicherauslastung	Verwendung:	RAM Usage OK: The total memory utilization is 84% (RAM-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	anhand von konfigurierten Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	• -w Warnung – Löst ein WARNUNGS-Ereignis aus, wenn der Prozentsatz der Speicherauslastung, der dem Muster entspricht, über dem im Prüfparameter angegebenen WARNUNGS-Parameterwert liegt. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn der Prozentsatz der Arbeitsspeicherauslastung, der dem Muster entspricht, über dem im Prüfparameter angegebenen Parameterwert KRITISCH liegt. Verwendungsbeispiel: `winchecks check-windows-ram -w 85 -c 95`	Auslastung OK: Die Arbeitsspeicherauslastung insgesamt beträgt 84 %.)
os.windows.check-system-process	Laufende Prozesse werden zur Ermittlung laufender Prozesse abgefragt, die den angegebenen Argumenten entsprechen. (Muster, Name, Muster und Name. Mindestens ein Argument muss angegeben werden.) Misst die laufenden Prozesse anhand von konfigurierten Schwellenwerten und Filtern und gibt ein Ereignis vom Typ KRITISCH	Verwendung: • -n name – Name der ausführbaren Prozessdatei zur Überprüfung der Prozessausführung. • -p Muster – Muster (Unterzeichenfolge), nach dem in dem Befehl gesucht werden soll, der den Prozess aufgerufen hat. Erzeugt nur dann gültige Ergebnisse, wenn der Benutzer, der den Agent	Check Process OK (Prozess überprüfen OK): OK Found 1 matching running processes named explorer (OK 1 übereinstimmender laufender Prozess mit Namen explorer gefunden)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	\WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	ausführt, der Besitzer des abgefragten Prozesses ist und über Anzeigeberechtigungen für den abgefragten Prozess verfügt. • -w warnover – Löst einen Status vom Typ WARNUNG aus, wenn von der Abfrage mehr Prozesse zurückgegeben werden, als vom Argument angegeben sind. • -W warnunder – Löst einen Status vom Typ WARNUNG aus, wenn von der Abfrage weniger Prozesse zurückgegeben werden, als vom Argument angegeben sind. • -c critover – Löst ein Ereignis vom Typ KRITISCH aus, wenn von der Abfrage mehr Prozesse zurückgegeben werden, als vom Argument angegeben sind. • -C critunder – Löst ein Ereignis vom Typ KRITISCH aus, wenn von der Abfrage weniger Prozesse zurückgegeben werden, als vom Argument angegeben sind.	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Verwendungsbeispiel: `winchecks check-windows-processes -n explorer`	
os.windows.check-directory	Überprüft, ob ein Windows-Verzeichnis vorhanden ist.	Verwendung: -d --directory – Pfad zum entsprechenden Verzeichnis; verwenden Sie „\" für die Trennung. Verwendungsbeispiel: `winchecks check-windows-directory -d dir_path`	Check Directory OK: The directory 'C:/Users/Public' exists (Verzeichnis überprüfen OK: Das Verzeichnis 'C:/Users/Public' ist vorhanden.)
os.windows.check-pagefile	Erfasst die *Pagefile*-Belegung und vergleicht sie mit den Schwellenwerten für WARNUNG und KRITISCH.	Verwendung: • -w Warnung – Löst ein WARNUNGS-Ereignis aus, wenn die Nutzung *Pagefile* von über dem im Prüfparameter angegebenen WARNUNGS-Parameterwert liegt. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn die Nutzung *Pagefile* von über dem im Prüfparameter angegebenen Parameterwert KRITISCH liegt. Verwendungsbeispiel: `winchecks check-windows-pagefile -w 75 -c 85`	Check Windows Page File OK: Page file usage at 31.63% (Windows-Auslagerungsdateien überprüfen OK: Belegung der Auslagerungsdateien bei 31,63 %)
os.windows.check-free-physical-memory	Misst den freien physischen Arbeitsspeicher anhand von konfigurierten	Verwendung: • -w Warnung – Löst ein WARNUNGS-Ereignis aus, wenn	Freier physischer Speicher OK: Der freie physische Speicher beträgt 20,25 %.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	der freie physische Arbeitsspeicher unter dem WARNUNGS-Parameterwert liegt, der im Prüfparameter angegeben ist. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn der freie physische Arbeitsspeicher unter dem Parameterwert KRITISCH liegt, der im Prüfparameter angegeben ist. Verwendungsbeispiel: `winchecks check-windows-free-physical-memory -w 10 -c 5`	
os.windows.check-free-virtual-memory	Misst den freien virtuellen Arbeitsspeicher anhand von konfigurierten Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -w Warnung – Löst ein WARNUNG-Ereignis aus, wenn der freie virtuelle Speicher über dem im Prüfparameter angegebenen Parameterwert WARNUNG liegt. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn der freie virtuelle Arbeitsspeicher über dem im Prüfparameter angegebenen Parameterwert KRITISCH liegt. Anwendungsbeispiel: `Winchecks Check-Windows-Free-`	Freier virtueller Speicher OK: Der freie virtuelle Speicher beträgt 25,66 %

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		`Virtual-Memory -w 10 -c 5`	
os.windows.check-process-cpu	Misst „CPU-Auslastung Prozess“ anhand von konfigurierten Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -p processname – Prozessname zum Erfassen der CPU-Auslastung. • -w Warnung – Löst ein WARNUNGS-Ereignis aus, wenn die CPU-Auslastung über dem im Prüfparameter angegebenen WARNUNGS-Parameterwert liegt. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn die CPU-Auslastung über dem im Prüfparameter angegebenen Parameterwert „KRITISCH“ liegt. Nutzungsbeispiel: `Winchecks check-windows-process-cpu-p acc -c 95 -w 85`	Check Process CPU OK: Process CPU usage is 0.0000% (Prozess-CPU überprüfen OK: CPU-Auslastung Prozess beträgt 0,0000 %.)
os.windows.check-process-memory	Misst die Prozessspeicherauslastung anhand von Schwellenwerten und gibt ein Ereignis vom Typ KRITISCH \WARNUNG\OK gemäß den in den Begleitparametern angegebenen Schwellenwerten zurück.	Verwendung: • -p processname – Prozessname zum Erfassen der Speicherauslastung. • -w Warnung – Löst ein WARNUNGS-Ereignis aus, wenn die Auslastung des Prozessspeichers über dem im Prüfparameter angegebenen WARNUNGS-	Check Process Memory OK: Process Memory usage is 0.0149% (Prozessspeicher überprüfen OK: Die Prozessspeicherauslastung beträgt 0,0149 %.)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystemereignisse (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Parameterwert liegt. • -c kritisch – Löst ein KRITISCHES Ereignis aus, wenn die Auslastung des Prozessspeichers über dem im Prüfparameter angegebenen Parameterwert „KRITISCH“ liegt. Anwendungsbeispiel: `Winchecks check-windows-process-memory-p acc -c 95 -w 85`	
os.windows.check-user-account	Verwendet die Liste der Anwendernamen als Eingabe und überprüft, ob der Anwenderaccount aktiv ist. Gibt einen Wert KRITISCH \WARNUNG\OK zurück.	Winchecks check-windows-user-disabled (Optionen) -u: Kommagetrennte Liste von Anwendernamen Anwendungsbeispiel: `Winchecks check-windows-user-disabled- u Administrator,Guest`	Anwendername und Status

Windows Prüfungen der Metriküberwachung

Richtlinie für Windows-Betriebssystem-Metriken

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
os.windows.check-processor-queue-length	Misst die Länge der Prozessorwarteschlange.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process)	win2019-dc-64bit.cpu.queuelength 0.00 1645371109

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Verwendungsbeispiel: `command: winchecks metric-windows-processor-queue-length --scheme hostname.proc`	
os.windows.check-system-cpu-load	Erfasst die durchschnittliche CPU-Last pro Sekunde.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-cpu-load -scheme hostname.proc`	win2019-dc-64bit.cpu.loadavgsec 15.07 1645371561
os.windows.check-system-cpu	Erfasst die CPU-Kern-Metrik.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-cpu -scheme hostname.proc`	win2019-dc-64bit.cpu.cpu0.cores 2 1645371681
os.windows.check-system-disk-usage	Erfasst die folgenden Metriken für die Datenträgerverwendung: • Summe in GB • Nutzung in GB • Verfügbarkeit in GB • verwendeter Prozentsatz	Verwendung: • -i, ignore_mnt – Kommagetrennte Liste der zu ignorierenden Bereitstellungspunkte (:C) • -I, include_mnt – Kommagetrennte	win2019-dc-64bit.disk_usage.disk_C.total(GB) 99.40 1645371774 win2019-dc-64bit.disk_usage.disk_C.used(GB) 50.72 1645371774

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Liste der einzubeziehenden Bereitstellungspunkte • --scheme, scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process). Verwendungsbeispiel: `command: winchecks metric-windows-disk-usage-scheme hostname.proc`	win2019-dc-64bit.disk_usage.disk_C.avail(GB) 48.68 1645371774 win2019-dc-64bit.disk_usage.disk_C.used_perc 51.02 1645371774
os.windows.check-system-memory-percent	Erfasst die prozentuale Auslastung des Arbeitsspeichers, des freien physischen Arbeitsspeichers und des freien virtuellen Arbeitsspeichers.	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-disk-usage-scheme hostname.proc`	win2019-dc-64bit.mem.free_physical_percento 13.30 1645371856 win2019-dc-64bit.mem.free_virtual_percentage 13.93 1645371856 win2019-dc-64bit.ram.usage_percentage 86.07 1645371856
os.windows.check-system-network	Erfasst die folgenden Metriken zu aktiven Netzwerkadaptern: • Gesamtanzahl Bytes/s • Pakete/s • Empfangene Pakete/s • Gesendete Pakete/s • Aktuelle Bandbreite • Empfangene Bytes/s	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-network --scheme hostname.proc`	Win2019-dc-64bit.system.network.Network_Inte name><metric value> Bytes_Total/ Sek. 98742,67 1645372042 Beispiel: Win2019-dc-64bit.system.network.Network_Inte sec 98742.67 1645372042

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	• Unicastpakete empfangen/s • Nicht-Unicastpakete empfangen/s • Empfangene Pakete, verworfen • Empfangene Pakete, Fehler • Empfangene Pakete, unbekannt • Gesendete Bytes/s • Unicastpakete gesendet/s • Nicht-Unicastpakete gesendet/s • Ausgehende Pakete, verworfen • Ausgehende Pakete, Fehler • Ausgabewarteschlangenlänge • Abgeladene Verbindungen • Aktive TCP-Verbindungen für RSC • TCP-RSC: zusammengefügte Pakete/Sek. • TCP-RSC: Ausnahmen/Sek. • TCP RSC: durchschnittliche Paketgröße		
os.windows.check-system-uptime	Erfasst die Systemverfügbarkeit	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen	win2019-dc-64bit.system.uptime(sec) 4614142.06 1645372124

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
		Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-uptime --scheme hostname.proc`	
os.windows.check-system-disk	Erfasst die folgenden Datenträgermetriken: • AvgDiskSecPerRead • AvgDiskSecPerWrite • DiskReadBytesPerSec • DiskWriteBytesPerSec	Verwendung: • -i, ignoriert_mnt: Kommagetrennte Liste der zu ignorierenden Bereitstellungspunkte (:C) • -I, include_mnt – Kommagetrennte Liste der einzubeziehenden Bereitstellungspunkte. • —scheme – Ersetzt „hostname +process“ der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process). Verwendungsbeispiel: `command: winchecks metric-windows-disk`	win2019-dc-64bit.disk._total.AvgDisksec/Read 0.000000 1645372198 win2019-dc-64bit.disk._total.AvgDisksec/Write 0.000608 1645372198 win2019-dc-64bit.disk._total.DiskReadBytes/sec 0.000000 1645372198 win2019-dc-64bit.disk._total.DiskWriteBytes/sec 34941.692255 1645372198 win2019-dc-64bit.disk.C.AvgDisksec/Read 0.000000 1645372200 win2019-dc-64bit.disk.C.AvgDisksec/Write 0.000000 1645372200 win2019-dc-64bit.disk.C.DiskReadBytes/sec 0.000000 1645372200 win2019-dc-64bit.disk.C.DiskWriteBytes/sec 0.000000 1645372200
os.windows.check-system-memory	Erfasst die folgenden Datenträgermetriken:	Verwendung: -s, schema – Ersetzt	win2019-dc-64bit.mem.free_physical(KB)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	• FreePhysicalMemory • TotalPhysicalMemory • FreeVirtualMemory • TotalVirtualMemorySize • AvailableMemory • TotalVisibleMemorySize	den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-memory --scheme hostname.proc`	1175440.00 1645372274 win2019-dc-64bit.mem.total_physical(KB) 8588898304.00 1645372274 win2019-dc-64bit.mem.free_virtual(KB) 1747636.00 1645372274 win2019-dc-64bit.mem.total_virtual(KB) 12263156.00 1645372274 win2019-dc-64bit.mem.available(KB) 1202032640.00 1645372274 win2019-dc-64bit.mem.total_visible(KB) 8387596.00 1645372274
os.windows.check-process-status	Erfasst den Windows-Prozessstatus mit CPU- und Arbeitsspeicherdaten, die vom Prozess verwendet werden.	Verwendung: • -n, prozess – Prozessname zum Erfassen der Statusmetrik. • —scheme – Ersetzt „hostname +process“ der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process).	win2019-dc-64bit.Process.Status 67 1645372421 win2019-dc-64bit.Process.CpuPercent 0 1645372421 win2019-dc-64bit.Process.Memory(KB) 1226444 1645372421
os.windows.metrics-process-status	Ruft die Anzahl der ausgeführten Instanzen, den Prozentsatz der CPU-Auslastung und die Auslastung des Arbeitsspeichers (in Kilobyte) des angegebenen	Verwendung: • -n, prozess – Prozessname zum Erfassen der Statusmetrik. • —scheme – Ersetzt „hostname	WIN-R493MKFE75G.Prozess.Status 1 1625478491 WIN-R493MKFE75G.Prozess.CpuPercent 0 1625478491

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für Windows-Betriebssystem-Metriken (Fortsetzung)

Prüfung	Beschreibung	Verwendung und Beispiel	Ausgabe
	Prozesses Windows ab.	+process“ der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process). Anwendungsbeispiel: `Befehl: Winchecks Metric-Windows-Process-Status -n Svchost -s hostname.proc`	WIN-R493MKFE75G.Prozess.Arbeitsspeicher 276 162547849

Windows BS-Ereignisprüfungen – Erweitert

Führt erweiterte Windows Prüfungen auf funktionsfähigen Windows Servern durch. Um diese Richtlinie auszuführen, aktivieren Sie eine der Prüfungen, und geben Sie auf der Registerkarte Überwachte CIs der Richtlinie einen CI-Filter an, um diese Prüfungen für ausgewählte CIs auszuführen.

Windows BS-Ereignisse: Erweiterte Richtlinie

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
os.windows.check-processor-queue-length	Misst die Länge der Prozessorwarteschlange.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-processor-queue-length --scheme hostname.proc`	win2019-dc-64bit.cpu.queuelength 0.00 1645371109
os.windows.check-system-cpu	Erfasst die CPU-Kern-Metrik.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process)	win2019-dc-64bit.cpu.cpu0.cores 2 1645371681

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
		Verwendungsbeispiel: `command: winchecks metric-windows-cpu -scheme hostname.proc`	
os.windows.check-system-cpu-load	Erfasst die durchschnittliche CPU-Last pro Sekunde.	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-cpu-load -scheme hostname.proc`	win2019-dc-64bit.cpu.loadavgsec 15.07 1645371561
os.windows.check-system-disk-usage	Erfasst die folgenden Metriken für die Datenträgerverwendung: • Summe in GB • Nutzung in GB • Verfügbarkeit in GB • verwendeter Prozentsatz	Verwendung: • -i, ignore_mnt – Kommagetrennte Liste der zu ignorierenden Bereitstellungspunkte (:C) • -I, include_mnt – Kommagetrennte Liste der einzubeziehenden Bereitstellungspunkte. • --scheme, scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process). Verwendungsbeispiel: `command: winchecks metric-windows-disk-`	win2019-dc-64bit.disk_usage.disk_C.total(GB) 99.40 1645371774 win2019-dc-64bit.disk_usage.disk_C.used(GB) 50.72 1645371774 win2019-dc-64bit.disk_usage.disk_C.avail(GB) 48.68 1645371774 win2019-dc-64bit.disk_usage.disk_C.used_perc 51.02 1645371774

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
		`usage-scheme hostname.proc`	
os.windows.check-system-memory-percent	Erfasst die prozentuale Auslastung des Arbeitsspeichers, des freien physischen Arbeitsspeichers und des freien virtuellen Arbeitsspeichers.	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-disk-usage-scheme hostname.proc`	win2019-dc-64bit.mem.free_physical_percento 13.30 1645371856 win2019-dc-64bit.mem.free_virtual_percentag 13.93 1645371856 win2019-dc-64bit.ram.usage_percentage 86.07 1645371856
os.windows.check-system-network	Erfasst die folgenden Metriken zu aktiven Netzwerkadaptern: • Gesamtanzahl Bytes/s • Pakete/s • Empfangene Pakete/s • Gesendete Pakete/s • Aktuelle Bandbreite • Empfangene Bytes/s • Unicastpakete empfangen/s • Nicht-Unicastpakete empfangen/s • Empfangene Pakete, verworfen • Empfangene Pakete, Fehler • Empfangene Pakete, unbekannt • Gesendete Bytes/s	Verwendung: -s scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-network --scheme hostname.proc`	Win2019-dc-64bit.system.network.Network_Inte name><metric value> Bytes_Total/ Sek. 98742,67 1645372042 Beispiel: Win2019-dc-64bit.system.network.Network_Inte sec 98742.67 1645372042

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
	• Unicastpakete gesendet/s • Nicht-Unicastpakete gesendet/s • Ausgehende Pakete, verworfen • Ausgehende Pakete, Fehler • Ausgabewarteschlangenlänge • Abgeladene Verbindungen • Aktive TCP-Verbindungen für RSC • TCP-RSC: zusammengefügte Pakete/Sek. • TCP-RSC: Ausnahmen/Sek. • TCP RSC: durchschnittliche Paketgröße		
os.windows.check-system-uptime	Erfasst die Systemverfügbarkeit	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-uptime --scheme hostname.proc`	win2019-dc-64bit.system.uptime(sec) 4614142.06 1645372124
os.windows.check-system-disk	Erfasst die folgenden Datenträgermetriken: • AvgDiskSecPerRead • AvgDiskSecPerWrite	Verwendung: • -i, ignoriert_mnt: Kommagetrennte Liste der zu	win2019-dc-64bit.disk._total.AvgDisksec/Read 0.000000 1645372198

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
	• DiskReadBytesPerSec • DiskWriteBytesPerSec	ignorierenden Bereitstellungspunkte (:C) • -I, include_mnt – Kommagetrennte Liste der einzubeziehenden Bereitstellungspunkte. • --scheme, scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process). Verwendungsbeispiel: `command: winchecks metric-windows-disk`	win2019-dc-64bit.disk._total.AvgDisksec/Write 0.000608 1645372198 win2019-dc-64bit.disk._total.DiskReadBytes/sec 0.000000 1645372198 win2019-dc-64bit.disk._total.DiskWriteBytes/sec 34941.692255 1645372198 win2019-dc-64bit.disk.C.AvgDisksec/Read 0.000000 1645372200 win2019-dc-64bit.disk.C.AvgDisksec/Write 0.000000 1645372200 win2019-dc-64bit.disk.C.DiskReadBytes/sec 0.000000 1645372200 win2019-dc-64bit.disk.C.DiskWriteBytes/sec 0.000000 1645372200
os.windows.check-system-memory	Erfasst die folgenden Datenträgermetriken: • FreePhysicalMemory • TotalPhysicalMemory • FreeVirtualMemory • TotalVirtualMemorySize • AvailableMemory • TotalVisibleMemorySize	Verwendung: -s, schema – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process) Verwendungsbeispiel: `command: winchecks metric-windows-memory --scheme hostname.proc`	win2019-dc-64bit.mem.free_physical(KB) 1175440.00 1645372274 win2019-dc-64bit.mem.total_physical(KB) 8588898304.00 1645372274 win2019-dc-64bit.mem.free_virtual(KB) 1747636.00 1645372274 win2019-dc-64bit.mem.total_virtual(KB)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows BS-Ereignisse: Erweiterte Richtlinie (Fortsetzung)

Überprüfen	Beschreibung	Verwendung und Beispiel	Ausgabe
			12263156.00 1645372274 win2019-dc-64bit.mem.available(KB) 1202032640.00 1645372274 win2019-dc-64bit.mem.total_visible(KB) 8387596.00 1645372274
os.windows.check-process-status	Erfasst den Windows-Prozessstatus mit CPU- und Arbeitsspeicherdaten, die vom Prozess verwendet werden.	Verwendung: • -n, prozess – Prozessname zum Erfassen der Statusmetrik. • --scheme, scheme – Ersetzt den Hostnamen + den Prozess der Ausgabe durch den angegebenen Wert (Beispiel: hostname.process).	win2019-dc-64bit.Process.Status 67 1645372421 win2019-dc-64bit.Process.CpuPercent 0 1645372421 win2019-dc-64bit.Process.Memory(KB) 1226444 1645372421

Windows-Metriken

In der folgenden Tabelle werden die Metriken aufgelistet, die als Ausgabe von Windows-Prüfungen erfasst werden. Einträge, die als **Empfohlene Metriken** angegeben sind, sind Metriken mit hoher Sichtbarkeit, die auf der Betreiber-Arbeitsbereich-Registerkarte „Metrik“ angezeigt werden, nachdem eine Warnung generiert wurde. Diese Metriken liefern dem Operator zusätzliche Informationen, damit das angegebene Problem weiter untersucht werden kann.

Windows-Metriken

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
Process.Status			Windows-Prozessstatus einschließlich CPU- und Speicherdaten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
Process.CpuPercent			Prozentsatz der vom Prozess verwendeten CPU.
Process.Memory(KB)		KB	Vom angegebenen Prozess verwendeter Arbeitsspeicher.
cpu.queuelength (empfohlene Metrik)			Länge der Prozessorwarteschlange.
cpu.loadavgsec (empfohlene Metrik)			Durchschnittliche CPU-Last pro Sekunde.
disk.AvgDisksec/ Read		seconds	Durchschnittliche Zeit eines Lesevorgangs vom Datenträger.
disk.AvgDisksec/Write		seconds	Durchschnittliche Zeit eines Schreibvorgangs auf dem Datenträger.
disk.DiskReadBytes/ sec		Byte/s	Rate, mit der Bytes während Lesevorgängen vom Datenträger übertragen werden.
disk.DiskWriteBytes/ sec		Byte/s	Rate, mit der Bytes während Schreibvorgängen auf den Datenträger übertragen werden.
disk_usage.avail(GB)		GB	Verfügbarer Datenträger.
disk_usage.used(GB)		GB	Verwendeter Datenträger.
disk_usage.total(GB)		GB	Datenträger insgesamt.
disk_usage.used_percentage (empfohlene Metrik)			Verwendeter Datenträger in Prozent.
mem.free_physical_percentage			Freier physischer Arbeitsspeicher in Prozent.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
mem.free_virtual_percentage			Freier virtueller Arbeitsspeicher in Prozent.
ram.usage_percentage (empfohlene Metrik)			Verwendeter Arbeitsspeicher in Prozent.
mem.free_physical(KB)		KB	Menge des freien physischen Arbeitsspeichers.
mem.total_physical(KB)		KB	Physischer Arbeitsspeicher insgesamt.
mem.free_virtual(KB)		KB	Menge des freien virtuellen Arbeitsspeichers.
mem.total_virtual (KB)		KB	Virtueller Arbeitsspeicher gesamt.
mem.available(KB)		KB	Gesamtmenge des verfügbaren virtuellen Arbeitsspeichers.
mem.total_visible(KB)		KB	Gesamtmenge des physischen Arbeitsspeichers, auf den vom Betriebssystem zugegriffen werden kann.
system.uptime(Sec)		seconds	Dauer der Betriebsbereitschaft des Systems.
system.network.Bytes_Received/ sec (empfohlene Metrik)		Byte/s	Für aktive Netzwerkadapter empfangene Bytes pro Sekunde.
system.network.Bytes_Sent/ sec (empfohlene Metrik)		Byte/s	Für aktive Netzwerkadapter gesendete Bytes pro Sekunde.
system.network.Bytes_Total/ sec (empfohlene Metrik)		Byte/s	Summe der pro Sekunde

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			empfangenen und gesendeten Bytes.
system.network.Current_Bandwidth		Bit/s	Geschätzte Bandbreite der Netzwerkschnittstelle.
system.network.Offloaded_Connections			Anzahl der IPv4- und IPv6-TCP-Verbindungen, die derzeit vom Netzwerkadapter verarbeitet werden, der TCP-Chimney-Abladung unterstützt.
system.network.Output_Queue_Length			Länge der Ausgabepaketwarteschlange.
system.network.Packets/sec			Rate, mit der Pakete im Netzwerk gesendet und empfangen werden.
system.network.Packets_Outbound_Discarded			Anzahl der ausgehenden Pakete, die verworfen wurden.
system.network.Packets_Outbound_Errors			Anzahl der ausgehenden Pakete, die aufgrund von Fehlern nicht gesendet werden konnten.
system.network.Packets_Received/sec			Rate, mit der Pakete empfangen werden.
system.network.Packets_Received_Discarded			Anzahl der eingehenden Pakete, die verworfen wurden.
system.network.Packets_Received_Errors			Anzahl der eingehenden Pakete, die aufgrund von Fehlern nicht gesendet werden konnten.
system.network.Packets_Received_Non-Unicast/sec			Die Rate, mit der Nicht-Unicastpakete (Subnetz-Broadcast

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			oder Subnetz-Multicast) an ein übergeordnetes Protokoll übergeben werden.
system.network.Packets_Received_Unicast/sec			Rate, mit der Unicastpakete (Subnetz) an ein übergeordnetes Protokoll übergeben werden.
system.network.Packets_Received_Unknown			Anzahl der empfangenen, aber aufgrund eines unbekannten oder nicht unterstützten Protokolls verworfenen Pakete.
system.network.Packets_Sent/sec			Rate, mit der Pakete gesendet werden.
system.network.Packets_Sent_Non-Unicast/sec			Rate, mit der Pakete von übergeordneten Protokollen an Nicht-Unicastadressen (Subnetz-Broadcast oder Subnetz-Multicast) übertragen werden sollen. Enthält Pakete, die verworfen oder nicht gesendet wurden.
system.network.Packets_Sent_Unicast/sec			Rate, mit der Pakete von übergeordneten Protokollen an Subnetz-Unicastadressen übertragen werden sollen. Enthält Pakete, die verworfen oder nicht gesendet wurden.
system.network.TCP_Active_RSC_Connections			Anzahl der IPv4- und IPv6-TCP-Verbindungen, über die momentan große Pakete

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Windows-Metriken (Fortsetzung)

Metriktyp	Ressource (Name der spezifischen Datenbank, falls relevant)	Einheiten	Beschreibung des Metriktyps
			vom RSC-fähigen Netzwerkadapter empfangen werden.
system.network.TCP_RSC_Average_Packet_Size		Byte	Durchschnittliche Größe der empfangenen Pakete über alle TCP-Verbindungen hinweg.
system.network.TCP_RSC_Coalesced_Packets/sec			Die Empfangsrate für große Pakete über alle TCP-Verbindungen hinweg.
system.network.TCP_RSC_Exceptions/sec			Die Rate für RSC-Ausnahmen für empfangene Pakete über alle TCP-Verbindungen hinweg.

Windows-Protokollüberwachung – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgende Richtlinie für die Windows-Protokollüberwachung.

Richtlinie für die Windows-Protokollüberwachung

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Event	os.windows.check-log	Aktiviert die Überwachung von Protokolldateien auf einem Windows-Server.	Verwendung: • -c crit N – Kritische Stufe, wenn das Muster eine Gruppe aufweist. • -f -log-file FILE – Pfad zur Protokolldatei. • -o --warn-only – Bei Übereinstimmung warnen statt kritisch. • -q pattern PAT – Muster,	Windows-Protokoll KRITISCH: 4 kritische gefunden, 0 Warnungen für Muster SEVERE | Exception | 404 | Errorin Datei C:\ProgramData\ServiceNow\agent-client-collector\log\acc.log

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinie für die Windows-Protokollüberwachung (Fortsetzung)

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			nach dem gesucht werden soll. Um nach mehreren Mustern zu suchen, trennen Sie die einzelnen Muster mit einem senkrechten Strich (|), und setzen Sie die Muster in Anführungszeichen. Beispiel: "SEVERE|404" • -w warn N – Warnstufe, wenn das Muster eine Gruppe aufweist.	

Linux-Protokollüberwachung – Standardprüfungen und Richtlinien

Agent Client Collector bietet die folgende Richtlinie für die Linux-Protokollüberwachung.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
Event	util.check-logs	Aktiviert die Überwachung von Protokolldateien, die einem normalen Benutzer gehören.	Verwendung: • -i --icase – Führt einen Abgleich aus, bei dem nicht nach Groß-/Kleinschreibung unterschieden wird. • -c, --crit N – Kritische Stufe (wenn das Muster eine Gruppe aufweist). • --encode-utf16u – Zeile	CheckLog CRITICAL: 0 warnings, 8 criticals for pattern SEVERE|Exception in log file /var/log/servicenow/agent-client-collector/acc.log (CheckLog KRITISCH: 0 Warnungen, 8 kritische Elemente für Muster SEVERE|Exception in

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			vor dem Abgleich mit utf16 codieren. • -e, --encoding ENCODING-PAGE – Spezifische Codierungsseite zum Lesen der Protokolldatei. • -E, --exclude PAT – Muster, das vom Abgleich ausgeschlossen werden soll. • -F, --filepattern FILE – Überprüft ein Muster von Dateien anstelle einer einzigen Datei. Testen Sie das Muster bei regulären Ausdrücken (REGEX) zuerst auf `https://rubular.com/`, um die erwarteten Ergebnisse zu erhalten, und übergeben Sie es dann in Anführungszeichen als Parameter. Um beispielsweise alle Dateien mit der Erweiterung *`.log`* abzurufen, übergeben Sie `"(.)*\.log$"` als regulären Ausdruck (REGEX).	Protokolldatei / var/log/ servicenow/ agent-client-collector/ acc.log)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			• -f, --log-file FILE – Pfad zur Protokolldatei. • -l, --log-pattern PAT – Protokollformat der einzelnen Protokolleinträge: • -o, --warn-only – Bei Übereinstimmung warnen statt kritisch. • -q, --pattern PAT – Muster, nach dem gesucht werden soll. Um nach mehreren Mustern zu suchen, trennen Sie die einzelnen Muster mit einem senkrechten Strich (|), und setzen Sie die Muster in Anführungszeichen (Beispiel: "SEVERE | 404"). • -r, --return – Gibt übereinstimmende Zeile zurück. • -L, --return-length N – Übereinstimmende Zeilenlänge. • -M, --return-error-limit N – Max. Anzahl der zurückgegebenen übereinstimmenden Zeilen (Protokolleinträge).	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			• -n, --name NAME – Legt das Statusdateiverzeichnis automatisch mit dem Namen fest. • -s, --state_dir DIR – Verzeichnis, unter dem die Statusdateien aufbewahrt werden sollen. • -w, --warn N – Warnstufe, wenn das Muster eine Gruppe aufweist. Verwendungsbeispiel: `command: check-log.rb -c 2 -w 1 -q "SEVERE|Exception" -s /tmp/cache/check-log -f /var/log/servicenow/agent-client-collector/acc.log`	
Event	util.check-logs-sudo	Aktiviert die Überwachung von Protokolldateien, die einem Root-Benutzer gehören.	Verwendung: • -i --icase – Führt einen Abgleich aus, bei dem nicht nach Groß-/Kleinschreibung unterschieden wird • -c, --crit N – Kritische Stufe (wenn das Muster eine Gruppe aufweist)	CheckLog CRITICAL: 0 warnings, 8 criticals for pattern SEVERE|Exception in log file /var/log/servicenow/agent-client-collector/acc.log (CheckLog KRITISCH: 0 Warnungen, 8 kritische Elemente für Muster SEVERE|

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			• --encode-utf16u – Zeile vor dem Abgleich mit utf16 codieren • -e, --encoding ENCODING-PAGE – Spezifische Codierungsseite zum Lesen der Protokolldatei. • -E, --exclude PAT – Muster, das vom Abgleich ausgeschlossen werden soll • -F, --filepattern FILE – Überprüft ein Muster von Dateien anstelle einer einzigen Datei. Testen Sie das Muster bei regulären Ausdrücken (REGEX) zuerst auf `https://rubular.com/`, um die erwarteten Ergebnisse zu erhalten, und übergeben Sie es dann in Anführungszeichen als Parameter. Um beispielsweise alle Dateien mit der Erweiterung *`.log`* abzurufen, übergeben Sie `"(.)*\.log$"` als regulären Ausdruck (REGEX).	Exception in Protokolldatei / var/log/ servicenow/ agent-client-collector/ acc.log)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			• -f, --log-file FILE – Pfad zur Protokolldatei. • -l, --log-pattern PAT – Protokollformat der einzelnen Protokolleinträge: • -o, --warn-only – Bei Übereinstimmung warnen statt kritisch • -q, --pattern PAT – Muster, nach dem gesucht werden soll. Um nach mehreren Mustern zu suchen, trennen Sie die einzelnen Muster mit einem senkrechten Strich (|), und setzen Sie die Muster in Anführungszeichen (Beispiel: "SEVERE | 404"). • -r, --return – Gibt übereinstimmende Zeile zurück. • -L, --return-length N – Übereinstimmende Zeilenlänge. • -M, --return-error-limit N – Max. Anzahl der zurückgegebenen übereinstimmenden Zeilen (Protokolleinträge).	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Prüfung	Beschreibung	Verwendung und Verwendungsbeispi	Ausgabe
			• -n, --name NAME – Legt das Statusdateiverzeichnis automatisch mit dem Namen fest. • -s, --state_dir DIR – Verzeichnis, unter dem die Statusdateien aufbewahrt werden sollen • -w, --warn N – Warnstufe, wenn das Muster eine Gruppe aufweist. Verwendungsbeispiel: `command: check-log.rb -c 2 -w 1 -q "SEVERE|Exception" -s /tmp/cache/check-log -f /var/log/servicenow/agent-client-collector/acc.log`	

Azure Metriken-Skript

Erstellen Sie beim Erstellen einer neuen Richtlinie für Cloud-Metriken Azure ein JSON-Skript, um die zu überwachenden Metriken zu bestimmen. Das Format für das Skript wird unten angezeigt, gefolgt von einer Tabelle, in der der Skriptinhalt erläutert wird.

```
{
  "namespace": "Microsoft.Network/loadBalancers",
  "metrics": [
          "AllocatedSnatPorts",
          "ByteCount",
          "DipAvailability",
          "PacketCount",
          "SnatConnectionCount",
          "SYNCount",
          "UsedSnatPorts",
          "VipAvailability"
```

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  ],
  "time_grain": "PT1M"
}
```

Ressourcen und ihre Metriken können auf der Seite Unterstützte Metriken für Azure-Ressourcen abgerufen werden.

Header	Beschreibung
namespace	Der Name der überwachten Ressource.
Metriken	Die Metriken, die von der überwachten Ressource abgerufen werden.
time_korn	Granularität der Erfassungshäufigkeit von Metriken. Mögliche Werte: • PT1M: Metrikwerte werden jede Minute gesammelt. • PT5M: Metrikwerte werden alle 5 Minuten erfasst. • PT15M: Metrikwerte werden alle 15 Minuten erfasst. • PT30M: Metrikwerte werden alle 30 Minuten erfasst. • PT1H: Metrikwerte werden stündlich gesammelt. • PT1D: Metrikwerte werden täglich gesammelt.

Windows Ereignisprotokoll-Filterparameter

Die konfigurierbaren Werte auf der Registerkarte Prüfungsparameter der Prüfung os.windows.check-event-log.

Werte der Registerkarte „Parameter“ überprüfen

Parameter	Typ	Beschreibung
provider_name	Zeichenfolge	Name des Anbieters, der das Ereignis generiert hat. **Hinweis:** Wenn Sie keinen Wert *log_file* zusammen mit *provider_name* angeben, durchsucht das System alle verfügbaren Protokolldateien, was die Zeit zum Empfangen von Ergebnissen erhöht.
log_file	Zeichenfolge	Der Name der Ereignisprotokolldatei Windows, aus der Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Werte der Registerkarte „Parameter“ überprüfen (Fortsetzung)

Parameter	Typ	Beschreibung
		Ereignisse abrufen. Mögliche Werte: • Anwendung • System **Hinweis:** Wenn Sie keinen Wert *provider_name* zusammen mit *log_file* angeben, durchsucht das System alle Ereignisse aus der Protokolldatei, wodurch die Anzahl der abgerufenen Ereignisse erhöht wird.
id	Ganzzahl	Die numerische ID des Ereignisses. Mögliche Werte sind 0–65535.
Warnung	Ganzzahl	Jeder Wert über dem angegebenen Parameter generiert ein Warnereignis.
event_level	Zeichenfolge	Der Schweregrad des Ereignisses. Mögliche Werte: • Kritisch • Fehler • Warnung • Informationen • Ausführlich
regex_pattern	Zeichenfolge	Das Muster des regulären Ausdrucks, das beim Durchsuchen der Ereignisprotokolle verwendet werden soll. Der Wert muss in doppelte Anführungszeichen eingeschlossen werden. Beispiel: „Fehler“.
Dauer_Stunde	Ganzzahl	Der Zeitraum, für den Sie Ereignisse aus dem Ereignisprotokoll Windows abrufen möchten. Der Wert wird in Stunden angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Werte der Registerkarte „Parameter“ überprüfen (Fortsetzung)

Parameter	Typ	Beschreibung
		Bruchteile von Stunden werden als Dezimalzahlen angegeben.
kritisch	Ganzzahl	Jeder Wert, der dem angegebenen Parameter entspricht oder darüber liegt, generiert ein kritisches Ereignis.

Parameter eines verteilten MID Server-Clusters

Die folgenden MID Server-Parameter unterstützen den MID-Server-Clustertyp „Verteilt“.

Sie können auf diese Parameter in der zugehörigen Liste **Konfigurationsparameter** eines MID Servers zugreifen. Informationen zum Hinzufügen und Festlegen dieser Parameter finden Sie unter MID-Server-Parameter hinzufügen .

Parameter	Beschreibung
mid.distributed.cluster.striped.threadpool.size	Größe des Striped-Thread-Pools im verteilten MID Server-Cluster. • **Typ**: Ganzzahl • **Standardwert**: Anzahl der Kerne des virtuellen Computers oder des Servers
mid.distributed.cluster.log.level	Protokollierungsebene für den verteilten MID Server-Cluster zur Unterstützung der Problembehandlung. Die Protokollierung wirkt sich jedoch auf die Leistung von Metric Intelligence aus. Bei einem leeren Wert erfolgt keine Protokollierung. • **Typ**: Ganzzahl • **Standardwert**: keiner • **Andere mögliche Werte**: info, debug, trace
mid.distributed.cluster.global.timeout	Globale Zeitüberschreitung in Sekunden für verteilte MID Server-Cluster. • **Typ**: Ganzzahl • **Standardwert**: 180 • **Andere mögliche Werte**: ◦ **Mindestwert**: 60 (nicht erzwungen) ◦ **Maximalwert**: 300 (nicht erzwungen)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter	Beschreibung
mid.distributed.cluster.node.max.off.heap.memory	Größe des Off-Heap-Speichers, der von Metric Intelligence zur Verarbeitung von Datenreihen pro Minute verwendet wird. Der Standardspeicherplatz von 4 GB entspricht der Menge an Off-Heap-Speicher, die für die Verarbeitung von 800.000 Datenreihen pro Minute erforderlich ist. Passen Sie diesen Wert proportional zur Menge der tatsächlichen Datenreihen an. Um beispielsweise 400.000 Datenreihen pro Minute zu verarbeiten, können Sie den Wert auf 2048 ändern. • **Typ**: Ganzzahl • **Standardwert**: 4096

Regelmäßige Aufgaben im verteilten MID Server-Cluster

Die folgende regelmäßige MID Server-Aufgabe ist im MID-Server-Clustertyp „Verteilt“ enthalten.

Name	Beschreibung
Verteilten MID Server-Cluster validieren	Validiert den Status des Clusterknotens für jeden MID Server im Cluster. Für einen MID Server, der inaktiv ist und dessen Status nicht „Gestoppt“ ist, wird der Knotenstatus auf „Gestoppt“ aktualisiert. Validiert auch den Gesamtstatus des Clusters. Während dieser Validierung wird der Cluster von der Aufgabe angehalten, wenn mehrere Untercluster in einem Cluster vorhanden sind.

Mit Metric Intelligence installierte Komponenten

Bei Aktivierung des Plugins „Metrikdaten“ (com.snc.sa.metric) werden mehrere Arten von Komponenten installiert, z. B. Tabellen, regelmäßige Aufgaben und Eigenschaften.

Hinweis: In der Tabelle „Anwendungsdateien“ sind die mit dieser Anwendung installierten Komponenten aufgeführt. Anweisungen für den Zugriff auf diese Tabelle finden Sie unter Komponenten finden, die mit dieser Anwendung installiert wurden .

Regelmäßige Aufgaben installiert

Name	Beschreibung
Metric Intelligence – Aufgabe zum Lernen von Metriken	Wird täglich ausgeführt und erstellt die statistischen Modelle für die Anomalie-Erkennung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
Metric Intelligence – Alte Metrikschemas und Anomaliepunktzahlen löschen	Bereinigt die Tabellen *sa_metric_anomaly_score* und *sa_metric_schema_definition*
Metric Intelligence – Metrikschema mit MID synchronisieren	Synchronisiert Daten aus der Instanz mit dem MID Server in der Metrikschematabelle *sa_metric_schema_definition*
Metric Intelligence – Tabellen mit MID synchronisieren	Synchronisiert Tabellendaten aus der Instanz mit dem MID Server
Metric Intelligence – Tabelle bereinigen	Bereinigt Tabellen im Zusammenhang mit verschiedenen Löschvorgängen
Metric Intelligence – Aufgabe zum Lernen des Beobachtungsintervalls	Berechnet das Beobachtungsintervall anhand gesammelter Datenpunkte für alle Datenreihen
Metric Intelligence – Anomaliepunktzahl für Prozessalterung – Täglich	Täglicher Job, der veraltete Anomaliepunktzahlen für ein bestimmtes Zeitfenster in der Tabelle „Anomaliepunktzahl der Metrik“ [sa_metric_anomaly_score] bereinigt. Verwendet die Eigenschaften *sa_metric.anomaly_score_stale_interval_in_days* und *sa_metric.anomaly_score_next_stale_interval_in_days*, um das Zeitfenster für die Bereinigung zu berechnen
Metric Intelligence – CI-Anomaliepunktzahlen synchronisieren	Hält Anomaliepunktzahlen beim Löschen von Metriken aktuell
Metric Intelligence – Konfigurationsaufgabe für Metriken	Synchronisiert Metrikkonfigurationen von der Instanz zu allen Metrikdaten-MID Servern
Metric Intelligence – Aufgabe zum Lernen des Kalman-Filtermodells auf lokaler Ebene	Erstellt Kalman-Filtermodelle auf lokaler Ebene, auf denen die Change-Erkennung ausgeführt wird
Metric Intelligence – Anomaliemodelltest	Regelmäßige Aufgabe, die bei Bedarf ausgeführt wird, wenn der Benutzer auf **Anomalietest ausführen** klickt
Metric Intelligence – Verteiltes MID-Cluster validieren	**1.** Überprüft den Status des Clusterknotens. Wenn der Status **Gestartet** lautet und der Status der Metrikdaten-Erweiterung nicht **Gestartet**/**Wird gestartet**/**Warnung** [Warnung mit bestimmten Fehlern] ist, ändert der Job den Status des Clusterknotens in **Gestoppt**. Dies passiert, wenn der MID Server unerwartet beendet wird, ohne dass die Instanz darüber benachrichtigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
	2. Überprüft den Status aller Clusterknoten auf allen MID Servern im Cluster. ◦ Wenn der Status aller Knoten **Gestoppt** und der Status des Clusters **Gestartet** lautet, ändert die Aufgabe den Status des Clusters in **Gestoppt**. ◦ Wenn der Status des Clusters **Gestoppt** lautet, aber MID Server mit einem Clusterknoten vorhanden sind, der ausgeführt wird, wird der Status des Clusters in **Gestartet** geändert. **3.** Überprüft die Anzahl der Clusterleiter: Wenn zwei erkannt werden, stoppt der Auftrag den gesamten Cluster. Dies passiert, wenn MID Server keine Verbindung mit anderen Mitgliedern des Clusters herstellen und mehrere Subcluster bilden können.
Event Management – Metrikbindungsevents verarbeiten [1000 – 1020]	Verarbeitet Metric Intelligence-Metrikbindungs-Events getrennt von Ereignismanagement-Events (Bucket-Bereich 1000 – 1020).
Event Management – Metrikbindungsevents verarbeiten [1020 – 1040]	Verarbeitet Metric Intelligence-Metrikbindungs-Events getrennt von Ereignismanagement-Events (Bucket-Bereich 1020 – 1040).
Event Management – Metrikbindungsevents verarbeiten [1040 – 1060]	Verarbeitet Metric Intelligence-Metrikbindungs-Events getrennt von Ereignismanagement-Events (Bucket-Bereich 1040 – 1060).
Event Management – Metrikbindungsevents verarbeiten [1060 – 1080]	Verarbeitet Metric Intelligence-Metrikbindungs-Events getrennt von Ereignismanagement-Events (Bucket-Bereich 1060 – 1080).
Event Management – Metrikbindungsevents verarbeiten [1080 – 1100]	Verarbeitet Metric Intelligence-Metrikbindungs-Events getrennt von Ereignismanagement-Events (Bucket-Bereich 1080 – 1100).
Metric Intelligence – Aufgabe zum Lernen des stationären nichtparametrischen Modells	Lernt das stationäre nicht-parametrische Modell
Metric Intelligence – Aufgabe zum Lernen des kombinierten Modells	Konstruiert alle Informationen, die für die Durchführung der Anomalie-Erkennung in Echtzeit (Berechnen der Datenhäufigkeit und Erstellen statistischer Modelle) erforderlich sind, für eine Teilmenge aller Reihen, für die Daten gesammelt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Installierte Tabellen

Tabelle	Beschreibung
Metrikzeitreihenmodell [sa_time_series]	Für Metrikdaten erstellte statistische Modelle
Alarm-Anomalie [em_alert_anomaly]	Anomaliewarnungen, die aus Anomalie-Events erstellt wurden, die von Metric Intelligence gesendet wurden, damit Benutzer sie überprüfen können. Anomaliewarnungen werden von regulären Systemwarnungen getrennt gehalten.
Anomaliepunktzahl der Metrik [sa_metric_anomaly_score]	Speichert Anomaliepunktzahlen für die Metrik
Metrik-Zuordnung an CI − Gelöschte SysIds [sa_metric_map_deleted]	SysIds gelöschter Datensätze für Metrik-an-CI-Zuordnungen
Metrik-Zuordnung an CI [sa_metric_map]	Derzeit gültige Zuordnungen von Metriktypen zu CIs
Registrierung des SA-Metriktyps [sa_metric_registration]	Details zur Metriktypregistrierung
Metriktypregistrierung − Gelöschte SysIds [sa_metric_registration_deleted]	SysIds von Datensätzen, die aus der Tabelle „Registrierung des SA-Metriktyps“ [sa_metric_registration] gelöscht wurden
Metrikschemadefinition [sa_metric_schema_definition]	Zuordnung der empfangenen Metriken basierend auf der CI-Klasse. Sie wird verwendet, um die Metrikdaten-Nutzlast zu optimieren, die vom MID Server an die Instanz gesendet wird.
Metriktyp [sa_metric_type]	Quellmetriktyp
Typ der Überwachungssystemmetrik − Gelöschte SysIds [sa_source_metric_type_deleted]	SysIds der gelöschten Überwachungssystemmetriken
Typ der Überwachungssystemmetrik [sa_source_metric_type]	Metriktypen pro CI-Klasse, Aktivitätsstatus und Metrikquelle
Metrikeinstellungen [sa_metric_config_setting]	Standardkonfigurationseinstellungen für Metric Intelligence-MID Server.
Metrikkonfigurationsregeln [sa_metric_config_rule]	Regeln zum Überschreiben von Konfigurationseinstellungen für MID Server

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
Überschriebene Konfigurationen der Metrik [sa_metric_config_rule_setting]	Ordnet überschriebene Konfigurationen benutzerdefinierten Regeln zu
Bereitgestellte Konfigurationen der Metrik [sa_metric_config_staging]	Gespeicherte codierte Konfigurationen für die MID Server
Gelernte Parameter der Metrik [sa_metric_learned_param]	Parameter, die für CI/Metrik-Kombinationen gelernt wurden und mit den MID Servern synchronisiert werden
Metrik-Zuordnung an CI − Gelöschte Details [sa_metric_map_deleted_detail]	Details zu aus der Metrik-an-CI-Zuordnungstabelle gelöschten Einträgen. Schließt CI, Metrik und SysId des gelöschten Eintrags in der Tabelle „Metrik-Zuordnungen an CIs“ [sa_metric_map] ein.
In Metrikzuordnung erstellte eindeutige CIs nachverfolgen [sa_metric_ci_tracker]	Alle eindeutigen CIs, für die ein Metrikzuordnungseintrag erstellt wurde
Metrikklasse [sa_metric_class]	Metrikklassen, die bestimmten Metriken zugeordnet werden können, um gelernte Werte für Grenzen und Breiten zu überschreiben
Change-Punktzahl der Metrik [sa_metric_change_score]	Change Event-Informationen
Anomalietestregeln [sa_metric_anomaly_test_rule]	Anomalietestregeln, die für Anomaliemodelltests verwendet werden
Anomalietestergebnisse [sa_metric_anomaly_test_result]	Ergebnisse aus Anomaliemodelltests, z. B. Grenzen und Anomaliepunktzahlen
Konfiguration des Metrikanomalietests − angepasste Parameter [sa_metric_anomaly_test_config_custom_param]	Angepasste Parameter für ausgewählte Reihen in Anomaliemodelltests
Eigenschaften von Metric Intelligence [sa_metric_property]	Eigenschaften von Metric Intelligence nach Domäne.
Hostname mit Metrik-CI nachverfolgen [sa_metric_ci_host]	CIs, die mit dem Knotennamen aus dem Bindungsevent verbunden sind
Von der Metrikausdruckssprache unterstützte Funktionen [sa_metric_expr_funktion]	Von der Metrikausdruckssprache unterstützte Funktionen
Argumenttypen für Funktionen, die von der Metrikausdruckssprache unterstützt werden	Argumenttypen für Funktionen, die von der Metrikausdruckssprache unterstützt werden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sa_metric_expr_func_arg]	
CI-Typen zu Metrikeinträgen nachverfolgen, die für verschiedene Quellen gültig sind [sa_metric_ci_type_map]	CI-Typen zu Metrikeinträgen nachverfolgen, die für verschiedene Quellen gültig sind
CI-Typ zu Ressourcenklasse [sa_ci_type_to_resource_class]	Enthält Zuordnungen des CI-Typs zur Ressourcenklasse. Wird für die Ressourcenbindung während der Ressourcensuche verwendet, wenn ein CI und ein *resource_path* im Event angegeben sind. Die Tabelle [sa_ci_type_to_resource_class] enthält einige Datensätze für Standardzuordnungen, und die Rolle evt_mgmt_admin ist zum Verwalten dieser Tabelle erforderlich.
CI-Ressource [ci_resource]	Übergeordnete Tabelle für Ressourcenbindungen
CI-Ressource – Hardware [ci_resource_hardware]	Eine Erweiterung der Tabelle „CI-Ressource“ [ci_resource], die für die Ressourcenbindung verwendet wird
CI-Ressource – Anwendung [ci_resource_appl]	Eine Erweiterung der Tabelle „CI-Ressource“ [ci_resource], die für die Ressourcenbindung verwendet wird
CI-Ressource – Service [ci_resource_service]	Eine Erweiterung der Tabelle „CI-Ressource“ [ci_resource], die für die Ressourcenbindung verwendet wird
CI-Ressource – virtueller Computer [ci_resource_vm_object]	Eine Erweiterung der Tabelle „CI-Ressource“ [ci_resource], die für die Ressourcenbindung verwendet wird
CI-Ressource – Datenbank [ci_resource_database]	Eine Erweiterung der Tabelle „CI-Ressource“ [ci_resource], die für die Ressourcenbindung verwendet wird
Event-Verlauf der Serie [sa_series_event_history]	Informationen zum Starten und Beenden des Wartungsmodus von CIs. Metrikdaten speichert Verlaufsinformationen über die Zeiten, zu denen CIs in den Wartungsmodus treten und ihn wieder verlassen, wenn die Systemeigenschaft „sa.model_learner.maint_event_record_history_enabled“ auf „true“ (Standard) festgelegt ist. Wenn dann auch die Systemeigenschaft „sa_metric.maint_exclusion“ auf „true“ (Standard) festgelegt ist, werden Metriken von CIs im Wartungsmodus vom Modelllernen ausgeschlossen.
Metadaten des Messgrößen-Dashboards	Diagrammkonfigurationen in Agent Workspace pro CI-Klasse für die Metriken, die für ein einer Warnung zugeordnetes CI angezeigt werden

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle	Beschreibung
[sa_metric_dashboard_metadata]	
Messgrößenkonfiguration – Bereitstellung der Anomalie-Erkennung [sa_metric_config_anomaly_detection_staging]	Interne Tabelle, die zur Berechnung der Aktionsebene für jeden Eintrag in der Tabelle „Metrik-Zuordnung an CI“ [sa_metric_map] verwendet wird

Installierte Eigenschaften

Hinweis: Um die Tabelle „Systemeigenschaft“ [sys_properties] zu öffnen, geben Sie im Navigationsfilter `sys_properties.list` ein. Zum Öffnen der Tabelle „Metrikeinstellungen“ [sa_metric_config_setting] geben Sie im Navigationsfilter `sa_metric_config_setting.list` ein.

Eigenschaft	Verwendung
sa.metric.map.with.ci.expiration.sec	Dauer (in Sekunden), die Datensätze für die Zuordn von Rohdaten zu CIs in Kraft bleiben, wenn die Zuordnung zum CI gefunden wird • **Typ**: Numerisch • **Standardwert**: 432000 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikdaten
sa.metric.map.without.ci.expiration.sec	Dauer (in Sekunden), die Datensätze für die Zuordn von Rohdaten zu CIs in Kraft bleiben, wenn die Zuordnung zum CI nicht gefunden wird • **Typ**: Numerisch • **Standardwert**: 86400 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikdaten
sa_metric.anomaly_score_stale_interval_in_days	Der Starttag des Zeitfensters, das die regelmäßige Aufgabe *Operational Metrics - Process Sta Anomaly Score - Daily* beim Überprüfen des Alterungsstatus der Anomaliepunktzahl verwendet. Das Zeitfenster reicht von heute so viele Tage zurüc in dieser Eigenschaft angegeben sind. • **Typ**: Numerisch • **Standardwert**: 3 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung
sa_metric.anomaly_score_next_stale_interval_in_days	Anzahl der Tage, um die das von der regelmäßigen Aufgabe *Operational Metrics - Process Sta Anomaly Score - Daily* verwendete Zeitfenster erweitert wird. Gilt, wenn der Auftrag ausgeführt wird, aber unter der Verwendung des in der Eigenschaft *sa_metric.anomaly_score_stale_interval_in* angegebenen Zeitfensters keine Daten zurückgege werden. • **Typ**: Numerisch • **Standardwert**: 7 • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties]
max_records_per_rest_request	Maximale Anzahl von Datensätzen, die in jedem Synchronisierungszyklus von der Instanz auf den MID Server heruntergeladen werden. Diese Eigenschaft ist für die interne Verwendung bestimmt. • **Typ**: Ganzzahl • **Standardwert**: 10.000 • **Andere mögliche Werte**: ◦ **Mindestwert**: 1000 ◦ **Maximalwert**: 20000 • **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]
normalized_metric_max_queue_size	Größe der Metrikwarteschlange. Der Anomaliedete liest diese Warteschlange und bestimmt für jede Me ob sie anomal ist. Diese Eigenschaft ist für die interne Verwendung bestimmt. • **Typ**: Ganzzahl • **Standardwert**: 3000000 • **Andere mögliche Werte**: ◦ **Mindestwert**: 1000000 ◦ **Maximalwert**: 5000000 • **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]
normalized_metric_queue_consumer_count	Anzahl der Threads, die die Anomalie-Erkennung gleichzeitig durchführen. Diese Eigenschaft ist für die interne Verwendung bestimmt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung
	• **Typ**: Ganzzahl • **Standardwert**: 12 • **Andere mögliche Werte**: ◦ **Mindestwert**: 8 ◦ **Maximalwert**: 16 • **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]
ignite_data_streamer_thread_count	Anzahl der Threads, die Datenstreamer zum Schreib von Daten in den Cache verwenden. Der Datenstreamer erstellt Stapel aus einzelnen Dateneinträgen und fügt diese Stapel dem Cache Diese Eigenschaft ist für die interne Verwendung bestimmt. • **Typ**: Ganzzahl • **Standardwert**: 8 • **Andere mögliche Werte**: ◦ **Mindestwert**: 8 ◦ **Maximalwert**: 32 • **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]
ignite_data_streamer_flush_frequency	Häufigkeit der automatischen Löschung von Datenstreamern. Der Datenstreamer erstellt Stapel aus einzelnen Dateneinträgen und fügt diese Stapel dem Cache Diese Eigenschaft ist für die interne Verwendung bestimmt. • **Typ**: Ganzzahl • **Standardwert**: 1.000 • **Andere mögliche Werte**: ◦ **Mindestwert**: 0 ◦ **Maximalwert**: 30000 • **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]
ignite_data_streamer_buffer_size	Puffergröße von Datenstreamern. Der Datenstreamer erstellt Stapel aus einzelnen Dateneinträgen und fügt diese Stapel dem Cache Diese Eigenschaft ist für die interne Verwendung bestimmt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung
	• **Typ**: Ganzzahl • **Standardwert**: 102400 • **Andere mögliche Werte**: ◦ **Mindestwert**: 1024 ◦ **Maximalwert**: 1024000 • **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]
ignite_data_streamer_batch_size	Größe des Stapels, der einem Datenstreamer hinzugefügt wird. Der Datenstreamer erstellt Stapel aus einzelnen Dateneinträgen und fügt diese Stapel dem Cache Diese Eigenschaft ist für die interne Verwendung bestimmt. • **Typ**: Ganzzahl • **Standardwert**: 5.000 • **Andere mögliche Werte**: ◦ **Mindestwert**: 1 ◦ **Maximalwert**: 10000 • **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]
ignite_data_streamer_batch_flush_frequency	Häufigkeit der automatischen Löschung der interne Stapelverarbeitung, bevor Daten zu Datenstreame hinzugefügt werden. Der Datenstreamer erstellt Stapel aus einzelnen Dateneinträgen und fügt diese Stapel dem Cache Diese Eigenschaft ist für die interne Verwendung bestimmt. • **Typ**: Ganzzahl • **Standardwert**: 5.000 • **Andere mögliche Werte**: ◦ **Mindestwert**: 1000 ◦ **Maximalwert**: 30000 • **Speicherort**: Tabelle „Metrikeinstellungen“ [sa_metric_config_setting]
sa.metric.use.resource.binding	Ermöglicht Ressourcenbindung • **Typ**: true | false • **Standardwert**: true

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung
	• **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikbindung an Ressourcen
sa.metric.display.mid.setup.action	Zeigt den zugehörigen Link **Metric Intelligence einri** im MID Server-Formular für einen MID Server an, der validiert wurde und ausgeführt wird. • **Typ**: true | false • **Standardwert**: true • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: MID Server und verteilter MID Serv Cluster für Metric Intelligence
sa.model_learner.maint_event_record_history_enabled	Speichert Verlaufsinformationen zu Start und Ende d Wartungsmodus von CIs in der Tabelle „Event-Verla Serie“ [sa_series_event_history]. • **Typ**: true | false • **Standardwert**: true • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikdaten verstehen
sa_metric.maint_exclusion	Schließt Metriken für CIs, die sich im Wartungsmodu befinden, vom Modelllernen aus • **Typ**: true | false • **Standardwert**: true • **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikdaten verstehen
sa.model_learner.maint_history_batch_size	Ermittelt beim Speichern von Verlaufsinformationen zu Start und Ende des Wartungsmodus von CIs in der Tabelle „Event-Verlauf der Serie“ [sa_series_event_history] die Anzahl von Datenreihen pro Stapel. Passen Sie die Einstellung dieser Eigenschaft an, we diesem Zusammenhang Leistungsprobleme auftret • **Typ**: Ganzzahl • **Standardwert**: 1.000

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaft	Verwendung
	• **Speicherort**: Tabelle „Systemeigenschaft“ [sys_properties] • **Mehr erfahren**: Metrikdaten verstehen
sa_metric.scheduled_jobs_to_monitor_sys_id_list	Enthält die sys_ids der 3 regelmäßigen Aufgaben, d von der Eigensystemüberwachung für Metric Intelli überwacht werden: • Metric Intelligence – Konfigurationsaufgabe für Metriken • Metric Intelligence – Tabellen mit MID synchronisi • Metric Intelligence – Verteiltes MID-Cluster validie

Schnellstarttests für Metrikdaten

Überprüfen Sie, ob Metrikdaten immer noch funktioniert, nachdem Sie eine Konfigurationsänderung vorgenommen haben, z. B. Anwendung eines Upgrades oder Entwickeln einer Anwendung. Kopieren Sie diese zu bestehenden Schnellstarttests und konfigurieren Sie sie mit Ihren instanzspezifischen Daten.

Metrikdaten-Schnellstarttests erfordern die Aktivierung des Metrikdaten-Plugins (com.snc.sa.metric).

Metrikdaten-Schnellstarttests

Test	Beschreibung	Release-Version
OI: Sammlung von Integritätsmetriken	Ein einzelner Test, der Folgendes überprüft: • Mindestens eine Metrikdaten Metriken-Erweiterung wird ausgeführt. • Die Tabelle „Metrik an CI“ enthält Einträge für die „Integritätsmetriken“. • Für jede der derzeit ausgeführten Metrikdaten Metriken-Erweiterungen sind Daten in MetricBase gespeichert. Wenn der Test anfänglich fehlschlägt, warten Sie, bis die Metrikdaten Metriken-Erweiterung mindestens 10-15 Minuten lang ausgeführt wird. Versuchen Sie es dann erneut.	Madrid

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Schnellstarttests

Ereignisschweregrade

Die Ereignisschweregradzahlen entsprechen den tatsächlichen Schweregraden auf der Seite „Anomaliepunktzahl der Metrik für Zuordnungen des Ereignisschweregrads“.

Zuordnung des Ereignisschweregrads

Ereignis-Schweregrad-Nummer	Ereignis-Schweregrad
0	Löschen (OK)
1	Kritisch
2	Hoher
3	Geringer
4	Warnung

Agent Client Collector Visibility – Inhalt

Agent Client Collector Visibility – Inhalt (ACC-VC) ist ein ServiceNow -Agent, der auf den Servern Windows, Linuxoder macOS installiert ist, um Hostdaten zu erfassen.

Agent Client Collector Visibility – Inhalt – Übersicht

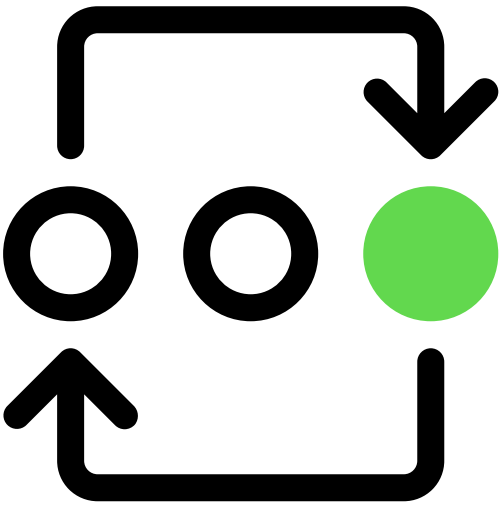
ACC-VC stellt Ruby-Skripts bereit, die OS-Abfragebefehle und betriebssystemspezifische Befehle ausführen, um Informationen auf Ihren Servern Windows, Linuxoder macOS zu sammeln. Sie können Daten aus verschiedenen Dateisystemen und Speichergeräten, TCP-Verbindungen, laufenden Prozessen und anderen Informationen über Zielhosts erkennen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

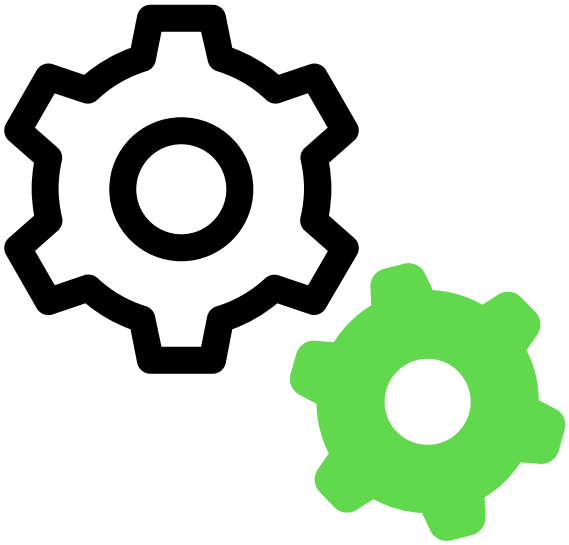
Erste Schritte

Untersuchen



Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen der Anwendung Agent Client Collector Visibility – Inhalt kennen.

Konfigurieren

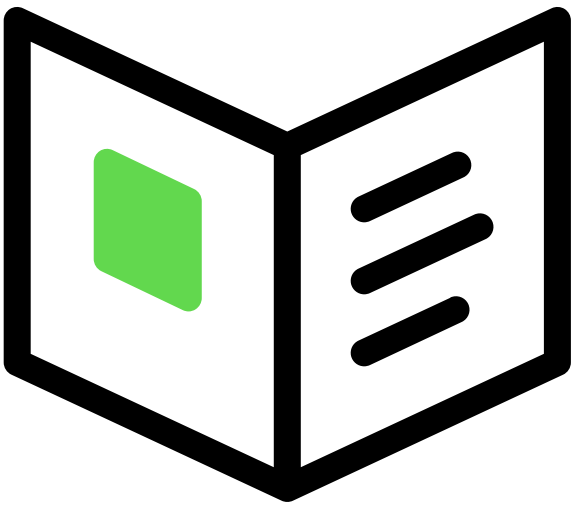


Konfigurieren Sie die Funktionen und Komponenten, um Agent Client Collector Visibility – Inhaltzu aktivieren.

Verwenden

Anweisungen für die Verwendung von Agent Client Collector Visibility – Inhalt.

Referenz



Rufen Sie zusätzliche Details zu Agent Client Collector Visibility – Inhaltab .

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängigkeiten

Eine Liste der Agent Client Collector Visibility – Inhalt Plugin-Abhängigkeiten finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Transparenz und Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Problembehandlung und Hilfe

- Stellen oder beantworten Sie Fragen im Community-Forum von Agent Client Collector.
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Agent Client Collector Visibility – Inhalt erkunden

Erfahren Sie, wie Sie mit Agent Client Collector Visibility – Inhalt (ACC-VC) Daten auf Ihren Zielhosts erkennen können.

Agent Client Collector Visibility – Inhalt – Übersicht

ACC-VC ist ein zusätzlicher Mechanismus zur Ausführung von Discovery. Es ist eine Alternative zu horizontalen IP-basierten Discovery für betriebssystembezogene Attribute wie Systeminformationen, Netzwerkschnittstellen, laufender Prozess usw. ACC-VC eignet sich für lokale Server und Cloud-Instanzen. ACC-VC erkennt neben herkömmlichen MSI-basierten Installationen auch Software aus anderen Installationsquellen, z. B. „Schkokolade“, „Klicken-zu-Ausführen“ und „Winget“.

Agent Client Collector Visibility – Inhalt unterstützt die folgenden Module:

- Datensammlung
- Erweiterter Bestand
- Seriennummern
- Speichergeräte
- Dateisysteme
- Netzwerkadapter
- TCP-Verbindungen
- Laufende Prozesse
- Installierte Software
- Lokaler Benutzer
- Intel vPro® Plattform

Hinweis:

- Agent Client Collector Visibility – Inhalt unterstützt derzeit keine mehreren Sprachen. Wenn die zurückgegebenen Werte nicht in Englisch vorliegen, können die zurückgegebenen Daten nicht richtig analysiert werden, und die Erkennung schlägt fehl.
- PowerShell wird in keinem der ACC-VC-Module unter MicrosoftMicrosoft Azure Event Hubs Windows Betriebssystemen verwendet.

Sie können Ihre Zielsysteme in ServiceNow Configuration Management Database (CMDB) mithilfe des pushbasierten ACC-VC-Modells registrieren und verwalten. Es ist nicht

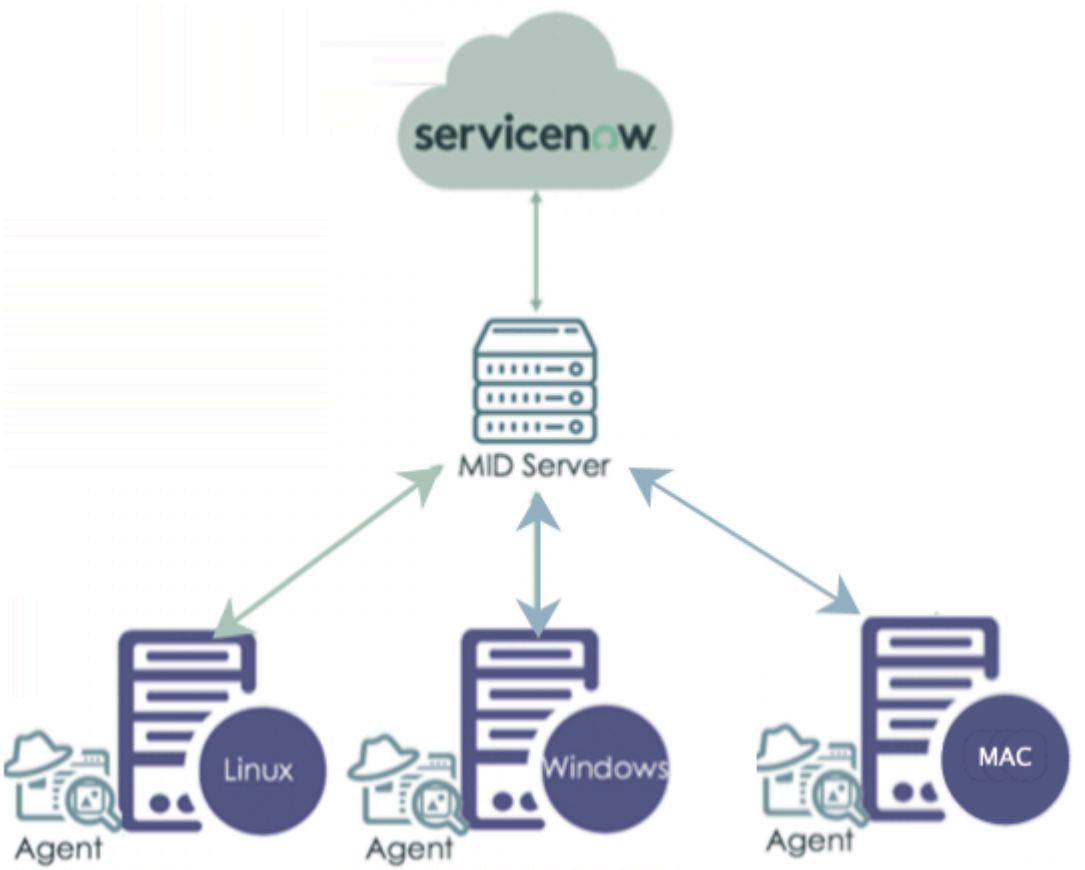
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erforderlich, Anmeldeinformationen anzugeben, Zeitpläne zu konfigurieren oder IP-Bereiche zu scannen.

Agent Client Collector Visibility – Inhalt – Workflow

Die folgende Abbildung beschreibt die allgemeine Architektur von Agent Client Collector Visibility – Inhalt.

ACC-VC-Architektur



ACC-VC funktioniert mit den folgenden Komponenten:

- ServiceNow Instanz
- ServiceNow MID-Server
- Zielhostcomputer
- ServiceNow Agent Client Collector welche auf den Zielhostcomputern ausgeführt wird

Unterstützte Betriebssysteme

ACC-VC Version 1.0.3 sammelt die Systemattribute und zugehörigen Listen, die normalerweise vom BS-Muster gesammelt werden. ACC-VC unterstützt derzeit die folgenden Betriebssysteme mit x86_64-Architektur:

- Linux
  - Red Hat Enterprise Linux (RHEL) und Oracle Linux (OL) 7, 8, 9
  - Centos 7, 8, 9
  - SLES 12, 15
  - Ubuntu 18, 20

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Amazon Linux 2
- Debian 9 und 10

- MicrosoftMicrosoft Azure Event Hubs Windows
  - Windows Server 2012, 2012r2, 2016, 2019, 2022
  - Windows 10 Enterprise Edition
  - Windows 11 Enterprise und Professional Edition
- macOS (ab ACC-VC Version 1.3.0)
  - 10.15 - Catalina
  - 11 - Big Sur
  - Monterey (x86)
  - 13: Venura
  - macOS ventura auf ARM64 – Apple Silicon M1/M2
  - Sonoma

Funktionsweise von Agent Client Collector Visibility – Inhalt

Agent Client Collector Visibility – Inhalt (ACC-VC) erfordert die Installation von ServiceNow Agent Client Collector (ACC) auf dem Zielhost. ACC ist ein Derivat von Sensu-Go, einer Open-Source-Software.

ACC-VC-Anwendungsfälle

ACC-VC wendet Prüfungen und Richtlinien an, um Hostdaten zu planen und zu erfassen. ACC-VC wird in den folgenden Fällen ausgelöst:

- Periodische Planung: Ein richtlinienbasierter Ansatz, bei dem Discovery regelmäßig ausgelöst wird.
- Bei CI-Löschung: Wenn der CI-Datensatz des Computers oder Servers gelöscht wird.
- MID-Server -Zyklus: Wenn MID-Server ausfällt und wieder hochkommt.
- Zielhost-Zyklus: Wenn der Zielhost ausfällt und wieder hochgefahren wird.
- Netzwerkbruch: Wenn der Netzwerklink zum Ziel unterbrochen wird.

Hinweis: Discovery wird für die Agents ausgelöst, deren Hosts bereits vorhanden sind. Agents, deren Hosts nicht vorhanden sind, werden über ACC-F erkannt.

ACC-VC – Prüfungen und Richtlinien

Die ACC-VC-Assets werden als Agent-Plugins mit dem Haupteinstiegspunkt [acc_visibility_main] und anderen Modulen für Betriebssystemfamilien gespeichert. Es gibt eine Hauptsystemprüfungsdefinition Discovery mit der Bezeichnung *`Enhanced Discovery`*, die von *`Enhanced Discovery Policy`* verwendet wird. Diese ACC-VC-Richtlinie wird anhand eines Zeitplans ausgeführt, der standardmäßig auf 24 Stunden (86.400 Sekunden) festgelegt ist. Diese Richtlinienkonfiguration wird mit allen Agents synchronisiert, die in der ACC-VC-Richtlinie definiert sind.

Wenn die Nutzlast von MID-Server an die Instanz zurückgegeben wird, delegiert der ACC-VC-Prüftyp *`EnhancedDiscovery`* Aufgaben an die von ACC-VC bereitgestellte Skripteinbindung EnhancedDiscoveryHandler. Das Skript enthält Logik zur Verarbeitung der Daten aus dem Scheck und behandelt Aufgaben wie:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Datentransformation in eine IRE-kompatible Nutzlast (Identification and Reconciliation Engine)
- Abgleich von Nicht-CI-Daten (cmdb_running_processes, cmdb_tcp_connections usw.)

Die ACC-VC-Prüfdefinition *Enhanced Discovery* wird von der Instanz ServiceNow initiiert. Anschließend wird in der Ausgabewarteschlange ein Datensatz der ECC-Warteschlange mit dem Thema MonitoringProbe mit relevanten Prüfungsinformationen erstellt. MID-Server verarbeitet den Scheck dann, indem eine Nachricht per WebSocket über TLS an den ACC gesendet wird.

Während dieser Zeit bedient der MID-Server auch alle relevanten Assets oder Plugins, die vom ACC angefordert werden, um sicherzustellen, dass sie für das jeweilige Betriebssystem, die Plattform, die Betriebssystemversion und die Architektur relevant sind, auf der ACC ausgeführt wird.

Sie können alle Teile der ACC-VC-Anwendung bearbeiten und ändern, einschließlich Prüfungstyp, Richtlinie und Prüfungsdefinition. Weitere Informationen finden Sie unter Prüfungen und Richtlinien.

Virtuelle Maschinen (VM) und Cloud-Instanzen

ACC-VC ordnet ein über Discoveryerkanntes Ziel einer bereits vorhandenen VM-Instanz-CIs zu. ACC-VC ordnet den erkannten CI-Datensatz einem bereits vorhandenen VM-Instanz-Datensatz oder Cloud-Server-Instanz-Datensatz mit entsprechenden CMDB-Beziehungen zu.

Die folgenden Varianten von Virtualisierungs- und Cloud-Server-Anbietern werden für ACC-VC unterstützt:

- vCenter
- Amazon AWS Cloud
- Google (GCP)
- Microsoft Azure

Agent Client Collector Visibility – Inhalt konfigurieren

Planen und konfigurieren Sie Ihre Agent Client Collector Visibility – Inhalt (ACC-VC)-Implementierung.

Konfiguration – Übersicht

ACC-VC erfordert die Installation von ServiceNow Agent Client Collector (ACC) auf dem Zielhost. ACC ist ein Derivat von Sensu-Go, einer Open-Source-Software.

Die Konfiguration von Agent Client Collector Visibility – Inhalt erfordert Folgendes:

- Das Plugin „Discovery“ (com.snc.discovery) muss installiert und aktiviert sein.
- Agent Client Collector Framework (ACC-F) muss in der Instanz ServiceNow installiert sein.
- Der Agent muss auf dem Zielhost installiert sein.
- Vergewissern Sie sich, dass Sie ein Upgrade auf Quebec, Patch 3 oder höher durchgeführt haben.
- Vergewissern Sie sich, dass Sie über die Berechtigungen local_system_account verfügen.
- ITOM Discovery oder ITOM-Transparenz SKUs (SU-basierte Lizenzierung) sind erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können dann die Anwendung Agent Client Collector Visibility – Inhalt (ACC-VC) von ServiceNow Store oder von der -Instanz [sn_acc_visibility] herunterladen und installieren. Weitere Informationen finden Sie unter Installation von Agent Client Collector.

Hinweis: Im ServiceNow Store werden regelmäßig neue Anwendungen und Updates für die von ServiceNow Store erstellten Anwendungen veröffentlicht. Wenn Sie die Anwendung bereits haben, können Sie die neueste Version herunterladen, um Ihre derzeitige Experience weiter zu verbessern. Da bei jeder Veröffentlichung einer Anwendung im Store neue Funktionen verfügbar sind oder Funktionen erweitert werden, werden die verfügbaren Inhalte und Features in der Dokumentation mit der Versionsnummer angegeben.

Agent Client Collector Visibility – Inhalt verwenden

Wenn Agent Client Collector Visibility – Inhalt (ACC-VC) auf Ihren Servern Windows, Linuxoder macOS installiert wird, werden verschiedene Informationen gesammelt, je nachdem, welche anderen Funktionen oder Produkte Sie installiert haben.

Apps im Store anfordern

Besuchen Sie die ServiceNow Store -Website, um alle verfügbaren Apps anzuzeigen und Informationen zum Senden von Anforderungen an den Store zu erhalten. Kumulative Informationen zum Release für alle veröffentlichten Apps finden Sie in den Release-Hinweisen zum ServiceNow Store-Versionsverlauf .

Push-basierte Discovery und horizontale IP-basierte Discovery zusammen verwenden

Discovery durchgeführt von Agent Client Collector Visibility – Inhalt (ACC-VC) ist kompatibel und kann mit horizontalem IP-basierten Discoverykoexistieren. Sie können ACC auf einem bestimmten Zielhost installiert haben und diesen Host noch als Teil eines horizontalen IP-basierten Zeitplans Discovery verwenden.

Zur Vermeidung von Konflikten führt ACC-VC Discovery nicht aus, wenn die IP des Zielhosts bereits über ein CI verfügt, das von einem horizontalen IP-basierten Discovery erkannt wurde (discovery_source ist ServiceNow). Um dieses Verhalten außer Kraft zu setzen, setzen Sie die Systemeigenschaft [*sn_agent.disco_disable_ci_clobber_of_agentless_disco*] auf false. Diese Einstellung wird ignoriert, wenn über einen bestimmten Zeitraum kein horizontales IP-basiertes Discovery durchgeführt wurde. Aktualisieren Sie gegebenenfalls die Systemeigenschaft [*sn_agent.disco_ci_clobber_of_agentless_disco_threshold_days*]. Der Standardwert ist 14 Tage. Weitere Informationen finden Sie unter Systemeigenschaften .

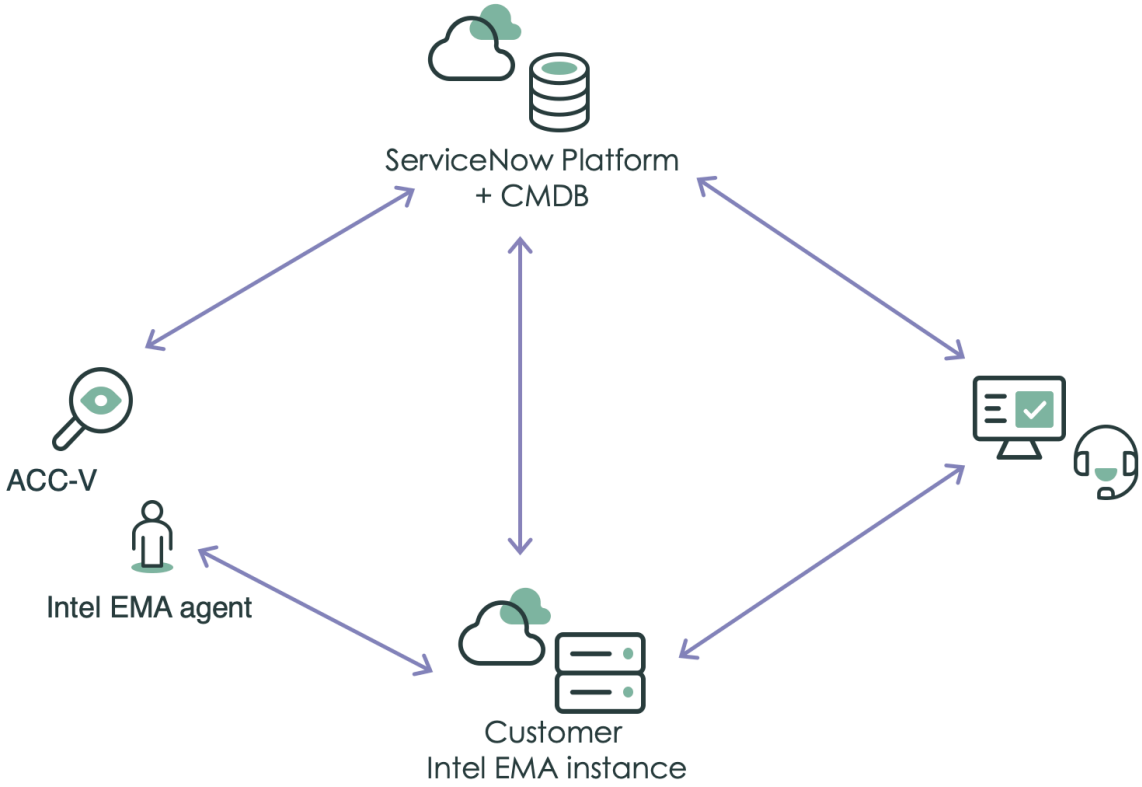
Pushbasierte Erkennung und Intel Endpoint Management Assistant (EMA) zusammen verwenden

Agent Client Collector Visibility – Inhalt (ACC-VC) kann Daten für Anwendungsfälle mit der Plattform Intel vPro® sammeln, wenn die Anwendung Intel ® EMA auf Endpunkten Windows von installiert ist. Sie können die Anwendung Intel EMA aus dem ServiceNow Store installieren. Attribute werden in der CMDB gespeichert, wenn diese aktiviert ist. Derzeit können Daten für Intel EMA nur für Windows-Endpunkte abgerufen werden.

Mit der Anwendung Intel EMA können Kunden den Zugriff auf die Intel-Instanz über ihre ServiceNow-Instanz konfigurieren. Beispielsweise können IT-Supportgruppen eine Remote-Konsole öffnen und Aktionen wie das Aus- und Wiedereinschalten ausgehend von einem ServiceNow-Incident ausführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Intel + ServiceNow Platform



Pushbasierte Erkennung und SAM zusammen verwenden

Agent Client Collector Visibility – Inhalt (ACC-VC) sammelt Daten der installierten Software für Anwendungsfälle für Software Asset Management (SAM), wenn das SAM-Plugin installiert ist. Die gemeinsame Verwendung von pushbasierter Discovery und SAM kann zur Optimierung der Softwareausgaben bei der Erfassung von Softwaredaten mit SAM-Basismessung und SAM-Metriken zur Gesamtnutzung beitragen. Sie können auch einige Informationen zur Software-Edition abrufen.

ACC-VC kann die letzte Zugriffszeit für die auf dem Ziel installierte Software oder Anwendungen über die pushbasierte Discovery erfassen. Diese Informationen werden zusammen mit der Ziel-CI-Referenz der Tabelle „Software-Update“ [samp_sw_usage] hinzugefügt.

Ab ACC-VC Version 2.2.0 werden die SAM-Basismessungen für Windows und macOSunterstützt.

Ab ACC-VC Version 3.3.0 werden SAM-Metriken zur Gesamtauslastung für Windows und macOSunterstützt.

Die Softwarenutzungsdatensätze sind domänengetrennt. Die Datensätze werden mit der Domäne des MID-Server beibehalten, der für die agentbasierte Discovery für das Ziel verwendet wird.

Hinweis: Für Softwareinstallationen (cmdb_sam_sw_install) wird, um das Einfügen doppelter Datensätze zu vermeiden, dieselbe Discovery-Quelle „ServiceNow“ für pushbasierte Discovery und horizontale IP-basierte Discoveryverwendet.

Anforderungen

SAM-Basismessung und SAM-Metriken zur Gesamtnutzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Für die SAM-Basismessung und die SAM-Gesamtauslastungsmetriken muss der nicht privilegierte servicenow-Anwender (als den sich der Agent-Service anmeldet) in der Registrierung mit schreibgeschütztem Lesezugriff konfiguriert sein. Dieser Zugriff ermöglicht die erfolgreiche Ausführung der OSQuery für die Tabelle „UserAssist“. Wechseln Sie zu „Regedit“, und lassen Sie den ServiceNow-Anwender UserAssist für alle anderen Anwenderaccounts lesen (Beispiel: `HKEY_USERS\SID...\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\UserAssist` für jeden Anwender in `HKEY_USERS`).

Hinweis: Der Schlüssel *`UserAssist`* erbt keine Berechtigungen vom übergeordneten Schlüssel *`HKEY_USERS|SID...`*. Daher müssen Sie zum Schlüssel *`UserAssist`* navigieren und die Berechtigung direkt für den Schlüssel hinzufügen.

Voraussetzungen für die Anwendung der SAM-Basismessung oder der SAM-Metriken zur Gesamtnutzung:

- Das SAM-Plugin ist (com.snc.samp) aktiviert.
- Die Systemeigenschaft *`sn_acc_vis_content.persist_sam_usage_metrics`* ist auf „true“ gesetzt. Weitere Informationen finden Sie unter Systemeigenschaften .

Weitere Informationen zum Setup der SAM-Messung mit Agent Client Collectorfinden Sie im Knowledge Base-Artikel KB1642676 .

Informationen zur Software-Edition

Zum Abrufen von Informationen über die Software-Edition muss das SAM-Plugin (com.snc.samp) aktiviert sein.

SAM-Basismessung

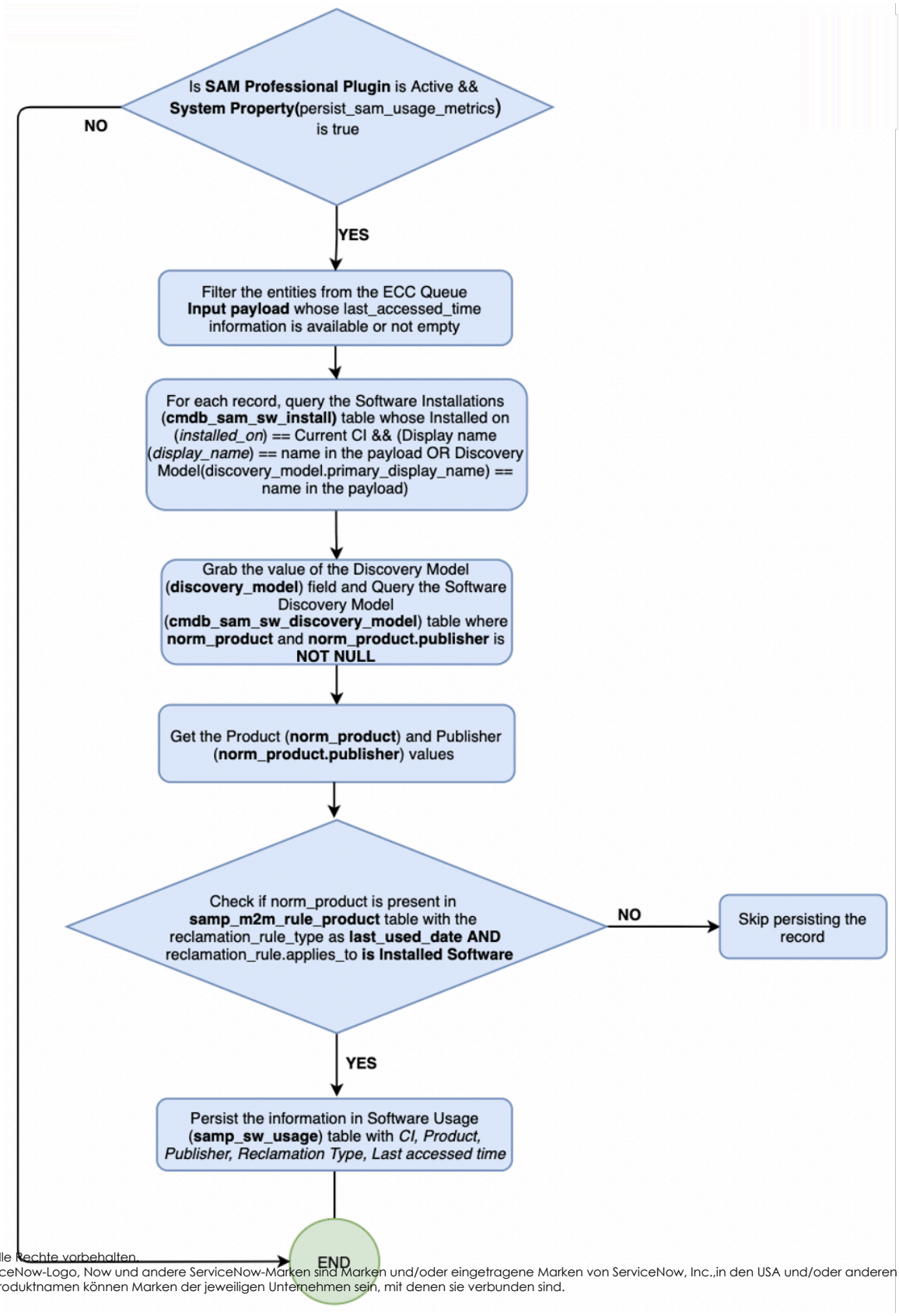
Hinweis: In der Betriebssystemebene Windows ist eine Konfiguration vorhanden, die die korrekte Erkennung der Daten nicht zulässt. Aktualisieren Sie die Konfiguration, damit die Daten erfolgreich vom ACC-VC-Agent gesammelt und korrekt auf die Plattform ServiceNow übertragen werden können. Erstellen Sie im Registrierungseditor die folgenden Schlüssel im Pfad: *`HKEY_CURRENT_USER|SOFTWARE|Microsoft|Windows|CurrentVersion|Explorer|Advanced.`*

- Name: Start_TrackProgs
  - Basis: Hexadezimalzahl
  - Wert:1
- Name: Start_TrackProgsBase
  - Basis: Hexadezimalzahl
  - Wert:1

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flussdiagramm zur SAM-Basismessung

Fragen Sie zum Beziehen einer Liste der Software in der Nutzlast die Tabelle „Software-Discovery-Modell“ [cmdb_sam_sw_discovery_model] ab, um das entsprechende Produkt und seinen Herausgeber abzurufen. Sobald das Produkt abgerufen wurde, überprüfen Sie, ob die Rückforderungsregel aktiviert ist, damit in der Tabelle „Softwarenutzung“ [samp_sw_usage] die Informationen über die letzte Nutzung dieses Produkts erhalten bleiben. Einzelheiten können Sie dem Flussdiagramm entnehmen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Fragen Sie mithilfe der OSQuery aus der Tabelle „UserAssist“ den Zeitpunkt des letzten Zugriffs für das Ziel ab. Verwenden Sie dabei den Anwendungs- oder Softwarenamen als Eingabe für die Abfrage.

Verwenden Sie die Eigenschaft *sn_acc_vis_content.disable_sam_reclamation_rules_for_licensable_softwares*, um Reklamationsregeln für lizenzierbare Software wie folgt zu definieren:

- **True**: Aufruf von Reklamationsregeln für lizenzierbare Software deaktivieren. Die SAM-Nutzung wird für alle lizenzierbaren und nicht lizenzierbaren Softwareanwendungen mit definierten Reklamationsregeln fortgesetzt.
- **False**: Speichert die SAM-Nutzung gemäß den definierten Reklamationsregeln.

Folgende häufig genutzte Anwendungen werden unterstützt:

- WinZip
- Google Chrome
- Sublime Text
- Notepad++
- Autodesk
- Microsoft Office 365
- Tableau

SAM-Metriken zur Gesamtnutzung

Mit SAM-Metriken zur Gesamtnutzung können Sie die Gesamtnutzungszeit und die Gesamtnutzungsanzahl für jede Anwendung messen, für die eine Rückforderungsregel für Software aktiviert ist.

Osquery stellt eine ausführbare Daemon-Datei namens Osqueryd bereit, die als Service ausgeführt werden kann. Osqueryd muss manuell bereitgestellt werden, damit die SAM-Metriken zur Gesamtnutzung ordnungsgemäß funktionieren. Jede Osqueryd-Bereitstellung erfordert die Datei osquery.conf, optional externe Pakete und Initialisierungskennzeichnungen (konfiguriert in der Datei osquery.flags), die beim Starten des Service bereitgestellt werden. Im Gegenzug führt der Daemon-Service geplante Abfragen auf dem Host aus und protokolliert dies in einem lokalen Dateisystem.

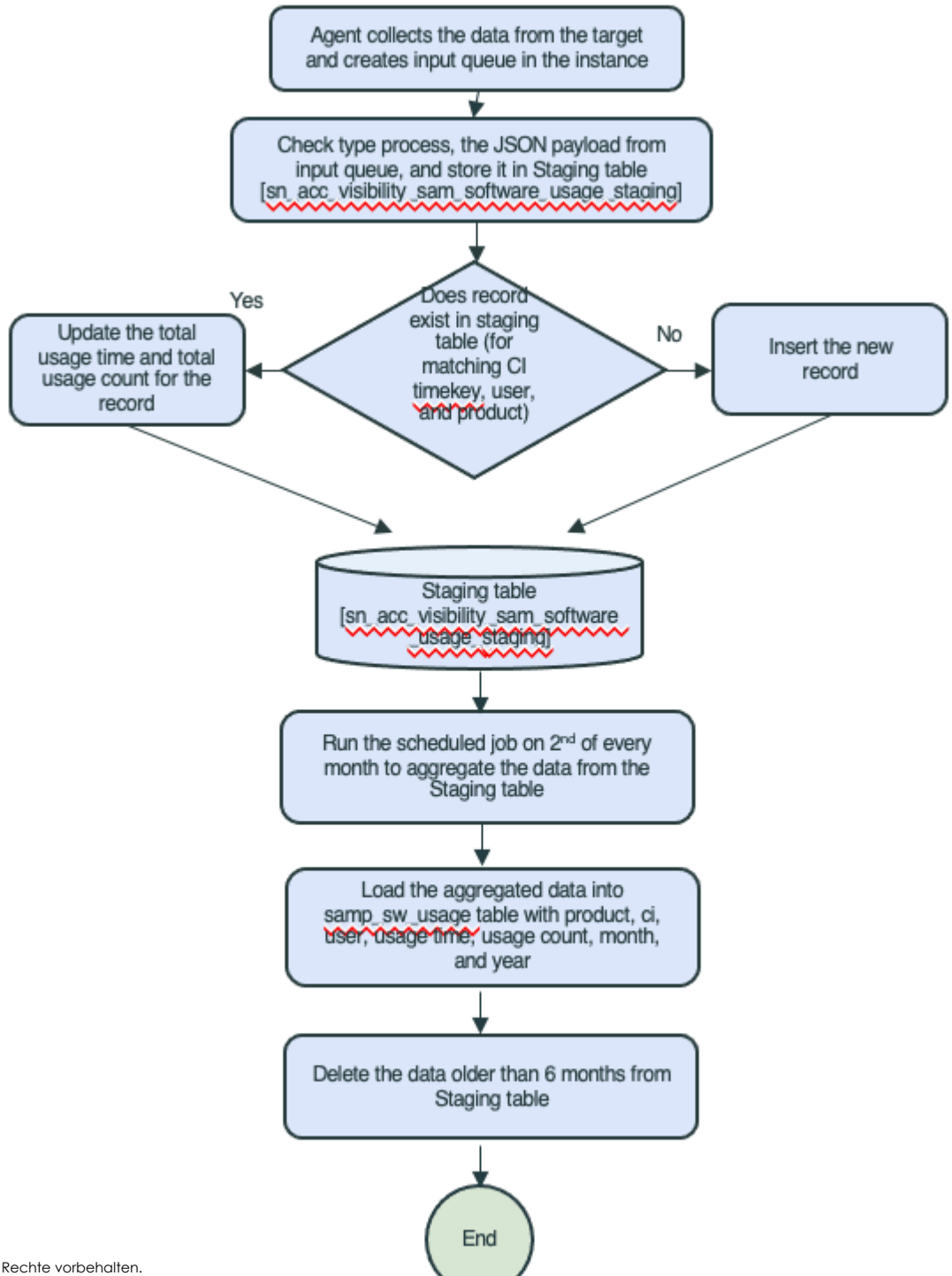
Hinweis: Osquery bietet standardmäßig Unterstützung für die dateisystembasierte Protokollierung. Diese Konfiguration wird bei jeder Neuinstallation von Osquery in der Datei osquery.conf bereitgestellt.

Domäneninformationen können während der Datenerfassung gesammelt werden. Dies kann großen Organisationen mit mehreren Mitarbeiterverzeichnissen helfen, Software dem richtigen Benutzer zuzuordnen. Derzeit wird dies nur für Windows unterstützt. Um die Softwareverwendung/assigned_to dem richtigen Benutzer in einer domänengetrennten Umgebung zuzuordnen, verwenden Sie die Systemeigenschaft [sn_acc_vis_content.column_name_for_user_mapping] mit einem gültigen Feldnamen. Standardmäßig ist der Wert dieser Systemeigenschaft leer. Dies bedeutet, dass nur der Anwendername und nicht die Domäne validiert wird. Sie können eines der folgenden Formate verwenden, um Anwendername und Domäne zu validieren: Anwendername@Domäne oder Domäne\Anwendername.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Flussdiagramm für SAM-Metriken zur Gesamtnutzung

Mithilfe der Liste der Prozesse können Sie eine SAM-Normalisierung durchführen, um die Prozesse für die relevanten installierten Softwaredatensätze zuzuordnen. Dies bietet Flexibilität, da Namen und Prozesse installierter Software normalerweise nicht identisch sind. Fragen Sie zum Beziehen einer Liste der Prozesse in der Nutzlast die Tabelle „Software-Discovery-Modell“ [cmdb_sam_sw_discovery_model] und die Tabelle „Softwareprodukt“ [samp_sw_product] ab, um das entsprechende Produkt und seinen Herausgeber abzurufen. Sobald das Produkt abgerufen wurde, überprüfen Sie, ob die Rückforderungsregel aktiviert ist, damit in der Tabelle „Softwarenutzung“ [samp_sw_usage] die Informationen über die gesamte Nutzungszeit dieses Produkts erhalten bleiben. Einzelheiten können Sie dem Flussdiagramm entnehmen.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

installieren und konfigurieren Sie Osqueryd für Windows mit dem folgenden Skript.

```
# Install latest osquery

$msi = "osquery-5.7.0.msi"
$url = "https://pkg.osquery.io/windows/$msi"
$dst = "$PSScriptRoot\$msi"
Invoke-WebRequest -Uri $url -OutFile $dst
# msiexec /i "$dst" /quiet /qn /norestart
Start-Process msiexec.exe -Wait "/i $dst /quiet /qn /norestart"

# Configure osqueryd service

$flags = "--logger_rotate=true
--logger_rotate_size=26214400
--logger_rotate_max_files=1
--watchdog_level=-1
--config_path=C:\Program Files\osquery\osquery-sam.conf"
Set-Content -Path 'C:\Program Files\osquery\osquery.flags.default' -Value
 "$flags"

$conf = @'
{
  "options": {
    "config_plugin": "filesystem",
    "logger_plugin": "filesystem",
    "utc": "true"
  },
  "schedule": {
    "sam_process_info": {
      "query": "SELECT name, pid, elapsed_time, start_time, user_time,
 system_time, username FROM processes p JOIN users u ON u.uid = p.uid
 WHERE p.elapsed_time != -1 AND u.type != 'special';",
      "snapshot" : true,
      "interval": 300
    },
    "system_info": {
      "query": "SELECT hostname, cpu_brand, physical_memory FROM
 system_info;",
      "interval": 3600
    }
  },
  "decorators": {
    "load": [
      "SELECT uuid AS host_uuid FROM system_info;",
      "SELECT user AS username FROM logged_in_users ORDER BY time DESC
 LIMIT 1;"
    ]
  },
  "packs": {
  }
}
'@
Set-Content -Path 'C:\Program Files\osquery\osquery-sam.conf' -Value
 "$conf"

cd 'C:\Program Files\osquery'
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
.\manage-osqueryd.ps1 -uninstall
.\manage-osqueryd.ps1 -install
Restart-Service osqueryd
```

Einzelheiten zu Windows und macOS finden Sie unter Osqueryd-Zeitplan für SAM-Metriken zur Gesamtnutzung konfigurieren und Osqueryd-Protokolle für SAM-Metriken zur Gesamtnutzung konfigurieren.

Informationen zur Software-Edition

Ab ACC-VC Version 2.3.0 werden Editionsinformationen für Adobe Acrobat und MS SQL Server unterstützt. In zukünftigen Releases wird zusätzliche Software unterstützt. Mit dieser Funktion können SAM-Administratoren die Editionen der installierten Software transparent nachvollziehen. Osquery-Befehle werden dazu verwendet, Informationen über Editionen abzurufen, die dann in der Softwareinstallationstabelle [cmdb_sam_sw_install] in der Spalte „Editionsüberschreibung“ angezeigt werden. Weitere Informationen finden Sie im Support-KB-Artikel https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB0721360 .

Osqueryd-Zeitplan für SAM-Metriken zur Gesamtnutzung konfigurieren

SAM-Gesamtnutzungsmetriken sind abhängig davon, dass auf dem Zielhost der Osqueryd-Service ausgeführt wird. Konfigurieren Sie den Osqueryd-Service, um den erforderlichen Zeitplan für Osquery auf dem Host auszuführen.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Osqueryd-Installationsordner**.
2. Suchen Sie nach der Datei osquery.conf und bearbeiten Sie sie.
3. Fügen Sie das folgende Osquery-Paket unter dem Stichwort packs hinzu.

   Für Windows:

```
"packs": {
      "sam-metering":
 "C:\\ProgramData\\ServiceNow\\agent-client-collector\\cache\
\acc-visibility-modules\\bin\\sam-metering.conf"
  }
```

   Für macOS:

```
"packs": {
    "sam-metering": "/Library/Application\
 Support/servicenow/agent-client-collector/cache/acc-visibility-modul
es/bin/sam-metering.conf"
  }
```

Ergebnisse
Sie können jetzt Osquery-Protokolle für SAM-Metriken zur Gesamtnutzung konfigurieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Osqueryd-Protokolle für SAM-Metriken zur Gesamtnutzung konfigurieren

Standardmäßig unterstützt Osquery die Protokollrotation basierend auf der Größe. Um sie für die SAM-Metriken zur Gesamtnutzung zu aktivieren und die Protokollgröße und -rotation zu konfigurieren, müssen Sie bestimmte Kennzeichnungen für den Osqueryd-Service hinzufügen.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: SAM mit Osqueryd verbraucht Arbeitsspeicher und CPU-Zyklen. Beispiel: Wenn der Agent auf einem Windows-Computer mit 2 CPU-Kernen, 8 GB RAM, 1.000 Softwareinstallationen und 500 laufenden Prozessen installiert ist, wurde Folgendes beobachtet:

- Die durchschnittliche CPU-Auslastung für Agent und Osqueryd betrug weniger als 10 % CPU-Auslastung und maximal 30 % CPU-Auslastung. Dies geschieht nur, wenn die SAM-Hintergrundrichtlinie ausgelöst wird. Standardmäßig erfolgt der Auslöser alle 480 Sekunden.
- Die durchschnittliche Arbeitsspeichernutzung für Agent und Osqueryd war kleiner als 10 MB und es wurden maximal 26 MB verbraucht.

Um die Daten für einen einzelnen laufenden Prozess für zwei Tage zu speichern, sollte die Protokolldateigröße im Durchschnitt 52.429 Byte betragen. Die Protokolldateigröße muss erhöht werden, wenn die Anzahl der laufenden Prozesse auf dem Computer höher ist. Bei 500 laufenden Prozessen würde die Protokollgröße beispielsweise durchschnittlich 25 MB betragen, was 26.214.400 Byte entspricht.

Prozedur

1. Navigieren zu **Osqueryd-Installationsordner**.
2. Suchen Sie nach der Datei osquery.flags und bearbeiten Sie sie.
3. Fügen Sie die folgenden Kennzeichnungen mit diesen Größenrichtlinien hinzu:

   Hinweis: Die Änderung der Protokolldateigröße sollte gemäß den Richtlinien für die Osqueryd-Protokolldateigröße erfolgen.

   Für Windows:

   - --logger_rotate=wahr
   - --logger_rotate_size = 26214400
   - --logger_rotate_max_files=1
   - --watchdog_level = 1

   Für macOS:

   - --logger_rotate=wahr
   - --logger_rotate_size = 26214400
   - --logger_rotate_max_files=1
   - --watchdog_level = 1
   - --logger_mode = 0644
4. Speichern Sie die Datei.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Sobald der Osqueryd-Zeitplan und die Osqueryd-Protokolle konfiguriert sind, kann der Osqueryd-Service gestartet werden.

Der Zeitplan führt die Osquery aus: Wählen Sie „name“, „pid“, „elapsed_time“, „start_time“, „user_time“, „system_time“ und „username“ aus den Prozessen p aus. Verbinden Sie Anwender u AUF u.uid = p.uid wobei p.elapsed_time != -1 UND u.type !='spezial ist „;“ wird alle 5 Minuten (300 Sekunden) auf dem Zielcomputer ausgeführt. Dadurch werden die Ergebnisse in der Protokolldatei protokolliert. Die Protokolldatei enthält Snapshot-Einträge aller Abfragen, die für die Ausführung durch Osqueryd konfiguriert sind. Diese Abfrage enthält alle Prozessattribute.

Hinweis:

Die temporäre Datei *„marker.json* "wird in einem temporären lokalen Ordner auf Ihrem Computer im folgenden Verzeichnis erstellt:

Für Windows `:`<userprofile> \\AppData\\Lokal\\\\AgentClientCollector\\SAM .

Für macOS: `/Library/Application\ Support/servicenow/agent-client-collector`

Diese Datei verfügt über Lese-/Schreibberechtigungen und enthält die Markerdaten: *Data and Last Read Unix Time stamp*.

Osqueryd kann auch so konfiguriert werden, dass die zugehörigen Protokolle in einen benutzerdefinierten Verzeichnispfad anstatt in das Standardverzeichnis geschrieben werden. Wenn Sie ein benutzerdefiniertes Verzeichnis auswählen, ändern Sie die Prüfungsdefinition [samadvanced-background-log-check].

Anwendungsmuster für Agent Client Collector

Anwendungsmuster erfassen Details zu den Anwendungen, die auf dem Host Agent Client Collector (ACC) ausgeführt werden. Anwendungsmuster werden nur für Server unterstützt und nach Abschluss des Agent Client Collector -Hosts Discovery ausgelöst.

Voraussetzungen für die Verwendung von Anwendungsmustern

Um Anwendungsmuster für Agent Client Collectorzu aktivieren, installieren Sie Folgendes:

- Agent Client Collector Framework
- Agent Client Collector Visibility – Inhalt
- Discovery

Legen Sie die Eigenschaft *sn_agent.appl_classification_behavior* auf **„vollständig“**fest, und starten Sie alle MID Servers, die mit dem -Agent verbunden sind, neu.

Wenn Sie in einer Windows -Umgebung arbeiten, vergewissern Sie sich, dass Sie mit PowerShell 3.0 oder höher arbeiten.

Erforderliche Rolle:

- In einer Linux -Umgebung: sudoers-Benutzer (mit Standard- Discovery -Befehlen)
- In einer Windows -Umgebung: servicenow-Benutzer (zur ServiceNow-Benutzergruppe hinzugefügt, mit Berechtigungen für **„Login As a Service“** und **„Programme debuggen** “)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

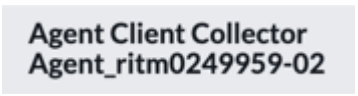
Verwenden der Allow-Listenfunktion für die Musterausführung

Legen Sie den Parameter *enable-patterns-on-agent* in der Datei `acc.yml` auf **„true“** fest. Weitere Informationen finden Sie im Knowledge Base-Artikel KB1585764 .

Unterstützte Anwendungsmuster werden angezeigt

Um die Liste der für Agent Client Collectorunterstützten Muster anzuzeigen, navigieren Sie zu **Alle** > **Musterdesigner** > **Unterstützte Muster für ACC**. Anwendungsmuster sind die einzigen Mustertypen, die für die Verwendung mit Agent Client Collectorunterstützt werden.

Sie können die Anwendungsmuster anzeigen, die auf einem bestimmten Agent ausgeführt wurden.

1. Navigieren zu **Alle** > **Musterdesigner** > **Unterstützte Muster für ACC**.
2. Wählen Sie einen HR-Mitarbeiter aus.
3. Wählen Sie den Namen des 

aus, und halten Sie ihn **Ansicht** > **Discovery**.
4. Wählen Sie die **Registerkarte Anwendungsmusterprotokolle** unten auf der Seite aus.

   Die Liste der auf dem Agent ausgeführten Muster wird angezeigt. Ausgeführte Muster werden in der Spalte Auf Agent ausgeführt mit dem Wert **true** angezeigt.

Nicht unterstützte Anwendungsmustervorgänge

Anwendungsmuster werden in den folgenden Mustervorgängen nicht unterstützt:

- Auslösen der WMI-Methode
- Anwender ändern/Änderung rückgängig machen
- Alle anwenderdefinierten Vorgänge
- SNMP-Abfrage
- Datei speichern

Agent Client Collector Musterausführungseigenschaften

Konfigurieren Sie die folgenden Eigenschaften (**Alle** > **Systemeigenschaften** > **Alle Eigenschaften**), um die Verwendung von Anwendungsmustern mit Agent Client Collectorzu maximieren:

Eigenschaften des Anwendungsmusters

Eigenschaft	Beschreibung
sn_agent.appl_classification_behavior	Legen Sie den Wert auf **„Vollständig“** fest, um die Arbeit mit Anwendungsmustern zu ermöglichen und auf Musterbefehle in der Allow-Liste zuzugreifen. Standard: einfach

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften des Anwendungsmusters (Fortsetzung)

Eigenschaft	Beschreibung
	Hinweis: Um die Ausführung von Anwendungsmustern mit der Allow-Liste zu aktivieren, verwenden Sie die Allow-Listenvorlage für Anwendungsmuster. Einzelheiten hierzu finden Sie im Artikel Musterausführung auf ACC: Beispiel-Allow-Liste für Musterinhalt in der Now Support Knowledge Base.

MID-Server Konfigurationsparametereigenschaften

mid.discovery.agent.command.mid.timeout	Die maximale Dauer in Sekunden, die der MID-Server auf eine Antwort vom Service Desk-Mitarbeiter wartet, bevor eine Zeitüberschreitung auftritt. Standard: 60 Sekunden
mid.discovery.agent.command.timeout	Die maximale Zeit in Sekunden, die der Befehl zur Ausführung auf dem Agent-Host angegeben wird. Standard: 60 Sekunden

Mit Musterdesigner-Debugging im ACC-Modus

Sie können Anwendungsmuster debuggen, die im ACC-Modus konfiguriert werden.

1. Legen Sie die Eigenschaft *sn_agent.appl_classification_behavior* auf **vollständig**fest.
2. Aktivieren Sie im Musterdesigner die Debug-Option, und wählen Sie **ACC-Verbindung verwenden** im Abschnitt Debugging-Identifizierung.

Das Musterprotokoll gibt an, ob das Muster erfolgreich auf dem Agent ausgeführt wurde.

Sie können Musterdetails auch in den folgenden Protokollen empfangen:

- MID-Server Protokolle: Legen Sie *mid.log.level* auf DEBUG fest, damit das MID-Agent-Protokoll Details zum Musterschritt, zur ACC-Prüfung und zur Musterantwort anzeigt.
- ACC-Protokolle: Suchen Sie nach der Zeichenfolge *PatternOnTheFlyCheck*, um Details zu Musterprüfungen zu erhalten.

Oracle Globale GLAS-Datensammlung (Global License Advisory Services)

Anwendungsmuster unterstützen Oracle die GLAS-Datenerfassung in einer Linux -Umgebung. Einzelheiten zur Oracle GLAS-Datenerfassung finden Sie unter Oracle Globale GLAS-Datensammlung (Global License Advisory Services).

Obwohl Oracle GLAS Dateioperationen unterstützt, werden die zugehörigen Dateien mithilfe von Agent Client Collector -Plugins anstelle von SSH oder WMI bereitgestellt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

DNS-Namen mithilfe pushbasierter Erkennung erkennen

CMDB-Verantwortliche sind darauf angewiesen, dass CIs alle Domänensystemnamen (DNS) enthalten, die dem System zugeordnet sind. Ab Agent Client Collector Visibility – Inhalt (ACC-VC) Version 2.3.0 kann ACC-VC DNS-Namenslisten für CIs Windows vom Typ und Linux erkennen.

Bei der Erkennung von DNS-Namen, die Systemen zugeordnet sind, geschieht Folgendes.

- network_adapters.rb wird dazu verwendet, den DNS-Namen für alle IP-Adressen mithilfe von Osquery auszufüllen. (Es gibt keine Begrenzung.)
- Nslookupcommand wird dazu verwendet, den DNS-Namen für alle IP-Adressen abzurufen.

Hinweis: Nslookup muss auf dem Zielsystem konfiguriert sein.

Dadurch wird eine Beziehung *Owns::Owned by* zwischen dem CI und den DNS-Namen erstellt.

Diese Informationen werden dann in die Tabelle [cmdb_ci_dns_name] eingetragen.

Portable Anwendungen mit pushbasierter Erkennung ermitteln

Portable Anwendungen sind Anwendungen, die nicht auf dem Zielsystem installiert werden müssen. Ab ACC-VC Version 2.3.0 kann das pushbasierte Discovery tragbare Anwendungen wie Firefox, VLC, Notepad# usw. nur für Windows erkennen.

Hinweis: Nur portable Anwendungen, die unter https://portableapps.com/ aufgeführt sind, werden unterstützt.

Wenn die portable Anwendung ausgeführt wird, wird ein laufender Prozess erstellt. Von der Anwendung wird ein Pfad ähnlich dem folgenden für die Konfigurationsdatei appinfo.ini erstellt:

```
-\ <--- Directory with FirefoxPortable.exe
 +\App
 +\firefox
 +\Data
 +\profile
 +\settings
 +\plugins\ (optional)
```

Hinweis: Benutzer von ServiceNow-Systemen müssen auf das lokale Konto zugreifen können, um die Daten abzurufen und die Datei appinfo.ini zu lesen.

Die Attribute Name, Version und Lieferant werden aus der portablen Software abgerufen und befinden sich in den appinfo.ini-Dateien. Die Datei appinfo.ini ist die zum Ausführen einer portablen Anwendung zwingend notwendige Datei. Wenn SAM installiert ist, werden die Informationen in der Softwareinstallationstabelle [cmdb_sam_sw_install] angezeigt. Wenn SAM nicht installiert ist, werden die Informationen in der Softwareinstanzentabelle [cmdb_software_instance] angezeigt.

Ausschlusslisten für IP-Adressen und NIC festlegen

Agent Client Collector Visibility – Inhalt (ACC-VC) Version 1.3.0 unterstützt die Ausschlussliste für IPs und Netzwerkschnittstellen-Controller (NICs) mit einem flexiblen Mechanismus zum Herausfiltern von Werten für IPs und/oder NICs beim Erstellen oder Aktualisieren des Host-CI und zugehöriger Elemente.

Die Eigenschaft [*sn_acc_visibility.network_adapter_exclusion_list*] enthält die Liste der regulären Ausdrücke für die Namen und IP-Adressen, die in den Tabellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

„Netzwerkadapter“ und „IP-Adresse“ ausgeschlossen sind. Der Wert dieser Eigenschaft sind durch Kommata getrennte reguläre Ausdrücke. Stellen Sie sicher, dass der reguläre Ausdruck kein Komma enthält. nic und ip_addr sollten in verschiedenen Zeilen stehen.

Beispielformat für den Wert sollte folgendes sein:

- nic = nameRegex1, nameRegex2, nameRegex3
- ip_addr = IPRegex1, IPRegex2

Attribut „Zugewiesen an“ in Computer-CI für ausfüllen Agent Client Collector Visibility – Inhalt

Um das Attribut „Zugewiesen an“ des Computer-CI zu aktualisieren, müssen Sie Informationen vom angemeldeten Benutzer sammeln.

Vorbereitungen

Erforderliche Rolle: Administrator

Sie können Zugewiesen an für Windows -Endpunktgeräte und macOS -Geräte, wie Workstations oder Mitarbeiter-Laptops, als Teil der agentenbasierten Discovery mit ACC-VC automatisch mit den folgenden beiden Systemeigenschaften ausfüllen. Weitere Informationen finden Sie unter Verfügbare Systemeigenschaften .

- **sn_acc_vis_content.set_assigned_to**
- **sn_acc_vis_content.assigned_to_user_order**

Prozedur

1. Erstellen Sie höhere Anwenderberechtigungen, um die Details des angemeldeten Anwenders abzurufen.
   Verwenden Sie „Als lokaler Systemanwender anmelden“ anstelle des Standardanwenders ServiceNow für die Ausführung von Agent Client Collector.

   Diese Befehle werden auf dem Computer Windows ausgeführt:

   - wmic COMPUTERSYSTEM GET USERNAME
   - Über osquery: SELECT l.user FROMlogged_in_users l Join users u ON l.sid = u.uuid WHERE u.type != 'spezial'

   Der folgende Befehl wird auf dem Computer macOS ausgeführt: SELECT Distinct(l.user) FROMlog_in_users l Join users u ON l.user = u.username

2. Der Abgleich der Anwendernamen wird für die Anwenderdatensätze in der Tabelle „sys_user“ durchgeführt.
   Das Attribut „Zugewiesen an“ wird ausgefüllt, und dann wird ein Verweis auf den Benutzer erstellt. Systemprotokolle zeigen eine Warnung an, wenn in „sys_user“ kein Anwender gefunden werden kann. Die für das Attribut „Zugewiesen an“ bezogenen Anwendernamen basieren auf der folgenden Systemeigenschaft: **sn_acc_vis_content.assigned_to_user_order**.
3. Das Attribut Assigned_to wird basierend auf Prioritäten festgelegt.
   Wenn assigned_to bereits vorhanden ist, behalten Sie standardmäßig bei. Sie können jedoch die Systemeigenschaft **sn_acc_vis_content.set_assigned_to** aktualisieren, um sie zu überschreiben. Wenn Abgleichsregeln definiert sind, füllt die IRE das Feld entsprechend aus.

Ergebnisse

In der Tabelle „sys_user“ wird kein neues Anwenderaccount erstellt. Stattdessen wird der vorhandene Benutzer abgefragt und als Zugewiesen an-Benutzer für ein CI referenziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausfüllen von Anwendern basierend auf Typ für Agent Client Collector Visibility – Inhalt

Sie können den Typ der Benutzer, die die CMDB füllen, abhängig von Ihren speziellen Interessen beibehalten. Derzeit werden „local“ und „system“ für Windows, Linuxund macOSunterstützt.

Sie können die Benutzertypen mithilfe der folgenden Systemeigenschaft filtern: **sn_acc_visibility.persist_os_user_type**. Weitere Informationen finden Sie unter Verfügbare Systemeigenschaften .

Für Windows

Sie müssen feststellen, ob ein Server ein Domänencontroller ist oder nicht. Da Domänencontroller-Computer keine lokalen Konten haben, werden lokale Anwenderinformationen für solche Computer nicht beibehalten und nicht ausgefüllt.

Verwenden Sie für Windows-Computer ohne Domänencontroller OSquery-Befehle, um Anwenderinformationen über ACC-VC abzurufen: Wählen Sie *uid*, *Anwendername*, *Verzeichnis*, *Typ* aus Anwendern aus, wobei **Typ = Lokal** oder **Typ = Spezial**.

Für Linux

Die userID definiert, ob ein Benutzer ein lokaler Account oder ein Systemaccount ist. Dies wird durch *UID_MIN* und *UID_MAX* definiert.

Verwenden Sie diesen Befehl, um Anwenderinformationen über ACC-VC abzurufen und den Wert *UID_MIN* und *UID_MAX* abzurufen: `grep -E '^UID_MIN|^UID_MAX' /etc/login.defs`.

Verwenden Sie diesen Befehl, um Anwendernamen abzurufen: `cat /etc/passwd | awk -F':' '{print $1,$3,$6}`.

Für macOS

Verwenden Sie OSquery-Befehle, um Anwenderinformationen über ACC-VC abzurufen: *uid*, *Anwendername*, *Verzeichnis* aus Anwendern auswählen. Anwendernamen, denen „_“ vorangestellt wird, werden als System-Accounts behandelt. Andere sind lokale Konten.

Cloud Native Operations für Transparenz

Cloud Native Operations für Transparenz (CNO für Transparenz) wurde Agent Client Collector für Kubernetes – Transparenzin umbenannt. Der Begriff Cloud Native Operations für Transparenz wurde als veraltet markiert.

Die Dokumentation Agent Client Collector für Kubernetes – Transparenz finden Sie unter Agent Client Collector für Kubernetes – Transparenz.

Agent Client Collector Visibility – Inhalt – Referenz

Die folgenden Informationen enthalten Details zu Abfrageskripts des Betriebssystems, zu erfassten Daten und zur Definition von Begriffen.

BS-Modulskripts für Agent Client Collector Visibility – Inhalt (ACC-VC)

Diese plattformspezifischen Plugins rufen plattformspezifische Modulskripts auf. Jedes Skript gibt an eine JSON-Standardnutzlast unabhängig von der Plattform aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betriebssystemfamilie/Plugin	Name des Modulskripts
Linux: acc-f-modules	basic_inventory.rb (Ab ACC-F Version 2.10.1 wird dieses Modulskript nicht mehr verwendet.)
	data_collection.rb
	running_processes.rb
	tcp_connections.rb
Windows: acc-f-modules	basic_inventory.rb (Ab ACC-F Version 2.10.1 wird dieses Modulskript nicht mehr verwendet.)
	data_collection.rb
	running_processes.rb
	tcp_connections.rb
macOS-Betriebssysteme: acc-f-modules	basic_inventory.rb (Ab ACC-F Version 2.10.1 wird dieses Modulskript nicht mehr verwendet.)
	running_processes.rb
	tcp_connections.rb
Linux: acc-visibility-modules	installed_software.rb
	file_systems.rb
	storages_devices.rb (nur Unterstützung zum Abrufen von physischen Datenträgern und entsprechenden Datenträgerpartitionen)
	network_adapters.rb
	local_users.rb
	enhanced_inventory.rb
	cloud.rb
Windows: acc-visibility-modules	installed_software.rb
	file_systems.rb
	storages_devices.rb (nur Unterstützung zum Abrufen von physischen Datenträgern und entsprechenden Datenträgerpartitionen)
	network_adapters.rb
	local_users.rb
	enhanced_inventory.rb
	cloud.rb
	sam_advanced.rb
	sam_processor.rb
	intel_ema.rb

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betriebssystemfamilie/Plugin	Name des Modulskripts
macOS-Betriebssysteme: acc-visibility-modules	installed_software.rb
	file_systems.rb
	storages_devices.rb (nur Unterstützung zum Abrufen von physischen Datenträgern und entsprechenden Datenträgerpartitionen)
	network_adapters.rb
	local_users.rb
	enhanced_inventory.rb
	cloud.rb

Hinweis:

running_processes.rb und tcp_connections.rb sind voneinander abhängig. Daher sollten Sie für eine effiziente Discovery sowohl tcp_connection.rb als auch running_processes.rb beibehalten. Beide Dateien werden benötigt, um vollständige Daten zu erhalten. Wenn eine nicht vorhanden ist, sind die entsprechenden Daten nicht verfügbar.

Um Informationen zu allen running_processes auf dem macOS abzurufen, müssen Sie sudo-Zugriff für osquery bereitstellen. Wenn diese Konfiguration nicht vorgenommen wird, wird von running_processes.rb nur das abgerufen, was vom _servicenow-Benutzer ausgelöst wird. Für tcp_connections.rb müssen Sie in der Datei „sudoers“ den Befehl „sudo lsof“ hinzufügen. Wenn diese Konfiguration nicht vorgenommen wird, wird von tcp_connections.rb nur das abgerufen, was vom _servicenow-Benutzer ausgelöst wird.

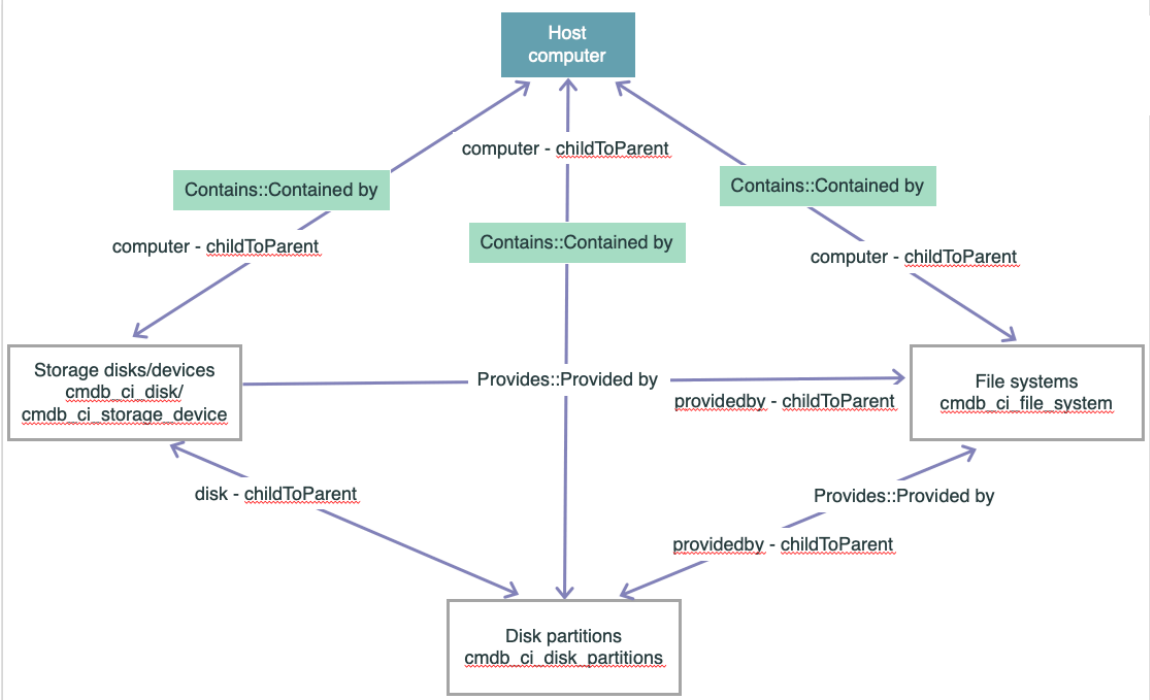
Erfasste Daten

ACC-VC verwendet für die Klassifizierung als Computer oder Server dieselben Klassifizierungskriterien wie IP-basiert Discovery. Die Teilmenge der erfassten Daten umfasst die folgenden Kategorien:

- Basisbestand – Ab ACC-F Version 2.10.1 wird diese Kategorie nicht mehr verwendet.
- Datensammlung – Sammelt die erforderlichen Daten für die Klassifizierung und Identifizierung eines Host-CI. Dazu gehören Hostname, Seriennummern und Betriebssysteminformationen.
- Installierte Software – cmdb_sam_sw_install (wenn SAM aktiviert ist) und cmdb_software_instance (wenn SAM nicht aktiviert ist)
- Dateisystem – cmdb_ci_file_system
- Speichergeräte – cmdb_ci_disk und cmdb_ci_storage_device
- Seriennummern – cmdb_serial_number
- Netzwerkadapter – cmdb_ci_network_adapter und cmdb_ci_ip_address
- TCP-Verbindungen – cmdb_tcp
- Laufende Prozesse – cmdb_running_process (ACC-VC klassifiziert auch die laufenden Prozesse und erstellt Anwendungs-CIs, sofern möglich, in „cmdb_ci_appl“).
- Lokaler Anwender – cmdb_os_user (füllt die lokalen Anwender für alle von ACC-VC unterstützten Betriebssysteme aus, indem ein neues Modul namens „local_user“ hinzugefügt wird)
- Erweiterter Bestand – Sammelt erweiterte Daten (z. B. CPU-Informationen, start_date, object_id), die zum Identifizieren eines eindeutigen Hosts nicht erforderlich sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beziehungen zwischen Hostcomputer, Dateisystemen und Speichergeräten



Agent Client Collector Begriffe

Agent Client Collector (ACC)

Die auf Zielhosts installierte Softwarekomponente, die mit dem MID-Server kommuniziert. Wird manchmal auch als Agent bezeichnet. Diese Komponente ist ein ServiceNow-Derivat von Sensu-Go.

Agent Client Collector Framework (ACC-F)

Eine bereichsbezogene Basisanwendung ServiceNow, die ACC nutzt und Kernfunktionen (einschließlich Prüfungstypen, Prüfungsdefinitionen, Richtlinien usw.) bereitstellt, die andere bereichsbezogene ACC-Anwendungen wie ACC-M und ACC-VC unterstützen.

Agent Client Collector-Überwachung Überwachung (ACC-M)

Eine bereichsbezogene ServiceNow-Anwendung, die die Überwachung von Anwendungsfällen ermöglicht.

Agent Client Collector Visibility – Inhalt (ACC – VC)

Eine bereichsbezogene ServiceNow-Anwendung, die pushbasierte Discovery mit ACC und ACC-F implementiert.

Horizontal IP-basiert Discovery

Herkömmliches Discovery für Kunden vor ACC-VC verfügbar. Dabei werden Daten über Probes und Muster durch den MID-Server erkannt. Hierzu ist das Plugin „Discovery“ erforderlich.

Module

Teilmenge der erkannten Daten, die im Rahmen der Discovery gefüllt werden. Beispiele für Module: Datensammlung, Installierte Prozesse, Seriennummern, Dateisysteme, Speichergeräte, Netzwerkadapter, Laufende Prozesse und TCP-Verbindungen.

Pushbasierte Discovery

Erkennen Sie Daten über ACC, ACC-F, ACC-VC und MID-Server mit einem direkten Push von Daten vom Zielhost. Discovery erfordert keine bestimmte IP-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bereichskonfiguration in einem Discovery Zeitplan oder die Bereitstellung von Discovery Anmeldeinformationen für den Zielhost.

Sensu-Go-Agent

Das kostenlose Open Source-Projekt, aus dem ACC abgeleitet ist.

VM-Instanz

Ein virtueller Zielhost, der innerhalb eines Hypervisor ausgeführt wird, entweder lokal oder innerhalb eines Cloud Service Providers wie AWS, GCP oder Microsoft Azure.

VM-Abbild

In einem Dateisystem oder Cloud-Speicher abgelegter Snapshot der Live-Instanz einer virtuellen Maschine (VM).

Agent Client Collector Visibility – Inhalt – Standardprüfungen und Richtlinien

Agent Client Collector Visibility – Inhalt (ACC-VC) bietet verschiedene Prüfungen und Richtlinien sowie eine Geschäftsregel.

Richtlinien

Hinweis: ACC-VC-Richtlinien werden mit einer Häufigkeit von einmal pro Tag ausgeführt. Die insgesamt erfasste Datenmenge beträgt etwa 572 KB. Dabei werden durchschnittlich etwa 1.500 installierte Softwareanwendungen und etwa 500 laufende Prozesse (mit Ausnahme von CI-Daten) pro Computer berücksichtigt.

ACC-VC-Richtlinien

Name	Beschreibung	Überprüfungen
Erweiterte Erkennung	Wird nach einem Zeitplan ausgeführt, standardmäßig alle 24 Stunden (86.400 Sekunden). Das Richtlinienintervall kann angepasst werden, z. B. so, dass es alle 4 Stunden ausgeführt wird (setzen Sie das Intervall auf 14.400). Die ACC-VC-Richtlinienkonfiguration wird basierend auf dem von ACC-VC definierten Richtlinienfilter mit allen Agents synchronisiert. Aktualisieren Sie bei Bedarf die folgenden ACC-F-Systemeigenschaften: • *sn_agent.disco_minimum_threshold_for_rediscovery_minutes*:, um zu vermeiden, dass das System zu häufig erkannt wird.	Erweiterte Erkennung

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC-VC-Richtlinien (Fortsetzung)

Name	Beschreibung	Überprüfungen
	• *sn_agent.disco_disable_ci_clobber_of_agentless_disco*: um Discovery -Konflikte zu vermeiden. • *sn_agent.disco_ci_clobber_of_agentless_disco_threshold_days*: um Discovery -Konflikte zu vermeiden.	
SAM-Discovery	Verantwortlich für das Erfassen der Software, die auf einem Endpunktgerät installiert ist, z. B. Windows -Desktops oder macOS -Server.	Windows SAM-Hintergrundprotokollprüfung
SAM-Hintergrund	Aktiviert einen Hintergrundauftrag für die Verarbeitung der Osqueryd-Protokolle für SAM auf den Endpunktgeräten Windows und macOS.	Windows Softwareinstallationen und -verwendungsmetriken
Software installiert	Verantwortlich für die Erfassung der auf allen Geräten mit Ausnahme von Windows -Endpunktgeräten installierten Software. Die erfassten Daten werden in der Tabelle [cmdb_sam_sw_install] gespeichert. Geplante Ausführung alle 24 Stunden.	installierte Software
Hintergrundrichtlinie für dateibasierte Discovery	Übernimmt die Konfigurationsdatei als Eingabe von der Instanz zu einem Agent. Scannt das System anhand von Konfigurationsdateiparametern und speichert die Ausgabe auf dem Agent. Wird auf dem Agent ausgeführt, wenn die dateibasierte Discovery aufgerufen wird. Details finden Sie unter File-based Discovery.	Hintergrund der dateibasierten Discovery
Richtlinie für dateibasierte Discovery	Sammelt die Ausgabedatei vom Agent. Sendet die gesammelten Informationen an die Konfigurationstabellen.	Dateibasierte Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC-VC-Richtlinien (Fortsetzung)

Name	Beschreibung	Überprüfungen
	Wird auf dem Agent ausgeführt, wenn die dateibasierte Discovery aufgerufen wird. Details finden Sie unter File-based Discovery. **Hinweis:** • Während der dateibasierten Discovery auf einem Windows -System verfügt der ServiceNow-Benutzer nicht über die erforderlichen Berechtigungen. Erteilen Sie daher manuell die Berechtigung zum Auflisten von Ordnerinhalten für den Ordner, den Sie scannen möchten. • Um sicherzustellen, dass die Dateiversion erfolgreich abgerufen werden kann, führen Sie den Agent als lokaler Systemkontobenutzer anstelle des Benutzers *servicenow* aus.	

Hinweis: Windows-Endpunktgeräte umfassen Geräte mit einem Windows-Betriebssystem, die zur Klasse „Computer“ gehören.

Weitere Informationen finden Sie unter Systemeigenschaften . Weitere Informationen zu Richtlinien finden Sie unter Prüfungen und Richtlinien.

Überprüfungstyp

ACC-VC besitzt die folgenden Prüfungstypen: *EnhancedDiscovery*, *SAM Advanced Discovery*und *Installed Software*.

EnhancedDiscovery

Dieser Überprüfungstyp ist für den Aufruf der Skripteinbindung EnhancedDiscoveryHandler verantwortlich, die die von endpoint_discovery.rb generierte Nutzlast verarbeitet, wie sie von ACC ausgeführt wird.

SAM Advanced Discovery

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Prüfungstyp gilt für die SAM-Discovery-Richtlinie, die die Skripteinbindung EnhancedDiscoveryHandler für die Verarbeitung der von der Datei „sam_advanced.rb“ erstellten SAM-Daten aufruft.

Installed Software

Dieser Überprüfungstyp ist für die *Software installed policy* vorgesehen, nach der die Skripteinbindung EnhancedDiscoveryHandler zur Verarbeitung der Daten über die installierte Software aufgerufen wird, die von der Datei installed_software.rb erzeugt werden.

Prüfungsdefinitionen

ACC-VC-Prüfungsdefinitionen

Name	Beschreibung

Erweiterte Erkennung	Wird basierend auf dem von ACC-VC definierten Richtlinienfilter mit allen Agents synchronisiert. Die Prüfungsdefinition ist für die Ausführung mit bestimmten Assets konfiguriert und bestimmt, was zwischen dem -Service Desk-Mitarbeiter und MID-Serversynchronisiert wird. Weitere Informationen zu Richtlinien finden Sie unter Prüfungen und Richtlinien.
	Hinweis:
	Damit der Agent die Betriebssystem-Seriennummern und TCP-Verbindungen zusammen mit den zugehörigen laufenden Prozessen abrufen kann, ist auf Systemen Linux ein sudo-Zugriff für „dmidecode“ und „ss“ erforderlich. Zum Beispiel kann dies zu /etc/sudoers oder zu einer einzelnen Datei in `/etc/sudoers.d/` hinzugefügt werden:
	`Cmnd_Alias AGENT_ACC_V = /usr/sbin/dmidecode -s baseboard-serial-number,/usr/sbin/dmidecode -s chassis-serial-number,/usr/sbin/dmidecode -s system-serial-number,/usr/sbin/dmidecode -s system-uuid,/usr/sbin/ss -tanp`
	`servicenow ALL=(root) NOPASSWD:AGENT_ACC_V`

SAM-Hintergrundprotokollprüfung	Wird alle 8 Minuten ausgeführt und führt eine Inline-Zusammenfassung der aus Osqueryd-Protokollen generierten Daten durch. Nach dem Sammeln der Daten werden alle Zwischendatenergebnisse in eine temporäre Markierungsdatei geschrieben, die bei der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC-VC-Prüfungsdefinitionen (Fortsetzung)

Name	Beschreibung
	nächsten Ausführung wiederverwendet wird. Diese Wiederverwendung begrenzt die Anzahl der Protokolldateien und den erforderlichen Speicherplatz auf den Zielsystemen. **Hinweis:** Möglicherweise stellen Sie eine Spitze beim Systemressourcenverbrauch fest, da die Prüfung der Hintergrundzusammenfassung in jedem Intervall ausgeführt wird.
Softwareinstallationen und Nutzungsmetriken	Erfasst alle 24 Stunden Daten.
Installierte Software	Ruft Daten der installierten Software für alle Geräte mit Ausnahme der Endpunktgeräte Windows und macOS ab.
Hintergrund der dateibasierten Discovery	Ruft die Dateidaten vom Agent ab.
Dateibasierte Discovery	Führt einen Hintergrundauftrag zum Scannen von Dateien auf dem Agent aus.

Business-Regel

Die Geschäftsregel *Enhanced Discovery - On CI Delete* löst die Endpunkterkennungsprüfung aus, wobei das einem bestimmten CI zugeordnete CI aus sn_agent_cmdb_ci_agent gelöscht wird.

Agent Client Collector Parameter des Installationsbefehls bei Verwendung von ITOM Cloud-Services

Beschreibung der Befehlszeilenparameter, die bei der Installation Agent Client Collector von mithilfe von ITOM Cloud Services verwendet werden.

Befehlszeilenparameter für die Installation

Parameter	Beschreibung
VERBINDEN_OHNE_MID	Geben Sie **„wahr“** an, um ITOM Cloud-Services zu aktivieren. Wenn Sie keinen Wert angeben, wird die reguläre Websocket-Installation MID-Server aufgerufen. Einzelheiten zur Konfiguration eines Websocket auf dem MID-Serverfinden Sie unter Websocket-Server auf MID-Server installieren.
ACC_CNC	Geben Sie einen öffentlichen Gateway-Endpunkt für Agent Client Collectoran.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Befehlszeilenparameter für die Installation (Fortsetzung)

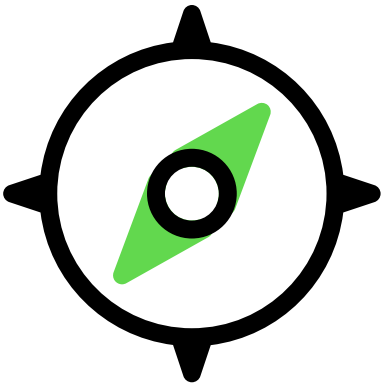
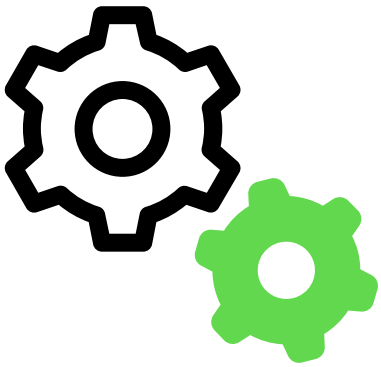
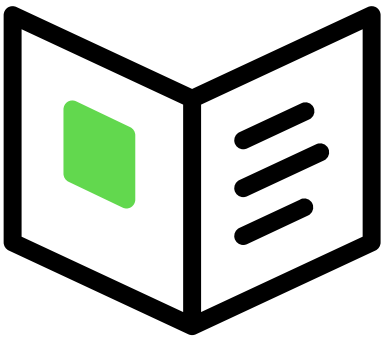
Parameter	Beschreibung
REGISTRATION_KEY	Aktiver und gültiger Registrierungsschlüssel, mit dem der Service Desk-Mitarbeiter kommunizieren soll.
INSTANCE_URL	ServiceNow Instanz, bei der der Agent registriert ist.
ACC_ALLOW_LIST	Optionale Zeichenfolge; Um die Allow-Liste zu deaktivieren, legen Sie *ACC_ALLOW_LIST=0* fest. Die Allow-Liste ist standardmäßig aktiviert. **Hinweis:** Das Deaktivieren der Allow-Liste beeinträchtigt die Sicherheit Ihres Systems und ist als vorübergehende Maßnahme gedacht, während Sie die Allow-Liste aktualisieren. Aktivieren Sie nach Abschluss des Updates die Allow-Liste, indem Sie **ACC_ALLOW_LIST=1** festlegen.
ACC_VALIDATE_SIG	Optionale Zeichenfolge; Um die Überprüfung der Validierung der Zertifizierung durch das Installationsprogramm zu deaktivieren, legen Sie den Wert *ACC_VALIDATE_SIG=0* fest, den Sie hinzufügen können, um die Überprüfung der Validierung der Zertifizierung durch das Installationsprogramm zu deaktivieren. Die Validierung ist standardmäßig aktiviert. **Hinweis:** Deaktivieren Sie die Zertifizierungsvalidierung nur, wenn Sie nicht standardmäßige Signaturvalidierungstools verwenden.

Agent Client Collector für Kubernetes – Transparenz

Agent Client Collector für Kubernetes – Transparenz erkennt Änderungen an Ressourcen in einem Kubernetes -Cluster. Es führt eine kontinuierliche Discovery durch, meldet Changes an Ihre Instanz zurück und aktualisiert Configuration Management Database (CMDB) mit den neuesten Daten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Konfigurieren	Referenz
		
Allgemeiner Überblick über Agent Client Collector für Kubernetes – Transparenz.	Agent Client Collector für Kubernetes – Transparenz Installations- und Konfigurationsaufgaben.	Referenzinformationen, wie z. B. gesammelte Daten, die Agent Client Collector für Kubernetes – Transparenz -Supportmatrix und erweiterte Konfigurationsoptionen.

Hilfreiche Ressourcen

Einige ServiceNow -Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

- ServiceNow Community
  ServiceNow Community
- Customer Success Center
  Customer Success Center
- Entwickler
  developer.servicenow.com
- Impact
  http://impact.servicenow.com
- ServiceNow University
  ServiceNow University
- NowCreate
  Now Create
- Partner
  https://www.servicenow.com/partners.html
- ServiceNow

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

https://www.servicenow.com/

ServiceNow Store

ServiceNow Store

Unterstützung

- https://support.servicenow.com/now
- Known Error-Portal

Agent Client Collector für Kubernetes – Transparenz erkunden

Agent Client Collector für Kubernetes – Transparenz ermöglicht Ihnen Einblick in lokale Kubernetes -Cluster sowie in die folgenden Cloud-Bereitstellungen: Amazon Elastic Kubernetes Service (EKS), Google Kubernetes Engine (GKE), Azure Kubernetes Engine (AKS), Red Hat OpenShiftund Rancher.

Agent Client Collector für Kubernetes – Transparenz erkennt Änderungen an Ressourcen in einem Kubernetes -Cluster. Es führt eine kontinuierliche Discovery durch, meldet Changes an Ihre Instanz zurück und aktualisiert Configuration Management Database (CMDB) mit den neuesten Daten.

Funktionsweise

Wenn Sie Agent Client Collector für Kubernetes – Transparenzbereitstellen, erstellt Kubernetes eine Bereitstellungsressource im Cluster. Diese Ressource verwendet ein in Kubernetes gespeichertes Geheimnis, um eine Verbindung zu Ihrer Instanz ServiceNow herzustellen.

Die Bereitstellungsressource Agent Client Collector für Kubernetes – Transparenz enthält einen Pod namens „Informer“, der eine Verbindung zum API-Server Kubernetes herstellt und von ihm Ereignisse für die Ressourcen im Cluster empfängt. Der Informer sendet die gesammelten Daten über die ECC-Warteschlangentabelle (External Communication Channel) an die Instanz. Er verwendet die Tabellen-API ServiceNow, um aus der Warteschlange zu lesen und in die Warteschlange zu schreiben. Der Informer aktualisiert dann die entsprechenden Tabellen in CMDB.

Hinweis: Wenn der Informer die Changes nicht melden kann, z. B. aufgrund eines Netzwerkproblems, werden die Ressourcen, die dem Cluster während des Ereignisses hinzugefügt wurden, nach dem nächsten vollständigen Discovery-Zyklus zu CMDB hinzugefügt. Die Ressourcen, die während des Ereignisses aus dem Cluster entfernt wurden, werden als Abwesend markiert und nach zwei vollständigen Discovery-Zyklen gelöscht.

Weitere Informationen zu den Ressourcen Kubernetes, für die der Informer Daten sammelt, und den Tabellen CMDB, die er füllt, finden Sie unter Durch Agent Client Collector für Kubernetes – Transparenz erfasste Daten.

Anfängliche und regelmäßige Discovery

Bei seiner ersten Discovery findet der Informer alle Ressourcen im Cluster Kubernetes und meldet sie an Ihre Instanz. Alle 30 Sekunden sendet der Informer bis zu 1 MB Daten an die -Instanz. Es dauert normalerweise bis zu zwei Minuten, um Daten in einem Cluster mit 1.000 Pods zu melden, und eine weitere Minute für jede weiteren 1.000 Pods. Ein einzelner Informer-Pod kann einen Cluster mit zehntausenden Pods verarbeiten. Wenn der Informer aus irgendeinem Grund beendet wird, wird er von Kubernetes automatisch neu gestartet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der ersten Discovery überwacht der Informer kontinuierlich das Hinzufügen, Aktualisieren und Löschen von Ressourcen im Cluster. Ressourcen, die aus dem Cluster gelöscht wurden, werden mit „install_status=Abwesend“ markiert und innerhalb von Stunden im Rahmen einer regelmäßigen Bereinigung aus dem CMDB gelöscht.

Auswirkung des Informers auf den Kubernetes API-Server

Der Informer hat minimale Auswirkungen auf den API-Server Kubernetes. Die vollständige Liste der relevanten Ressourcen wird nur einmal abgerufen und im Arbeitsspeicher gespeichert. Von da an wird eine Synchronisierung mit dem API-Server Kubernetes durchgeführt, und die vollständige Liste wird nie mehr abgerufen. Während der regelmäßigen und bedarfsgesteuerten vollständigen Discovery-Zyklen sendet der Informer die gespeicherte Liste der Ressourcen erneut an die Instanz.

Agent Client Collector für Kubernetes – Transparenz Leistungs- und Skalierbarkeits-Benchmark

Informationen zu Agent Client Collector für Kubernetes – Transparenz -Benchmarks finden Sie im Artikel Leistungsergebnisse für CNO für Transparenz [KB1555851] in der Knowledge Base Now Support.

Agent Client Collector für Kubernetes – Transparenz konfigurieren

Richten Sie Agent Client Collector für Kubernetes – Transparenz ein, indem Sie die beschriebenen Schritte ausführen.

Informationen zu erweiterten Konfigurationsoptionen finden Sie im Artikel Administrating and Troubleshooting CNO for Visibility (Cloud-Native-Operations) [KB1532614] in der Knowledge Base Now Support.

Bereiten Sie die Bereitstellung von Agent Client Collector für Kubernetes – Transparenz vor

Bereiten Sie Ihre Instanz ServiceNow und den Cluster Kubernetes auf die Bereitstellung Agent Client Collector für Kubernetes – Transparenz vor.

Vorbereitungen

- Stellen Sie sicher, dass die folgenden Anwendungen installiert und aktiviert sind:
  - Muster für Discovery und Service-Mapping
  - Die neueste Version von Agent Client Collector Visibility – Inhalt
- Stellen Sie sicher, dass das Befehlszeilentool Kubernetes kubectl installiert und für die Kommunikation mit Ihrem Cluster konfiguriert ist. Weitere Informationen finden Sie in der Kubectl -Dokumentation.
- Wenn Sie ein Helm-Diagramm für die Installation verwenden möchten, stellen Sie sicher, dass das Tool „Helm“ verfügbar ist. Weitere Informationen finden Sie in der Helm-Dokumentation.

Erforderliche Rolle: admin für Schritte, die in der Instanz ServiceNow ausgeführt werden.

Prozedur

1. Navigieren Sie in der Instanz ServiceNow zu **Alle** > **Anwenderadministration** > **Anwender**.
2. Wählen oder erstellen Sie einen Anwender mit mindestens der Rolle discovery_admin. Informationen zum Hinzufügen neuer Benutzer zu Ihrer -Instanz finden Sie unter Einen Benutzer erstellen . Informationen zum Gewähren des Erteilens von Rollen an einen Benutzer finden Sie unter Einem Benutzer eine Rolle zuweisen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen oder erstellen Sie im Cluster Kubernetes einen Namespace, in dem Sie Agent Client Collector für Kubernetes – Transparenzbereitstellen möchten.
   So erstellen Sie einen Namespace:
   a. Öffnen Sie das Befehlszeilentool kubectl.
   b. Führen Sie den folgenden Befehl aus, nachdem Sie NAMESPACE durch den entsprechenden Wert ersetzt haben:

      ```
      Kubectl – Namespace erstellen NAMESPACE
      ```

4. Erstellen Sie ein Kubernetes -Geheimnis, das die ServiceNow -Anmeldeinformationen für den Zugriff auf Ihre ServiceNow -Instanz enthält.

   Hinweis: Stellen Sie sicher, dass die Anmeldeinformationen dem Benutzer entsprechen, den Sie im vorherigen Schritt erstellt oder identifiziert haben.

   a. Öffnen Sie das Befehlszeilentool kubectl.
   b. Führen Sie den folgenden Befehl aus, nachdem Sie INSTANCE_NAME, USERNAME, PASSWORD und NAMESPACE durch die entsprechenden Werte ersetzt haben:

      ```
      kubectl create secret generic k8s-informer-cred-INSTANCE_NAME
       --from-literal=.user=USERNAME --from-literal=.password=PASSWORD -n
       NAMESPACE
      ```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Wenn der Informer über einen Proxy-Server eine Verbindung zur Instanz ServiceNow herstellt, können Sie den Proxy-Anwender und das Passwort bereitstellen, indem Sie dem Geheimnis die Schlüssel .proxyUser und .proxyPassword hinzufügen. Zum Beispiel:

```
kubectl create secret generic k8s-informer-cred-INSTANCE_NAME
 --from-literal=.user=USERNAME --from-literal=.password=PASSWORD
 --from-literal=.proxyUser=PROXY_USER
 --from-literal=.proxyPassword=PROXY_PASSWORD -n NAMESPACE.
```

  Wenn Sie „.proxyUser“ nicht angeben, geht Agent Client Collector für Kubernetes – Transparenz davon aus, dass eine Authentifizierung nicht erforderlich ist. Wenn Sie .proxyUser, aber nicht .proxyPassword angeben, gibt das System einen Fehler in den Protokollen zurück und bricht den Informer ab.

- Wenn Ihre Organisation Amazon Elastic Kubernetes Service (EKS)verwendet, können Sie das Geheimnis im AWS Geheimnismanager speichern. Der Informer ruft dann die ServiceNow -Anmeldeinformationen für den Zugriff auf Ihre Instanz aus dem AWS -Geheimnismanager ab. Weitere Informationen finden Sie im Artikel CNO für Transparenz: Speichern der Instanzanmeldeinformationen im AWS Secrets Manager [KB1581074] in der Knowledge Base Now Support.
- Wenn Ihre Organisation den Azure-Service Kubernetes (AKS) verwendet, können Sie das Geheimnis im Key Vault Microsoft Azure speichern. Der Informer ruft dann die Anmeldeinformationen ServiceNow für den Zugriff auf Ihre Instanz aus dem Azure Key Vault ab. Weitere Informationen finden Sie im Artikel Stornieren der Instanzanmeldeinformationen in Microsoft Azure Key Vault [KB1647736] in der Knowledge Base Now Support.
- Wenn Ihre Organisation Google Kubernetes Engine (GKE)verwendet, können Sie das Geheimnis im Geheimnismanager Google Cloud speichern. Der Informer ruft dann die ServiceNow -Anmeldeinformationen für den Zugriff auf Ihre Instanz vom Google Cloud -Geheimnismanager ab. Weitere Informationen finden Sie im Artikel CNO für Transparenz: Stornieren von Anmeldeinformationen in Google Cloud Secret Manager [KB1709597] in der Knowledge Base Now Support.
- Wenn Ihre Organisation eine anwenderdefinierte Stammzertifizierungsstelle (Zertifizierungsstelle) verwendet, können Sie eine anwenderdefinierte Zertifizierungsstelle im Informer-Pod bereitstellen, damit der Informer mit der Instanz ServiceNow kommunizieren kann. Weitere Informationen finden Sie im Artikel Verwenden einer benutzerdefinierten Stammzertifizierungsstelle beim Verbinden des Informers mit der Instanz [KB1710906] in der Knowledge Base Now Support.
- Alternativ zur Standardauthentifizierung kann der Informer die OAuth 2.0-Autorisierung verwenden, um eine Verbindung zur Instanz ServiceNow herzustellen und die Sicherheit zu erhöhen. Wenn der Informer OAuth 2.0 verwendet, gibt die Instanz ein Zugriffstoken mit einer Ablaufzeit aus, anstatt bei jeder Ressourcenanforderung Anmeldeinformationen abzurufen. Weitere Informationen finden Sie im Artikel Connecting CNO for Visibility unter Verwendung des OAuth-Protokolls [KB1648198] in der Knowledge Base Now Support.

5. Wahlweise: Wenn die Richtlinien Ihrer Organisation dies erfordern, platzieren Sie das Informer-Docker-Image im Image-Repository Ihrer Organisation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Ab Version Agent Client Collector für Kubernetes – Transparenz Version 3.9.0 (Informer-Version 2.3.0), die im November 2024 veröffentlicht wurde, unterstützt das Docker-Image sowohl ARM64- als auch AMD64-Architekturen. Ein Upgrade vom vorherigen Image auf das neue verursacht keine Unterbrechungen. Das neue Image erfordert jedoch mehr Speicherplatz in Ihrem Image-Repository als das vorherige.

a. Rufen Sie das Image aus dem Docker-Hub ab, und verschieben Sie es in das Repository Ihrer Organisation.

(Optional) Ersetzen Sie `VERSION` durch die Nummer des aktuellen Release, wie im Artikel CNO für YAML-Dateireleases für Transparenz-Helmdiagramm und Kubernetes [KB1564347] in der Knowledge Base Now Support angegeben.

```
Docker pull docker.io/servicenowdocker/informer:VERSION
 Docker tag docker.io/servicenowdocker/informer:VERSION
 COMPANY_REPO:VERSION
 Docker push COMPANY_REPO:VERSION
```

b. Wenn das Image-Repository eine Authentifizierung erfordert, erstellen Sie im angegebenen Namespace ein Geheimnis mit dem Namen „k8s-informer-repo-cred“.

Zum Beispiel:

```
kubectl create secret docker-registry k8s-informer-repo-cred
 --docker-server https://index.docker.io/v2/ --docker-username
 DOCKER_USERNAME --docker-password DOCKER_TOKEN
 --docker-email=user@servicenow.com -n NAMESPACE
```

6. Wahlweise: Wenn ausgehender Datenverkehr von Ihrem Cluster über einen Proxy geleitet wird, geben Sie den Namen und Port des Proxy-Hosts an, der in Ihrem Cluster verwendet wird.

   Hinweis: Fragen Sie das -Team Kubernetes Ihrer Organisation nach diesen Informationen. Sie müssen es im Installationsprozess angeben.

7. Wahlweise: Aktivieren Sie Agent Client Collector für Kubernetes – Transparenz, um mehr Daten gleichzeitig zu verarbeiten.
   Standardmäßig kann die Back-End-Seite von Informer Daten aus etwa 300 Clustern gleichzeitig verarbeiten. Wenn Sie mehr Cluster haben oder Ihre Cluster häufig geändert werden, können Sie die Anzahl der gleichzeitigen Worker-Threads erhöhen, die für die Verarbeitung der Daten verwendet werden. Weitere Informationen finden Sie im Artikel Controlling the number of CNO for Visibility Concurrent Worker Threads [KB1580241] in der Knowledge Base Now Support.

Ergebnisse

Ihre Instanz ServiceNow und der Cluster Kubernetes sind bereit für die Bereitstellung Agent Client Collector für Kubernetes – Transparenz von .

Nächste Maßnahme

Agent Client Collector für Kubernetes – Transparenz installieren.

Agent Client Collector für Kubernetes – Transparenz installieren

Sie können Agent Client Collector für Kubernetes – Transparenz entweder mit einem Helm-Diagramm oder der YAML-Datei Kubernetes installieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Dieses Verfahren beschreibt den standardmäßigen Agent Client Collector für Kubernetes – Transparenz -Installationsprozess. In der Regel wird für die Installation ein Helm-Diagramm verwendet. Sie können jedoch auch die von ServiceNowbereitgestellte YAML-Datei Kubernetes konfigurieren und ausführen.

Hinweis: Alternativ können Sie Agent Client Collector für Kubernetes – Transparenz mit dem Terraform-Helm-Anbieter bereitstellen. Weitere Informationen finden Sie im Artikel CNO for Visibility mithilfe des Terraform-Helm-Providers installieren [KB1540556] in der Knowledge Base Now Support.

Prozedur

Installieren Sie Agent Client Collector für Kubernetes – Transparenz entweder mit einem -Helm-Diagramm oder mit der von KubernetesServiceNow] bereitgestellten YAML-Datei .

- Installieren Sie Agent Client Collector für Kubernetes – Transparenz mit einem Helm-Diagramm.

  a. Bearbeiten Sie den Befehl „Helm installieren“.

  i. Ersetzen Sie im folgenden Befehl NAMESPACE, INSTANCE_NAME und CLUSTER_NAME durch die relevanten Werte, und ersetzen Sie HELM_URL durch die URL der aktuellen Version, die im Artikel CNO für Visibility-Helmdiagramm und Kubernetes-YAML-Dateiveröffentlichungen [KB1564347] in der Now Support bereitgestellt wird. Knowledge Base.

```
helm install -n NAMESPACE --set acceptEula=Y --set
 instance.name=INSTANCE_NAME --set clusterName="CLUSTER_NAME" {--set
 image.repository=COMPANY_REPO --set image.tag=COMPANY_TAG} {--set
 proxyUrl=http://proxy_host:proxy_port} k8s-informer HELM_URL
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Die geschweiften Klammern zeigen an, dass die Codesegmente, die sie umgeben, optional sind. Verwenden Sie diese Codesegmente, wenn das Image aus dem Image-Repository Ihrer Organisation abgerufen werden muss oder wenn ausgehender Datenverkehr von Ihrem Cluster über einen Proxy geleitet wird.
- Durch die Übergabe `von --set akzeptierenEula=Y`stimmen Sie der Endanwender-Lizenzvereinbarung zu. Sie können die Endanwender-Lizenzvereinbarung lesen, indem Sie die Datei „EULA.pdf“ aus „informer-höher-“ extrahieren.<VERSION_NUMBER> .tgz
- Wenn Informer in OpenShift installiert ist, fügen Sie dem Befehl den Parameter *`openShift`* hinzu, und legen Sie ihn auf `true`fest:

```
helm install -n NAMESPACE --set acceptEula=Y
 --set instance.name=INSTANCE_NAME
 --set clusterName="CLUSTER_NAME" {--set
 image.repository=COMPANY_REPO --set image.tag=COMPANY_TAG}
 {--set proxyUrl=http://proxy_host:proxy_port} {--set
 openShift=true} k8s-informer HELM_URL
```

Hinweis: Wenn Informer nicht in OpenShift installiert ist, muss dieser Parameter nicht festgelegt werden.

ii. Konfigurieren Sie im Befehl nach Bedarf zusätzliche Einstellungen:

- Konfigurieren Sie das Arbeitsspeicherlimit des Informer-Pods
- Ändern Sie die Häufigkeit für die vollständige Discovery in Agent Client Collector für Kubernetes – Transparenz
- Kontinuierliche Discovery in deaktivieren Agent Client Collector für Kubernetes – Transparenz
- Unterdrücken Sie häufige Changes im Cluster Kubernetes, um die Last Ihrer Instanz zu reduzieren. Wenn diese Funktion aktiv ist, meldet der Informer keine Changes, die über dem konfigurierten Schwellenwert liegen, an die Instanz zurück. Weitere Informationen finden Sie im Artikel Unterdrückend häufige Änderungen in Kubernetes-Clustern, die von CNO für Transparenz gemeldet werden [KB1580745] in der Knowledge Base Now Support.
- Steuern Sie die maximale Anzahl vollständiger Erkennungen, die Informer in mehreren Clustern gleichzeitig ausführen können. Weitere Informationen finden Sie im Artikel Zeitplanung für vollständige Erkennungen in CNO für Transparenz [KB1580250] in der Knowledge Base Now Support.

b. Führen Sie den Befehl aus.

- Installieren Sie Agent Client Collector für Kubernetes – Transparenz mithilfe der YAML-Datei Kubernetes.

a. Laden Sie die YAML-Zip-Datei Kubernetes herunter, die im Artikel CNO für YAML-Dateireleases für Transparenz-Helmdiagramm und Kubernetes [KB1564347] in der Knowledge Base Now Support bereitgestellt wird.

b. Extrahieren Sie die Dateien k8s_informer.yaml und EULA.pdf aus der ZIP-Datei.

c. Bearbeiten Sie die Datei k8s_informer.yaml.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ändern Sie den Wert von ACCEPT_EULA wie folgt in „Y“:

```
- name: ACCEPT_EULA
  value: "Y"
```

Hinweis: Indem Sie den Wert in „Y“ändern, stimmen Sie der Endanwender-Lizenzvereinbarung zu, die in der Datei EULA.pdf enthalten ist.

- Ersetzen Sie alle Vorkommen von<NAMESPACE> durch den Namespace, in dem Sie den Informer installieren möchten.
- Ersetzen Sie alle Vorkommen von<INSTANCE_NAME> mit dem Namen Ihrer Instanz, ohne den Domänennamen.
- Ersetzen<CLUSTER_NAME> mit dem Namen Ihres Clusters, wie er in CMDBangezeigt wird.
- Wenn Informer in OpenShift installiert ist, ändern Sie den Wert der Umgebungsvariablen OPENSHIFT in `true`.

d. Führen Sie den folgenden Befehl aus:

```
kubectl apply -f k8s_informer.yaml
```

Ergebnisse
Agent Client Collector für Kubernetes – Transparenz wird im Cluster Kubernetes bereitgestellt und beginnt mit dem Streamen von Daten in Ihre Instanz.

Nächste Maßnahme
Informationen zur Verwaltung von Agent Client Collector für Kubernetes – Transparenz und zur Problembehandlung finden Sie im Artikel Administrating and Troubleshooting CNO for Visibility (Cloud-Native-Operations) [KB1532614] in der Knowledge Base Now Support.

Konfigurieren Sie das Arbeitsspeicherlimit des Informer-Pods

Legen Sie das Arbeitsspeicherlimit des Informer-Pods Agent Client Collector für Kubernetes – Transparenz fest.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Der Speicherverbrauch des Informer-Pods hängt hauptsächlich von der Anzahl der im Cluster enthaltenen Ressourcen ab. Legen Sie das Arbeitsspeicherlimit des Informer-Pods auf mindestens (Anzahl der Pods)/8 MB mit einem Mindestwert von 200 MB fest. Zum Beispiel:

Geschätzte Pod-Anzahl	1000	5.000	30000
Mindestgrenze für Arbeitsspeicher	200Mi	625Mi	3,75 Gi

Prozedur

Führen Sie einen der folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie ein Helm-Diagramm verwenden, fügen Sie im Befehl „Helm Installation“ das folgende Befehlszeilenargument hinzu:

  `--set_memoryLimit=MEM_limit`

  Beispiel: `--set_memoryLimit=625Mi`

- Wenn Sie k8s_informer.yaml verwenden, fügen Sie unter der Zeile mit „limits:“ die Zeile „`memory: MEM_limit`“ hinzu.

  Im folgenden Beispiel ist MEM_limit gleich 625Mi.

```
resources:
  limits:
    cpu: 100m
    memory: 625Mi
```

Ändern Sie die Häufigkeit für die vollständige Discovery in Agent Client Collector für Kubernetes – Transparenz

Passen Sie an, wie oft der Informer Agent Client Collector für Kubernetes – Transparenz eine vollständige Discovery ausführen soll.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig führt der Informer alle 24 Stunden (1440 Minuten) eine vollständige Erkennung durch. Sie können diese Häufigkeit ändern, indem Sie das folgende Verfahren durchführen. Ändern Sie beispielsweise den Wert in 2880, damit Agent Client Collector für Kubernetes – Transparenz alle 48 Stunden (2880 Minuten) eine vollständige Discovery ausführt.

Prozedur

Führen Sie einen der folgenden Schritte aus:

- Bei Verwendung eines Helm-Diagramms: Fügen Sie im Befehl „Helm Installation“ das folgende Befehlszeilenargument hinzu:

  `--set fullDiscoveryMin=<Frequency in minutes>`

- Bei Verwendung von k8s_informer.yaml: Ersetzen Sie den Standardwert durch den erforderlichen Wert in der Zeile unter FULL_DISCOVERY_MIN.

Kontinuierliche Discovery in deaktivieren Agent Client Collector für Kubernetes – Transparenz

Deaktivieren Sie die kontinuierliche Erkennung von Agent Client Collector für Kubernetes – Transparenz, wenn Sie nur regelmäßige Snapshots Ihrer Clusterressourcen benötigen. Wenn Sie mehrere -Cluster mit häufigen Änderungen haben, können Sie durch Deaktivieren der kontinuierlichen Discovery die Last auf Ihrer -Instanz reduzieren.

Vorbereitungen
Erforderliche Rolle: keine

Prozedur

Führen Sie einen der folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie ein Helm-Diagramm verwenden, fügen Sie im Befehl „Helm Installation“ das folgende Befehlszeilenargument hinzu: `--set kontinuierlicheDiscovery=falsch`
- Wenn Sie die Datei k8s_informer.yaml verwenden, geben Sie in der Zeile unter CONTINOUUS_DISCOVERY den Wert „false“ ein.

Kubernetes -Clusterversion in CMDBanzeigen

Lassen Sie den Informer Agent Client Collector für Kubernetes – Transparenz das relevante Feld im CI cmdb_ci_kubernetes_cluster ausfüllen, um die Clusterversion Kubernetes anzuzeigen.

Vorbereitungen

Verwenden Sie die Anwendung ServiceNow Muster für Discovery und Service-Mapping Version 1.11.0 oder höher.

Erforderliche Rolle: keine

Prozedur

Führen Sie einen der folgenden Schritte aus:

- Wenn Sie ein Helm-Diagramm verwenden, legen Sie im Befehl „Helm Installation“ den Parameter *`getClusterVersion`* auf „wahr“ fest:

  ```
  --set getClusterVersion=wahr
  ```

- Wenn Sie die Datei „k8s_informer.yaml“ verwenden, legen Sie die Umgebungsvariable GET_CLUSTER_VERSION auf „wahr“ fest.

Erstellen Sie ein cmdb_ci_linux_server-CI für jeden Kubernetes -Knoten

Konfigurieren Sie, ob der Informer Agent Client Collector für Kubernetes – Transparenz für jeden Knoten Kubernetes ein cmdb_ci_linux_server-CI erstellen soll.

Vorbereitungen

Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird

Standardmäßig erstellt der Informer ein cmdb_ci_linux_server-CI für jeden Kubernetes -Knoten. Wenn dieses CI redundant ist oder andere Flows in Ihrer Organisation beeinträchtigt, können Sie den zugehörigen Konfigurationsparameter auf „false“ festlegen.

Prozedur

Führen Sie einen der folgenden Schritte aus:

- Wenn Sie ein Helm-Diagramm verwenden, legen Sie im Befehl „Helm Installation“ den Parameter *`createServerCi`* auf „falsch“ fest:

  ```
  --set createServerCi=falsch
  ```

- Wenn Sie die Datei „k8s_informer.yaml“ verwenden, legen Sie die Umgebungsvariable CREATE_SERVER_CI auf „falsch“ fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Definieren Sie Ein- und Ausschlusslisten von Bezeichnungen und Anmerkungen

Definieren Sie in Agent Client Collector für Kubernetes – TransparenzEinschluss- und Ausschlusslisten von Bezeichnungen und Anmerkungen in Ressourcen Kubernetes, die der Informer in Configuration Management Database (CMDB)abruft.

Vorbereitungen
Erforderliche Rolle: keine

Prozedur

Erstellen Sie eine Einschluss- oder Ausschlussliste, indem Sie das entsprechende Verfahren ausführen.

Aufgabe	Verfahren
Erstellen Sie eine Einschlussliste	• Wenn Sie ein Helm-Diagramm verwenden, fügen Sie im Befehl „Helm Installation“ eine durch Kommas getrennte Include-Liste mit Bezeichnungen und Anmerkungen hinzu. Beispiel: `--set IncludeLabelsAndAnnotations="label1,label2"` • Wenn Sie die Datei k8s_informer.yaml verwenden, fügen Sie Werte unter der Umgebungsvariablen INCLUDE_LABELS_AND_ANNOTATIONS hinzu.
Erstellen Sie eine Ausschlussliste	• Wenn Sie ein Helm-Diagramm verwenden, fügen Sie im Befehl „Helm Installation“ eine durch Kommas getrennte Include-Liste mit Bezeichnungen und Anmerkungen hinzu. Beispiel: `--set ExcludeLabelsAndAnnotations="label1,label2"` • Wenn Sie die Datei „k8s_informer.yaml“ verwenden, fügen Sie Werte unter der Umgebungsvariablen EXLUDE_LABELS_AND_-ANNOTATIONS hinzu.

Automatische Übersetzung

Fügen Sie Ressourcen Kubernetes anwenderdefinierte Bezeichnungen und Anmerkungen hinzu

Fügen Sie allen von Agent Client Collector für Kubernetes – Transparenz bereitgestellten Ressourcen im Cluster Kubernetes anwenderdefinierte Bezeichnungen und Anmerkungen hinzu.

Vorbereitungen
Erforderliche Rolle: keine

Prozedur

Führen Sie einen der folgenden Schritte aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Wenn Sie ein Helm-Diagramm verwenden, fügen Sie im Befehl „Helm Installation“ die anwenderdefinierten Attribute der Datei „values.yaml“ hinzu.

  Verwenden Sie das im folgenden Beispiel gezeigte Format:

  ```
  --set commonLabels.mylabel1=value1 --set commonLabels.mylabel2=value2 --set commonAnnotations.myannotation1=value3.
  ```

- Wenn Sie die Datei k8s_informer.yaml verwenden, fügen Sie anwenderdefinierte Bezeichnungen und Anmerkungen manuell zu den relevanten Ressourcen in der Datei hinzu.

Hinweis:

Bezeichnungs- und Anmerkungsnamen müssen alphanumerisch sein und dürfen keine Leerzeichen oder Sonderzeichen enthalten. Informationen zu Einschränkungen für Bezeichnungswerte finden Sie in der Kubernetes-Dokumentation .

Upgrade Agent Client Collector für Kubernetes – Transparenz

Sie können Agent Client Collector für Kubernetes – Transparenz entweder mit einem Helm-Diagramm oder der YAML-Datei Kubernetes aktualisieren.

Vorbereitungen
Erforderliche Rolle: keine

Warum und wann dieser Vorgang ausgeführt wird
Dieses Verfahren beschreibt den Standard-Upgrade-Prozess Agent Client Collector für Kubernetes – Transparenz. Normalerweise verwenden Sie ein Helm-Diagramm, um das Upgrade durchzuführen. Alternativ können Sie ein Upgrade Agent Client Collector für Kubernetes – Transparenz von durchführen, indem Sie die von ServiceNowbereitgestellte YAML-Datei Kubernetes konfigurieren und ausführen. In beiden Fällen muss vor dem Upgrade nicht deinstalliert werden.

Sie können Agent Client Collector für Kubernetes – Transparenz Informer-Pods in Kubernetes -Clustern auch remote über die Instanz ServiceNow aktualisieren. Weitere Informationen finden Sie unter Führen Sie ein Remote-Upgrade für Agent Client Collector für Kubernetes – Transparenz Informer durch.

Prozedur

Führen Sie ein Upgrade Agent Client Collector für Kubernetes – Transparenz von entweder mit einem -Helm-Diagramm oder mit der von Kubernetes bereitgestellten YAML-Datei ServiceNowdurch.

- Upgrade von Agent Client Collector für Kubernetes – Transparenz mit einem Helm-Diagramm.

  a. Bearbeiten Sie den Befehl „Helm upgraden“.

  i. Ersetzen Sie im folgenden Befehl NAMESPACE, INSTANCE_NAME und CLUSTER_NAME durch die relevanten Werte, und ersetzen Sie HELM_URL durch die URL der aktuellen Version, die im Artikel CNO für Visibility-Helmdiagramm und Kubernetes-YAML-Dateiveröffentlichungen [KB1564347] in der Now Support bereitgestellt wird. Knowledge Base.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
helm upgrade -n NAMESPACE --set acceptEula=Y --set
 instance.name=INSTANCE_NAME --set clusterName="CLUSTER_NAME" {--set
 image.repository=COMPANY_REPO --set image.tag=COMPANY_TAG} {--set
 proxyUrl=http://proxy_host:proxy_port} k8s-informer HELM_URL
```

Hinweis:

- Die geschweiften Klammern zeigen an, dass die Codesegmente, die sie umgeben, optional sind. Verwenden Sie diese Codesegmente, wenn das Image aus dem Image-Repository Ihrer Organisation abgerufen werden muss oder wenn ausgehender Datenverkehr von Ihrem Cluster über einen Proxy geleitet wird.
- Durch die Übergabe `von --set akzeptierenEula=Y`stimmen Sie der Endanwender-Lizenzvereinbarung zu. Sie können die Endanwender-Lizenzvereinbarung lesen, indem Sie die Datei „EULA.pdf“ aus „informer-höher-“ extrahieren.<VERSION_NUMBER> .tgz
- Wenn Informer in OpenShift installiert ist, fügen Sie dem Befehl den Parameter *`openShift`* hinzu, und legen Sie ihn auf `true`fest:

```
helm upgrade -n NAMESPACE --set acceptEula=Y
 --set instance.name=INSTANCE_NAME
 --set clusterName="CLUSTER_NAME" {--set
 image.repository=COMPANY_REPO --set image.tag=COMPANY_TAG}
 {--set proxyUrl=http://proxy_host:proxy_port} {--set
 openShift=true} k8s-informer HELM_URL
```

Hinweis: Wenn Informer nicht in OpenShift installiert ist, muss dieser Parameter nicht festgelegt werden.

ii. Konfigurieren Sie im Befehl nach Bedarf zusätzliche Einstellungen:

- Konfigurieren Sie das Arbeitsspeicherlimit des Informer-Pods
- Ändern Sie die Häufigkeit für die vollständige Discovery in Agent Client Collector für Kubernetes – Transparenz
- Kontinuierliche Discovery in deaktivieren Agent Client Collector für Kubernetes – Transparenz
- Unterdrücken Sie häufige Changes im Cluster Kubernetes, um die Last Ihrer Instanz zu reduzieren. Wenn diese Funktion aktiv ist, meldet der Informer keine Changes, die über dem konfigurierten Schwellenwert liegen, an die Instanz zurück. Weitere Informationen finden Sie im Artikel Unterdrückend häufige Änderungen in Kubernetes-Clustern, die von CNO für Transparenz gemeldet werden [KB1580745] in der Knowledge Base Now Support.
- Steuern Sie die maximale Anzahl vollständiger Erkennungen, die Informer für mehrere Cluster gleichzeitig ausführen können. Weitere Informationen finden Sie im Artikel Zeitplanung für vollständige Erkennungen in CNO für Transparenz [KB1580250] in der Knowledge Base Now Support.

b. Führen Sie den Befehl aus.

- Aktualisieren Sie Agent Client Collector für Kubernetes – Transparenz mit der YAML-Datei Kubernetes.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Laden Sie die YAML-Zip-Datei Kubernetes herunter, die im Artikel CNO für YAML-Dateireleases für Transparenz-Helmdiagramm und Kubernetes [KB1564347] in der Knowledge Base Now Support bereitgestellt wird.

b. Extrahieren Sie die Dateien k8s_informer.yaml und EULA.pdf aus der ZIP-Datei.

c. Bearbeiten Sie die Datei k8s_informer.yaml.

- Ändern Sie den Wert von ACCEPT_EULA wie folgt in „Y“:

```
- name: ACCEPT_EULA
  value: "Y"
```

Hinweis: Indem Sie den Wert in „Y“ändern, stimmen Sie der Endanwender-Lizenzvereinbarung zu, die in der Datei EULA.pdf enthalten ist.

- Ersetzen Sie alle Vorkommen von<NAMESPACE> durch den Namespace, in dem Sie den Informer installieren möchten.
- Ersetzen Sie alle Vorkommen von<INSTANCE_NAME> mit dem Namen Ihrer Instanz, ohne den Domänennamen.
- Ersetzen<CLUSTER_NAME> mit dem Namen Ihres Clusters, wie er in CMDBangezeigt wird.
- Wenn Informer in OpenShift installiert ist, ändern Sie den Wert der Umgebungsvariablen OPENSHIFT in `true`.

d. Führen Sie den folgenden Befehl aus:

```
kubectl apply -f k8s_informer.yaml
```

Nächste Maßnahme

Informationen zur Verwaltung von Agent Client Collector für Kubernetes – Transparenz und zur Problembehandlung finden Sie im Artikel Administrating and Troubleshooting CNO for Visibility (Cloud-Native-Operations) [KB1532614] in der Knowledge Base Now Support.

Führen Sie ein Remote-Upgrade für Agent Client Collector für Kubernetes – Transparenz Informer durch

Führen Sie ein Remote-Upgrade Agent Client Collector für Kubernetes – Transparenz für Informer-Pods in Kubernetes -Clustern über die Instanz ServiceNow durch, um eine Abhängigkeit von Ihrem Kubernetes -Administrator zu vermeiden. Sie können einen einzelnen Informer oder mehrere Informer gleichzeitig upgraden.

Vorbereitungen

Erforderliche Rolle: discovery_admin

Prozedur

1. Navigieren zu **Alle** > **Kubernetes-Transparenz-Agent** > **Eigenschaften**.
2. Legen Sie im Feld **Kubernetes-Transparenz-Agent-Image** das Image fest, auf das Sie ein Upgrade für derzeit ausgeführte Informer durchführen möchten, und wählen Sie dann **Speichern**aus.
   Verwenden Sie das folgende Format: Repository:Tag. Beispiel: `servicenowdocker/informer:2.1.1`.
3. Navigieren zu **Alle** > **Kubernetes-Transparenz-Agent** > **Startseite**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Führen Sie in der Liste „Informer“ Kubernetes die entsprechenden Schritte aus, um einen oder mehrere Informer gleichzeitig zu aktualisieren.

   Hinweis: Nur Informer mit dem Wert Upgrade Pending (Upgrade ausstehend) im Feld **Upgrade-Status** können aktualisiert werden. Der Ausführungsstatus der Informer muss entweder „In Betrieb“ oder „Angehalten“ sein.

Upgrade	Schritte
OneInformer	**a.** Wählen Sie den Informer in der Liste aus, um das entsprechende Formular anzuzeigen. **b.** Wählen Sie im Abschnitt „Zugehörige Links“ des Formulars **Upgrade Informer**aus.
Mehrere Informer	**a.** Wählen Sie in der Liste mehrere Informer aus. **b.** Wählen Sie im Listenmenü **Aktionen für ausgewählte Zeilen...** das Menüelement **Upgrade Informers** aus.

   Der Upgrade-Vorgang beginnt, und im Feld **Upgrade-Status** für jeden ausgewählten Informer wird der Wert Wird aktualisiert angezeigt. Das System lädt das neue Image herunter und startet den neuen Pod für jeden ausgewählten Informer.

   Wenn ein aktualisierter Pod eine Verbindung zur Instanz herstellt, wird im Feld **Informer-Version (Informer-Version)** die neue Versionsnummer angezeigt. Im Feld **Upgrade-Status** wird Gewünschtes Image wird verwendet angezeigt.

Überschreibt Informer-Parameter von der Instanz

Steuern Sie Agent Client Collector für Kubernetes – Transparenz die Informer-Ausführungsparameter von der Instanz ServiceNow aus, um eine Abhängigkeit von Ihrem Kubernetes -Administrator zu vermeiden.

Vorbereitungen
Erforderliche Rolle: discovery_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Informer-Ausführungsparameter werden während der Bereitstellung mit der YAML-Datei Kubernetes oder dem -Helm-Befehl konfiguriert. Wenn Sie diese Einstellungen später ändern müssen, können Sie dies direkt über die -Instanz tun, ohne Ihr Kubernetes -Team bitten zu müssen, die Bereitstellung zu aktualisieren oder neu zu installieren.

Wenn Sie einen Parameter hinzufügen oder ändern, wird er über die ECC-Warteschlange mit dem Informer synchronisiert. Je nach Parameter muss der Informer-Pod möglicherweise neu gestartet werden. Für Parameter, die einen Neustart erfordern, muss die Umgebungsvariable SELF_PATCHING_ALLOWED auf „wahr“ festgelegt sein, damit Änderungen beim Neustart wirksam werden. Wenn diese Variable auf „false“ festgelegt ist, wird der Informer nicht neu gestartet und verwendet weiterhin die alten Werte.

Hinweis: Informer-spezifische Parameter wirken sich nur auf einen bestimmten Informer aus. Wenn Sie einen Parameter hinzufügen, ohne ihn einem Informer zuzuweisen, wird standardmäßig ein globaler Parameter verwendet und wirkt sich auf alle Informer im System aus. Wenn sowohl globale als auch Informer-spezifische Parameter vorhanden sind, haben Informer-spezifische Parameter Vorrang.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die folgenden Parameter von der Instanz aus aktualisieren:

Parameter	Bei Änderung neu starten
VERBOSE_LOGGING	Nein
OFFENSCHICHT	Ja
CREATE_SERVER_CI	Nein
INCLUDE_LABELS_AND_ANNOTATIONS	Nein
EXLUDE_labels_and_ANNOTATIONS	Nein
FULL_DISCOVERY_MIN	Ja
SEND_INTERVAL_SEC	Ja
CONTINOUUS_DISCOVERY	Ja
CLUSTER_RESOURCE_ID	Nein
CLUSTER_NAME	Nein

Informationen zum Zweck der einzelnen Parameter finden Sie im Artikel CNO für erweiterte Konfigurationsoptionen für Transparenz [KB1648891] in der Knowledge Base Now Support.

Prozedur

1. Navigieren zu **Alle** > **Kubernetes-Transparenz-Agent** > **Konfigurationsparameter**.
2. Wählen Sie einen Parameter in der Liste **der Kubernetes-Informer-Parameter** aus.
3. Ändern Sie den konfigurierten Wert nach Bedarf, und wählen Sie dann **Aktualisieren**aus.

Zusätzliche Ressourcen aus Kubernetes -Clustern werden in CMDB-Cluster abgerufen

Sie können den Informer Agent Client Collector für Kubernetes – Transparenz so konfigurieren, dass zusätzlich zu den standardmäßig an die Datenbank gesendeten Ressourcen zusätzliche Ressourcen aus den Clustern Kubernetes in den Cluster Configuration Management Database (CMDB)abgerufen werden. Durch das Abrufen zusätzlicher Ressourcen, die über den Standardsatz hinausgehen, können Sie die Transparenz in Ihren Kubernetes -Clustern verbessern.

Der Informer sammelt Daten zu Ressourcen Kubernetes, sendet die gesammelten Daten an die -Instanz und aktualisiert die entsprechenden Tabellen in CMDB. Eine Liste der Ressourcen, die der Informer standardmäßig in CMDB abruft, finden Sie unter Von CNO für Transparenz gesammelte Daten.

Für jede zusätzliche Ressource Kubernetes, die der Informer in die CMDBabrufen soll, erstellt das System ein Configuration Item (CI) in der Zieltabelle cmdb_ci_kubernetes_component. Alternativ können zusätzliche Ressourcen in anwenderdefinierte Tabellen abgerufen werden, die die Tabelle cmdb_ci_kubernetes_component erweitern. Sie können beispielsweise eine Tabelle u_cmdb_ci_kubernetes_configmap für alle ConfigMap-Ressourcen im Cluster erstellen. Für jede zusätzliche Ressource erstellt das System eine Beziehung und einen Verweis von der Tabelle auf das Cluster-CI. Wenn die Ressource namespaced ist, wird eine Beziehung zum Namespace-CI erstellt.

Standardmäßig ruft der Informer für jede zusätzliche Ressource die folgenden Informationen aus dem Cluster Kubernetes ab:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Name
- Namespace (für Namespace-Ressourcen)
- Kubernetes-ID
- API-Version
- Art
- Bezeichnungen und Anmerkungen

Zusammen mit diesen Standarddaten können Sie festlegen, dass der Informer weitere Informationen zu den zusätzlichen Ressourcen in CMDBabruft. Standardmäßig speichert das System diese zusätzlichen Daten im Attributfeld der Tabelle cmdb_ci_kubernetes_component. Sie können auch ein anwenderdefiniertes Feld pro zusätzlicher Ressource zum Speichern zusätzlicher Informationen erstellen.

Agent Client Collector für Kubernetes – Transparenz Mit können Sie zusätzliche Ressourcen filtern, indem Sie Filterbedingungen definieren. Wenn eine Bedingung eine Übereinstimmung anzeigt, sendet der Informer die Ressource an CMDB.

Ausführlichere Informationen und Verfahren zum Abrufen zusätzlicher Ressourcen aus Kubernetes -Clustern in CMDBfinden Sie im Artikel Discovery zusätzlicher Kubernetes-Ressourcen mit CNO für Transparenz (Informer) [KB1638668] in der Knowledge Base Now Support.

Agent Client Collector für Kubernetes – Transparenz – Referenz

Referenzinformationen zu Agent Client Collector für Kubernetes – Transparenz.

Durch Agent Client Collector für Kubernetes – Transparenz erfasste Daten

Der Agent Client Collector für Kubernetes – Transparenz Informer sammelt Daten zu Kubernetes -Ressourcen und füllt verschiedene CMDB -Tabellen.

Der Agent Client Collector für Kubernetes – Transparenz Informer sammelt Daten zu den folgenden Kubernetes -Ressourcen:

- Namespaces
- Knoten
- Bereitstellungen
- Statefulsets
- Daemonsets
- Replikatesätze
- Aufträge
- Cron-Jobs
- Pods
- Services
- ReplicationController
- Ein-/Ausgänge

Informer sammelt Daten zu den folgenden OpenShift -Ressourcen:

- Bereitstellungskonfiguration
- BuildConfig

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Routen
- Gruppen
- Anwender
- Projekte
- Bilder
- ImageStreams

Der Informer füllt die folgenden CMDB -Tabellen:

- cmdb_ci_kubernetes_cluster
- cmdb_ci_kubernetes_namespace
- cmdb_ci_kubernetes_node
- cmdb_ci_kubernetes_deployment
- cmdb_ci_kubernetes_statefulset
- cmdb_ci_kubernetes_daemonset
- cmdb_ci_kubernetes_replicaset
- cmdb_ci_kubernetes_job
- cmdb_ci_kubernetes_cronjob
- cmdb_ci_kubetnetes_pod
- cmdb_ci_kubernetes_service
- cmdb_ci_kubernetes_replicationcontroller
- cmdb_ci_kubernetes_ingdress
- cmdb_ci_docker_container
- cmdb_ci_docker_image
- cmdb_ci_container_repository_entry
- cmdb_ci_container_repository
- cmdb_ci_linux_server
- cmdb_ci_openshift_dep_conf
- cmdb_ci_openshift_build_conf
- cmdb_ci_openshift_route
- cmdb_ci_openshift_group
- cmdb_ci_openshift_user
- cmdb_ci_openshift_project
- cmdb_ci_openshift_images
- cmdb_ci_openshift_images_stream

Agent Client Collector für Kubernetes – Transparenz Informer-Statusfelder

Die Felder in der Tabelle Agent Client Collector für Kubernetes – Transparenz „ Informer beschreiben den Status der in Ihren Kubernetes -Clustern bereitgestellten Informer-Pods.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector für Kubernetes – Transparenz Tabelle „Informer“.

Feld	Beschreibung
Informer-Name	Vom System generierter Name des Informers, basierend auf der eindeutigen ID des Clusters. Wenn ein neues Cluster-CI erstellt wird, ist der Informer-Name mit dem Namen identisch, den Sie für den Cluster konfiguriert haben. Wählen Sie dieses Feld aus, um die verfügbaren Aktionen für den ausgewählten Informer anzuzeigen.
Kubernetes Cluster	Verweis auf das Cluster-CI. Wählen Sie dieses Feld aus, um Details zum Cluster anzuzeigen.
Vollständiger Discovery-Status	Status der aktuellen vollständigen Discovery. Mögliche Werte: „Leer“, „In Bearbeitung“, „In Warteschlange“, „Abgeschlossen“, „Fehlgeschlagen“. **Hinweis:** Eine vollständige Erkennung wird entweder regelmäßig oder bei Bedarf durchgeführt. Standardmäßig wird er einmal pro Tag ausgeführt.
Letzte vollständige Discovery	Die Uhrzeit, zu der die letzte vollständige Discovery abgeschlossen wurde.
Informer-Version	Die Version des Informer-Pods, der im Cluster ausgeführt wird.
Status	Der Status des Informers. Mögliche Werte: „In Betrieb“, „Ausgeschaltet“, „Angehalten“. **Hinweis:** Der Status eines Informers wird als „Ausgefallen“ betrachtet, wenn in den letzten 15 Minuten keine Nachricht empfangen wurde.
Status der kontinuierlichen Discovery	Der Status der kontinuierlichen Discovery. Mögliche Werte: Ein oder Aus.
Upgrade-Status	Der Upgrade-Status von Informern im Cluster. Mögliche Werte: „Upgrade ausstehend“, „Upgrade läuft“, „Gewünschtes Image wird verwendet“, „Upgrade mit kubectl/Helm“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector für Kubernetes – Transparenz Tabelle „Informer“. (Fortsetzung)

Feld	Beschreibung
	Hinweis: Wenn der Upgrade-Status eines Informers „Upgrade mit kubectl/ Helm“ lautet, wenden Sie sich an Ihren Kubernetes -Administrator, um den Informer manuell zu aktualisieren.

Agent Client Collector für Kubernetes – Transparenz Support-Matrix

Die Komponente Agent Client Collector für Kubernetes – Transparenz wird in mehreren Versionen von Kubernetes und OpenShift und in verschiedenen Kubernetes -Umgebungen unterstützt.

Die neuesten Informationen finden Sie im Artikel „CNO für Transparenz-Supportmatrix“ [KB1700730] in der Knowledge Base Now Support.

Agent Client Collector für Kubernetes – Transparenz Erweiterte Konfiguration

Dieser Abschnitt bezieht sich auf erweiterte Konfigurationsoptionen für die Komponente Agent Client Collector für Kubernetes – Transparenz, die in einem Cluster Kubernetes ausgeführt wird.

Die neuesten Informationen finden Sie im Artikel CNO für erweiterte Konfigurationsoptionen für Transparenz [KB1648891] in der Knowledge Base Now Support.

Agent Client Collector Log Analytics

Agent Client Collector Log Analytics (ACC-L) ermöglicht es Ihnen, Protokolldaten von Linux- und Windows-Hosts mit Agent Client Collector an eine ServiceNow-Instanz zu streamen.

Wie bei Agent Client Collector Framework (ACC-F) wird von Agent Client Collector eine Verbindung zu einem MID-Server hergestellt. Ein einzelner MID-Server kann mehrere Agents unterstützen. Im Rahmen des Failover-Schutzes funktioniert ein einzelner Agent jeweils mit einem MID-Server und wechselt bei Bedarf auf einen anderen MID-Server.

Verwenden Sie Agent Client Collector, um Protokolldaten mithilfe eines Protokollversenders an Ihre ServiceNow®-Instanz zu streamen. Die Protokolldaten werden in der Anwendung ServiceNow® Health Log Analytics zugeordnet und strukturiert. Weitere Informationen finden Sie in der Produktdokumentation Health Log Analytics.

Agent Client Collector Log Analytics hat eine Abhängigkeit von der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und höher, verfügbar im ServiceNow Store . Das Streaming von Protokolldaten von Windows-Hosts wird in Agent Client Collector Log Analytics, Version 3.1.0 und höher, unterstützt.

Die Anwendung Agent Client Collector Log Analytics (ACC-L), Version 3.2.0, August 2022, ist abhängig von der Anwendung Agent Client Collector Framework (ACC-F), Version 2.10.1, August 2022.

Um Agent Client Collector Log Analytics zu aktivieren, aktivieren Sie Protokollanalysen in Agent Client Collector, wie in Richten Sie Agent Client Collector Log Analytics ein, ohne das geführte Setup zu verwenden beschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abhängigkeiten

Eine Liste der Agent Client Collector Log Analytics-Plugin-Abhängigkeiten finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Setup von Agent Client Collector Log Analytics

Konfigurieren Sie Agent Client Collector Log Analytics in Ihrer Instanz von ServiceNow entweder mit oder ohne geführtes Setup.

Einrichtung von Agent Client Collector Log Analytics mit Guided Setup

Das Guided Setup für Agent Client Collector Log Analytics stellt eine Reihe von Aufgaben bereit, die Sie bei der Konfiguration von Agent Client Collector Log Analytics für Ihre Instanz unterstützen. Die Verwendung des geführten Setups stellt sicher, dass Sie über das erforderliche Mindest-Setup verfügen, um die Anwendung zu verwenden. Weitere Informationen finden Sie unter Agent Client Collector Log Analytics mithilfe eines Setups mit Anleitung einrichten.

Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Einrichtung von Agent Client Collector Log Analytics ohne Guided Setup

Wenn Sie das geführte Setup nicht verwenden, müssen Sie mehrere Konfigurationsschritte manuell ausführen. Weitere Informationen finden Sie unter Richten Sie Agent Client Collector Log Analytics ein, ohne das geführte Setup zu verwenden.

Agent Client Collector Log Analytics mithilfe eines Setups mit Anleitung einrichten

Konfigurieren Sie Agent Client Collector Log Analytics in Ihrer Instanz ServiceNow mithilfe des geführten Setups.

Vorbereitungen

- Agent Client Collector Log Analytics hat eine Abhängigkeit von der Anwendung ServiceNow® Ereignismanagement. Richten Sie Ereignismanagement ein, bevor Sie Agent Client Collector Log Analyticskonfigurieren. Weitere Informationen finden Sie unter Setup von Ereignismanagement.
- ServiceNow Service Operations-Arbeitsbereich ITOM Apps müssen installiert sein. Wenn es noch nicht installiert ist, installieren Sie es manuell. Weitere Informationen finden Sie unter Installieren Sie Service Operations-Arbeitsbereich für die Anwendung ITOM ..

Hinweis: Derzeit unterstützt das Setup der ACC-Dateneingabe nur die Standardauthentifizierung mit MID-Server. mTLS wird nicht unterstützt.

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

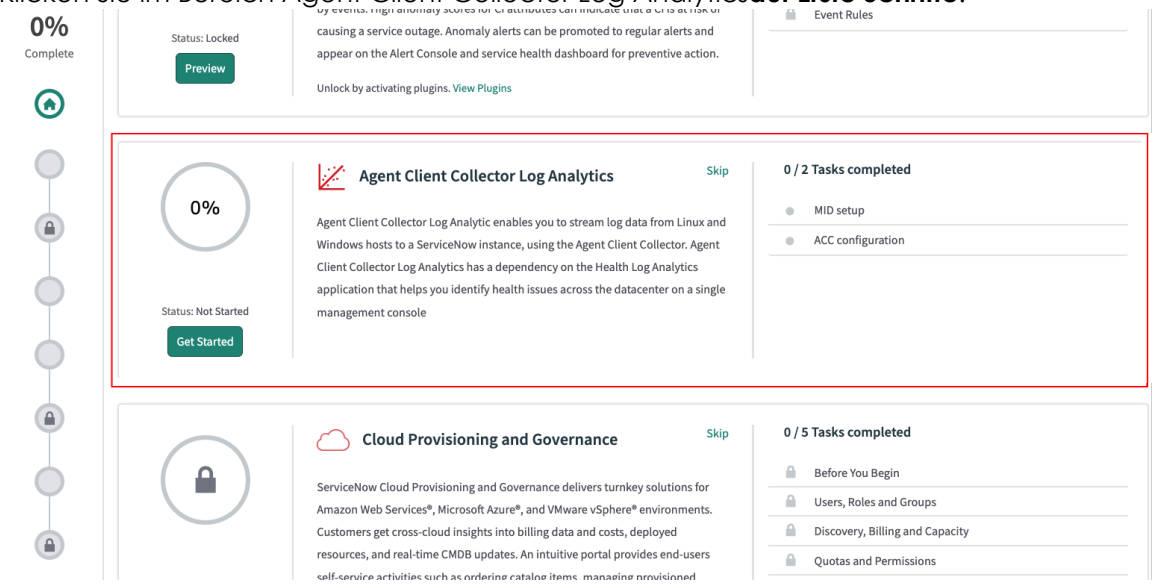
Das geführte Setup fürAgent Client Collector Log Analytics stellt eine Reihe von Aufgaben bereit, die Sie bei der Konfiguration Agent Client Collector Log Analyticsvon unterstützen. Die Verwendung des geführten Setups stellt sicher, dass Sie über das erforderliche Mindest-Setup verfügen, um die Anwendung zu verwenden.

Hinweis: Wenn Sie das geführte Setup nicht verwenden, müssen Sie mehrere Konfigurationsschritte manuell ausführen. Weitere Informationen finden Sie unter Richten Sie Agent Client Collector Log Analytics ein, ohne das geführte Setup zu verwenden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

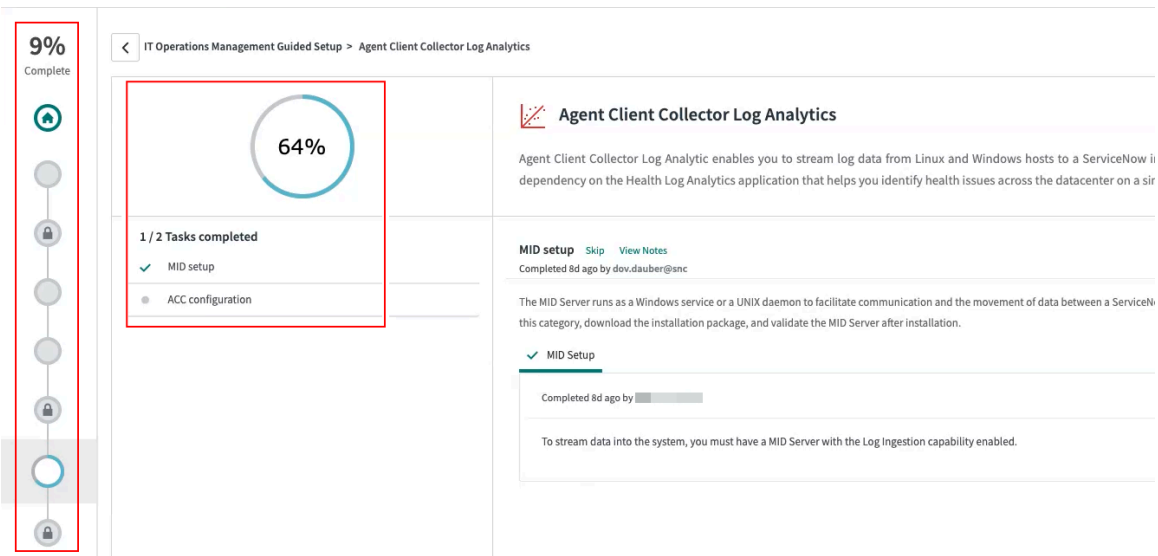
1. Navigieren zu **Alle** > **Geführtes Setup** > **Geführtes Setup für ITOM**.
   Der Begrüßungsbildschirm IT Operations Management Geführtes Setup wird angezeigt.
2. Wählen Sie **Erste Schritte**aus.
3. Klicken Sie im Bereich Agent Client Collector Log Analytics**auf Erste Schritte**.



4. Führen Sie im Abschnitt **„MID-Setup“** die entsprechende Aktion aus:
   - Wenn Sie bereits MID-Serverkonfiguriert haben, wählen Sie **Als abgeschlossen markieren**aus.
   - Wenn Sie kein MID-Serverkonfiguriert haben, wählen Sie **Konfigurieren**, richten Sie ein MID-Serverein, und wählen Sie dann **Als abgeschlossen markieren**aus. Weitere Informationen hierzu finden Sie unter Geführtes Setup für MID-Server verwenden.

   Hinweis: Um Daten in das System zu streamen, benötigen Sie einen MID-Server mit aktivierter Protokollerfassungsfunktion.

Wenn MID-Server konfiguriert ist, zeigt die Statusanzeige für das geführte Setup für Agent Client Collector Log Analytics an, dass 64 % der Konfiguration abgeschlossen sind. Die Fortschrittsanzeige zeigt den Prozentsatz der Fertigstellung für alle IT Operations Management -Aufgaben an.

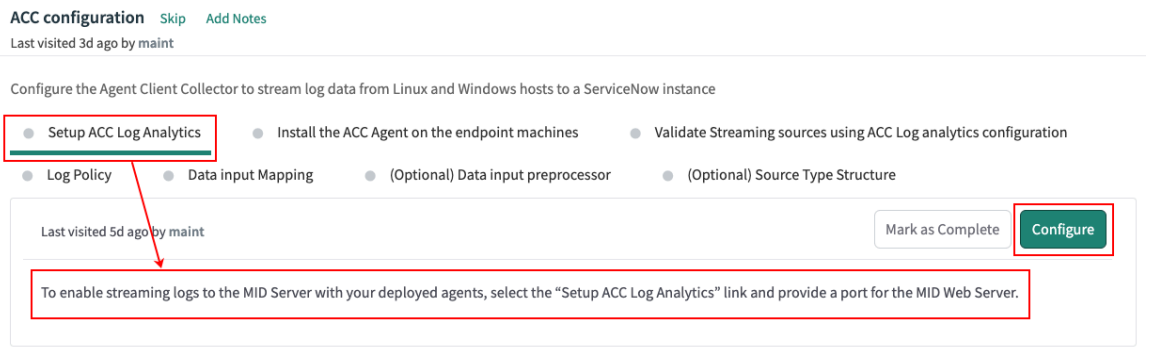


Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Konfigurieren Sie Agent Client Collector Log Analytics.

   a. Wählen Sie im Abschnitt **„ACC-Konfiguration“** eine Setupaufgabe aus, und lesen Sie die Anweisungen im Hilfebereich.



   b. Wählen Sie **Konfigurieren** aus, und schließen Sie die Aufgabe ab. Ausführliche Informationen zu den einzelnen Setupaufgaben finden Sie in der Produktdokumentation Agent Client Collector Log Analytics.

   c. Führen Sie alle erforderlichen Setup-Aufgaben in der Aufgabenliste aus.

   d. Wählen Sie **Als abgeschlossen markieren** aus, um die Konfiguration Agent Client Collector Log Analytics abzuschließen.

Richten Sie Agent Client Collector Log Analytics ein, ohne das geführte Setup zu verwenden

Konfigurieren Sie Agent Client Collector, um Protokolldaten von den Hosts Linux und Windows an eine Instanz ServiceNow zu streamen, ohne das geführte Setup zu verwenden.

Vorbereitungen

Hinweis: Sie können Agent Client Collector Log Analytics mithilfe des geführten Setups konfigurieren. Das geführte Setup stellt sicher, dass Sie über das Mindestsetup verfügen, das für die Verwendung der Anwendung erforderlich ist. Weitere Informationen finden Sie unter Agent Client Collector Log Analytics mithilfe eines Setups mit Anleitung einrichten.

- Das Plugin „Agent Client Collector Log Analytics“ (ACC-L) muss installiert sein. Das Plugin wird mit den Plugins „Agent Client Collector Framework“ (ACC-F) und „Agent Client Collector Monitoring“ (ACC-M) bereitgestellt. Weitere Informationen finden Sie unter Agent Client Collector Installation.
- ServiceNow Service Operations-Arbeitsbereich ITOM Apps müssen installiert sein. Wenn es noch nicht installiert ist, installieren Sie es manuell. Weitere Informationen finden Sie unter Installieren Sie Service Operations-Arbeitsbereich für die Anwendung ITOM ..
- Agent Client Collector Log Analytics hat eine Abhängigkeit von der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und höher, verfügbar im ServiceNow Store . Das Streaming von Protokolldaten von Windows-Hosts wird in Agent Client Collector Log Analytics, Version 3.1.0 und höher, unterstützt.

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Agent Client Collector wird mit dem standardmäßigen *servicenow*-Benutzer bereitgestellt. Vergewissern Sie sich, dass dieser Benutzer Lesezugriff hat, damit von Agent Client Collector alle konfigurierten Protokollpfade angezeigt werden können. Beispielsweise verfügt der Agent Client Collector *servicenow*-Benutzer, der zusammen mit dem Basissystem installiert wird, nicht über Berechtigungen zum Anzeigen des Pfads zu `/var/log/` unter Linux und des Pfads zu `C:\Windows\System32` unter Windows. Informationen zum Konfigurieren von Berechtigungen für den *servicenow*-Benutzer finden Sie in der Now Support-Knowledge Base im Artikel ACC-L Permission Denied issues [KB1117271] (Probleme verweigerter ACC-L-Berechtigungen).

Hinweis: Derzeit unterstützt das Setup der ACC-Dateneingabe nur die Standardauthentifizierung mit MID-Server. mTLS wird nicht unterstützt.

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **MID-Server**.
2. Wählen Sie auf der Seite MID-Server ein MID-Server aus, das validiert ist und den Statuswert In **Betrieb**hat.
3. Wählen Sie im Abschnitt „Zugehörige Links“ der MID-Server-Seite für den ausgewählten Server **Setup ACC Log Analytics** (ACC Log Analytics einrichten) aus.
   Das Setup von Agent Client Collector Log Analytics beginnt.

   Ferner wird vom System automatisch eine ACC-Dateneingabe erstellt. Nach der Erstellung wird der Dateneingabe-Datensatz der ACC-Dateneingabetabelle hinzugefügt, und die Dateneingabe ist zum Streamen von Protokollen bereit.

   Hinweis: Es ist wichtig, dass Sie eine ACC-Dateneingabe für jeden MID-Server konfigurieren, mit dem eine Verbindung von Agent Client Collector-Systemen hergestellt werden kann. Weitere Informationen finden Sie unter Zusätzliche ACC-Dateneingaben einrichten.

   Außerdem werden Sie vom System aufgefordert, den MID-Webserver einzurichten. Weitere Informationen finden Sie unter MID-Webserver.
4. Konfigurieren Sie im Dialogfeld „ACC Log Analytics Setup“ (ACC Log Analytics einrichten) die Ports.

   a. Geben Sie in den Feldern **Port des MID Web Server** und **ACC data input Port** (ACC-Dateneingabe-Port) die entsprechenden Port-Nummern ein.

   b. Wählen Sie **OK** aus.
   Die URL mit dem konfigurierten Endpunkt wird im Dialogfeld angezeigt.

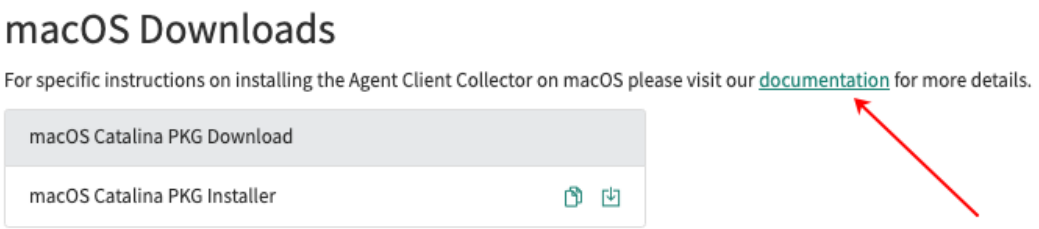
   c. Kopieren und speichern Sie die Endpunkt-URL, um sie bei der Installation des ACC-Agent auf dem Endpunkt-Computer zu verwenden.
5. Navigieren zu **Alle** > **Agent Client Collector** > **MID-Webserver API-Schlüssel** Anschließend kopieren und speichern Sie den MID-Webserver-API-Schlüssel zur Verwendung bei der Installation des ACC-Agent auf dem Endpunktcomputer.
6. Installieren Sie den ACC-Agent auf dem Endpunkt-Computer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Wenn Sie den ACC-Agent bereits installiert haben, fahren Sie mit den Agent Client Collector-Protokollrichtlinien fort.

a. Navigieren zu **Alle** > **Agent Client Collector** > **Bereitstellung** > **Agent-Downloads**.

b. Laden Sie den ACC-Agent für das entsprechende Betriebssystem herunter.
Um detaillierte Anweisungen zu erhalten, klicken Sie auf den Dokumentationslink für das Betriebssystem. Beispiel:



Ergebnisse
Agent Client Collector Log Analytics und der ACC-Agent sind installiert. Sie können die Anwendung nun verwenden.

Nächste Maßnahme
Siehe Agent Client Collector-Protokollrichtlinien.

Zusätzliche ACC-Dateneingaben einrichten

Dateneingaben für das Streamen von Protokollnachrichten an Ihre ServiceNow-Instanz mit Agent Client Collector werden automatisch als Teil des Agent Client Collector-Setups erstellt. Richten Sie zusätzliche ACC-Dateneingaben nach Bedarf manuell ein, indem Sie den Setup-Flow für Health Log Analytics-Dateneingaben verwenden.

Vorbereitungen

- Die Anwendung Agent Client Collector Log Analytics hat eine Abhängigkeit von den folgenden ServiceNow-Anwendungen, die im ServiceNow Store verfügbar sind:
  - Health Log Analytics, Version 22.0.12 - Dezember 2021 und spätere Releases.
  - Agent Client Collector Framework, Version 2.7.0 – Dezember 2021 und spätere Releases.
- Stellen Sie sicher, dass ein MID Server installiert und konfiguriert ist.
- MID-Server muss für die Verwendung mit Agent Client Collector konfiguriert sein. Weitere Informationen finden Sie unter Agent Client Collector Monitoring auf dem MID-Server aktivieren.

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Es ist wichtig, dass Sie eine ACC-Dateneingabe für jeden MID-Server konfigurieren, mit dem eine Verbindung von Agent Client Collector-Systemen hergestellt werden kann, auch wenn derzeit keine Verbindung mit einem Agent besteht. Ein Agent ist jeweils nur mit einem MID-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Server verbunden, wird jedoch bei Bedarf mit einem anderen MID-Server verbunden, wenn dies zur Failover-Absicherung notwendig ist.

Wichtig: Als Teil des standardmäßigen Setups von Health Log Analytics-Dateneingaben können Sie JavaScript-Funktionen für die Zuordnung und Vorverarbeitung von nicht aufbereiteten Protokolldaten definieren. Die JavaScript-Funktion muss für alle ACC-Dateneingaben identisch sein, da Agents zu einer anderen ACC-Dateneingabe wechseln, wenn sie zum Zweck der Failover-Absicherung vom System mit einem anderen MID-Server verbunden werden. Die zuletzt veröffentlichte JavaScript-Funktion wird für alle vorhandenen und zukünftigen ACC-Dateneingaben bereitgestellt und ersetzt die vorherige Funktion. Diese Funktion wird in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und höher, die im ServiceNow Store verfügbar ist, unterstützt.

Prozedur

1. Richten Sie zusätzliche ACC-Dateneingaben manuell mit dem Setup-Flow für Dateneingaben Health Log Analytics ein.
   Weitere Informationen finden Sie unter ACC-Dateneingaben manuell konfigurieren.
2. Identifizieren und beheben Sie Probleme beim Protokoll-Streaming, um sicherzustellen, dass Ihre Dateneingaben ordnungsgemäß Daten streamen.
   Weitere Informationen hierzu finden Sie unter Sicherstellen, dass die Dateneingabe Streamingdaten sind.
3. Legen Sie fest, wie Health Log Analytics Protokollrohdaten behandelt, die in Ihre -Instanz gestreamt werden.
   Standardmäßig wird jede eingehende Protokollzeile automatisch dem richtigen Tag zugeordnet. Wenn Eigenschaften nicht automatisch erkannt werden, ordnen Sie die Dateneingabequellen manuell zu, indem Sie eine JavaScript-Funktion definieren. Weitere Informationen finden Sie unter Rohdaten zuordnen.
4. Wahlweise: Ändern Sie Protokollrohdaten, und löschen oder teilen Sie Protokollnachrichten auf, bevor sie verarbeitet werden.
   Definieren Sie eine JavaScript-Funktion, die Ihre Protokolldaten im Rohzustand ändert, bevor Health Log Analytics sie zuordnet und strukturiert. Weitere Informationen finden Sie unter Rohprotokolldaten vor der Verarbeitung bearbeiten.
5. Wahlweise: Verfeinern Sie die Quelltypstruktur, um sicherzustellen, dass Health Log Analytics alle Eigenschaften korrekt extrahiert und klassifiziert.
   Weitere Informationen finden Sie unter Quelltypstruktur verfeinern.

ACC-Dateneingaben manuell konfigurieren

Beim Setup von Agent Client Collector wird automatisch eine ACC-Dateneingabe zum Streamen von Protokollnachrichten an Ihre ServiceNow-Instanz erstellt. Sie können zusätzliche ACC-Dateneingaben nach Bedarf manuell einrichten.

Vorbereitungen

- Die Anwendung Agent Client Collector Log Analytics hat eine Abhängigkeit von den folgenden ServiceNow-Anwendungen, die im ServiceNow Store verfügbar sind:
  - Health Log Analytics, Version 22.0.12 - Dezember 2021 und spätere Releases.
  - Agent Client Collector Framework, Version 2.7.0 – Dezember 2021 und spätere Releases.
- Stellen Sie sicher, dass ein MID Server installiert und konfiguriert ist.
- MID-Server muss für die Verwendung mit Agent Client Collector konfiguriert sein. Weitere Informationen finden Sie unter Agent Client Collector Monitoring auf dem MID-Server aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Health Log Analytics bietet keine Unterstützung für IPv6. Konfigurieren Sie den MID-Server auf IPv4, um mit der Anwendung zu arbeiten.

Hinweis: Derzeit unterstützt das Setup der ACC-Dateneingabe nur die Standardauthentifizierung mit MID-Server. mTLS wird nicht unterstützt.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **ACC Log Analytics** > **ACC-Dateneingaben**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.
   Feldbeschreibungen finden Sie unter ACC-Dateneingabe – Konfigurationsfelder.
4. Wahlweise: Wählen Sie **Advanced** (Erweitert), um zusätzliche Konfigurationsfelder festzulegen.
5. Wählen Sie **Speichern**.
   Health Log Analytics fügt den Dateneingabedatensatz in die Dateneingabentabelle ein.
6. Stellen Sie sicher, dass die Dateneingabe richtig konfiguriert ist, indem Sie **Verbindung testen**auswählen.

   Health Log Analytics versucht, den MID-Server mit dem Daten-Repository zu verbinden.

   - Wenn die Verbindung erfolgreich hergestellt wurde, ist die Schaltfläche **Verbindung testen** deaktiviert und die Schaltfläche **Veröffentlichen** aktiviert.
   - Wenn die Verbindung fehlgeschlagen ist, wird der Grund für den Fehler im Feld **Fehlermeldung** angezeigt. Dieses Feld wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

     Beheben Sie das Problem, wählen Sie **Speichern**, wenn Sie die Konfiguration geändert haben, und wählen Sie **Verbindung testen**, um die Verbindung erneut zu testen.

     Hinweis: Sie können die Dateneingabekonfiguration nur veröffentlichen, wenn die Verbindung erfolgreich erstellt wurde.

   Hinweis: Sie können zur zuletzt veröffentlichten Konfiguration zurückkehren, indem Sie **Changes rückgängig machen**auswählen. Diese Option ist nur verfügbar, wenn Sie eine zuvor veröffentlichte -Konfiguration ändern.

7. Wählen Sie **Veröffentlichen** aus, um die Dateneingabe im MID-Serverzu veröffentlichen.

Ergebnisse

Mit der neuen Dateneingabe können Protokolle gestreamt werden.

Hinweis: Der Datensatz einer Dateneingabe enthält die folgenden zugehörigen Listen:

- Agents – Listet alle aktiven Agents auf, die mit dem MID-Server für diese Dateneingabe verbunden sind.
- Streaming-Quellen: Listet alle Quellen für diese Dateneingabe und den MID-Server auf, der Protokolle davon empfängt.

Nächste Maßnahme

Vergewissern Sie sich, ob von der Dateneingabe Daten gestreamt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ACC-Dateneingabe – Konfigurationsfelder

Beschreibung der Felder im Konfigurationsformular für ACC-Dateneingaben.

Basiskonfiguration

Feld	Beschreibung
MID	Der MID-Server, an den die Protokolle gestreamt werden **Hinweis:** • Pro MID-Server kann nur eine ACC-Dateneingabe definiert werden. Sie können nur MID Servers mit AgentClientCollector-Funktionalität auswählen, die die Standardauthentifizierung unterstützen. MID Servers, die mTLS unterstützen, werden nicht aufgeführt. • Die standardmäßige maximale Anzahl von Dateneingaben, die Protokolle an einen einzelnen MID-Server streamen, beträgt 10. Sie können diese Anzahl in den MID-Server-Eigenschaften ändern. Wenn jedoch 10 Dateneingaben, die keine ACC-Dateneingaben sind, für einen MID-Server definiert wurden, kann dennoch eine ACC-Dateneingabe für ihn definiert werden, sodass insgesamt 11 Dateneingaben für diesen MID-Server definiert sind. • Wenn Sie das Formular absenden, wird dieses Feld schreibgeschützt. Dies ist ein Pflichtfeld.
Port	Port auf dem MID-Server. Der Port muss konfiguriert und aktiv sein. Er darf nicht von einem anderen Prozess belegt sein. Stellen Sie sicher, dass das Sicherheitsteam Ihrer Organisation den Port öffnet, bevor Sie ihn zuweisen. **Hinweis:** Wenn Sie den Port aktualisieren, aktualisiert das System Agent Client Collector mit der neuen Port-Konfiguration. Das Protokollstreaming wird nach 1 bis 3 Minuten ohne Protokollverlust fortgesetzt. Dies ist ein Pflichtfeld.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Basiskonfiguration (Fortsetzung)

Feld	Beschreibung
Beschreibung	Beschreibung der Dateneingabe

Die Felder in der folgenden Tabelle zeigen schreibgeschützte Informationen.

Feld	Beschreibung
Name	Der Name der Dateneingabe: Agent Log Analytics. **Hinweis:** Alle ACC-Dateneingaben haben denselben Namen. Sie können eine ACC-Dateneingabe anhand des Namens des MID-Servers identifizieren, der für ihn definiert ist.
Status	Status der Dateneingabe.
Übertragung	Protokoll zum Senden der Protokolldaten. Die ACC-Dateneingabe sendet Daten mit einem ServiceNow-Agent.
Quellenanzahl	Die Gesamtzahl der Protokollquellen, die zusammen aus allen ACC-Dateneingaben stammen. Diese Funktion wird unterstützt in der Anwendung Health Log Analytics, Version 22.0.12 – Dezember 2021 und später, verfügbar im ServiceNow Store .
Deaktiviert seit	Zeitpunkt, zu dem die Dateneingabe beendet wurde oder fehlgeschlagen ist
Zeit des letzten Protokolls	Zeitpunkt, zu dem das letzte Protokoll in der Dateneingabe gestreamt wurde
Fehlermeldung	Der Streaming-Fehler. Dieses Feld wird automatisch ausgefüllt. Wird nur angezeigt, wenn ein Streaming-Fehler aufgetreten ist.

Erweiterte Konfiguration

Feld	Beschreibung	Standardwert
Look up hostnames (Nach Hostnamen suchen)	Hiermit geben Sie an, ob eine DNS-Suche durchgeführt wird, um IPs in Hostnamen aufzulösen.	false

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erweiterte Konfiguration (Fortsetzung)

Feld	Beschreibung	Standardwert
SSL verwenden	Option für die Verwendung von SSL.	Wahr
Client inactivity timeout (sec) (Zeitüberschreitung bei Client-Inaktivität (Sek.))	Die Zeitüberschreitung in Sekunden, nach der ein inaktiver Kanal geschlossen wird	15
Anzahl der Worker-Threads	Anzahl der Threads, mit denen eingehende Daten verarbeitet werden	4
Default time zone (Standardzeitzone)	Standardzeitzone von Events. Das System verwendet diesen Standard, wenn im Protokoll keine Zeitzone angegeben ist.	GMT
Anteil der zu verwerfenden Unterstichproben	Verhältnis der zu verwerfenden Events	-1
Anteil der zu empfangenden Unterstichproben	Verhältnis der zu empfangenden Events	-1
Maximale Länge in Bytes	Maximale Länge von Protokollnachrichten in Byte	32.766
Zeichencodierung	Zeichencodierung für diese Dateneingabe	UTF-8
Verwerfen, wenn Warteschlange voll ist	Option zum Auswählen, dass Protokolle verworfen werden, wenn viele Prozesse in der Warteschlange auf den Zugriff auf den MID-Server warten.	false

Agent Client Collector-Protokollrichtlinien

Von Agent Client Collector-Dateneingaben werden Protokollnachrichten mit ServiceNow Agent Client Collector in Ihre ServiceNow-Instanz gestreamt. Die Anwendung Agent Client Collector Log Analytics (ACC-L) bietet vordefinierte Protokollrichtlinien zum Sammeln von Protokolldaten aus den von ACC überwachten CIs.

Mit Agent Client Collector-Protokollrichtlinien können Sie auf folgende Weise arbeiten:

- Verwenden Sie die vordefinierten Protokollrichtlinien des Systems.

  Die Standardprotokollrichtlinien von ACC-L bestehen aus den überwachten CIs und der Prüfung, die für diese CIs ausgeführt wird. Eine vollständige Liste der vordefinierten Protokollrichtlinien und überwachten CI-Typen finden Sie unter Agent Client Collector Log Analytics Standardrichtlinien und -prüfungen.

- Bearbeiten Sie eine vordefinierte Protokollrichtlinie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können beispielsweise eine Standardrichtlinie ändern, wenn Ihre Organisation immer einen bestimmten nicht standardmäßigen Protokollpfad verwendet. Weitere Informationen finden Sie unter Protokollrichtlinie bearbeiten.

- Passen Sie eine veröffentlichte Protokollrichtlinie an, indem Sie daraus eine untergeordnete Richtlinie erstellen.

  Sie können eine vorhandene Protokollrichtlinie (die übergeordnete Richtlinie) als Vorlage verwenden, um eine neue Protokollrichtlinie (die untergeordnete Richtlinie) zu erstellen. Anschließend passen Sie die Parameter an, die die untergeordnete Richtlinie von der übergeordneten Richtlinie zum Zweck der Konzentration auf eine Untergruppe ihrer CIs oder Services übernimmt. Erstellen Sie beispielsweise eine untergeordnete Richtlinie, wenn Ihre Organisation eine Teilmenge der IIS-Serverprotokolle an einem anderen Ort speichert. Weitere Informationen finden Sie unter Untergeordnete Protokollrichtlinie erstellen.

  Hinweis: Die untergeordnete Richtlinie ist von Natur aus spezifischer als die übergeordnete Richtlinie. Wenn von Agent Client Collector eine Übereinstimmung mit einer in der untergeordneten Richtlinie definierten Bedingung festgestellt wird, erfolgt kein Abgleich mit der übergeordneten Richtlinie.

- Definieren Sie eine neue Protokollrichtlinie, wenn für das CI, das von Agent Client Collector überwacht werden soll, keine Richtlinie vorhanden ist.

  Weitere Informationen finden Sie unter Agent Client Collector-Protokollrichtlinie erstellen. Eine allgemeine Erklärung der Agent Client Collector-Richtlinien finden Sie unter Prüfungen und Richtlinien.

Agent Client Collector Log Analytics Standardrichtlinien und -prüfungen

Agent Client Collector Log Analytics bietet verschiedene Standardrichtlinien und -prüfungen.

Das Streaming von Protokolldaten von Windows-Hosts wird in Agent Client Collector Log Analytics, Version 3.1.0 und höher, unterstützt.

ACC-L-Standardrichtlinien

Name	BS	Beschreibung	Prüfung
Protokolle Apache unter Linux	Linux	Sammelt Protokolle von Apache-Servern, die unter einem Linux-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle Apache unter Windows	Windows	Sammelt Protokolle von Apache-Servern, die unter einem Windows-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	BS	Beschreibung	Prüfung
Protokolle IIS	Windows	Sammelt Protokolle von MicrosoftMicrosoft Azure Event Hubs IIS-Webservern und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle JBoss/WildFly-Anwendungsserver unter Linux	Linux	Sammelt Protokolle von JBoss/WildFly-Anwendungsservern, die unter einem Linux-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle JBoss/WildFly-Anwendungsserver unter Windows	Windows	Sammelt Protokolle von JBoss/WildFly-Anwendungsservern, die unter einem Windows-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle Linux-BS	Linux	Sammelt Protokolle vom Linux-Betriebssystem und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle MSSQL unter Linux	Linux	Sammelt Protokolle von MSSQL-DBs, die unter Linux ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	log_shipper
Protokolle MSSQL unter Windows	Windows	Sammelt Protokolle von MSSQL-Datenbanken, die unter einem Windows-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	BS	Beschreibung	Prüfung
Protokolle MySQL-DB unter Linux	Linux	Sammelt Protokolle von MySQL-DBs, die unter einem Linux-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle MySQL-DB unter Windows	Windows	Sammelt Protokolle von MySQL-DBs, die unter einem Windows-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Nginx in Linux Protokollen	Linux	Sammelt Protokolle von Nginx-Servern, die auf dem Betriebssystem Linux ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server.	Protokollversender
Protokolle Tomcat unter Linux	Linux	Sammelt Protokolle von Tomcat-Servern, die unter einem Linux-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle Tomcat unter Windows	Windows	Sammelt Protokolle von Tomcat-Servern, die unter einem Windows-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Oracle WebLogic	Windows und Linux	Sammelt Protokolle von WebLogic-Servern Oracle und sendet sie zur weiteren Analyse an MID-Server.	Protokollversender

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	BS	Beschreibung	Prüfung
		Hinweis: • Der von WebLogic verwendete Protokollpfad weist zwei Umgebungsvariablen auf, wie in der WebLogic-Dokumentation beschrieben. Weitere Informationen finden Sie unter Umgebungsvariablen. • In Windows und Linuxfügt Agent Client Collector Log Analytics dem Protokollpfad eine Standardumgebungsvariable aus der WebLogic-Dokumentation hinzu. Sie können entweder diese Standardumgebungsvariable verwenden, um das vollständige Verzeichnis abzurufen, oder sie manuell ändern, wenn Sie ein bekanntes direktes Verzeichnis verwenden möchten. Informationen zum Anpassen der Umgebungsvariablen finden Sie unter Protokollpfadkonfigurationen bearbeiten.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	BS	Beschreibung	Prüfung
Protokolle WebSphere-Anwendungsserver unter Linux	Linux	Sammelt Protokolle von WebSphere-Anwendungsservern, die unter einem Linux-Betriebssystem ausgeführt werden, und sendet sie zur weiteren Analyse an den MID-Server	Protokollversender
Protokolle Windows-Betriebssystemereignisse	Windows	Sammelt Windows-Ereignisprotokolle von Windows-Servern und sendet sie zur weiteren Analyse an den MID-Server	log shipper for win events

Umgebungsvariablen

Der zum Sammeln von Protokollen von bestimmten Servern verwendete Protokollpfad kann Umgebungsvariablen enthalten. Es ist wichtig zu beachten, dass der ACC-Agent auf Systemen Linux mit nur auf Umgebungsvariablen zugreifen kann, die sich in der Datei „`/etc/environment`" befinden. Fügen Sie die Umgebungsvariablen, auf die der Agent zugreifen muss, der Datei `/etc/environment` im Format *<NAME>='<VALUE>'* hinzu. In Windows -Systemen können Sie Umgebungsvariablen auf die übliche Weise erstellen.

Standardmäßige ACC-L-Prüfungen

Agent Client Collector Log Analytics (ACC-L) bietet die folgenden Standardprüfungen **vom Typ Typ = Protokoll**.

- Von der *`log shipper`*-Prüfung wird ein Hintergrundprozess gestartet, über den entsprechend dem konfigurierten Protokollpfad der Prüfung Protokolle an eine Agent-Dateneingabe gesendet werden. Wenn Zugriffsberechtigungen fehlen oder der Protokollpfad falsch konfiguriert ist, wird vom System eine Warnung an die Instanz gesendet. Vergewissern Sie sich für eine ordnungsgemäße Protokollkonfiguration, dass der *`servicenow`*-Benutzer über Berechtigungen für den Zugriff auf den konfigurierten Protokollpfad auf dem Computer verfügt, auf dem der Agent gehostet wird, und dass der Protokollpfad richtig konfiguriert ist.
- Die Prüfung *`log shipper for win events`* ähnelt der Prüfung *`log shipper`*, aber es werden Ereignisprotokolle von Windows-Servern an die Agent-Dateneingabe gesendet.

  Hinweis: Zum Erfassen von Windows-Sicherheitsereignisprotokollen müssen *`servicenow`*-Benutzer auf einem Computer, auf dem der Agent gehostet wird, über Administratorrechte verfügen.

Agent Client Collector-Protokollrichtlinie erstellen

Erstellen Sie eine neue ACC-Protokollrichtlinie, wenn für das CI, das von Agent Client Collector überwacht werden soll, keine Standardrichtlinie vorhanden ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Die im ServiceNow Store verfügbare Anwendung Agent Client Collector Log Analytics (ACC-L) muss installiert sein. Weitere Informationen finden Sie unter Installation von Agent Client Collector.
- Agent Client Collector wird mit dem standardmäßigen *servicenow*-Benutzer bereitgestellt. Vergewissern Sie sich, dass dieser Benutzer Lesezugriff hat, damit von Agent Client Collector alle konfigurierten Protokollpfade angezeigt werden können. Beispielsweise verfügt der Agent Client Collector *servicenow*-Benutzer, der zusammen mit dem Basissystem installiert wird, nicht über Berechtigungen zum Anzeigen des Pfads zu `/var/log/` unter Linux und des Pfads zu `C:\Windows\System32` unter Windows. Informationen zum Konfigurieren von Berechtigungen für den *servicenow*-Benutzer finden Sie in der Now Support-Knowledge Base im Artikel ACC-L Permission Denied issues [KB1117271] (Probleme verweigerter ACC-L-Berechtigungen).

Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **ACC Log Analytics** > **ACC-Protokollrichtlinien**.
   Auf der Seite **Richtlinien** werden alle Log Analytics-Richtlinien angezeigt. Eine Liste der Richtlinien, die mit dem Basissystem bereitgestellt werden, finden Sie unter Agent Client Collector Log Analytics Standardrichtlinien und -prüfungen.
2. Klicken Sie auf **Neu**.

   Hinweis: Allgemeine Informationen zum Erstellen einer ACC-Richtlinie finden Sie unter Neue Agent Client Collector-Richtlinie erstellen.

3. Füllen Sie die Felder des Formulars aus.

Formular „Policy Definition“ (Richtliniendefinition)

Feld	Beschreibung
Name	Beschreibender Name für die Richtlinie
Beschreibung	Beschreibung der Richtlinie
Veröffentlichungsstatus	Hartcodiert als **Draft** (Entwurf), was bedeutet, dass die Richtlinie noch nicht veröffentlicht wurde. Dieses Feld können Sie nicht bearbeiten.
Hierarchie	Hartcodiert als **Keine**. Wenn der Richtlinie eine untergeordnete Richtlinie hinzugefügt wird, ändert sich der Wert in **Übergeordnet**. Untergeordnete Richtlinien haben den Wert **Untergeordnetes Element**.

4. Verknüpfen Sie auf der Registerkarte **Überprüfungen** die Protokollrichtlinie mit der entsprechenden Protokollversender-Überprüfung.
   - Wählen Sie für Linux und Windows (mit Ausnahme von Windows-Ereignisprotokollen) die Prüfungsdefinition *log shipper* aus.
   - Wählen Sie für Windows-Ereignisprotokolle die Prüfungsdefinition *log shipper for win events* aus.
5. Geben Sie auf der Registerkarte **Überwachte CIs** die CIs an, für die die Richtlinie gilt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie den zu überwachenden CI-Typ aus.

- **Überwachter CI-Typ nach Filter**: Wählen Sie den überwachten CI-Typ aus. Sie können die zu überwachenden CIs mithilfe von Filterbedingungen eingrenzen.
- **Überwachter CI-Typ nach Skript**: Geben Sie die überwachten CIs mithilfe eines Skripts an.
- **Überwachter CI-Typ nach CMDB-Gruppe**: Geben Sie die überwachten CIs mithilfe von CMDB-Gruppenabfragen an.

Weitere Informationen zur Auswahl überwachter CI-Typen finden Sie unter Neue Agent Client Collector-Richtlinie erstellen.

b. Wahlweise: Wenn Sie ausschließlich CIs überwachen möchten, die einem Anwendungsservice zugeordnet sind, wählen Sie **Überwachte CIs nach Anwendungsservice filtern** aus.
Sie können die zu überwachenden Anwendungsservices mithilfe von Filterbedingungen angeben. Von Agent Client Collector werden dann ausschließlich die Protokolle von CIs abgerufen, die diesen Anwendungsservices zugeordnet sind.

6. Speichern Sie die Protokollrichtlinie.
In der zugehörigen Liste „Instanzen überprüfen“ wird ein Datensatz für die Überprüfungsinstanz angelegt.

7. Öffnen Sie den entsprechenden Datensatz für die Überprüfungsinstanz, und wählen Sie dann **In Sandbox bearbeiten** aus.

8. Wählen Sie die zugehörige Liste „Log path configuration“ (Protokollpfadkonfigurationen) aus.

9. Fügen Sie einen Protokollpfad für die Überprüfungsinstanz hinzu.

Hinweis: Für eine Prüfung muss mindestens ein Protokollpfad konfiguriert sein, damit Protokoll-Streaming aktiviert werden kann. Weitere Informationen zu Prüfungen finden Sie unter Prüfungen und Richtlinien.

a. Wählen Sie **Neu**.

b. Füllen Sie die Felder des Formulars aus.

Formular für neue Pfadkonfiguration

Feld	Beschreibung
Pfad	Vollständiger Pfad, aus dem die Protokolle gestreamt werden sollen. Sie können einen Platzhalter verwenden. Dies ist ein Pflichtfeld.
Komponente	Gerätetypen oder Stapelebenen, die Kontext für die Protokolle bieten, die zur Anomalieerkennung und -korrelation verwendet werden. Beispiel: Tomcat.
Quelltyp	Definiert, wie von Health Log Analytics bestimmte Protokolltypen verarbeitet und die Protokolldaten analysiert werden sollen. Beispiel: Tomcat Catalina.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Wahlweise: Konfigurieren Sie für den Versand von mehrzeiligen Protokollen mit Filebeat die folgenden Eigenschaften.

(Optional) Mit diesen Parametern wird gesteuert, wie von Agent Client Collector Log Analytics (ACC-L) Nachrichten verarbeitet werden, die sich über mehrere Textzeilen erstrecken.

Weitere Informationen finden Sie unter Mehrzeilige Nachrichten verwalten in der Elastic-Dokumentation.

Feld	Beschreibung
multiline.pattern (regex)	Der entsprechende reguläre Ausdruck **Hinweis:** Sie müssen diese Eigenschaft definieren, bevor Sie die Eigenschaften multiline.match und multiline.negate konfigurieren können.
multiline.match	Wie ACC-L übereinstimmende Zeilen zu einer einzigen Protokollzeile kombiniert. (Optional) Die verfügbaren Optionen sind Keine, Vorher und Nachher. Standard ist Keine.
multiline.negate	Option, um zu bestimmen, ob das in den Protokollzeilen identifizierte Muster negiert wird. (Optional) Die verfügbaren Optionen sind Keine, Wahr und Falsch. Standard ist Keine.

d. Wahlweise: Definieren Sie die folgenden Eigenschaften, mit denen die Filebeat-YML-Konfiguration gesteuert wird.

Feld	Beschreibung
Felder	Feld, mit dem Sie Informationen in die Ausgabe einbeziehen und aus der Ausgabe ausschließen können. Sie können beispielsweise ein Feld zum Filtern der Protokolldaten hinzufügen. (Optional) Mit dem Plus-Symbol neben dem Wertfeld fügen Sie weitere Feldzeilen hinzu: ⊕. Mit dem Minus-Symbol entfernen Sie eine Feldzeile: ⊖. Weitere Informationen finden Sie in der Beschreibung der Felder

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	der Protokolleingabe in der Elastic-Dokumentation.
Konfigurationsoptionen	Feld, mit dem Sie den Protokollzeilen Konfigurationsoptionen hinzufügen können. Sie können beispielsweise die zu verwendende Codierung hinzufügen. **Hinweis:** Legen Sie nur Konfigurationsoptionen fest, die von Filebeat unterstützt werden. Weitere Informationen finden Sie in der Elastic-Dokumentation bei der Beschreibung der Konfigurationsoptionen der Protokolleingabe.

e. Wählen Sie **OK** aus.
Der Protokollpfad wird erstellt.

10. Wählen Sie **Zurück zur Richtlinie** aus.

11. Wählen Sie im Richtlinienformular die Option **Veröffentlichen** aus.
Der Veröffentlichungsstatus der Richtlinie ändert sich in **Veröffentlicht**.

12. Wahlweise: Aktivieren Sie die Richtlinie, indem Sie **Aktivieren** auswählen.

Nächste Maßnahme
Vergewissern Sie sich, ob von der Dateneingabe Daten gestreamt werden.

Untergeordnete Protokollrichtlinie erstellen

Verfeinern Sie eine vorhandene Protokollrichtlinie, um sich auf eine Teilmenge von CIs oder Services zu konzentrieren, indem Sie eine untergeordnete Richtlinie erstellen.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
Eine veröffentlichte Protokollrichtlinie (die übergeordnete Richtlinie) kann als Vorlage zum Erstellen einer neuen Protokollrichtlinie (der untergeordneten Richtlinie) verwendet werden. Sie können die Parameter anpassen, die die untergeordnete Richtlinie von der übergeordneten Richtlinie zum Zweck der Konzentration auf eine Untergruppe ihrer CIs oder Services übernimmt.

Die untergeordnete Richtlinie erbt Parameter von der übergeordneten Richtlinie, die nach der Erstellung der untergeordneten Richtlinie geändert werden, es sei denn, Sie deaktivieren diese Option in der untergeordneten Richtlinie. Sie können diese geänderten Parameter im Entwurfsmodus in jeder untergeordneten Richtlinie überprüfen, bevor Sie sie akzeptieren.

Hinweis: Die untergeordnete Richtlinie ist von Natur aus spezifischer als die übergeordnete Richtlinie. Wenn von Agent Client Collector eine Übereinstimmung mit einer in der untergeordneten Richtlinie definierten Bedingung festgestellt wird, erfolgt kein Abgleich mit der übergeordneten Richtlinie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **ACC Log Analytics** > **ACC-Protokollrichtlinien**.
2. Wählen Sie auf der Seite **Policies** (Richtlinien) eine veröffentlichte Richtlinie mit dem Hierarchiewert **None** (Keine) oder **Parent** (Übergeordnet) aus.
3. Wählen Sie **Untergeordnetes Element erstellen** aus.
   Es wird eine neue Richtlinie geöffnet, die dieselben Parameter aufweist, wie die veröffentlichte Richtlinie. Der Name der neuen Richtlinie lautet *<Policy name><date and time created>*.

   Beispiel: MySQL DB on Linux Logs 2022-02-13 04:44:12.

   Die folgenden Felder sind schreibgeschützt:

   Felder für untergeordnete Richtlinie

Feld	Wert
Veröffentlichungsstatus	Entwurf
Hierarchie	Untergeordnetes Element
Übergeordnet	<Name der übergeordneten Richtlinie>

   Der Wert im Feld **Reihenfolge** gibt die Priorität an, mit der der Agent im Verhältnis zu den gleichgeordneten Richtlinien an die untergeordnete Richtlinie angehängt wird. Eine niedrigere Zahl zeigt eine im Verhältnis höhere Priorität für die betreffende untergeordnete Richtlinie an. Standardmäßig nimmt jede neue untergeordnete Richtlinie einen höheren Wert (und daher eine niedrigere Priorität) an als die vorherige. Den Reihenfolgenwert können Sie bei Bedarf ändern.
4. Passen Sie die Parameter der untergeordneten Richtlinie an.
   Eine Beschreibung der Parameter finden Sie unter Agent Client Collector-Protokollrichtlinie erstellen.
5. Wählen Sie **Speichern** aus, um die untergeordnete Richtlinie zu erstellen.
6. Wahlweise: Wählen Sie **Vererbungsoption deaktivieren** aus, um die Option zu deaktivieren, dass geänderte Parameter automatisch von der übergeordneten Richtlinie geerbt werden.
7. Wählen Sie **Veröffentlichen** aus, um die untergeordnete Richtlinie zu veröffentlichen.

Ergebnisse
Die untergeordnete Richtlinie wird veröffentlicht und auf der Registerkarte **Untergeordnete Richtlinien** der übergeordneten Richtlinie angezeigt.

Protokollrichtlinie bearbeiten

Sie können veröffentlichte Agent Client Collector-Protokollrichtlinien bearbeiten. Ändern Sie beispielsweise eine Standardprotokollrichtlinie, wenn Ihre Organisation immer einen bestimmten nicht standardmäßigen Protokollpfad verwendet.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Prozedur

1. Navigieren zu **Alle** > **ACC Log Analytics** > **ACC-Protokollrichtlinien**.
2. Wählen Sie eine Richtlinie aus, für die der **Veröffentlichungsstatus** auf **Veröffentlicht** festgelegt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie **In Sandbox bearbeiten**.
   Daraufhin wird die Richtlinie in der **Draft view** (Entwurfsansicht) angezeigt, und Sie können ihre Felder und Prüfungsinstanzen bearbeiten.

   Hinweis: Auch in der **Draft view** (Entwurfsansicht) bleibt der Veröffentlichungsstatus der Richtlinie **Veröffentlicht**.

4. Bearbeiten Sie auf der Registerkarte **Überwachte CIs** die CIs, für die die Richtlinie gilt, je nach Bedarf.

   a. Wählen Sie den zu überwachenden CI-Typ aus.

   - **Überwachter CI-Typ nach Filter**: Wählen Sie den überwachten CI-Typ aus. Sie können die zu überwachenden CIs mithilfe von Filterbedingungen eingrenzen.
   - **Überwachter CI-Typ nach Skript**: Geben Sie die überwachten CIs mithilfe eines Skripts an.
   - **Überwachter CI-Typ nach CMDB-Gruppe**: Geben Sie die überwachten CIs mithilfe von CMDB-Gruppenabfragen an.

   Weitere Informationen zur Auswahl überwachter CI-Typen finden Sie unter Neue Agent Client Collector-Richtlinie erstellen.

   b. Wahlweise: Wenn Sie ausschließlich CIs überwachen möchten, die einem Anwendungsservice zugeordnet sind, wählen Sie **Überwachte CIs nach Anwendungsservice filtern** aus.
   Sie können die zu überwachenden Anwendungsservices mithilfe von Filterbedingungen angeben. Von Agent Client Collector werden dann ausschließlich die Protokolle von CIs abgerufen, die diesen Anwendungsservices zugeordnet sind.

5. Wahlweise: Wählen Sie in der Tabelle **Instanzen überprüfen** den Datensatz der Prüfungsinstanz des Protokollversenders aus, und bearbeiten Sie ihn.
   Weitere Informationen finden Sie unter Protokollpfadkonfigurationen bearbeiten.
6. Wählen Sie **Speichern** aus, um die Änderungen zu speichern, die Sie in den Richtlinienfeldern in der Sandbox eingegeben haben.
   Die Richtlinie bleibt in der **Draft view** (Entwurfsansicht), der **Publish status** (Veröffentlichungsstatus) lautet **Published*** (Veröffentlicht*). Das Sternchen (*) zeigt an, dass die aktuell veröffentlichte Version nicht die aktuellste ist, da sie gespeicherte Änderungen enthält, die noch nicht veröffentlicht wurden.
7. Wählen Sie **Erneut veröffentlichen** aus, um die Updates zu veröffentlichen.
   Die Richtlinie wird in den Status **Veröffentlicht** zurückversetzt und als veröffentlichte Richtlinie geöffnet.

   Hinweis: Diese Option wird nur nach der Bearbeitung von Richtlinienfeldern einer Richtlinie angezeigt, deren **Veröffentlichungsstatus** auf **Veröffentlicht*** festgelegt ist.

8. Bestimmen Sie den aktiven Status der Richtlinie, indem Sie entweder **Aktivieren** oder **Deaktivieren** auswählen.
9. Wahlweise: Wählen Sie **Löschen** aus, um sowohl die veröffentlichten Richtlinien als auch die Entwurfsrichtlinien zu löschen.

Protokollpfadkonfigurationen bearbeiten

Ändern Sie eine Protokollpfadkonfiguration in der Prüfungsinstanz des Protokollversenders.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **ACC Log Analytics** > **ACC-Protokollrichtlinien**.
2. Wählen Sie einen Richtliniendatensatz aus.
3. Wählen Sie in der zugehörigen Liste „Instanzen überprüfen“ den Datensatz der Prüfungsinstanz des Protokollversenders aus.
4. Wählen Sie **In Sandbox bearbeiten** aus, um die Bearbeitung des Datensatzes zu aktivieren.
5. Bearbeiten Sie in der zugehörigen Liste „Protokollpfadkonfiguration“ eine Protokollpfadkonfiguration.

   a. Wählen Sie die Protokollpfadkonfiguration aus, die Sie bearbeiten möchten.

   b. Bearbeiten Sie die Konfiguration.

   - Sie können anwenderdefinierte Felder hinzufügen, um zusätzliche Informationen in die Ausgabe aufzunehmen.
   - Sie können zusätzliche Konfigurationsoptionen hinzufügen, z. B. `„coding“`, `„include_lines“`und `„exclude_lines“`, um Ihre Protokolldaten zu filtern. Informationen zum Erkennen der Dateicodierung finden Sie im Artikel How to Detect File Encoding on Windows, Linux and Mac [KB1702770] (Erkennen der Dateicodierung unter Windows, Linux und Mac) in der Knowledge Base Now Support.

     Diese Konfigurationsoptionen wirken sich auf alle Dateien aus, die über die Dateneingabe an Ihre Instanz gestreamt werden.

     Hinweis: Legen Sie nur Konfigurationsoptionen fest, die von Filebeat unterstützt werden. Weitere Informationen finden Sie in der Elastic-Dokumentation bei der Beschreibung der Konfigurationsoptionen der Protokolleingabe.

   c. Wählen Sie **Aktualisieren** aus, um Ihre Änderungen zu speichern.

6. Wahlweise: Fügen Sie eine Umgebungsvariable hinzu, oder bearbeiten Sie eine vorhandene im Feld **Pfad**.
   Verwenden Sie das relevante Format für den Namen:
   - Schreiben Sie bei Linuxden Namen groß und stellen Sie ihm ein Dollar-Zeichen voran: $. Beispiel: `$HOME`. Beim Namen wird zwischen Groß- und Kleinschreibung unterschieden.
   - Bei Windowsumgeben Sie den Namen in Prozentzeichen: %. Beispiel: `%HOMEPATH%`. Beim Namen wird zwischen Groß- und Kleinschreibung unterschieden.

   Wichtig: Der ServiceNow-Anwender und der ACC-Mitarbeiter müssen Zugriff auf die Umgebungsvariable haben. Auf Linux -Systemen sind nur Umgebungsvariablen zugänglich, die sich in der Datei `„/etc/environment“` befinden. Fügen Sie dieser Datei die Umgebungsvariable im Format *<NAME>='<VALUE>'* hinzu.

7. Wahlweise: Löschen Sie einen Protokollpfad.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Aktivieren Sie das Kontrollkästchen neben der Protokollpfadkonfiguration, die Sie löschen möchten.

> **Hinweis:** Sie können mehrere Protokollpfadkonfigurationen auswählen, aber für eine Prüfung muss mindestens ein Protokollpfad konfiguriert sein, damit Protokoll-Streaming aktiviert werden kann. Weitere Informationen zu Prüfungen finden Sie unter Prüfungen und Richtlinien.

b. Wählen Sie **Löschen**.

8. Wählen Sie **Zurück zur Richtlinie** aus, um zum Datensatz der Protokollrichtlinie zurückzukehren.
9. Wählen Sie **Erneut veröffentlichen** aus, und bestätigen Sie dann den Vorgang, um die Richtlinie mit den aktualisierten Protokollpfadkonfigurationen erneut zu veröffentlichen. Die Änderungen werden in wenigen Minuten wirksam.

Probleme beim Protokoll-Streaming identifizieren und beheben

Vergewissern Sie sich, ob von den ACC-Dateneingaben Daten ordnungsgemäß gestreamt werden, indem Sie Probleme beim Protokoll-Streaming identifizieren und beheben.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird

Im Datensatz der ACC-Dateneingabe werden in der zugehörigen Liste „Streamingquellen“ die Streaming-Daten der Quellen der betreffenden Dateneingabe angezeigt. Anhand dieser Daten können Sie Streaming-Probleme und deren mögliche Ursache identifizieren.

Wenn beispielsweise der letzte Zeitpunkt des Ereignisses für den Endpunktserver einer Dateneingabe gestern war, ist dieser Server möglicherweise ausgefallen oder falsch konfiguriert. Ein Streaming-Problem kann auch dadurch verursacht werden, dass die Dateneingabe-Konfigurationsdatei nicht auf dem Endpunkt installiert ist.

> **Hinweis:** Sie können die Streaming-Daten aller Dateneingaben und die MID Servers, die Protokolle von ihnen empfangen, auf der Seite „Streamingquellen“ anzeigen. Weitere Informationen finden Sie in der Dokumentation der Anwendung ServiceNow Health Log Analytics unter Probleme beim Protokoll-Streaming identifizieren und beheben.

Prozedur

1. Navigieren zu **Alle** > **ACC-Dateneingaben** und wählen Sie einen Dateneingabedatensatz aus.
2. Wählen Sie im Dateneingabeformular die zugehörige Liste „Streamingquellen“ aus.
3. Überprüfen Sie die Streaming-Daten der Quellen dieser Dateneingabe.
   Eine Beschreibung der Filter finden Sie unter Streaming-Quellen für ACC-Dateneingaben.
4. Beheben Sie etwaig vorhandene Probleme beim Daten-Streaming.
   a. Navigieren zu **Alle** > **ACC Log Analytics** > **ACC-Protokollwarnungen**.
   b. Öffnen Sie Warnungen, und beheben Sie die angegebenen Probleme.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

Fahren Sie mit dem nächsten Schritt im Setup-Flow für Health Log Analytics-Dateneingaben fort. Weitere Informationen finden Sie unter Zusätzliche ACC-Dateneingaben einrichten.

Streaming-Quellen für ACC-Dateneingaben

Im Datensatz der ACC-Dateneingabe werden in der zugehörigen Liste „Streamingquellen“ die Streaming-Daten der Quellen der betreffenden Dateneingabe angezeigt.

Zugehörige Liste „Streamingquellen“

Filter	Beschreibung
Status	Status der Quelle. Ein rotes Aufzählungszeichen zeigt an, dass diese Quelle in der letzten Stunde keine Daten gestreamt hat.
Last event time (Zeit des letzten Events)	Die letzte aufgezeichnete Zeit, zu der auf dem MID-Server ein Event im letzten Ein-Minuten-Intervall eingetroffen ist. Health Log Analytics aktualisiert kontinuierlich die Zeit des letzten Events. Wenn die Zeit des letzten Events nicht aktuell ist, werden keine Daten gestreamt.
Raw log lines/sec (Protokollzeilen im Rohzutand/Sek.)	Die durchschnittliche Anzahl der Protokollzeilen im Rohzutand, die im letzten Ein-Minuten-Intervall pro Sekunde an den MID-Server gestreamt wurden. **Hinweis:** Dieser Wert stellt die Anzahl der Protokollzeilen im Rohzutand vor der Vorverarbeitung dar.
Preprocessed log lines/sec (Vorverarbeitete Protokollzeilen/Sek.)	Die durchschnittliche Anzahl der vorbearbeiteten Protokollzeilen, die im letzten Ein-Minuten-Intervall pro Sekunde an MID-Server gestreamt wurden. **Hinweis:** Dieser Wert kann sich von der Anzahl der Protokollzeilen im Rohzutand pro Sekunde unterscheiden. Beispielsweise kann der Unterschied darauf zurückzuführen sein, dass Protokolle während der Vorverarbeitung gelöscht wurden.

Protokollversenderwarnungen anzeigen

Zeigen Sie alle Protokollversender-Überprüfungswarnungen für Agents von Agent Client Collector Log Analytics (ACC-L) an.

Vorbereitungen

Erforderliche Rolle: agent_client_collector_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

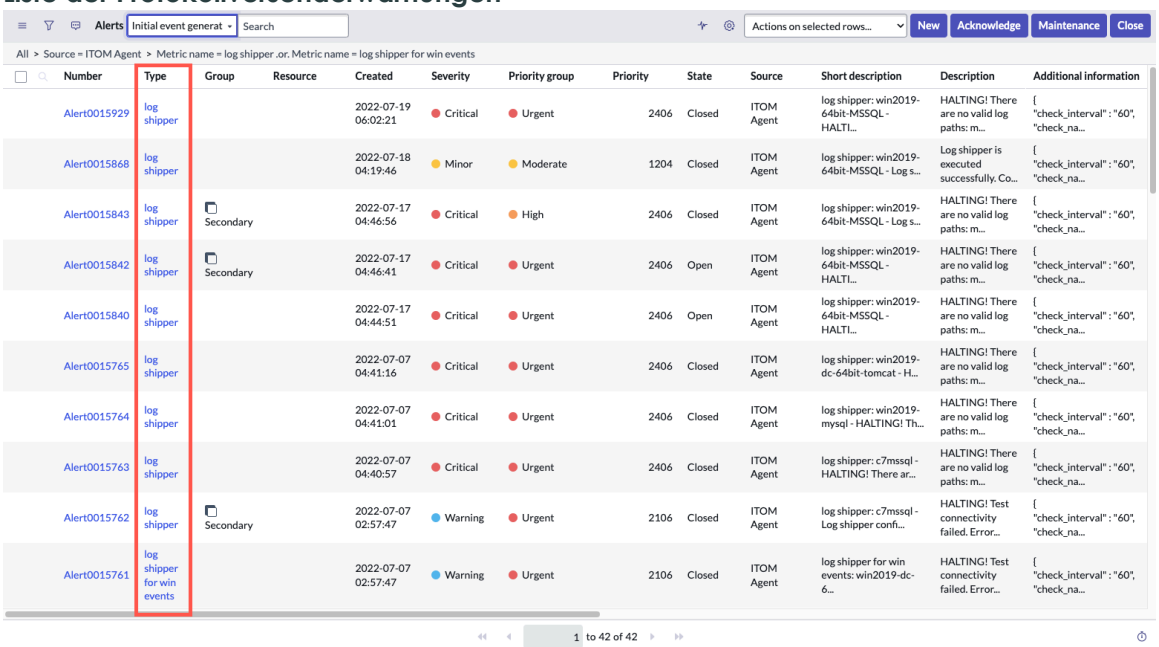
In der ACC-Warnungsliste können Sie auf einen Blick sehen, ob Probleme den Protokollversender daran hindern, Daten zu erfassen. In der Liste werden alle Warnungen im Zusammenhang mit dem Protokollversender an einem Ort angezeigt und Informationen zur Lösung der betreffenden Probleme bereitgestellt.

Die ACC-Warnungsliste enthält ausschließlich Warnungen über den Erfolg oder Misserfolg der Ausführung des Protokollversenders für ein CI für einen bestimmten Agent. Diese Warnungen sind eine Teilmenge der Warnungen, die in der Ereignismanagement-Warnungsliste angezeigt werden, die Warnungen aller Typen enthält. Weitere Informationen zur Ereignismanagement-Warnungsliste finden Sie unter Warnungsinformationen anzeigen.

Protokollversenderwarnungen werden aus Protokollversendererereignissen mit dem Schweregrad „Schwerwiegend“ oder „Kritisch“ generiert. Diese Warnungen beziehen sich normalerweise auf Protokollpfadprobleme oder fehlende Berechtigungen.

Hinweis: Wenn ein Ereignis mit Status **OK** für den Protokollversender für ein CI empfangen wird, für das eine offene Protokollversenderwarnung vorhanden ist, wird die offene Protokollversenderwarnung für dieses CI geschlossen.

Liste der Protokollversenderwarnungen



Prozedur

1. Navigieren zu **Alle** > **ACC Log Analytics** > **ACC-Protokollwarnungen**.
2. Überprüfen Sie die Informationen in der Warnungsliste.
   Details und eine Beschreibung der Spalten finden Sie unter Eingehende Warnungen überwachen.

Zugehörige Informationen

Protokollversendererereignisse anzeigen

Protokollversendererereignisse anzeigen

Zeigen Sie alle Protokollversendererereignisse mit allen Schweregraden für Agents von Agent Client Collector Log Analytics (ACC-L) an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: agent_client_collector_admin

Warum und wann dieser Vorgang ausgeführt wird
In der ACC-Ereignisliste werden alle Ereignisse im Zusammenhang mit dem Protokollversender an einem zentralen Ort angezeigt. Die Liste enthält ausschließlich Ereignisse über den Erfolg oder Misserfolg der Ausführung des Protokollversenders für ein CI für einen bestimmten Agent. Diese Ereignisse sind eine Teilmenge der Ereignisse, die in der Ereignismanagement-Ereignisliste angezeigt werden, die Ereignisse aller Arten enthält.

Prozedur

1. Navigieren zu **Alle** > **ACC Log Analytics** > **ACC-Protokollereignisse**.
2. Überprüfen Sie die Informationen in der Ereignisliste.
   Details und eine Beschreibung der Spalten finden Sie unter Events anzeigen.

Zugehörige Informationen

Protokollversenderwarnungen anzeigen

CI-Zuordnung zu einer dynamischen CI-Gruppe in Agent Client Collector Log Analytics

Wenn die Anwendung Agent Client Collector Log Analytics (ACC-L) ein CI erkennt, das keinem Anwendungsservice zugeordnet ist, erstellt die Anwendung eine dynamische CI-Gruppe und ordnet ihr das CI zu.

Eine dynamische CI-Gruppe ist eine Gruppe von CIs, die nach Attributen organisiert sind, z. B. dem CI-Typ. Standardmäßig werden mit Protokollrichtlinienprüfungen von Agent Client Collector nur CIs überwacht, die einem Anwendungsservice zugeordnet sind. Die Anwendung Agent Client Collector Log Analytics überprüft die CIs, die von Agent Client Collector erkannt werden. Wenn sie ein CI erkennt, das keinem Anwendungsservice zugeordnet ist, erstellt die Anwendung eine dynamische CI-Gruppe und ordnet ihr das CI zu.

Wenn das CI später einem tatsächlichen Anwendungsservice zugeordnet wird, wird seine Zuordnung zur dynamischen CI-Gruppe automatisch gelöscht. Die Baseline für das CI geht in diesem Prozess verloren. Während das System die neue Baseline einrichtet, gibt es keine Warnungen für den Anwendungsservice aus, dem das CI jetzt zugeordnet ist.

Sie können die Zuordnung nicht zugeordneter CIs zu einer dynamischen CI-Gruppe deaktivieren, indem Sie die Standardeinstellung der entsprechenden Systemeigenschaft *sn_accl.dynamic_service.creation.enabled* zu „false“ ändern. Die Anwendung Agent Client Collector Log Analytics verknüpft dann nicht zugeordnete CIs nicht mit dynamischen CI-Gruppen. In diesem Fall werden keine Protokolle für CIs gestreamt, die keinem Anwendungsservice zugeordnet sind.

Agent Client Collector Security Incident Response

Mit Agent Client Collector Security Incident Response (ACC-SIR) können Sie die Datenerfassungs- und Antwortaktionen für die Erweiterung von Security Incidents mit Agent Client Collector automatisieren. Diese Funktionalität wird durch Security Operations Security Incident Response (SIR) gemessen.

Wählen Sie aus einer Liste von Aktionen (Fähigkeiten), die mit dem Basissystem bereitgestellt werden, damit sie für Security Incidents ausgeführt werden können. Von der Agent Client Collector Security Incident Response-Funktionalität werden die Prüfungsdefinitionen `util.command.agent` und `util.osquery.agent` (ausgeführt von der Agent Client Collector-Spoke) dazu verwendet, Befehle und Betriebssystemabfragen für Security Incidents

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auszuführen. Fähigkeiten sind Teil vorhandener System-Subflows in der Agent Client Collector Security Incident Response-Integrations-App. Sie können auch benutzerdefinierte Befehle und OSquery-SQL-Abfragen hinzufügen, die für die Security Incidents ausgeführt werden.

Einzelheiten zu den mit Security Incident Responseinstallierten Plugins finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Agent Client Collector Security Incident Response-Fähigkeiten

Agent Client Collector Security Incident Response Die im Basissystem enthaltenen Fähigkeiten sind auf der Seite „ACC-Fähigkeiten“ aufgeführt (**Agent Client Collector-SIR-Integration > ACC-Integration – Fähigkeiten**) an. Diese Fähigkeiten werden für Security Incidents ausgeführt, um Informationen über den Incident zu sammeln.

Wählen Sie im Abschnitt „Zugehörige Links“ des Security Incident eine Fähigkeit aus der Option **Agent Client Collector Capabilities** (Agent Client Collector-Fähigkeiten) aus. Fähigkeiten sind Teil vorhandener System-Flows, auf die auf der Seite der ACC-Fähigkeiten verwiesen wird.

Agent Client Collector Security Incident Response-Fähigkeiten

Fähigkeitsname	Beschreibung	Flow
Angemeldete Anwender abrufen	Sammelt Daten zu angemeldeten Benutzern und bezieht sie auf den Security Incident	ACC SIR – Angemeldete Anwender abrufen
Netzwerkstatistiken abrufen	Sammelt Netzwerkstatistiken für das CI, das dem Security Incident zugeordnet ist	ACC SIR – Netzwerkstatistiken abrufen
Prozesse abrufen	Sammelt Prozessdaten und bezieht sie auf den Security Incident	ACC SIR – Prozesse abrufen
Get Services (Services abrufen)	Sammelt Servicedaten und bezieht sie auf den Security Incident	ACC SIR – Get Services (Services abrufen)
Systemdetails abrufen	Sammelt Systemdetails für das CI, das dem Security Incident zugeordnet ist	ACC SIR – Systemdetails
Befehl auf Agent ausführen	Führt einen benutzerdefinierten Befehl für Agent Client Collector aus und sendet Ergebnisse an den Security Incident	ACC SIR – Befehl aus Security Incident ausführen
OSQuery auf Agent ausführen	Führt eine benutzerdefinierte OSQuery für Agent Client Collector aus und sendet Ergebnisse an den Security Incident	ACC SIR – OSQuery aus Security Incident ausführen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion für einen Security Incident ausführen

Führen Sie eine Agent Client Collector Security Incident Response-Aktion aus, um weitere Informationen zu einem Security Incident zu sammeln. Aktionen werden im System als **Fähigkeiten** bezeichnet und mit dem Basissystem konfiguriert.

Vorbereitungen

Fügen Sie das folgende JSON-Skript Ihrer Allow-Liste von Agent Client Collector hinzu, um die Ausführung der im Basissystem enthaltenen Aktionen zu ermöglichen.

```
{
  "args": [
    "--logger_min_status 1",
    "--json",
    "SELECT p.name, p.state, p.pid, p.parent as ppid, p.path,
 p.total_size, p.start_time, p.elapsed_time as run_time, p.cmdline,
 p.uid, p.username, u.type as owner_domain, u.uuid FROM processes as p
 LEFT JOIN users as u ON u.uid = p.uid",
    "select name, process_open_sockets.pid, parent as ppid,
 processes.path, process_open_sockets.state, total_size,
 process_open_sockets.protocol, local_address, local_port,
 remote_address, remote_port from process_open_sockets, processes where
 process_open_sockets.pid = processes.pid",
    "select * from services order by service_type",
    "select computer_name, hardware_serial, hostname, name as
 os, build, version, mac, address from system_info, os_version,
 interface_details, interface_addresses where address like '%:%' and
 interface_addresses.type='manual' or interface_addresses.type ='dhcp'
 limit 1",
    "select * from logged_in_users order by time"
  ],
  "exec": "osqueryi",
  "skip_arguments": false
}
```

Erforderliche Rolle: sn_si.admin oder sn_si.basic

Warum und wann dieser Vorgang ausgeführt wird

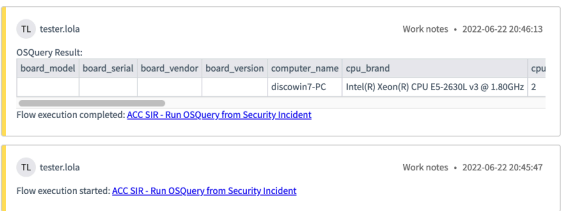
Weitere Informationen zu den Fähigkeiten, die mit dem Basissystem bereitgestellt werden, finden Sie unter Agent Client Collector Security Incident Response-Fähigkeiten.

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie einen Incident aus.
3. Wählen Sie im Abschnitt „Zugehörige Links“ **Agent Client Collector Capabilities** (Agent Client Collector-Fähigkeiten) aus.
   Das Dialogfeld **Agent Client Collector Capabilities** (Agent Client Collector-Fähigkeiten) wird geöffnet.
4. Wählen Sie die Fähigkeit aus, die Sie ausführen möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Agent Client Collector-Fähigkeiten

Feld	Beschreibung
ACC Integration Capabilities (ACC-Integrationsfähigkeiten)	Die ACC-Integrationsfähigkeiten. Wenn die Fähigkeit „Osquery auf Agent ausführen“ ausgewählt ist, werden die Daten in den Arbeitsnotizen tabellarisch formatiert.
ACC Integration OSQuery (OSQuery-Abfrage der ACC-Integration)	Die Osquery-Abfrage der ACC-Integration. Beispiel: ausgewählte Systeminformationsspalten.
Kontrollkästchen „Transpose Data“ (Daten transponieren)	Transponieren Sie die Daten. Bei Auswahl werden die Informationen mit vertikalen Spalten angezeigt. TL tester.lola Work notes • 2022-06-22 21:01:57 *All system info columns* result on *discowin7-PC* board_model board_serial board_vendor board_version computer_name discowin7-PC cpu_brand Intel(R) Xeon(R) CPU E5-2630L v3 @ 1.80GHz cpu_logical_cores 2 cpu_microcode cpu_physical_cores 1 cpu_subtype -1 cpu_type x86_64 hardware_model VMware Virtual Platform hardware_serial VMware-42 1d e0 2b db d0 a4 28-c6 45 ef 26 8c 0a 72 37 hardware_vendor VMware, Inc. hardware_version -1 hostname discowin7-PC.discolab1.service-now.com local_hostname discowin7-PC physical_memory 4277657600 uuid 2BE01D42-D0DB-28A4-C645-EF268C0A7237 Flow execution completed: ACC SIR - Run OSQuery on Affected CI Wenn diese Option deaktiviert ist, werden die Informationen horizontal angezeigt.  TL tester.lola Work notes • 2022-06-22 20:46:13 OSQuery Result: board_model board_serial board_vendor board_version computer_name cpu_brand cpu discowin7-PC Intel(R) Xeon(R) CPU E5-2630L v3 @ 1.80GHz 2 Flow execution completed: ACC SIR - Run OSQuery from Security Incident TL tester.lola Work notes • 2022-06-22 20:45:47 Flow execution started: ACC SIR - Run OSQuery from Security Incident

5. Wählen Sie **Absenden** aus.
   Die ausgewählte Fähigkeit wird für das CI des Security Incident ausgeführt.

Zugehörige Informationen

Agent Client Collector-Zulassungsliste generieren

Agent Client Collector Security Incident Response-Befehl erstellen

Definieren Sie einen Befehl oder eine Befehlszeichenfolge, der/die auf einem Computer ausgeführt werden soll, auf den ein Security Incident verweist. Befehle werden nach Betriebssystem aufgelistet. Beispielsweise wird mit einem *ps*-Befehl unter einem Windows-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Betriebssystem der Status aktiver Windows-Betriebssystemprozesse auf dem System abgerufen.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector-SIR-Integration** > **ACC-Integration – Befehle**.
2. Wählen Sie **Neu**.
   Die Seite **ACC Integration Commands – New Record** (ACC-Integrationsbefehle – Neuer Datensatz) wird angezeigt.
3. Konfigurieren Sie die Felder auf der Seite.

ACC Integration Commands (ACC-Integrationsbefehle)

Feld	Beschreibung
Name	Ein beschreibender Name für den Befehl
Betriebssystem	Das von Agent Client Collector unterstützte Betriebssystem des CI
Befehl	Der tatsächlich auszuführende Befehl oder die tatsächlich auszuführende Befehlszeichenfolge

4. Um zu überprüfen, ob der von Ihnen geschriebene Befehl funktioniert, wählen Sie **Test Command**(Befehl testen) aus.
   Die Seite **Test Command** (Befehl testen) wird angezeigt.

Test Command (Befehl testen)

Feld	Beschreibung
Mitarbeiter	Der spezifische Endpunkt, an dem der Befehl ausgeführt wird.

5. Geben Sie den spezifischen Endpunkt-Agent ein, auf dem das Ergebnis des Tests angezeigt wird.
   - – im Erfolgsfall
   - – Ausgabe zu groß
   - – oder es ist ein Fehler mit der Fehlermeldung aufgetreten, die für den sn_si.admin angezeigt wird.
6. Wählen Sie **Absenden** aus.

Agent Client Collector Security Incident Response-Befehl ausführen

Führen Sie einen angegebenen Befehl auf einem Computer aus, auf den ein Incident verweist, um Informationen zum CI des Incidents abzurufen. Wenn Sie beispielsweise einen *ps*-Befehl für einen Incident ausführen, wird mit dem Befehl der Status aktiver Prozesse auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dem System abgerufen. Befehle werden entsprechend dem CI-Betriebssystem aufgelistet, das dem Security Incident zugeordnet ist.

Vorbereitungen
Erforderliche Rolle: sn_si.admin oder sn_si.basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie einen Incident aus.
3. Wählen Sie im Abschnitt „Zugehörige Links“ **Agent Client Collector Capabilities** (Agent Client Collector-Fähigkeiten) aus.
   Das Dialogfeld **Agent Client Collector Capabilities** (Agent Client Collector-Fähigkeiten) wird geöffnet.
4. Wählen Sie **Befehl auf Agent ausführen** aus.
5. Wählen Sie im Feld **ACC Integration Capabilities** (ACC-Integrationsfähigkeiten) die Option **Befehl auf Agent ausführen** aus.
   Das Feld**ACC Integration Command** (ACC-Integrationsbefehl) wird angezeigt.
6. Wählen Sie den Befehl aus, den Sie ausführen möchten.
   Die verfügbaren Befehle sind diejenigen, die auf der Seite „ACC Integration Commands“ (ACC-Integrationsbefehle) konfiguriert sind, wie in Agent Client Collector Security Incident Response-Befehl erstellen beschrieben.
7. Wählen Sie **Absenden** aus.
   Der Befehl wird gemäß dem im Befehl angegebenen Betriebssystem für das CI des Security Incident ausgeführt.

Agent Client Collector Security Incident Response-OSQuery erstellen

Definieren Sie eine OSQuery, um Informationen zum CI eines Security Incident zu sammeln. OSQuery bietet eine SQL-Ebene zusätzlich zu BS-Tabellen und wird zusammen mit Agent Client Collector als Teil des Basissystems gebündelt.

Vorbereitungen
Erforderliche Rolle: sn_si.admin

Prozedur

1. Navigieren zu **Alle** > **Agent Client Collector-SIR-Integration** > **ACC-Integration – OSQuery**.
2. Wählen Sie **Neu**.
   Die Seite **ACC Integration OSQuery – New Record** (ACC-Integrations-OSQuery – Neuer Datensatz) wird angezeigt.
3. Konfigurieren Sie die Felder auf der Seite.

ACC Integration OSQuery (OSQuery-Abfrage der ACC-Integration)

Feld	Beschreibung
Name	Ein beschreibender Name für die Abfrage
Abfrage	Abfragezeichenfolge.

4. Um zu überprüfen, ob die von Ihnen geschriebene Abfrage funktioniert, wählen Sie **Test Osquery**(Osquery testen) aus.
   Die Seite **Test Osquery** (Osquery testen) wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Test Osquery (Osquery testen)

Feld	Beschreibung
Mitarbeiter	Der spezifische Endpunkt, an dem die Abfrage ausgeführt wird.

5. Geben Sie den spezifischen Endpunkt-Agent ein, auf dem das Ergebnis des Tests angezeigt wird.

- – im Erfolgsfall
- – Ausgabe zu groß
- – oder es ist ein Fehler mit der Fehlermeldung aufgetreten, die für den sn_si.admin angezeigt wird.

6. Wählen Sie **Absenden** aus.
Von OSQueries werden Informationen auf dem Zielcomputer erfasst, wobei die Incident-Befehle nach Betriebssystem aufgelistet sind. Beispielsweise werden von einer Abfrage, die als *`select * from system_info`* definiert ist, alle Informationen aus der OSQuery-Tabelle *`system_info`* abgerufen.

Agent Client Collector Security Incident Response-OSQuery ausführen

Führen Sie eine Osquery auf einem Computer aus, auf den ein Incident verweist, um Informationen zum CI des jeweiligen Incidents abzurufen. Wenn Sie beispielsweise die Abfrage *`select * from system_info`* ausführen, werden mit der Abfrage alle Informationen aus der OSQuery-Tabelle *`system_info`* abgerufen.

Vorbereitungen

Erforderliche Rolle: sn_si.admin oder sn_si.basic

Prozedur

1. Navigieren zu **Alle** > **Security Incident** > **Incidents** > **Alle Incidents anzeigen**.
2. Wählen Sie einen Incident aus.
3. Wechseln Sie im Abschnitt „Zugehörige Links“ zur Liste der **Konfigurationselemente**, und wählen Sie die CIs der einzelnen Incidents aus, für die Sie die Informationen abrufen möchten.
4. Wählen Sie im Kontextmenü die Option **Run ACC Osquery** (ACC-Osquery ausführen) aus.
Das Dialogfeld **Osquery to run** (Auszuführende Osquery) wird geöffnet.
5. Wählen Sie den Namen der Abfrage aus, die Sie ausführen möchten.
Die verfügbaren Abfragen sind diejenigen, die auf der Seite „ACC Integration Osquery“ (Osquery-Abfrage der ACC-Integration) konfiguriert sind, wie in Agent Client Collector Security Incident Response-OSQuery erstellen beschrieben. Optionen können entsprechend ihrem Wert für „Name“ ausgewählt werden.
6. Wählen Sie **Absenden** aus.
Die Abfrage wird für die CIs der jeweils ausgewählten Security Incidents ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Live-CI-Daten mit Agent Client Collector anzeigen

Zeigen Sie über Agent Client Collector Live-Daten für Incident-bezogene CIs an, um Informationen zu erhalten, die zur Lösung der Incidents beitragen können.

Vorbereitungen

- Das Sammeln laufender Prozesse für ein System macOS erfordert `sudo` -Berechtigungen. Wenn keine `sudo` -Berechtigungen gewährt werden, werden nur Prozesse erfasst, die von Agent Client Collector ausgeführt werden.

  Um `sudo` -Berechtigungen für osquerii zu aktivieren, fügen Sie die folgenden Zeichenfolgen entweder der Datei „`/etc/sudoers`“ oder einer einzelnen Datei im Verzeichnis „`/etc/sudoers.d`“ hinzu:

  - `Cmnd_Alias live_CI_VIEW = /Library/Application\ Support/servicenow/agent-client-collector/osquery/bin/osqueryp`
  - `_servicenow ALL=(ALLE) NOPASSWD:live_CI_VIEW`
- Damit die ausführbare OSQuery-Datei Informationen zu angemeldeten Benutzern in einer Windows-Umgebung abrufen kann, muss der Agent als lokales SYSTEM-Konto ausgeführt werden.

Vergewissern Sie sich, dass Agent Client Collector Framework und Mitarbeiterbereich (*com.agent_workspace*) in Ihrer -Instanz installiert sind.

Erforderliche Rolle: itil

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereicherfahrung** > **Arbeitsbereiche** > **Mitarbeiterbereich-Startseite**.
2. Wählen Sie das Listensymbol ( ) aus.
3. Auswahlvorgang **Incidents** > **Alle**.
4. Wählen Sie einen Incident aus der Liste aus.
5. Auf der<name of incident> Wählen Sie im Formular die Registerkarte **Live-CI-Daten**.
   Die CI-Daten werden auf den in der folgenden Tabelle beschriebenen Karten angezeigt.

Karten der Registerkarte „Live CI Data“ (Live-CI-Daten)

Karte	Beschreibung
Gerätedetails	Allgemeine Details zum CI
Speicherauslastung	Vom CI verwendeter Arbeitsspeicher
Top 5 running processes by CPU usage (Top 5 der laufenden Prozesse nach CPU-Auslastung)	Die fünf CI-Prozesse mit der meiste CPU.
Top 5 der laufenden Prozesse nach Arbeitsspeichernutzung	Die fünf CI-Prozesse, die den meisten Arbeitsspeicher verwenden.
Festplattenauslastung in %	Prozentsatz des vom CI verwendeten Speicherplatzes
Angemeldete Benutzer	Benutzer, die beim CI angemeldet sind. Ob diese Daten sichtbar sind, hängt von Ihren Betriebssystemberechtigungen ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Karte	Beschreibung
	◦ MacOS: sudo-Berechtigungen erforderlich ◦ Windows-System: Erfordert Administratorrechte ◦ Linux: Es sind keine besonderen Berechtigungen erforderlich

Zeigen Sie Live-CI-Datenprotokolle an

Zeigen Sie CI-Protokolle an, um zusätzliche Details zu einem Incident zu erhalten, wenn Sie Live-CI-Daten anzeigen. Wenn Sie beispielsweise Protokollinformationen für einen Prozess mit hoher CPU-Auslastung anzeigen, können Sie genau bestimmen, wann die Auslastung gestiegen ist, und die Ursache des Problems ermitteln.

Vorbereitungen

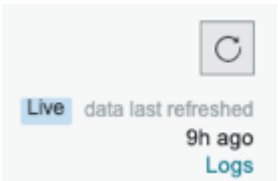
Vergewissern Sie sich, dass Agent Client Collector Framework und Mitarbeiterbereich (*com.agent_workspace*) in Ihrer -Instanz installiert sind.

Erforderliche Rolle: itil

Prozedur

1. Navigieren zu **Alle** > **Arbeitsbereicherfahrung** > **Arbeitsbereiche** > **Mitarbeiterbereich-Startseite**.
2. Wählen Sie das Listensymbol ( ) aus.
3. Auswahlvorgang **Incidents** > **Alle**.
4. Wählen Sie einen Incident aus der Liste aus.
5. Wählen Sie die Registerkarte **Live CI Data** (Live-CI-Daten) aus.
6. Wählen Sie den Link **Protokolle** auf der rechten Seite des Bereichs.

Link „Protokolle“



Hinweis: Der Wert **data last refreshed** (letzte Aktualisierung der Daten) folgt der Zeitzone der Instanz und nicht der Zeitzone Ihres lokalen Systems. Stellen Sie daher sicher, dass die Zeitzone Ihres lokalen Systems mit der Zeitzone der Instanz übereinstimmt.

Die Protokolle werden auf der Seite **„Protokoll“** angezeigt.

Weisen Sie seinem Incident ein problematisches CI zu, um Live-CI-Daten anzuzeigen

Rufen Sie Live-CI-Daten ab, um die Probleme zu beheben, die einen Incident verursacht haben, indem Sie das problematische CI seinem Incident zuweisen. Ein Incident ist normalerweise dem CI zugeordnet, das den Incident verursacht hat. Wenn dies jedoch bei der Incident-Erstellung vernachlässigt wurde, können Sie das CI manuell zuweisen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: itil

Prozedur

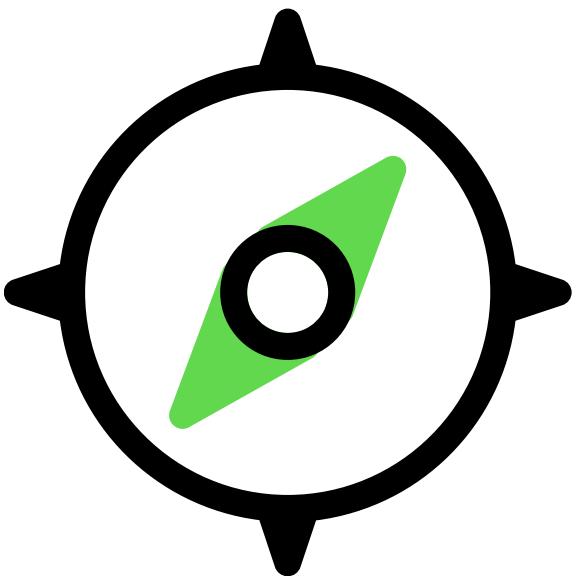
1. Navigieren zu **Alle** > **Arbeitsbereicherfahrung** > **Arbeitsbereiche** > **Mitarbeiterbereich-Startseite**.
2. Wählen Sie das Symbol Listen ( ) aus.
3. Auswahlvorgang **Incidents** > **Alle**.
4. Wählen Sie einen Incident mit dem Wert **Configuration item = (leer)**aus.
5. Wählen Sie die Registerkarte **Live CI Data** (Live-CI-Daten) aus.
6. Geben Sie im Feld **Primäres Konfigurationselement** die ersten Zeichen des CI ein, das den Incident verursacht hat.
   Eine Liste der CIs, die der Zeichenfolge entsprechen, wird angezeigt.
7. Wählen Sie das relevante CI aus der Liste aus.
   Der Name des CI wird im Feld **Primäres Konfigurationselement** angezeigt, und die Live-Daten des CI werden auf der Registerkarte **Live-CI-Daten** angezeigt.

Metrikdaten

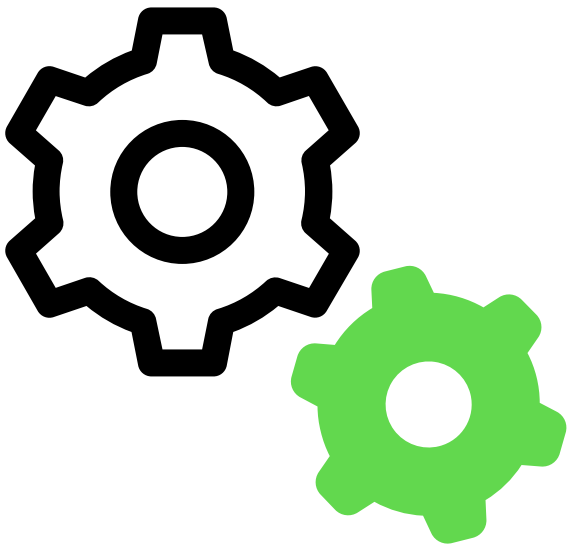
ServiceNow® Metrikdaten bietet die Möglichkeit, operative Metrikdaten zu erfassen und anschließend zu untersuchen und zu analysieren, um Anomalien zu identifizieren und anzuzeigen. Metrikdaten generiert Anomaliewarnungen, die zu IT-Warnungen hochgestuft werden können und im Service Operations-Arbeitsbereich und im Dashboard für Serviceintegrität angezeigt werden können. Sie können diese Analyse nutzen, um potenzielle Serviceausfälle zu vermeiden.

Erste Schritte

Untersuchen



Konfigurieren



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

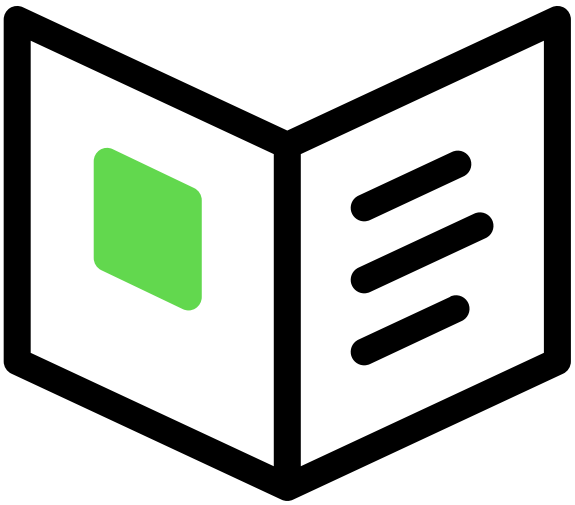
Lernen Sie die wichtigsten Funktionen und den Geschäftsnutzen der Anwendung Metrikdaten kennen.

Konfigurieren Sie die Funktionen und Komponenten, um Metrikdatenzu aktivieren.

Optimieren

Verwalten Sie Metriken, Ereignisse, Warnungen und Anomalien, um Ihre Metrikdaten optimal zu nutzen.

Referenz



Rufen Sie zusätzliche Informationen zu den Einstellungen und Eigenschaften Metrikdaten von ab.

Hilfreiche Ressourcen

Einige ServiceNow -Ressourcen, die Ihnen hilfreiche Informationen liefern können, sind:

- ServiceNow Community
  ServiceNow Community
- Customer Success Center
  Customer Success Center
- Entwickler
  developer.servicenow.com
- Impact
  http://impact.servicenow.com
- ServiceNow University
  ServiceNow University
- NowCreate
  Now Create
- Partner
  https://www.servicenow.com/partners.html

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

ServiceNow

http://ServiceNow.com

ServiceNow Store

http://ServiceNow.com

Unterstützung

- https://support.servicenow.com/now
- Known Error-Portal

Metrikdaten erkunden

Erfahren Sie mehr über die Verwendung von Metrikdaten zum Analysieren von Metrikdaten und Identifizieren von Anomalien.

Metrikdaten – Übersicht

Metrikdaten hilft, potenzielle Serviceausfälle zu erkennen und zu vermeiden. Metrikdaten zeigt basierend auf historischen Metrikdaten ein anomales Verhalten von CIs an, das von Ereignissen möglicherweise nicht erfasst wird.

Metrikdaten – Anwender

Anwender

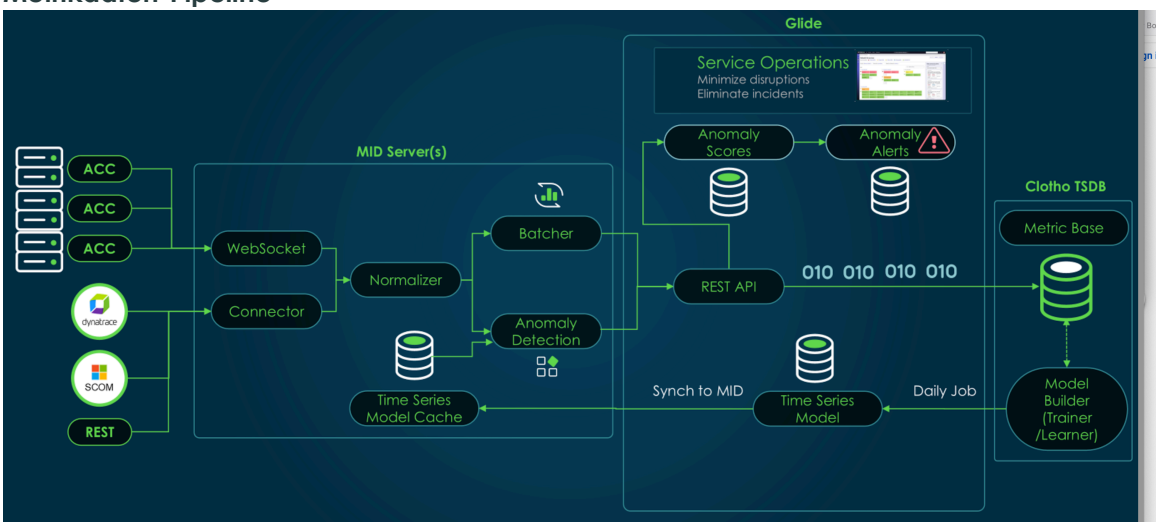
Anwender	Beschreibung
Ereignismanagement-Anwender [evt_mgmt_user]	Kann Warnungen und die zugrunde liegenden Metriken anzeigen.
Ereignismanagement-Administrator [evt_mgmt_admin]	Kann alle Metrikdefinitionen und Connector-Einstellungen konfigurieren.
Betreiber [evt_mgmt_operator]	Kann alle Metrikdefinitionen und Connector-Einstellungen anzeigen.

Metrikdaten – Workflow

In der folgenden Abbildung werden das Layout und der Datenfluss in der Anwendung Metrikdaten beschrieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikdaten-Pipeline



1. Datenerfassung: -Agents, Drittanbieter-Connectors und anwenderdefinierte Connectors (REST) erfassen Leistungsdaten von Servern und Infrastrukturkomponenten. Von Agents erfasste Daten werden über WebSocket an MID-Server übergeben, und von Drittanbieter-Connectors und benutzerdefinierten Connectors erfasste Daten werden über den -Connector an MID-Server übergeben.
2. Datennormalisierung: Rohdaten werden vom Normalizer so formatiert, dass sie für die Metrikbasis lesbar sind.
3. Datengruppierung: Daten werden vom Batcher gruppiert und an die REST API in der Instanz (Glide) gesendet.
4. Datenübertragung an Clotho-TSDB: Die REST API verarbeitet Daten und sendet sie an die Clotho-TSDB.
5. Modellerstellung: Der Trainer/Lerner-Auftrag wird ausgeführt und erstellt ein Modell basierend auf den empfangenen Daten. Beispielsweise kann die Aufgabe erfahren, dass der Schwellenwert für die normale CPU-Auslastung 60 % beträgt. Jeden Tag wird ein neues Modell erstellt, das auf den Daten dieses Tages und früheren Daten basiert (die meisten Modelle sammeln Daten aus den letzten 14 Tagen).
6. Übertragung von Modelldaten in die Zeitreihenmodell-Cache-DB: Die Daten werden über die Instanz (Glide) an die Zeitreihenmodell-Cache-DB auf dem MID-Server gesendet. Der Modell-Cache speichert die Grenzen des „normalen“ Modells.
7. Anomalie-Erkennung: Daten außerhalb der Grenzen des Normalwerts werden von MID-Server erkannt und als Anomaliepunktzahl gerendert. Anomalien werden in der Instanz gespeichert und im Service Operations-Arbeitsbereichangezeigt. Die Erkennung von Anomalien wird in Echtzeit durchgeführt, sodass Kunden sofort auf Anomalien aufmerksam gemacht werden.

Metrikdaten – Vorteile

Vorteil	Funktion	Anwender
Überwachen Sie den Zustand, die Leistung und die Verfügbarkeit Ihres Systems durch die automatisierte Erfassung von Ereignissen und Metriken und nutzen Sie automatisierte Konfigurationen.	Agent Client Collector-Überwachung	NOC-Operator, Ereignismanagement Administrator

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorteil	Funktion	Anwender
Reduzieren Sie Rauschen, indem Sie nur die relevantesten Anomalien heraufstufen.	Zeigen Sie Anomaliewarnungen an Metrikregeln erstellen	Ereignismanagement-Administrator
Erkennen Sie Anomalien mit der KI-basierten Anomalie-Erkennung, entweder mit der nicht überwachten Erkennung von anomalen Mustern durch maschinelles Lernen (kein Benutzereingriff) oder durch Festlegen deterministischer Warnungsregeln (manuelles Festlegen eines statischen Schwellenwerts).	Wie Health Log Analytics Warnungen generiert	Ereignismanagement-Administrator
Verbessern Sie die Lösungszeit offener Warnungen und Incidents mit der Visualisierung von Metrikrohdaten.	Metric Explorer	NOC-Operator, Ereignismanagement Administrator

Empfehlungen für weitere Themen

Weitere Informationen über die Konfiguration und den Einsatz von Metrikdaten finden Sie unter:

- Metrikdaten konfigurieren
- Wird optimiert Metrikdaten
- Metrikdaten – Referenz

Metrikdaten verstehen

Verwenden Sie Metrikdaten, um potentielle Serviceausfälle zu erkennen und zu verhindern. Metrikdaten, das auf historischen Metrikdaten basiert, weist auf anomales Verhalten von CIs hin, das von Events möglicherweise nicht erfasst wird. Anomaliewarnungen können zu regulären IT-Warnungen hochgestuft werden und werden im Service Operations-Arbeitsbereich und im Dashboard für Serviceintegrität angezeigt, um vorbeugende Maßnahmen zu ergreifen.

Anomalie-Erkennung

Metrikdaten werden von verschiedenen Datenquellen wie SCOM, dem SolarWinds-Überwachungssystem oder dem Nagios XI-Server (einige sind teilweise standardmäßig für die Metriksammlung konfiguriert) gesammelt. Diese Überwachungssysteme sammeln regelmäßig Metrikdaten aus der Quellumgebung. Metrikdaten erfasst die Rohdaten aus diesen Überwachungssystemen und verwendet Ereignisregeln und die CMDB-Identifizierungs-Engine, um Daten zu bestehenden CIs und deren Ressourcen zuzuordnen. Die Daten werden dann analysiert, um Anomalien zu erkennen und andere statistische Punktzahlen bereitzustellen.

Metrikdaten verwendet historische Metrikdaten, um statistische Modelle zu erstellen. Diese Modelle erleichtern die Projektion der erwarteten Metrikwerte zusammen mit der oberen und der unteren Grenze. Metrikdaten verwendet dann diese Projektionen, um statistische Ausreißer zu erkennen und Anomaliepunktzahlen zu berechnen. Anomalien werden in einem Bereich von 0 bis 10 bewertet. Hohe Anomaliepunktzahlen für CI-Metriken können darauf hinweisen, dass bei einem CI das Risiko eines Serviceausfalls besteht.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nach der Verarbeitung zeigt der Explorer für Einblicke Metrikstatistiken und Diagramme an, und die Anomaliezuordnung zeigt über eine Zeitleiste korrelierte Punktzahlen für die CIs mit den höchsten Anomaliepunktzahlen an.

Gegebenenfalls empfiehlt es sich, die Anomalie-Erkennung während der Systemwartung zu deaktivieren, da Anomalien irrelevant sein können, wenn sie während der Wartung erkannt werden. Legen Sie dazu die Eigenschaft *mid.mi.anomaly_detection.disable* auf **true** fest.

Um die Anzeige von Anomalien für als nahezu konstant klassifizierte Metriken anzupassen, wenden Sie sich an den Kundensupport.

Metrikdaten ist verfügbar, wenn Sie das Plugin Metrikdaten (com.snc.sa.metric) aktivieren.

Mit Metrikdaten verwendete Begriffe

Quellmetriktyp

Eine Metrik wie „% freier Speicherplatz“ oder „Aktuelle Bandbreite“, die von einer Datenquelle für ein CI gemessen werden kann. Für jede Datenquelle können Sie auswählen, welcher der möglichen Quellmetriktypen verarbeitet wird. Beispielsweise sind etwa 380 Quellmetriktypen für die SCOM-Datenquelle standardmäßig aktiv.

Abweichung

Daten, die außerhalb der Kontrollgrenzen liegen, werden als statistische Ausreißer betrachtet. Diese Ausreißer werden zur Berechnung einer Anomaliepunktzahl verwendet, die einem Wert zwischen 0 und 10 entspricht und den Grad angibt, zu dem die Metrik unwahrscheinlich erscheint. Wenn eine Anomaliepunktzahl über einem Schwellenwert liegt, wird eine Anomaliewarnung generiert. Anomaliewarnungen werden getrennt von regulären IT-Warnungen gemeldet.

Ressource

Eine Komponente eines CI, die aus mehreren einzelnen Komponenten ähnlichen Typs besteht, wobei jede Unterkomponente separat überwacht werden kann. Beispielsweise einzelne Webseiten oder bestimmte Datenträger wie „Datenträger C:“ und „Datenträger D:“.

Zeitreihen

Eine Reihe von Werten (z. B. Metrikwerte) über einen Zeitbereich, die einem CI und einem Metriktyp zugeordnet sind. Da für jede Metrik eine Anomaliepunktzahl ausgewertet wird, entspricht die Reihe der Anomaliepunktzahlen über einen Zeitraum auch einer Zeitreihe. Zeitreihen werden vom statistischen Modell berechnet, das für eine Metrikdatenreihe erstellt wurde, und werden mit Metrikdatenwerten, Anomaliepunktzahlen sowie der oberen und der unteren Kontrollgrenze verwendet.

Statistische Modelle

Metric Intelligence-Aufträge lernen aus vergangenen Metrikdaten (bis zu 32 Tage alt). Ein Modelltrainingsprozess analysiert historische Daten, um ein Modell zu erstellen, das zukünftige Werte projiziert. In der Regel sind Modelle bis zur nächsten Ausführung des Modelllernprozesses gültig. Diese Modelle werden zur Berechnung der oberen und der unteren Grenze verwendet. Eingehende Werte, die diese Grenzen überschreiten und deren statistische Signifikanz von den erwarteten Werten abweicht, generieren Anomalien. Jedes Modell weist ein eindeutiges Muster auf und ist mit einem Klassifizierer versehen, der das allgemeine Verhalten des Modells veranschaulicht. Diese Klassifizierung bestimmt, ob eine Anomalie-Erkennung angewendet werden kann. Die meisten Modelle können projizieren, welche zukünftigen Werte von den erwarteten Werten abweichen. Derartige Modelle sind

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontrollgrenzen zugeordnet und die Anomalie-Erkennung kann angewendet werden (falls aktiviert).

Für einige Modelle sind jedoch nicht genügend Daten vorhanden, um zu bestimmen, welche Werte anomal sind. In diesem Fall kann die Anomalie-Erkennung nicht ohne zusätzliche Informationen angewendet werden (selbst wenn die Anomalie-Erkennung aktiviert ist).

Die gelernten Datenmodelle werden in der Tabelle „Metrikzeitreihenmodell“ [sa_time_series] gespeichert.

Die folgenden statistischen Modelle und Klassifizierer werden bei der Anomalie-Erkennung verwendet:

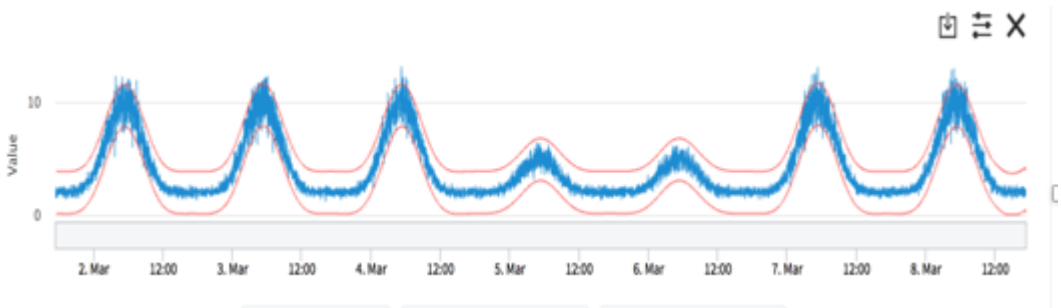
Statistisches Zeitreihenmodell

Nach der Einrichtung passt sich ein Zeitreihenmodell nicht an Änderungen in den eingehenden Metrikdaten an. Wenn sich daher das Muster eingehender Daten ändert, werden diese Änderungen wahrscheinlich als anomal eingestuft. Die obere und die untere Kontrollgrenze bleiben, nachdem sie erlernt wurden, bis zur nächsten Ausführung des Lernprozesses bestehen (Daten werden jeden Tag gelernt).

Wöchentlich

Daten mit einem Muster, das sich über wöchentliche Intervalle wiederholt (saisonales Modell).

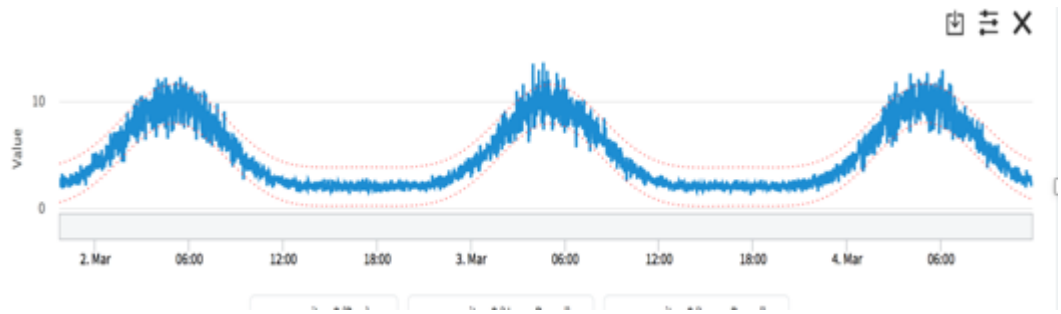
Erfordert Daten von mindestens 15 Tagen in der Reihe, wie in der Konfigurationseinstellung week_model_min_days festgelegt.



Täglich

Daten mit einem Muster, das sich über tägliche Intervalle wiederholt (saisonales Modell).

Erfordert Daten von mindestens 3 Tagen in der Reihe, wie in der Konfigurationseinstellung daily_model_min_days festgelegt.

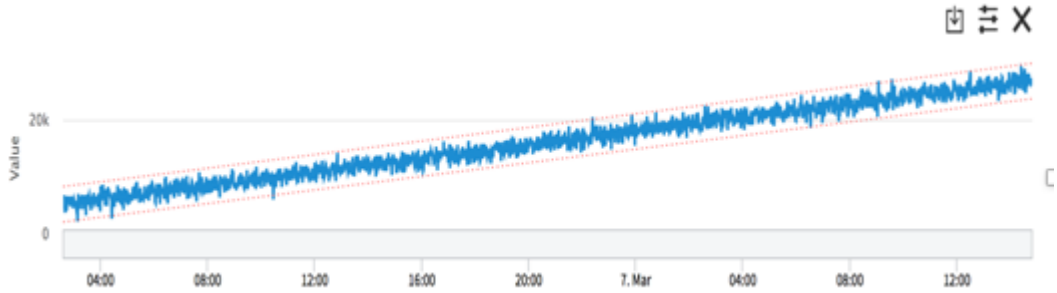


Mit Trend

Daten mit einem linearen Trend mit einer gewissen Steigung und mit einigem Rauschen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

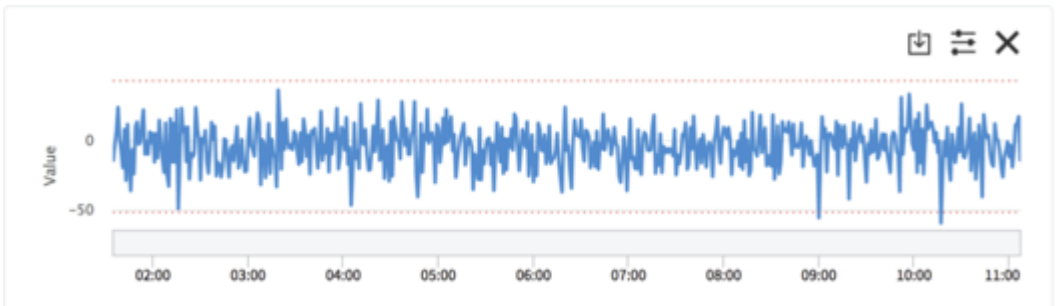
Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.



Verrauscht

Typische verrauschte Daten, die eine grundlegende Musterklassifizierung in einem Datenmodell darstellen. Das Muster lässt sich nicht mit einem bestimmten Trend oder einer bestimmten Saisonabhängigkeit identifizieren.

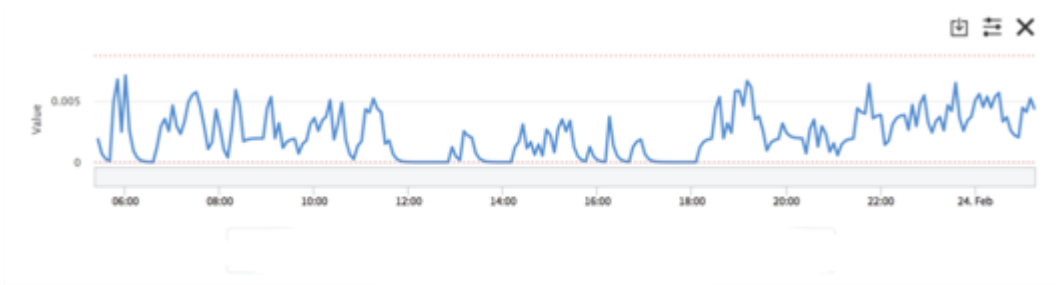
Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.



Positiv abgeschnitten verrauscht

Ähnlich dem verrauschten Klassifizierer mit Ausnahme der unteren Grenze, die auf 0 festgelegt ist.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.



Zentriert verrauscht

Verrauschte Daten, die sich typischerweise symmetrisch zwischen der benutzerdefinierten oberen und unteren Grenze ausbreiten. Die Formel, die zum Festlegen von Begrenzungen und Breitenwerten verwendet wird, ignoriert die statistischen Daten, und die untere und die obere Breite haben einen identischen Wert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erfordert, dass die Anzahl der Datenpunkte in der Reihe gleich Null ist.

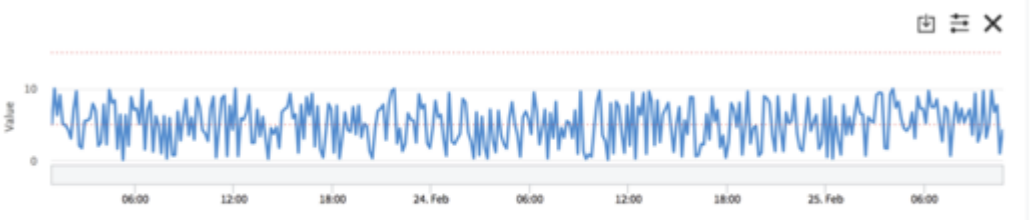
Weitere Informationen finden Sie unter Benutzerdefinierte Ober- und Untergrenzen für Metriken festlegen.

Verzerrt verrauscht

Verrauschte Daten, die nicht gleichmäßig zwischen der benutzerdefinierten oberen und unteren Grenze verteilt sind, sondern sich stattdessen tendenziell näher an einer der Grenzen konzentrieren. Der Median der Daten wird verwendet, um eine obere und eine untere Breite getrennt zu berechnen.

Erfordert mindestens einen Datenpunkt in der Reihe.

Weitere Informationen finden Sie unter Benutzerdefinierte Ober- und Untergrenzen für Metriken festlegen.



Verzerrtes Rauschen – Allgemeine Extremwertverteilung (Genaralized Extreme Value, GEV)

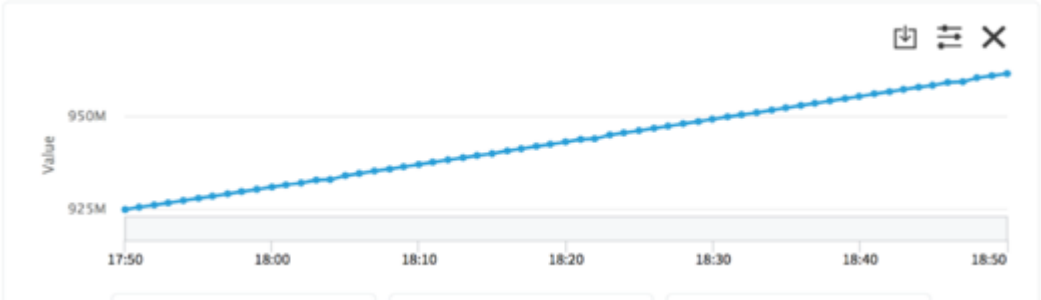
Verrauschte Daten, die nicht gleichmäßig zwischen der benutzerdefinierten oberen und unteren Grenze verteilt sind, sondern sich stattdessen tendenziell näher an einer der Grenzen konzentrieren. Außerdem weist die Datenverteilung ein langes Verteilungsende oder einen schweren Rand auf. Der vom Rand/Ende der Verteilung abgeleitete Median der Daten wird dazu verwendet, gesondert eine obere und eine untere Breite zu berechnen. Die Serie muss mindestens einen Datenpunkt enthalten.

Akkumulator

Datenmuster ähnlich dem Trend-Klassifizierer, aber mit monotonem Anstieg und ohne Rauschen. Für diesen Klassifizierer gibt es kein Datenmodell und keine Anomalie-Erkennung.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.

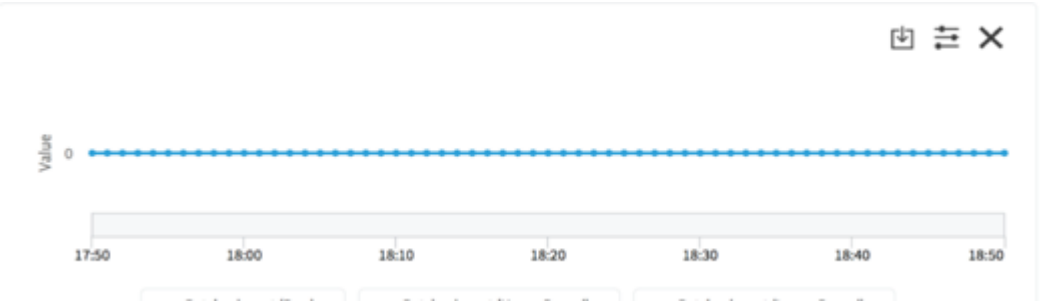
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Nahezu konstant

Nahezu konstante Daten, bei denen die meisten Werte einem spezifisch konstanten Wert entsprechen. Für diesen Klassifizierer gibt es kein Datenmodell und keine Anomalie-Erkennung.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.



Erkannte Konstante

Aktiviert die Überprüfung von nahezu konstanten Metriken auf Anomalien. Dazu müssen Sie die Metriken über ein System-Token in das Modell für erkannte Konstanten verschieben. Um der Tokenliste Token hinzuzufügen und die Messung weiterer Metriken für Anomalien zu ermöglichen, wenden Sie sich an den Kundensupport.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.

Aktiviert, wenn die Systemeigenschaft `metric_name_analyse.add_detected_constant_candidate` auf **wahr**festgelegt ist. Um den Wert dieser Eigenschaft für einen bestimmten Metriktyp zu überschreiben, aktualisieren Sie das Feld **Erkannter Konstantenkandidat** in der Tabelle Metriktypen wie folgt:

1. Geben Sie im Instanznavigationsfeld `sa_metric_type.list` ein.
2. Wählen Sie in der Spalte **„Kandidat für erkannte Konstante“** den entsprechenden Wert für den Eintrag aus, den Sie aktualisieren möchten.

Erkannte konstante Kandidatenwerte

Wert	Beschreibung
<empty>	Ein Algorithmus hat automatisch entschieden, ob die Metrik für das erkannte Konstantenmodell berücksichtigt werden soll.

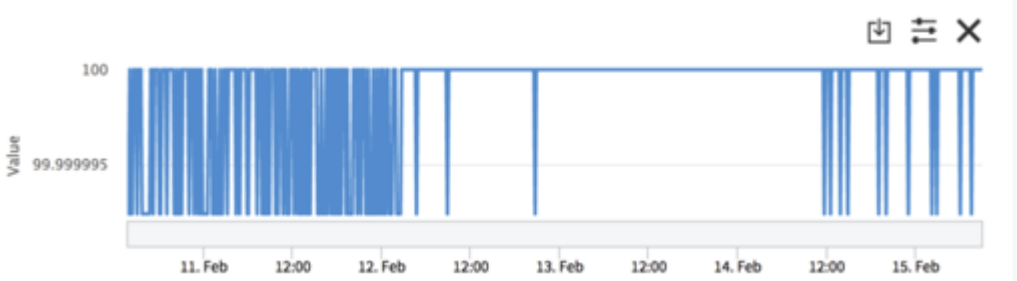
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
	Dies ist der Standardwert.
Ja	Die Metrik wird für das erkannte konstante Modell berücksichtigt.
Nein	Die Metrik wird für das erkannte Konstantenmodell nicht berücksichtigt.

Multinomial

Datenmuster, in dem alle Werte zu einer relativ kleinen Anzahl von Werten gehören. Beispielsweise lauten die Werte immer 100 oder 99,9. Für diesen Klassifizierer gibt es kein Datenmodell und keine Anomalie-Erkennung.

Erfordert mindestens 400 Datenpunkte in der Reihe, berechnet als 10-facher Wert der Konfigurationseinstellung multinomial_count_threshold.



Beschädigt

Die Daten haben nicht genügend Datenpunkte, um ein Muster zu identifizieren. Für diesen Klassifizierer gibt es kein Datenmodell und keine Anomalie-Erkennung.

Erfordert, dass die Anzahl der Datenpunkte in der Reihe kleiner als der Wert der Konfigurationseinstellung corrupt_data_count_threshold (standardmäßig 30) ist.

Kalman-Filter – statistisches Modell

Add-on zum statistischen Zeitreihenmodell, das nur auf den verrauschten und positiv verrauschten Klassifizierer anwendbar ist. Dieses Modell ist eine allgemeine Methode zum Schätzen von Modellparametern aus einem Datenstrom, bei dem das Level der einzige Parameter im Modell ist. Das Kalman-Filtermodell kann an neue Werte in eingehenden Metrikdaten angepasst werden. Wenn das Rauschen keine eindeutigen Muster aufweist oder zu viel Rauschen vorhanden ist, wird das Kalman-Filtermodell nicht verwendet.

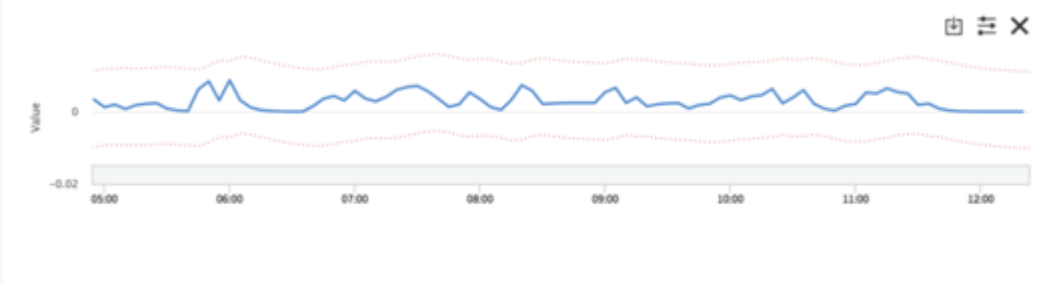
Lokales Level

Wenn eingehende Daten entsprechend den aktuellen Kontrollgrenzen um einen neuen Wert herum gruppiert werden, passt der Lernende das Datenmodell an, um einer permanenten Änderung Rechnung zu tragen. Dieses Clustering wird als neuer Wert im Datenmodell erkannt, sodass die meisten eingehenden Daten wieder innerhalb der Kontrollgrenzen liegen und nicht anomal sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine solche Change-Erkennung ist nützlich, wenn z. B. einem Server Kerne oder Arbeitsspeicher hinzugefügt werden, die sich auf die Baselines auswirkt.

Erfordert mindestens 30 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung corrupt_data_count_threshold festgelegt.



Nicht erkannt

Wenn Daten nicht zum Klassifizierer auf lokalem Level passen, werden Klassifizierer für Zeitreihen verwendet. Dies geschieht, wenn es nicht möglich ist, das Abweichungsverhältnis in einem erlernten Modell auf lokalem Level auf angemessene Werte anzupassen.

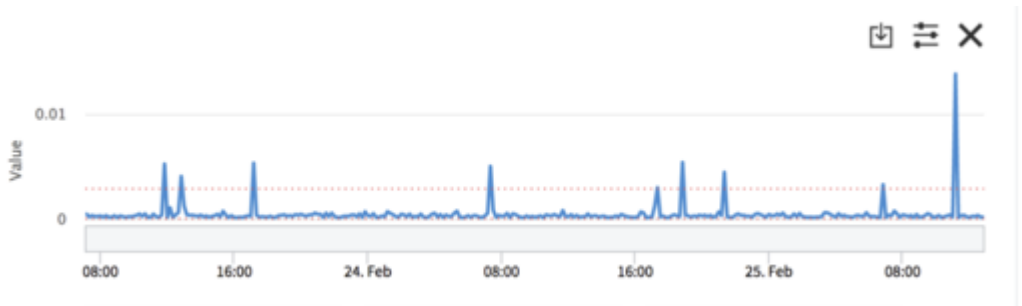
Nicht-parametrisches statistisches Modell

Add-on zum positiven verrauschten Klassifizierer. Im nicht-parametrischen Modell ist die Rauschverteilung nicht symmetrisch und entspricht keinem saisonalen Muster. Das nicht-parametrische Modell erstellt Kontrollgrenzen, die besser zu den tatsächlichen Daten passen, und die einmal gelernten Kontrollgrenzen bleiben bis zum nächsten Lernzyklus erhalten. Dieses Modell passt sich nicht an Änderungen in den Daten an, und es dauert länger, bis eine Abweichung als Anomalie erkannt wird.

Stationär, nicht parametrisch

Daten, die nicht zeitabhängig sind, was bedeutet, dass es bei der zeitlichen Verschiebung von Daten zu keiner signifikanten Verschiebung von Parametern wie Mittelwert und Abweichung kommt.

Erfordert mindestens 5.000 Datenpunkte in der Reihe, wie durch die Konfigurationseinstellung snpm_minimum_data_count festgelegt.



Nicht erkannt

Wenn Daten nicht zum stationären Klassifizierer passen, werden Klassifizierer für Zeitreihen verwendet.

Statistisches Modell der mittleren absoluten Abweichung vom Median (Median Absolute Deviation, MAD)

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ein Add-on zum verzerrten verrauschten Klassifizierer. Bei diesem Datentyp ist die Rauschverteilung nicht symmetrisch und entspricht keinem saisonalen Muster. Darüber hinaus entsprechen die Daten einer Verteilung mit langem Verteilungsende oder schwerem Rand. Im statistischen Modell der mittleren absoluten Abweichung vom Median werden Kontrollgrenzen erstellt, die besser zu den tatsächlichen Daten passen; die einmal gelernten Kontrollgrenzen bleiben dabei bis zum nächsten Lernzyklus erhalten. Durch Verwendung dieses Modells fällt die Entschlüsselung der Datenerfassung etwa 30 % effizienter aus.

MID Server und verteilter MID Server-Cluster für Metric Intelligence

Zur Nutzung von Metrikdaten muss mindestens ein verteiltes MID-Server-Cluster vorhanden sein, das einen einzelnen MID-Server enthält, der für Metrikdaten konfiguriert ist.

Wenn Sie einen einzelnen Metrikdaten MID-Server verwenden, muss dieser Server einem verteilten MID-Server-Cluster hinzugefügt werden.

Um den angegebenen Durchsatz zu unterstützen, erstellen Sie ein verteiltes Cluster mit einem einzelnen MID-Server, der die Metrikdaten MID-Server-Anforderungen erfüllt. Bei Verwendung eines virtuellen Computers (Virtual Machine, VM) kann nur ein einzelner MID-Server ausgeführt werden, der Metrikdaten unterstützt. Bei der Arbeit mit Agent Client Collector kann ein MID-Server auch mit mehreren Agents (ACC-M und ACC-L) verbunden werden.

Ein MID-Server, der Discovery unterstützt, kann auch mit anderen Anwendungen verwendet werden.

Weitere Informationen zum Einrichten von Metrikdaten finden Sie unter Erste Schritte mit Metrikdaten.

Verteilte MID Server-Cluster

Durch die Aktivierung Metrikdaten von (com.snc.sa.metric) wird automatisch MID-Server der verteilte Cluster (com.snc.agent.distributed.cluster) aktiviert. Ein verteilter Cluster MID-Server unterstützt den Clustertyp Verteilt MID-Server, der ausschließlich mit Metrikdatenverwendet wird.

Wenn die automatische Erstellung eines verteilten Clusters MID-Server fehlschlägt, können Sie den Cluster manuell konfigurieren. Weitere Informationen erhalten Sie vom Kundensupport.

Metrikdaten MID-Server

Der Metrikdaten MID-Server unterstützt die Metrikdaten-Funktion, indem Daten verarbeitet und Anomalien erkannt werden. Vom MID-Server werden Stapel verarbeiteter Daten an die Instanz übermittelt. Wenn eine Anomalie erkannt wird, werden Informationen über die Anomalie zusammen mit den Rohdaten sofort an die Instanz gesendet.

Jeder Metrikdaten MID-Server muss mit den folgenden Einstellungen konfiguriert werden:

- Metrikdaten als unterstützte Anwendung
- Die Metriken-Fähigkeit
- Metriken-Erweiterung Metrikdaten wird ausgeführt

Mit der Metrikdaten-Anwendung, mit der der Metrikdaten MID Server konfiguriert ist, können Sie zusätzliche unterstützte Anwendungen auf dem gleichen MID Server hinzufügen. Standardmäßig ist Metrikdaten in der Definition der MID Server-Option „ALLE“ enthalten. Informationen zum Ändern des Verhaltens der Option ALLE bei der Auswahl unterstützter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendungen finden Sie unter In ALLEN Anwendungen enthaltene Anwendungen konfigurieren .

Wenn „Domain Support – Domain Extensions Installer“ aktiviert ist, können Sie einen MID Server mit der Metrics-Fähigkeit pro Domäne konfigurieren. In diesem Fall werden Metriken für einen Business Service auf dem MID Server verarbeitet, der sich in derselben Domäne wie der Business Service befindet. Andernfalls wird ein MID Server aus der globalen Domäne verwendet.

Stellen Sie für den MID Server, den Sie für Metric Intelligence konfigurieren möchten, Folgendes sicher:

- Er ist validiert. Weitere Informationen finden Sie unter MID-Server validieren
- Er wird ausgeführt.
- Er erfüllt alle Software-, Hardware- und Konfigurationsanforderungen.

Hardwareanforderungen für den virtuellen Computer/Host, auf dem der MID Server ausgeführt wird (skaliert für 5.000 CIs mit 100 Metriken pro CI)

Anforderung	
Eine MID-Server mit: • Arbeitsspeicher: 12 GB • Prozessor: 4 Kerne	Unterstützt bis zu ca. 1,2 Millionen Metriken (12.000 CIs mit 100 Metriken pro CI).
Eine MID-Server mit: • Arbeitsspeicher: 24 GB • Prozessor: 8 Kerne	Unterstützt bis zu ca. 1,7 Millionen Metriken (17.000 CIs mit 100 Metriken pro CI).

Software-Anforderungen

Software	Unterstützte Versionen	Zusätzliche Anforderungen
Windows	32-Bit- und 64-Bit-Versionen: • Windows 2008 R2 • Windows Server 2012 R2 • Windows Server 2019	32-Bit- oder 64-Bit-Version des MID-Servers
Linux	• Red Hat Enterprise Edition Linux 6.6 oder höher • CentOS Linux 6.6 oder höher	32-Bit- oder 64-Bit-Version des MID-Servers

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsanforderungen

Konfiguration	Anforderung
MID-Server-Serviceanmeldeanwender (nur zum Abrufen erforderlich)	Muss auf einen Benutzer mit Lesezugriff auf die SCOM-Datenbank (OperationsManagerDW) festgelegt werden. **1.** Öffnen Sie auf dem MID Server das MID Server-Dialogfeld **Eigenschaften**. **2.** Klicken Sie auf die Registerkarte **Anmeldung**. **3.** Wählen Sie **Dieser Account** aus, und geben Sie die Anmeldeinformationen für einen Benutzer mit dem erforderlichen Zugriff ein. **4.** Klicken Sie auf **Übernehmen**.

MID-Server-Drosselungsmechanismus

Der MID-Server-Drosselungsmechanismus schützt vor Daten-Bursts in der Instanz. Der Daten-Burst-Schutz verhindert eine Überlastung der Instanz und stellt gleichzeitig sicher, dass keine Daten verloren gehen.

Der MID-Server-Drosselungsmechanismus ist standardmäßig aktiviert. Es empfiehlt sich, diesen Mechanismus bei der Problembehandlung zu deaktivieren, damit gewährleistet ist, dass der Mechanismus keine Systemfehlfunktionen verursacht.

- Um diese Funktion für Metriken zu deaktivieren, legen Sie den Parameter mid.oi.metric_token_bucket_enabled auf **false** fest.
- Um diese Funktion für Anomalien zu deaktivieren, legen Sie den Parameter mid.oi.anomaly_token_bucket_enabled auf **false** fest.

Konfigurationsüberschreibung

Aktualisieren Sie die Datei `wrapper-override.conf` im Ordner `../agent/conf`:

- Fügen Sie den folgenden Code am Ende der Datei hinzu:

```
# GC
wrapper.java.additional.5=-XX:+AlwaysPreTouch
wrapper.java.additional.6=-XX:+UseG1GC
wrapper.java.additional.7=-XX:+ScavengeBeforeFullGC
wrapper.java.additional.8=-XX:+DisableExplicitGC

# IP4
wrapper.java.additional.9=-DpreferIPv4Stack=true
```

- Vergewissern Sie sich, dass `wrapper.java.initmemory=1024` (oder höher) und `wrapper.java.maxmemory=4096` (oder höher) festgelegt sind, damit Metrikdaten ordnungsgemäß funktioniert.
- Optional können Sie, wenn auf einem Server zusätzlicher Arbeitsspeicher verfügbar ist, z. B. 16 GB RAM, in `wrapper.java.maxmemory=4096` den Wert 4096 durch 8192 ersetzen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikkonfigurationsregeln

Mit Metrikkonfigurationsregeln können Sie bestimmen, wie eingehende Metriken aus Agent Client Collector verarbeitet werden sollen.

Wenn eine neue Metrik von Agent Client Collector eintrifft, wird in der Tabelle „Metrik-Zuordnung an CIs“ ein neuer Datensatz mit dem Wert **Aktionsebene der Anomalie-Erkennung = Grenzen** erstellt.

Um die Ausführung einer Metrikkonfigurationsregel auszulösen, navigieren Sie zur Tabelle „Metrikkonfigurationsregeln“ (**Ereignismanagement** > **Anomalie-Erkennung** > **Konfig.-Regeln für Metrik**), und wählen Sie die Schaltfläche **Mit MID synchronisieren** oben auf der Seite aus. Damit werden auch alle mit der Instanz verbundenen MID Server synchronisiert.

Beim Ausführen der Regel überschreibt die in der Regel definierte Aktionsebene der Anomalie-Erkennung (durch den Parameter *anomaly_detection_action_level* festgelegt) rückwirkend die Aktionsebene der Anomalie-Erkennung, die für die Metrik in der Tabelle „Metrik-Zuordnung an CIs“ konfiguriert ist.

Wenn Sie die Regelausführung nicht auslösen, wird während der Ausführung der stündlich geplanten Aufgabe **Metric Intelligence – Metrikkonfiguration** der Parameter *Anomaly detection action level* rückwirkend überschrieben.

Beim Konfigurieren einer Metrikkonfigurationsregel werden Regeln mit einem Filter vor Regeln ohne Filter ausgeführt. Wenn mehrere Regeln dieselbe Priorität aufweisen, wird die zuletzt konfigurierte Regel zuerst ausgeführt.

Weitere Informationen zum Erstellen von Konfigurationseinstellungsregeln finden Sie unter Regel für Konfigurationseinstellungen erstellen.

Einzelheiten zu den verfügbaren Aktionsebenen der Anomalie-Erkennung finden Sie unter Konfigurieren Sie die Aktionsebene für die Anomalie-Erkennung.

Empfindlichkeit der Metrikgrenzen

Beim Messen von Metriken im Explorer für Einblicke können Metrikgrenzen zu sensibel sein, was zu einer ungewöhnlich großen Anzahl von Anomalien führt. In diesem Fall passt sich das System selbst an, um sicherzustellen, dass weniger Anomalien erzeugt werden.

Wenn 95 % der Metrikwerte eines CI innerhalb von 2 Standardabweichungen (STDs) der mittleren Metrikwerte liegen, werden diese als *sensitive bounds* betrachtet. Mit sensiblen Grenzen wird eine große Anzahl von Anomalien generiert, von denen einige möglicherweise nicht relevant sind. Wenn sensible Grenzen erkannt werden, passt sich das System an und misst Metrikwerte innerhalb von 5 STDs, um weniger Anomalien zu generieren. Wenn keine sensiblen Grenzen erkannt werden (d. h. 95 % der Metriken liegen nicht innerhalb von 2 STDs des mittleren Metrikwerts), misst das System Metrikwerte innerhalb von 3 STDs. Alle Metrikwerte, die außerhalb der konfigurierten Grenzen liegen, werden zu Anomalien.

Die vorherigen Werte sind standardmäßig festgelegt. Details zum Anpassen dieser Werte finden Sie unter Eigenschaften der Empfindlichkeitsgrenzen für Metriken im Explorer für Einblicke.

Metriksammlungsquellen

Beim Einrichten von Metrikdatenmüssen Sie eine Quelle für die Metriksammlung konfigurieren. Die Metriksammlung kann entweder von Agent Client Collectoroder von Metrik-Connectors durchgeführt werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Metriksammlungsquelle bestimmt, woher Metrikdaten Metriken sammelt. Weitere Informationen zum Sammeln von Metriken mit Agent Client Collectorfinden Sie unter Agent Client Collector-Überwachung konfigurieren.

Verwenden Sie zum Sammeln von Metriken mit Connectors entweder einen SCOM- oder einen Dynatrace -Connector. Einzelheiten zum Verbinden von Metriken mit einem SCOM-Connector finden Sie unter SCOM-Connector-Instanz konfigurieren.

Einzelheiten zum Verbinden von Metriken mit dem Connector Dynatrace finden Sie unter Konfigurieren Sie die Connector-Instanz Dynatrace ..

Metrikbindung

Nachdem Metrikdaten gesammelt wurden, identifiziert Metric Intelligence die CIs und die Ressourcen, an die die Daten gebunden werden sollen.

Die auf dem MID Server erfassten Daten sind Rohdaten, die sich nicht auf ein bestimmtes CI oder eine bestimmte Ressource in der CMDB beziehen. Um nützlich zu sein, durchlaufen die Daten einen **Normalisierungsprozess**, der CMDB-Identifizierungsregeln und Ereignisregeln verwendet, um CIs eindeutig zu identifizieren und sie den Rohdaten zuzuordnen und an diese zu binden. Rohdaten können auch Ressourcen zugeordnet und an diese gebunden werden, wenn die Bindung an ein CI erfolgreich und die Ressourcenbindung konfiguriert ist.

Datensätze für die Zuordnung von Rohdaten zu CIs werden automatisch generiert und bleiben für eine bestimmte, durch die Eigenschaften festgelegte Zeitspanne wirksam:

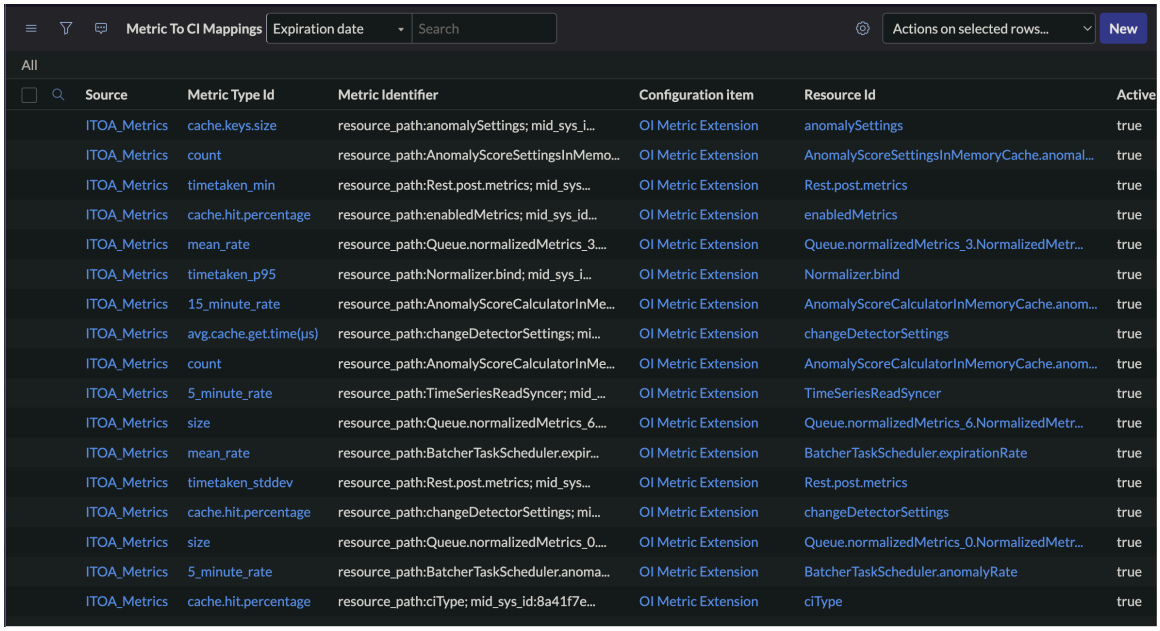
- *sa.metric.map.with.ci.expiration.sec*: Wenn die Zuordnung zum CI gefunden wurde. Standardmäßig auf eine Gültigkeitsdauer von fünf Tagen eingestellt.
- *sa.metric.map.without.ci.expiration.sec*: Wenn die Zuordnung zum CI nicht gefunden wurde. Standardmäßig auf eine Gültigkeitsdauer von 24 Stunden eingestellt.

Wenn ähnliche Metrikdaten innerhalb dieses Zeitraums eingehen, wird die vorhandene Zuordnung verwendet, um die Daten den CIs zuzuordnen. Am Ende des Zeitraums laufen Metrik-zu-CI-Datensätze ab. Außerdem führt eine Änderung der Ereignisregeln zum sofortigen Ablaufen der entsprechenden Metrik-zu-CI-Datensätze. Wenn Metrikrohdaten das nächste Mal eingehen, werden sie erneut normalisiert. Wenn Discovery CIs hinzufügt oder entfernt, werden die Zuordnungen so angepasst, dass diese Änderungen im nächsten Zyklus berücksichtigt werden.

Alle Informationen zur kürzlich vorhandenen Zuordnung werden in der Tabelle sa_metric_map in „Metrik zu CI“-Datensätzen gespeichert (siehe unten). Sie können auf die Tabelle „Metrik zu CI“ zugreifen, indem Sie zu **Alle > Event Management > Metriken > Metrik zu CI** navigieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Tabelle „Metrik zu CI“



Source	Metric Type Id	Metric Identifier	Configuration item	Resource Id	Active
ITOA_Metrics	cache.keys.size	resource_path:anomalySettings; mid_sys_i...	OI Metric Extension	anomalySettings	true
ITOA_Metrics	count	resource_path:AnomalyScoreSettingsInMemo...	OI Metric Extension	AnomalyScoreSettingsInMemoryCache.anomal...	true
ITOA_Metrics	timetaken_min	resource_path:Rest.post.metrics; mid_sys...	OI Metric Extension	Rest.post.metrics	true
ITOA_Metrics	cache.hit.percentage	resource_path:enabledMetrics; mid_sys_id...	OI Metric Extension	enabledMetrics	true
ITOA_Metrics	mean_rate	resource_path:Queue.normalizedMetrics_3....	OI Metric Extension	Queue.normalizedMetrics_3.NormalizedMetr...	true
ITOA_Metrics	timetaken_p95	resource_path:Normalizer.bind; mid_sys_i...	OI Metric Extension	Normalizer.bind	true
ITOA_Metrics	15_minute_rate	resource_path:AnomalyScoreCalculatorInMe...	OI Metric Extension	AnomalyScoreCalculatorInMemoryCache.anom...	true
ITOA_Metrics	avg.cache.get.time(µs)	resource_path:changeDetectorSettings; mi...	OI Metric Extension	changeDetectorSettings	true
ITOA_Metrics	count	resource_path:AnomalyScoreCalculatorInMe...	OI Metric Extension	AnomalyScoreCalculatorInMemoryCache.anom...	true
ITOA_Metrics	5_minute_rate	resource_path:TimeSeriesReadSyncer; mid_...	OI Metric Extension	TimeSeriesReadSyncer	true
ITOA_Metrics	size	resource_path:Queue.normalizedMetrics_6....	OI Metric Extension	Queue.normalizedMetrics_6.NormalizedMetr...	true
ITOA_Metrics	mean_rate	resource_path:BatcherTaskScheduler.expir...	OI Metric Extension	BatcherTaskScheduler.expirationRate	true
ITOA_Metrics	timetaken_stddev	resource_path:Rest.post.metrics; mid_sys...	OI Metric Extension	Rest.post.metrics	true
ITOA_Metrics	cache.hit.percentage	resource_path:changeDetectorSettings; mi...	OI Metric Extension	changeDetectorSettings	true
ITOA_Metrics	size	resource_path:Queue.normalizedMetrics_0....	OI Metric Extension	Queue.normalizedMetrics_0.NormalizedMetr...	true
ITOA_Metrics	5_minute_rate	resource_path:BatcherTaskScheduler.anoma...	OI Metric Extension	BatcherTaskScheduler.anomalyRate	true
ITOA_Metrics	cache.hit.percentage	resource_path:ciType; mid_sys_id:8a41f7e...	OI Metric Extension	ciType	true

Metrikbindung an Ressourcen

Binden Sie Metriken an Ressourcen, um die Bindung von Metrikereignissen zu vereinfachen, indem Sie zusätzlich zu CIs die Bindung an Ressourcen wie bestimmte Datenträger oder Webseiten aktivieren.

Metric Intelligence modelliert Metrikreihen mit einer der folgenden Methoden:

- Bindung einer Metrikreihe an ein CI und an die für dieses CI überwachte Metrik im Format „CI/Metrik“. Beispiel: „win_server_001/response_time_mean“.
- Bindung einer Metrikreihe an ein CI, eine Ressource innerhalb dieses CI und die für diese Ressource überwachte Metrik im Format „CI/Resource/Metrik“. Beispiel: „win_server_001/Disk — C/disk_usage“. Diese Methode wird als *`resource binding`* bezeichnet.

Die erste Methode ermöglicht das Modellieren, Speichern, Aggregieren und Abfragen von Daten auf CI-Level. Die Ressourcenbindung erstellt jedoch Ressourcendatensätze für bestimmte überwachte Entitäten wie einzelne Webseiten oder Datenträger. Daher ist die Ressourcenbindung effizienter, wenn mehrere Ressourcen ähnlichen Typs in einem CI vorhanden sind und Metriken, die für eine Kategorie dieser Ressourcen gelten, diesen Ressourcen zugeordnet werden.

Anwendungsfälle:

- Häufige Beispiele sind Laufwerke, Prozessoren und Netzwerkschnittstellen. In Fällen, in denen diese Entitäten überwacht werden, aber in der CMDB nicht vorhanden sind, ist die Verwendung von Ressourcen für die Metrikbindung hilfreich.
- Einige Überwachungslösungen erfassen Metrikdaten in Services wie KPIs für einzelne Webseiten in einer Anwendung. In solchen Fällen, in denen die überwachte Entität kein Konfigurationselement ist, kann die Metrikbindung an Ressourcen hilfreich sein.

In diesen Situationen führt die Verwendung der Ressourcenbindung zu aussagekräftigeren Zusammenfassungen für ähnliche Metriken (z. B. „avg disk_usage“ für einen Host auf allen Datenträgern).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcenbindungsprozess

Der MID Server generiert Metrikbindungsereignisse, die von der Instanz verarbeitet werden. Bei der Verarbeitung eines Metrikbindungsereignisses wird versucht, das CI zu identifizieren, zu dem dieses Metrikbindungsereignis gehört. Wenn dieser Versuch erfolgreich ist, wird das Metrikbindungsereignis an das identifizierte CI gebunden und eine Bindung an eine Ressource wird versucht. Die folgenden Schritte beschreiben den Versuch, ein Metrikbindungsereignis an eine Ressource zu binden:

1. Identifizieren Sie die CI-Klasse des CI, das an das Metrikbindungsereignis gebunden wurde.
2. Ermitteln Sie die Ressourcenklasse, die dieser CI-Klasse zugeordnet ist (mithilfe der Tabelle „CI-Typ zu Ressourcenklasse“ [sa_ci_type_to_resource_class]).
3. Lesen Sie den Attributwert *resource_path* im Feld **additional_information** im Metrikbindungsereignis.
4. Überprüfen Sie, ob in der Ressourcenklassentabelle ein Ressourcendatensatz vorhanden ist, in dem *name* gleich *resource_path* und *cmdb_ci* gleich dem CI ist, das an das Metrikbindungsereignis gebunden wurde.
5. Wenn ein solcher Ressourcendatensatz vorhanden ist, wird das Metrikbindungsereignis an diese Ressource gebunden. Andernfalls wird ein neuer Ressourcendatensatz mit den vorherigen Werten erstellt und das Metrikbindungsereignis wird an die neu erstellte Ressource gebunden.

Ressourcenbindungen konfigurieren

- Stellen Sie sicher, dass die Systemeigenschaft „sa.metric.use.resource.binding“ auf „true“ (Standard) festgelegt ist.
- Stellen Sie für Reihen, die an Ressourcen gebunden werden sollen, sicher, dass das Attribut *resource_path* ausgefüllt wird, indem Sie einen der folgenden Schritte ausführen:
  - Verwenden Sie eine Ereignisregel, um das Attribut *resource_path* dem Feld **Zusätzliche Informationen** in Ereignissen hinzuzufügen. Weitere Informationen finden Sie unter Erstellen einer Ereignisregel zum Zuordnen von Metriken zu bestimmten CIs.
  - Füllen Sie das Attribut *resource_path* als Teil des jeweiligen CI-Bezeichners aus, wenn Daten zur Verarbeitung an den MID Server gesendet werden.
- Überprüfen Sie die Standardzuordnungen in der Tabelle „CI-Typ zu Ressourcenklasse“ [sa_ci_type_to_resource_class], und passen Sie sie nach Bedarf an. Es ist wichtig, dass Zuordnungen vor der Datenverarbeitung wie gewünscht festgelegt werden.

  Zum Verwalten der Tabelle „CI-Typ zu Ressourcenklasse“ ist die Rolle „evt_mgmt_admin“ erforderlich.

Ressourcentabellen

Die Ressourcenbindung verwendet eine zugrunde liegende Hierarchiestruktur von Ressourcen, die eine Teilmenge der [cmdb_ci]-Hierarchie ist. Metric Intelligence installiert die folgenden Ressourcentabellen:

- CI-Ressource [ci_resource] (übergeordnete Tabelle):
- Tabellen, die die CI-Ressource [ci_resource] erweitern:
  - ci_resource_hardware
  - ci_resource_appl
  - ci_resource_service

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- ci_resource_vm_object
- ci_resource_database

CIs zu Ressourcen zuordnen

Zuordnungen von CI-Klassen zu Ressourcenklassen werden in der Tabelle „CI-Typ zu Ressourcenklasse“ [sa_ci_type_to_resource_class] gespeichert. Diese Tabelle wird mit Metric Intelligence installiert und während der Metrikbindung an Ressourcen verwendet.

Zuordnungen in der Tabelle „CI-Typ zu Ressourcenklasse“ (Standard)

CI-Klasse	Ressourcenklasse
cmdb_ci_hardware	ci_resource_hardware
cmdb_ci_appl	ci_resource_appl
cmdb_ci_service	ci_resource_service
cmdb_ci_database	ci_resource_database
cmdb_ci_vm_object	ci_resource_vm_object

Erstellen einer Ereignisregel zum Zuordnen von Metriken zu bestimmten CIs

Erstellen Sie Ereignisregeln, um eingehende Metrikrohdaten bestimmten CIs zuzuordnen, Metriknamen optional zu ändern und das Attribut *resource_path* für die Ressourcenbindung auszufüllen.

Das System generiert Ereignisse für alle neuen Metrikdaten, für die keine CI-Bindungsspezifikationen vorhanden sind. Sie können Ereignisregeln erstellen, die diese Ereignisse filtern, um die eingehenden Metrikdaten bestimmten CIs zuzuordnen. In solchen Ereignisregeln haben Sie z. B. die Möglichkeit zum Definieren eines Filters, der auf dem Überwachungsobjekt (z. B. SCOM) basiert.

Zur Verwendung der Ressourcenbindung muss das Attribut *resource_path* von Ereignissen ausgefüllt werden. Sie können eine Ereignisregel konfigurieren, um sicherzustellen, dass das Attribut *resource_path* dem Feld **Zusätzliche Informationen** in Ereignissen hinzugefügt wird. Weitere Informationen zum Konfigurieren und Verwenden der Ressourcenbindung finden Sie unter Ressourcenbindung.

Beispielsweise können Sie im Designer für Ereignisregeln die Ereignisregel **SCOM-IIS-Webserver** wie folgt aktualisieren:

- Definieren Sie auf der Registerkarte **Ereignisfilter** einen Filter, sodass nur IIS-Webserver zugeordnet werden.
- Legen Sie auf der Registerkarte **Bindung** für **Klasse** den Wert `Microsoft IIS-Webserver` fest.

Zugehörige Informationen

Event-Regeln

Zuordnung zwischen Metriken und CI sowie Ressourcenbindung anzeigen

Erste Schritte mit Metrikdaten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CIs im Wartungsmodus

Konfigurieren Sie die Anomalie-Erkennung, um Metriken für CIs, die sich im Wartungsmodus befinden, vom Modelllernen auszuschließen.

Sie können die Einstellungen der Systemeigenschaften ändern, um Metrikdaten für CIs im Wartungsmodus ein- oder auszuschließen.

Wenn die Systemeigenschaft sa.model_learner.maint_event_record_history_enabled auf „true“ festgelegt ist (Standard), speichert Metric Intelligence Verlaufsinformationen über die Zeiten, zu denen CIs in den Wartungsmodus wechseln bzw. diesen verlassen. Wenn die Systemeigenschaft sa_metric.maint_exclusion auf „true“ festgelegt ist (Standard), werden Metriken von CIs, die sich im Wartungsmodus befinden, vom Modelllernen ausgeschlossen.

Anomaliemodelltests

Verwenden Sie Anomaliemodelltests zum Anwenden und Auswerten der Anomalie-Erkennung für einen kleinen Satz von CIs und Metriken unter Verwendung tatsächlicher Metrikdaten. Vergleichen Sie die Testergebnisse mit den erwarteten Ergebnissen, und optimieren Sie dann das Anomalie-Erkennungsmodell, bevor Sie die Anomalie-Erkennung für die getesteten CIs und Metriken in der Produktionsumgebung aktivieren.

Beispiel: Bevor Sie die Anomalie-Erkennung für Linux-Server aktivieren, können Sie Anomaliemodelltests mit tatsächlichen Metrikdaten verwenden, die für diese Linux-Server gesammelt wurden. Vorhandene Warnungen weisen möglicherweise auf eine Anomalie für eine bestimmte Metrik und ein bestimmtes CI hin. Sie können eine Anomalietestregel erstellen, um die Anomalie-Erkennung für diese CIs und Metriken zu testen und dann zu überprüfen, ob die erwartete Anomalie erkannt wird. Sie können auch die durch das Anomaliemodell berechneten Grenzen überprüfen, um festzustellen, ob sie den erwarteten Grenzen entsprechen. Nach der Feinabstimmung des Testmodells können Sie die Anomalie-Erkennung für Linux-Server aktivieren.

Anomaliemodelltests unterstützen bis zu 20 Zeitreihen, die 20 Metriktypen für dasselbe CI, denselben Metriktyp für 20 verschiedene CIs oder eine beliebige Kombination dieser Optionen enthalten können.

Testergebnisse im Explorer für Einblicke anzeigen

Nach Abschluss einer Testausführung wird eine URL für einen Explorer für Einblicke verfügbar. Die Testergebnisse des Anomaliemodells werden in dieser eingeschränkten Version des Explorers für Einblicke angezeigt. In diesem Explorer für Einblicke werden die Diagramme und Punktzahlen der in der Anomalietestregel angegebenen Metrikserien im Voraus geladen. Sie können diesem Explorer für Einblicke keine CMDB-Gruppen und Anwendungsservices hinzufügen.

Alle Diagramme im Explorer für Einblicke enthalten in den **Diagrammeinstellungen** den Abschnitt „Anomalieteststatistiken“. Dieser Abschnitt bezieht sich speziell auf Anomaliemodelltests und bietet die folgenden Optionen:

- **Grenzen anzeigen**: Zeigt die berechnete obere und untere Grenze für die Metrik in einem Anomaliemodelltest an, die auf dem Lernen vergangener Metrikwerte basiert. Die obere und die untere Grenze werden immer zusammen angezeigt.
- **Abweichende Punktzahlen anzeigen**: Zeigt abweichende Punktzahlen auf einer virtuellen Achse von 0–10 für einen Anomaliemodelltest an. Dabei basiert der Farbcode auf den Punktzahlschwellenwerten, die in der Tabelle der Zuordnung der Anomaliepunktzahl zum Event-Schweregrad [sa_metric_anomaly_score_to_event_severity_map] definiert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Testergebnisse zum Optimieren der Anomalie-Erkennung verwenden

Beim Anomaliemodelltest werden die obere und die untere Grenze verwendet, die für die ausgewählte Serie in der Anomalietestregel konfiguriert sind. Die Ergebnisse des Anomaliemodelltests zeigen, wie viele Anomaliewarnungen basierend auf den angegebenen Einstellungen generiert worden wären, wenn die Anomalie-Erkennung für die getesteten CIs und Metriken aktiviert wäre. Anschließend können Sie entscheiden, ob dieses Ergebnis akzeptabel ist. Optimieren Sie die Grenzen so, dass die Anzahl der generierten Anomaliewarnungen nicht übermäßig, aber ausreichend ist, um eine Punktzahl außerhalb der Grenzen genau anzugeben.

Advanced Promotion Engine

Sie können eine Definition für Advanced Promotion Engine erstellen, um die Bedingungen für das Heraufstufen der Anomaliewarnungen in die Tabelle „Alle Warnungen“ zu definieren. Durch das Heraufstufen der Warnungen, die die Bedingungen erfüllen, werden nur die relevantesten Anomaliewarnungen in die Tabelle verschoben.

Advanced Promotion Engine verschiebt die relevantesten Warnungen aus der Liste der Anomaliewarnungen in die Tabelle „Alle Warnungen“. Wenn eine Gruppe von Anomaliewarnungen in einem Configuration Item (CI) die Bedingungen erfüllt, die Sie in der Definition festgelegt haben, die Sie für Advanced Promotion Engineerstellt haben, gruppiert der Gruppierungsmechanismus die heraufgestuften Warnungen in der Tabelle „Alle Warnungen“. Sie können beispielsweise eine Bedingung erstellen, die angibt, dass nur die Anomaliewarnungen, die zu einer bestimmten CI-Klasse mit dem Mindestschweregrad „Schwerwiegend“ gehören, in die Tabelle „Alle Warnungen“ hochgestuft werden sollen.

Die Tabelle „Alle Warnungen“ enthält die Probleme, die Ihre sofortige Aufmerksamkeit erfordern. Die Anomaliewarnungen für die verschiedenen Metriken innerhalb eines CI in einem bestimmten Zeitraum weisen auf ein Problem hin, das in der Tabelle „Alle Warnungen“ hochgestuft werden muss.

Anomaliewarnungen weisen auf eine Abweichung von den prognostizierten Metrikwerten für überwachte CIs hin. Details finden Sie unter Zeigen Sie Anomaliewarnungen an.

Advanced Promotion Engine wird automatisch als Teil der Anwendung Metrikdaten aktiviert.

Sie können die Advanced Promotion Engine -Definitionen verwenden, die mit dem Basissystem geliefert werden (für den Linux -Server und den Windows -Server), oder Sie können Definitionen für die anderen CI-Klassen erstellen. Die Basissystemdefinitionen geben an, dass die CIs auf den Servern Linux und Windows betriebsbereit sind und dass CIs mit dem Mindestschweregrad „Schwerwiegend“ in die Tabelle „Alle Warnungen“ hochgestuft werden sollen.

Alle Advanced Promotion Engine -Aufgaben erfordern die Rolle evt_mgmt_admin. Mit der Rolle evt_mgmt_user können Sie nur Definitionen und Eigenschaften anzeigen.

Metric Explorer

Metric Explorer bietet eine einfach zu bedienende Benutzeroberfläche, auf der Servicemitarbeiter die Integrität eines CI anzeigen können, das einer Warnung zugeordnet ist. Integritätsdetails für ein CI umfassen verschiedene Metrikdiagramme mit Steuerungsgrenzen und Zusammenfassungen für einen Zeitraum.

Welche Metrikdiagramme für eine CI-Klasse in Metric Explorer angezeigt werden, hängt von den Metrikdiagrammkonfigurationen in der Metrik-Dashboard-Metadatentabelle [sa_metric_dashboard_metadata] ab. Die Tabelle „Metadaten des Messgrößen-Dashboards“ wird anfänglich mit Konfigurationen für allgemeine Klassen und wichtigen Metriken für diese Klassen ausgefüllt. Ein Benutzer mit der Rolle admin oder evt_mgmt_admin

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

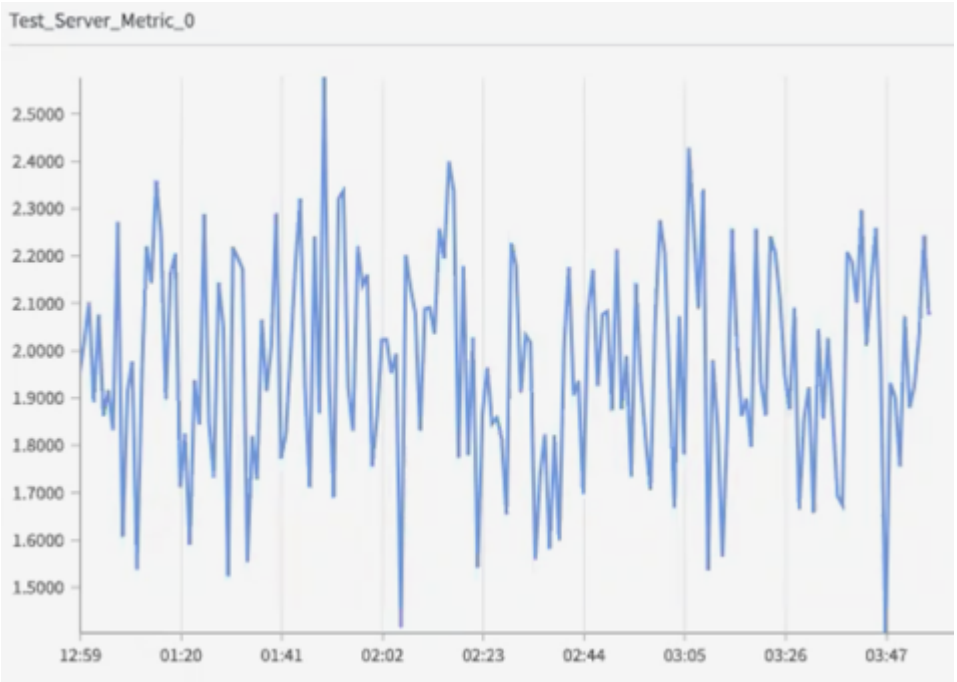
kann die Standardkonfigurationen des Metrikdiagramms in der Tabelle „Metadaten des Messgrößen-Dashboards“ aktualisieren.

Es können jeweils bis zu 10 aktive Metrikdiagramme für eine Klasse konfiguriert werden.

Diagrammtypen

Ein Metrikdiagramm, das im Formular „Metrikdiagramme“ in Metric Explorer angezeigt wird, kann ein Diagramm vom Typ **Zeitreihe** oder **Einzelne Punktzahl** sein.

Zeitreihendiagramm



Der Zeitreihendiagrammtyp ist ein Diagramm aller Datenpunkte im angegebenen Zeitbereich für die Metriken des dem Diagramm zugeordneten CI. Zeitreihendiagramme ähneln Diagrammen im Explorer für Einblicke und enthalten je nach den Einstellungen eine obere oder untere Grenze.

Diagramm für einzelne Punktzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Diagrammtyp für einzelne Punktzahl zeigt eine einzelne Zahl an, die einer Zusammenfassung der Datenpunkte in der Zeitreihe für die Metrik und das CI des Diagramms entspricht. Die Zusammenfassung ist ein Durchschnitt der Datenpunkte oder des Höchst-, Mindest- oder letzten Datenpunkts in der Zeitreihe.

Vorlagen

Die Vorlage ITOM Service Operations-Arbeitsbereich Metric Explorer ermöglicht einen Drilldown in Metrikdiagramme von Dashboards für digitale Analytics (DA) in Metric Explorer. Einzelheiten hierzu finden Sie unter Express-Listenübersicht im Developer-Portal ServiceNow®.

Eigensystemüberwachung für Metric Intelligence

Verwenden Sie Eigensystemüberwachungen von Ereignismanagement, um den allgemeinen Betriebszustand von Komponenten und Prozessen der Metric Intelligence-Infrastruktur zu überwachen und auf potenzielle Probleme aufmerksam zu machen. Die Selbstintegritätsüberwachung ermöglicht Ihnen, Probleme proaktiv zu beheben und Datenverluste zu minimieren.

Metric Intelligence ist für die Verwendung der Eigensystemüberwachung von Ereignismanagement vorkonfiguriert, um sicherzustellen, dass wichtige Komponenten und Prozesse ordnungsgemäß funktionieren. Wenn ein Monitor einen Fehler erkennt, erstellt die Selbstintegritätsüberwachung von Ereignismanagement ein Ereignis für das Problem. Diese Ereignisse werden dann in einen Ereignismanagement-Alarm umgewandelt oder an einen vorherigen Alarm angehängt. Die Eigensystemüberwachung von Metric Intelligence wird alle 60 Sekunden ausgeführt.

Wenn beispielsweise in einem verteilten Cluster mit einem Metric Intelligence-MID Server ein Problem auftritt, wird ein Event mit dem Status **Schwerwiegend** generiert. Anschließend wird dieses Ereignis in einen Alarm umgewandelt. Später, wenn das Problem gelöst wurde, wird ein neues Ereignis mit dem Status **Info** generiert, und die ursprüngliche Warnung wird geschlossen.

Überwachte Komponenten und Prozesse

Komponenten-/Prozessprüfung	Fehlerbedingung
Metric Intelligence-Erweiterung wird ordnungsgemäß ausgeführt	Der Monitor überprüft das *status*-Feld der *ecc_agent_ext_context_metric*-Tabelle, um einen **Fehler**- oder **Warnung**-Status zu erkennen.
Verteilter Cluster von Metric Intelligence-MID Servern wird ordnungsgemäß ausgeführt	Die Überwachung prüft das Feld *status* der Tabelle *ecc_agent_cluster* auf den Status **Fehler**, **Segmentiert**oder**Gestoppt**. **Hinweis:** Für den Status **Gestoppt** wird nur dann ein Ereignis erstellt, wenn das Feld *error_message* nicht leer ist.
Metriken werden von aktiven Connectors erfasst, die für die Metriksammlung konfiguriert sind	Für jeden Connector, für den die Kennzeichnung *Metrics collection* auf **true** festgelegt ist:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten-/Prozessprüfung	Fehlerbedingung
	Der Monitor überprüft den Status des *last_kpi_status*-Felds der *em_connector_instance*-Tabelle, um einen **Fehler**-Status zu erkennen.
Wichtige regelmäßige Metric Intelligence-Aufgaben sind aktiv	Der Monitor überprüft die folgenden wesentlichen geplanten Aufträge, um festzustellen, ob einer davon inaktiv ist: • Metric Intelligence – Konfigurationsaufgabe für Metriken • Metric Intelligence – Tabellen mit MID synchronisieren • Metric Intelligence – Verteiltes MID-Cluster validieren

Weitere Informationen zum Aktivieren oder Deaktivieren einer Metric Intelligence-Eigensystemüberwachung finden Sie unter Eigensystemüberwachung konfigurieren.

Zugehörige Informationen

Eigensystemüberwachung für Ereignismanagement

Mit Metric Intelligence installierte regelmäßige Aufgaben

Domänentrennung und Metric Intelligence

Die Domänentrennung wird in Metrikdaten unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

So funktioniert Domänentrennung in Metrikdaten

Wenn Domänen in Metrikdaten getrennt sind, können Benutzer Warnungen und Ereignisse nur in ihrer eigenen (Mandanten-)Domäne anzeigen und verwalten. Nach Abschluss des Bindungsprozesses wird die Domäne des Configuration Item (CI) verwendet, damit Benutzer in dieser Domäne Metrikdaten untersuchen können. Es gibt eine Domänenspalte in Metrikdaten-Tabellen, die im Basissystem bereitgestellt werden. Die Domänenspalte zeigt den Namen der Domäne an, zu der das CI gehört.

Hinweis: Wenn die Domänenspalte nicht in der Liste angezeigt wird, klicken Sie auf (Liste personalisieren), und fügen Sie die erforderliche Spalte hinzu. Darüber hinaus können Sie eine Spalte hinzufügen, die den Domänenpfad anzeigt.

Die folgenden Funktionen von Metrikdaten unterstützen die Domain Separation nur eingeschränkt.

Funktion	Support
Metriktypen	Auf globaler Ebene unterstützt. Der Instanzbesitzer kann die Metriktypen für alle Domänen steuern.
Registrierung des Metriktyps	Auf globaler Ebene unterstützt. Der Instanzbesitzer kann die Metriktypregistrierung für alle Domänen steuern.
Metrikklasse	Auf globaler Ebene unterstützt. Der Instanzbesitzer kann die Metrikklassen, die für alle Domänen genutzt werden, steuern.
Regeln für Konfigurationseinstellungen	Auf globaler Ebene unterstützt. Der Instanzbesitzer kann die Regeln für die Konfigurationseinstellungen für alle Domänen steuern

Zugehörige Informationen

Domänentrennung für Service Provider

Metrikdaten konfigurieren

Planen und konfigurieren Sie Ihre Metrikdaten-Implementierung.

Konfiguration – Übersicht

Metrikdaten Die -Konfiguration folgt normalerweise den folgenden Schritten:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Installieren Sie das Plugin AIOps-Experience [sn_sow_aiops].
2. MID-Server für Metrikdaten manuell konfigurieren.
3. Metrikdaten aktivieren.
4. Streamen Sie Metriken über die entsprechende Datenquelle oder den entsprechenden Connector an die -Instanz.
5. Zu überwachende Metriken auswählen und konfigurieren.
6. Stellen Sie sicher, dass Metriken ordnungsgemäß an CIs gebunden sind.
7. Konfigurieren Sie die Aktionsebene für die Anomalie-Erkennung.
8. Definieren Sie eine erweiterte Heraufstufungsregel, um die Bedingungen für das Heraufstufen einer Anomaliewarnung zu einer IT-Warnung zu bestimmen.

Erste Schritte mit Metrikdaten

Führen Sie die folgenden Setup- und Erstkonfigurationsschritte aus, um Metrikdatenzu verwenden.

Vorbereitungen

Aktivieren Sie das Plugin Metrikdaten (com.snc.sa.metric).

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Metriken haben ein Ablaufdatum. Sie können weiterhin Daten ohne Unterbrechung empfangen, wenn das Ablaufdatum einer Metrik ansteht, indem Sie das Ablaufdatum entsprechend verschieben. Wenden Sie sich an den Kundensupport, um Einzelheiten zu erfahren.

Metrikdaten Das geführte Setup von stellt eine Reihe von Aufgaben bereit, mit denen Sie Metrikdaten in Ihrer ServiceNow-Instanz konfigurieren können. Um das geführte Setup für Metrikdaten zu öffnen, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**und klicken Sie auf **Fortfahren**. Scrollen Sie dann zu **Metric Intelligence**, und klicken Sie auf **Fortsetzen**. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Alternativ können Sie folgende Vorgehensweise verwenden.

Prozedur

1. Konfigurieren Sie ein MID-Server für Metrikdaten.
   Einzelheiten finden Sie unter MID-Server und verteilter MID-Server-Cluster für Metrikdaten.
2. Verwenden Sie das Automatisiertes Setup von Metrikdaten.
3. Wählen Sie eine Quelle zum Sammeln von Metriken.
4. Zu überwachende Metriken auswählen und konfigurieren.
5. Erstellen Sie Ereignisregeln, um Metrikrohdaten bestimmten CIs und Ereignisregel zum Binden von Metrikereignissen an Host-CIs erstellenzuzuordnen.
6. Ungefähr 10 Minuten nach dem Start der Erweiterung „Metric Intelligence Metrics“ führen Sie die Schnellstarttests für Metric Intelligence durch, um die Funktionalität zu überprüfen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikdaten aktivieren

Metrikdaten ermöglicht Ihnen das Erfassen, Untersuchen und Analysieren von operativen Metrikdaten sowie das Erkennen und Anzeigen von Anomalien. Diese Analyse kann potenzielle Serviceausfälle verhindern.

Zeigen Sie Daten im Einblick-Explorer, im Mitarbeiterbereich und in den Anwenderoberflächen Service Operations-Arbeitsbereich von Metrikdaten an , und arbeiten Sie mit ihnen.

Einzelheiten zu den mit Metrikdatenaktivierten Plugins finden Sie unter Mit installierte Plugins oder Anwendungen ITOM-Integrität.

Automatisiertes Setup von Metrikdaten

Beim ersten Setup von Metrikdaten können Sie viele Setupschritte automatisieren. Beispielsweise konfiguriert das automatisierte Setup einen MID-Server für Metrikdaten und erstellt einen verteilten MID-Server-Cluster, der diesen MID-Server enthält.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn die folgenden Bedingungen erfüllt sind, wird im MID-Server-Formular der zugehörige Link **Metric Intelligence einrichten** angezeigt, um das automatisierte Setup zu ermöglichen:

- Der MID-Server wurde validiert.
- Der MID-Server wird ausgeführt.
- Die Eigenschaft *sa.metric.display.mid.setup.action* ist auf „true“ festgelegt (Standardwert).

Das automatisierte Setup für Metrikdaten führt die folgenden Setupaufgaben aus:

1. Es konfiguriert den MID-Server mit der Anwendung *Operation Intelligence*.
2. Es fügt dem MID Server die *Metrics*-Fähigkeit hinzu.
3. Es erstellt einen neuen MID-Server-Cluster vom Typ „Verteilt“ mit dem Standardport 47100 für Apache Ignite.
4. Es fügt den MID-Server dem neuen verteilten MID-Server-Cluster hinzu.
5. Es erstellt eine Erweiterung „Metrikdaten Metrics“ und startet sie.
6. Es öffnet das Formular „Metrikdaten Metrics Context“ (Metric Intelligence Metrics-Kontext). In diesem Formular können Sie auf die UI-Aktion **REST-Listener einrichten** klicken, um die MID Web Server-Erweiterung zu erstellen, die mit der Option „REST-Listener aktivieren“ und dem Standardport 8097 konfiguriert ist.

Wenn das automatische Setup fehlschlägt, können Sie manuell einen verteilten Cluster MID-Server erstellen. Wie unter Link **Metrikdaten einrichten** beschrieben, nur um den ersten verteilten Cluster MID-Server zu erstellen, der einen einzelnen MID-Serverenthält, mit Standardwerten. Nach Abschluss des automatisierten Setups müssen Sie manuell zusätzliche verteilte MID-Server -Cluster erstellen oder Metrikdaten MID Servershinzufügen.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Server**.
2. Wählen Sie den MID-Server aus, den Sie als Metrikdaten MID-Serverkonfigurieren möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie im Formular „MID-Server“ im Abschnitt „Zugehörige Links“ **die Option Metrikdaten einrichten**.
4. Im neu erstellten Formular Metrikdaten Metrikerweiterung:
   a. Warten Sie, bis der Statuswert **Gestartet**lautet.
   b. Wenn Sie MID-Server für die Push-Übertragung konfigurieren, wählen Sie die UI-Aktion **REST-Listener einrichten**aus.
   Es wird eine Benachrichtigung angezeigt, dass die MID-Server-Erweiterung erstellt wird. Das Feld **MID-Webservererweiterung** wird mit der ausgewählten Option **REST-Listener aktivieren** angezeigt. Sie können eine Vorschau des MID-Server Extension-Datensatzes anzeigen, um zu überprüfen, ob der Status-Wert **Gestartet lautet**.

Zugehörige Informationen

MID Server und verteilter MID Server-Cluster für Metric Intelligence

MID-Server für Metrikdaten manuell konfigurieren

Konfigurieren Sie zur Verwendung von Metrikdaten mindestens einen MID Server mit Metrikdaten als unterstützter Anwendung mit Metrikfunktionalität, der zudem die Erweiterung „Metrikdaten Metrics“ ausführt. Fügen Sie dann Metrikdaten MID-Server als Mitglied zu einem verteilten MID-Server-Cluster hinzu.

Vorbereitungen

Stellen Sie sicher, dass der MID-Server alle Software-, Hardware- und Konfigurationsanforderungen erfüllt, die für Metric Intelligence konfiguriert werden sollen.

Erforderliche Rolle: Für den Zugriff auf den MID-Server ist die Rolle mid_server erforderlich. Informationen zum Konfigurieren eines MID-Server in einer Instanz (z. B. zum Hinzufügen einer unterstützten Anwendung) finden Sie in der MID-Server-Dokumentation.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Server**.
2. Klicken Sie auf den MID Server, den Sie für Metrikdaten konfigurieren möchten.
3. Fügen Sie die Anwendung Metrikdaten hinzu:
   a. Klicken Sie in der Mitte des MID-Serverformulars auf **Unterstützte Anwendungen**.
   b. Klicken Sie im Abschnitt **Unterstützte Anwendungen** auf **Bearbeiten**.
   c. Wählen Sie im Slushbucket das Element **OperationalIntelligence** aus, und klicken Sie auf die Hinzufügen-Schaltfläche **>**.
   d. Klicken Sie auf **Speichern**.
4. Fügen Sie die Metrics-Fähigkeit hinzu:
   a. Klicken Sie in der Mitte des MID-Server-Formulars auf **Funktionen**.
   b. Klicken Sie im Abschnitt **Fähigkeiten** auf **Bearbeiten**.
   c. Wählen Sie im Slushbucket **Metrics** aus, und klicken Sie auf die Hinzufügen-Schaltfläche „>“.
   d. Klicken Sie auf **Speichern**.
5. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Erstellen Sie einen verteilten MID-Server-Cluster, und fügen Sie diesem Cluster den Metrikdaten MID-Server als Mitglied hinzu.

Konfigurieren Sie die Erweiterung Metrikdaten manuell

Konfigurieren Sie die Erweiterung MID-Server Metrikdaten, damit MID-Server Rohmetriken aus externen Systemen abrufen kann, um Anomalien zu erkennen und sie zusammen mit Rohdaten an die Instanz zu melden. Diese MID-Server Metrikdaten -Erweiterung ist erforderlich und muss ausgeführt werden, damit Ihr System Metrikdaten -Daten erfassen kann.

Vorbereitungen
Unter Erste Schritte mit Metrikdaten finden Sie allgemeine Schritte zum Setup von Metrikdaten.

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Erweiterung MID-Server Metrikdaten normalisiert die Rohdaten und überträgt sie dann an die -Instanz. Wenn die Erweiterung Anomalien über einem angegebenen Schwellenwert erkannt hat, werden diese an die Instanz gesendet. Die Erweiterung wird ausgeführt, solange sie aktiviert ist. Dies stellt eine dauerhafte Verbindung zu MID-Server bereit, um ständig auf Rohdaten Metrikdaten aus externen Systemen zu lauschen.

Die Erweiterung MID-Server Metrikdaten :

- Empfängt Metrikrohdaten, fasst sie zu Stapeln zusammen und sendet sie in festgelegten Intervallen an die Instanz.
- Erkennt Anomalien und sendet einen Bericht an die Instanz.
- Die Informationen, die an die ServiceNow-Instanz gesendet werden, sind für Metrikdatenrelevant, sodass die Datenverarbeitung effizient ist.

Die Erweiterung MID-Server Metrikdaten stellt keine API-Aufrufe bereit. Wenn jedoch die Option **REST-Listener aktivieren** ausgewählt ist, fügt die Erweiterung einen Handler für die unterstützten REST APIs hinzu.

Hinweis:

- Erst wenn die Erweiterung Metrikdaten konfiguriert wird, treten die Metrikdaten MID Servers dem verteilten Cluster für Metrikdatenbei.
- Nach der Erstkonfiguration wird die erste Metrik nicht in die Metrikdaten aufgenommen.
- Der Empfang von Metrikinformationen aufgrund der Synchronisierung der -Instanz mit MID-Serververzögert sich um eine Minute.

Prozedur

1. Navigieren zu **Alle** > **MID-Server** > **Profile und Bereitstellungen** > **Metrikdaten**.
2. Klicken Sie in der Liste Metrikdaten Metrikkontexte auf **Neu**.
3. Füllen Sie die Felder entsprechend aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Ein eindeutiger Name für diese Erweiterung zur einfachen Identifizierung
Kurzbeschreibung	Eine Beschreibung dieser Erweiterung
Status	Dieses Feld wird automatisch mit dem Status der Erweiterung ausgefüllt. Das Feld ist leer, bis die Erweiterung gestartet ist. Nach der Ausgabe eines Befehls an die Erweiterung wird einer der folgenden Werte angezeigt: ◦ **Gestartet**: Die Erweiterung wird ausgeführt. ◦ **Gestoppt**: Die Erweiterung wird nicht ausgeführt. ◦ **Offline**: Der MID-Server ist nicht erreichbar. ◦ **Fehler**: Die Erweiterung ist mit einem Fehler fehlgeschlagen (die Fehlermeldung wird im Feld **Fehlermeldung**angezeigt). ◦ **Warnung**: Eine Laufzeitausnahme ist aufgetreten. Die Erweiterung funktioniert weiterhin.
Fehlermeldung	Nachricht, die Fehler beschreibt, die dazu führen, dass Befehle wie **Starten** oder **Stoppen**fehlschlagen. Dieses Feld wird angezeigt, wenn das Feld **Status** den Wert **Fehler** hat oder wenn das Feld **Status** den Wert **Warnung** hat.
Ausführen auf	Ausführungsort dieser Erweiterung. Wenn Sie diese Option zur Verwendung mit Metrikdatenkonfigurieren, legen Sie sie auf **Spezifischer MID-Server**fest. Geben Sie dann MID-Server mit *Operationalintelligence* als unterstützte Anwendung und der Fähigkeit *Metrics* an.
MID-Server	Der Name des bezeichneten MID-Server, der mit *Operationalintelligence* als unterstützte Anwendung und der Fähigkeit *Metrics* konfiguriert ist.
Ausführung auf	[Schreibgeschützt] Der Name von MID-Server, auf dem die Erweiterung ausgeführt wird. Dieses Feld zeigt den Namen des MID-Server an, auch wenn der MID-Server nicht erreichbar ist. Wenn der Benutzer die Erweiterung stoppt, ist dieses Feld leer.

4. Wenn Sie die Push-Methode zum Sammeln von Metrikdaten -Daten verwenden, muss die Erweiterung MID-Server Metrikdaten mit **aktivierter Option „REST-Listener**

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

aktivieren“ konfiguriert werden. Diese Option aktiviert einen Listener, damit ein REST-Endpunkt Metrikrohdaten empfangen kann. Die Metrikrohdaten werden dann im regulären Datenfluss platziert, wo die Daten an die Instanz gesendet werden und der Anomaliedetektor nach Anomalien sucht. Wenn diese Option ausgewählt ist, wird dem Webserver ein -Handler hinzugefügt, um auf alle Metriken zu lauschen, die an die MID-Serverübertragen werden. Wenn diese Option ausgewählt ist, muss auch die Webservererweiterung konfiguriert werden, die einen Webserver auf dem MID-Serverstartet. Weitere Informationen finden Sie unter MID-Webservererweiterung konfigurieren.

5. Rechtsklicken Sie auf die Formularüberschrift, und wählen Sie **Speichern** aus.
6. Klicken Sie unter **Zugehörige Links** auf **Start**, um die Daten Metrikdaten in dieser Erweiterung zu speichern und die Erweiterung zu starten.

In der Erweiterung „MID Server Metric Intelligence“ verfügbare Befehle

Zugehöriger Link	Beschreibung
Starten	Startet die Erweiterung auf dem konfigurierten MID-Server, wenn sie derzeit nicht ausgeführt wird.
Stoppen	Stoppt die ausgeführte Erweiterung auf dem konfigurierten MID-Server. Wenn die Erweiterung nicht läuft, wird keine Aktion ausgeführt.
Neu starten	Stoppt die Erweiterung am konfigurierten MID-Serverund startet sie dann wieder.
Test	Der Test ist für Metrikdatennicht relevant. Parameter werden bei Ausführung des **Tests** nicht getestet oder validiert.
Parameter aktualisieren	Sendet die zuletzt gespeicherten Parameter an die Erweiterung

Advanced Promotion Engine aktivieren

Bevor Sie die Funktion Advanced Promotion Engine verwenden können, müssen Sie sie in der Liste der Plugins aktivieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Systemdefinition** > **Plugins**.
2. Suchen Sie **die Advanced Promotion Engine** (ID: sn_metric_promote).
3. Wählen Sie den Eintrag aus, und überprüfen Sie die App-Details im Formular **„Store Application Advanced Promotion Engine“**.
4. Wählen Sie im Abschnitt „Zugehörige Links“ **die Option Aktivieren/Upgrade aus**.
5. Wählen Sie **Aktivieren**.

Domänentrennung für Metric Intelligence konfigurieren

Konfigurieren Sie Metrikdaten für Domain Separation, um logisch definierte Domänen zu erstellen, die den nicht autorisierten Zugriff auf Daten beschränken.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin und evt_mgmt_integration

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Aktivieren Sie das Plugin „Domain Support – Domain Extension Installer“.
2. Konfigurieren Sie den MID Server für Operational Intelligence als Benutzer, der zur gewünschten Domäne gehört, und dem die Rolle mid_server zugewiesen ist.
3. Konfigurieren Sie einen verteilten MID Server-Cluster in der gewünschten Domäne, und fügen Sie Operational Intelligence MID Server hinzu, die zur gleichen Domäne gehören. Weitere Informationen zum Einrichten von MID-Servern für Metrikdaten finden Sie unter MID Server und verteilter MID Server-Cluster für Metric Intelligence.

Hinweis: Die Bindungsereignisse von Event Management werden mithilfe der Domäne des angemeldeten MID Server-Benutzers konfiguriert. Sobald der Prozess abgeschlossen ist, wird die Domäne des Datensatzes aktualisiert, um die Domäne aus dem CI zu verwenden, sodass jeder Benutzer in dieser Domäne die Metrikdaten sehen kann.

Wird optimiert Metrikdaten

Sie können verschiedene Aufgaben ausführen, um Metrikdatenoptimal zu nutzen.

Anomalietestregel erstellen

Zur Verwendung von Anomaliemodelltests erstellen Sie eine Anomalietestregel, in der Sie bis zu 20 Metrikserien angeben, für die die Anomalie-Erkennung getestet werden soll. Führen Sie den Anomalietest aus, und verwenden Sie nach Abschluss die bereitgestellte URL, um den Explorer für Einblicke mit den Modelltestergebnissen zu laden.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_user

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Anomaliemodelltests**.
2. Wählen Sie eine vorhandene Anomalietestregel aus, die Sie bearbeiten und erneut ausführen möchten, oder klicken Sie auf **Neu**, und füllen Sie das Formular „Anomalietestregeln“ aus.

Feld	Beschreibung
Name	Name für die Modelltestregel
Betrifft	Die Tabelle, aus der CI/Metrik-Paare für die Modelltestregel ausgewählt werden. Hierfür wird die Tabelle „Metrik-Zuordnung an CI“ [sa_metric_map] verwendet.
Regel	Filterbedingungen, um CI/Metrik-Paare für Anomaliemodelltests anzugeben. Ergibt die Regel mehr als 20 CI/Metrik-Paare, wird die Liste auf 20 Einträge beschränkt.
Startdatum/Enddaten	Der Zeitraum, für den die Anomalie-Erkennungstests angewendet werden sollen. Der Zeitraum muss innerhalb der letzten 7 Tage liegen.

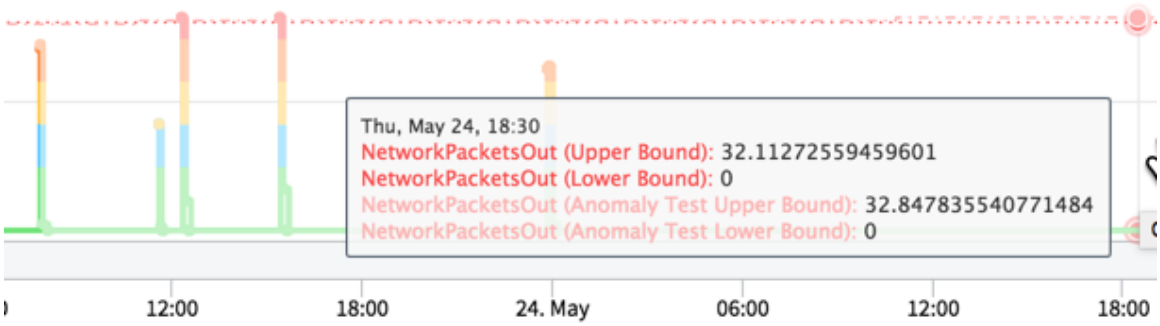
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Status	Der Status des Tests. Wird während der Ausführung von Testläufen automatisch vom System aktualisiert. Der Status lautet anfänglich „Geplant“ und wird schließlich in „Abgeschlossen“ geändert.
URL	URL zum Explorer für Einblicke, in dem die Ergebnisse des Anomaliemodelltests vorab geladen werden
Hinweise	Protokollierungszusammenfassung, die automatisch vom System mit Details zu jeder Testausführung der Anomalietestregel aktualisiert wird.

3. Klicken Sie auf **Anomalietest ausführen**.
   Während der Testausführung werden die Felder **Status**, **URL** und **Hinweise** automatisch aktualisiert, um den Fortschritt des Auftrags widerzuspiegeln.
4. Nachdem **Status** zu „Abgeschlossen“ geändert wurde, klicken Sie auf den **URL**-Link, um den Explorer für Einblicke mit den Testergebnissen zu öffnen.

Ergebnisse

Die Grenzen und das Diagramm für den Anomaliemodelltest werden im Explorer für Einblicke in blassen Farben angezeigt. Außerdem wird für die obere und die untere Grenze, die durch den Test berechnet werden, ein Linienmuster verwendet, das sich von dem Linienmuster unterscheidet, das für tatsächliche Anomalie-Erkennungsergebnisse verwendet wird. Anhand dieser Unterschiede können Sie zwischen den Ergebnissen der tatsächlichen Anomalie-Erkennung und von Anomaliemodelltests unterscheiden, wenn beide in den Diagrammeinstellungen ausgewählt sind.



Nächste Maßnahme

- Ändern Sie den Datumsbereich für den Test, oder wählen Sie eine andere Zeitreihe aus, und klicken Sie erneut auf **Anomalietest ausführen**, um fortzufahren und das Modell zu optimieren.
- Klicken Sie auf das Symbol **Diagrammeinstellungen** für ein Diagramm, um zwischen der Anzeige von Statistiken und Zusammenfassungen im Diagramm umzuschalten. Wählen Sie in den Abschnitten mit den Anomalietststatistiken und den Anomaliestatistiken die Optionen **Grenzen anzeigen** und **Abweichende Punktzahlen anzeigen** aus, um Testergebnisse neben den Ergebnissen der tatsächlichen Anomalie-Erkennung anzuzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Ergebnisse von Anomaliemodelltests können den Ergebnissen der tatsächlichen Anomalie-Erkennung sehr ähnlich sein. Wenn Sie das Diagramm so konfigurieren, dass beide gleichzeitig angezeigt werden, ist es möglicherweise schwierig, Unterschiede zu erkennen, wenn Sie mit der Maus über das Diagramm fahren.

- Wenn Sie mit den Anomalietestergebnissen zufrieden sind, aktivieren Sie die Anomalie-Erkennung in der Produktionsumgebung für die im Test angegebenen Metriken und CIs. Unter Zu überwachende Metriken auswählen und konfigurieren finden Sie weitere Details.

Zugehörige Informationen

Metrikwerte im Explorer für Einblicke anzeigen

Benutzerdefinierte Ober- und Untergrenzen für Metriken festlegen

Mit dem Assistenten für Grenzeneinstellungen können Sie gelernte Kontrollgrenzen außer Kraft setzen, indem Sie benutzerdefinierte Ober- und Untergrenzen für eine Metric Intelligence-Metrik festlegen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Metric Intelligence berechnet obere und untere **Kontrollgrenzen** für Metriken mithilfe von statistischen Modellen, die aus historischen Metrikdaten gelernt wurden. Die Ober- und Untergrenzen werden dann in der Analyse verwendet, um auffällige CIs oder Ressourcen zu erkennen, die sich auf die Anomaliepunktzahlen auswirken. Basierend auf historischen Daten können einige CIs, Ressourcen oder Metriken Werte aufweisen, über die Sie trotz der berechneten Bereiche ausdrücklich informiert werden möchten oder nicht. Beispielsweise der Versuch, eine SLA zu erfüllen, ohne dass eine Metrik einen bestimmten Wert zu lange über- oder unterschreiten darf, ohne darüber benachrichtigt zu werden. Wenn konkrete obere oder untere Grenzwerte für eine Metrik bekannt sind, können Sie diese Metrik mit benutzerdefinierten Grenzen konfigurieren, um die berechneten Grenzwerte außer Kraft zu setzen. Beispielsweise eine CPU-Metrik, die 85 % nicht überschreitet.

Mit dem Assistenten für Grenzeneinstellungen können Sie benutzerdefinierte statische Grenzen oder Grenzwertbereiche festlegen und eine Vorschau der Anomalieanalyse der tatsächlichen Daten basierend auf den benutzerdefinierten Einstellungen anzeigen. Der Assistent für Grenzeneinstellungen generiert automatisch die Metrikklasse und die Regel für die Konfigurationseinstellungen, mit denen benutzerdefinierte Grenzen verknüpft werden müssen.

Im Assistenten für Grenzeneinstellungen können Sie eine der folgenden Optionen für benutzerdefinierte Kontrollgrenzen auswählen:

Statische Ober- und Untergrenzen

Benutzerdefinierte statische Grenzwerte für die Ober- und Untergrenze werden als effektive Kontrollgrenzen verwendet, wobei die gelernten Werte für die Ober- und Untergrenze für die Metrik vollständig außer Kraft gesetzt werden. Der Mittelwert der Metrikdaten muss innerhalb des angegebenen Wertebereichs der statischen Grenzen liegen, andernfalls werden die statischen Grenzen nicht angewendet.

Wertebereiche für Unter- und Obergrenzen

Benutzerdefinierte Ober- und Untergrenzen, jeweils ausgedrückt als ein Wertebereich. Die geltenden Grenzen sind eine Kombination aus den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

benutzerdefinierten Minimal- und Maximalwerten, die den Grenzwertbereich definieren, und den erlernten oberen und unteren Grenzen:

- Wenn ein gelernter Grenzwert für einen Zeitpunkt innerhalb des benutzerdefinierten Wertebereichs der Ober- bzw. Untergrenze liegt, ist der gelernte Grenzwert wirksam.
- Wenn ein erlernter Grenzwert für einen Zeitpunkt außerhalb des benutzerdefinierten Wertebereichs liegt, gelten die **Max.**- bzw. **Min.**-Werte des benutzerdefinierten Bereichs. Wenn der erlernte Wert den benutzerdefinierten Bereich überschreitet, gilt der benutzerdefinierte **Max.**-Wert, und wenn er darunter liegt, gilt der benutzerdefinierte **Min.**-Wert.

Wenn ein metrischer Wert außerhalb einer Kontrollgrenze liegt, wird die Abweichung von der Kontrollgrenze durch einen **Breitenwert** normalisiert, den das System aus Daten berechnet. Die unteren und oberen Breitenwerte bestimmen, um wie viel ein Metrikwert die Kontrollgrenzen überschreiten muss, damit eine Anomalie vorliegt. Die Änderung einer Breite für die Kontrollgrenzen beeinflusst die Geschwindigkeit, mit der eine hohe Anomaliepunktzahl erreicht und über die Anomalie informiert wird. Neben der Einstellung benutzerdefinierter Kontrollgrenzen können Sie Breitenwerte außer Kraft setzen, indem Sie benutzerdefinierte Abweichungs- und Zeitwerte angeben, mit denen das System benutzerdefinierte Breitenwerte berechnet.

Das System speichert benutzerdefinierte Kontrollgrenzen und benutzerdefinierte Breiten für eine Metrik in einer **Metrikklasse**. Benutzerdefinierte Werte in einer Metrikklasse haben Vorrang vor den gelernten Grenzen und Breiten für die Metrik und werden dann in der nachfolgenden Anomalieanalyse verwendet.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Grenzwerteinstellungen**.
2. Klicken Sie in der Listenansicht „Grenzeneinstellungen“ auf **Hinzufügen**, um den Assistenten für Grenzeneinstellungen zu öffnen.
3. Konfigurieren Sie auf der Registerkarte **Umfang auswählen** die folgenden Einstellungen, und klicken Sie dann auf **Weiter**.

Feld	Beschreibung
Quellmetriktypen	Quellmetriktyp, für den diese Grenzeneinstellung gilt. Wählen Sie ein Element aus der Dropdown-Liste und klicken Sie dann auf das Symbol „Quellenmetriktyp hinzufügen“ (**+**), um das ausgewählte Element zu **Ausgewählte Quellmetriktypen** hinzuzufügen.
Bereich	Umfang der CIs oder Ressourcen, für die diese Grenzeneinstellung gilt. Sie können für den Umfang **Alle CIs**, **Spezifisches CI oder spezifische Klasse**, **Bestimmte Ressourcen oder Ressourcenklassen**festlegen. Je nach

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Einstellung können Sie den Umfang dann weiter filtern.

4. Konfigurieren Sie auf der Registerkarte **Grenzeneinstellungen anwenden** die folgenden Einstellungen, und klicken Sie dann auf **Weiter**.

Feld	Beschreibung
Name der Grenzeneinstellungen	Eindeutiger Name für diese Grenzeneinstellung
Grenzentyp	Methode zur Angabe der benutzerdefinierten statischen Grenzen: ◦ Statische Unter- und Obergrenzen festlegen ◦ Wertebereiche für Ober- und Untergrenzen festlegen
Erweiterte Einstellungen anzeigen	Die folgenden Felder werden angezeigt: ◦ **Wenn die untere Grenze** und **Der Metrikwert ist niedriger als die Untergrenze von** ◦ **Wenn die obere Grenze** und **Der Metrikwert ist höher als die Obergrenze von** ◦ **Kritischen Alarm nach der Dauer (Min.) senden** Geben Sie die Abweichung für ungewöhnliche Werte (in absoluten Werten) und die Dauer für das Senden einer Anomaliewarnung an. Diese Werte werden intern verwendet, um den Breitenwert für die Metrik zu berechnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: ◦ Wenn die für die Grenzwerteinstellung angegebene Metrikklasse mit Werten für das Überschreiben der Breite aus einer aktualisierten Version konfiguriert ist, können Sie keine erweiterten Einstellungen festlegen. Um erweiterte Einstellungen festzulegen, akzeptieren Sie die angezeigten Benachrichtigung und erklären Sie sich damit einverstanden, dass diese Werte für das Überschreiben der Breite gelöscht werden. ◦ Alle Felder müssen Werte enthalten. Wenn Sie keinen Metrikwert festlegen möchten, müssen Sie `0` entweder im Feld **Der Metrikwert ist niedriger als die Untergrenze von** oder im Feld **Und der Metrikwert liegt über der oberen Grenze von** eingeben. ◦ Für die Mindestanzahl an Minuten können Sie den Wert `2` eingeben.
Untere Grenze	Statischer Wert der Untergrenze, der die gelernte Untergrenze für die Metrik ersetzt. Gilt für die Einstellung `Statische Ober- und Untergrenzen`.
Obere Grenze	Statischer Wert der Obergrenze, der die gelernte Obergrenze für die Metrik ersetzt. Gilt für die Einstellung `Statische Ober- und Untergrenzen`. Der Wert muss größer als der Wert für die **Untergrenze** sein.
Wertebereich für die Untergrenze	**Min.** und **Max.** des benutzerdefinierten Wertebereichs der Untergrenze. Gilt für die Einstellung `Wertebereiche für Ober- und Untergrenzen festlegen`.
Wertebereich für die Obergrenze	**Min.** und **Max.** des benutzerdefinierten Wertebereichs der Obergrenze. Gilt für die Einstellung `Wertebereiche für Ober- und Untergrenzen festlegen`.

5. Auf der Registerkarte **Vorschau anzeigen und bestätigen**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie einen **Quellmetriktyp**aus.

b. Wahlweise: Wählen Sie einen **Metriktyp** für die Vorschau aus.

c. Wahlweise: Geben Sie einen **CI-Namen** und einen **Ressourcennamen** ein, die Sie in die Vorschau aufnehmen möchten.
Wenn Sie ein CI oder eine Ressource angeben, müssen sich diese innerhalb des zuvor angegebenen Umfangs befinden.

d. Klicken Sie auf **Vorschau**, um eine Anomalie-Erkennung für die angegebene Metrik und das angegebene CI mithilfe der neu angegebenen benutzerdefinierten Grenzen durchzuführen.

e. Überprüfen Sie die Vorschauergebnisse, und klicken Sie auf **Fertig stellen**, wenn die Ergebnisse den Erwartungen entsprechen.
Andernfalls kehren Sie zur vorherigen Registerkarte **Grenzeneinstellungen anwenden** zurück, passen Sie die Einstellungen an, und führen Sie dann die Vorschau erneut aus. Die Vorschauergebnisse sind eine abgespeckte Version des Anomaliemodelltests. Weitere Informationen zu den Ergebnissen und zum Ändern von Diagrammeinstellungen finden Sie unter Anomaliemodelltests.

Zugehörige Informationen

Regel für Konfigurationseinstellungen erstellen

Zuordnung zwischen Metriken und CI sowie Ressourcenbindung anzeigen

Sie können die Ergebnisse der Bindungen zwischen Metriken und CIs bzw. Ressourcen anzeigen, einschließlich Details zu fehlgeschlagenen Bindungen, die Sie zur Eindämmung des Fehlers verwenden können. Wenn Metric Intelligence eine Metrik nicht zuordnen und nicht an ein CI oder eine Ressource binden kann, wird das CI bzw. die Ressource erst dann in der Anomalie-Erkennung berücksichtigt, wenn es bzw. sie ordnungsgemäß zugeordnet wurde.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Wenn die Ressourcenbindung nicht aktiviert ist, werden keine Ergebnisse zur Ressourcenbindung angezeigt.

Warum und wann dieser Vorgang ausgeführt wird

Metric Intelligence verwendet Event-Regeln, um Metrikdaten einem spezifischen CI oder einer Ressource zuzuordnen, das bzw. die mit dem Metrik-Event verbunden ist. Die Ergebnisse dieser Zuordnungen werden in der Tabelle „Metrik-Zuordnung an CIs“ [sa_metric_map] gespeichert. Wenn die Zuordnung fehlschlägt, gibt der Bindungsstatus für die Metrik den allgemeinen Grund für den Fehler an, und weitere Details zum Fehler werden bereitgestellt. Untersuchen Sie die Details eines Zuordnungsfehlers und mindern Sie das Problem, um die genaue und effektive Verarbeitung der Metrikdaten zu verbessern.

- Wenn die Zuordnung zu einem CI erfolgreich ist, wird das zugeordnete CI in der Spalte **Configuration Item** angezeigt. Wenn die Ressourcenbindung versucht wurde, aber fehlgeschlagen ist, wird das zugeordnete CI nicht angezeigt, selbst wenn die Zuordnung zu einem CI erfolgreich war. Fehlende oder doppelte CIs können zum Fehlschlagen der CI-Zuordnung führen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Bei erfolgreicher Zuordnung zu einer Ressource wird die zugeordnete Ressource in der Spalte **Ressource** angezeigt. Fehlt eine Ressourcentabelle, die dem CI-Typ zugeordnet ist, an den das Event gebunden ist, oder fehlt ein *resource_path*-Attribut im Event, schlägt die Ressourcenbindung fehl.

Datensätze in der Tabelle „CI-Zuordnungen“ [sa_metric_map] bleiben 24 Stunden (standardmäßig, wenn die Zuordnung zum CI nicht erfolgreich ist) oder 5 Tage (standardmäßig, wenn die Zuordnung zum CI erfolgreich ist) gültig. Später, wenn innerhalb dieses Zeitraums Rohdaten für ein Metrik-CI-Paar ankommen, das bereits einen Datensatz hat, wird die vorhandene Zuordnung verwendet, um die Daten einem vorhandenen CI zuzuordnen. Nach dem Ablauf der Datensätze der Metrik-CI-Zuordnungen müssen die neu eingehenden Rohdaten neu zugeordnet werden. Diese Datensätze laufen ab, wenn:

- Der 24-Stunden- oder 5-Tage-Zyklus endet
- Sich eine Event-Regel geändert hat – dies löst ein sofortiges Ablaufen des jeweiligen Zuordnungsdatensatzes aus.

Das Anpassen von Zuordnungen an das Hinzufügen oder Entfernen von CIs durch Discovery wirkt sich erst ab dem Beginn des nächsten Zyklus aus.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Metrik an CI**.
   Die Seite **Metrik-Zuordnung an CIs** wird angezeigt.

Spalte	Beschreibung
Quelle	Datenquelle für die Metrik
Metriktyp-ID	Metrik, die für das CI gemessen wird, z. B. Datenträger% und CPU%
Metrik-Identifier	Eine Zeichenfolge in Form von CI/Ressource/Metrik, durch die ein CI und eine Metrik eindeutig identifiziert werden
Configuration Item	Das einer Metrik zugeordnete CI in der CMDB. Ein fehlender Wert bedeutet Folgendes: ◦ Die Zuordnung der Metrik zu einem CI war nicht erfolgreich. ◦ Die Ressourcenbindung ist aktiviert, jedoch fehlgeschlagen. **Configuration Item** fehlt, obwohl die Bindung an ein CI erfolgreich war.
Ressource	Die einer Metrik zugeordnete Ressource. Wenn die Ressourcenbindung aktiviert ist, deutet ein fehlender Wert darauf hin, dass die Zuordnung der Metrik zu einer Ressource nicht erfolgreich war.
Ablaufdatum	Ablaufdatum des Datensatzes
Aktionsebene der Anomalie-Erkennung	Die Ebene der Verarbeitung und Analyse der Erkennung von Anomalien, die auf CIs und Metriken angewendet wird. Verfügbare Optionen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Spalte	Beschreibung
	◦ **Nur Metriken**: Die Metriken aus der Datenquelle werden nur erfasst, ohne sie weiter zu verarbeiten. ◦ **Grenzen**: Beinhaltet die Verarbeitungsebene „Nur Metriken“. Zusätzlich werden statistische Modelle erzeugt und Grenzen im Explorer für Einblicke angezeigt. ◦ **Anomaliepunktzahlen**: Beinhaltet die Verarbeitungsebene „Grenzen“. Zusätzlich werden Anomaliepunktzahlen berechnet und angezeigt. ◦ **Anomaliewarnungen**: Beinhaltet die Verarbeitungsebene „Anomaliepunktzahlen“. Zusätzlich werden gegebenenfalls Anomaliewarnungen erzeugt. ◦ **IT-Warnungen**: Beinhaltet die Verarbeitungsebene „Anomaliewarnungen“. Zusätzlich werden gegebenenfalls IT-Warnungen auf Grundlage der Anomaliewarnungen erzeugt.
Bindungsstatus	Status der Zuordnung der Metrik zu einem CI oder einer Ressource. Der Status **CI gefunden** gibt an, dass die Zuordnung erfolgreich war. In diesem Fall wird das zugeordnete CI in der Spalte **Configuration Item** angezeigt. Jeder andere Status gibt an, dass die Zuordnung fehlgeschlagen ist, und es wird ein allgemeiner Grund für den Fehler angegeben. Weitere Details zum Fehler finden Sie in der Spalte **Grund für Bindungsfehler**.
Grund für Bindungsfehler	Spezifische Details zur fehlgeschlagenen Zuordnung, z. B. Klassen- und Hostnamen und die verwendeten Abfragen. Klicken Sie auf den entsprechenden **Event**-Link, um weitere Details im Feld **Verarbeitungsnotizen** anzuzeigen.

2. Überprüfen Sie ggf. den **Bindungsstatus** und den **Grund für den Bindungsfehler**. Lösen Sie das Problem anhand der angegebenen Details:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bindungsstatus	Fehlerkorrektur
Host-CI fehlt	Führen Sie Discovery aus oder füllen Sie die CMDB auf andere Weise mit dem fehlenden Host-CI aus.
Nicht-Host-CI fehlt	Führen Sie Discovery aus oder füllen Sie die CMDB auf andere Weise mit dem fehlenden Nicht-Host-CI aus.
Nicht-Host-CI-Duplikat	Verwenden Sie die Nachbesserung von CI-Duplikaten, um dieses Duplikat zu korrigieren.
Abhängiges CI-Duplikat	Verwenden Sie die Nachbesserung von CI-Duplikaten, um dieses Duplikat zu korrigieren.
Abhängiges CI fehlt	Führen Sie Discovery aus oder füllen Sie die CMDB auf andere Weise mit dem fehlenden abhängigen CI aus.
Doppelter Metrikzuordnungseintrag ist vorhanden	Überprüfen Sie **Grund für Bindungsfehler**, und vergleichen Sie die Metrikbezeichner, die den doppelten Metrikzuordnungseinträgen zugeordnet sind. Wenn sich Metrik-IDs geändert haben (z. B. wurde ein Bezeichner hinzugefügt), legen Sie den Eintrag für diese Reihe in der Tabelle „CI-Zuordnungen“ [sa_metric_map] so fest, dass sie ablaufen, oder löschen Sie den Eintrag. Überprüfen Sie auch die zugehörige Event-Regel und vergewissern Sie sich, dass sie die Attribute korrekt extrahiert und nicht die gleiche CI für zwei verschiedene Metrikbezeichner extrahiert. Dieser Fehler kann auftreten, wenn zwei verschiedene Metrik-IDs derselben CI/Metrik zugeordnet sind.
Ressourcen-ID nicht gefunden	Verifizieren Sie, dass die Tabelle „CI-Typ zu Ressourcenklasse“ [sa_ci_type_to_resource_class] einen Zuordnungsdatensatz für den jeweiligen CI-Typ oder für einen seiner übergeordneten Typen enthält. Vergewissern Sie sich dann, dass es eine Tabelle mit dem Namen der Ressourcenklasse für diesen Datensatz gibt.

Nächste Maßnahme

Gruppieren Sie den **Grund für den Bindungsfehler** nach dem **Bindungsstatus**, um eine Zusammenfassung mit der Anzahl der Datensätze pro Fehlerkategorie zu erstellen. Mit diesem Bericht können Sie die Probleme effizient beheben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Erstellen einer Ereignisregel zum Zuordnen von Metriken zu bestimmten CIs

Metrik für ein CI deaktivieren

Metric Intelligence kann so konfiguriert werden, dass erhebliche Datenmengen erfasst werden, von denen einige möglicherweise nicht erforderlich sind. Zur Optimierung der Leistung können Sie eine bestimmte Metrik für ein bestimmtes CI deaktivieren, um die Verarbeitung von Daten im Zusammenhang mit der angegebenen Metrik und dem CI zu beenden.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Die Einstellung *Active* („true“ oder „false“) für eine Quellenmetrik in der Tabelle „Überwachungssystemmetriken“ [sa_source_metric_type] hat Vorrang vor der Einstellung für die entsprechende Metrik in der Tabelle „Metrik-Zuordnung an CIs“ [sa_metric_map]. Wenn ein Quellmetriktyp in der Tabelle „Überwachungssystemmetriken“ [sa_source_metric_type] deaktiviert ist, werden alle Datensätze, die sich auf die entsprechenden Metriken beziehen, aus der Tabelle „Metrik-Zuordnung an CIs“ [sa_metric_map] entfernt.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Metrik an CI**.
2. Suchen Sie den Datensatz für die Metrik bzw. das CI, die bzw. das Sie deaktivieren möchten, und legen Sie für die Spalte **Aktiv false** fest.

Event-Sammlung deaktivieren

Aus leistungstechnischen Gründen ist es vielleicht sinnvoll, die Erfassung von Ereignissen aus einer Datenquelle, aus der auch metrische Daten erfasst werden, zu deaktivieren. Sie können die Event-Sammlung für Datenquellen wie Nagios XI-Server, SolarWinds-Überwachungssystem und Zabbix-Server deaktivieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Hinweis: Um die Event-Sammlung nach der Deaktivierung wieder zu starten, müssen Sie das Originalskript des Connector wiederherstellen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Integrationen** > **Anschlussinstanzen**.
2. Wählen Sie eine Connector-Instanz für die Datenquelle aus, für die die Event-Sammlung deaktiviert werden soll.
   Wählen Sie beispielsweise eine Connector-Instanz für Nagios, SolarWinds oder Zabbix aus.
3. Legen Sie einen hohen Wert für **Zeitplan für Eventsammlung (Sekunden)** fest, z. B. 20.000.000.
   Diese Einstellung vermeidet unnötige eine Kommunikation mit MID Server und optimiert die Leistung.
4. Klicken Sie auf **Aktualisieren**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Navigieren zu **MID-Server** > **Skripteinbindungen** und erweitern das Skript des Connectors (z. B. *NagiosMetrics_JS*, *SolarWindsJS*oder *ZabbixJS*), indem Sie die Methode *execute* überschreiben.
   Fügen Sie ein Code-Snippet wie das Folgende hinzu, und klicken Sie dann auf **Aktualisieren**:

Example: Snippet für Nagios

```
var NagiosJSCustom = Class.create();

// Extending Nagios default script
NagiosJSCustom.prototype = Object.extendsObject(NagiosJS, {

// Override execute method
                    execute: function() {
        var retVal = {};
        retVal['status'] = SUCCESS.toString();
       retVal['error_message'] = "Disabled by custom Class, 'Last event
 collection status' will be 'error' and this is normal. To achieve
 success status, enable event pull in custom class(NagiosJSCustom)";

        return retVal;
    });
```

Für den SolarWinds-Connector verwenden Sie:

```
var SolarWindsJSCustom = Class.create();

// Extending solarwinds default script
SolarWindsJSCustom.prototype = Object.extendsObject(SolarWindsJS, {
```

Für den Zabbix-Connector verwenden Sie:

```
var ZabbixJSCustom = Class.create();

// Extending zabbix default script
ZabbixJSCustom.prototype = Object.extendsObject(ZabbixJS, {
```

Schwellenwerte für Anomaliepunktzahlen konfigurieren

Metric Intelligence ordnet Anomalien eine Punktzahl zwischen 0 und 10 zu. Dieser Bereich ist in die fünf Stufen des Schweregrades von Ereignissen unterteilt, die im Explorer für Einblicke und in der Anomaliezuordnung jeweils durch eine andere Farbe dargestellt werden.
Sie können den Schwellenwert für die Anomaliepunktzahl für jede Schweregradstufe konfigurieren.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Schwellenwerte für die Anomaliepunktzahl sind in der Tabelle „Zuordnung der Anomaliepunktzahl an den Event-Schweregrad“ [sa_metric_anomaly_score_to_event_severity_map] definiert. Beispielsweise haben Anomaliepunktzahlen von 8 bis 9 standardmäßig den Schweregrad 2 (Schwerwiegend) und werden im Explorer für Einblicke und in der Anomaliezuordnung dunkelorange angezeigt.

Informationen zu den Ereignis-Schweregraden, denen die einzelnen Zahlen entsprechen, finden Sie unter Ereignisschweregrade.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Anomalie-Erkennung** > **Zuordnung der Anomaliepunktzahl zu Schweregrad**.
2. Doppelklicken Sie in der Listenansicht **Zuordnung der Anomaliepunktzahl der Metrik an Event-Schweregrad** auf den Event-Schweregrad, den Sie ändern möchten.
3. Ändern Sie den Wertebereich der Anomaliepunktzahlen, die dem jeweiligen Event-Schweregrad zugeordnet sind.
4. Klicken Sie auf **Aktualisieren**.

Zeigen Sie Anomaliewarnungen an

Anomaliewarnungen weisen auf eine Abweichung von den projizierten Metrikwerten für überwachte CIs hin. Anomaliewarnungen sind von den regulären IT-Warnungen getrennt und werden nicht im Service Operations-Arbeitsbereich angezeigt. Sie können eine Heraufstufungsregel für Anomaliewarnungen definieren, um eine IT-Warnung zu generieren, die auf Anomaliewarnungen basiert.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Das statistische Modell wird verwendet, um Standardabweichungen, die obere und die untere Grenze sowie statistische Ausreißer zu berechnen, die dann zum Erkennen von Anomalien verwendet werden. Eine Anomalie tritt auf, wenn Metrikwerte außerhalb der prognostizierten Werte gemäß dem statistischen Modell liegen. Das System überwacht die Häufigkeit und Beständigkeit von statistischen Ausreißern im Zeitverlauf, um eine Punktzahl zwischen 0 und 10 zu berechnen, die angibt, wie anomal eine Abweichung ist.

Metrikdaten generiert ständig Anomaliewarnungen, wenn die Anomaliepunktzahl über Null liegt. Wenn eine Punktzahl über vier vorhanden ist und sich gegenüber der vorherigen Punktzahl geändert hat, wird sie an die Instanz gesendet. Auf der Instanz kann dann die gesamte Sequenz von Anomaliepunktzahlen im Zeitverlauf im Explorer für Einblicke angezeigt werden.

Metrikdaten überwacht Verlaufsdaten, um sicherzustellen, dass die Metrikgrenzen genau sind und die Warnungen geschlossen werden, wenn das anomale Verhalten aufhört. Metrikdaten ignoriert auch irrelevante Anomalien basierend auf den Bezeichnungen der Metrik. Wenn beispielsweise die verfügbare CPU von ihrer Obergrenze von 50 % auf 60 % ansteigt, wird die Bezeichnung *available* als Indikator dafür identifiziert, dass das Verhalten nicht als Anomalie registriert werden darf. Dies liegt daran, dass die Erhöhung der verfügbaren CPU ein positives Ergebnis darstellt, auch wenn die Metrik von 60 % ansonsten eine Anomalie darstellen würde.

Sie können eine Liste von Anomaliewarnungen wie unten beschrieben anzeigen. Für Zusammenfassungen und Berichte können Sie die Anomaliezuordnung anzeigen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Metriken** > **Anomaliewarnungen**.
2. Doppelklicken Sie in der Listenansicht **Alarm-Anomalien** auf den Alarm, den Sie anzeigen möchten.
   Informationen zu einer Anomaliewarnung umfassen Details wie Metrikwert, Heraufstufungsparameter, für die Warnung relevante Ereignisse (die in den Arbeitsnotizen für die Warnung angezeigt werden) sowie die obere und die untere Grenze (Untergrenzen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

dürfen nicht kleiner als 0 sein). Die Beschreibung enthält Details dazu, warum die Anomaliewarnung generiert wurde, und andere Details wie den Metriknamen und die Anomaliepunktzahl.

Nächste Maßnahme
Erstellen Sie eine Advanced Promotion Engine -Definition, um die Bedingungen zu definieren, die erfüllt sein müssen, um Anomaliewarnungen zu IT-Warnungen heraufzustufen. Details finden Sie unter Erstellen Sie eine Definition für Advanced Promotion Engine.

Metrikwerte im Explorer für Einblicke anzeigen

Metric Intelligence berechnet Statistiken für CI-Metrikdaten. Der Explorer für Einblicke zeigt diese Metrikwerte als Metrikdiagramme für die CIs in der CMDB an. Mit dem Explorer für Einblicke können Sie Metriken für beliebige CIs in einem einzelnen Diagramm überlappen, um eine mehrschichtige Ansicht von Metrikwerten über einen Zeitbereich zu erstellen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird
Der Explorer für Einblicke bietet eine Canvas, auf die Sie verschiedene Metriken für CIs ziehen und auf der Sie Diagramme erstellen können. Sie können eine einzelne Metrik auf der Canvas für eine einzelne Metrik für ein CI platzieren. Für ein umfassenderes Diagramm können Sie mehrere Metriken für ein einzelnes CI oder für verschiedene CIs übereinander legen, um ein Diagramm mit mehreren Metriken zu erstellen. In einem solchen Diagramm mit Ebenen wird jede Metrik durch eine eindeutige Farbe unterschieden, sodass Sie Metrikwerte über CIs innerhalb eines bestimmten Zeitbereichs vergleichen können.

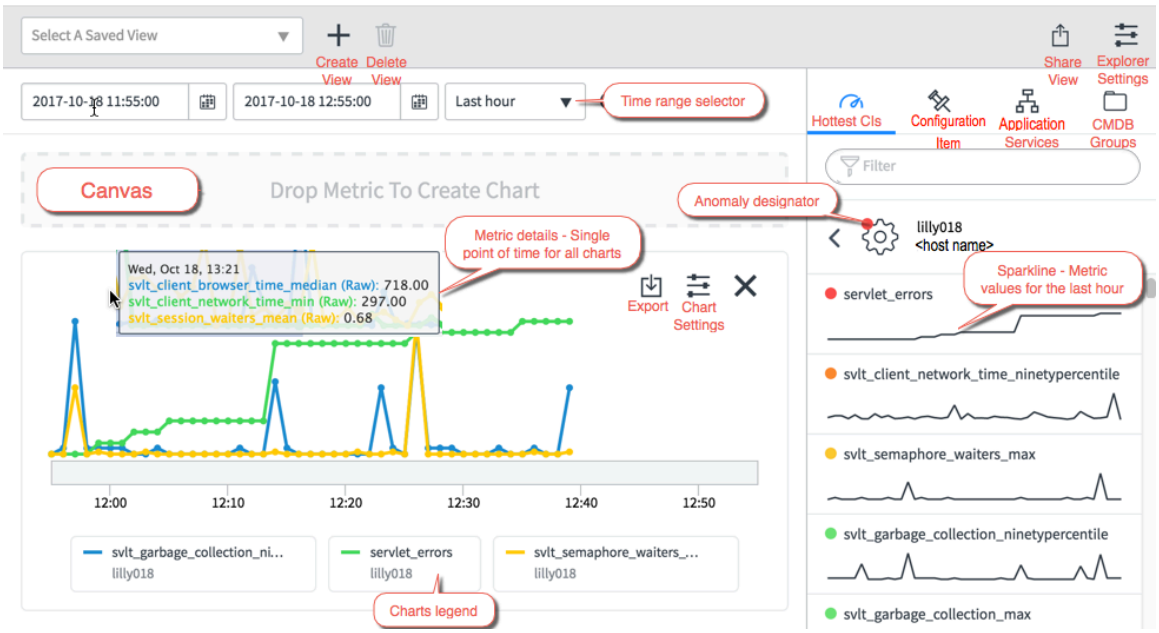
Der Explorer für Einblicke zeigt Metrikgrenzen gemäß dem zuletzt konfigurierten Modell an. Daher können Legacy-Anomalien aus einem früheren Build weiterhin als Anomalien angezeigt werden, auch wenn die Warnung gemäß den aktuellen Grenzen nicht als Anomalie gilt.

Sie können den Explorer für Einblicke auch über die folgenden Zuordnungen aufrufen:

- Zeigen Sie Metriken in einer Abhängigkeitsansichten-Karte an
- Zeigen Sie Metriken aus einer Business Service-Übersicht an

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Explorer für Einblicke



Wenn der Hostname des CI verfügbar ist, wird er unter dem CI-Namen angezeigt. Der Hostname wird ausgefüllt, indem die Knoteninformationen aus dem generierten Bindungsereignis als Teil der Metrikbindung abgerufen werden.

So navigieren Sie zu einem CI, für das Metriken angezeigt werden sollen:

- Verwenden Sie „Heißeste Configuration Items“ ( ), um schnell auf die 10 anomalsten CIs zuzugreifen.
- Verwenden Sie „Configuration Items“ ( ), um eine separate benutzerdefinierte Liste aller CIs aus der CMDB zu erstellen und dann die Metriken für diese CIs der Canvas hinzuzufügen.
- Verwenden Sie Anwendungsservices ( ), um eine anwenderdefinierte Liste von Anwendungsservices zu erstellen, mit denen Sie Detailinformationen zu den CIs dieser Services anzeigen können. Anschließend können Sie der Canvas Metriken für diese CIs hinzufügen.
- Verwenden Sie „CMDB-Gruppen“ ( ), um eine benutzerdefinierte Liste von CMDB-Gruppen zu erstellen, mit der Sie Detailinformationen der CIs dieser Gruppen anzeigen können. Anschließend können Sie der Canvas Metriken für diese CIs hinzufügen.

Die folgenden Farben, die auf Farbeinstellungen für Warnungsschweregrade basieren, geben Anomalieschweregrade an:

Rot

Schweregrad „Kritisch“ (höchster Schweregrad)

Orange

Schweregrad „Schwerwiegend“

Gelb

Schweregrad „Gering“

Blau

Schweregrad „Warnung“ (niedrigster Schweregrad)

Grün

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Informativ. Kein Schweregrad

Die Punkte oben links auf den CI-Symbolen zeigen den allgemeinen Nachverfolgungsstatus für Anomalien an:

- Grau: Metriken werden für das CI nachverfolgt, aber bei keiner dieser Metriken ist jemals eine Anomalie aufgetreten.
- Grün: Metrik für CI hatte mindestens eine Anomalie in der Vergangenheit, aber die Anomaliepunktzahl ist derzeit 0.
- Farbig: Entspricht dem zuletzt aufgezeichneten Schweregrad gemäß der Konfiguration der Farbbandbereiche.
- Kein Punkt: Es gibt keine Metriken für das CI und es sind keine Daten vorhanden, für die eine Anzeige der Detailinformationen ausgeführt werden kann.

Hinweis: **Configuration Items** und **Anwendungsservices** enthalten wahrscheinlich CIs, für die keine Metrikdaten vorhanden sind.

Metric Intelligence verfolgt keine Änderungen an einer Anomaliepunktzahl nach, wenn sie sich im grünen Bandbereich befindet.

Beim Erstellen von Diagrammen wird automatisch eine Legende für jedes Seriendiagramm unter dem Diagramm angezeigt. Bei einem Diagramm mit einer Metrik enthält die Legende Einträge für die Zusammenfassungen im Diagramm. Bei einem Diagramm mit mehreren Metriken enthält die Legende Einträge für die Metriken in dem Diagramm.

Änderungen im Explorer für Einblicke bleiben während der Sitzung erhalten, sobald der Explorer für Einblicke aktualisiert wird, kehrt er jedoch in seinen Ausgangszustand zurück.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Metriken** > **Explorer für Einblicke**.
2. Klicken Sie auf ein CI, um Detailinformationen zur zugehörigen Liste von Metriken anzuzeigen, geordnet nach den neuesten Anomaliepunktzahlen.

   Für jede Metrik werden in einer Sparkline Metrikwerte für das CI für die letzte Stunde angezeigt. Zeigen Sie auf die Sparkline, um den Metrikwert zu jedem Zeitpunkt anzuzeigen.

   Wenn Ressourcenbindung aktiviert ist, enthält die Liste der für ein CI überwachten Reihen auch Reihen, die zu einer Ressource und Metrik gehören. Die Benennungskonvention für solche Reihen lautet „<Ressourcenname>/<Metrikname>“. Für eine Reihe, die nur an ein CI gebunden ist, lautet die Benennungskonvention „<Metrikname>“.

3. Ziehen Sie eine Metrik in den Bereich **Metrik in Diagrammerstellung verwerfen** auf der Canvas, und zeigen Sie auf das Diagramm, um den genauen Metrikwert zu jedem Zeitpunkt anzuzeigen.
   Das Metrikdiagramm zeigt Daten für den angegebenen Zeitraum gemäß den Diagrammeinstellungen an. Standardmäßig werden Rohdaten angezeigt. Wenn der Zeitraum länger als eine Woche ist oder vor der vergangenen Woche liegt, werden Durchschnittsdaten angezeigt. Ziehen Sie die nachfolgende Metrik wie folgt auf die Canvas:
   - In den Bereich **Metrik zum Erstellen von Diagramm ablegen**, damit sie einzeln in einem neuen Diagramm angezeigt wird.
   - Auf ein vorhandenes Diagramm im hervorgehobenen Block **Diagramm ersetzen**, um das vorhandene Diagramm zu überschreiben.
   - Auf ein vorhandenes Diagramm im hervorgehobenen Block **Metrik hinzufügen**, um sie mit den im Diagramm vorhandenen Metriken zu überlappen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie mehrere Metriken in einem einzelnen Diagramm anzeigen, gilt dieselbe Zusammenfassungsauswahl für alle Metriken und die Statistikeinstellungen sind nicht verfügbar. Wenn beispielsweise **Durchschnitt** in den **Diagrammeinstellungen** ausgewählt ist, werden Durchschnittswerte für alle Metriken im Diagramm angezeigt.

4. Verwenden Sie das Feld **Suchen**, um nach bestimmten Configuration Items, Anwendungsservices oder CMDB-Gruppen zu suchen und zu filtern, die standardmäßig nicht aufgeführt sind.
   Klicken Sie im Abschnitt SUCHERGEBNISSE auf das +-Symbol neben dem Element, das Sie dem Abschnitt HINZUGEFÜGTE ELEMENTE hinzufügen möchten. Oder verwenden Sie die erweiterte Suche:
   - Wählen Sie aus, und klicken Sie dann auf **Configuration Item hinzufügen**, um bestimmte CIs hinzuzufügen. Wählen Sie im Dialogfeld „Konfigurationselemente hinzuzufügen“ einen **CI-Klassentyp** wie „Linux-Server“ aus.
   - Wählen Sie und klicken Sie dann auf **Fügen Sie einen Anwendungsservice hinzu**, um alle CIs hinzuzufügen, die in einem angegebenen Anwendungsservice enthalten sind. Wählen Sie im Dialogfeld „Add Application Services“ (Anwendungsservices hinzufügen) `„Erkannter Service“` oder `„Manueller Service“` als **CI-Klassentyp** aus, und geben Sie dann Filterbedingungen an, um die Suche einzugrenzen.

     Hinweis: Sie können Anwendungsservices nur hinzufügen, wenn *`Operational Status`* auf „funktionsfähig“ festgelegt ist.

   - Wählen Sie aus, und klicken Sie dann auf **CMDB-Gruppe hinzufügen**, um alle CIs hinzuzufügen, die in einer angegebenen CMDB-Gruppe enthalten sind. Geben Sie im Dialogfeld „CMDB-Gruppen“ Filterbedingungen wie **[Gruppenname] [beginnt mit] [d]** an, um die Suche einzugrenzen.

   Nachdem Sie die Elemente ausgewählt haben, die Sie hinzufügen möchten, klicken Sie auf **Hinzufügen**.

5. Fügen Sie die zugehörigen CIs hinzu:

   a. Klicken Sie auf das Symbol **Zugehörige CIs hinzufügen** ( ) neben einem CI.
   Das Dialogfeld „Zugehörige Configuration Items hinzufügen“ wird mit allen Beziehungen angezeigt, in denen das ausgewählte CI ein übergeordnetes oder untergeordnetes Element ist.

   b. Um die Liste weiter zu filtern, können Sie bestimmte Bedingungen definieren, die erfüllt werden müssen.

   c. Wählen Sie die Beziehungen aus, aus denen Sie das übergeordnete oder untergeordnete CI hinzufügen möchten, je nachdem, welches nicht das ausgewählte CI ist.

   d. Klicken Sie auf **Hinzufügen**.

   Die CIs aus den ausgewählten Beziehungen, die nicht dem ausgewählten CI entsprechen, werden der Liste der CIs im Explorer für Einblicke hinzugefügt.

6. Zeigen Sie auf ein Legendenelement, und klicken Sie auf das **X**-Symbol, um die entsprechende Metrik aus dem Diagramm zu entfernen oder die entsprechende Zeile in den **Diagrammeinstellungen** zu deaktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf das Zahnradsymbol **Einstellungen**, um die Anwendungseinstellungen zu öffnen:
   - Aktivieren oder deaktivieren Sie die Aktualisierung von Anomaliedaten im Explorer für Einblicke bzw. legen Sie die Häufigkeit dafür fest.
   - Aktivieren oder deaktivieren Sie die Anzeige zugehöriger Listen wie „Alle Warnungen“, „Incidents“ und „Probleme“. Weitere Informationen finden Sie unter Kartenindikatoren erstellen oder ändern .
8. Klicken Sie auf das Symbol **Diagrammeinstellungen**, um zwischen der Anzeige von Statistiken und Zusammenfassungen im Diagramm umzuschalten.
   Durch Aktivieren oder Deaktivieren eines Elements zum Hinzufügen oder Entfernen von Metriken aus einem Diagramm wird auch die Legende des Diagramms aktualisiert, um die Änderung widerzuspiegeln.

Diagrammeinstellung	Beschreibung
Grenzen anzeigen	Zeigt die berechnete obere und untere Grenze für die Metrik an, die auf dem Lernen vergangener Metrikwerte basiert. Die obere und die untere Grenze werden immer zusammen angezeigt.
Abweichende Punktzahlen anzeigen	Zeigt Anomaliepunktzahlen auf einer virtuellen Achse von 0–10 an. Dabei basiert der Farbcode auf den Punktzahlschwellenwerten, die in der Tabelle der Zuordnung der Anomaliepunktzahl zum Event-Schweregrad [sa_metric_anomaly_score_to_event_severity_map] definiert sind.
Durchschnitt	Zeigt zusammengefasste durchschnittliche Metrikwerte an, die in Intervallen von einer Stunde berechnet werden. Zusammengefasste Durchschnittswerte werden wie folgt angezeigt: ◦ Für Daten, die bis zu 8 Tage alt sind: Zeigt 10-Minuten-Zusammenfassungsfenster an. ◦ Für Daten, die bis zu 94 Tage alt sind: Zeigt 10-Minuten-Zusammenfassungsfenster an. ◦ Für ältere Daten: Zeigt Zusammenfassungsfenster von 1 Stunde an.
Minimum	Zeigt zusammengefasste minimale Metrikwerte an, die pro Stunde berechnet werden. Für Daten, die bis zu 8 Tage alt sind: Zeigt 10-Minuten-Zusammenfassungsfenster an.
Maximum	Zeigt zusammengefasste maximale Metrikwerte an, die pro Stunde berechnet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammeinstellung	Beschreibung
	Für Daten, die bis zu 8 Tage alt sind: Zeigt 10-Minuten-Zusammenfassungsfenster an.
Roh	Zeigt die rohen, nicht zusammengefassten Metrikwerte an. Diese Werte werden nur für die letzten 8 Tage gespeichert.

Nächste Maßnahme

- Zeigen Sie auf das Symbol eines CI in der rechten Leiste, um den CI-Typ anzuzeigen.
- Vergrößern oder verkleinern Sie die Ansicht, indem Sie die Standardauswahl **Letzte Stunde** für den Zeitbereich ändern. Wählen Sie einen der voreingestellten Zeiträume aus, um beispielsweise Anomaliepunktzahlen für die letzten **6 Stunden** anzuzeigen, oder geben Sie einen benutzerdefinierten Zeitraum für die letzten maximal 90 Tage an.

  Um die Anzeige zu vergrößern, markieren Sie einen Diagrammbereich, indem Sie auf die linke obere Ecke des Abschnitts zeigen und die Maus in die rechte untere Ecke des Abschnitts ziehen. Der Zeitbereich des Diagramms wird entsprechend geändert. Wenn sich auf der Canvas weitere Diagramme befinden, werden alle automatisch synchronisiert, um Daten für denselben Zeitbereich anzuzeigen. Der Zeitbereich in der Titelleiste wird automatisch entsprechend dem neuen Zeitbereich aktualisiert.
- Klicken Sie mit der rechten Maustaste auf ein CI in der rechten Seitenleiste, und wählen Sie **Formular anzeigen** aus, um das zugehörige CI- Formular zu öffnen.
- Klicken Sie auf das Kartensymbol neben einem Anwendungsservice, der auf der Registerkarte **Anwendungsservices** aufgeführt ist, um die zugehörige Anwendungsservicezuordnung zu öffnen.
- Klicken Sie neben einem CI auf „Entfernen“ (⊖), um es aus dem Explorer für Einblicke zu entfernen.
- Klicken Sie auf das Exportsymbol in einem Diagramm, um es als PNG- oder SVG-Bild oder als PDF-Dokument herunterzuladen.

Ansicht des Explorers für Einblicke erstellen

Sie können eine benutzerdefinierte Ansicht im Explorer für Einblicke erstellen, in der alle der Canvas hinzugefügten Metrikdiagramme und alle hinzugefügten Konfigurationselemente gespeichert werden. Nachdem Sie eine Ansicht erstellt haben, können Sie einen Link zur Ansicht freigeben.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Metriken** > **Explorer für Einblicke**.
2. Klicken Sie auf **Ansicht erstellen** (+), und geben Sie im Dialogfeld „Neue Ansicht erstellen“ einen **Namen** ein.
   Wenn Sie bereits dabei sind, eine Ansicht zu erstellen, können Sie **Mit vorhandenen Elementen erstellen** auswählen, um eine vorhandene Ansicht zur Bearbeitung zu laden, anstatt mit einer leeren Canvas zu beginnen.
3. Klicken Sie auf **Erstellen**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Fügen Sie Elemente hinzu, die in der Ansicht enthalten sein sollen:

   a. Ziehen Sie Metriken, und erstellen Sie Diagramme auf der Canvas.

   b. Fügen Sie Konfigurationselemente hinzu.
   Während Sie eine Ansicht ändern, wird sie bei jeder Aktualisierung automatisch gespeichert. Die Zeiteinstellungen werden nicht in Ansichten gespeichert, und wenn eine gespeicherte Ansicht geladen wird, wird ihr Zeitraum immer auf **Letzte Stunde** mit aktuellen Informationen festgelegt.

Nächste Maßnahme

- Freigeben einer Ansicht: Klicken Sie auf **Freigabeansicht** ( ), und klicken Sie dann im Dialogfeld „Freigeben“ auf **Link kopieren**. Senden Sie den Link, oder fügen Sie ihn ein, um ihn für alle Personen zugänglich zu machen, für die Sie die Ansicht freigeben möchten. Ein freigegebener Link erfasst den Zeitbereich der Ansicht, die der Canvas hinzugefügten Diagramme und alle hinzugefügten Konfigurationselemente.
- Gespeicherte Ansicht anzeigen: Öffnen Sie die Dropdown-Liste **Gespeicherte Ansicht auswählen**, und wählen Sie eine zuvor gespeicherte Ansicht aus, die Sie anzeigen möchten.

Metrikdiagramme in Agent Workspace anzeigen

Agent Workspace für Metric Intelligence bietet einfachen Zugriff auf Metrikdiagramme für ein CI. Auf einem Warnungsformular können Sie Detailinformationen zu wichtigen Metrikdiagrammen für das CI anzeigen, das der Warnung zugeordnet ist.

Vorbereitungen

- Das CI, für das Sie Metrikdiagramme anzeigen möchten, muss einer Warnung zugeordnet sein.
- Die Tabelle „Metadaten des Messgrößen-Dashboards“ [sa_metric_dashboard_metadata] muss aktive Diagrammkonfigurationen für die CI-Klasse enthalten, für die Sie Metrikdiagramme anzeigen möchten.

Erforderliche Rolle: workspace_user und itil

Warum und wann dieser Vorgang ausgeführt wird

Der Satz der Metrikdiagramme, Diagrammtypen und anderen Diagrammmerkmalen wird durch die Diagrammkonfigurationen in der Tabelle „Metadaten des Messgrößen-Dashboards“ [sa_metric_dashboard_metadata] für die CI-Klasse bestimmt.

Prozedur

1. Navigieren Sie zu **Agent Workspace** und klicken Sie auf **Agent Workspace-Startseite**.
2. Klicken Sie in Agent Workspace auf **Liste**, und wählen Sie im Bereich **Listen** eine der kategorisierten Listen unter **Warnungen** wie **Alle Alarme** oder **Höchste Priorität** aus.
3. Öffnen Sie in der Warnungslistenansicht eine Warnung.
   Der Warnung muss ein **Configuration Item** zugeordnet sein.
4. Klicken Sie auf der Registerkarte **Details** des Warnungsformulars auf **Metriken**.

Ergebnisse

Alle Metrikdiagramme, die für das der Warnung zugeordnete CI konfiguriert und aktiv sind, werden im Metrikdiagrammformular auf der Registerkarte **Metriken** angezeigt. Die Berechnung des Standardzeitbereichs für die Diagramme basiert auf den Zeiten, zu denen das erste und das letzte Ereignis aufgetreten sind, von denen die Warnung generiert wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Ändern Sie den Zeitbereich für die Diagramme, indem Sie die **Startzeit** und **Endzeit** ändern. Wenn Sie den Zeitbereich ändern, werden alle Diagramme entsprechend dem neuen Zeitbereich aktualisiert.
- Klicken Sie auf das Zahnradsymbol **Einstellungen öffnen**, und ändern Sie die Einstellungen für alle Diagramme:
  - **Grenzen anzeigen**: Zum Anzeigen der Grenzen im Diagramm. Auch wenn diese Option aktiviert ist, sind in dem Diagramm keine Grenzen für zusammengefasste Ressourcen vorhanden.
  - **Legende anzeigen**: Zum Anzeigen der Diagrammlegende.
- Klicken Sie auf **Explorer für Einblicke**, um den Explorer für Einblicke in einer neuen Browserregisterkarte zu öffnen. Dieser Explorer für Einblicke wird mit dem aktuell vorausgewählten CI und den aktuellen Zeitbereichseinstellungen in Agent Workspace geöffnet.

Metrikdiagramme für Agent Workspace konfigurieren

Konfigurieren Sie den Satz von Metric Intelligence-Metrikdiagrammen, Diagrammtypen und anderen Diagrammeigenschaften, die in Agent Workspace angezeigt werden.

Vorbereitungen

Erforderliche Rolle: admin oder evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Bis zu 10 Metrikdiagramme für eine Klasse können so konfiguriert werden, dass sie im Metrikdiagrammformular von Metrikdaten in Agent Workspace erscheinen. Die Metrikdiagrammkonfigurationen werden in der Tabelle „Metadaten des Messgrößen-Dashboards“ [sa_metric_dashboard_metadata] gespeichert und bestimmen, welche Metrikdiagramme für ein CI angezeigt werden, das einer Warnung zugeordnet ist. Standardmäßig enthält die Tabelle „Metadaten des Messgrößen-Dashboards“ vorkonfigurierte Metrikdiagramme für mehrere Klassen.

Wenn die Ressourcenbindung aktiviert ist und Sie einen **Ressourcentyp** in der Metrikdiagrammkonfiguration angeben, werden alle Ressourcen für das CI in das Diagramm aufgenommen. Die von Ihnen angegebene Klassentabelle für die Ressourcenklasse (z. B. *ci_resource_metric_extension*) wird zum Abrufen aller Ressourcen für das CI verwendet. Dann werden die Werte der Ressourcen für jeden Zeitpunkt in der Datenreihe zu einem einzelnen Datenpunkt zusammengefasst, der den Durchschnitt der Metrikwerte aller Ressourcen für diesen Zeitpunkt darstellt.

Diagrammzusammenfassung

Die Zusammenfassung wird je nach Einstellung des **Diagrammtyps** *und je nachdem, ob Ressourcen im Diagramm enthalten sind, unterschiedlich angewendet, wie durch die Einstellung des* **Ressourcentyps** *angegeben:*

Diagrammtyp	Ressourcen	Zusammenfassung
Time_Series	Nein	Keine Zusammenfassung
Time_Series	Ja	Ressourcen werden pro Datenpunkt gemittelt.
Single_Score	Nein	Datenpunkte werden gemäß der Einstellung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Diagrammzusammenfassung
Die Zusammenfassung wird je nach Einstellung des **Diagrammtyps** *und je nachdem, ob Ressourcen im Diagramm enthalten sind, unterschiedlich angewendet, wie durch die Einstellung des* **Ressourcentyps** *angegeben:*

(Fortsetzung)

Diagrammtyp	Ressourcen	Zusammenfassung
		Diagrammzusammenfassung zusammengefasst.
Single_Score	Ja	Datenpunkte werden pro Datenpunkt gemittelt und die Datenpunkte werden dann gemäß der Einstellung **Diagrammzusammenfassung** zusammengefasst.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Administration** > **Konfiguration der Metrikansicht**.
2. Wählen Sie in der Listenansicht „Metadaten des Messgrößen-Dashboards“ (Dashboard-Metadaten) eine vorhandene Konfiguration aus, oder klicken Sie auf **Neu**.
3. Füllen Sie das Formular „Metadaten des Messgrößen-Dashboards“ aus.

Feld	Beschreibung
Aktiv	Fügen Sie das Diagramm in das Formular für Metric Intelligence-Diagramme in Agent Workspace ein.
Ressourcentyp	Ressourcenklasse, die dem CI zugeordnet ist und für die alle Ressourcen abgerufen und zusammengefasst werden sollen
Configuration Item-Typ	CI-Klasse, für die das Diagramm gilt, z. B. *cmdb_ci_metric_extension*
Diagrammzusammenfassung	Typ der Zusammenfassung, die auf Diagramme mit einer Punktzahl angewendet wird. Die Zusammenfassung kann dem Durchschnitt der Datenpunkte in der Zeitreihe entsprechen. Oder dem Mindest-, Höchst- oder letzten Datenpunkt in der Zeitreihe.
Quellmetriktyp	Metriken wie „% freier Speicherplatz“, die für den CI-Typ überwacht werden
Reihenfolge	Reihenfolge, in der das Metrikdiagramm in allen für die Klasse angegebenen Metrikdiagrammen angezeigt wird. Für eine ordnungsgemäße Darstellung und Ausrichtung werden alle Diagramm für einzelne Punktzahl unabhängig von

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	den Reihenfolgeeinstellungen immer nach Zeitreihendiagrammen angezeigt.
Diagrammtyp	◦ Time_Series: Stellt alle Datenpunkte in der Zeitreihe für die Metrik und das CI des Diagramms dar. ◦ Single_Score: Eine einzelne Zahl, die einer Zusammenfassung der Datenpunkte in der Zeitreihe für die Metrik und das CI des Diagramms entspricht. Die Zusammenfassung wird durch die Einstellung von **Diagrammzusammenfassung** bestimmt.

Statistiken der Eigensystemüberwachung für Metric Intelligence anzeigen

Überwachen Sie den Status von Metric Intelligence-Komponenten und -Prozessen. Verwenden Sie die Seite „Xmlstats“, um Statistiken und Diagnosedetails anzuzeigen, die bei der Behebung von Problemen mit Metric Intelligence helfen können.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Öffnen Sie einen Browser, und geben Sie die URL der Instanz ein.
   Geben Sie ein: `http://<Instanzname>.service-now.com`
2. Hängen Sie den folgenden Text an die URL der Instanz an: `xmlstats.do?include=XMLStatsOI`.
   Das vollständige URL-Format ist: `http://<Instanzname>.service-now.com/xmlstats.do?include=XMLStatsOI`
3. Drücken Sie die Eingabetaste.

Ergebnisse

Details werden zwischen zwei Abschnitten getrennt: Statistiken auf Instanzebene und Statistiken auf Knotenebene. Details im Knotenabschnitt beziehen sich auf den Knoten in der URL.

Knotenabschnitt

Eintrag	Beschreibung
batches_recieved	Die Anzahl der Metrikstapel, die der Knoten vom MID Server erhalten hat
batches_processed	Anzahl der auf dem Knoten verarbeiteten Metrikstapel

Details im Instanzabschnitt beziehen sich auf die gesamte Instanz und zeigen den Status der Selbstintegritätsüberwachung an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Instanzabschnitt

Eintrag	Beschreibung
scheduled_jobs_monitor	Status der Eigensystemüberwachung, die überprüft, ob die wesentlichen regelmäßigen Metric Intelligence-Aufgaben aktiv sind.
distributed_cluster_monitor	Status der Eigensystemüberwachung, die überprüft, ob der verteilte Cluster von Metric Intelligence-MID Servern ordnungsgemäß ausgeführt wird.
oi_extension_monitor	Status der Eigensystemüberwachung, die überprüft, ob die Metric Intelligence-Erweiterung ordnungsgemäß ausgeführt wird.
metrics_collection_monitor	Status der Selbstintegritätsüberwachung, die überprüft, ob Metriken von aktiven Connectors erfasst werden, die für die Metriksammlung konfiguriert sind

Vergewissern Sie sich, dass die Definitionen für Advanced Promotion Engine aktiv sind

Stellen Sie sicher, dass die Advanced Promotion Engine -Definitionen, die mit dem Basissystem geliefert werden, aktiv sind.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Die aktiven Definitionen stufen eine Gruppe von Anomaliewarnungen in die Tabelle „Alle Warnungen“ herauf, wenn alle Bedingungen der Definition erfüllt sind.

Sie können die Bedingungen der im Basissystem enthaltenen Definitionen nicht ändern. Informationen zum Erstellen von anwenderdefinierten Definitionen finden Sie unter Erstellen Sie eine Definition für Advanced Promotion Engine.

Prozedur

1. Navigieren zu **Alle** > **Advanced Promotion Engine** > **Erweiterte Heraufstufungsdefinitionen**.
2. Wählen Sie die Advanced Promotion Engine -Definition aus, die aktiv sein soll:
   - Windows-Server
   - Linux-Server
3. Stellen Sie sicher, dass die Checkbox **Aktiv** aktiviert ist.
4. Wählen Sie **Speichern**.

Erstellen Sie eine Definition für Advanced Promotion Engine

Erstellen Sie eine Definition für Advanced Promotion Engine, damit Sie die Bedingungen für das Heraufstufen der Anomaliewarnungen zu IT-Warnungen definieren können. Durch das Heraufstufen der Warnungen, die die Bedingungen erfüllen, werden nur die relevantesten Warnungen in die Tabelle verschoben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

IT-Warnungen werden in der Express-Liste angezeigt und von einem Operator behandelt.

Nur Metriken, die einer Metrikkonfigurationsregel mit **der Anomaliepunktzahlstufe = Anomaliewarnungen** zugeordnet sind, werden für die Heraufstufung zu IT-Warnungen berücksichtigt. Einzelheiten zu Konfigurationsregeln für Metriken finden Sie unter Metrikkonfigurationsregeln.

Vorbereitungen

Stellen Sie sicher, dass das Plugin Metrikdaten (com.snc.sa.metric) installiert ist.

Erforderliche Rolle: evt_mgmt_admin

Prozedur

1. Navigieren zu **Alle** > **Advanced Promotion Engine** > **Erweiterte Heraufstufungsdefinitionen**.
2. Wählen Sie **Neu**.
3. Geben Sie im Feld **Name** einen beschreibenden Namen für die Definition ein.
4. Legen Sie im Feld **Reihenfolge** die Ausführungsreihenfolge für die Definition fest. Die Definitionen mit einer niedrigeren Reihenfolge werden zuerst ausgeführt.
5. Aktivieren Sie die Definition, indem Sie das Kontrollkästchen **Aktiv** aktivieren.
6. Füllen Sie auf der Registerkarte **CIs** die Felder für die CI-Warnungen aus, die Sie bei der Heraufstufung berücksichtigen möchten.

Registerkartenfelder „CIs“.

Feld	Beschreibung
CI-Klasse	CI-Klassenwarnungen, die in die Tabelle „Alle Warnungen“ hochgestuft werden sollen.
Filter	Filtern Sie, um einzuschränken, für welche CIs diese Definition gilt. Wählen Sie **Neue Kriterien**, um die Bedingungen zu konfigurieren, für die diese Definition gilt. Sie können weitere Bedingungen hinzufügen, indem Sie entweder **ODER** oder **AND**auswählen.
CIs überspringen, die vor weniger als dieser Anzahl von Tagen erstellt wurden	Anzahl der Tage in der Vergangenheit, in denen ein während dieser Zeit erstelltes CI ignoriert wird. Der Wert 7 gibt beispielsweise an, dass CIs, die vor weniger als 7 Tagen erstellt wurden, nicht für die Heraufstufung in die Tabelle „Alle Warnungen“ berücksichtigt werden.

7. Geben Sie auf der Registerkarte **Schweregrad** den Mindestschweregrad der Warnungen ein, die für die Heraufstufung berücksichtigt werden sollen.
   Warnungen mit dem angegebenen Schweregrad und höheren Ebenen werden für die Heraufstufung berücksichtigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Geben Sie auf der Registerkarte **Anzahl der Warnungenim Feld Anzahl der Warnungen für CI** die Mindestanzahl von Warnungen eines CI mit identischem Schweregrad (oder höher) ein, die für die Heraufstufung berücksichtigt werden sollen.
   Der Wert 3 gibt beispielsweise an, dass mindestens drei Warnungen mit dem angegebenen Schweregrad (oder höher) in einem CI vorhanden sein müssen, damit die Warnung für die Heraufstufung berücksichtigt wird.
9. Auf der Registerkarte **Zeitfenster** :
   - Geben Sie im Feld **Warnungen berücksichtigen, die vor mindestens dieser Minutenanzahl aktualisiert wurden** an, wie viele Minuten eine Warnung mindestens alt sein muss, damit sie für die Heraufstufung berücksichtigt wird.

     Wenn der Wert des Felds beispielsweise 5 ist, werden nur Warnungen für die Heraufstufung berücksichtigt, die vor mindestens fünf Minuten aktualisiert wurden.
   - Wählen Sie im blauen Feld den Link „Anzahl der Minuten“ aus, um die Anzahl der Minuten zu ändern, in denen Warnungen für die Heraufstufung berücksichtigt werden sollen.

     Die Seite **„Eigenschaften“** wird geöffnet, und Sie ändern den Wert im Feld **Breite der Zeit....**

     Standard = 30.

   Zum Beispiel:
   - Die aktuelle Uhrzeit ist 10:05 Uhr.
   - Im Feld **Breite der Zeit...** haben Sie einen Wert von 30 eingegeben.
   - Im Feld **Warnungen berücksichtigen, die vor mindestens dieser Minutenanzahl aktualisiert wurden** haben Sie 5 eingegeben.

   Warnungen, die zwischen 9:30 und 10:00 Uhr auftreten, werden für die Heraufstufung berücksichtigt.

Nächste Maßnahme

Stellen Sie sicher, dass eine Metrikkonfigurationsregel vorhanden ist, die Metriken enthält, die zu einer IT-Warnung heraufgestuft werden sollen, und dass die Anomaliepunktzahlebene der Regel **Anomaliewarnungen**lautet. Einzelheiten zum Konfigurieren einer Metrikkonfigurationsregel finden Sie unter Regel für Konfigurationseinstellungen erstellen.

Zeigen Sie die heraufgestuften Ereignisse an

Zeigen Sie die Anomaliewarnungen an, die von Advanced Promotion Engine zu IT-Ereignissen hochgestuft wurden. Durch das Anzeigen von IT-Ereignissen können Sie die Quelle des Ereignisses nachverfolgen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Das System generiert ein IT-Ereignis, wenn eine Anomaliewarnung heraufgestuft wird. Diese Ereignisse werden dann zu IT-Warnungen. Details finden Sie unter Zeigen Sie die heraufgestuften Anomaliewarnungen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Erweiterte Heraufstufungs-Events**.
2. Zeigen Sie auf der Seite Events die IT-Ereignisse an, die von Advanced Promotion Engineaus den Anomaliewarnungen erstellt werden.

Zeigen Sie die heraufgestuften Anomaliewarnungen an

Zeigen Sie die Anomaliewarnungen an, die von Advanced Promotion Engine zu Ereignissen heraufgestuft wurden, die dann in der Tabelle „Alle Warnungen“ als Warnungen verarbeitet werden. Durch das Anzeigen von Warnungen in der Tabelle „Alle Warnungen“ können Sie die Quelle der Warnung nachverfolgen.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_user

Warum und wann dieser Vorgang ausgeführt wird

Die Warnungsgruppierungsfunktion Ereignismanagement verwendet die Anomaliewarnungen, die zu IT-Ereignissen heraufgestuft werden, und gruppiert sie in neue IT-Warnungen.

In der Warnungstabelle werden alle relevanten Probleme im System angezeigt.

Prozedur

1. Navigieren zu **Alle** > **Advanced Promotion Engine** > **Anomaliewarnungen**.
2. Zeigen Sie im Header der Spalte „Is Advanced Heraufgestuft“ die Warnungen mit dem Wert **true**an.
   Die IT-Warnung, die aus der Anomaliewarnung erstellt wird, wird in der Spalte IT-Warnung angezeigt.
3. Wahlweise: Wählen Sie eine Warnung aus, um weitere Informationen über sie zu erhalten. Einzelheiten zu den angezeigten zusätzlichen Informationen finden Sie unter Warnungen in Service Operations-Arbeitsbereich.

Metrikregeln erstellen

Erstellen Sie eine Metrikregel, um die Metrik, die Schwellenwerte und -bereiche sowie den Schweregrad generierter Ereignisse zu bestimmen. Sie können einen Filter hinzufügen, der die Typen von Configuration Items (CI) oder Ressourcen bestimmt, für die Sie Warnungen erhalten. Sie können beispielsweise einen Filter konfigurieren, um Warnungen nur für die Server Windows zu erhalten.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Metrik einen konfigurierten Schwellenwert überschreitet oder in dessen Bereich fällt, erstellt das System ein einzelnes Ereignis, das schließlich zu einer IT-Warnung verarbeitet wird. Der Schweregrad des Ereignisses (und der Warnung) wird durch einen definierten Schwellenwert bestimmt, und das Ereignis ist an ein CI gebunden.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Metriken** > **Metrikregeln**.
2. Wählen Sie **Neue Metrikregel**aus.
   Die **CI-** Auswahlseite wird geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Wählen Sie im Feld CI-Klasse die **CI-Klasse** aus, für die die Regel ausgeführt werden soll. Nur CIs, die Metriken enthalten, können ausgewählt werden.
4. Wahlweise: Wenden Sie einen Filter innerhalb der ausgewählten CI-Klasse an. Wenn Sie beispielsweise die CI-Klasse **Linux-Server**ausgewählt haben, können Sie einen Filter anwenden, um anzugeben, dass die Regel nur für Server gilt, deren Hostname mit einer angegebenen Zeichenfolge beginnt.
5. Wählen Sie **Weiter**.
   Die Seite **Warnungskriterien** wird geöffnet.
6. Wählen Sie die Metrik und die Kriterien aus, um eine Warnung zu erstellen.

   a. Wählen Sie im Feld Warnungsschweregrad den **Warnungsschweregrad** aus, den Sie konfigurieren möchten.
   Wählen Sie aus Folgendem:
   - Kritisch
   - Hoher
   - Geringer
   - Warnung

   b. Wählen Sie im Feld **Metrik** die Metrik aus, auf die der Warnungsschweregrad angewendet werden soll.

   c. Wählen Sie den Vergleichsoperator (ist gleich, ist größer als, ist größer als oder gleich usw.) im Feld **Vergleichsoperator** aus.

   d. Geben Sie einen Wert in das Feld **Wert** ein.

   Sie können beispielsweise Kriterien konfigurieren, um anzugeben, dass eine kritische Warnung generiert wird, wenn die Metrik **node_rx_packets** größer als 10 ist.

   Um zusätzliche Warnungsschweregrade zu definieren, wählen Sie **Weiteren Warnungsschweregrad hinzufügen,** und wiederholen Sie diesen Schritt.

7. Wählen Sie im Abschnitt „ **Warnen, wenn** “ aus, wann die Warnung generiert werden soll.
   Wählen Sie aus Folgendem:
   - **Alle als Stichproben erfassten Werte müssen im folgenden Zeitraum gegen die Kriterien verstoßen**.

     Wählen Sie den Zeitraum in Minuten aus.

   - **Der Durchschnitt der als Stichproben erfassten Werte muss im folgenden Zeitraum gegen die Kriterien verstoßen**.

     Wählen Sie den Zeitraum in Minuten aus.

   - **Jedes Mal, wenn die als Stichproben erfassten Werte gegen die Kriterien verstoßen**.
8. Wählen Sie **Weiter**.
   Die Seite **Name und Aktivierung** wird geöffnet.
9. Überprüfen Sie den Namen und die Details der Metrikregel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Um die Regel zu aktivieren, stellen Sie sicher, dass der Umschalter **Aktiv**

ist aktiviert.

10. Wählen Sie **Fertigstellen** aus.

Ereignisregel zum Binden von Metrikereignissen an Host-CIs erstellen

Erstellen Sie Ereignisregeln, um die Bindung von Metrikereignissen an Host-CIs explizit zuzulassen.

Vorbereitungen
Erforderliche Rolle: evt_mgmt_admin

Warum und wann dieser Vorgang ausgeführt wird
Ab Release London stützt sich Metric Intelligence nicht mehr auf den standardmäßigen Ereignismanagement-Workflow, der Knoten an Host-CIs bindet. Ereignismanagement ist so konfiguriert, dass der standardmäßige Hostbindungsalgorithmus angewendet wird, wenn eine Event-Regel basierend auf Event-Daten keine CIs für die Bindung finden kann. In Metric Intelligence kann mit einer bestimmten Event-Regel und zwei verschiedenen Events eine Situation auftreten, in der ein Event an das richtige CI gebunden wird, ein anderes Event aber nicht. In diesem Fall wird für das ausgewählte CI und das CI auf Hostebene derselbe Metriktyp erstellt, was zu Verwirrung führt.

Beispiel: Mit einer Ereignisregel, die die Prozentsatzmetrik des Datenträgers an einen Speicherdatenträger bindet, kann ein Ereignis ein Datenträger-CI finden, ein anderes Ereignis jedoch nicht. Dies führt dazu, dass die Prozentsatzmetrik des Datenträgers für ein Datenträger-CI und ein Host-CI erstellt wird.

Um diese Verwirrung zu vermeiden, ist die standardmäßige Ereignismanagement-Hostbindung für Metrikereignisse im Basissystem deaktiviert. Um die Hostbindung für Metrikereignisse zuzulassen, erstellen Sie die folgende Ereignisregel explizit im Ereignismanagement Designer für Ereignisregeln. Die zugrunde liegende Bindungsfunktionalität des Designers für Ereignisregeln wird verwendet, um CIs Metriken zuzuordnen.

Prozedur

1. Navigieren zu **Alle** > **Ereignismanagement** > **Regeln** > **Ereignisregeln** um den Ereignisregel-Designer zu öffnen.
2. Klicken Sie auf **Neu**, und stellen Sie sicher, dass der **Aktiv**-Umschalter nach rechts gesetzt ist (Aktiv).
3. Auf der Registerkarte **Ereignisregel-Informationen**:
   a. Legen Sie **Quelle** auf die Datenquelle fest, für die diese Regel gilt.
   b. Wahlweise: Geben Sie eine **Beschreibung** wie `Metriken auf Hostebene binden` ein.
4. Legen Sie auf der Registerkarte **Ereignisfilter** eine Filterbedingung fest, um anzugeben, dass **Klassifizierung** auf **Metrik** gesetzt ist.
5. Klicken Sie auf **Speichern**.

Zugehörige Informationen

Event-Regel erstellen oder bearbeiten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Metrikdaten – Referenz

Referenzthemen enthalten zusätzliche Informationen zu den Einstellungen und Eigenschaften Metrikdaten von .

Einstellungen für den Explorer für Einblicke

Sie können die Einstellungen des Explorers für Einblicke konfigurieren, um z. B. die Aktualisierungshäufigkeit oder die Anzeige zugehöriger Datensätze zu steuern.

Klicken Sie auf das Zahnradsymbol **Einstellungen**, um das Dialogfeld „Anwendungseinstellungen“ zu öffnen.

Einstellung	Beschreibung
Aktualisierungsintervall	Aktivieren Sie die Aktualisierung von Metrikdaten im Explorer für Einblicke bzw. legen Sie die Häufigkeit dafür fest.
Indikatoren	Aktivieren Sie einen beliebigen Indikator, um zugehörige Datensätze wie Incidents oder Probleme für CIs anzuzeigen. Das entsprechende Symbol wird auf der Zeitleiste im Metrikdiagramm angezeigt und gibt die Anzahl der Datensätze für das CI an. Ein Umschalter ist nur verfügbar, wenn das Feld **In Metriken aktiv** im Formular „Kartenindikator“ für die entsprechende Tabelle ausgewählt ist. Beispiel: Der Umschalter **Incident** ist nur verfügbar, wenn **In Metriken aktiv** im Formular „Kartenindikator“ für die Incident-Tabelle [Incident] ausgewählt ist.

Zugehörige Informationen

Dependency Views-Kartenindikatoren

Eigenschaften der Empfindlichkeitsgrenzen für Metriken im Explorer für Einblicke

Die folgenden Eigenschaften können konfiguriert werden, um das Systemverhalten bei der Erkennung sensibler Grenzen für Metriken im Explorer für Einblicke anzupassen. Um Änderungen an den Standardwerten vorzunehmen, navigieren Sie zu **Systemeigenschaften** > **Alle Eigenschaften** und fügen Sie die angegebenen Eigenschaften hinzu (standardmäßig sind sie nicht sichtbar).

Eigenschaften von sensiblen Grenzen

Eigenschaftsname	Beschreibung
sa_metric.sensitive_bounds_calculation_enable	Aktivieren/Deaktivieren Sie die Berechnung sensibler Grenzen. Standardwert: True

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eigenschaften von sensiblen Grenzen (Fortsetzung)

Eigenschaftsname	Beschreibung
sa_metric.sensitive_bounds_percentile	Prozentwert der Berechnung der Empfindlichkeitsgrenzen. Wenn der konfigurierte Prozentsatz der Metrikwerte innerhalb der in der Eigenschaft *sa_metric.sensitive_bounds_sensitivity_factor* angegebenen Anzahl der Standardabweichungen (STDs) liegt, werden sensible Grenzen erkannt und die Empfindlichkeitsberechnung ändert sich auf den in der Eigenschaft *sa_metric.sensitive_bounds_control_factor* angegebenen Wert. Standard: 95 %
sa_metric.sensitive_bounds_control_factor	Anzahl der Standardabweichungen (STDs) vom mittleren Metrikwert, mit denen Metrikgrenzen gemessen werden, nachdem das System sensible Grenzen erkannt hat. Standard: 5,0
sa_metric.sensitive_bounds_sensitivity_factor	Anzahl der Standardabweichungen (STDs) vom mittleren Metrikwert, anhand denen das System auf sensible Grenzen testet. Standard: 2,0

Zugehörige Informationen

Empfindlichkeit der Metrikgrenzen

ITOM-Optimierung

Die Anwendung IT Operations Management (ITOM) Optimization bietet Automatisierung für die Cloud-Workflows, die während ihres gesamten Lebenszyklus zur Verwaltung der Cloud-Ressourcen verwendet werden. Sie ermöglicht eine zertifizierte und unternehmenskonforme Cloud-Bereitstellung, Kostentransparenz und andere Cloud-Managementprozesse.

Funktionen von ITOM-Optimierung

Die Funktionen von ITOM-Optimierung bieten einen integrierten, serviceorientierten Ansatz, der die Qualität von Business Services maximiert, effiziente Prozesse fördert und eine robuste Governance gewährleistet.

Cloud Provisioning and Governance

Die ServiceNow® Cloud Provisioning and Governance (CPG) dient als einheitliche Schnittstelle für den Zugriff auf Cloud-Ressourcen, die Bereitstellung von Cloud-Angeboten für einen Katalog und die Überwachung der Ressourcennutzung. Diese Anwendung wird in die Anwendung Cloud-Services-Katalog umgewandelt, die eine verfeinerte und optimierte Verwaltung der Nutzung und des Lebenszyklus von Cloud-Ressourcen bietet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Workflow-Migration

Alle standardmäßig vordefinierten Workflows wurden mit Flow Designerneu gestaltet.

Richtlinienregelaktionen können jetzt Subflows Flow Designer anstelle von Legacy-Workflows verwenden. Wenn Sie die Standard-Workflows nicht angepasst haben, werden die Legacy-Workflows automatisch zu Subflows migriert. Wenn Sie die Standardworkflows angepasst haben, werden sie nicht migriert, und ihre Anwendungsfälle funktionieren weiterhin mit den vorhandenen Workflows.

Die folgenden Workflows wurden zu Flow Designer Flows oder Subflow migriert:

- Change-Anforderung für Cloud-Vorgang
- Cloud-Aufgabenverarbeitung
- Cloud-Genehmigungs-Workflow
- Nachbearbeitungs-Workflow
- Vorverarbeitungs-Workflow

Die folgenden Workflows sind veraltet:

- Rufen Sie Cloud Billing-Daten ab
- Cloud-Abrechnungsmonat abrufen
- Startprogramm für den Workflow des Cloud-Vorgangsschritts

ITOM-Optimierung Lizenzierung

Bei der für Now Platform® verwendeten Lizenzierungsmethode zahlt Ihre Organisation für die Nutzung von ITOM-Optimierung Anwendungen. Die ServiceNow-Produktdokumentation enthält keine Informationen zu Preisen, Verpackungen oder anderen Details, die durch den Kundenvertrag Ihrer Organisation festgelegt werden. Allgemeine Informationen zu Lizenzierung und Abonnements finden Sie unter ITOM/OT SU-Lizenzierung und -Abonnements.

Guided Setup zum Implementieren der IT Operations Management-Anwendungen

Das Guided Setup von IT Operations Management bietet eine Reihe von Aufgaben, die Sie beim Konfigurieren von IT Operations Management-Anwendungen in Ihrer ServiceNow-Instanz unterstützen. Um das geführte Setup für IT Operations Management zu öffnen, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**. Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Nächste Schritte

Unter Mit aktivierte Plugins ITOM-Optimierung finden Sie die Liste der Plugins, die Sie mit IT Operations Managementaktivieren.

Cloud Provisioning and Governance

Die ServiceNow® Cloud Provisioning and Governance (CPG) dient als einheitliche Schnittstelle für den Zugriff auf Cloud-Ressourcen, die Bereitstellung von Cloud-Angeboten für einen Katalog und die Überwachung der Ressourcennutzung. Diese Anwendung wird in die Anwendung Cloud-Services-Katalog umgewandelt, die eine verfeinerte und optimierte Verwaltung der Nutzung und des Lebenszyklus von Cloud-Ressourcen bietet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance ist sowohl in private als auch in öffentliche Cloud-Anbieter wie Amazon Web Services, Microsoft Azure, Google Cloud Platform und VMware integriert.

Hinweis:

Migration von Workflow zu Subflows:

- Wenn die Standard-Workflows nicht angepasst werden, werden die Flows zu Subflows migriert.
- Wenn die Standard-Workflows angepasst werden, verwenden die Flows weiterhin den vorhandenen Workflow.

Die Cloud Provisioning and Governance-Anwendung ist mit der veralteten Cloud-Management v1-Anwendung nicht kompatibel und kann nicht gleichzeitig mit dieser verwendet werden. Die Anwendung Cloud Provisioning and Governance (früher Cloud-Management) ist ab dem Jakarta-Release kompatibel.

Erkunden	Einrichten	Verwalten
• Yokohama • Domain Separation und Cloud Provisioning and Governance	• Setup-Leitfaden für Tag 1 für Amazon Web Services auf Cloud Provisioning and Governance • Setup-Leitfaden für Tag 1 für Microsoft Azure Cloud auf Cloud Provisioning and Governance • Setup-Leitfaden für Tag 1 für VMware auf Cloud Provisioning and Governance	Cloud Provisioning and Governance-Administrationsleitfaden
Verwenden	**Entwickeln**	**Problembehandlung und Hilfe**
• Cloud-Adminportal • Cloud-Benutzerportal	• Entwicklerschulungen • Entwicklerdokumentation	• Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen • Fragen in der ITOM-Community stellen oder beantworten • Kontakt Kundenservice und Support

Guided Setup zur Implementierung von Cloud Provisioning and Governance verwenden

Das Guided Setup für Cloud Provisioning and Governance stellt eine Reihe von Aufgaben bereit, die Sie bei der Konfiguration von Cloud Provisioning and Governance für Ihre Instanz unterstützen. Um das geführte Setup für Cloud Provisioning and Governance zu öffnen, navigieren Sie zu **Geführtes Setup** > **Geführtes Setup für ITOM**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mehr Informationen zur Nutzung der Anwenderoberfläche des geführten Setups finden Sie unter Geführtes Setup verwenden .

Die Anwendung Cloud Provisioning and Governance anfordern

Die Anwendung Cloud Provisioning and Governance ist als separates Abonnement verfügbar und erfordert das Cloud Provisioning and Governance-Plugin (com.snc.cloud.mgmt).

Vorbereitungen

Erforderliche Rolle: Administrator

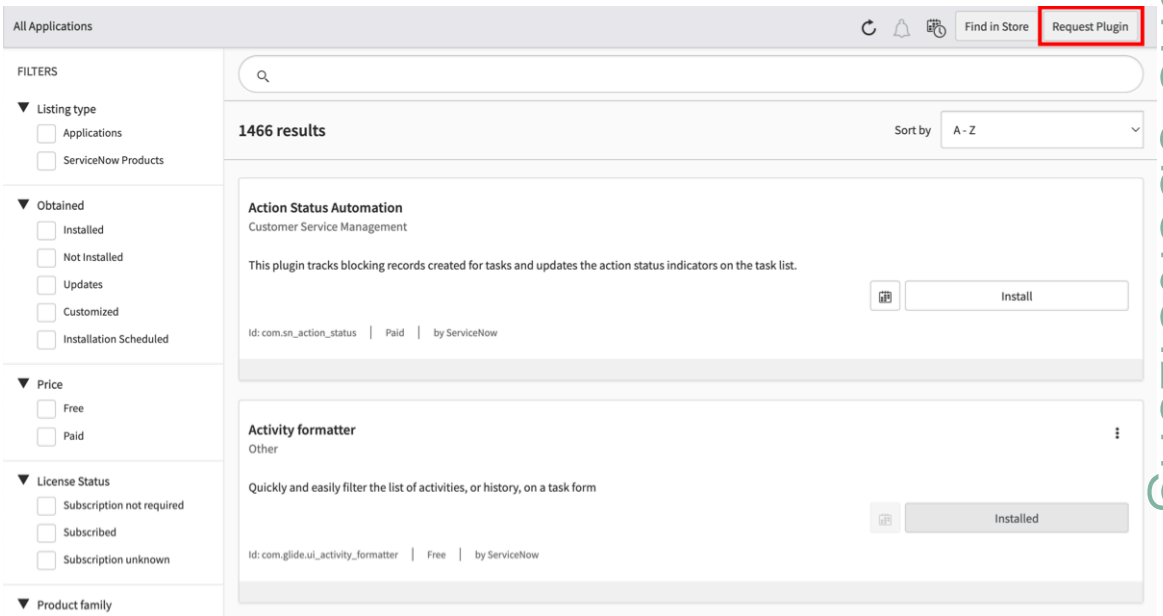
Warum und wann dieser Vorgang ausgeführt wird

Wenden Sie sich an Ihren ServiceNow-Kundenbetreuer, um ein Abonnement zu erwerben. Der Account Manager sorgt im Allgemeinen innerhalb weniger Tage für die Aktivierung des Plugins in der Produktionsinstanz bzw. untergeordneten Produktionsinstanz Ihrer Organisation.

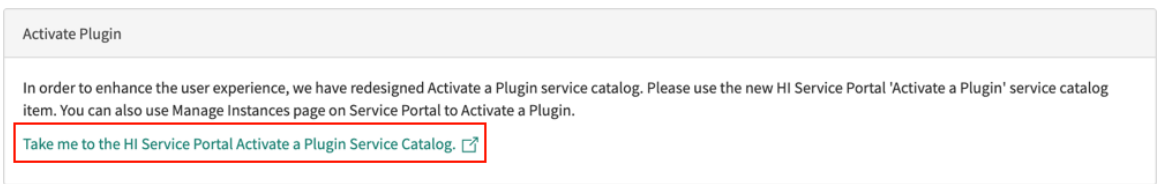
Wenn Sie keinen Account Manager haben, die Aktivierung nach dem Kauf verzögern oder das Produkt in einer Test- und Entwicklungsumgebung kostenlos testen möchten, führen Sie die folgenden Schritte aus.

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.
2. Klicken Sie auf der Seite „Alle Anwendungen“ auf **Plugin anfordern**, um das Formular **Plugin aktivieren** auf Now Support zu öffnen.



3. Wählen Sie unter Now Support den Link aus, um auf Now Support Serviceportal Servicekatalog zuzugreifen.



4. Wählen Sie Ihre Instanz aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie **Aktionen > Plugin aktivieren** aus.
6. Geben Sie im Formular **Plugin aktivieren** die folgenden Informationen an.

Formular „Plugin anfordern“

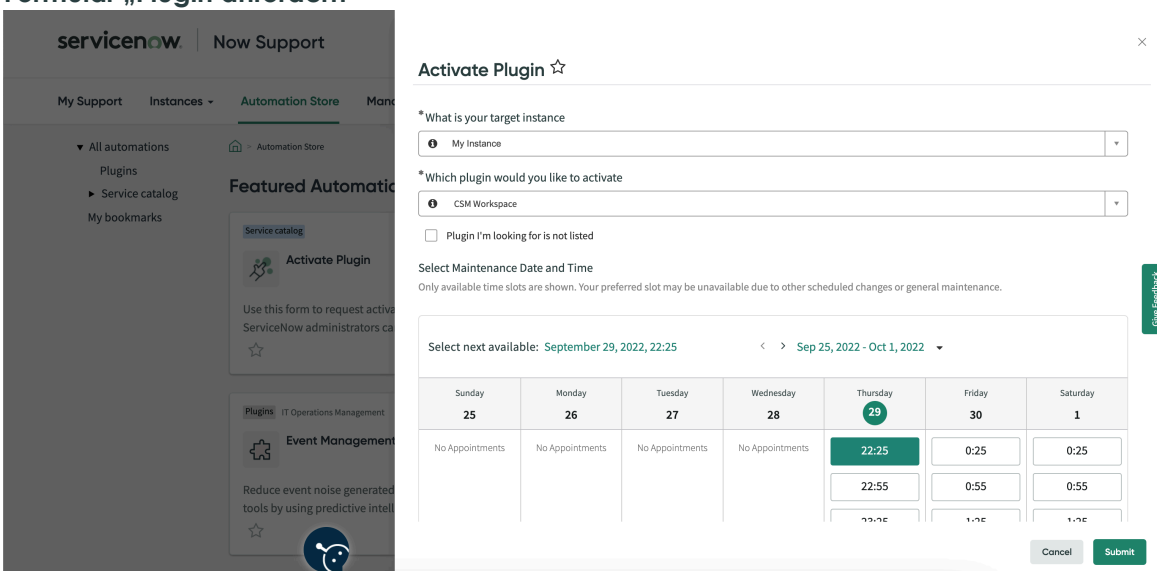
Feld	Beschreibung
What is your target instance (Ihre Zielinstanz)	Instanz, auf der das Plugin aktiviert werden soll.
Which plugin would you like to activate (Welches Plugin möchten Sie aktivieren?)	Name des zu aktivierenden Plugins **Hinweis:** Wenn das System das gewünschte Plugin nicht auflistet oder wenn Sie das Plugin auf einer OEM- oder lokalen Instanz aktivieren, aktivieren Sie das Kontrollkästchen **Plugin I'm looking for is not listed (Gesuchtes Plugin ist nicht aufgelistet)**, und geben Sie dann den Namen des Plugins ein.
Select Maintenance Date and Time (Datum und Uhrzeit der Wartung)	Datum und Uhrzeit zum Aktivieren des Plugins. **Hinweis:** Plugins werden in der pazifischen Zeitzone jeden Werktag in zwei Batches aktiviert, einmal am Morgen und einmal am Abend. Wenn das Plugin zu einem bestimmten Zeitpunkt aktiviert werden muss, geben Sie die Anforderung bei **Grund/ Kommentare** ein.

Example

Betrachten Sie beispielsweise das folgende Formular, um das Plugin „CSM Workspace“ in einer Instanz mit dem Namen „My Instance“ zu aktivieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Plugin anfordern“



7. Wählen Sie **Absenden**.
   Weitere Informationen zum Anfordern eines Plugins finden Sie unter Anfordern eines Plugins aus dem Servicekatalog-Artikel [KB0751715] in Now Support Knowledge Base.

Zugehörige Informationen

- Setup-Leitfaden für Tag 1 für Amazon Web Services auf Cloud Provisioning and Governance
- Setup-Leitfaden für Tag 1 für Microsoft Azure Cloud auf Cloud Provisioning and Governance
- Setup-Leitfaden für Tag 1 für Cloud Provisioning and Governance: Google Cloud Connector
- Setup-Leitfaden für Tag 1 für VMware auf Cloud Provisioning and Governance

Produktnamensänderung

Ab dem Release Paris wurde die Anwendung ServiceNow® Cloud-Management als ServiceNow® Cloud Provisioning and Governancebezeichnet. Die Anwendung wird in Cloud-Services-Katalog eine Anwendung umgewandelt, die eine verbesserte und effiziente Verwaltung der Nutzung und des Lebenszyklus von Cloud-Ressourcen ermöglicht.

Das eigenständige Abonnement für Cloud Provisioning and Governance wird eingestellt. Es wird umstrukturiert und in Cloud Accelerate integriert. Darüber hinaus wurde es in die Bereiche Bewertung der Cloud-Migration, Verwaltung von Cloud-Accounts, Cloud-Services-Katalog, Cloud-Konfiguration und Governance sowie Cloud-Aktionsbibliothek unterteilt.

Obwohl Produktnamenreferenzen in der gesamten Produktdokumentation und der grafischen Benutzeroberfläche (GUI) aktualisiert werden, stoßen Sie möglicherweise je nach Kontext gelegentlich auf Verweise auf ihre alten Namen. Bei einigen Kernkomponenten bleibt der Produktname absichtlich unverändert, um die vorhandene Funktionalität beizubehalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponentennamensmatrix

Komponente	Vorheriger Name	Neuer Name
ITOM-Optimierung > Cloud Provisioning and Governance	Cloud-Management-Anwendung	Cloud Provisioning and Governance-Anwendung
com.snc.cloud.mgmt	Plugin Cloud-Management	Plugin Cloud Provisioning and Governance
com.snc.cloud.core	Cloud-Management Core-Plugin	Cloud Provisioning and Governance Core-Plugin
Anwendungskontext (**Einstellungen** > **Entwickler** > **Anwendung** > **Cloud Provisioning and Governance**)	Cloud-Management	Cloud Provisioning and Governance
com.sn_cmp_ibm	Cloud Management: IBM Cloud Connector	Cloud Provisioning and Governance: IBM Cloud Connector
com.sn_cmp_gcp	Cloud Management: Google Cloud Connector	Cloud Provisioning and Governance: Google Cloud Connector
MID-Server-Fähigkeit > Cloud-Management	MID-Server-Fähigkeit > Cloud-Management	Cloud Provisioning and Governance
Unveränderte Komponentennamen		
MID-Server-Anwendung > Cloud-Management	MID-Server-Anwendung > Cloud-Management	Nicht geändert

Setup-Leitfaden für Tag 1 für Amazon Web Services auf Cloud Provisioning and Governance

Zur Ersteinrichtung von Cloud Provisioning and Governance führen Sie die Schritte in diesem Setupleitfaden für „Tag 1“ durch. Achten Sie darauf, die Schritte in der richtigen Reihenfolge auszuführen. Nachdem Sie das Setup für „Tag 1“ durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration für „Tag 2“ je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Fordern Sie die Anwendung Cloud Provisioning and Governance an

Die Anwendung Cloud Provisioning and Governance ist als separates Abonnement verfügbar und erfordert das Cloud Provisioning and Governance-Plugin (com.snc.cloud.mgmt). Weitere Informationen finden Sie unter Die Anwendung Cloud Provisioning and Governance anfordern.

Zum Einrichten von Cloud Provisioning and Governance erforderliche Rollen

- Für Vorgänge in der AWS-Verwaltungskonsole ist die Administratorrolle erforderlich.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Von Cloud Provisioning and Governance verwendete Begriffe

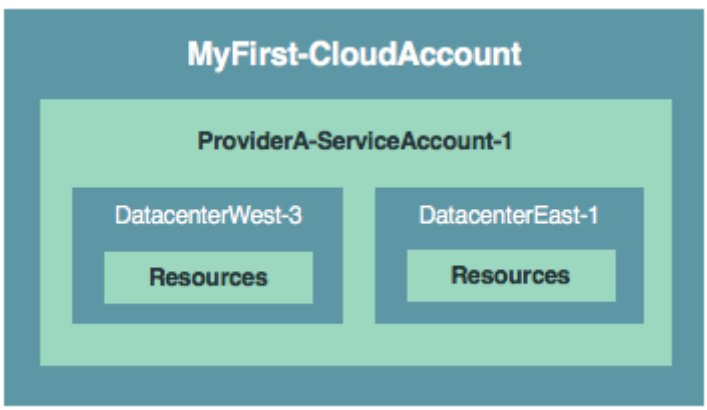
Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet. In AWS werden die bereichsspezifischen Container für virtuelle Ressourcen als Regionen bezeichnet. In Cloud Provisioning werden Regionen als Rechenzentren oder logische Rechenzentren (Logical Datacenters, LDCs) bezeichnet. Der Begriff „logisch“ wird zur Verdeutlichung der Tatsache verwendet, dass Cloud Provisioning anbieterunabhängig ist. Alle Infrastrukturen oder Anwendungen, die mit Cloud Provisioning bereitgestellt werden, sind einem Rechenzentrum zugeordnet.

Schneller Überblick über den Setup-Prozess

Der Setup-Prozess umfasst folgende Aufgaben:

- Falls erforderlich: Die Anwendung Cloud Provisioning and Governance anfordern.
- Weisen Sie Cloud-Benutzern die entsprechenden Rollen zu.
- Richten Sie die MID Servers für die sichere Kommunikation mit den Provider-API-Endpunkten ein.
- Erfassen Sie im Provider-Portal Ihre Kontoeinstellungen und die Anmeldeinformationen, die beim Discovery-Prozess (über einen MID-Server) dazu verwendet werden, programmgesteuert auf Ihre Provider-Konten zuzugreifen. Ordnen Sie die Kontoeinstellungen und Anmeldeinformationen sicher einem Servicekonto in Cloud Provisioning and Governance zu.
- Richten Sie ein Cloud-Konto ein, um Ihre gesamte verwaltete Cloud-Infrastruktur darzustellen, und richten Sie ein Servicekonto ein, das mit einem Ihrer Provider-Konten funktioniert. Sie geben an, welche Rechenzentren im Servicekonto in das Cloud-Konto aufgenommen werden sollen. (Später, am „Tag 2“, können Sie zusätzliche Cloud-Accounts und Servicekonten vom selben Provider oder anderen Providern einrichten.)
- In Cloud Provisioning werden CMDB-Daten dafür verwendet, Benutzer beim Anfordern und Verwalten von Cloud-Ressourcen und beim Verwalten der Cloud-Infrastruktur zu unterstützen. Zum Füllen der CMDB mit Ressourcendaten für alle Rechenzentren führen Sie den Discovery-Prozess manuell für jedes im Servicekonto enthaltene Rechenzentrum aus. Anschließend konfigurieren Sie Discovery so, dass die Anwendung regelmäßig ausgeführt wird und somit die kontinuierliche Aktualisierung der Daten sichergestellt ist. Ihr Cloud-Konto könnte wie folgt aussehen:

Struktur eines Cloud-Kontos an Tag 1



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Provider bieten Services, mit denen die CMDB automatisch aktualisiert werden kann, wenn für eine Ressource ein Lebenszyklus-Change (erstellt/geändert/beendet) oder Konfigurations-Update durchgeführt wird. Sie können den Service für die direkte Integration mit Cloud Provisioning and Governance konfigurieren.

Aktionen zur Integration von Cloud Provisioning and Governance in Ihre AWS-Konten

Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

1. Weisen Sie AWS Anwendern von Rollen zu Cloud Provisioning and Governance

   Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

2. Installieren und konfigurieren Sie MID Servers für den Zugriff auf Cloud-Umgebungen

   Damit eine sichere und zuverlässige Kommunikation gewährleistet ist, findet eine Kommunikation zwischen dem Discovery-Prozess und Ihren Cloud Provider-Konten und Cloud-Ressourcen über mindestens einen MID Servers statt. Sie können MID Servers in Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke einrichten. Sie können den MID-Server für Cloud Provisioning and Governance für die Verwendung eines Proxy-Servers konfigurieren. Durch die Verwendung eines Proxy-Servers werden alle cloudbasierten Aktivitäten wie Ausführen von Discovery, Abrechnungsdownloads, Bereitstellen virtueller Computer und Ausführen von Lebenszyklusvorgängen auf virtuellen Computern unterstützt.

   Hinweis: Daten werden bei der Übertragung zum MID-Server und zwischen dem MID-Server und dem API-Endpunkt verschlüsselt. Um hohe Leistung und Sicherheit zu gewährleisten, sollten Sie mindestens einen MID-Server für jedes verwaltete Rechenzentrum konfigurieren. Konfigurieren Sie einen MID-Server, auch wenn Sie bereits andere MID Servers beim Einrichten von Cloud Provisioning and Governance für einen anderen Cloud Provider konfiguriert haben.

3. Zugriff auf AWS-Konten mit permanenten AWS-Anmeldeinformationen konfigurieren

   Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Damit die Anmeldeinformationen für Discovery und Cloud Provisioning and Governance verfügbar sind, müssen Sie in der AWS-Verwaltungskonsole zunächst einen Benutzer mit programmgesteuertem Zugriff erstellen. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Now Platform.

4. Erstellen Sie AWS GovCloud-Anmeldeinformationen für Cloud Provisioning and Governance

   Hinweis: Überspringen Sie dieses Verfahren, wenn Ihre Organisation AWS GovCloud (US) nicht verwendet.

   Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Eine AWS GovCloud (US)-Region ist eine isolierte AWS-Region, die die strengen Sicherheits- und Complianceanforderungen der US-Regierung zum Hosten sensibler Arbeitsauslastungen erfüllt. Cloud Provisioning and Governance bietet Unterstützung für alle AWS GovCloud (US)-Services.

5. Servicekonten für AWS GovCloud erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Überspringen Sie dieses Verfahren, wenn Ihre Organisation AWS GovCloud (US) nicht verwendet.

Wenn Ihr Unternehmen AWS GovCloud (US)-Regionen verwendet, erstellen Sie ein Servicekonto für jede Region. Diese von Ihnen erstellten Anmeldeinformationen werden für Cloud-Discovery, Cloud Provisioning and Governance und Cloud-Einblicke verwendet.

6. Richten Sie Cloud-Konto und Servicekonto für ein AWS

   Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

8. Zeitplan für das Herunterladen von AWS-Abrechnungsdaten definieren

   Definieren Sie den geplanten Auftrag, mit dem unter Verwendung eines MID-Servers regelmäßig Abrechnungsdaten vom Provider heruntergeladen werden. Von Cloud Provisioning and Governance werden die Daten in einer Kostentabelle gespeichert und die Informationen zum Erstellen von Berichten verwendet.

Nächste Schritte

Wenn Sie alle Verfahren für „Tag 1“ und „Tag 2“ in diesem Setupleitfaden abgeschlossen haben, finden Sie unter Cloud Provisioning and Governance-Administrationsleitfaden weitere Informationen zur Verwendung der Anwendung Cloud Provisioning and Governance in Ihrem Unternehmen.

Weisen Sie AWS Anwendern von Rollen zu Cloud Provisioning and Governance

Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

Vorbereitungen

Erforderliche Rolle: user_admin oder admin

Prozedur

Weisen Sie Gruppen und Benutzern nach Bedarf die folgenden Rollen zu:

Beschreibender Name und Rollenname	**Beschreibung und Aufgaben**	**Zugriffsberechtigungen in** Cloud Provisioning and Governance
Root-Administrator `[sn_cmp.cmp_root_admin]`	Höchste Anwendungszugriffsebene für Cloud Provisioning and Governance.	Alle
Cloud-Administrator `[sn_cmp.cloud_admin]`	Konfiguriert die Cloud Provisioning and Governance-Anwendung	Cloud-Infrastruktur:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	**Beschreibung und Aufgaben**	**Zugriffsberechtigungen in** Cloud Provisioning and Governance
	und richtet die Cloud-Infrastruktur ein.	Servicekonten und Cloud-Konto Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • IBM Cloud-Update • VMware-Events
Kontrolle `[sn_cmp.cloud_governor]`	Überwacht die gesamte Cloud-Nutzung und setzt die Einhaltung der Regeln, Kontingente und Richtlinien der Organisation durch. Verwaltet auch Tags und Berechtigungen für verschiedene Objekte.	Governance: • Richtlinien • Pools • Kontingente • Berechtigungen
Service Designer `[sn.cmp.cloud_service_designer]`	Erstellt Blaupausen, ARM- und CloudFormation-Vorlagen und Katalogelemente.	Cloud-Servicedesign: • Cloud-Vorlagen • Blaupausen • Blaupausenkatalogelemente • Ressourcenblöcke
Cloud-Benutzer `[sn_cmp.cloud_service_user]`	Fordert Stapel und Ressourcen an und verwaltet sie.	Cloudbenutzerportal. Wenn Sie die Rolle einer Gruppe zuweisen, teilen sich alle Mitglieder der Gruppe die Kontingentbeschränkungen und den Besitz bestimmter Ressourcen. Sie können auf alle Aufgabendatensätze zugreifen, die Ihnen oder anderen zugewiesen sind, wenn Sie die Rolle „Cloud-Service-Benutzer“ innehaben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	**Beschreibung und Aufgaben**	**Zugriffsberechtigungen in** Cloud Provisioning and Governance
Cloud-Betreiber `[sn_cmp.cloud_operator]`	Überwacht die Cloud Provisioning and Governance-Anwendung und behebt Probleme damit.	Dashboards und Berichte: • Dashboard für Cloud-Vorgänge • Cloud-Ursachenanalyse • Cloud-Orchestrierungspfad • Cloud-API-Pfad
Cloud-Event-Integration `[sn_cmp.cloud_event_integration]` **Hinweis:** Von IBM Cloud Connector nicht unterstützt	Autorisiert den Zugriff auf die Instanz für externe Services, mit denen die CMDB bei Auftreten von Cloud-Events automatisch aktualisiert wird. Diese Rolle gewährt den Zugriff auf den REST-Endpunkt des Cloud Events.	Cloud-Infrastruktur: • Servicekonten und Cloud-Konto • Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • VMware-Events
Cloud-Gruppenadministrator `[sn_cmp.cloud_group_admin]`	Gewährt Administrator-Zugriff für alle Gruppen, denen Sie angehören.	

Zugehörige Informationen

Einer Gruppe eine Rolle zuweisen

Einem Benutzer eine Rolle zuweisen

Richten Sie Cloud-Konto und Servicekonto für ein AWS

Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Vorbereitungen

Erforderliche Rolle: keine

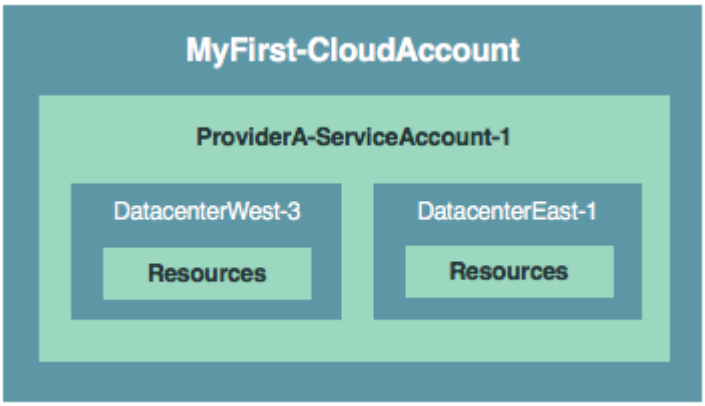
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Für Vorgänge in der AWS-Verwaltungskonsole ist die Administratorrolle erforderlich.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie das Setup für „Tag 1“ abgeschlossen haben, sieht Ihr Cloud-Konto möglicherweise so aus:

Struktur eines Cloud-Kontos an Tag 1



Prozedur

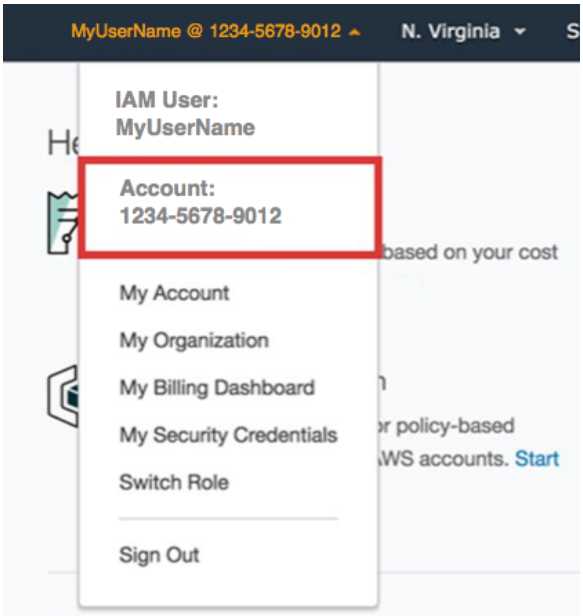
1. Navigieren Sie im Cloud-Adminportal zu **Verwalten** > **Cloud-Accounts**.
2. Wählen Sie das Cloud-Konto aus, oder erstellen Sie es:
   - Wählen Sie ein vorhandenes Cloud-Konto aus:
     a. Klicken Sie auf der Seite des Cloud-Kontos auf **Konfigurieren**.
     b. Klicken Sie auf der Seite „Allgemeine Informationen“ auf **Weiter**, und fahren Sie dann mit dem nächsten Schritt fort.
   - Cloud-Konto erstellen:
     a. Klicken Sie auf der Seite „Allgemeine Informationen“ auf **Neu**, und geben Sie dann einen eindeutigen und aussagekräftigen **Namen** und eine **Beschreibung** für das Cloud-Konto ein.
     b. Provider auswählen.
     c. Klicken Sie auf **Weiter**, und fahren Sie dann mit dem nächsten Schritt fort.
3. Erstellen Sie auf der Seite „Rechenzentren“ ein Servicekonto: Klicken Sie neben dem Feld **Servicekonto** auf das **+**, und füllen Sie dann das Formular für Servicekonto aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für dieses Servicekonto.
Account-ID	12-stellige Nummer des Benutzerkontos. Erweitern Sie die Liste unter dem AWS-Kontonamen in der AWS-Verwaltungskonsole, um die Nummer anzuzeigen. **Wichtig:** Entfernen Sie im Feld **Konto-ID** die Bindestriche (-) aus der Nummer.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Nummer des IAM-Benutzerkontos 
Discovery-Anmeldeinformationen	Anmeldeinformationen, die für ServiceNow-Anwendungen für den Zugriff auf dieses Konto erforderlich sind. Sie können dieses Feld zu einem späteren Zeitpunkt konfigurieren, während Sie den Zugriff auf AWS-Konten konfigurieren. ◦ Wenn Sie hat die AWS-Anmeldeinformationen unter konfiguriert Now Platform , wählen Sie das Lupensymbol und dann den Namen der entsprechenden AWS -Anmeldeinformationen aus. ◦ Um andere AWS-Konten für den Zugriff auf diesen Account zu verwenden, lassen Sie das Feld leer. Beispielsweise müssen Sie die AWS-Anmeldeinformationen nicht für Konten angeben, die IAM-Rollen oder Mitgliedskonten annehmen und ihr Verwaltungskonto für den Zugriff verwenden.
Rechenzentrums-URL	URL des Rechenzentrums. Dieses Feld ist für die Konten AWS Region China und AWS GovCloud (US) erforderlich. Zum Beispiel: ◦ AWS Region China: `https://organizations.cn-northwest-1.amazonaws.com.cn` ◦ AWS GovCloud (USA): `https://aws.amazon.com/ec2/`
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie das **AWS-Rechenzentrum**.
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übergeordneter Account	Name des Verwaltungskontos, das die Organisation in AWS darstellt, zu der dieses Mitgliedskonto gehört. Dieser Name wird angezeigt, wenn Sie **AWS-Rechenzentrum** auswählen. Wenn dieses Konto nicht Teil einer AWS-Organisation ist, lassen Sie dieses Feld leer.
Ist Master-Konto	Kennzeichnung des Verwaltungskontos. Sie wird angezeigt, wenn Sie in der Dropdown-Liste „Rechenzentrumstyp“ die Option **AWS-Rechenzentrum** auswählen. Aktivieren Sie das Kontrollkästchen, um das AWS-Servicekonto dem Verwaltungskonto zuzuordnen. Aktivieren Sie dieses Kontrollkästchen nur für Konten, die Sie zuvor in der AWS-Verwaltungskonsole als Verwaltungskonten konfiguriert haben und zu denen einige Mitgliedskonten gehören. In der AWS-Dokumentation finden Sie weitere Informationen zu AWS-Organisationen. **Hinweis:** Sie müssen die richtige Berechtigung in AWS oder der Organisationsrolle für Standardanmeldeinformationen einrichten. Weitere Informationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern.
Account des Zugriffsberechtigten	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, bei denen keine permanenten AWS-Anmeldeinformationen verwendet werden und bei denen IAM-Rollen für den Zugriff genutzt werden.

4. Klicken Sie auf **Absenden**, um das Servicekonto zu erstellen.
5. Klicken Sie auf **Rechenzentren erkennen**
6. Wenn die Rechenzentren angezeigt werden, wählen Sie die Rechenzentren aus, die in das Cloud-Konto einbezogen werden sollen, und klicken anschließend auf **Speichern**.

Hinweis:

- Wählen Sie nur die LDCs/Regionen aus, in denen Ihre Infrastrukturressourcen vorhanden sind. Wenn Sie in diesen neuen Rechenzentren nicht über Ressourcen verfügen, schließen Sie diese aus, während Sie die vollständige Erkennung durchführen.
- Um Ressourcen in Regionen/LDCs wie Nordamerika (USA Ost, USA West und Zentralkanada), Südamerika, Europa, Afrika, Naher Osten und Asien-Pazifik zu erkennen, lösen Sie eine Zugriffsanforderung auf die erforderlichen Endpunkte beim GCP Support aus.

Das Dashboard „Cloud-Konto“ wird angezeigt. Die ausgewählten Rechenzentren werden auf der Registerkarte **Rechenzentren** angezeigt.

7. Klicken Sie auf ein Rechenzentrum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die folgenden Listen werden angezeigt:

- **Ressourcen**: Cloud-Ressourcen für das aktuelle Rechenzentrum. Führen Sie Discovery aus, um die CMDB für das Rechenzentrum und die Registerkarte auszufüllen. Weitere Informationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
- **Kapazitätsgrenzen**: Grenzwerte für virtuelle CPUs, virtuelle Netzwerke, Speicher-Volume-Größe und andere Services. Weitere Informationen finden Sie unter Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen.
- **Discovery-Protokoll**: Mit dem Prozess wird ein Protokolldatensatz für jede Aktion im Zusammenhang mit einem Discovery-Status erstellt.

Nächste Maßnahme

- Konfigurieren Sie zusätzliche Berechtigungen zum Bereitstellen von Amazon AWS Cloud-Ressourcen mit Cloud Provisioning and Governance.
- Nachdem Sie alle Verfahren in dieser Ersteinrichtung für „Tag 1“ abgeschlossen haben, können Sie zusätzliche Cloud-Accounts und Servicekonten erstellen, um Ihre Cloud-Infrastruktur zu organisieren und aufzuteilen.

Zugehörige Informationen

Zusätzliches Cloud-Konto einrichten

Fügen Sie ein AWS Servicekonto zu hinzu Cloud-Konto

Amazon AWS Cloud Discovery

Benutzerdefinierte AWS-Mitgliedsrolle konfigurieren

Passen Sie die AWS-Rollen an, die ein MID Server annehmen kann, um temporäre Anmeldeinformationen für Mitgliedskonten zu erhalten. Sie können zusätzliche Parameter konfigurieren, um die Sicherheit zu verbessern und um anzupassen, wie die Rolle des Mitgliedskontos angenommen wird, wenn Cloud-Ressourcen erkannt werden.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

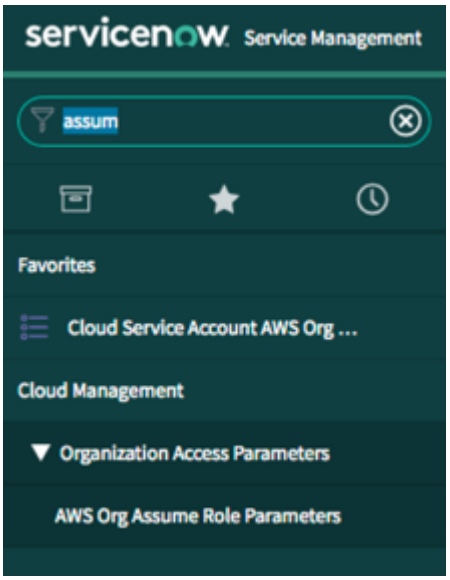
Werte, die Sie in der Tabelle „Cloud-Servicekonto > AWS-Org. - Parameter für Rollenübernahme“ [cloud_service_account_aws_org_assume_role_params] eingeben, werden als Parameter für das Konto des benannten Services an die AWS AssumeRole API weitergegeben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Zugriffsparameter der Organisation** > **AWS-Org. – Parameter für Rollenübernahme**.



2. Klicken Sie auf **Neu**, und füllen Sie dann das Formular mit diesen Parametern aus:

Feld	Beschreibung
Zugriffsrollenname [access_role_name]	Name der AWS-Rolle im Mitgliedskonto, die vom Verwaltungskonto zum Abrufen temporärer Anmeldeinformationen verwendet wird. Standard: OrganizationAccountAccessRole
Rollensitzungsname [role_session_name]	Name für die Sitzung unter Verwendung der temporären Sicherheitsanmeldeinformationen, der dazu beitragen kann, die Verwendung einer Rolle nach einem Prinzipal oder Zweck zu unterscheiden. Dieser Sitzungsname ist in den AWS Cloud Trail-Protokollen sichtbar. Weitere Informationen finden Sie unter Cloud-API-Pfad und in der AWS-Dokumentation zu AWS Cloud Trail. Standard: Master_account_id__<management account ID number> Ein Beispiel hierfür ist: `Master_account_id__321003876149`.
Anmeldeinformations-TTL in Sekunden [credential_ttl_seconds]	Gültigkeitsdauer der temporären Sicherheitsanmeldeinformationen in Sekunden. Standard: Wird wie folgt berechnet: **a.** Rufen Sie den Wert in der *mid.aws.sts.assume_role.credential_ttl_minutes* Eigenschaft „MID-Server“ ab. **b.** Beschränken Sie diesen Wert auf einen Wert zwischen 15 und 720 Minuten. Wenn die Einstellung in der Eigenschaft weniger als 15 Minuten beträgt, werden vom System 15 Minuten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	eingegeben. Wenn die Einstellung größer als 720 Minuten ist, werden vom System 720 Minuten eingegeben. **c.** Konvertieren Sie den resultierenden Wert in Sekunden.
Externe ID [external_id]	Ein eindeutiger Bezeichner, der für die Vertrauensrichtlinie der angenommenen Rolle erforderlich ist. Standard: ServiceNow_MID_Server
Sitzungsrichtlinie [session_policy]	IAM-Richtlinie im JSON-Format, die die Berechtigungen der temporären Sicherheitsanmeldeinformationen über die von der Rolle konfigurierte Richtlinie hinaus weiter einschränkt. (JSON in der AWS-Richtliniensprache.) Standard: leer
MFA [multifactor authentication]	Seriennummer des MFA-Geräts (Hardware oder virtuell), das zur Authentifizierung des Verwaltungskontos verwendet wird. Standard: leer
MFA-Tokencode [mfa_token_code]	Vom MFA-Gerät (Hardware oder virtuell), das zur Authentifizierung des Verwaltungskontos verwendet wird, bereitgestellter Tokencode. Standard: leer
Cloud-Servicekonto [cloud_service_account]	Erforderlich. Servicekonto, der den Zugriffsparametern zugeordnet werden soll, die Sie an die AWS AssumeRole API übergeben. Geben Sie eine Konto-ID (entweder ein Verwaltungskonto oder ein Mitgliedskonto) aus der Tabelle „Servicekonten“ [cmdb_ci_cloud_service_account] ein.

Hinweis: Weitere Informationen zur Verwendung dieser Parameter und zu ihrer Bedeutung finden Sie in der AWS-Dokumentation zur AWS Security Token Service API für die Aktion „AssumeRole“.

Erstellen Sie AWS GovCloud-Anmeldeinformationen für Cloud Provisioning and Governance

Überspringen Sie dieses Verfahren, wenn Ihre Organisation AWS GovCloud (US) nicht verwendet. Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Eine AWS GovCloud (US)-Region ist eine isolierte AWS-Region, die die strengen Sicherheits- und Complianceanforderungen der US-Regierung zum Hosten sensibler Arbeitsauslastungen erfüllt. Cloud Provisioning and Governance bietet Unterstützung für alle AWS GovCloud (US)-Services.

Vorbereitungen

Hinweis:

- ServiceNow® ITOM-Produkte werden für die Regionen Deutschland und China nicht offiziell zertifiziert oder unterstützt.
- Überspringen Sie dieses Verfahren, wenn Ihre Organisation AWS GovCloud (US) nicht verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Sie benötigen die AWS GovCloud (US)-Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel, den Sie auf der AWS-Verwaltungskonsole generiert haben.

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Cloud Provisioning and Governance greift auf GovCloud Regionen mit einem Satz von Anmeldeinformationen für jede Region zu. Zur Konfiguration von Cloud Provisioning and Governance zur Unterstützung einer GovCloud-Region erstellen Sie ein AWS-Standardkonto für jede Region (erforderlich für die Abrechnung), rufen die Anmeldeinformationen für das Konto ab und erstellen dann einen Servicekonto für die Region. Weitere Informationen zur Abrechnung finden Sie auf der Seite zur Abrechnung und Zahlung bei AWS GovCloud (US) in der AWS-Dokumentation .

Prozedur

1. Geben Sie in der AWS-Verwaltungskonsole im Suchfeld `AWS-Services` **IAM** ein, um den Identitäts- und Zugriffsverwaltungsservice (Identity and Access Management, IAM) zu öffnen.
2. Klicken Sie im IAM-Ressourcenportal auf **Benutzer**.
3. Erstellen Sie den Discovery-Benutzer, der über programmgesteuerten Zugriff auf Ihre AWS GovCloud (US)-Ressourcen und -Abrechnungsdaten verfügt.
4. Wählen Sie **Anwender hinzufügen** aus.
   Konfigurieren Sie auf der Seite „Details“ die Benutzereinstellungen, und klicken Sie dann auf **Weiter**.

Anwendername	Name für den Benutzer mit programmgesteuertem Zugriff, z. B. `servicenowcloud`.
Zugriffstyp	Wählen Sie **Programmatic access** (Programmgesteuerter Zugriff) aus.

5. Fügen Sie auf der Seite „Berechtigungen“ den Benutzer einer Richtlinie hinzu, indem Sie die folgenden Einstellungen konfigurieren, und klicken Sie dann auf **Weiter**.

Berechtigungen für <Benutzername> festlegen	Wählen Sie **Attach existing policies directly** (Vorhandene Richtlinien direkt anhängen) aus.
Attach one or more policies … (Mindestens eine Richtlinie anhängen …)	Wählen Sie die entsprechende Richtlinie aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Die Richtlinie **AdministratorAccess** hat die umfassendste Berechtigungsstufe, einschließlich der Berechtigung zum Bereitstellen von Cloud-Ressourcen. Die Richtlinie ermöglicht den gleichen Zugriff, der der Instanz gewährt würde, wenn Sie nicht IAM, sondern die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel Ihres AWS-Kontos verwenden würden. Sie können stattdessen eine Richtlinie erstellen oder mehrere Richtlinien kombinieren, um die entsprechende Berechtigungsstufe zu gewähren. Weitere Detailinformationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern.

6. Überprüfen Sie auf der Überprüfungsseite Ihre Auswahl, und klicken Sie dann auf **Create user** (Benutzer erstellen).
7. Führen Sie auf der Abschlussseite zwei Schritte aus:

   Hinweis: Verlassen Sie die Seite erst, wenn Sie beide Schritte abgeschlossen haben. Der Wert des **geheimen Zugriffsschlüssels** wird nicht erneut angezeigt. Fügen Sie die in diesen Schritten generierten Werte in ein Cloud Provisioning and Governance-Formular ein.

   a. Klicken Sie auf **Show** (Anzeigen), um den geheimen Zugriffsschlüssel anzuzeigen. Kopieren Sie den Wert.
   b. Klicken Sie auf **Download .csv** (.csv herunterladen), um die Datei, die den Benutzernamen, die Zugriffsschlüssel-ID und den Wert des geheimen Zugriffsschlüssels enthält, im CSV-Format zu speichern. Erstellen Sie die Datei als Sicherung für den Fall, dass Sie die Werte verlieren. Stellen Sie sicher, dass die Datei erstellt wurde, und speichern Sie sie dann sicher.
8. Navigieren Sie in Ihrer -Instanz zu **Orchestration** > **Anmeldeinformationen und Verbindungen** > **Anmeldeinformationen**.
9. Klicken Sie auf **Neu**, wählen Sie **AWS-Anmeldeinformationen** aus, geben Sie einen eindeutigen und aussagekräftigen **Namen** ein (z. B. `AWS GovCloud Creds 01`), und füllen Sie dann das Formular aus.

Formularfelder mit AWS-Anmeldeinformationen

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen.
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Eingabewert
Zugangsschlüssel-ID	Die **Zugriffsschlüssel-ID**, die Sie in der AWS-Verwaltungskonsole generiert haben, z. B: APIAIOSFODNN7BEISPIEL.
Geheimer Zugangsschlüssel	Der **geheime Zugriffsschlüssel**, den Sie in der AWS-Verwaltungskonsole generiert haben, z. B.: wPalrXUtnFEMI/K7MDENG/bPxRfiCYBEISPIELSCHLÜSSEL.

10. Klicken Sie auf **Absenden**.
    Die Instanz zeichnet die Anmeldeinformationen auf. Als Nächstes können Sie einen Servicekonten für AWS GovCloud erstellen.

Servicekonten für AWS GovCloud erstellen

Wenn Ihr Unternehmen AWS GovCloud (US)-Regionen verwendet, erstellen Sie ein Servicekonto für jede Region. Diese von Ihnen erstellten Anmeldeinformationen werden für Cloud-Discovery, Cloud Provisioning and Governance und Cloud-Einblicke verwendet.

Vorbereitungen

Hinweis: Überspringen Sie dieses Verfahren, wenn Ihre Organisation AWS GovCloud (US) nicht verwendet.

- Erforderliche Rolle: sn_cmp.cloud_admin
- AWS GovCloud (US)-Anmeldeinformationen für jede GovCloud-Region.
- AWS GovCloud (US)-Konto-ID (über die AWS-Verwaltungskonsole).

Warum und wann dieser Vorgang ausgeführt wird

Ein Servicekonto enthält die Anmeldeinformationen und Kontoinformationen, die Sie in Ihrem Provider-Konto erstellt haben. Discovery verwendet die Informationen, um auf Ihren Provider-Konto zuzugreifen und dann Informationen zu jedem logischen Rechenzentrum abzurufen, das dem Konto zugeordnet ist.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal** > **Service-Accounts**.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und `aussagekräftigen` Namen für das Konto ein (z. B. AWS GovCloud SA O1), und füllen Sie dann das Formular „Cloud-Servicekonto“ aus.

Feld	Beschreibung
Konto-ID	Konto-ID, zu der die Anmeldeinformationen gehören.
Discovery-Anmeldeinformationen	Wählen Sie den Namen der Anmeldeinformationen aus, die Sie unter Erstellen Sie AWS GovCloud-Anmeldeinformationen für Cloud Provisioning and Governance erstellt haben. Im Beispiel haben Sie den Namen `AWS GovCloud Creds O1` verwendet.
Rechenzentrums-URL	URL des Rechenzentrums. Beispiel: https://aws.amazon.com/ec2/

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Rechenzentrumstyp	Wählen Sie die CMDB-Tabelle aus, die für den Typ des Rechenzentrums steht. Beispiel: Tabelle [cmdb_ci_aws_datacenter]
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.

3. Klicken Sie auf **Aktualisieren** oder **Absenden**.
   Das Servicekonto wird vom System erstellt, und es wird die Liste aller erkannten Rechenzentren angezeigt.

Nächste Maßnahme

Wiederholen Sie den Vorgang, um nach Bedarf weitere Servicekonten zu erstellen. Führen Sie Discovery für jedes Rechenzentrum aus.

Zeitplan für das Herunterladen von AWS-Abrechnungsdaten definieren

Definieren Sie den geplanten Auftrag, mit dem unter Verwendung eines MID-Servers regelmäßig Abrechnungsdaten vom Provider heruntergeladen werden. Von Cloud Provisioning and Governance werden die Daten in einer Kostentabelle gespeichert und die Informationen zum Erstellen von Berichten verwendet.

Vorbereitungen

Wichtig:

Ab dem Vancouver-Release ist das Abrechnungs-Dashboard nicht mehr verfügbar, wenn Sie die ServiceNow Store Cloud-Kostenmanagement-App heruntergeladen und aktiviert haben. Die folgenden Changes finden statt:

- Sie werden standardmäßig zur Startseite von Cloud-Kostenmanagement weitergeleitet.
- Das Widget „Dashboard anzeigen“ im Cloud-Benutzerportal wird durch das Widget „Ressourcen anzeigen“ ersetzt.
- Das Widget „Aktuelle Monatsausgaben“ und das Widget „Budget“ im Cloud-Benutzerportal zeigen keine Daten an, wenn das Cloud-Kostenmanagement in der Instanz aktiviert ist.

Wenn Sie die App „Cloud-Kostenmanagement“ aktiviert haben, können Sie nur dann zum Abrechnungs-Dashboard navigieren, wenn Sie Cloud Provisioning and Governance in einer domänengetrennten Instanz verwenden.

- Richten Sie ein Bezahlkonto ein, der die Abrechnungsinformationen für alle verknüpften Konten empfängt.
- Erstellen Sie den Amazon S3-Bucket, der den Datenspeicherbereich für die täglichen detaillierten Abrechnungsdatensätze im AWS-Konto darstellt. Die Anmeldeinformationen, die für den Zugriff auf den Bericht verwendet werden, müssen über Berechtigungen für den S3-Bucket verfügen. Legen Sie den S3-Bucket basierend auf dem Auftragsstandort fest. Die `AssumeRole`-Richtlinien MÜSSEN eine S3-Zugriffsrichtlinie enthalten. Unter Umständen sind Sie der Meinung, dass von dem AWS-Konto, das Sie immer verwenden, ein S3-Bucket in der Region erstellt werden kann, in der die CloudFormation-Vorlage bereitgestellt wird. Wenn Sie STS-basierte Authentifizierung verwenden, kann der Bucket jedoch möglicherweise nicht vom AWS-Konto erstellt werden, da die Authentifizierung an die `AssumeRole`-Richtlinien gebunden ist. Weitere Informationen finden Sie in der AWS-Dokumentation

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

auf der Seite zum Thema der Einrichtung des Amazon S3-Bucket für AWS-Kosten- und -Nutzungsberichte.

- Aktivieren Sie detaillierte Abrechnungsberichte in AWS. Weitere Informationen finden Sie in der AWS-Dokumentation .

> **Hinweis:** Die Funktion für detaillierte Abrechnungsberichte wird von Amazon AWS Cloud für neue Kunden zurückgezogen. Weitere Informationen und Migrationsdetails finden Sie in der AWS-Dokumentation zu detaillierten Abrechnungsberichten .

Erforderliche Rolle: sn_cmp.cloud_governor

Warum und wann dieser Vorgang ausgeführt wird

Dieses Verfahren umfasst zwei Aufgaben:

1. Füllen Sie das Formular des AWS-Abrechnungszeitplans mit Informationen aus, die Sie aus dem AWS-Portal kopieren. Mit dieser Aktion können AWS-Abrechnungsdaten aus der Instanz heruntergeladen werden.
2. Geben Sie den Zeitplan zum Herunterladen von AWS-Rechnungsinformationen an.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Analysieren** > **Abrechnung**.
2. Klicken Sie auf der Registerkarte **Abrechnungszeitpläne** auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** ein, und füllen Sie dann das Formular aus.

Feld	Beschreibung
Anbieter	Wählen Sie **AWS** aus.
Servicekonto	Der AWS-Servicekonto, den Sie bei der Ersteinrichtung erstellt haben. (Das AWS-Konto, für das der Abrechnungsbericht ausgeführt werden soll.)
Bucket	Datenspeicherbereich für die täglichen Abrechnungsdatensätze im AWS-Konto. Führen Sie die folgenden Schritte aus, um den Wert zu erhalten: **a.** Melden Sie sich bei der AWS-Verwaltungskonsole an, und wählen Sie im Menü **My Billing Dashboard** (Mein Abrechnungsdashboard) aus. **b.** Wählen Sie im Dashboard **Billing Preferences** (Abrechnungseinstellungen) aus. **c.** Erweitern Sie im Abschnitt **Cost Management Preferences** (Kostenmanagementeinstellungen) die Option **Detailed Billing Reports [Legacy]** (Detaillierte Abrechnungsberichte [veraltet]) aus und stellen Sie sicher, dass das Kontrollkästchen **Turn on the legacy Detailed Billing Reports feature to receive ongoing reports of your AWS charges** (Alte Funktion „Detaillierte Abrechnungsberichte“ aktivieren,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	um fortlaufend Berichte Ihrer AWS-Gebühren zu erhalten) ausgewählt ist. **d.** Kopieren Sie den Wert aus dem Feld **Save the S3 bucket:** (S3-Bucket speichern:) in das Feld **Bucket** des Formulars. **Hinweis:** AWS wählt standardmäßig den S3-Bucket aus, der dem AWS-Konto zugeordnet ist, bei dem Sie derzeit angemeldet sind. Ein grünes Häkchen zeigt an, dass der Bucket ordnungsgemäß konfiguriert ist.
Aktiv	Aktivieren Sie das Kontrollkästchen, um den Job zum Herunterladen zu aktivieren.
Ausführen	Frequenz, in der der Job zum Herunterladen ausgeführt werden soll.
Uhrzeit	Uhrzeit, zu der der Job zum Herunterladen ausgeführt werden soll.

3. Klicken Sie auf **Speichern**.
   Um den Job bei Bedarf auszuführen, klicken Sie auf **Jetzt ausführen**. Wählen Sie im Fenster **Abrechnungsdaten abrufen** einen Datumsbereich aus, und klicken Sie dann auf **Herunterladen**.

Nächste Maßnahme
Lassen Sie Cloud-Kosten auf dem Abrechnungsdashboard anzeigen.

Zugehörige Informationen

Cloud-Anmeldeinformationen

Downloadgröße von AWS-Abrechnungsdaten konfigurieren

Ein einzelner Satz Cloud Billing-Daten kann umfangreich sein. Vom MID-Server werden die Daten daher in verwaltbaren Blöcken an die ECC-Warteschlange gesendet. Optional können Sie eine Systemeigenschaft so konfigurieren, dass die Größe der einzelnen Blöcke begrenzt wird. So vermeiden Sie Leistungsprobleme, die durch die Übertragung großer Datenmengen verursacht werden.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie die Tabelle „Systemeigenschaften“, indem Sie im Anwendungsfilter `sys_properties.list` eingeben.
2. Filtern Sie die Liste, um die Eigenschaft `sn_cmp.billing.page_size` zu öffnen.
   Der Standardwert ist 3 MB.
3. Modifizieren Sie den Wert nach Bedarf.
   Der Höchstwert beträgt 5 MB.
4. Speichern Sie die Eigenschaft.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fügen Sie ein AWS Servicekonto zu hinzu Cloud-Konto

Im Rahmen des Tag-1-Setups von Cloud Provisioning and Governance haben Sie ein Servicekonto zum Cloud-Konto hinzugefügt. Um Ihre Infrastruktur aufzuteilen oder verschiedene Rechenzentren einzubeziehen, können Sie ein weiteres Servicekonto hinzufügen. Ein bestimmtes Rechenzentrum kann jedoch nicht in mehr als einem Servicekonto in einem Cloud-Konto ausgewählt werden.

Vorbereitungen

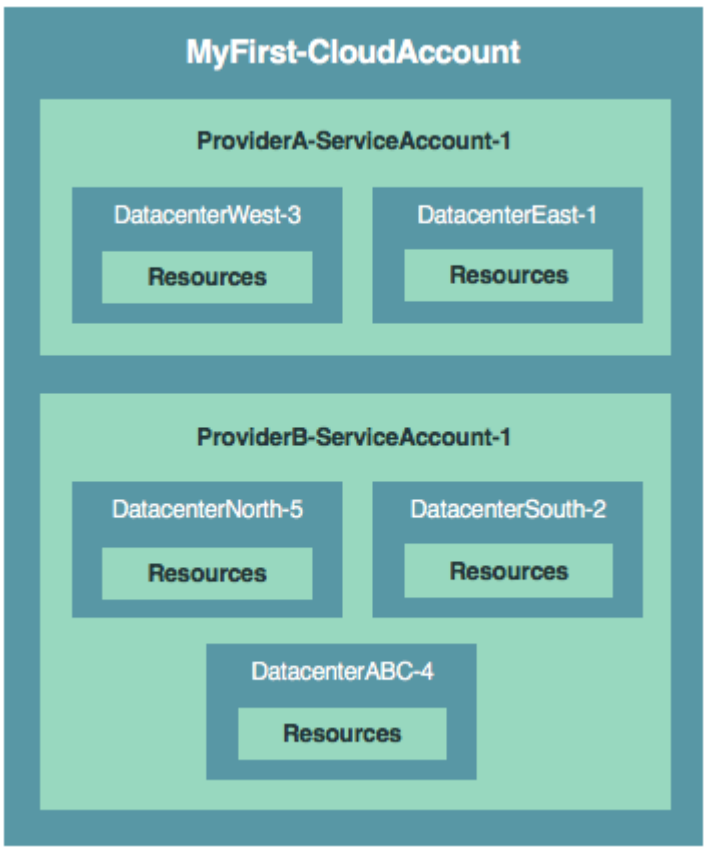
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.

In diesem Beispiel haben Sie ein Servicekonto mit dem Namen **ProviderB-ServiceKonto-1** hinzugefügt und drei Rechenzentren zur Einbindung in das Cloud-Konto ausgewählt:

Servicekonto mit drei ausgewählten Rechenzentren



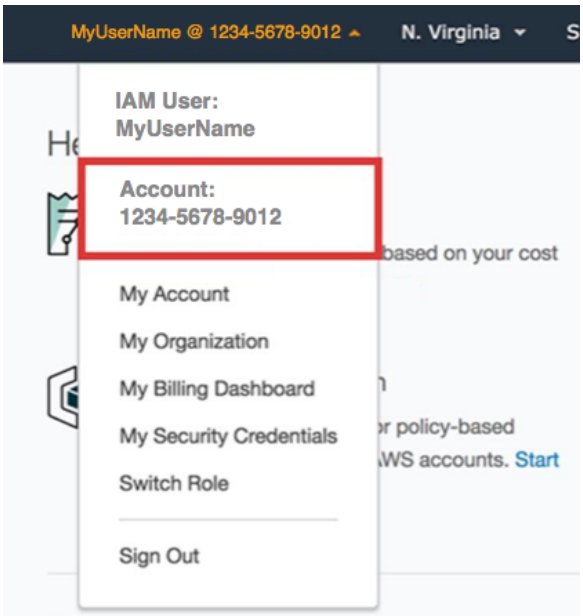
Wichtig: In einem Cloud-Konto können Sie kein bestimmtes Rechenzentrum in zwei verschiedenen Servicekonten auswählen.

Prozedur

1. Navigieren zu **Cloud-Adminportal** > **Service-Accounts**.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und aussagekräftigen **Namen** ein, und füllen Sie dann das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für dieses Servicekonto.
Account-ID	12-stellige Nummer des Benutzerkontos. Erweitern Sie die Liste unter dem AWS-Kontonamen in der AWS-Verwaltungskonsole, um die Nummer anzuzeigen. **Wichtig:** Entfernen Sie im Feld **Konto-ID** die Bindestriche (-) aus der Nummer. **Nummer des IAM-Benutzerkontos** 
Discovery-Anmeldeinformationen	Anmeldeinformationen, die für ServiceNow-Anwendungen für den Zugriff auf dieses Konto erforderlich sind. Sie können dieses Feld zu einem späteren Zeitpunkt konfigurieren, während Sie den Zugriff auf AWS-Konten konfigurieren. ◦ Wenn Sie hat die AWS-Anmeldeinformationen unter konfiguriert Now Platform , wählen Sie das Lupensymbol und dann den Namen der entsprechenden AWS -Anmeldeinformationen aus. ◦ Um andere AWS-Konten für den Zugriff auf diesen Account zu verwenden, lassen Sie das Feld leer. Beispielsweise müssen Sie die AWS-Anmeldeinformationen nicht für Konten angeben, die IAM-Rollen oder Mitgliedskonten annehmen und ihr Verwaltungskonto für den Zugriff verwenden.
Rechenzentrums-URL	URL des Rechenzentrums. Dieses Feld ist für die Konten AWS Region China und AWS GovCloud (US) erforderlich. Zum Beispiel:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ AWS Region China: `https://organizations.cn-northwest-1.amazonaws.com.cn` ◦ AWS GovCloud (USA): `https://aws.amazon.com/ec2/`
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie das **AWS-Rechenzentrum**.
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Übergeordneter Account	Name des Verwaltungskontos, das die Organisation in AWS darstellt, zu der dieses Mitgliedskonto gehört. Dieser Name wird angezeigt, wenn Sie **AWS-Rechenzentrum** auswählen. Wenn dieses Konto nicht Teil einer AWS-Organisation ist, lassen Sie dieses Feld leer.
Ist Master-Konto	Kennzeichnung des Verwaltungskontos. Sie wird angezeigt, wenn Sie in der Dropdown-Liste „Rechenzentrumstyp“ die Option **AWS-Rechenzentrum** auswählen. Aktivieren Sie das Kontrollkästchen, um das AWS-Servicekonto dem Verwaltungskonto zuzuordnen. Aktivieren Sie dieses Kontrollkästchen nur für Konten, die Sie zuvor in der AWS-Verwaltungskonsole als Verwaltungskonten konfiguriert haben und zu denen einige Mitgliedskonten gehören. In der AWS-Dokumentation finden Sie weitere Informationen zu AWS-Organisationen. **Hinweis:** Sie müssen die richtige Berechtigung in AWS oder der Organisationsrolle für Standardanmeldeinformationen einrichten. Weitere Informationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern.
Account des Zugriffsberechtigten	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, bei denen keine permanenten AWS-Anmeldeinformationen verwendet werden und bei denen IAM-Rollen für den Zugriff genutzt werden.

3. Klicken Sie auf **Aktualisieren** oder **Absenden**.
   Das Servicekonto wird vom System erstellt, und es wird die Liste aller erkannten Rechenzentren angezeigt.
4. Wiederholen Sie den Vorgang, um so viele Servicekonten wie erforderlich hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Setup-Leitfaden für Tag 1 für Microsoft Azure Cloud auf Cloud Provisioning and Governance

Zur Ersteinrichtung von Cloud Provisioning and Governance führen Sie die Schritte in diesem Setupleitfaden für „Tag 1“ durch. Achten Sie darauf, die Schritte in der richtigen Reihenfolge auszuführen. Nachdem Sie das Setup für „Tag 1“ durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration für „Tag 2“ je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Fordern Sie die Anwendung Cloud Provisioning and Governance an

Die Anwendung Cloud Provisioning and Governance ist als separates Abonnement verfügbar und erfordert das Cloud Provisioning and Governance-Plugin (com.snc.cloud.mgmt). Weitere Informationen finden Sie unter Die Anwendung Cloud Provisioning and Governance anfordern.

Zum Einrichten von Cloud Provisioning and Governance erforderliche Rollen

- Vorgänge im Azure-Portal erfordern eine der folgenden Rollen:
  - Administrator für Azure oder Azure AD (Active Directory)
  - Applikationsadministrator
  - Anwendungsentwickler
  - Cloud-Anwendungsadministrator

  und die Rolle „Mitwirkender bei Ressourcenrichtlinien“ zum Erstellen oder Ändern von Ressourcenrichtlinien.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Von Cloud Provisioning and Governance verwendete Begriffe

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet. In Azure werden die bereichsspezifischen Container für virtuelle Ressourcen als Regionen bezeichnet. In Cloud Provisioning and Governance werden Regionen als Rechenzentren oder logische Rechenzentren (Logical Datacenters, LDCs) bezeichnet. Der Begriff „logisch“ wird zur Verdeutlichung der Tatsache verwendet, dass Cloud Provisioning anbieterunabhängig ist. Alle Infrastrukturen oder Anwendungen, die mit Cloud Provisioning bereitgestellt werden, sind einem Rechenzentrum zugeordnet.

Schneller Überblick über den Setup-Prozess

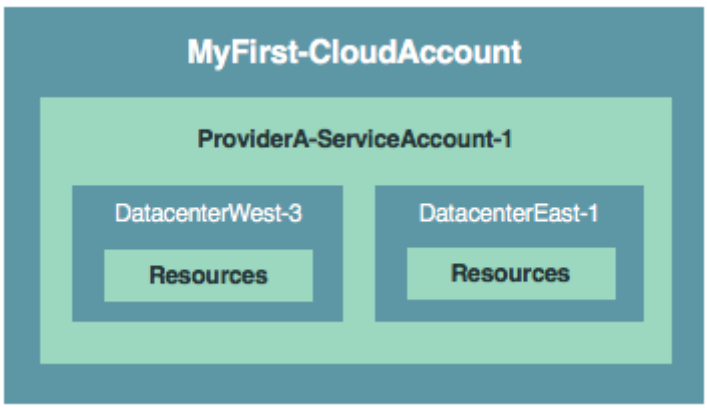
Der Setup-Prozess umfasst folgende Aufgaben:

- Falls erforderlich: Die Anwendung Cloud Provisioning and Governance anfordern.
- Weisen Sie Cloud-Benutzern die entsprechenden Rollen zu.
- Richten Sie die MID Servers für die sichere Kommunikation mit den Provider-API-Endpunkten ein.
- Erfassen Sie im Provider-Portal Ihre Kontoeinstellungen und die Anmeldeinformationen, die beim Discovery-Prozess (über einen MID-Server) dazu verwendet werden, programmgesteuert auf Ihre Provider-Konten zuzugreifen. Ordnen Sie die Kontoeinstellungen und Anmeldeinformationen sicher einem Servicekonto in Cloud Provisioning and Governance zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Richten Sie ein Cloud-Konto ein, um Ihre gesamte verwaltete Cloud-Infrastruktur darzustellen, und richten Sie ein Servicekonto ein, das mit einem Ihrer Provider-Konten funktioniert. Sie geben an, welche Rechenzentren im Servicekonto in das Cloud-Konto aufgenommen werden sollen. (Später, am „Tag 2“, können Sie zusätzliche Cloud-Accounts und Servicekonten vom selben Provider oder anderen Providern einrichten.)
- In Cloud Provisioning werden CMDB-Daten dafür verwendet, Benutzer beim Anfordern und Verwalten von Cloud-Ressourcen und beim Verwalten der Cloud-Infrastruktur zu unterstützen. Zum Füllen der CMDB mit Ressourcendaten für alle Rechenzentren führen Sie den Discovery-Prozess manuell für jedes im Servicekonto enthaltene Rechenzentrum aus. Anschließend konfigurieren Sie Discovery so, dass die Anwendung regelmäßig ausgeführt wird und somit die kontinuierliche Aktualisierung der Daten sichergestellt ist. Ihr Cloud-Konto könnte wie folgt aussehen:

Struktur eines Cloud-Kontos an Tag 1



- Provider bieten Services, mit denen die CMDB automatisch aktualisiert werden kann, wenn für eine Ressource ein Lebenszyklus-Change (erstellt/geändert/beendet) oder Konfigurations-Update durchgeführt wird. Sie können den Service für die direkte Integration mit Cloud Provisioning and Governance konfigurieren.

Aktionen zur Integration von Cloud Provisioning and Governance in Ihre Microsoft Azure-Konten

Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

1. Weisen Sie Azure Anwendern von Rollen zu Cloud Provisioning and Governance

   Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

2. Installieren und konfigurieren Sie MID Servers für den Zugriff auf Cloud-Umgebungen

   Damit eine sichere und zuverlässige Kommunikation gewährleistet ist, findet eine Kommunikation zwischen dem Discovery-Prozess und Ihren Cloud Provider-Konten und Cloud-Ressourcen über mindestens einen MID Servers statt. Sie können MID Servers in Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke einrichten.

   Hinweis: Daten werden bei der Übertragung zum MID-Server und zwischen dem MID-Server und dem API-Endpunkt verschlüsselt. Um hohe Leistung und Sicherheit zu gewährleisten, sollten Sie mindestens einen MID-Server für jedes verwaltete Rechenzentrum konfigurieren. Konfigurieren Sie einen MID-Server, auch wenn Sie bereits andere MID Servers beim Einrichten von Cloud Provisioning and Governance für einen anderen Cloud Provider konfiguriert haben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Microsoft Azure-Dienstprinzipal erstellen

   Für den sicheren Zugriff auf Ressourcen und Abrechnungsdaten in Ihrem Microsoft Azure-Konto muss der Discovery-Prozess entsprechende Anmeldeinformationen für das Microsoft Azure-Konto bereitstellen. Sie erstellen ein spezielles programmgesteuertes Konto – einen Microsoft Azure-Dienstprinzipal –, um die erforderlichen Anmeldeinformationen zu generieren.

4. Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern

   Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Um die Anmeldeinformationen für Discovery verfügbar zu machen, erstellen Sie zuerst die Anmeldeinformationen des Azure-Dienstprinzipals in der Azure-Portal. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz.

5. Fügen Sie eine hinzu Azure Servicekonto

   Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.

6. Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

   Discovery nutzt die Informationen im Servicekonto dazu, alle dem Anbieter-Account zugeordneten logischen Rechenzentren zu identifizieren.

7. Richten Sie ein Cloud-Konto für ein Azure

   Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

8. Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

   Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder des zusammengefassten Speichers ein. Sie können Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

10. Erstellen Sie Microsoft Azure Anmeldeinformationen für den Abrechnungsdownload

    Definieren Sie den geplanten Auftrag, mit dem unter Verwendung eines MID-Servers regelmäßig Abrechnungsdaten vom Provider heruntergeladen werden. Von Cloud Provisioning and Governance werden die Daten in einer Kostentabelle gespeichert und die Informationen zum Erstellen von Berichten verwendet.

Nächste Schritte

Wenn Sie alle Verfahren für „Tag 1“ und „Tag 2“ in diesem Setupleitfaden abgeschlossen haben, finden Sie unter Cloud Provisioning and Governance-Administrationsleitfaden weitere Informationen zur Verwendung der Anwendung Cloud Provisioning and Governance in Ihrem Unternehmen.

Microsoft Azure Government Cloud auf Cloud Provisioning and Governance einrichten

Richten Sie Microsoft Azure Government Cloud zum ersten Mal auf Cloud Provisioning and Governance ein. Anschließend können Sie Microsoft Azure Government Cloud-Ressourcen mit Cloud Provisioning and Governance erkennen, bereitstellen und verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Hinweis: ServiceNow® ITOM-Produkte werden für die Regionen Deutschland und China nicht offiziell zertifiziert oder unterstützt.

Warum und wann dieser Vorgang ausgeführt wird

Achten Sie darauf, die Schritte in der richtigen Reihenfolge auszuführen. Nachdem Sie das Setup für Tag 1 durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration für Tag 2 je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Zum Einrichten von Microsoft Azure Government Cloud auf Cloud Provisioning and Governance müssen Sie folgende Schritte ausführen:

- Richten Sie im Azure Government-Portal einen Microsoft Azure-Dienstprinzipal ein, und registrieren Sie das Servicekonto in der Cloud Provisioning and Governance-Anwendung.
- Konfigurieren Sie einen MID-Server mit den erforderlichen Eigenschaften, damit Microsoft Azure Government und die ServiceNow-Instanz richtig kommunizieren können.
- Verwenden Sie die Anmeldeinformationen des Microsoft Azure-Dienstprinzipals, um zugehörige Servicekonten und Cloud-Ressourcen zu erkennen.

Prozedur

1. Erstellen von Microsoft Azure Serviceprinzipal im Portal der Microsoft Azure -Behörden.

   Hinweis: Navigieren zu **App-Registrierungen** > **Registrieren Sie eine Anwendung** > **Unterstützte Account-Typen** Abschnitt. Wählen Sie dann die Option **Accounts in this organizational directory only (Single tenant)** (Konten nur in diesem Organisationsverzeichnis (Einzelner Mandant)), um sicherzustellen, dass das Active Directory, das für die Microsoft Azure Government Cloud konfiguriert ist, für die Authentifizierung verwendet wird.

   Weitere Informationen finden Sie unter Erstellen einer Azure AD-Anwendung und eines Dienstprinzipals mit Ressourcenzugriff über das Portal .

2. Konfigurieren MID Servers um Cloud Provisioning and Governance mit einem Behörden-Cloud-Account Microsoft Azure von zu verbinden.

   a. Navigieren zu **MID-Server** > **Fähigkeiten**.

   b. Klicken Sie auf **Bearbeiten**, und fügen Sie die folgenden Optionen hinzu:

      - **Azure**
      - **Cloud Management**

   c. Klicken Sie auf **Speichern**.

   d. Wahlweise: Navigieren zu **MID-Server** > **Unterstützte Anwendungen**. Überspringen Sie den nächsten Schritt, wenn **ALLE** Anwendungen ausgewählt sind.

   e. Wahlweise: Klicken Sie auf **Bearbeiten**, und fügen Sie die folgenden Anwendungen zur **Liste der unterstützten Anwendungen** hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Discovery**
- **Cloud Management**
- **Orchestration**

f. Klicken Sie auf **Speichern**.

Hinweis: Weitere Informationen finden Sie unter:

- MID-Server-Auswahl
- Fähigkeiten des MID-Servers

3. Navigieren zu **MID-Server** > **Eigenschaften**.

a. Klicken Sie auf **Neu**, und fügen Sie für jedes der folgenden Name-Wert-Paare neue Datensätze hinzu:
MID-Server -Eigenschaften

Name	Wert
mid.cmp.azure_api.base_endpoint	https://management.usgovcloudapi.net/${apiPath}
mid.cmp.azure_api.storage.container.path	https://${accountName}.blob.core.usgovcloudapi.net/?comp=list
mid.property.azure_token_manager.endpoint	https://login.microsoftonline.us/${tenantId}/oauth2/token
mid.property.azure_token_manager.endpoint_content	grant_type=client_credentials&client_id=${clientId}&resource=https%3A%2F%2Fmanagement.usgovcloudapi.net%2F&client_secret=${clientSecret}
mid.cmp.azure_api.storage.blob.path	https://${accountName}.blob.core.usgovcloudapi.net/${containerName}?restype=container&include=snapshots&comp=list

b. Klicken Sie auf **Absenden**.

4. Speichern Sie die Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz.

5. Navigieren Sie im **Cloud-Adminportal zu Verwalten** > **Anmeldeinformationen**, und wählen Sie den Datensatz Azure-Dienstprinzipal aus.

6. Zum Erkennen von Servicekonten, die den Azure-Abonnements zugeordnet sind, die für diesen Dienstprinzipal verfügbar sind, klicken Sie auf den zugehörigen Link **Abonnements ermitteln**.

Ergebnisse

In der zugehörige Liste **Azure-Abonnements** sind alle Abonnements aufgeführt, die mit dem Azure-Dienstprinzipal verknüpft sind.

Nächste Maßnahme

Definieren Sie den Zeitplan für den Download Microsoft Azure Abrechnungsdaten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Weisen Sie Azure Anwendern von Rollen zu Cloud Provisioning and Governance

Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

Vorbereitungen

Erforderliche Rolle: user_admin oder admin

Prozedur

Weisen Sie Gruppen und Benutzern nach Bedarf die folgenden Rollen zu:

Beschreibender Name und Rollenname	**Beschreibung und Aufgaben**	**Zugriffsberechtigungen in** Cloud Provisioning and Governance
Root-Administrator `[sn_cmp.cmp_root_admin]`	Höchste Anwendungszugriffsebene für Cloud Provisioning and Governance.	Alle
Cloud-Administrator `[sn_cmp.cloud_admin]`	Konfiguriert die Cloud Provisioning and Governance-Anwendung und richtet die Cloud-Infrastruktur ein.	Cloud-Infrastruktur: Servicekonten und Cloud-Konto Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • IBM Cloud-Update • VMware-Events
Kontrolle `[sn_cmp.cloud_governor]`	Überwacht die gesamte Cloud-Nutzung und setzt die Einhaltung der Regeln, Kontingente und Richtlinien der Organisation durch. Verwaltet auch Tags und Berechtigungen für verschiedene Objekte.	Governance: • Richtlinien • Pools • Kontingente • Berechtigungen
Service Designer `[sn.cmp.cloud_service_designer]`	Erstellt Blaupausen, ARM- und CloudFormation-Vorlagen und Katalogelemente.	Cloud-Servicedesign: • Cloud-Vorlagen • Blaupausen • Blaupausenkatalogelemente • Ressourcenblöcke

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	**Beschreibung und Aufgaben**	**Zugriffsberechtigungen in** Cloud Provisioning and Governance
Cloud-Benutzer `[sn_cmp.cloud_service_user]`	Fordert Stapel und Ressourcen an und verwaltet sie.	Cloudbenutzerportal. Wenn Sie die Rolle einer Gruppe zuweisen, teilen sich alle Mitglieder der Gruppe die Kontingentbeschränkungen und den Besitz bestimmter Ressourcen. Sie können auf alle Aufgabendatensätze zugreifen, die Ihnen oder anderen zugewiesen sind, wenn Sie die Rolle „Cloud-Service-Benutzer“ innehaben.
Cloud-Betreiber `[sn_cmp.cloud_operator]`	Überwacht die Cloud Provisioning and Governance-Anwendung und behebt Probleme damit.	Dashboards und Berichte: • Dashboard für Cloud-Vorgänge • Cloud-Ursachenanalyse • Cloud-Orchestrierungspfad • Cloud-API-Pfad
Cloud-Event-Integration `[sn_cmp.cloud_event_integration]` **Hinweis:** Von IBM Cloud Connector nicht unterstützt	Autorisiert den Zugriff auf die Instanz für externe Services, mit denen die CMDB bei Auftreten von Cloud-Events automatisch aktualisiert wird. Diese Rolle gewährt den Zugriff auf den REST-Endpunkt des Cloud Events.	Cloud-Infrastruktur: • Servicekonten und Cloud-Konto • Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • VMware-Events
Cloud-Gruppenadministrator `[sn_cmp.cloud_group_admin]`	Gewährt Administrator-Zugriff für alle Gruppen, denen Sie angehören.	

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Einer Gruppe eine Rolle zuweisen

Einem Benutzer eine Rolle zuweisen

Microsoft Azure-Dienstprinzipal erstellen

Für den sicheren Zugriff auf Ressourcen und Abrechnungsdaten in Ihrem Microsoft Azure-Konto muss der Discovery-Prozess entsprechende Anmeldeinformationen für das Microsoft Azure-Konto bereitstellen. Sie erstellen ein spezielles programmgesteuertes Konto – einen Microsoft Azure-Dienstprinzipal –, um die erforderlichen Anmeldeinformationen zu generieren.

Vorbereitungen

Erforderliche Rollen:

- Rollen discovery_admin, service_mapping_admin, sn_cmp.cloud_admin in Cloud Provisioning and Governance oder Rolle sn_cloud_ops_ws.cloud_ops_admin in Arbeitsbereich für Cloud-Vorgänge.
- Vorgänge im Microsoft Azure-Portal erfordern eine der folgenden Rollen:
  - Administrator für Azure oder Azure AD (Active Directory)
  - Applikationsadministrator
  - Anwendungsentwickler
  - Cloud-Anwendungsadministrator

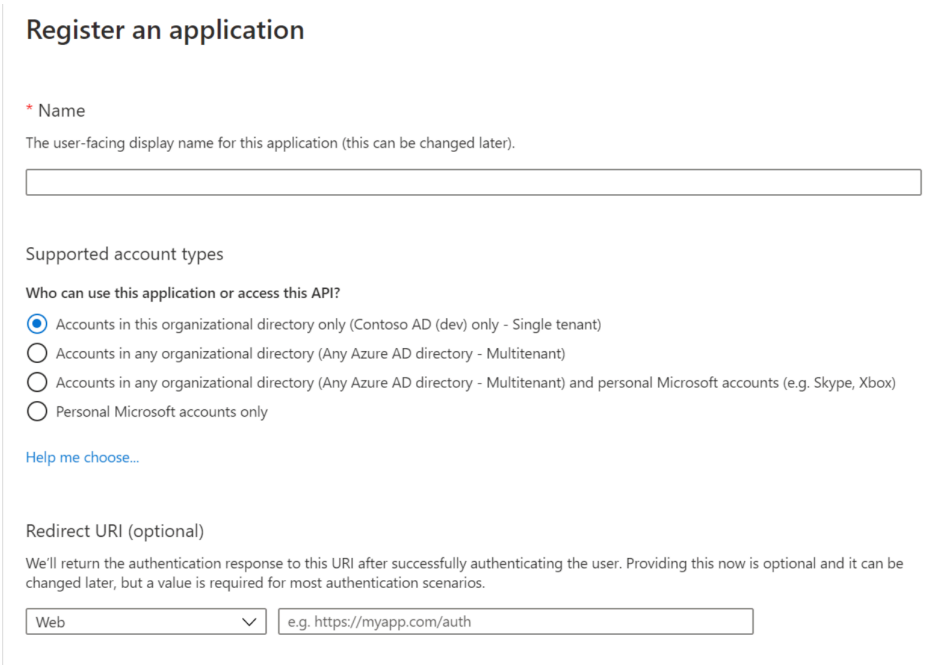
  und die Rolle „Mitwirkender bei Ressourcenrichtlinien“ zum Erstellen oder Ändern von Ressourcenrichtlinien.
- Aktivieren Sie die interne Netzwerkverbindung zwischen den MID-Servern und den Azure Cloud-API-Endpunkten:
  - Die US-GovCloud-URL lautet `https://management.usgovcloudapi.net/`.
  - Die URL für die kommerzielle Azure-Cloud lautet *„management.azure.com*“.

  Hinweis: Das Hinzufügen von Anmeldeinformationen ist nicht erforderlich, wenn das hinzugefügte Konto bereits ein GovCloud-Konto ist.

Prozedur

1. Melden Sie sich beim Azure-Portal an, und navigieren Sie zu **Azure Active Directory**.
2. Navigieren Sie zum Abschnitt **App registrations** (Appregistrierungen), und klicken Sie auf **New application registration** (Neue Anwendungsregistrierung).
   Geben Sie für Ihre Anwendung folgende Informationen ein:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
Name	Eindeutiger Name für die Anwendung und ihre Integrationsanmeldeinformationen. Beispiel: `ServiceNow Integration`.
Unterstützte Account-Typen	Geben Sie an, wer die Anwendung verwenden kann.
Redirect URI (optional, Umleitungs-URI)	URL, die auf Azure zugreift. Normalerweise die URL der ServiceNow-Instanz

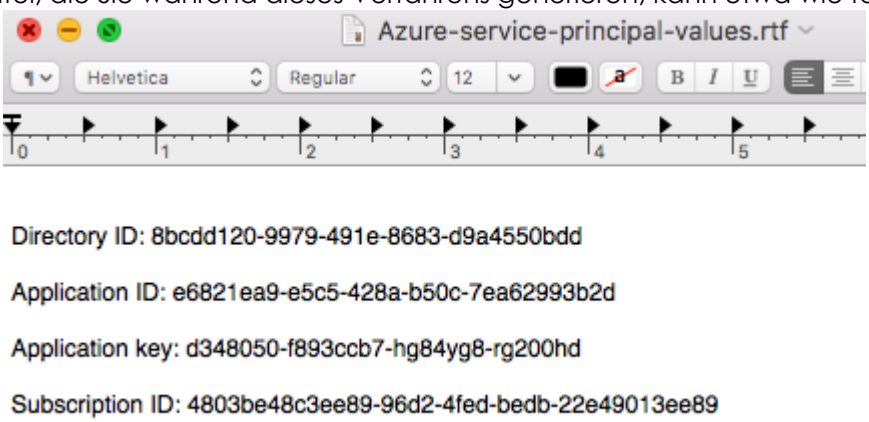
3. Wählen Sie **Register** aus, um die Registrierung der App abzuschließen.
4. Wenn die Registrierung abgeschlossen ist, kopieren Sie die Werte für Anwendungs-ID (Client) und Verzeichnis-ID (Mandant), und fügen Sie sie in den Texteditor ein.
5. Beschriften Sie die Werte **Anwendungs-ID** bzw. **Verzeichnis-ID**.
6. Navigieren Sie im Azure-Portal zum Abschnitt **Certificates & secrets** (Zertifikate und geheime Schlüssel), und geben Sie dann unter **New client secret** (Neuer Client-Geheimschlüssel) die folgenden Werte an:

Feld	Beschreibung
Schlüsselbeschreibung	Beschreibung für den Schlüssel
Dauer	Ablauf für den Schlüssel. **Hinweis:** Ihre Organisation kann Richtlinien anwenden, um die Gültigkeitsdauer des Schlüssels einzuschränken. Wählen Sie die entsprechende Dauer aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Hinzufügen**.
8. Kopieren Sie den Schlüsselwert, fügen Sie ihn in den Texteditor ein, und beschriften Sie den Wert als **Anwendungsschlüssel**.
9. Damit der Dienstprinzipal mit verschiedenen Azure-Abonnements arbeiten kann, navigieren Sie zu **Abonnements**.
   Zum Verwalten mehrerer Abonnements müssen Sie das folgende Verfahren für jedes Abonnement ausführen:

   a. Fügen Sie die Abonnements-ID in den Texteditor ein, und beschriften Sie sie als **Abonnements-ID**.
   Die Textdatei, die Sie während dieses Verfahrens generieren, kann etwa wie folgt



   aussehen:

   b. Navigieren Sie zum Abonnement, und wählen Sie im Menü die Option **Zugriffssteuerung (IAM)** aus.

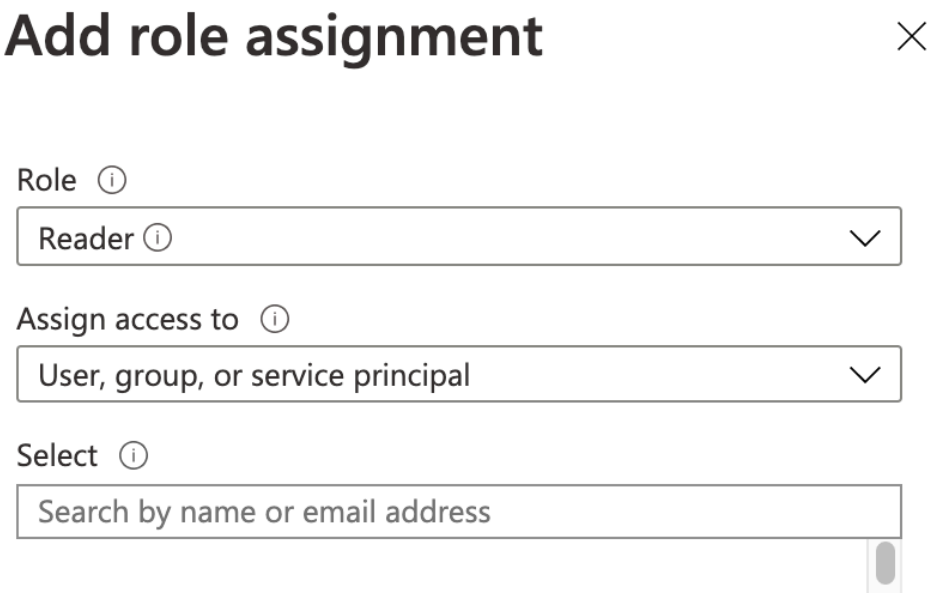
   c. Klicken Sie oben im Bildschirm auf **+ Hinzufügen** und dann auf **Add role assignment** (Rollenzuweisung hinzufügen).

   d. Wählen Sie im Feld **Rolle** den Wert **Leser** aus.
   Lassen Sie den Standardwert für **User, group, or service principal** (Benutzer, Gruppe oder Service-Prinzipal) für das Feld **Assign Access to** (Zugriff zuweisen an) unverändert.

   > **Hinweis:** Die Rolle **Mitwirkender bei Ressourcenrichtlinien** ist nur für die Bereitstellung erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Wählen Sie im Feld **Auswählen** den Namen aus, den Sie in Schritt 2 erstellt haben, und klicken Sie auf **Speichern**.



10. Führen Sie die entsprechende Aktion aus.

- Wenn Sie Cloud-Discovery nicht über Arbeitsbereich für Cloud-Vorgänge verwenden, gehen Sie wie folgt vor:

  Klicken Sie im Discovery Manager auf das Plus-Symbol (**+**), und wählen Sie in der Liste **Azure-Dienstprinzipal** aus.

- Wenn Sie Cloud-Discovery über Arbeitsbereich für Cloud-Vorgänge verwenden, gehen Sie wie folgt vor:

  a. Navigieren zu **Alle** > **Verbindungen und Anmeldeinformationen** > **Anmeldeinformationen**.

  b. Wählen Sie **Neu**.

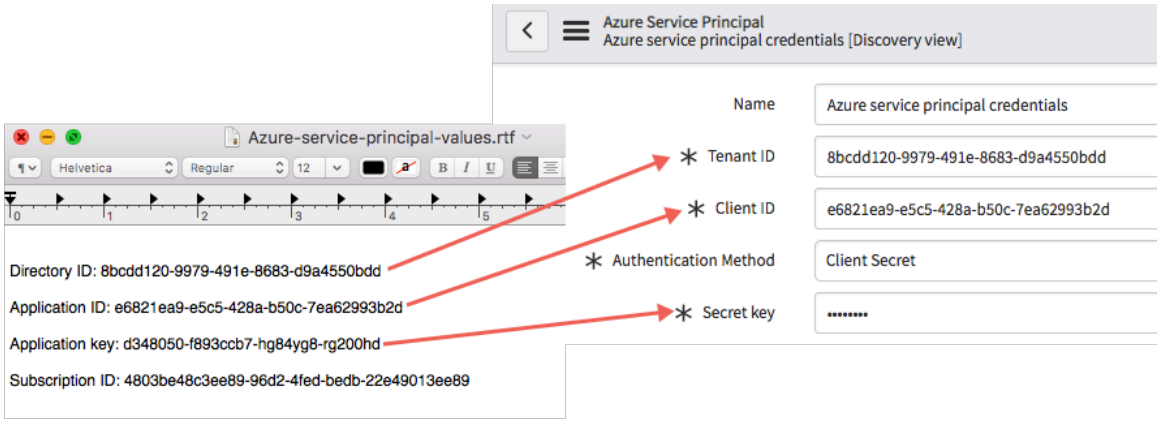
  c. Wählen Sie **Azure-Service-Prinzipal** aus.

11. Geben Sie die folgenden Werte im Azure-Service-Principal-Formular an:

Feld	Wert
Name	Name des Dienstprinzipals, der bei der Instanz registriert werden soll. Beispiel: `Azure service principal credentials`.
Authentifizierungsmethode	Wählen Sie **Client-Geheimnis**. Das Feld **Geheimer Schlüssel** wird angezeigt, wenn Sie **Geheimer Clientschlüssel** auswählen. **Hinweis:** **Client-Zusicherung** wird nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Kopieren Sie die Werte aus der temporären Textdatei, und fügen Sie sie in die verbleibenden Felder ein.



Formularfeld „Anmeldeinformationen“	Wert „Azure-Dienstprinzipal“
Mandanten-ID	Wert der Azure-**Verzeichnis-ID** aus der Textdatei
Client-ID	Wert der Azure-**Anwendungs-ID** aus der Textdatei
Geheimer Key	Wert des Azure-**Anwendungsschlüssels** aus der Textdatei

13. Klicken Sie auf **Speichern**, um den Azure-Dienstprinzipal zu erstellen.
14. Klicken Sie auf den zugehörigen Link **Abonnements erkennen**, um alle Abonnements für den Azure-Dienstprinzipal zu suchen.
    Die Instanz erstellt ein Servicekonto für jedes erkannte Abonnement. In der zugehörigen Liste **Azure-Abonnements** sind alle Abonnements aufgeführt, die mit dem Azure-Dienstprinzipal verknüpft sind.
15. Klicken Sie auf ein Abonnement, um das für das Abonnement erstellte Servicekonto anzuzeigen.
16. Klicken Sie auf einen Discovery-Statuseintrag in der Liste **Berechtigung Discovery-Status**, um das Discovery-Protokoll anzuzeigen.
    Bei jedem Klicken auf **Discovery-Abonnement** generiert die Instanz einen neuen Discovery-Status und zeigt ihn in der Liste **Berechtigung Discovery-Status** an.

Nächste Maßnahme

Nur Cloud Provisioning and Governance: Erstellen Sie einen Datensatz der Anmeldeinformationen des Dienstprinzipals in der ServiceNow-Instanz, damit über Cloud Provisioning and Governance-Prozesse auf Microsoft Azure-Daten zugegriffen werden kann. Weitere Informationen finden Sie unter Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern.

Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern

Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Um die Anmeldeinformationen für Discovery verfügbar zu machen, erstellen Sie zuerst die Anmeldeinformationen des Azure-Dienstprinzipals in der Azure-Portal. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle:

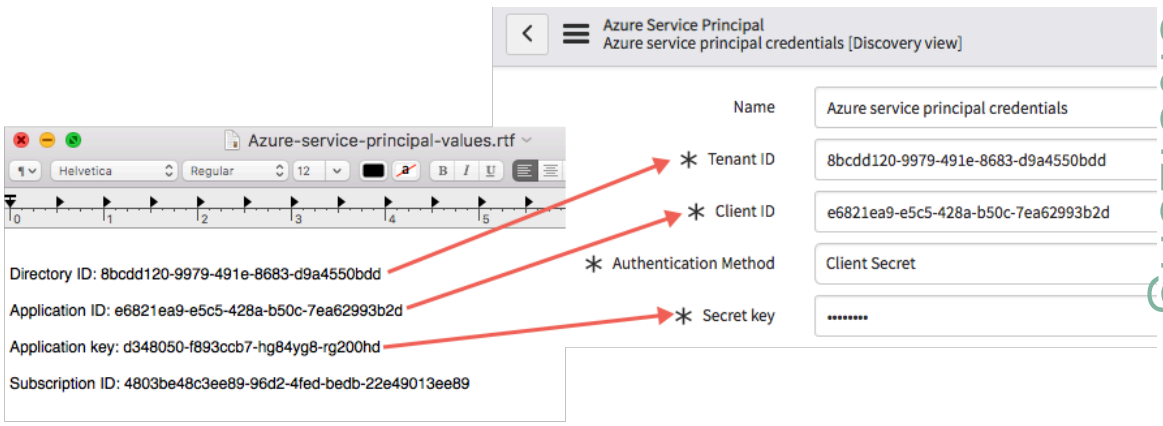
- Azure-Portal Active Directory-Administrator (AD)
- Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin, discovery_admin

Prozedur

1. Microsoft Azure-Dienstprinzipal erstellen und öffnen Sie die Textdatei, die Sie während des Verfahrens erstellt haben.
2. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Anmeldeinformationen**.
3. Klicken Sie auf **Neu**, und wählen Sie dann **Azure-Dienstprinzipal** aus.
4. Geben Sie die folgenden Werte im Azure-Service-Principal-Formular an:

Feld	Wert
Name	Name des Dienstprinzipals, der bei der Instanz registriert werden soll. Beispiel: `Azure service principal credentials`.
Authentifizierungsmethode	Wählen Sie **Client-Geheimnis** aus. Das Feld **Geheimer Schlüssel** wird angezeigt, wenn Sie **Geheimer Clientschlüssel** auswählen. **Hinweis:** **Client-Zusicherung** wird nicht unterstützt.

5. Kopieren Sie die Werte aus der Textdatei `Azure-Credentials.txt`, und fügen Sie sie in die verbleibenden Felder ein.



6. Wählen Sie die entsprechenden **EA-Anmeldeinformationen** aus der Liste aus, wählen Sie das Kontrollkästchen **Aktiv** aus, und klicken Sie dann auf **Speichern** , um den Datensatz zu erstellen.
7. Klicken Sie auf den zugehörigen Link **Abonnements ermitteln**, um alle Abonnements zu finden, die mit dem Azure-Dienstprinzipal verknüpft sind.
   Die Instanz erstellt für jedes ermittelte Abonnement einen Servicekonto.In der zugehörigen Liste **„Azure-Abonnements“** werden alle Abonnements angezeigt, die dem Azure-Serviceprinzipal zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf ein Abonnement, um den Servicekonto zu sehen, der für dieses Abonnement erstellt wurde.
9. Klicken Sie in der Liste **Discovery-Status für Anmeldeinformationen** auf den Eintrag eines Discovery-Status, um das zugehörige Discovery-Protokoll aufzurufen.
   Jedes Mal, wenn Sie auf **Abonnements ermitteln** klicken, generiert die Instanz einen neuen Discovery-Status und führt den Status in der Liste **Discovery-Status für Anmeldeinformationen** auf.

Fügen Sie eine hinzu Azure Servicekonto

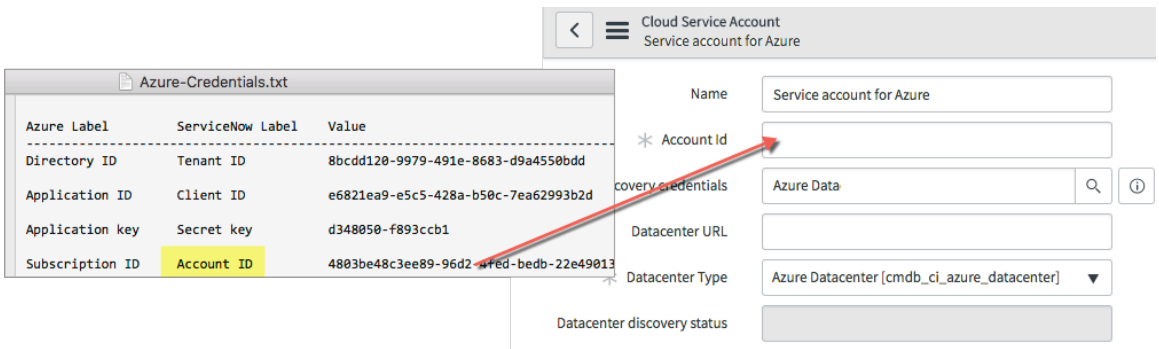
Im Rahmen des Setup-Leitfadens für Tag 1 für Cloud Provisioning haben Sie dem Cloud-Konto ein Servicekonto hinzugefügt. Um Ihre Infrastruktur aufzuteilen oder verschiedene Rechenzentren einzubeziehen, können Sie ein weiteres Servicekonto hinzufügen. Ein bestimmtes Rechenzentrum kann jedoch nicht in mehr als einem Servicekonto in einem Cloud-Konto ausgewählt werden.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Öffnen Sie die Textdatei `Azure-Credentials.txt`, die Sie während der Anleitung Microsoft Azure-Dienstprinzipal erstellen erstellt haben.
2. Navigieren zu **Cloud-Adminportal** > **Verwalten** > **Service-Accounts**.
3. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** ein, und füllen Sie dann das Formular aus.



Feld	Beschreibung
Konto-ID	Der Wert der Azure-**Abonnement-ID**, den Sie aus der Azure-Portal in die Textdatei kopiert haben. Unter Erkennung von Azure-Clouds finden Sie Informationen zu Abonnement-IDs für Verwaltungsgruppen.
Discovery-Anmeldeinformationen	Name der Anmeldeinformationen, die Sie unter Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern erstellt haben. Im Beispiel haben Sie den Namen `Azure service principal credentials` verwendet.
Rechenzentrums-URL	URL des Rechenzentrums.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Dieses Feld ist nur für Behörden- und Regionalaccounts erforderlich. Muster für Discovery und Service-Mapping unterstützt die Behörden-Clouds für die USA, Deutschland und Microsoft Azure China .
Rechenzentrumstyp	Wählen Sie **Azure-Rechenzentrum** aus.
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.
Sollte Events abrufen	Option, um in der Now Platform® das Sammeln von Informationen über Ressourcen-Changes aus der Microsoft Azure-Cloud zu aktivieren. Die Now Platform® verwendet die Informationen über Ressourcen-Changes zur Aktualisierung der Configuration Management Database (CMDB). Weitere Informationen zu den unterstützten Azure -Ressourcentypen finden Sie unter Azure Verarbeitung von Changes. Wenn Sie das Kontrollkästchen Soll Ereignisse abrufen für eine Verwaltungsgruppe aktivieren, aktiviert Now Platform die Verarbeitung von Changes Azure für alle Abonnements in der Verwaltungsgruppe.

4. Klicken Sie auf **Aktualisieren** oder **Absenden**.
   Das Servicekonto wird vom System erstellt, und es wird die Liste aller erkannten Rechenzentren angezeigt.

Nächste Maßnahme
Nachdem Sie alle Verfahren in dieser Ersteinrichtung für „Tag 1“ abgeschlossen haben, können Sie zusätzliche Cloud-Accounts und Servicekonten erstellen, um Ihre Cloud-Infrastruktur zu organisieren und aufzuteilen.

Hinweis:

Wenn Sie sich in einer domänengetrennten Instanz befinden, sind nur die Events sichtbar, die zur CMDB aktualisiert wurden und zu Ihrer Domäne gehören. Events erstellen Configuration Items (CIs) in der gleichen Domäne wie das Cloud-Servicekonto, dem sie zugeordnet sind.

Zugehörige Informationen

Erkennung von Azure-Clouds

Richten Sie ein Cloud-Konto für ein Azure

Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

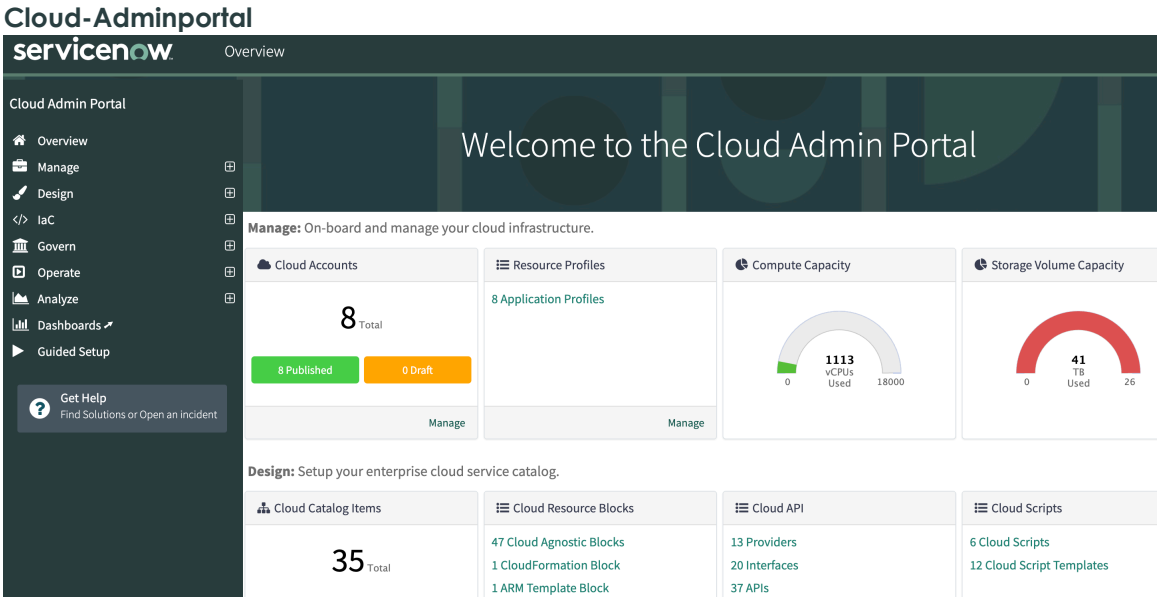
Warum und wann dieser Vorgang ausgeführt wird
Weitere Informationen zu Cloud-Accounts finden Sie unter Cloud-Accounts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet. In Azure werden die bereichsspezifischen Container für virtuelle Ressourcen als Regionen bezeichnet. In Cloud Provisioning and Governance werden Regionen als Rechenzentren oder logische Rechenzentren (Logical Datacenters, LDCs) bezeichnet. Der Begriff „logisch“ wird zur Verdeutlichung der Tatsache verwendet, dass Cloud Provisioning anbieterunabhängig ist. Alle Infrastrukturen oder Anwendungen, die mit Cloud Provisioning bereitgestellt werden, sind einem Rechenzentrum zugeordnet. .

Prozedur

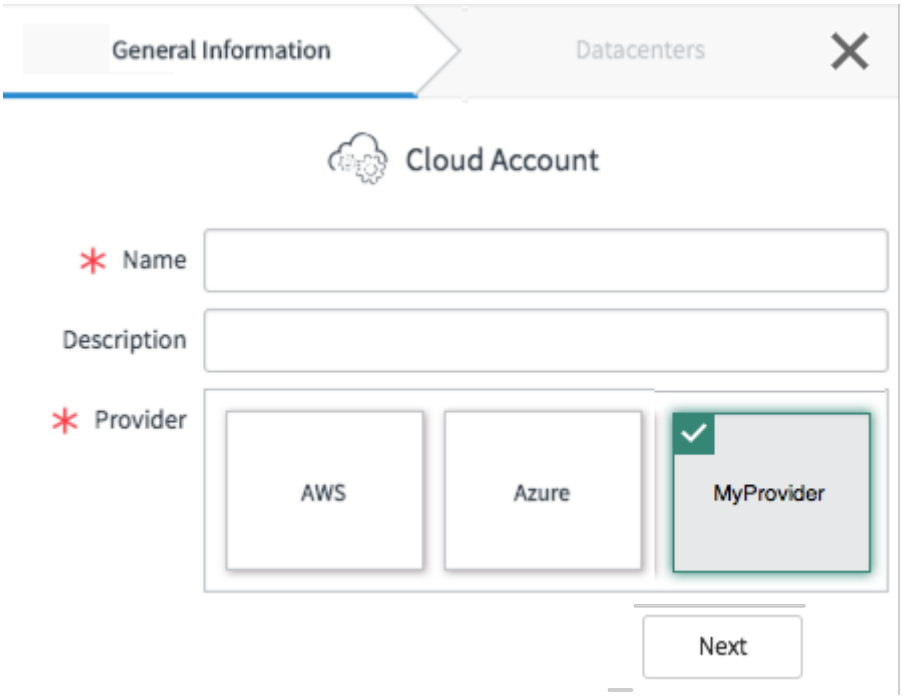
1. Navigieren Sie im Cloud-Administrationsportal zu **Verwalten** > **Cloud-Accounts**.



2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** und eine **Beschreibung** ein, und wählen Sie dann den Cloud-**Provider** für das Konto aus (Azure).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



3. Klicken Sie auf **Next** (Weiter).
   Das Feld **Servicekonto** wird basierend auf dem von Ihnen ausgewählten Provider ausgefüllt, und eine Liste der ermittelten Rechenzentren wird angezeigt. Wenn keine Rechenzentren angezeigt werden, klicken Sie auf **Rechenzentren erkennen**, um sie zu suchen. Weitere Detailinformationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
4. Wenn die Rechenzentren angezeigt werden, wählen Sie die Rechenzentren aus, die in das Cloud-Konto einbezogen werden sollen, und klicken anschließend auf **Speichern**.

   Hinweis:

   - Wählen Sie nur die LDCs/Regionen aus, in denen Ihre Infrastrukturressourcen vorhanden sind. Wenn Sie in diesen neuen Rechenzentren nicht über Ressourcen verfügen, schließen Sie diese aus, während Sie die vollständige Erkennung durchführen.
   - Um Ressourcen in Regionen/LDCs wie Nordamerika (USA Ost, USA West und Zentralkanada), Südamerika, Europa, Afrika, Naher Osten und Asien-Pazifik zu erkennen, lösen Sie eine Zugriffsanforderung auf die erforderlichen Endpunkte beim GCP Support aus.

   Das Dashboard „Cloud-Konto“ wird angezeigt. Die ausgewählten Rechenzentren werden auf der Registerkarte **Rechenzentren** angezeigt.
5. Klicken Sie auf ein Rechenzentrum.
   Die folgenden Listen werden angezeigt:
   - **Ressourcen**: Cloud-Ressourcen für das aktuelle Rechenzentrum. Führen Sie Discovery aus, um die CMDB für das Rechenzentrum und die Registerkarte auszufüllen. Weitere Informationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kapazitätsgrenzen**: Grenzwerte für virtuelle CPUs, virtuelle Netzwerke, Speicher-Volume-Größe und andere Services. Weitere Informationen finden Sie unter Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen.
- **Discovery-Protokoll**: Mit dem Prozess wird ein Protokolldatensatz für jede Aktion im Zusammenhang mit einem Discovery-Status erstellt.

6. Wiederholen Sie den Vorgang, um so viele Servicekonten wie erforderlich hinzuzufügen.

Erstellen Sie Microsoft Azure Anmeldeinformationen für den Abrechnungsdownload

Definieren Sie den geplanten Auftrag, mit dem unter Verwendung eines MID-Servers regelmäßig Abrechnungsdaten vom Provider heruntergeladen werden. Von Cloud Provisioning and Governance werden die Daten in einer Kostentabelle gespeichert und die Informationen zum Erstellen von Berichten verwendet.

Vorbereitungen

Wichtig:

Ab Release Vancouver ist das Dashboard „Abrechnungen“ nicht mehr verfügbar, wenn Sie die Anwendung ServiceNow Store Cloud-Einblicke heruntergeladen und aktiviert haben. Folgende Änderungen finden statt:

- Sie werden standardmäßig zur Homepage Cloud-Einblicke umgeleitet.
- Das Widget „Dashboard anzeigen“ im Cloud-Benutzerportal wird durch das Widget „Ressourcen anzeigen“ ersetzt.
- Das Widget „Aktuelle Monatsausgaben“ und das Widget „Budget“ im Cloud-Benutzerportal zeigen keine Daten an, wenn Cloud-Einblicke in der Instanz aktiviert ist.

Wenn Sie die Anwendung Cloud-Einblicke aktiviert haben, können Sie nur zum Abrechnungs-Dashboard navigieren, wenn Sie Cloud Provisioning and Governance in einer domänengetrennten Instanz verwenden.

Sie müssen über einen API-Zugriffsschlüssel-Anmeldeinformationen für ein MicrosoftMicrosoft Azure Event Hubs Enterprise Agreement EA für alle Azure -Accounts verfügen, für die Sie Abrechnungsinformationen erhalten möchten.

Erforderliche Rolle: sn_cmp.cloud_governor

Warum und wann dieser Vorgang ausgeführt wird

Während des Downloadvorgangs für die Abrechnung werden alle Ressourcen in das System abgerufen. Azure Datenbanken werden in der Tabelle Datenbank [cmdb_ci_database] platziert.

Prozedur

1. Erstellen Sie einen geheimen Clientschlüssel, indem Sie zur Seite „Übersicht“ der zuvor bereitgestellten Serviceprinzipalanwendung navigieren.

   a. Wählen Sie im linken Bereich **Zertifikate und Geheimnisse**aus.

   b. Wählen Sie im Abschnitt Geheime Clientschlüssel die **Option Neuer geheimer Clientschlüssel**aus.

   c. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Beschreibung	Beschreibung des geheimen Clientschlüssels. Beispiel: `Geheimer Clientschlüssel für MyServicePrincipal`.
Läuft ab	Ablaufzeitraum, der Ihren Anforderungen entspricht. Zum Beispiel `6 Monate`, `12 Monate`, `24 Monate`oder `Nie`.

d. Wählen Sie **Hinzufügen**.

Nach dem Hinzufügen des geheimen Clientschlüssels wird ein Wert generiert und angezeigt.

Hinweis: Kopieren Sie diesen Wert sofort, da er nicht erneut angezeigt würde. Dies ist Ihr Client-Geheimnis (Zugriffsschlüssel).

2. Kopieren Sie die Anwendungs-ID (Client) und die Verzeichnis-ID (Mandant) zur späteren Verwendung.
3. Weisen Sie dem Serviceprinzipal eine Rolle zu.
   a. Wählen Sie im linken Bereich **Azure Active Directory**aus.
   b. Wählen Sie **Rollen und Administratoren**aus.
   c. Wählen Sie **Alle Rollen** aus, und suchen Sie die Rolle, die Sie zuweisen möchten.
   d. Wählen Sie die Rolle und dann **Zuweisung hinzufügen**aus.
   e. Suchen Sie Ihren Serviceprinzipal anhand seines Namens, wählen Sie ihn aus, und wählen Sie dann **Hinzufügen**aus.
4. Rufen Sie eine Abonnement-ID ab, indem Sie **Abonnements**auswählen.
   a. Wählen Sie das Abonnement aus, das Sie verwenden möchten.
   b. Kopieren Sie die Abonnement-ID von der Seite „Abonnementübersicht“.

Downloadgröße von Microsoft Azure-Abrechnungsdaten konfigurieren

Ein einzelner Satz Cloud Billing-Daten kann umfangreich sein. Vom MID-Server werden die Daten daher in verwaltbaren Blöcken an die ECC-Warteschlange gesendet. Optional können Sie eine Systemeigenschaft so konfigurieren, dass die Größe der einzelnen Blöcke begrenzt wird. So vermeiden Sie Leistungsprobleme, die durch die Übertragung großer Datenmengen verursacht werden.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur
1. Öffnen Sie die Tabelle „Systemeigenschaften“, indem Sie im Anwendungsfilter `sys_properties.list` eingeben.
2. Filtern Sie die Liste, um die Eigenschaft `sn_cmp.billing.page_size` zu öffnen. Der Standardwert ist 3 MB.
3. Modifizieren Sie den Wert nach Bedarf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern. Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Höchstwert beträgt 5 MB.

4. Speichern Sie die Eigenschaft.

Setup-Leitfaden für Tag 1 für Cloud Provisioning and Governance: Google Cloud Connector

Zur Ersteinrichtung der Anwendung ServiceNow® Google Cloud Connector führen Sie die Schritte in diesem Setupleitfaden für „Tag 1“ durch. Achten Sie darauf, die Schritte in der richtigen Reihenfolge auszuführen. Nachdem Sie das Setup für „Tag 1“ durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration für „Tag 2“ je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Zum Einrichten von Google Cloud Platform erforderliche Rollen

- Vorgänge in der Google Cloud Console erfordern die Rolle „Google-Administrator“.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Von Cloud Provisioning and Governance verwendete Begriffe

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet. Bei der Google Cloud Platform werden die bereichsspezifischen Container für virtuelle Ressourcen als Regionen bezeichnet. Im ServiceNow-Clouddatenmodell werden Regionen als Rechenzentren oder logische Rechenzentren (Logical Datacenters, LDCs) bezeichnet. Der Begriff „logisch“ wird zur Verdeutlichung der Tatsache verwendet, dass Cloud Provisioning anbieterunabhängig ist. Alle Infrastrukturen oder Anwendungen, die mit Cloud Provisioning bereitgestellt werden, sind einem Rechenzentrum zugeordnet.

Schneller Überblick über den Setup-Prozess

Ihr Setup-Prozess an „Tag 1“ umfasst folgende Aufgaben:

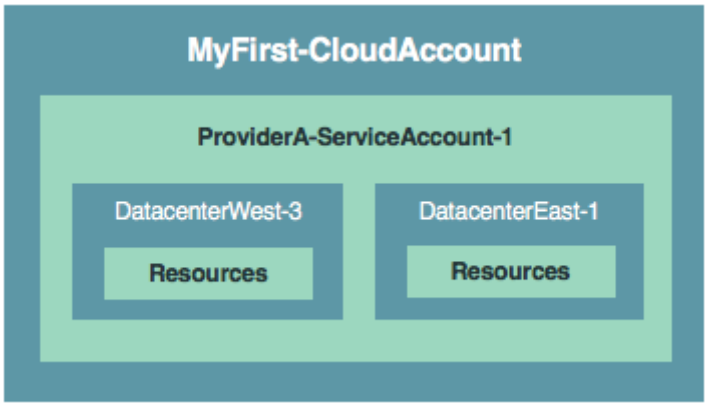
- Falls erforderlich: Die Anwendung Cloud Provisioning and Governance anfordern.
- Laden Sie die App Connector und unterstützende Store-Apps aus dem ServiceNow Store herunter, und aktivieren Sie die Store-Anwendungen.
- Weisen Sie Cloud-Administratoren und Endanwendern die entsprechenden Rollen zu.
- Erfassen Sie im Provider-Portal Ihre Kontoeinstellungen und die Anmeldeinformationen, die beim Discovery-Prozess (über einen MID-Server) dazu verwendet werden, programmgesteuert auf Ihre Provider-Konten zuzugreifen. Ordnen Sie die Kontoeinstellungen und Anmeldeinformationen sicher einem Servicekonto in Cloud Provisioning zu.
- Richten Sie die MID Servers für die sichere Kommunikation mit den Provider-API-Endpunkten ein.
- Richten Sie ein Cloud-Konto ein, um Ihre gesamte verwaltete Cloud-Infrastruktur darzustellen, und richten Sie ein Servicekonto ein, das mit einem Ihrer Provider-Konten funktioniert. Sie geben an, welche Rechenzentren im Servicekonto in das Cloud-Konto aufgenommen werden sollen. (Später, am „Tag 2“, können Sie zusätzliche Cloud-Accounts und Servicekonten vom selben Provider oder anderen Providern einrichten.)
- Zum Füllen der CMDB mit Ressourcendaten für alle Rechenzentren führen Sie den Discovery-Prozess manuell für jedes im Servicekonto enthaltene Rechenzentrum aus. Anschließend konfigurieren Sie Discovery so, dass die Anwendung regelmäßig ausgeführt

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

wird und somit die kontinuierliche Aktualisierung der Daten sichergestellt ist. Ihr Cloud-Konto könnte wie folgt aussehen:

Struktur eines Cloud-Kontos an Tag 1



- Provider bieten Services, mit denen die CMDB automatisch aktualisiert werden kann, wenn für eine Ressource ein Lebenszyklus-Change (erstellt/geändert/beendet) oder Konfigurations-Update durchgeführt wird. Sie können den Service für die direkte Integration mit Cloud Provisioning and Governance konfigurieren.

Aktionen zur Integration Ihrer Google Cloud Platform-Cloud-Konten

Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

1. Abrufen der Cloud Provisioning and Governance: Google Cloud Connector-App aus dem ServiceNow Store

   Die Google Cloud Connector-App erfordert Cloud Provisioning and Governance oder höher. Nachdem Sie Cloud Provisioning and Governance eingerichtet haben, rufen Sie auf der Website des ServiceNow Store die App Google Cloud Connector und die dazugehörigen Plugins und Apps ab.

2. Rollen an Google Cloud Platform-Benutzer zuweisen

   Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

3. Installieren und konfigurieren Sie MID Servers für den Zugriff auf Cloud-Umgebungen

   Damit eine sichere und zuverlässige Kommunikation gewährleistet ist, findet eine Kommunikation zwischen dem Discovery-Prozess und Ihren Cloud Provider-Konten und Cloud-Ressourcen über mindestens einen MID Servers statt. Sie können MID Servers in Ihrem Netzwerk oder in einem Ihrer Cloud-Netzwerke einrichten.

   Hinweis: Daten werden bei der Übertragung zum MID-Server und zwischen dem MID-Server und dem API-Endpunkt verschlüsselt. Um hohe Leistung und Sicherheit zu gewährleisten, sollten Sie mindestens einen MID-Server für jedes verwaltete Rechenzentrum konfigurieren. Konfigurieren Sie einen MID-Server, auch wenn Sie bereits andere MID Servers beim Einrichten von Cloud Provisioning and Governance für einen anderen Cloud Provider konfiguriert haben.

4. Anmeldeinformationen angeben, die Cloud Provisioning and Governance: Google Cloud Connector für den Zugriff auf Google Cloud Platform-Daten verwendet

   Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Um die

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anmeldeinformationen für Discovery verfügbar zu machen, öffnen Sie die Google Cloud Console, um das Google Cloud Platform-Projekt anzugeben, das über programmgesteuerten Zugriff auf Ihre Google Cloud Platform-Daten verfügt. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz.

5. Richten Sie Cloud-Konto und Servicekonto für ein Google Cloud Platform

   Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.

Nächste Schritte

Wenn Sie alle Verfahren für „Tag 1“ und „Tag 2“ in diesem Setupleitfaden abgeschlossen haben, finden Sie unter Cloud Provisioning and Governance-Administrationsleitfaden weitere Informationen zur Verwendung der Anwendung Cloud Provisioning and Governance in Ihrem Unternehmen.

Rollen an Google Cloud Platform-Benutzer zuweisen

Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

Vorbereitungen

Erforderliche Rolle: user_admin oder admin

Prozedur

Weisen Sie Gruppen und Benutzern nach Bedarf die folgenden Rollen zu:

Beschreibender Name und Rollenname	**Beschreibung und Aufgaben**	**Zugriffsberechtigungen in** Cloud Provisioning and Governance
Root-Administrator `[sn_cmp.cmp_root_admin]`	Höchste Anwendungszugriffsebene für Cloud Provisioning and Governance.	Alle
Cloud-Administrator `[sn_cmp.cloud_admin]`	Konfiguriert die Cloud Provisioning and Governance-Anwendung und richtet die Cloud-Infrastruktur ein.	Cloud-Infrastruktur: Servicekonten und Cloud-Konto Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	**Beschreibung und Aufgaben**	**Zugriffsberechtigungen in** Cloud Provisioning and Governance
		• IBM Cloud-Update • VMware-Events
Kontrolle `[sn_cmp.cloud_governor]`	Überwacht die gesamte Cloud-Nutzung und setzt die Einhaltung der Regeln, Kontingente und Richtlinien der Organisation durch. Verwaltet auch Tags und Berechtigungen für verschiedene Objekte.	Governance: • Richtlinien • Pools • Kontingente • Berechtigungen
Service Designer `[sn.cmp.cloud_service_designer]`	Erstellt Blaupausen, ARM- und CloudFormation-Vorlagen und Katalogelemente.	Cloud-Servicedesign: • Cloud-Vorlagen • Blaupausen • Blaupausenkatalogelemente • Ressourcenblöcke
Cloud-Benutzer `[sn_cmp.cloud_service_user]`	Fordert Stapel und Ressourcen an und verwaltet sie.	Cloudbenutzerportal. Wenn Sie die Rolle einer Gruppe zuweisen, teilen sich alle Mitglieder der Gruppe die Kontingentbeschränkungen und den Besitz bestimmter Ressourcen. Sie können auf alle Aufgabendatensätze zugreifen, die Ihnen oder anderen zugewiesen sind, wenn Sie die Rolle „Cloud-Service-Benutzer“ innehaben.
Cloud-Betreiber `[sn_cmp.cloud_operator]`	Überwacht die Cloud Provisioning and Governance-Anwendung und behebt Probleme damit.	Dashboards und Berichte: • Dashboard für Cloud-Vorgänge • Cloud-Ursachenanalyse • Cloud-Orchestrierungspfad • Cloud-API-Pfad
Cloud-Event-Integration `[sn_cmp.cloud_event_integration]`	Autorisiert den Zugriff auf die Instanz für externe Services, mit denen die CMDB bei Auftreten von Cloud-Events automatisch aktualisiert wird.	Cloud-Infrastruktur: • Servicekonten und Cloud-Konto • Netzwerke und IPAM

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
Hinweis: Von IBM Cloud Connector nicht unterstützt	Diese Rolle gewährt den Zugriff auf den REST-Endpunkt des Cloud Events.	Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • VMware-Events
Cloud-Gruppenadministrator `[sn_cmp.cloud_group_admin]`	Gewährt Administrator-Zugriff für alle Gruppen, denen Sie angehören.	

Zugehörige Informationen

Einer Gruppe eine Rolle zuweisen

Einem Benutzer eine Rolle zuweisen

Anmeldeinformationen angeben, die Cloud Provisioning and Governance: Google Cloud Connector für den Zugriff auf Google Cloud Platform-Daten verwendet

Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Um die Anmeldeinformationen für Discovery verfügbar zu machen, öffnen Sie die Google Cloud Console, um das Google Cloud Platform-Projekt anzugeben, das über programmgesteuerten Zugriff auf Ihre Google Cloud Platform-Daten verfügt. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz.

Vorbereitungen

Erforderliche Rollen:

- Vorgänge in der Google Cloud Console erfordern die Rolle „Google-Administrator“.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Warum und wann dieser Vorgang ausgeführt wird

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die Anwendung ServiceNow mehrere Cloud-Anbieter unterstützt, verwendet die App allgemeine Namen für die Einstellungen.

Prozedur

1. Wenn Sie bereits die Anmeldeinformationen generiert haben, die Cloud Provisioning and Governance: Google Cloud Connector verwenden soll, fahren Sie mit dem letzten Schritt fort.
   Andernfalls fahren Sie mit dem nächsten Schritt fort.
2. Wählen Sie im Google Cloud Console-Dashboard das Projekt aus.
3. Navigieren zu **APIs und Services** > **Anmeldeinformationen**.
4. Klicken Sie auf der Registerkarte **Anmeldeinformationen** auf **Anmeldeinformationen erstellen** > **Serviceaccountschlüssel**, und erstellen Sie dann den Schlüssel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

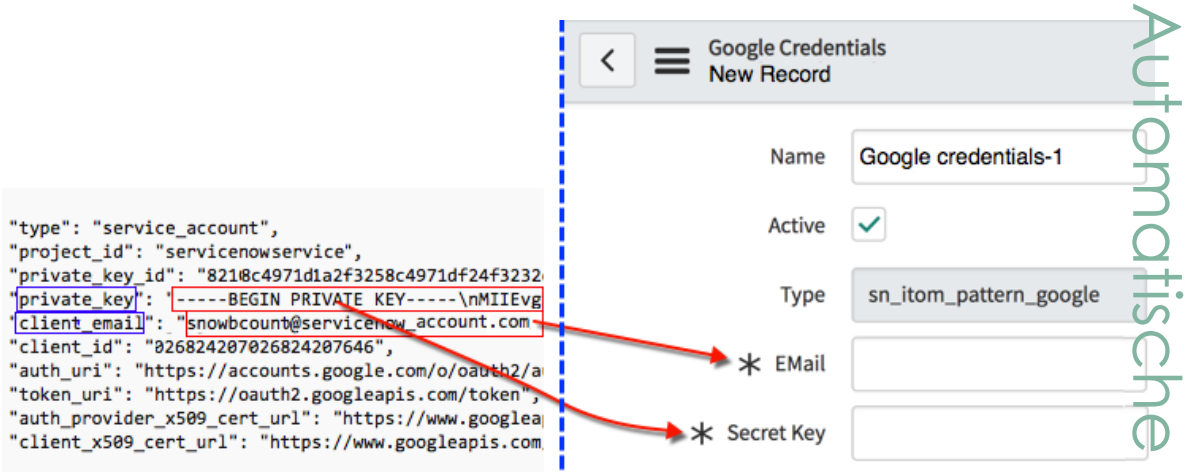
Geben Sie den **JSON-**-Schlüsseltyp an.

5. Identifizieren Sie die Anmeldeinformationen, die Google Cloud Connector und Discovery auf Ihrer Instanz für den Zugriff auf Google Cloud Platform-Daten verwenden sollen:

   a. Öffnen Sie die JSON-Datei in einem Texteditor.

   b. Navigieren Sie im Cloud-Administrationsportal zu **Verwalten** > **Anmeldeinformationen**, klicken Sie auf **Neu**, und wählen Sie **Google-Anmeldeinformationen**aus.

   c. Geben Sie den **Namen** der Anmeldeinformationen an, die bei der Instanz registriert werden sollen.
   Geben Sie beispielsweise `Google credentials-1` ein, und kopieren Sie dann die Werte aus der JSON-Schlüsseldatei in die Formularfelder. Fügen Sie den Wert von `private_key` in das Feld **Geheimer Schlüssel** und den Wert von `client_email` in das Feld **E-Mail** ein.



   d. Wählen Sie die Checkbox **Aktiv** aus, um die Anmeldeinformationen zu verwenden, und klicken Sie dann auf **Absenden**.

Richten Sie Cloud-Konto und Servicekonto für ein Google Cloud Platform

Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Vorbereitungen

Erforderliche Rolle: keine

- Laden Sie den Google Cloud Connector aus dem ServiceNow® Store herunter, und aktivieren Sie ihn.
- Vorgänge in der Google Cloud Console erfordern die Rolle „Google-Administrator“.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

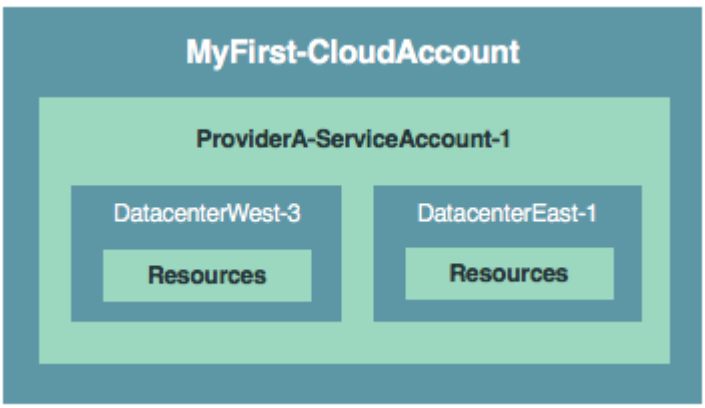
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

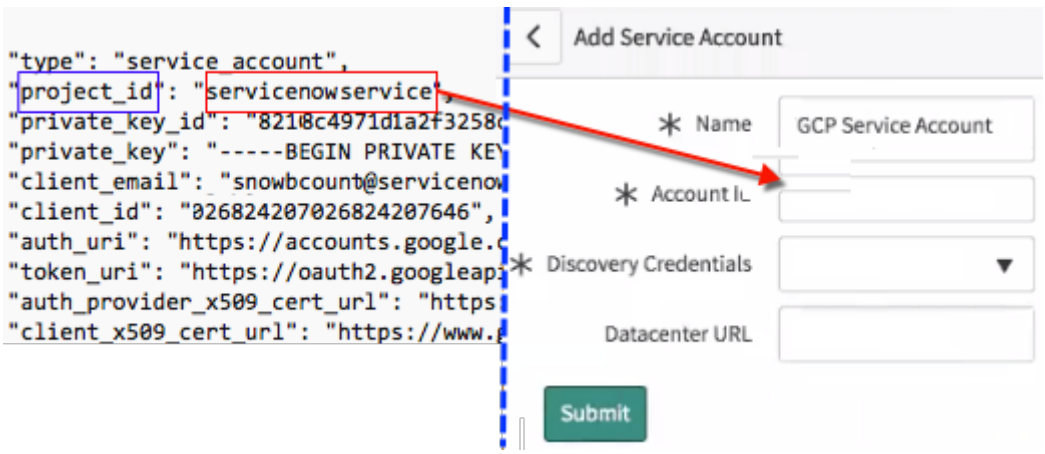
Wenn Sie das Setup für „Tag 1“ abgeschlossen haben, sieht Ihr Cloud-Konto möglicherweise so aus:

Struktur eines Cloud-Kontos an Tag 1



Prozedur

1. Navigieren Sie im Cloud-Adminportal zu **Verwalten** > **Cloud-Accounts**.
2. Wählen Sie das Cloud-Konto aus, oder erstellen Sie es:
   - Wählen Sie ein vorhandenes Cloud-Konto aus:
     a. Klicken Sie auf der Seite des Cloud-Kontos auf **Konfigurieren**.
     b. Klicken Sie auf der Seite „Allgemeine Informationen“ auf **Weiter**, und fahren Sie dann mit dem nächsten Schritt fort.
   - Cloud-Konto erstellen:
     a. Klicken Sie auf der Seite „Allgemeine Informationen“ auf **Neu**, und geben Sie dann einen eindeutigen und aussagekräftigen **Namen** und eine **Beschreibung** für das Cloud-Konto ein.
     b. Provider auswählen.
     c. Klicken Sie auf **Weiter**, und fahren Sie dann mit dem nächsten Schritt fort.
3. Erstellen Sie auf der Seite „Rechenzentren“ ein Servicekonto: Klicken Sie neben dem Feld **Servicekonto** auf das **+**, und füllen Sie dann das Formular für Servicekonto aus.
4. Kopieren Sie aus der JSON-Schlüsseldatei, die Servicekonto zugeordnet ist, den Wert für **project_id** in das Feld **Konto-ID**.



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Feld **Discovery-Anmeldeinformationen** die entsprechenden Anmeldeinformationen für das Servicekonto aus.
   Dies sind die Anmeldeinformationen, die Sie im Anmeldeinformationen angeben, die Cloud Provisioning and Governance: Google Cloud Connector für den Zugriff auf Google Cloud Platform-Daten verwendet-Vorgang generiert haben.
6. Lassen Sie das Feld **Rechenzentrums-URL** leer.
7. Füllen Sie die restlichen Felder aus:

Feld	Beschreibung
Rechenzentrumstyp	Wählen Sie **Google Cloud Platform Datacenter** (Google Cloud Platform-Rechenzentrum) aus.
Status der Rechenzentrumserkennung	Wählen Sie **Google Cloud Platform Datacenter** (Google Cloud Platform-Rechenzentrum) aus.
Sollte Events abrufen	Aktiviert Cloud Provisioning and Governance zum Sammeln von Events von Ressourcentypen in Google-Projekt-LDCs in der `sn_cmp_cloud_event_list` .

8. Klicken Sie auf **Absenden**, um das Servicekonto zu erstellen.
9. Klicken Sie auf **Rechenzentren erkennen**
10. Wenn die Rechenzentren angezeigt werden, wählen Sie die Rechenzentren aus, die in das Cloud-Konto einbezogen werden sollen, und klicken anschließend auf **Speichern**.

    Hinweis:

    - Wählen Sie nur die LDCs/Regionen aus, in denen Ihre Infrastrukturressourcen vorhanden sind. Wenn Sie in diesen neuen Rechenzentren nicht über Ressourcen verfügen, schließen Sie diese aus, während Sie die vollständige Erkennung durchführen.
    - Um Ressourcen in Regionen/LDCs wie Nordamerika (USA Ost, USA West und Zentralkanada), Südamerika, Europa, Afrika, Naher Osten und Asien-Pazifik zu erkennen, lösen Sie eine Zugriffsanforderung auf die erforderlichen Endpunkte beim GCP Support aus.

    Das Dashboard „Cloud-Konto“ wird angezeigt. Die ausgewählten Rechenzentren werden auf der Registerkarte **Rechenzentren** angezeigt.
11. Klicken Sie auf ein Rechenzentrum.
    Die folgenden Listen werden angezeigt:
    - **Ressourcen**: Cloud-Ressourcen für das aktuelle Rechenzentrum. Führen Sie Discovery aus, um die CMDB für das Rechenzentrum und die Registerkarte auszufüllen. Weitere Informationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Kapazitätsgrenzen**: Grenzwerte für virtuelle CPUs, virtuelle Netzwerke, Speicher-Volume-Größe und andere Services. Weitere Informationen finden Sie unter Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen.
- **Discovery-Protokoll**: Mit dem Prozess wird ein Protokolldatensatz für jede Aktion im Zusammenhang mit einem Discovery-Status erstellt.

12. Wiederholen Sie den Vorgang, um so viele Servicekonten wie erforderlich hinzuzufügen.

Nächste Maßnahme
Nachdem Sie alle Verfahren in dieser Ersteinrichtung für „Tag 1“ abgeschlossen haben, können Sie zusätzliche Cloud-Accounts und Servicekonten erstellen, um Ihre Cloud-Infrastruktur zu organisieren und aufzuteilen.

Zugehörige Informationen

Zusätzliches Cloud-Konto einrichten

(Optional) Fügen Sie ein Google Cloud Platform Servicekonto zu hinzu Cloud-Konto

Erkennung von Google Cloud Platform

(Optional) Fügen Sie ein Google Cloud Platform Servicekonto zu hinzu Cloud-Konto

Im Rahmen des Tag-1-Setups von Cloud Provisioning and Governance haben Sie ein Servicekonto zum Cloud-Konto hinzugefügt. Um Ihre Infrastruktur aufzuteilen oder verschiedene Rechenzentren einzubeziehen, können Sie ein weiteres Servicekonto hinzufügen. Ein bestimmtes Rechenzentrum kann jedoch nicht in mehr als einem Servicekonto in einem Cloud-Konto ausgewählt werden.

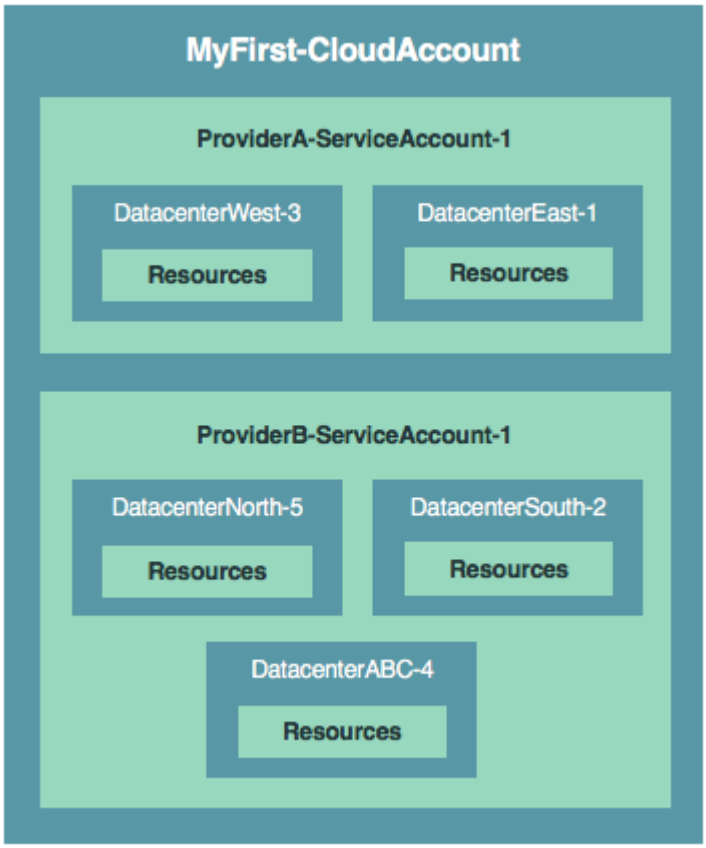
Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.

In diesem Beispiel haben Sie ein Servicekonto mit dem Namen **ProviderB-ServiceKonto-1** hinzugefügt und drei Rechenzentren zur Einbindung in das Cloud-Konto ausgewählt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

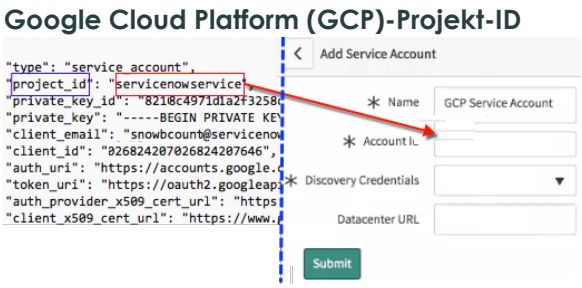
Servicekonto mit drei ausgewählten Rechenzentren



Wichtig: In einem Cloud-Konto können Sie kein bestimmtes Rechenzentrum in zwei verschiedenen Servicekonten auswählen.

Prozedur

1. Navigieren zu **Cloud-Adminportal** > **Service-Accounts**.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und aussagekräftigen **Namen** ein, und füllen Sie dann das Formular aus.
3. Füllen Sie die restlichen Felder aus:

Feld	Beschreibung
Konto-ID	Kopieren Sie aus der JSON-Schlüsseldatei, die Servicekonto zugeordnet ist, den W **project_id** in das Feld **Konto-ID**. 
Discovery-Anmeldeinformationen	Wählen Sie die entsprechenden Anmeldeinformationen für das Servicekonto aus. Informationen zum Generieren oder Abrufen der Anmeldeinformationen finden Si

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Anmeldeinformationen angeben, die Cloud Provisioning and Governance: Goog Connector für den Zugriff auf Google Cloud Platform-Daten verwendet.
Rechenzentrums-URL	Lassen Sie das Feld **Rechenzentrums-URL** leer.
Rechenzentrumstyp	Wählen Sie **Google Cloud Platform Datacenter** (Google Cloud Platform-Rechenze
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Rechenzentrum.

4. Klicken Sie auf **Aktualisieren** oder **Absenden**.
   Das Servicekonto wird vom System erstellt, und es wird die Liste aller erkannten Rechenzentren angezeigt.
5. Wiederholen Sie den Vorgang, um so viele Servicekonten wie erforderlich hinzuzufügen.

Setup-Leitfaden für Tag 1 für VMware auf Cloud Provisioning and Governance

Zur Ersteinrichtung von Cloud Provisioning and Governance führen Sie die Schritte in diesem Setupleitfaden für „Tag 1“ durch. Achten Sie darauf, die Schritte in der richtigen Reihenfolge auszuführen. Nachdem Sie das Setup für „Tag 1“ durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration für „Tag 2“ je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Fordern Sie die Anwendung Cloud Provisioning and Governance an

Die Anwendung Cloud Provisioning and Governance ist als separates Abonnement verfügbar und erfordert das Cloud Provisioning and Governance-Plugin (com.snc.cloud.mgmt). Weitere Informationen finden Sie unter Die Anwendung Cloud Provisioning and Governance anfordern.

Zum Einrichten von Cloud Provisioning and Governance erforderliche Rollen

- Vorgänge in der VMware-Konsole erfordern die Rolle „VMware-Administrator“.
- Vorgänge in Cloud Provisioning and Governance erfordern die Rolle „sn_cmp.cloud_admin“.

Von Cloud-Management verwendete Begriffe

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet.

Schneller Überblick über den Setup-Prozess

Der Setup-Prozess umfasst folgende Aufgaben:

- Falls erforderlich: Die Anwendung Cloud Provisioning and Governance anfordern.
- Weisen Sie Cloud-Benutzern die entsprechenden Rollen zu.
- Richten Sie die MID Servers für die sichere Kommunikation mit den Provider-API-Endpunkten ein.
- Erfassen Sie im Provider-Portal Ihre Kontoeinstellungen und die Anmeldeinformationen, die beim Discovery-Prozess (über einen MID-Server) dazu verwendet werden, programmgesteuert auf Ihre Provider-Konten zuzugreifen. Ordnen Sie die

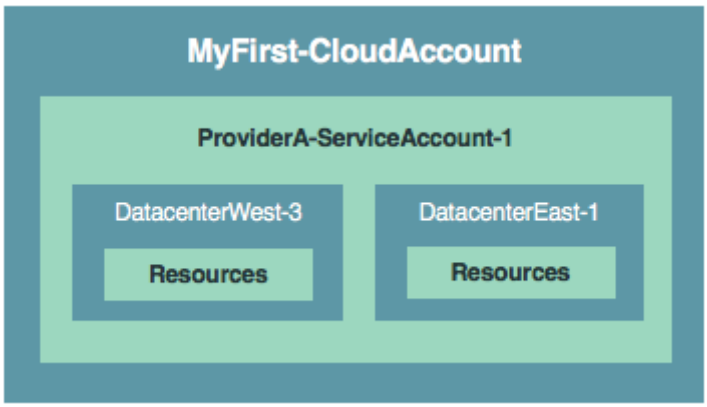
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontoeinstellungen und Anmeldeinformationen sicher einem Servicekonto in Cloud Provisioning and Governance zu.

- Richten Sie ein Cloud-Konto ein, um Ihre gesamte verwaltete Cloud-Infrastruktur darzustellen, und richten Sie ein Servicekonto ein, das mit einem Ihrer Provider-Konten funktioniert. Sie geben an, welche Rechenzentren im Servicekonto in das Cloud-Konto aufgenommen werden sollen. (Später, am „Tag 2“, können Sie zusätzliche Cloud-Accounts und Servicekonten vom selben Provider oder anderen Providern einrichten.)
- In Cloud Provisioning werden CMDB-Daten dafür verwendet, Benutzer beim Anfordern und Verwalten von Cloud-Ressourcen und beim Verwalten der Cloud-Infrastruktur zu unterstützen. Zum Füllen der CMDB mit Ressourcendaten für alle Rechenzentren führen Sie den Discovery-Prozess manuell für jedes im Servicekonto enthaltene Rechenzentrum aus. Anschließend konfigurieren Sie Discovery so, dass die Anwendung regelmäßig ausgeführt wird und somit die kontinuierliche Aktualisierung der Daten sichergestellt ist. Ihr Cloud-Konto könnte wie folgt aussehen:

Struktur eines Cloud-Kontos an Tag 1



- Provider bieten Services, mit denen die CMDB automatisch aktualisiert werden kann, wenn für eine Ressource ein Lebenszyklus-Change (erstellt/geändert/beendet) oder Konfigurations-Update durchgeführt wird. Sie können den Service für die direkte Integration mit Cloud Provisioning and Governance konfigurieren.

Aktionen zur Integration vom Cloud Provisioning and Governance in Ihre VMware Cloud-Konten

Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

1. Weisen Sie VMware Anwendern von Rollen zu Cloud Provisioning and Governance

   Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

2. Anmeldeinformationen und Servicekonto erstellen, der auf Ihre VMware-Daten zugreift

   Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Um die Anmeldeinformationen für Discovery verfügbar zu machen, erstellen Sie zuerst einen Account in der VMware-Konsole. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz. Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen.

3. Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery nutzt die Informationen im Servicekonto dazu, alle dem Anbieter-Account zugeordneten logischen Rechenzentren zu identifizieren.

4. Richten Sie Cloud-Accounts für ein VMware

   Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

5. Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

   Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder des zusammengefassten Speichers ein. Sie können Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

vSphere

- Enterprise oder Enterprise Plus Edition 5.5 oder höher.
- Aktivieren Sie die vSphere-Umgebung für verteilte Ressourcenplanung (Distributed Resource Scheduling, DRS).
- Richten Sie Datenspeicher in Speicher-DRS (Storage DRS) ein.

Lesen und ändern Sie bei der Bereitstellung von virtuellen Computern unter Windows die genannten Anpassungsspezifikationen.

ESXi-Hosts

Wenn die IP-Adresse eines virtuellen Computers manuell mithilfe eines Skripts oder Post-Init-Skripts festgelegt wird, das auf der VM ausgeführt wird, müssen Sie HTTPS-Datenverkehr zwischen dem MID-Server und dem ESXi-Host für die VM zulassen.

Aktivieren Sie die NTP-Zeitsynchronisierung. Aktivieren Sie den NTP-Client für den Hypervisor auf dem vSphere-Webclient. Weitere Informationen finden Sie in der vSphere-Dokumentation .

vCenter Server-Anforderungen

vCenter 5.5 oder 6.0 Standard oder Foundation Edition.

vCenter-Zugriffsanforderungen

Mindestberechtigungen für den Benutzer, der über die Instanz eine Verbindung zu vSphere herstellt:

- Datenspeicher: Alle
- Datenspeicher-Cluster: Alle
- Ordner: Erstellen, Löschen
- Global: Aufgabe abbrechen, Lizenz
- Host > Lokale Vorgänge: Virtuelle Computer erstellen/löschen/neu konfigurieren
- Profilgesteuerte Speicherung: Alle
- Netzwerk: Netzwerk zuweisen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Ressource: Empfehlung anwenden; virtuelle Computer erstellen/ändern/ zuweisen/entfernen
- Virtuelle Computer: Alle

vCenter-Anmeldeinformationen

- Anwendername
- Passwort
- URL oder IP-Adresse des vCenter-Servers, auf den von der Instanz über den MID-Server zugegriffen wird
- vCenter-Instanz-UUID. Unter Anmeldeinformationen und Servicekonto erstellen, der auf Ihre VMware-Daten zugreift finden Sie Anweisungen zum Abrufen der UUID.

Nächste Schritte

Wenn Sie alle Verfahren für „Tag 1“ und „Tag 2“ in diesem Setupleitfaden abgeschlossen haben, finden Sie unter Cloud Provisioning and Governance-Administrationsleitfaden weitere Informationen zur Verwendung der Anwendung Cloud Provisioning and Governance in Ihrem Unternehmen.

Weisen Sie VMware Anwendern von Rollen zu Cloud Provisioning and Governance

Sie weisen den Benutzergruppen und einzelnen Benutzern Cloud Provisioning and Governance-Rollen basierend auf Benutzeraktivitäten und Zuständigkeiten zu.

Vorbereitungen

Erforderliche Rolle: user_admin oder admin

Prozedur

Weisen Sie Gruppen und Benutzern nach Bedarf die folgenden Rollen zu:

Beschreibender Name und Rollenname	**Beschreibung und Aufgaben**	**Zugriffsberechtigungen in** Cloud Provisioning and Governance
Root-Administrator `[sn_cmp.cmp_root_admin]`	Höchste Anwendungszugriffsebene für Cloud Provisioning and Governance.	Alle
Cloud-Administrator `[sn_cmp.cloud_admin]`	Konfiguriert die Cloud Provisioning and Governance-Anwendung und richtet die Cloud-Infrastruktur ein.	Cloud-Infrastruktur: Servicekonten und Cloud-Konto Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	**Beschreibung und Aufgaben**	**Zugriffsberechtigungen in** Cloud Provisioning and Governance
		• AWS Config • Azure-Warnung • Google Stackdriver Logging • IBM Cloud-Update • VMware-Events
Kontrolle `[sn_cmp.cloud_governor]`	Überwacht die gesamte Cloud-Nutzung und setzt die Einhaltung der Regeln, Kontingente und Richtlinien der Organisation durch. Verwaltet auch Tags und Berechtigungen für verschiedene Objekte.	Governance: • Richtlinien • Pools • Kontingente • Berechtigungen
Service Designer `[sn.cmp.cloud_service_designer]`	Erstellt Blaupausen, ARM- und CloudFormation-Vorlagen und Katalogelemente.	Cloud-Servicedesign: • Cloud-Vorlagen • Blaupausen • Blaupausenkatalogelemente • Ressourcenblöcke
Cloud-Benutzer `[sn_cmp.cloud_service_user]`	Fordert Stapel und Ressourcen an und verwaltet sie.	Cloudbenutzerportal. Wenn Sie die Rolle einer Gruppe zuweisen, teilen sich alle Mitglieder der Gruppe die Kontingentbeschränkungen und den Besitz bestimmter Ressourcen. Sie können auf alle Aufgabendatensätze zugreifen, die Ihnen oder anderen zugewiesen sind, wenn Sie die Rolle „Cloud-Service-Benutzer“ innehaben.
Cloud-Betreiber `[sn_cmp.cloud_operator]`	Überwacht die Cloud Provisioning and Governance-Anwendung und behebt Probleme damit.	Dashboards und Berichte: • Dashboard für Cloud-Vorgänge • Cloud-Ursachenanalyse • Cloud-Orchestrierungspfad • Cloud-API-Pfad

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Beschreibung und Aufgaben	Zugriffsberechtigungen in Cloud Provisioning and Governance
Cloud-Event-Integration `[sn_cmp.cloud_event_integration]` **Hinweis:** Von IBM Cloud Connector nicht unterstützt	Autorisiert den Zugriff auf die Instanz für externe Services, mit denen die CMDB bei Auftreten von Cloud-Events automatisch aktualisiert wird. Diese Rolle gewährt den Zugriff auf den REST-Endpunkt des Cloud Events.	Cloud-Infrastruktur: • Servicekonten und Cloud-Konto • Netzwerke und IPAM Einstellungen für Provider Services, mit denen die CMDB automatisch aktualisiert wird: • AWS Config • Azure-Warnung • Google Stackdriver Logging • VMware-Events
Cloud-Gruppenadministrator `[sn_cmp.cloud_group_admin]`	Gewährt Administrator-Zugriff für alle Gruppen, denen Sie angehören.	

Zugehörige Informationen

Einer Gruppe eine Rolle zuweisen

Einem Benutzer eine Rolle zuweisen

Anmeldeinformationen und Servicekonto erstellen, der auf Ihre VMware-Daten zugreift

Für den sicheren Zugriff auf Daten in Ihrem Providerkonto muss der Discovery-Prozess entsprechende Anmeldeinformationen bereitstellen. Um die Anmeldeinformationen für Discovery verfügbar zu machen, erstellen Sie zuerst ein Konto in der VMware-Konsole. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Ihrer Instanz.

Vorbereitungen

Erforderliche Rollen:

- VMware-Konsole Administrator
- Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Anmeldeinformationen**.
2. Klicken Sie auf der Registerkarte **Anmeldeinformationen** auf **Neu**, wählen Sie **VMware-Anmeldeinformationen** aus, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Felder des Formulars für VMware-Anmeldeinformationen

Feld	Eingabewert
Name	Eindeutiger und aussagekräftiger Name für die Anmeldeinformationen (z. B. `Cloud Management VMware-Anmeldeinformationen`)
Aktiv	Aktivieren Sie das Kontrollkästchen, um die Anmeldeinformationen zu aktivieren.
Benutzername	Benutzername für den Zugriff auf Ihr vSphere-Konto.
Passwort	Passwort für den Zugriff auf das vSphere-Konto

3. Navigieren zu **Cloud-Adminportal** > **Verwalten** > **Service-Accounts**, klicken Sie auf **Neu**, geben Sie einen eindeutigen und aussagekräftigen **Namen** ein (z. B. `Servicekonto für Cloud-Bereitstellung`), und füllen Sie das Formular aus.

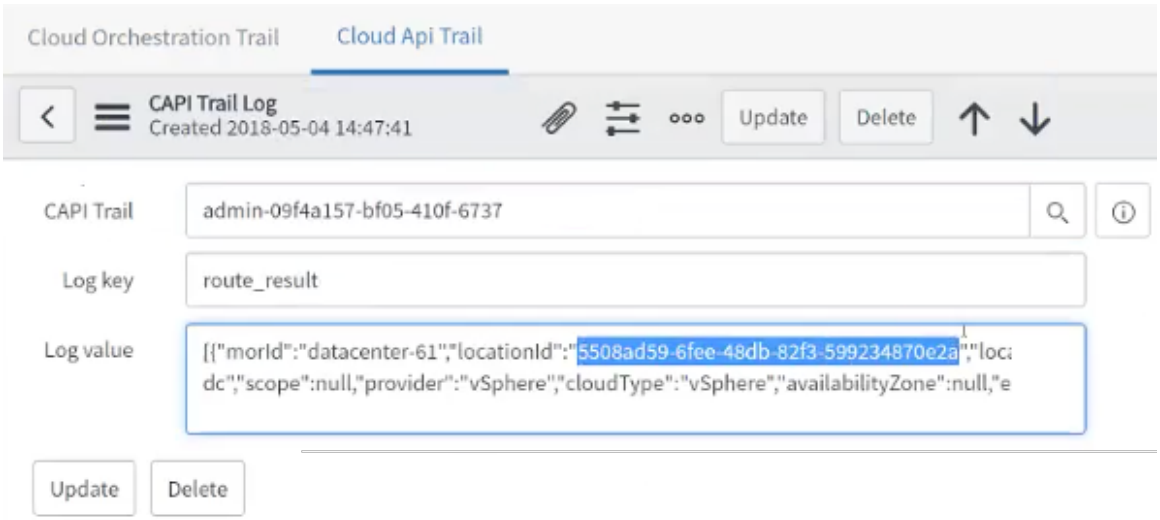
Neuer Service-Account für VMware

Account-ID	Es gibt zwei Methoden, den Wert festzulegen: ◦ Wenn Sie Zugriff auf den Browser für verwaltete Objekte (Managed Object Browser, MOB) für das vCenter haben: Die Konto-ID ist die Instanz-UUID. Öffnen Sie das MOB, und klicken Sie dann auf **Inhalt** > **Über**. Fügen Sie den Wert der Eigenschaft **instanceUuid** in das Feld **Konto-ID** ein. ◦ Wenn Sie nicht auf den Managed Object Browser (MOB) zugreifen können, geben Sie in das Feld **Konto-ID** einen temporären alphanumerischen Text wie `5ca3033a-1290-4a02-8221-2c5f2f29be8b` ein. In einem Schritt nach dieser Tabelle erstellen Sie den tatsächlichen Wert und kehren dann zu diesem Formular zurück, um den temporären Text durch den tatsächlichen Wert zu ersetzen.
Discovery-Anmeldeinformationen	Name der Anmeldeinformationen, die Sie im vorherigen Schritt erstellt haben. Im Beispiel: `Cloud Provisioning VMware Credentials`.
Rechenzentrums-URL	Vollständige URL des vCenters, z. B.: `https://<IP-Adresse>/sdk`.
Datencenter-Typ	Wählen Sie **VMware vCenter-Rechenzentrum [cmdb_ci_vcenter_datacenter]** aus.
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sollte Events abrufen	Aktiviert Cloud Provisioning and Governance zum Sammeln von Events von Ressourcentypen im VMware vCenter-Rechenzentrum in der Liste `sn_cmp_cloud_event_list`.

4. Klicken Sie auf den zugehörigen Link **Rechenzentren erkennen**.
   Mit den Anmeldeinformationen greift Discovery auf das vCenter unter der angegebenen URL zu, um VMware-Rechenzentren zu erkennen.
5. Wenn Sie den UUID-Wert der Instanz im Feld **Konto-ID** verwendet haben, klicken Sie auf **Absenden** und überspringen Sie die verbleibenden Schritte in diesem Verfahren.
   Das System erstellt den Servicekonto und zeigt die Liste aller Servicekonten an.
6. Navigieren Sie im Portal für Cloud-Admin.zu **Betreiben** > **Pfade**.
7. Suchen Sie auf der Registerkarte **Cloud API-Pfad** den Eintrag mit dem Wert **ListDatacenters** für **Methodenname** und dem Wert **vmware-compute** für **Providername** (normalerweise der neueste Eintrag).
   Öffnen Sie den Eintrag.
8. Öffnen Sie in der zugehörigen Liste **CAPI-Pfadprotokolle** den Eintrag **route_result**.
9. Kopieren Sie im Textfeld **Protokollwert** den Wert für **locationId**.
   Dieser Wert ist die **Konto-ID**, die Sie im nächsten Schritt in das Formular einfügen.



10. Navigieren Sie in der Instanz zu **Cloud-Adminportal** > **Verwalten** > **Service-Accounts** und klicken Sie dann auf das Feld Servicekonto, das Sie zuvor erstellt haben (im Beispiel`Cloud Provisioning Serviceaccount`).
11. Fügen Sie den Wert für **locationId** (den Sie aus dem Formular **CAPI-Pfadprotokoll** kopiert haben) in das Feld **Konto-ID** des Formulars ein, und klicken Sie dann auf **Aktualisieren**.
12. Klicken Sie auf **Absenden**.
    Das Servicekonto wird vom System erstellt, und es wird die Liste aller erkannten Rechenzentren angezeigt.

Zugehörige Informationen

Erkennung von VMware-Clouds

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie Cloud-Accounts für ein VMware

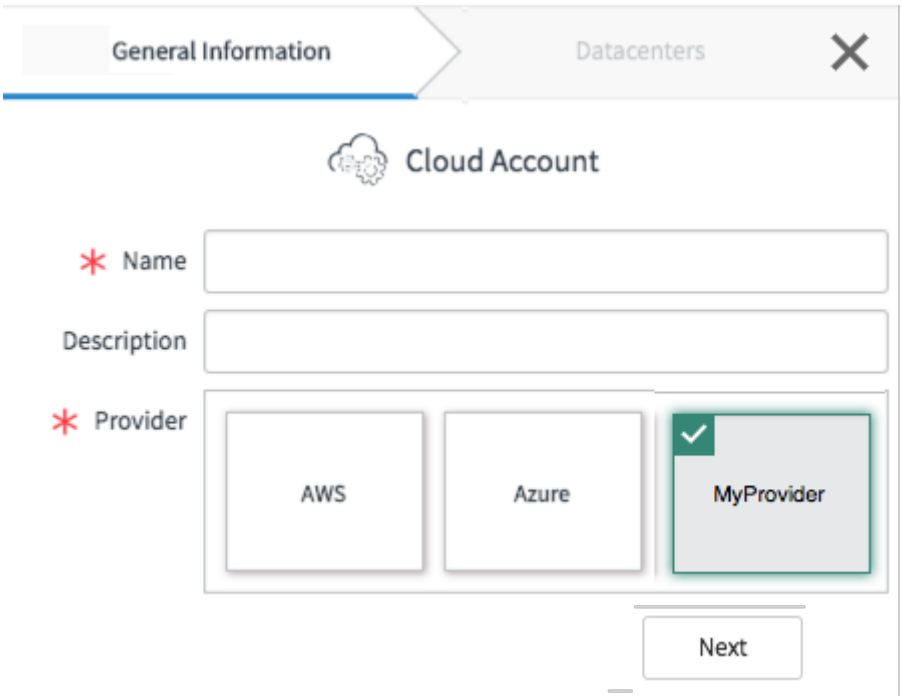
Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Ausführliche Informationen finden Sie unter Cloud-Accounts.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Verwalten** > **Cloud-Accounts**.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** und eine **Beschreibung** ein, und wählen Sie dann den Cloud-**Provider** für das Konto aus (VMware vCenter).



3. Klicken Sie auf **Next** (Weiter).
   Das Feld **Servicekonto** wird basierend auf dem von Ihnen ausgewählten Provider ausgefüllt, und eine Liste der ermittelten Rechenzentren wird angezeigt. Wenn keine Rechenzentren angezeigt werden, klicken Sie auf **Rechenzentren erkennen**, um sie zu suchen. Weitere Detailinformationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
4. Wählen Sie ein oder mehrere Rechenzentren aus, die dem Cloud-Konto zugeordnet werden sollen, klicken Sie auf **Speichern**, und schließen Sie dann das Popup.
   Das Dashboard „Cloud-Konto“ wird angezeigt. Die ausgewählten Rechenzentren werden auf der Registerkarte **Rechenzentren** angezeigt.
5. Klicken Sie auf ein Rechenzentrum.
   Die folgenden Listen werden angezeigt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- **Ressourcen**: Cloud-Ressourcen für das aktuelle Rechenzentrum. Führen Sie Discovery aus, um die CMDB für das Rechenzentrum und die Registerkarte auszufüllen. Weitere Informationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
- **Kapazitätsgrenzen**: Grenzwerte für virtuelle CPUs, virtuelle Netzwerke, Größe des Speichervolume und andere Services. Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen
- **Discovery-Protokoll**: Der Prozess erstellt einen Protokolldatensatz für jede Aktion in einem Rechenzentrum.

Hinweis:

Wenn Sie sich in einer domänengetrennten Instanz befinden, sind nur die Events sichtbar, die zur CMDB aktualisiert wurden und zu Ihrer Domäne gehören. Events erstellen Configuration Items (CIs) in der gleichen Domäne wie das Cloud-Servicekonto, dem sie zugeordnet sind.

Nächste Maßnahme

Wiederholen Sie den Vorgang, um nach Bedarf zusätzliche Cloud-Accounts zu erstellen. Führen Sie Discovery aus, und legen Sie Kapazitätsgrenzen für jedes Rechenzentrum fest.

Fügen Sie ein Rechenzentrum zu einem hinzu Cloud-Konto

Sie können der Cloud-Infrastruktur jederzeit ein logisches Rechenzentrum hinzufügen, das durch einen Cloud-Konto dargestellt wird.

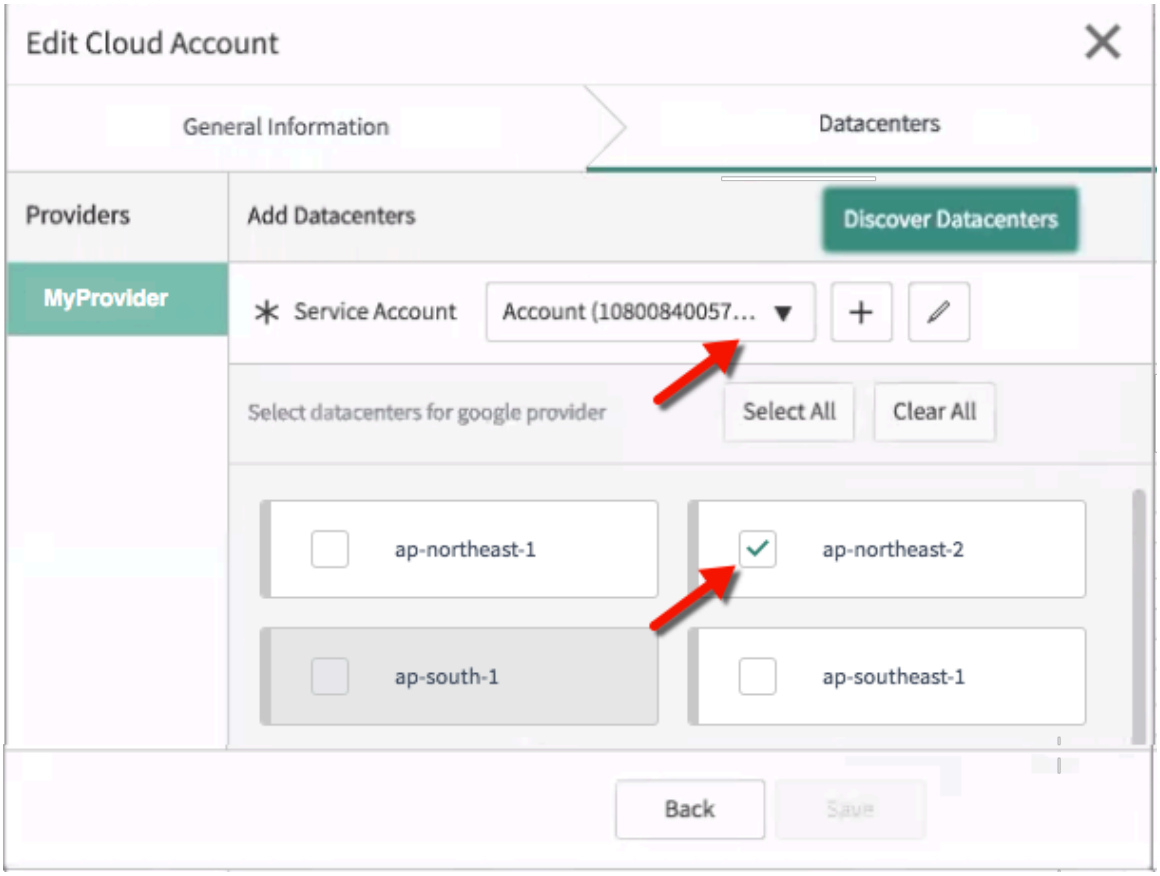
Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Verwalten** > **Cloud-Accounts**.
2. Öffnen Sie einen Cloud-Konto, legen Sie den Status auf **Entwurf** fest, und klicken Sie dann im Formularheader auf **Konfigurieren**.
3. Klicken Sie auf die Registerkarte **Rechenzentren**, und wählen Sie dann das **Servicekonto** aus, der die Anmeldeinformationen enthält, die den Zugriff auf das Provider-Konto mit dem hinzuzufügenden Rechenzentrum ermöglichen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Wenn Sie den Servicekonto auswählen, wird die Liste der erkannten Rechenzentren für den Servicekonto angezeigt.

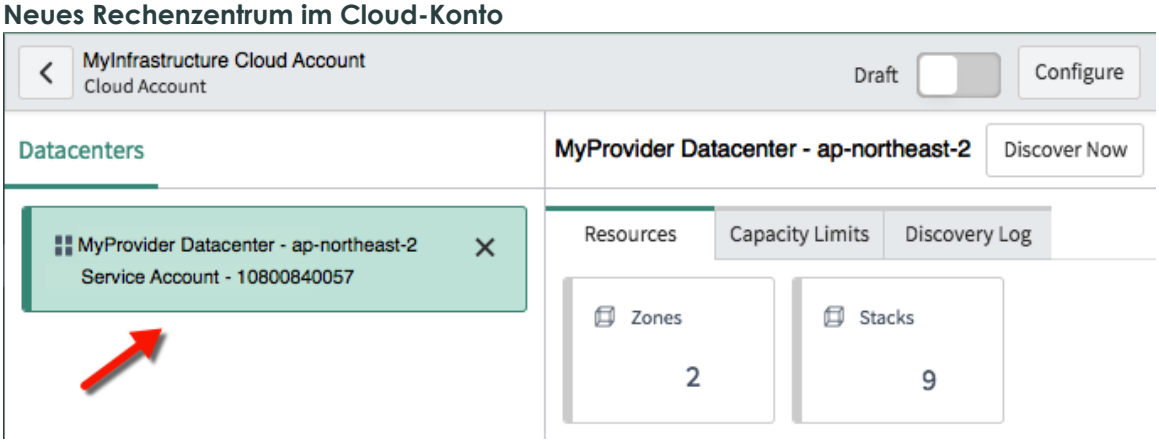
Hinweis: Wenn die erwarteten Rechenzentren nicht angezeigt werden, klicken Sie auf **Rechenzentren erkennen**, um die Liste zu aktualisieren. Discovery wird ausgeführt und zeigt alle mit dem Servicekonto verknüpften Rechenzentren an.

4. Wählen Sie die hinzuzufügenden Rechenzentren aus, und klicken Sie dann auf **Speichern**. Im Beispiel wählen Sie **ap-northeast-2** aus.

Ergebnisse

Die Rechenzentren werden dem Cloud-Konto hinzugefügt und auf der Registerkarte **Rechenzentren** angezeigt. Wenn Discovery ausgeführt wird, werden die Ressourcen im Rechenzentrum auf der Registerkarte „Ressourcen“ angezeigt.

Neues Rechenzentrum im Cloud-Konto



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliches Setup von Cloud Provisioning and Governance an Tag 2

Nachdem Sie das Setup für „Tag 1“ durchgeführt haben, können Sie die optionalen Schritte des Setups und der Konfiguration je nach Bedarf und in beliebiger Reihenfolge durchführen. Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Zusätzliche Setup- und Konfigurationsvorgänge

Detaillierte Anweisungen für die einzelnen Vorgehensweisen finden Sie in dieser Übersicht.

Zusätzliches Cloud-Konto einrichten

Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Planen Sie die Discovery aller Ressourcen in einer Servicekonto

Fügen Sie einen anwenderdefinierten Zeitplan für Discovery hinzu, um alle Ressourcen in jedem Rechenzentrum in einem Servicekonto zu erkennen, und aktualisieren Sie dann die CMDB mit den neuen Informationen.

Sie können die auf der Cloud-Discovery-Zeitplanseite angebotenen Discovery-Zeitpläne verwenden.

Hinweis:

Ab dem Xanadu-Release führen alle neuen Benutzer standardmäßig die musterbasierte Discovery aus. In Szenarien, in denen die neueste Musteranwendung nicht installiert ist, schlägt die Erkennung fehl, und der Systemadministrator wird aufgefordert, die CAPI-basierte Erkennung zu installieren oder zu migrieren.

Durch die Installation von Arbeitsbereich für Cloud-Vorgänge wird die automatische Installation der neuesten Musteranwendung ausgelöst.

Weitere Informationen finden Sie unter Migrieren Sie von CAPI zu Mustern.

Bei Bedarf alle Ressourcen in einem Rechenzentrum erkennen

Sie können jederzeit Discovery für ein Rechenzentrum ausführen, um die CMDB zu aktualisieren.

Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder des zusammengefassten Speichers ein. Sie können Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

Nächste Schritte

Wenn Sie alle Verfahren für „Tag 1“ und „Tag 2“ in diesem Setupleitfaden abgeschlossen haben, finden Sie unter Cloud Provisioning and Governance-Administrationsleitfaden weitere Informationen zur Verwendung der Anwendung Cloud Provisioning and Governance in Ihrem Unternehmen.

Zusätzliches Cloud-Konto einrichten

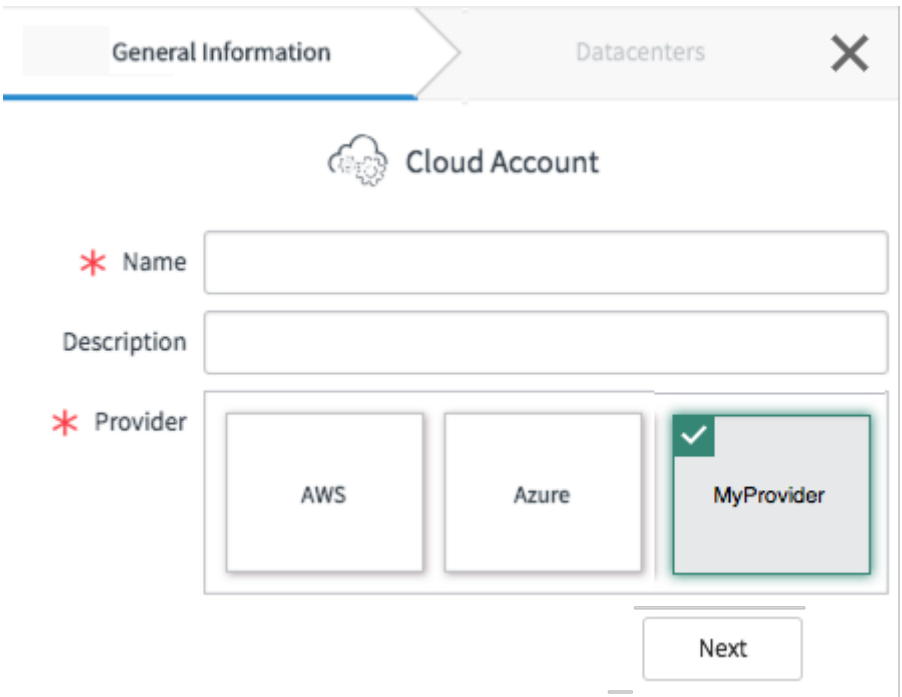
Während der Erstinstallation richten Sie einen Cloud-Konto ein. Zum Organisieren und Aufteilen Ihrer Infrastruktur können Sie zusätzliche Cloud-Accounts einrichten, um verschiedene Provider, Servicekonten oder Rechenzentren einzubeziehen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen. Ausführliche Informationen finden Sie unter Cloud-Accounts.

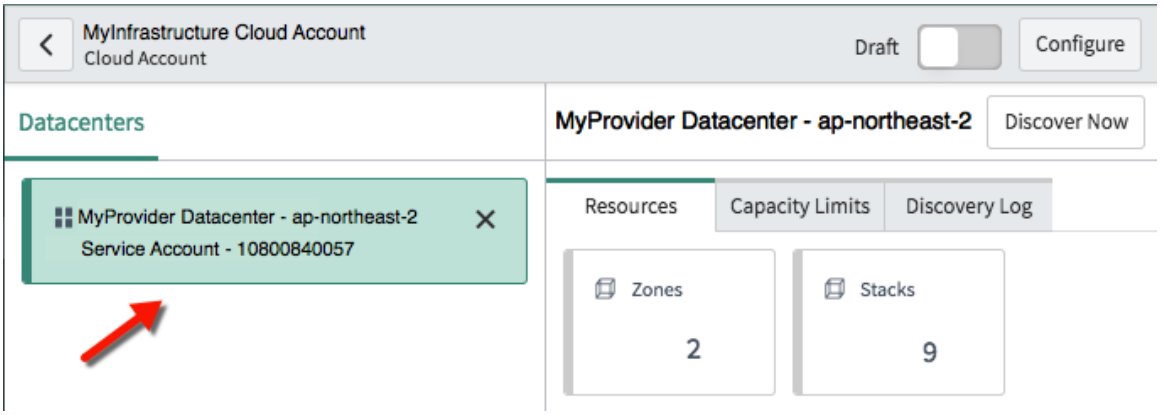
Prozedur
1. Navigieren Sie im Cloud-Administrationsportal zu **Verwalten** > **Cloud-Accounts**.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** und eine **Beschreibung** ein, wählen Sie den Cloud-**Provider** für das Konto aus (im Beispiel **MyProvider**), und klicken Sie dann auf **Weiter**.



   Das Feld **Servicekonto** wird basierend auf dem von Ihnen ausgewählten Provider ausgefüllt.
3. Wählen Sie das entsprechende **Servicekonto** aus.
   Eine Liste der erkannten Rechenzentren wird angezeigt. Wenn keine Rechenzentren angezeigt werden, klicken Sie auf **Jetzt erkennen**. Details siehe Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
4. Wählen Sie alle Rechenzentren aus, die dem Cloud-Konto zugeordnet werden sollen, klicken Sie auf **Speichern**, und schließen Sie dann das Popup.

   Die Rechenzentren werden auf der Registerkarte **Rechenzentren** für den Cloud-Konto angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wenn die Rechenzentren angezeigt werden, wählen Sie die Rechenzentren aus, die in das Cloud-Konto einbezogen werden sollen, und klicken anschließend auf **Speichern**.

   Hinweis:

   - Wählen Sie nur die LDCs/Regionen aus, in denen Ihre Infrastrukturressourcen vorhanden sind. Wenn Sie in diesen neuen Rechenzentren nicht über Ressourcen verfügen, schließen Sie diese aus, während Sie die vollständige Erkennung durchführen.
   - Um Ressourcen in Regionen/LDCs wie Nordamerika (USA Ost, USA West und Zentralkanada), Südamerika, Europa, Afrika, Naher Osten und Asien-Pazifik zu erkennen, lösen Sie eine Zugriffsanforderung auf die erforderlichen Endpunkte beim GCP Support aus.

   Das Dashboard „Cloud-Konto“ wird angezeigt. Die ausgewählten Rechenzentren werden auf der Registerkarte **Rechenzentren** angezeigt.

6. Klicken Sie auf ein Rechenzentrum.
   Die folgenden Listen werden angezeigt:
   - **Ressourcen**: Cloud-Ressourcen für das aktuelle Rechenzentrum. Führen Sie Discovery aus, um die CMDB für das Rechenzentrum und die Registerkarte auszufüllen. Weitere Informationen finden Sie unter Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen.
   - **Kapazitätsgrenzen**: Grenzwerte für virtuelle CPUs, virtuelle Netzwerke, Speicher-Volume-Größe und andere Services. Weitere Informationen finden Sie unter Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen.
   - **Discovery-Protokoll**: Mit dem Prozess wird ein Protokolldatensatz für jede Aktion im Zusammenhang mit einem Discovery-Status erstellt.
7. Wiederholen Sie den Vorgang, um so viele Servicekonten wie erforderlich hinzuzufügen.

Nächste Maßnahme
Wiederholen Sie den Vorgang, um nach Bedarf zusätzliche Cloud-Accounts zu erstellen. Führen Sie Discovery aus, und legen Sie Kapazitätsgrenzen für jedes Rechenzentrum fest.

Verwenden Sie Arbeitsbereich für Cloud-Vorgänge und Muster

Sie können jetzt eine Discovery mit Arbeitsbereich für Cloud-Vorgänge und Muster für Discovery und Service-Mappingplanen und durchführen.

Vorbereitungen
Erforderliche Rolle: Systemadministrator

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Arbeitsbereich für Cloud-Vorgänge ist jetzt als Arbeitsbereich für Cloud-Vorgänge oder CDW bezeichnet.

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Überprüfen Sie, ob *Arbeitsbereich für Cloud-Vorgänge* (CDW) installiert ist.
2. Navigieren zu **Cloud-Adminportal** > **Verwalten** > **Discovery-Zeitpläne** > **Verwalten SieDiscovery-Zeitpläne**.

   Folgen Sie diesen Szenarien für die nächsten Schritte.

Szenario	Nächste Schritte
Cloud-Discovery-Zeitpläne werden für die Systemadministratoranmeldung nicht angezeigt	◦ *Arbeitsbereich für Cloud-Vorgänge* ist nicht installiert. Die Seite mit der Benachrichtigung, dass *Arbeitsbereich für Cloud-Vorgänge* installiert werden muss, wird angezeigt. ◦ Auf der Seite werden Sie aufgefordert, **zum Anwendungsmanager zu wechseln,** um die Installation zuzulassen
Cloud-Discovery-Zeitpläne werden für die Anmeldung als Cloud-Administrator „sn_cmp“ nicht angezeigt	◦ *Arbeitsbereich für Cloud-Vorgänge* ist nicht installiert. Die Seite mit der Benachrichtigung, dass *Arbeitsbereich für Cloud-Vorgänge* installiert werden muss, wird angezeigt. ◦ Auf der Seite werden Sie aufgefordert, sich für die Installation *Arbeitsbereich für Cloud-Vorgänge* von an den Systemadministrator zu wenden.
Cloud-Discovery wird angezeigt	Cloud-Discovery-Zeitpläne werden auf einer neuen Registerkarte Ihres Browsers angezeigt.

3. Stellen Sie sicher, dass die Cloud-Administratorrolle „sn_cmp“ die Rolle „sn_cloud_ops_ws.cloud_ops_admin“ enthält.
4. Navigieren zu **Cloud-Adminportal** > **Verwalten** > **Discovery-Zeitpläne**.
5. Klicken und bestätigen Sie, wenn Discovery-Zeitpläne auf einer neuen Registerkarte geöffnet werden.
6. Stellen Sie sicher, dass der Cloud-Administrator „sn_cmp“ standardmäßig die Seite „Discovery-Zeitpläne“ anzeigen kann.

Nächste Maßnahme

Installieren und verwenden Sie die neueste Version Muster für Discovery und Service-Mappingvon , mindestens Version 1.15, als Standardmechanismus für die Ausführung Discoveryvon .

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

Nachdem Sie ein Servicekonto eingerichtet haben, führen Sie Discovery aus, um die Rechenzentren im Konto auszufüllen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Es muss ein Cloud-Konto mit Servicekonten und zugehörigen Rechenzentren vorhanden sein. Sie müssen Discovery bei Bedarf ausführen, um Rechenzentren zu erkennen, bevor Sie Discovery planen können.
- Verwenden Sie Arbeitsbereich für Cloud-Vorgängeund mindestens Version 1.15 von Muster für Discovery und Service-Mapping aus ServiceNow Store.

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet. Bei der Google Cloud Platform werden die bereichsspezifischen Container für virtuelle Ressourcen als Regionen bezeichnet. Im ServiceNow-Clouddatenmodell werden Regionen als Rechenzentren oder logische Rechenzentren (Logical Datacenters, LDCs) bezeichnet. Der Begriff „logisch“ wird zur Verdeutlichung der Tatsache verwendet, dass Cloud Provisioning anbieterunabhängig ist. Alle Infrastrukturen oder Anwendungen, die mit Cloud Provisioning bereitgestellt werden, sind einem Rechenzentrum zugeordnet.

Sie können Discovery bei Bedarf ausführen.

Wichtig: Verwenden Sie Arbeitsbereich für Cloud-Vorgänge (CDW), um den Discovery-Zeitplan auszuführen. Die UI-Aktion „Rechenzentrum erkennen“ ist veraltet, und der bevorzugte Ansatz besteht in der Einrichtung von Zeitplänen über CDW.

Prozedur

1. Navigieren Sie zur Tabelle „Cloud-Servicekonten“ [cmdb_ci_cloud_service_account_list]. Weitere Informationen zum direkten Navigieren zu einer Tabelle finden Sie unter Direkt zu einer Tabelle navigieren .
2. Wählen Sie den Serviceaccount aus, dessen LDCs erkannt werden sollen.
3. Wählen Sie den zugehörigen Link **Discovery-Zeitplan erstellen aus**.
4. Wählen Sie **Weiter**.
5. Wählen Sie **Rechenzentren aktualisieren**aus.
6. Wählen Sie **Abbrechen**.
7. Wählen Sie den Serviceaccount aus, dessen LDCs Sie erkennen möchten.
   Bei einer erfolgreichen Discovery des Rechenzentrums wird das Statusfeld des Discovery-Rechenzentrums auf `JJJJ-MM-TT HH:MM:SS: Abgeschlossen … Laden Sie dieses Formular neu, um eine aktualisierte Liste mit Rechenzentren anzuzeigen.`

Ergebnisse

Die erkannten Rechenzentren werden in der zugehörigen Liste der logischen Rechenzentren angezeigt.

Zugehörige Informationen

Protokolle für horizontale Erkennung

Planen Sie die Discovery aller Ressourcen in einer Servicekonto

Fügen Sie einen anwenderdefinierten Zeitplan für Discovery hinzu, um alle Ressourcen in jedem Rechenzentrum in einem Servicekonto zu erkennen, und aktualisieren Sie dann die CMDB mit den neuen Informationen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Es muss ein Cloud-Konto mit Servicekonten und zugehörigen Rechenzentren vorhanden sein. Sie müssen Discovery bei Bedarf ausführen, um Rechenzentren zu erkennen, bevor Sie Discovery planen können.
- Verwenden Sie Arbeitsbereich für Cloud-Vorgängeund mindestens Version 1.15 von Muster für Discovery und Service-Mapping aus ServiceNow Store.

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

- Die geplante Cloud-Discovery erkennt nur Rechenzentren, die Teil von Servicekonto sind, wenn der Zeitplan erstellt wird. Wenn seit der Erstellung des Zeitplans Rechenzentren hinzugefügt wurden, erkennt Discovery diese Rechenzentren nicht. Löschen Sie den alten Zeitplan und erstellen Sie jedes Mal einen Zeitplan, wenn sich die Rechenzentren in einem Servicekonto ändern.
- Discovery füllt die CMDB mit den erkannten Ressourcen und aktualisiert die entsprechenden Informationen auf der Registerkarte **Ressourcen**. Sie können sich die Discovery-Ergebnisse auf der Registerkarte **Discovery-Protokoll** ansehen.

Wichtig: Verwenden Sie Arbeitsbereich für Cloud-Vorgänge, um den Discovery-Zeitplan auszuführen. Die UI-Aktion „Rechenzentrum erkennen“ ist veraltet, und der bevorzugte Ansatz besteht in der Einrichtung von Zeitplänen über CDW.

Prozedur

1. Navigieren Sie im **Cloud-Administrationsportal** zu **Verwalten** > **Discovery-Zeitpläne**.
2. Wählen Sie **Cloud-Zeitplan hinzufügen** aus.
3. Wählen Sie auf der Seite „Konto hinzufügen“ den Cloud-**Provider** aus, und geben Sie einen eindeutigen, beschreibenden **Namen** für den Zeitplan ein.
4. Wählen Sie im Abschnitt **„Serviceaccount“Account auswählen**aus, geben Sie den Serviceaccount an, und klicken Sie dann auf **Weiter**.

   Hinweis: Um ein Servicekonto zu erstellen, wählen Sie **Account hinzufügen**, und füllen Sie dann das Formular aus. Einzelheiten hierzu finden Sie unter Vorgang zum Einrichten eines Servicekontos im Setupleitfaden für Tag 1.

5. Geben Sie auf der Seite „Rechenzentren auswählen“ an, welche der Rechenzentren im Servicekonto erkannt werden sollen, indem Sie die zu erkennenden Rechenzentren in die Liste **Ausgewählt** verschieben oder indem Sie **Alle unten aufgeführten Rechenzentren erkennen** auswählen, um alle Rechenzentren in die Liste **Ausgewählt** zu verschieben.
6. Klicken Sie auf **Next (Weiter)**.
7. Auf der Seite „Zeitplan“ erstellen geben Sie den Zeitpunkt und die Häufigkeit der Discovery an.

   Hinweis: Die Einstellung **Laufzeit** verwendet immer die Systemzeitzone.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Discovery Planausführungsoptionen

Häufigkeit	Beschreibung
Bei Bedarf	Wird nicht nach einem Zeitplan ausgeführt. Wählen Sie **Jetzt erkennen**, um Disc Standardoption.
Täglich	Läuft jeden Tag. Verwenden Sie das Feld **Startzeit**, um die Uhrzeit anzugeben.
Wöchentlich	Läuft an einem bestimmten Wochentag. Verwenden Sie das Feld **Startzeit**, um
Monatlich	Läuft an einem bestimmten Tag jedes Monats. Verwenden Sie das Feld **Tag**, um auszuwählen. Verwenden Sie das Feld **Startzeit**, um die Uhrzeit anzugeben. Wer in dem Monat vorkommt, wird der Zeitplan in diesem Monat nicht ausgeführt. W festlegen, wird der Zeitplan im Februar nicht ausgeführt.
Regelmäßig	Wird zu jeder angegebenen Zeit ausgeführt. Verwenden Sie das Feld **Wiederho** in Tagen, Stunden, Minuten und Sekunden zu definieren. Das erste Mal, wenn D **Start** festgelegten Zeitpunkt ausgeführt wird. Die nachfolgenden Erkennungen **Wiederholungsintervall**-Zeitraums ausgeführt.
Einmal	Einmal ausführen, wie durch das Datum und die Uhrzeit festgelegt, die im festge
An Wochentagen	Läuft jeden Montag, Dienstag, Mittwoch, Donnerstag und Freitag. Verwenden Uhrzeit auszuwählen.
An Wochenenden	Läuft jeden Samstag und Sonntag. Verwenden Sie das Feld **Startzeit**, um die Uh
Letzter Tag des Monats	Führen Sie den letzten Tag jedes Monats aus. Verwenden Sie das Feld **Startzeit**,
Ende des Kalenderquartals	Läuft am 31. März, 30. Juni, 30. September und 31. Dezember. Verwenden Sie d auszuwählen. Ändern Sie das Skript `DiscoveryScheduleRunType`, um das Datu
Nach Discovery	Ermöglicht die sequenzielle Staffelung des Zeitplans. Verwenden Sie diese Optio dem im Feld **Ausführen nach** bezeichneten Discovery auszuführen. Wählen Sie **Abbruch**, um anzugeben, dass diese Erkennung auch dann ausgeführt werden Discovery vor Abschluss abgebrochen wird. ◦ Diese Option ist nicht gültig, wenn Discovery über DiscoverNow gestartet wird erkennen“ verwendet wird. ◦ Sie können keinen inaktiven Discovery -Zeitplan festlegen. ◦ Sie können keine Schleife erstellen, indem Sie festlegen, dass die Ausführung Discoveryidentisch ist. ◦ Discovery wird nicht ausgeführt, wenn **Ausführen nach** Discovery nicht abges Ausnahme, dass das Kontrollkästchen **Auch bei Abbruch** aktiviert ist und Disc
Discovery abbrechen, wenn länger als	Zeitbegrenzung für die Ausführung der Discovery. Wenn die angegebene Zeit v verbleibenden Aufgaben für Discovery abgebrochen, auch wenn Discovery ni Kontrollkästchen nicht aktiviert ist, wird Discovery bis zum Abschluss ausgeführt. Systemlast auf ein gewünschtes Zeitfenster.

8. Wählen Sie **Fertigstellen** und **Jetzt ausführen** aus.

Automatisierte Übersetzung

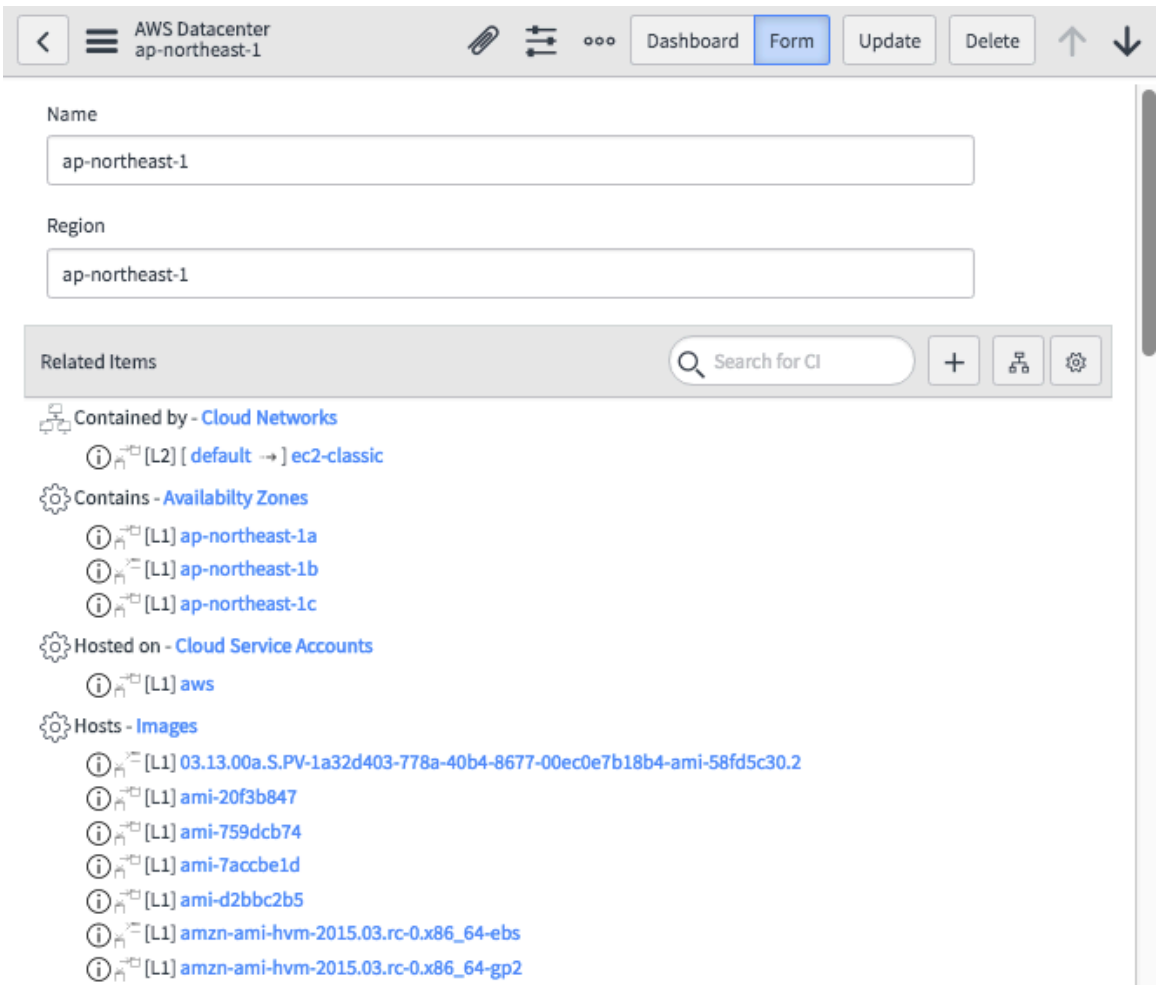
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Discovery wird sofort ausgeführt. Discovery wird zu den angegebenen Zeiten ausgeführt und fügt erkannte Rechenzentren der zugehörigen Liste „Logische Rechenzentren“ hinzu.

Wenn Sie einen Discovery-Zeitplan konfiguriert haben, wird dieser in der zugehörigen Liste „Discovery-Konfiguration – logische Rechenzentren“ angezeigt. Um Discovery für ein einzelnes Rechenzentrum auszuführen, fügen Sie das Rechenzentrum dem Discovery-Zeitplan in der zugehörigen Liste hinzu und führen Sie dann Discovery erneut aus.

Öffnen Sie einen Rechenzentrums-Datensatz, um die Beziehungen zwischen dem Rechenzentrum und den Ressourcen im Rechenzentrum anzuzeigen.

Ressourcen in einem AWS-Rechenzentrum



Hinweis: Standardmäßig werden die erkannten VM-Hardwaretypen von Discovery in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] gespeichert. Wenn Sie in dieser Tabelle eine ungewöhnlich große Anzahl von Datensätzen feststellen, verwenden Sie die Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type], um die erkannten VM-Hardwaretypen zu speichern. Weitere Informationen finden Sie unter Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren. Alle Funktionen von Cloud Provisioning and Governance wie Bereitstellung, Kontingente usw. funktionieren auch nach dem Wechsel zur Tabelle „Cloud-Hardwaretyp“ unverändert.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Zum Anzeigen des Discovery-Status, der Discovery-Protokolle, der erkannten Geräte und der ECC-Warteschlange klicken Sie auf **Erweiterte Ansicht**.
- Wenn Discovery fehlschlägt, überprüfen Sie die Cloud-Discovery-Ergebnisse auf Discovery-Homepage.

Bei Bedarf alle Ressourcen in einem Rechenzentrum erkennen

Sie können jederzeit Discovery für ein Rechenzentrum ausführen, um die CMDB zu aktualisieren.

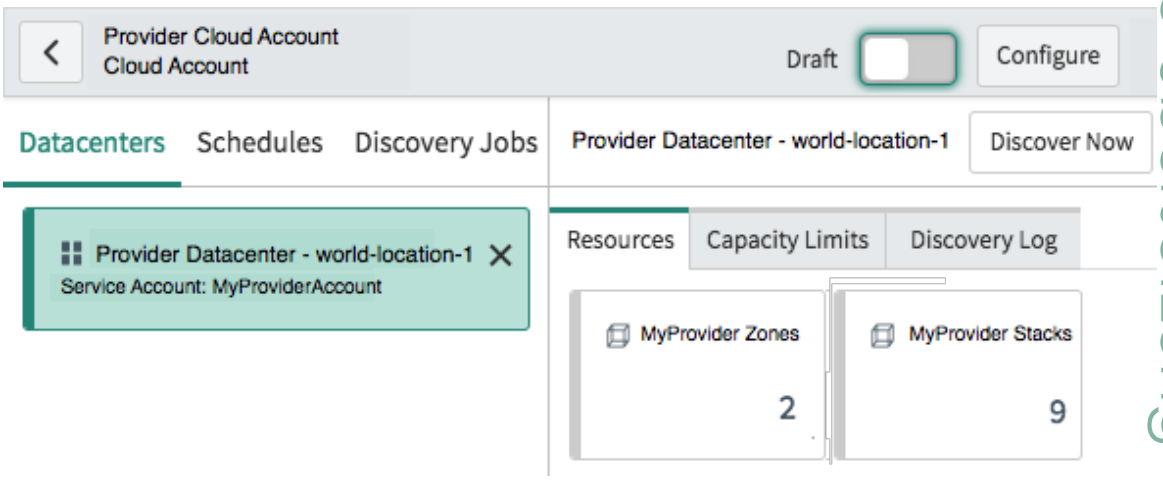
Vorbereitungen

- Es muss ein Cloud-Konto mit Servicekonten und zugehörigen Rechenzentren vorhanden sein. Sie müssen Discovery bei Bedarf ausführen, um Rechenzentren zu erkennen, bevor Sie Discovery planen können.
- Verwenden Sie Arbeitsbereich für Cloud-Vorgängeund mindestens Version 1.15 von Muster für Discovery und Service-Mapping aus ServiceNow Store.

Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Cloud-Accounts**.
2. Klicken Sie auf einen Cloud-Konto, und wählen Sie auf der Registerkarte **Rechenzentren** ein Rechenzentrum aus.
   Auf der Registerkarte **Ressourcen** werden die Ressourcen in der CMDB aufgeführt.



3. Ändern Sie den Status in **Entwurf**, und klicken Sie dann auf **Discovery starten**.
   Beachten Sie, dass **„Jetzt erkennen“** deaktiviert ist, wenn weder CAPI noch Muster installiert sind. Folgen Sie diesen Szenarien, um fortzufahren.

   Hinweis: **„Jetzt erkennen“** wird ebenfalls deaktiviert und in einer Meldung aufgefordert, die neueste Version Muster für Discovery und Service-Mappingvon zu installieren. Dies kann durch die Installation von mindestens Version 1.15.1 oder durch Auslösen des manuellen Migrationsschritts behoben werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Szenario	Nächste Schritte
„Jetzt erkennen“ ist für die Systemadministratoranmeldung deaktiviert	◦ Auf der Seite wird empfohlen, die neueste Musteranwendung zu installieren, um fortzufahren. ◦ Das Banner oben auf der Seite fordert Sie auf, zur Installation **zum Anwendungsmanager** zu wechseln
„Jetzt erkennen“ ist für die Anmeldung als Cloud-Administrator „sn_cmp“ deaktiviert	◦ Auf der Seite wird empfohlen, die neueste Musteranwendung zu installieren, um fortzufahren. ◦ Auf der Seite werden Sie aufgefordert, sich wegen der Installation der Musteranwendung an den Systemadministrator zu wenden.
Die Anwendung mit den neuesten Mustern wird installiert	Jetzt erkennen ist aktiviert. **Hinweis:** Discovery verwendet jetzt Muster als Standardmechanismus.

4. Führen Sie **„Discovery starten“** aus, und warten Sie, bis Discovery abgeschlossen ist.
5. Ändern Sie den Status des Cloud-Kontos in **Veröffentlicht**.

   „Jetzt erkennen“ wird deaktiviert, und es wird dieselbe Meldung angezeigt. Dies kann durch die Installation von Version 1.15.1+ oder durch Auslösen des manuellen Migrationsschritts behoben werden

Ergebnisse

Discovery füllt die CMDB mit den erkannten Ressourcen aus und aktualisiert die Informationen auf der Registerkarte **Ressourcen**. Sie können sich die Discovery-Ergebnisse auf der Registerkarte **Discovery-Protokoll** ansehen.

Hinweis: Standardmäßig werden die erkannten VM-Hardwaretypen von Discovery in der Tabelle „Hardwaretyp“ [cmdb_ci_compute_template] gespeichert. Wenn Sie in dieser Tabelle eine ungewöhnlich große Anzahl von Datensätzen feststellen, verwenden Sie die Tabelle „Cloud-Hardwaretyp“ [cmdb_ci_cloud_hardware_type], um die erkannten VM-Hardwaretypen zu speichern. Weitere Informationen finden Sie unter Klassenerweiterung „Cloud-Hardwaretyp“ aktivieren. Alle Funktionen von Cloud Provisioning and Governance wie Bereitstellung, Kontingente usw. funktionieren auch nach dem Wechsel zur Tabelle „Cloud-Hardwaretyp“ unverändert.

Zugehörige Informationen

Discovery-Protokoll anzeigen

Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder des zusammengefassten Speichers ein. Sie können Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Es muss ein Cloud-Konto mit Servicekonten und zugehörigen Rechenzentren vorhanden sein. Sie müssen Discovery bei Bedarf ausführen, um Rechenzentren zu erkennen, bevor Sie Discovery planen können.
- Verwenden Sie Arbeitsbereich für Cloud-Vorgängeund mindestens Version 1.15 von Muster für Discovery und Service-Mapping aus ServiceNow Store.

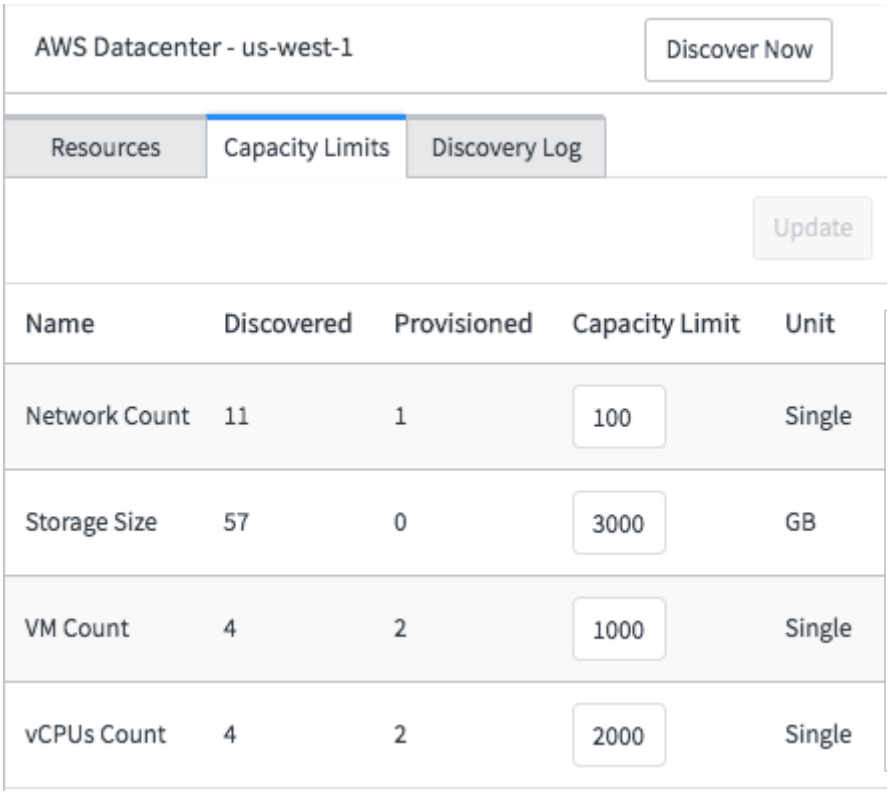
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Sie können auch Kontingente verwenden, um Beschränkungen pro Benutzer und eine Gesamtkapazität für Ressourcen festzulegen. Weitere Informationen finden Sie unter Kontingente und Steuerungen für Ressourcenbestellungen.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Adminportal** > **Verwalten** > **Cloud-Accounts**.
2. Klicken Sie auf einen Cloud-Konto, und wählen Sie auf der Registerkarte **Rechenzentren** ein Rechenzentrum aus.
3. Legen Sie den Status auf **Entwurf** fest.
4. Legen Sie auf der Registerkarte **Kapazitätsgrenzen** die **Kapazitätsgrenzen** nach Bedarf fest.



Wert	Beschreibung
Erkannt	Vom Discovery-Prozess erkannter Gesamtwert für alle Ressourcen im ausgewählten Servicekonto.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wert	Beschreibung
Bereitgestellt	Gesamtwert, der für den ausgewählten Servicekonto bereitgestellt wurde.
Kapazitätsgrenze	Maximal zulässiger Wert, berechnet als Summe für alle Ressourcen im ausgewählten Servicekonto.
Einheit	Maßeinheit für den angegebenen Wert. Beispielsweise wird Speicher in GB gemessen.

5. Klicken Sie auf **Aktualisieren**.
6. Legen Sie den Status auf **Veröffentlicht** fest.

Nächste Maßnahme
Klicken Sie auf **Discover starten**, um Discovery für die logischen Rechenzentren auszuführen.

Verwenden Sie Besitzer und Zuweisungsgruppen

Sie müssen die Anwendergruppen in Cloud Provisioning and Governance als Teil der Tag-2-Aufgabe einrichten und verwenden.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Besitzergruppe: Wird in der Kontingentverwaltung verwendet. Während jeder Stapelbereitstellung muss der Anwender die „Anwendergruppe“ im Bestellformular auswählen. Eine Prüfung des Kontingents wird basierend auf der im Formular ausgewählten Anwendergruppe durchgeführt. Diese Anwendergruppe wird später als „Besitzergruppe“ des Stapels in der Tabelle „sn_cmp_stack“ hinzugefügt. Quotenprüfungen können auf Benutzergruppenebene definiert werden. Weitere Einzelheiten finden Sie unter Kontingente und Steuerungen für Ressourcenbestellungen.

Hinweis: Wenn der Stapel gelöscht wird oder sich das Feld Besitzergruppe für den Stapel ändert, wird das Kontingent neu berechnet. Das Kontingent wird in der Business-Regel neu berechnet: Verbrauchtes Kontingent bei Stapelaktualisierung neu berechnen.

Gruppe zuweisen: Die Discovery-Zeitplanausführungen bringen die aus anderen Instanzen erstellten Ressourcen in Ihre Instanz. Diese Ressourcen werden nicht verwaltet. In ähnlicher Weise erstellt die geplante Aufgabe „Tag-Zuweisungen eingeben“ nicht verwaltete Stapel. Um diese Stapel und Ressourcen zu verwalten, können Sie ihnen eine Change-Gruppe zuweisen.

Weisen Sie einem nicht verwalteten Stapel oder einer Ressource eine Change-Gruppe zu, um sie im **Cloud-Anwenderportal**sichtbar zu machen, damit Sie Tag-2-Vorgänge für diese Ressource ausführen können.

Prozedur

1. Navigieren Sie zu **Cloud-Benutzerportal**.
2. Klicken Sie auf **Stapel anzeigen**, und navigieren Sie zu **Erkannte Stapel** für nicht verwaltete Stapel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie **auf Ressourcen anzeigen**, und navigieren Sie zu **Virtuelle Computer**für nicht verwaltete Ressourcen.
4. Ändern Sie die Ansicht in **Meine Gruppen**.
5. Wählen Sie einen der virtuellen Computer aus, und führen Sie den Tag-2-Vorgang aus.

Cloud Provisioning and Governance-Administrationsleitfaden

Nachdem Sie die Anwendung Cloud Provisioning and Governance auf Ihrer Instanz eingerichtet haben, müssen Sie viele Elemente konfigurieren, bevor Ihre Benutzer Cloud-Ressourcen anfordern und verwalten können.

Anforderungen

Für die Verwendung des -Administrationsleitfadens Cloud Provisioning and Governance ist die Rolle cloud_admin erforderlich.

Bevor Sie beginnen

Cloud Provisioning and Governance einrichten

Weitere Informationen finden Sie im entsprechenden Setup-Leitfaden für Ihren Cloud-Provider:

- Cloud Provisioning and Governance Setupleitfaden für AWS
- Cloud Provisioning and Governance Setupleitfaden für Azure
- Cloud Provisioning and Governance Setupleitfaden für VMware

.

Demonstriert Setup-Optionen für die Bereitstellung von Cloud Provisioning and Governance

Aktionen nach dem Setup

Erstellen Ressourcenprofile

Ressourcenprofile enthalten die Attribute, die eine Ressource haben kann. Benutzer wählen Werte für diese Attribute aus, wenn sie eine Cloud-Ressource bestellen. Sie können die folgenden Typen von Ressourcenprofilen konfigurieren: Computing (z. B. Größe einer VM), Betriebssystem (z. B. Typ und Version), Speicher (z. B. Sicherung) und Sicherheitsgruppen (z. B. Verwenden von HTTPS). Weitere Informationen finden Sie unter Ressourcenprofile.

Governance konfigurieren

Governance-Tools, mit denen Sie die Bereitstellung von Cloud-Ressourcen einschränken können, umfassen unter anderem Kontingente und Richtlinien. Sie können z. B. den Genehmigungs-Workflow konfigurieren, der verwendet wird, nachdem ein Benutzer eine Cloud-Ressource angefordert hat. Sie können auch konfigurieren, ob eine E-Mail gesendet wird, nachdem eine Cloud-Ressource angehalten wurde, und welches Rechenzentrum automatisch ausgewählt werden soll, wenn ein Benutzer eine Ressource eines bestimmten Cloud-Providers auswählt. Weitere Informationen finden Sie unter Cloud-Governance.

Cloud-Servicekatalog ausfüllen

Nachdem Sie Governance-Kontingente und -Richtlinien angewendet haben, erstellen Sie Servicekatalogelemente. Sie haben folgende Möglichkeiten, um ein Katalogelement zu erstellen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vorlagen aus AWS oder Microsoft Azure importieren
- Basissystem-Katalogelement verwenden oder ändern
- Terraform-Vorlage verwenden

Domain Separation und Cloud Provisioning and Governance

Die Domänentrennung wird in Cloud Provisioning and Governance unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Support-Stufe: Basis

- Geschäftslogik: Stellen Sie sicher, dass Daten in die richtige Domäne für die Anwendungsfälle des Application Service Providers übertragen werden.
- Die Anwendung unterstützt die Domänentrennung zur Laufzeit. Zur Domänentrennung gehören die Trennung von der Anwenderoberfläche, Cache-Schlüssel, Berichterstellung, Rollups und Zusammenfassungen.
- Der Besitzer der Instanz muss die Anwendung einrichten, damit sie über mehrere Mandanten hinweg funktioniert.

Beispiel-Anwendungsfall: Wenn ein Service Provider (SP) den Chat verwendet, um auf die Nachricht eines Mandanten (Kunden) zu antworten, muss der Kunde die Antwort des Service Providers sehen können.

Weitere Informationen zu den Supportstufen finden Sie unter Anwendungssupport für die Domänentrennung .

Cloud Provisioning and Governance Übersicht über Domain Separation

Alle Tabellen in Cloud Provisioning and Governance sind nicht domänengetrennt. Delegierte Domänentrennung wird nicht unterstützt.

Domänentrennung für Cloud Provisioning and Governance unterstützt:

Service Provider (SPs), die die Anwendung zur Bereitstellung von Datentrennung verwenden.

In diesem Szenario kann ein SP Datentrennung für mehrere Kunden anbieten, wobei Domänen erforderlich sind, um alle relevanten Kundendaten und -prozesse zu enthalten. Beispielsweise bietet ein SP Support für Kunden, die normalerweise Cloud Provisioning and Governance für die Verwaltung ihrer IT-Infrastruktur in der Cloud verwenden. SPs können ihren Kunden Kataloge, Vorlagenprofile, Ressourcenpools und -filter, Ressourcenprofile, Kontingente, Berechtigungen, IP-Adressenverwaltung (IPAM), Miet- und Geschäftszeitenplanung und Abrechnungsansicht als domänengetrennte Angebote bieten.

So funktioniert Domain Separation in Cloud Provisioning and Governance

Die Domänentrennung für Cloud Provisioning and Governance richtet ein oder mehrere Unternehmen an einer Domäne aus. Zur Verwendung der Domänentrennung in der Anwendung weisen Sie alle Benutzerkonten einem bestimmten Unternehmen zu, das dieser Domäne zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle mit dem Unternehmen verknüpften Entitäten, z. B. Cloud-Konten und Servicekonten, werden in derselben Domäne wie das Unternehmen erstellt. Wenn ein neues Unternehmen erstellt wird, erstellen Sie eine Domäne mit einem eindeutigen Namen und weisen Sie sie dem Unternehmen zu. Alle zugehörigen Entitäten für ein Konto, z. B. Kontakte und Fälle, müssen sich in derselben Domäne befinden. Wenn eine zugehörige Entität für ein domänengetrenntes Konto erstellt wird, wird die Entität der Unternehmensdomäne zugewiesen.

Mitglieder einer Domäne können nur die Daten aufrufen, die in ihrer Domäne oder in untergeordneten, in der Domänenhierarchie niedriger angesiedelten Domänen enthalten sind. Standardmäßig sind alle Benutzer und alle Datensätze Mitglieder der globalen Domäne, sofern Sie sie nicht einer bestimmten Domäne zuweisen. Sobald Sie einer Domäne einen Benutzer oder einen Datensatz zugewiesen haben, vergleicht die Instanz die Domäne des Benutzers mit der Domäne des Datensatzes, um zu bestimmen, ob der Benutzer den Datensatz aufrufen kann.

Service Provider (SPs) verwenden Domänentrennung, um Daten für jeden Kunden zu trennen. Benutzer in einer bestimmten Domäne können nur Daten in ihrer eigenen oder einer untergeordneten Domäne anzeigen lassen. SPs haben üblicherweise die Kontrolle über die oberste Domäne, wodurch sie Daten aller Domänen anzeigen lassen können. Delegieren Sie die Verwaltung nicht an Cloud-Administratorbenutzer der untergeordneten Domänen in Cloud Provisioning and Governance.

Domänentrennung für Cloud Provisioning and Governance einrichten

Aktivieren Sie die folgenden Plugins:

Plugin „Domain Support – Domain Extensions Installer“ (com.glide.domain.msp_extensions.installer), um Domänentrennung in Cloud Provisioning and Governance zu ermöglichen.

Plugin „Service Catalog – Domänentrennung“ (glideapp.servicecatalog.domain_separation), um die Trennung von Katalogelementen in unterschiedlichen Domänen in Cloud Provisioning and Governance zu ermöglichen.

Änderungen an Cloud Provisioning and Governance-Tabellen

Die Domänentrennung für Cloud Provisioning and Governance fügt den Listenansichten die Felder **Domäne** und **Domänenpfad** hinzu. Diese Felder werden standardmäßig nicht verfügbar gemacht. Als Domänenadministrator können Sie Listen und Formulare anpassen, um diese Felder anzuzeigen. Nicht alle Tabellen in Cloud Provisioning and Governance sind domänengetrennt. Während einige Tabellen der obersten Ebene domänengetrennt sind, sind mehrere untergeordnete Tabellen nicht domänengetrennt. Dies hat jedoch keinen Einfluss darauf, wie die Anwendung Cloud Provisioning and Governance in einem domänengetrennten Kontext funktioniert.

Konto-Domänen und zugehörige Entitäten

Beim Erstellen zugehöriger Entitäten für ein Konto wird die Domäne für die zugehörigen Entitäten auf die Kontodomäne festgelegt.

Domänensichtbarkeit für Cloud-Administratoren und -Benutzer

Weisen Sie Benutzer mit den Rollen „Cloud-Benutzerportal“ (sn_cmp.cloud_service_user) und „Cloud-Adminportal“ (sn_cmp.cmp_root_admin) für jede Domäne manuell der Domäne **TOP/MSP/Standard/Unternehmen** oder der Blattdomäne zu. Domänenadministratoren und Benutzer in Cloud Provisioning and Governance können Daten nur in der Domäne anzeigen,

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in der sie erstellt wurden, bis sie der TOP-Domäne zugewiesen werden. Die Top-Domäne stellt eine einzige gemeinsame übergeordnete Domäne dar, die als einzelner übergeordneter Knoten für die Service Provider-Domänen fungiert.

Nächste Schritte

Weitere Informationen zum Erstellen, Implementieren und Verwalten der Domänentrennung für Cloud Provisioning and Governance-Services in der Instanz, die Sie für Ihre Kunden einrichten, finden Sie unter Domain Separation in Cloud Provisioning and Governance : Überlegungen für Service Provider.

Zugehörige Informationen

Domänentrennung für Service Provider

Domain Separation in Cloud Provisioning and Governance : Überlegungen für Service Provider

Berücksichtigen Sie die folgenden Überlegungen, um die Domänentrennung für Cloud Provisioning and Governance-Services in der Instanz, die Sie für Ihre Kunden einrichten, effektiv zu erstellen, zu implementieren und zu verwalten.

- Umfasst alle Aspekte des **Basis** -Supports.
- Anwendungseigenschaften sind bei Bedarf domänenfähig.
- Geschäftslogik: Der Service Provider (SP) erstellt oder ändert Prozesse für einzelne Kunden. Die Anwendungsfälle spiegeln die ordnungsgemäße Verwendung der Anwendung durch mehrere SP-Kunden in einer einzigen Instanz wider.
- Der Besitzer der Instanz muss die MVP-Geschäftslogik (Minimum des lebensfähigen Produkts) und die Datenparameter pro Mandant wie erwartet für die spezifische Anwendung konfigurieren.

So funktioniert Domain Separation in Cloud Provisioning and Governance

Die Domänentrennung für Cloud Provisioning and Governance richtet ein oder mehrere Unternehmen an einer Domäne aus. Zur Verwendung der Domänentrennung in der Anwendung weisen Sie alle Benutzerkonten einem bestimmten Unternehmen zu, das dieser Domäne zugeordnet ist.

Alle mit dem Unternehmen verknüpften Entitäten, z. B. Cloud-Konten und Servicekonten, werden in derselben Domäne wie das Unternehmen erstellt. Wenn ein neues Unternehmen erstellt wird, erstellen Sie eine Domäne mit einem eindeutigen Namen und weisen Sie sie dem Unternehmen zu. Alle zugehörigen Entitäten für ein Konto, z. B. Kontakte und Fälle, müssen sich in derselben Domäne befinden. Wenn eine zugehörige Entität für ein domänengetrenntes Konto erstellt wird, wird die Entität der Unternehmensdomäne zugewiesen.

Mitglieder einer Domäne können nur die Daten aufrufen, die in ihrer Domäne oder in untergeordneten, in der Domänenhierarchie niedriger angesiedelten Domänen enthalten sind. Standardmäßig sind alle Benutzer und alle Datensätze Mitglieder der globalen Domäne, sofern Sie sie nicht einer bestimmten Domäne zuweisen. Sobald Sie einer Domäne einen Benutzer oder einen Datensatz zugewiesen haben, vergleicht die Instanz die Domäne des Benutzers mit der Domäne des Datensatzes, um zu bestimmen, ob der Benutzer den Datensatz aufrufen kann.

Service Provider (SPs) verwenden Domänentrennung, um Daten für jeden Kunden zu trennen. Benutzer in einer bestimmten Domäne können nur Daten in ihrer eigenen oder einer untergeordneten Domäne anzeigen lassen. SPs haben üblicherweise die Kontrolle über die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

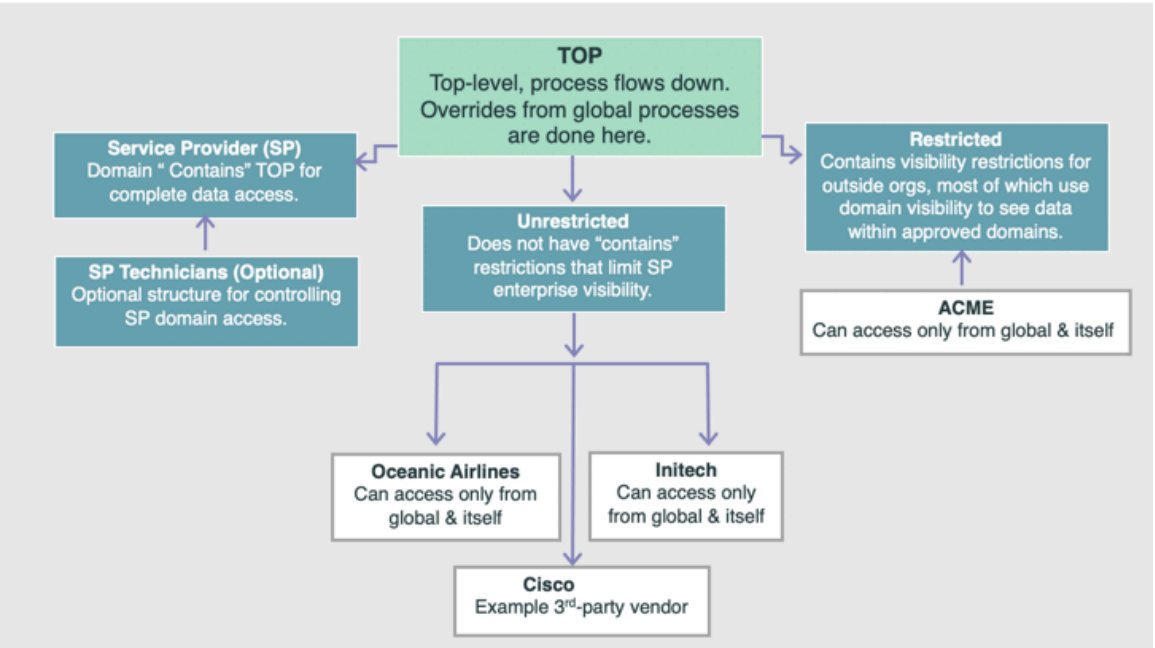
oberste Domäne, wodurch sie Daten aller Domänen anzeigen lassen können. Delegieren Sie die Verwaltung nicht an Cloud-Administratorbenutzer der untergeordneten Domänen in Cloud Provisioning and Governance.

Poolfilter, Ressourcenprofil, Abrechnung, Kontingent, Berechtigungen, IPAM, Budget und Benachrichtigungen sind domänengetrennt. Nicht alle Tabellen in Cloud Provisioning and Governance sind domänengetrennt. Während die meisten Tabellen der obersten Ebene domänengetrennt sind, sind mehrere untergeordnete Tabellen nicht domänengetrennt. Die Tatsache, dass nicht alle Tabellen domänengetrennt sind, wirkt sich jedoch nicht auf das Funktionieren der Anwendung in einem domänengetrennten Kontext aus.

⚠ **Warnung:** Ändern Sie die blaupausenbezogenen Tabellen nicht direkt in den Tabellendatensätzen.

Überlegungen zum Instanz-Setup für Service Provider

Die Domänentrennung bietet zwar Unterstützung für mehrere Mandanten, die Mehrmandantenfähigkeit ist jedoch auch weiterhin in einer einzelnen Instanz enthalten. Einige globale Eigenschaften, Daten und Prozesse werden über alle Domänen hinweg gemeinsam genutzt. Die folgende Abbildung zeigt die Hierarchie der Domänentrennung für uneingeschränkte und eingeschränkte Anwendungsfälle.



Führen Sie die folgenden Aufgaben aus, um Ihre domänengetrennte Instanz einzurichten:

- Erstellen Sie eine Domäne.

    - Sie können beliebig viele Domänen erstellen, stellen Sie jedoch sicher, dass Sie keine unnötigen Domänen auf der Instanz erstellen. Eine große Anzahl von Domänen auf der Instanz kann die Leistung beeinträchtigen. Bevor Sie neue Domänen erstellen, überprüfen Sie die Domänenhierarchie unter **Domänenadministrator** > **Domänenzuordnung**. Überprüfen Sie, ob Sie tatsächlich eine neue Domäne erstellen müssen oder ob stattdessen eine vorhandene Domänenhierarchie verwendet werden kann.

      Wählen Sie eine primäre Domäne aus, um die Domäne der obersten Ebene in der Domänenzuordnung anzugeben. Die Top-Domäne stellt eine einzige gemeinsame übergeordnete Domäne dar, die als einzelner übergeordneter

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Knoten für die Service Provider-Domänen fungiert. Weitere Informationen finden Sie unter Primäre Domäne auswählen .

- Erstellen Sie die SP-Domäne unter der Top-Domäne, und legen Sie die Domäne als Standard fest. Die Organisation Ihrer Domänen ist ein wichtiger Teil des Domänentrennungsprozesses. Stellen Sie sicher, dass Sie sich der Bedeutung des Festlegens eines Standards bewusst sind. Das System weist der Standarddomäne automatisch Aufgaben- und Benutzerdatensätze zu, die noch keiner Domäne zugewiesen sind. Weitere Informationen zum Erstellen einer Standarddomäne finden Sie unter Domäne zum Standard machen.
- Erstellen Sie eine Domänenhierarchie. Weitere Informationen finden Sie unter Domänenhierarchie erstellen .

  Erstellen Sie eine Domänenhierarchie, die Organisationsstrukturen widerspiegelt, um die Gruppierung unter der obersten Domäne zu übernehmen. Da Sie Discovery und Bereitstellung nur von der Blattdomäne aus ausführen können, richten Sie Blattdomänen in der Hierarchie ein, die konkrete Entitäten und Organisationen darstellen.

  Basierend auf der Domänenhierarchie haben Benutzer Zugriff auf Daten in ihrer Stammdomäne und allen untergeordneten Domänen. Der Prozess-Flow ist nach unten gerichtet, während der Daten-Flow nach oben gerichtet ist. Sie können Benutzerdatensätzen einen Domänenwert zuweisen, der die Stammdomäne des Benutzers darstellt. Benutzer haben zwar keinen Zugriff auf Daten in übergeordneten Domänen, Peer-Domänen oder Domänen in anderen Zweigen der Hierarchie. Ein Prozess, der in einer übergeordneten Domäne eingerichtet ist, gilt aber für alle untergeordneten Domänen. Weitere Informationen finden Sie unter

  - Referenzarchitektur des Service Providers
  - Daten der Domain Separation-Architektur

  Kundendaten sind basierend auf Domänenhierarchien betroffen:

  - Über-/untergeordnet: betroffener Prozess und betroffene Daten
    - Design, das auf einem Prozess-Flow basiert.
    - Denken Sie daran, dass die übergeordneten Domänen auf alle Daten in den untergeordneten Domänen zugreifen können.
  - Domäne „Enthält“: Nur Daten sind betroffen. Beispiel: Wenn SP im Diagramm „TOP“ enthält, werden Prozesse in SP nicht in der Domäne „TOP“ und abwärts ausgeführt.
    - Gewährt Personen in Gruppen Datenzugriffsrechte, die dedizierten Zugriff auf bestimmte Domänen erfordern.
    - Enthält Ursachen oder Bedingungen, die Datenbankabfragen hinzugefügt werden sollen, die Leistungsprobleme bei großen Domänen und Datensätzen verursachen können
  - Sichtbarkeit: Hierarchie, die für Benutzer immer sichtbar ist, sobald Sie Zugriff gewähren. Nur die Daten sind betroffen, nicht die Prozesse.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Gewährt einer anderen Domäne, die beim Erstellen der über- und untergeordneten Hierarchie keinen Zugriff hatte, Datenzugriff auf eine Domäne
- Ermöglicht es Benutzern, alle Daten in den Domänen zu sehen, für die sie Sichtbarkeitszugriff haben, und zwar jederzeit, unabhängig von dem Datensatz, an dem sie gerade arbeiten

Hinweis: Gehen Sie sparsam damit um, da mit „Sichtbarkeit“ vollständiger Zugriff gewähren werden kann, was Sie möglicherweise nicht beabsichtigen.

◦ Neues Unternehmen hinzufügen

Sie können Unternehmen hinzufügen, die Lieferanten, Hersteller oder Kunden repräsentieren, mit denen Sie Geschäfte tätigen. Diese Unternehmen bieten eine Möglichkeit, Benutzer, Gruppen und Assets zu kategorisieren.

Erstellen Sie Unternehmen und Blattdomänen für jeden Kunden, den Sie auf einer einzelnen Instanz unterstützen. Unternehmen helfen Ihnen, Benutzer mit der Domäne zu verknüpfen. Unternehmen und Domäne müssen entweder eine Eins-zu-Eins-Zuordnung oder eine Viele-zu-Eins-Zuordnung aufweisen. Dies macht das Zuweisen von Benutzern zu einer Domäne für SPs einfacher und überschaubarer.

Wichtig: Wenn Sie ein Unternehmen für jede Domäne erstellen, verwenden Sie ein Präfix mit einem eindeutigen Bezeichner, z. B. „COMPANY_“ oder „ORG_“.

Zum Anpassen der ServiceNow-Instanz für jedes Unternehmen können Sie Telefonnummern, Adressen und zusätzliche Hinweise eingeben. Sie können auch das Unternehmenslogo und den Bannertext anpassen, die Ihren Endbenutzern oben auf jeder Seite angezeigt werden. Weitere Informationen finden Sie unter Neues Unternehmensprofil erstellen .

- Erstellen Sie Benutzergruppen, und weisen Sie den Benutzern jedes neuen Unternehmens Rollen und eine Domäne zu. Sie weisen Unternehmen Benutzer zu, um sie Domänen zuzuordnen. Ordnen Sie einem Unternehmen einen Benutzer zu, um den Benutzer einer Domäne zuzuordnen.

1. Navigieren zu **Organisationen** > **Unternehmen**, und klicken Sie auf **Neu**, um neue Benutzer zu erstellen. Weitere Informationen zum Erstellen von Benutzern finden Sie unter Benutzer erstellen

   Hinweis: Verwenden Sie nicht die Option für manuell verwaltete Domänen, um die Domäne für Benutzer auszuwählen.

2. Erstellen Sie Gruppen, und weisen Sie den Gruppen Rollen zu. Benutzer, die der Gruppe zugewiesen sind, erben die Rollen. Sie können Cloud-Benutzerportal-Benutzer für ein Unternehmen in der Blattdomäne erstellen. Weitere Informationen zum Erstellen von Gruppen finden Sie unter Benutzergruppen erstellen .
3. Erstellen Sie diese Benutzer in jeder der Blattdomänen:
   - MID Server-Benutzer für jede Blattdomäne und jedes Unternehmen. Weisen Sie MID-Server-Benutzern die Rolle „mid_server“ zu.
   - Domänenadministrator für jede Blattdomäne und jedes Unternehmen. Weisen Sie Cloud-(Domänen-)Administratoren die Rolle „sn_cmp.cmp_root_admin“ zu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Domänenbenutzer für jede Blattdomäne. Weisen Sie Cloud-Benutzern die Rolle „sn_cmp.cloud_service_user“ zu.
- (Optional) Erstellen Sie Benutzer für zusätzliche Rollen in Blattdomänen (Rollen wie Designer, Kontrolle).

  Um bestimmten Benutzern eingeschränkte Sichtbarkeit für bestimmte Domänen bereitzustellen, fügen Sie sie über Gruppen hinzu. Weitere Informationen hierzu finden Sie unter Einem einzelnen Benutzer Domänen mit Sichtbarkeit gewähren .

4. Erstellen Sie eine Domänenbeziehung „Enthält“ zwischen der SP-Domäne und der TOP-Domäne.

   Hinweis: Indem Sie eine Beziehung vom Typ „Enthält“ erstellen, ermöglichen Sie allen Administratoren in der Service Provider-Domäne Zugriff auf alle Domänendaten. Benutzer der globalen Domäne können keine Daten aus dem Kartenlayout sehen, da die Erweiterung des Domänenbereichs standardmäßig nicht zulässig ist.

   Weitere Informationen dazu, wie Sie steuern können, was bestimmte Benutzer und was eine ganze Domäne von Benutzern anzeigen kann, finden Sie unter Sichtbarkeitsdomänen und Enthält Domänen .

Nächste Schritte

Weitere Informationen zum Onboarding von Kunden oder Unternehmen in einer domänengetrennten Instanz für -Services Cloud Provisioning and Governance finden Sie unter Onboarding eines Unternehmens.

Zugehörige Informationen

Domain Separation

Domänentrennung verstehen

Onboarding eines Unternehmens

Prüfen Sie die folgenden Überlegungen zum Onboarding von Kunden oder Unternehmen in einer domänengetrennten Instanz für Cloud Provisioning and Governance-Services.

Übersicht über Domain Separation für Cloud Provisioning and Governance .

Die Domänentrennung für Cloud Provisioning and Governance soll Service Providern eine mehrmandantenfähige Instanzarchitektur bieten, die ihren Kunden Angebote effizient und sicher bereitstellt. Starke allgemeine Prozessstandards, datenbasiertes Prozessdesign, strikte Governance und zentralisierte Administration maximieren diese Vorteile.

Kundenonboarding durch Service Provider

- Erstellen Sie den MID-Server-Anwender, und gewähren Sie die Rolle .

  Die Domänentrennung in Cloud Provisioning and Governance erfolgt durch die Installation und Konfiguration von mindestens einem dedizierten MID Servers für jedes Unternehmen/jede Domäne, die Sie in Ihrer Instanz verwalten. Durch Angabe eines MID-Servers für jede Domäne/jedes Unternehmen wird sichergestellt, dass Konfigurationselemente (Configuration Items, CIs) der gewünschten Domäne zugewiesen werden. Für jede Domäne ist mindestens ein MID Servers für Cloud Discovery, Bereitstellung und andere Orchestrierung eingerichtet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Erstellen Sie in der globalen Domäne einen MID-Server, damit Sie Ziele in anderen Domänen untersuchen können. Weitere Informationen hierzu finden Sie unter Domänentrennung für MID-Server einrichten

Der MID Server (Management, Instrumentation, and Discovery) ist eine Java-Anwendung, die als Windows-Dienst oder UNIX-Daemon auf einem Server in Ihrem lokalen Netzwerk ausgeführt wird. MID-Server ermöglicht die Kommunikation und die Bewegung von Daten zwischen einer Instanz ServiceNow® und externen Anwendungen, Datenquellen und Services.

Für die Kommunikation mit der Instanz benötigen MID Server eine Benutzer-ID und die entsprechende Rolle. Erstellen Sie die Benutzer-ID für einen MID Server, und geben Sie der ID die Rolle **mid_server**. Um ein Fehlschlagen der MID Server-Validierung zu verhindern, werden vom System Geschäftsregeln zur Überwachung der für MID Server-Benutzer ausgewählten Einstellungen ausgeführt.

- Einrichtung von MID-Server .

  Weitere Informationen zum Einrichten des MID-Servers finden Sie unter:

  - Installieren von MID-Server
  - Konfigurieren MID Servers
- Ressourcenblöcke in Cloud Provisioning and Governance

  Erstellen Sie Ressourcenblöcke in der globalen Domäne, da zwischen CI und Ressourcenblock eine 1:1-Beziehung besteht. Erstellen Sie keine Ressourcenblöcke in einer der untergeordneten Domänen oder Blattdomänen. Ressourcenblöcke fungieren als Prozessdatensatz, sodass jede Vorlage einer übergeordneten Domäne in der untergeordneten Domäne sichtbar ist und funktioniert.

  Ressourcenblöcke fungieren als eine Art Middleware-Komponente zwischen Katalogelementen, der Cloud-API (CAPI) und der CMDB.

  - ▪ Wenn die Blöcke im Basissystem nicht die erforderlichen Cloud-Ressourcen bereitstellen, können Sie einen benutzerdefinierten Ressourcenblock erstellen.
    ▪ In der Cloud Provisioning and Governance-Anwendung ist die Skriptausführung in Cloud-Skripts und Cloud-Skriptvorlagen unterteilt. Verwenden Sie Skripts in Katalogelementen, Ressourcenblöcken, BS-Profilen, und verwenden Sie Richtlinienskripts, um Anforderungsformularattribute festzulegen. Richtlinienskripts können Benutzerdaten nicht überschreiben. Weitere Informationen finden Sie unter Cloud-Skripts und Cloud-Skriptvorlagen.
    ▪ BS-Profil ein Skript zuordnen

      Um geskriptete Aktionen während der VM-Bereitstellung auszuführen, können Sie einem BS-Profil ein Skript zuordnen. Das Skript wird auf VMs ausgeführt, die basierend auf der Bildvorlage im BS-Profil erstellt werden.
  - Ressourcenprofile definieren

    Erstellen Sie Ressourcenprofildefinitionen in der globalen Domäne, und erstellen Sie Zuordnungen zu diesen Definitionen in den untergeordneten (Blatt-)Domänen. Löschen Sie keine Ressourcenprofile, ohne allen betroffenen Unternehmen zu überprüfen. Sie können domänenspezifische Ressourcenpools und Poolfilter für alle unterstützten Cloud-Provider erstellen. Als Domänenadministrator können Sie globale, Domänen- und benutzerdefinierte Ressourcenpools für Unterdomänen anzeigen lassen. Ein Ressourcenpool ist eine Abfrage oder ein Skript zur Filterung einer Tabelle. Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

konfigurieren einen Ressourcenpool, um die Werte zu beschränken, die Benutzern bei der Anforderung eines Katalogelements zur Verfügung stehen. Für domänengetrennte Ressourcenpools werden nur Datensätze der relevanten Domäne zurückgegeben.

Ressourcen-Profile sind vom Cloud Provider unabhängige Definitionen, die die zulässigen Attributwerte für eine Ressource angeben. Ressourcen-Profile ermöglichen Ihnen die Steuerung der Auswahlmöglichkeiten, die dem Benutzer beim Anfordern einer Cloud-Ressource angezeigt werden. Daher müssen Sie nicht für jede Variation der Ressource eine eindeutige Blaupause definieren.

- Richten Sie Cloud Provisioning and Governance für Kontingent, Richtlinien, Pools, Berechtigungen ein und verwalten Sie diese. Governance bezieht sich auf die Einschränkungen, die Sie für verfügbare Cloud-Ressourcen festlegen können. Als SP können Sie die Prozesstrennung in Cloud Provisioning and Governance-Richtlinien und Berechtigungen für jedes Unternehmen oder jede Domäne verwalten, die Sie in Ihrer Instanz verwalten. Es wird empfohlen, dass Richtlinien nur in der globalen Domäne eingerichtet werden. Prozesstrennung auf Domänenebene ist für Governance und Richtlinien durchführbar. Für eine benutzerdefinierte Richtlinienerzwingung verwenden Sie das Unternehmensfeld in der Richtlinienregelbedingung, um eine Richtlinie auf die bestimmte Domäne auszurichten.

Typ	Beschreibung
Kontingente	Kontingente sind für Konfigurationselemente oder Cloud-Ressourcen geltende Einschränkungen oder Anforderungen für Gruppen und Benutzer. Verwenden Sie Kontingente, um eine verschwenderische Ressourcennutzung in Ihrer Cloud-Umgebung zu verhindern.
Richtlinien	Eine Cloud-Richtlinie kann einen von einem Benutzer festgelegten Eigenschaftswert überschreiben, eine Genehmigungsaufgabe erstellen, eine IP-Adresse reservieren, Formularfelder vorausfüllen oder ausblenden, benutzerdefinierte Skripts ausführen, die Cloud-API aufrufen oder Workflows starten oder abbrechen. Eine Cloud-Richtlinie gibt Ihnen eine systemweite Kontrolle über Genehmigungen, Ressourcenvorgänge, Blaupausenvorgänge oder Katalogelementeinstellungen.
Pools	Ein Ressourcenpool ist eine Abfrage oder ein Skript zur Filterung einer Tabelle. Sie konfigurieren einen Ressourcenpool, um die Werte zu beschränken, die Benutzern bei der Anforderung eines Katalogelements zur Verfügung stehen.
Berechtigungen	Berechtigungen sind Zugriffsrechte auf Benutzergruppenebene für verschiedene Funktionen in der Cloud Provisioning and Governance-Anwendung und für bestimmte Datensätze in der Instanz, wie beispielsweise Blaupausen oder Cloud-Accounts.

Berechtigungen sind Zugriffsrechte auf Benutzergruppenebene für verschiedene Funktionen in der Cloud Provisioning and Governance-Anwendung und für bestimmte Datensätze in der Instanz, wie beispielsweise Katalogelemente oder Cloud-Konten. Sie können auch grundlegende Governance-Richtlinien, Kontingente und Pools einrichten und dem Cloud-Administratorbenutzer gestatten, diese je nach Bedarf weiter anzupassen. Erstellen Sie eine Benutzergruppe, die die Domänenbenutzer darstellt, und ordnen Sie dieser Benutzergruppe Berechtigungen zu, um Berechtigungen auf Domänenebene einzurichten. Weitere Informationen zum Verwalten von Berechtigungen für Cloud Provisioning and Governance-Rollen finden Sie unter Cloud-Berechtigungen verwalten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Konfigurieren und verwalten Sie Richtlinien, und verwalten Sie die Miete für den bereitgestellten Stapel. Eine Richtlinienregel ist eine Sammlung von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das Richtlinienmodul die Aktionen aus. Wird eine Bedingung als „false“ ausgewertet, führt das Richtlinienmodul die Aktionen nicht aus.

  Richten Sie Richtlinien in der globalen Domäne nur ein, wenn die Richtlinien für alle Domänen gelten sollen. Sie können Cloud Provisioning and Governance anpassen und spezifische Richtlinien für einen Kunden oder eine Domäne festlegen, wenn keine globalen Richtlinien auf eine Domäne angewendet werden sollen. Für eine benutzerdefinierte Richtlinienerzwingung verwenden Sie das Domänenfeld in der Richtlinienregelbedingung, um eine Richtlinie auf die bestimmte Domäne auszurichten. Wenn globale und Domänenrichtlinien gleichzeitig vorhanden sind, werden beide Richtlinien in der für die einzelnen Richtlinien konfigurierten Reihenfolge ausgeführt. Wenn die in den Sortierungsspalten festgelegten Werte identisch sind, ist die Reihenfolge, in der die Richtlinien ausgeführt werden, nicht bestimmt. Stellen Sie sicher, dass Richtlinienaktionen nach Domänen getrennt sind, d. h. alle Aktionsregeln befinden sich innerhalb einer einzelnen Domäne und sind nicht von Regeln in anderen Domänen abhängig.

  Weitere Informationen finden Sie unter:

  - Richtlinien-Governance in Cloud Provisioning and Governance
  - Cloud-Richtlinienregel konfigurieren
  - Aktion für eine Richtlinie „Mietvertragsende“ erstellen
  - Cloud-Richtlinienbeispiel
- Cloud-Katalogelement erstellen

  Erstellen Sie, basierend auf einer Vorlage, ein Cloud-Katalogelement für die Bereitstellung, und veröffentlichen Sie das Katalogelement, um einen Service bereitzustellen.

  Sie können allgemeine oder globale Katalogelemente basierend auf Vorlagen in der SP-Domäne erstellen, um sie für alle von Ihnen verwalteten Domänen verfügbar zu machen. Sie können auch benutzerdefinierte Katalogelemente für jede Domäne/jedes Unternehmen basierend auf Ihren Anforderungen erstellen. Ein Benutzer mit der Rolle Domänenadministrator oder Cloud-Designer kann Cloud-Skripts aktualisieren oder löschen. Cloud-Skriptvorlagen gehören zur Domäne und Unterdomänen. Sie können keine allgemeinen Kataloge mit unterschiedlichen Poolfiltern für jede Domäne verwenden. Erstellen Sie stattdessen einen benutzerdefinierten Katalog für jede Domäne.

  Bereitstellungs-, Nachbereitstellungs- und Tag-2-Vorgänge sind domänengetrennt. Beispiel: Wenn ein Cloud-Portalbenutzer eines bestimmten Unternehmens eine VM bestellt, werden der Stapel, die Anforderung, der virtuelle Computer und alle Komponenten im Stapel in ihrer jeweiligen Domäne gespeichert. Nachfolgende Vorgänge für eine Domäne werden ebenfalls auf dieselbe Weise behandelt. Sie können ein Katalogelement basierend auf der Terraform-Konfigurationsverwaltungsvorlage generieren oder Azure Resource Manager- und AWS CloudFormation-Vorlagen verwenden.

- Cloud-Vorlagen erstellen

  Fügen Sie dem Vorlageninhalt keine sensiblen und privaten Informationen wie CIDR-Werte, IP-Adressen, Anmeldeinformationen usw. hinzu, wenn Sie das Katalogelement als globales Katalogelement einrichten. Die sensiblen Informationen könnten anderen Cloud-Administratoren zugänglich gemacht werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie eine Cloud-Vorlage, und ordnen Sie die Vorlage einem Katalogelement zu. Sobald Sie eine Vorlage erstellt haben, können Sie die Vorlage erneut verwenden, um zusätzliche Katalogelemente für die Services zu erstellen, die Sie bereitstellen möchten.

- Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

  Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen ein, z. B. die Anzahl der virtuellen Computer und virtuellen CPUs oder den zusammengefassten Speicher. Sie können für jedes logische Rechenzentrum in einem Cloud-Konto separate Beschränkungen festlegen.

- Cloud-Kontingentdefinition erstellen

  Sie können für jede Domäne, die Sie in einer Instanz verwalten, separate Kontingentdefinitionen einrichten.

  Sie wenden Kontingente auf eine Ressource, z. B. einen virtuellen Server, ein Rechenzentrum oder eine generische Cloud-Ressource sowie auf Benutzer einer bestimmten Gruppe an. Sie können für die Ressource ein Limit pro Benutzer und ein Gesamtlimit für die Gruppe festlegen. In einer Cloud-Kontingentdefinition werden die Einschränkungen für einen Ressourcenblock angegeben. Sie können Vorlagen verwenden oder manuell verschiedene Konfigurationstypen für jede Kontingentdefinition erstellen.

- IPAM-Integration verwenden

  Die IP-Adressenverwaltung (IP Address Management, IPAM) in Cloud Provisioning and Governance unterstützt die Domänentrennung.

  Wenn Sie ein Tool zur IP-Adressverwaltung (IP Address Management, IPAM) wie Infoblox verwenden, können Sie Cloud-IP-Adressen, Netzwerke und Subnetze in Ihren Cloud-Katalogangeboten verwalten.

- Planung von Geschäftszeiten

  Richten Sie die Geschäftszeitenplanung auf allen virtuellen Computern in einem Stapel ein. Geschäftszeitpläne können für Stapel zum Zeitpunkt der Bereitstellung oder für bereits vorhandene Stapel eingerichtet werden. Zeitpläne können dafür festgelegt werden, wann ein Stapel gestartet, gestoppt und/oder seine Bereitstellung aufgehoben werden soll, indem Parameter wie Geschäftszeiten, Feiertage oder lange Wochenenden definiert werden.

  Sie ordnen einem Instanzzeitplan ein Zeitplanprofil zu. Das Zeitplanprofil gilt für alle neu bereitgestellten Ressourcen, die das Profil verwenden. Beispielsweise können in einem Zeitplanprofil die Wochentage und Tageszeiten angegeben werden, zu denen ein Stapel gestartet und gestoppt werden soll.

  Hinweis: Globale Geschäftszeitpläne gelten für alle Domänen. Sie können keine domänenspezifischen Zeitpläne einrichten, wenn ein aktiver globaler Zeitplan vorhanden ist.

- Zeitplanprofil erstellen

  Stellen Sie zum Einrichten domänenspezifischer Mietzeitpläne sicher, dass keine globalen Mietzeitpläne vorhanden sind. Sie können einen domänenspezifischen Mietvertrag oder Zeitplan nur erstellen, wenn keine aktiven globalen Richtlinien vorhanden sind. Sie können zwar mehrere Mietverträge oder Zeitpläne im Entwurfsstatus haben, es kann jedoch nur ein Mietvertrag oder Zeitplan aktiv sein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Schritte

Weitere Informationen zur Bereitstellung von Cloud-Ressourcen und zur Bereitstellung von Cloud Provisioning and Governance-Lebenszyklusvorgängen für jede Domäne, die Sie in Ihrer Instanz verwalten, finden Sie unter Überlegungen zum Domänenadministrator.

Überlegungen zum Domänenadministrator

Bevor Sie die Domänentrennung für Kunden konfigurieren, sollten Sie vor der Bereitstellung von Cloud-Ressourcen für jede Domäne, die Sie in der Cloud Provisioning and Governance-Anwendung verwalten, die folgenden Überlegungen berücksichtigen.

Domänenadministratoraktivitäten in der Organisation eines Service Providers

Im folgenden Abschnitt werden Aktivitäten aufgelistet, die der Administrator einer Domäne für das Unternehmen ausführt, das von einem Service Provider verwaltet wird. Richten Sie Servicekonten und Cloud-Konten über das Cloud-Adminportal ein. Erstellen Sie die Bereitstellung vorbereitende Vorgänge, die Sie für Cloud-Ressourcen konfigurieren können, bevor Ihre Benutzer sie bereitstellen oder Lebenszyklusvorgänge ausführen.

Starke allgemeine Prozessstandards, datenbasiertes Prozessdesign, strikte Governance und zentralisierte Administration maximieren die Vorteile der Domänentrennung in Cloud Provisioning and Governance in einer einzelnen Instanz. Die Domänenadministratorrolle muss streng auf Benutzer in der Organisation des Service Providers beschränkt sein und darf nicht den Cloud-Administratorbenutzern aus der Organisation des Kunden zugewiesen werden. Diese Einschränkung ermöglicht dem SP sicherzustellen, dass ein Kunde keinen vollständigen Zugriff auf die Daten einer anderen Domäne erhält. Da Daten häufig von mehreren Clients gemeinsam verwendet werden, machen Sie als Domänenadministratoren keine Berechtigungen verfügbar oder gewähren solche, die zu Datenlecks führen könnten.

Cloud-Ressourcen bereitstellen

- Stellen Sie sicher, dass Sie Cloud-Konten in jeder Domäne relevante Servicekonten zuordnen. Beispielsweise wird beim Erkennen eines primären Abonnements in der Azure-Cloud mindestens ein untergeordnetes Servicekonto in derselben Domäne erstellt. Dies bedeutet, dass alle Servicekonten in einem Master-Abonnement aus der Azure-Cloud zu einem einzigen Unternehmen und einer Domäne gehören müssen.

  Melden Sie sich als Benutzer mit Rolle „root_admin“ oder „cloud_admin“ an, wenn Sie Cloud- und Servicekonten einrichten und eine Erkennung für eine beliebige Domäne ausführen. Verwenden Sie die Domänenauswahl, wenn Sie Aktionen wie Discovery oder das Erstellen und Zuordnen von Cloud- und Servicekonten ausführen.

  Hinweis:

  - Cloud Provisioning and Governance unterstützt das Erweitern und Reduzieren des Domänenbereichs nicht.
  - Weitere Informationen dazu, worauf ein Benutzer zugreifen kann und worauf nicht, finden Sie unter Domänenbereich

  Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert werden. In Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dazu verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten enthalten – sogar Servicekonten verschiedener Provider. Für jedes Servicekonto geben Sie an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass Verwaltungsschlüssel und Anmeldeinformationen von Servicekonten für jede Domäne eindeutig sind und nicht freigegeben werden. Führen Sie zum Einrichten von Cloud-Konten und Servicekonten für mehrere Cloud-Provider Aktionen für Tag 1 durch:

- Setupleitfaden für Tag 1 für Amazon Web Services auf Cloud Provisioning and Governance
- Setupleitfaden für Tag 1 für Azure unter Cloud Provisioning and Governance
- Setupleitfaden für Tag 1 für Google Cloud Connector unter Cloud Provisioning and Governance
- Setupleitfaden für Tag 1 für VMware auf Cloud Provisioning and Governance

- Cloud API (CAPI) und Cloud-Skripts und Cloud-Skriptvorlagen

  CAPI ist nicht domänengetrennt, Domänentrennung wird in Cloud Provisioning and Governance unterstützt. Da CAPI in einer globalen Domäne eingerichtet und über Blattdomänen hinweg gemeinsam genutzt wird, stellen Sie sicher, dass Skripts keine hartcodierten vertraulichen Informationen wie Kontodetails, Anmeldeinformationen oder Namen enthalten, nicht einmal in Kommentaren oder Anmerkungen.

  CAPI ermöglicht mithilfe von REST APIs die Integration von Cloud Provisioning and Governance in Cloud-Provider. Cloud-Skripts sind einfache Java-Skripts, die Plattformfunktionen verwenden. In der Cloud Provisioning and Governance-Anwendung ist die Skriptausführung in Cloud-Skripts und Cloud-Skriptvorlagen unterteilt. Verwenden Sie Skripts in Vorlagen, Ressourcenblöcken, BS-Profilen, und verwenden Sie Richtlinienskripts, um Anforderungsformularattribute festzulegen. Richtlinienskripts können Benutzerdaten nicht überschreiben. Cloud-Skriptvorlagen sind tatsächliche ausführbare Dateien, die zur Ausführung an einen virtuellen Computer übergeben werden. Erstellen Sie zuerst eine Cloud-Vorlage, und ordnen Sie sie dann einem Cloud-Skript zu.

- Cloudbasierter Discovery-Vorgang

  Service Provider (SPs) verwenden Domänentrennung, um Daten für jeden Kunden zu trennen. Benutzer in einer bestimmten Domäne können Daten nur in ihrer eigenen oder einer untergeordneten Domäne anzeigen. SPs haben üblicherweise die Kontrolle über die oberste Domäne, wodurch sie Daten aller Domänen anzeigen können. Obwohl die Unterstützung der Domänentrennung für Discovery als Ebene 2 angesehen wird, wird die Verwaltung in Cloud Provisioning and Governance nicht an untergeordnete Domänen delegiert. Die SPs müssen die administrative Kontrolle behalten. Als SP führen Sie Discovery immer von einer Blattdomäne aus, indem Sie sich als Domänenadministrator anmelden oder die Identität eines solchen annehmen, um Ihre Cloud-Ressourcen zu erkennen.

  Cloud Discovery enthält einen Assistenten, mit dem Sie Cloud-Zeitpläne in einer einzigen Benutzeroberfläche erstellen und ausführen können. Wenn Sie mit dem Discovery Manager einen Zeitplan erstellen, wählen Sie die zu erkennenden Konten, die Anmeldeinformationen für den Zugriff auf diese Konten und die MID Server zum Scannen der Ressourcen aus. Anschließend können Sie die Ergebnisse auf der Discovery-Homepage ansehen und eventuell aufgetretene Fehler nachverfolgen.

  Weitere Informationen finden Sie unter

  - Discovery-Manager
  - Erkennungen im Netzwerk ausführen
    - Erkennung von Amazon AWS Cloud
    - Microsoft Azure Cloud-Discovery
    - Erkennung von VMware-Clouds

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erkennung der Google Cloud Platform
- Erkennung von IBM-Clouds

- Richten Sie Event Management ein und konfigurieren Sie es, um externe Events zu empfangen und Warnungen basierend auf den Event- und Warnungsverwaltungsregeln zu generieren. Die Sichtbarkeit von Events hängt von der Domäne des zugeordneten Servicekontos ab. Nur Benutzer, die zu dieser Domäne gehören, können die Eventdetails für verarbeitete Events sehen. Events, die keinem Servicekonto zugeordnet sind, sind für alle Domänen sichtbar.

  Überwachen Sie die Integrität der Business Services und der Infrastruktur mithilfe einer einzigen Managementkonsole, und reagieren Sie angemessen auf alle auftretenden Probleme. Event Management bietet intelligente Event- und Warnungsanalysen und stellt so die Kontinuität Ihrer Business Service-Leistung sicher. Von Event Management werden Events über den MID Server empfangen und verarbeitet.

  Weitere Informationen finden Sie unter

  - Ereignismanagement erkunden
  - Ereignismanagement-Setup
    - Konfigurieren Sie den Konfigurationsservice AWS, um Ereignisbenachrichtigungen an die Instanz ServiceNow zu senden
    - Konfigurieren Sie den Warnungsservice Microsoft Azure so, dass er automatisch aktualisiert wird CMDB
    - Konfigurieren Sie den Service Google Stackdriver Logging für die automatische Aktualisierung von CMDB
    - Konfigurieren Sie den Service VMware-Events für die automatische Aktualisierung von CMDB

- Die Cloud Provisioning and Governance-Anwendung unterstützt die Integration in Lösungen zur kontinuierlichen Bereitstellung (auch bekannt als Konfigurationsverwaltung). Erstellen Sie einen Provider für die Ansible- oder Terraform-Konfigurationsverwaltung, und führen Sie dann Discovery für den Provider aus, um seine Ressourcen zu finden. Weitere Informationen finden Sie unter Unterstützung für kontinuierliche Bereitstellung (Konfigurationsverwaltung) und Arbeitsauslastungs-Provider-Typ für jeden neuen Konfigurationsverwaltungs-Provider erstellen. Diese Informationen werden im Bestellkatalogformular als Verwaltungsattribute angezeigt, die Ihre Benutzer auswählen können, wenn sie eine virtuelle Ressource über einen Konfigurationsverwaltungs-Provider bereitstellen.

- Wenn Sie Kataloge basierend auf Terraform-Vorlagen erstellen und den Katalog für mehrere Domänen freigeben. Führen Sie eine Modulauflistung (Konfigurationserkennung) in der globalen Domäne durch. Der MID-Server sollte in der globalen Domäne erstellt werden, und ihm sollte nur die Terraform-Fähigkeit für die Discovery zugewiesen werden. Dadurch können SPs Kataloge für mehrere Domänen freigeben.

  ⚠ Warnung:

  Erstellen Sie einen globalen MID-Server mit keiner anderen Funktionalität als der Konfigurationsverwaltung für Terraform.

  Gemeinsamen Terraform-Katalog erstellen und für mehrere Kunden freigeben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie als globaler Administrator einen MID-Server in der globalen Domäne.
- Erstellen Sie einen Terraform Open Source-Konfigurationsanbieter.

  Hinweis: Fügen Sie nur „Terraform“ als Konfigurations-Provider hinzu.

- Erstellen Sie ein Katalogelement basierend auf einer Terraform-Vorlage.

- Cloud Provisioning and Governance unterstützt die Verwendung von Now Platform-Regeln mit Workflows. Regeln sind Sammlungen von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das System die Aktionen aus. Wenn eine Bedingung als „false“ ausgewertet wird, führt das System die Aktionen nicht aus. Das Erstellen von Regeln hilft Ihnen, Aktivitäten nachzuverfolgen und schneller auf Probleme zu reagieren und sie zu lösen. Nutzen Sie das Framework der Workflows, um Ihre Abläufe an Tag 2 zu automatisieren. Schreiben Sie schnell einen Workflow, der mit einer Cloud API oder einer bestimmten Ressource kommuniziert. Verwenden Sie SSH, PowerShell oder ein ähnliches Tool, um auf die Workflow-Fähigkeiten zuzugreifen und sie dann zu erweitern. Weitere Informationen finden Sie unter Tag-2-Abläufe mit Workflows.

- Budgetbasierte Benachrichtigung und Genehmigung

  Die Domänentrennung in Cloud Provisioning and Governance unterstützt die Datentrennung von Budgets. Sie können domänenspezifische Budgets zuweisen. Weisen Sie ein Budget für eine Gruppe und einen Benutzer innerhalb der Gruppe zu. Wenn der Benutzer oder die Gruppe den Schwellenwert für das Budgetlimit erreicht, werden sie darüber benachrichtigt. Weitere Informationen finden Sie unter Budgets konfigurieren

  - Tags für Cloud-Ressourcen erstellen

    Mithilfe von Tags werden Cloud-Ressourcen kategorisiert, um umfangreichere und detailliertere Nachverfolgungs- und Abrechnungsberichtsdaten bereitzustellen. Tag-Schlüssel sind nicht domänengetrennt und werden Benutzern anderer Domänen angezeigt. Die Tag-Sichtbarkeit hängt von der zugeordneten CI-Domäne oder der zugehörigen Domäne des Abrechnungsdatensatzes ab. Tags, die keinem CI oder Abrechnungsdatensatz zugeordnet sind, sind für alle Domänenadministratoren sichtbar. Wenn ein Tag erstellt wird, wird es in jedem neu erstellten Katalog angezeigt. Der Cloud-Administrator muss die gewünschten Tags für seinen Katalog auswählen.

  - Abrechnungsdaten können für jede Domäne separat angezeigt werden. Abrechnungsaufträge verwenden die Domäne des konfigurierten Servicekontos. Konfigurieren Sie die Abrechnungseinrichtung so, dass Cloud-Administratoren und Cloud-Benutzer Berichte wie Cloud-Abrechnungsdaten und Cloud Tag-Nutzung auf dem Abrechnungsdashboard anzeigen lassen können.

    Definieren Sie den geplanten Auftrag, mit dem unter Verwendung eines MID Servers regelmäßig Abrechnungsdaten vom Provider heruntergeladen werden. Von Cloud Provisioning and Governance werden die Daten in einer Kostentabelle gespeichert und die Informationen zur Erstellung von Berichten verwendet.

    Weitere Informationen zum Einrichten von Abrechnungszeitplänen und zum Herunterladen von Abrechnungsberichten finden Sie unter:

    - Zeitplan für das Herunterladen von AWS-Abrechnungsdaten definieren
    - Zeitplan für das Herunterladen von Azure-Abrechnungsdaten definieren

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Schritte

Wichtig:

Stellen Sie beim Erstellen benutzerdefinierter Vorgänge, die Workflows für Ressourcenblöcke aufrufen, sicher, dass Sie den Kontext in die entsprechende Domäne ändern.

Zum Ändern des Kontexts in die richtige Domäne bearbeiten Sie die **Workflow-Aktivität**, um das folgende Skript aus dem Workflow heraus aufzurufen. Stellen Sie sicher, dass ein entsprechender Benutzer vom Servicekontoersteller oder vom Auftragsbenutzer abgerufen wird. Durch Aufrufen dieses Identitätswechselskripts kann der Workflow im richtigen Kontext ausgeführt und der richtige MID-Server der zugehörigen Domäne ausgewählt werden.

```
//var orderContext = json.decode(workflow.inputs.ordercontext) ;
new
 CMPDomainSeparationUtil() .impersonateUser(current.request.requested
_for);
```

Weitere Informationen zur Durchführung von Cloud Provisioning and Governance -Lebenszyklusvorgängen, die für jede Domäne verfügbar sind, die Sie in Ihrer -Instanz verwalten, finden Sie unter Cloud-Benutzerportal.

Zugehörige Informationen

Zusätzliches Setup von Cloud Provisioning and Governance an Tag 2

Von ITOM Visibility verwendete Erkennungsmuster

Cloud Provisioning and Governance Rezepte

Multi-Cloud-Rezepte bieten bereitstehende Inhalte für typische Cloud-Bereitstellungen und allgemeine Betriebsszenarien auf verschiedenen Cloud-Plattformen.

Rezepte für Enterprise-Workloads und Tag-2-Vorgänge

Cloud Provisioning and Governance-Rezepte sind gebrauchsfertige Katalogelemente, die aus CFT- und ARM-Beispielvorlagen erstellt wurden, um reale Anwendungsfälle von Cloud-Bereitstellungen zu unterstützen. Diese Rezepte können für den Proof-of-Concept und in Umgebungen außerhalb der Produktion verwendet werden. Stellen Sie in Produktionsumgebungen sicher, dass die Rezepte gut getestet und intern ausgewertet werden. Sie können die Rezepte als Update Sets zum Herunterladen von SHARE im Developer Program unter der Kategorie „Cloud Provisioning-Rezepte“ verwenden.

Liste der Update Sets

Name	Beschreibung
Katalogelemente für Amazon Web Service	
CFT Single Linux VM	Katalogelement für einen einzelnen virtuellen Linux-Computer über ein CFT.
CFT Single Windows VM	Katalogelement für einen einzelnen virtuellen Windows-Computer über ein CFT.
CFT Linux VM with Multiple NICs	Katalogelement für einen virtuellen Linux-Computer mit mehreren Netzwerkschnittstellen über ein CFT.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
CFT Linux VM with LB and Storage	Katalogelement für einen virtuellen Linux-Computer mit Lastenausgleich und Speicher über ein CFT.
CFT Linux VM with Multi VM Multi Disk	Cloud Formation-Vorlage für eine Linux-VM mit mehreren VMs und mehreren Schnittstellen für virtuelle Datenträger.
CFT Linux Install Apache	Katalogelement zur Installation eines Apache-Servers auf einer Linux-VM über ein CFT.
CFT Simple VM with Approval Policy	Katalogelement für eine einfache VM mit einer Genehmigungsrichtlinie über ein CFT.
CFT Windows VM Multi Disk and LB	Katalogelement für eine Windows-VM mit mehreren Schnittstellen für virtuelle Datenträger und mit Lastenausgleich über ein CFT.
Katalogelemente für Azure	
ARM Windows VM with Multi NICs	Katalogelement für eine Windows-VM mit mehreren Netzwerkschnittstellen über eine ARM-Vorlage.
ARM Windows Single VM Multi Disk	Katalogelement für eine einzelne VM mit mehreren Schnittstellen für virtuelle Datenträger über eine ARM-Vorlage.
ARM Windows Stack Multi Disk	Katalogelement für einen Windows-Stapel mit mehreren Schnittstellen für virtuelle Datenträger über eine ARM-Vorlage.
ARM Windows Stack Multi NIC	Katalogelement für eine Windows-Stapel-VM mit mehreren Netzwerkschnittstellen über eine ARM-Vorlage.
ARM Linux VM Multi NIC Multi Disk	Katalogelement für eine Linux-VM mit mehreren Schnittstellen für virtuelle Datenträger und mehreren Netzwerkschnittstellen über eine ARM-Vorlage.
ARM Linux VM Install Apache	Katalogelement zur Installation eines Apache-Servers auf einer Linux-VM über eine ARM-Vorlage.
ARM Linux VM Install MySQL	Katalogelement zur Installation eines MySQL-Servers auf einer Linux-VM über eine ARM-Vorlage.
ARM WebApp MySQL	Katalogelement zum Erstellen einer Web-App mit Azure-Datenbank für MySQL über eine ARM-Vorlage.
ARM VNET Multi Subnet with Approval Policy	Katalogelement für Multi-Subnetz-VNET mit Genehmigungsrichtlinie über eine ARM-Vorlage.
ARM VNIC Multi Subnet with Naming Policy	Katalogelement für Multi-Subnetz-VNIC mit einer Benennungsrichtlinie über eine ARM-Vorlage.

Tag-2-Vorgänge für AWS-VM

Ein Update Set wird für einige der wichtigen Vorgänge von Tag 2 beim AWS Cloud-Provider bereitgestellt. Allgemein sind Tag-2-Vorgänge der Typ von Vorgängen, die für Workloads ausgeführt werden, nachdem sie bereitgestellt wurden. Tag-2-Vorgänge können komplexe Lebenszyklusprozesse oder einfache Dienstprogramme umfassen. In diesem Update Set haben Sie Zugriff auf die folgenden Vorgänge:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Name	Beschreibung
AttachVolume	Fügt der Instanz mit dem angegebenen Gerätenamen ein Amazon EBS-Volume (Elastic Block Store) an und macht es verfügbar.
CreateSnapshot [Erkennungsvorgang auf AWS-Rechenzentrumsebene]	Erstellt einen Snapshot Ihres Amazon EBS-Volumes (Elastic Block Store).
DescribeSnapshots	Beschreibt die angegebenen für Sie verfügbaren Amazon EBS-Snapshots (Elastic Block Store) oder alle für Sie verfügbaren EBS-Snapshots.
DetachVolume	Trennt ein EBS-Volume von einer Instanz.
ModifyInstanceAttribute [Nur InstanceType]	Ändern Sie das angegebene Attribut der angegebenen Instanz.
ModifyVolume [Nur Größe]	Ändern Sie die Parameter eines vorhandenen Amazon EBS-Volumes (Elastic Block Store).
Day 2 Operations for AWS VM – Set 1	Katalogelement für Vorgänge am Tag 2 für eine AWS-VM, Satz 1.

Cloud-Accounts

Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

Mit einem Cloud-Konto können Sie:

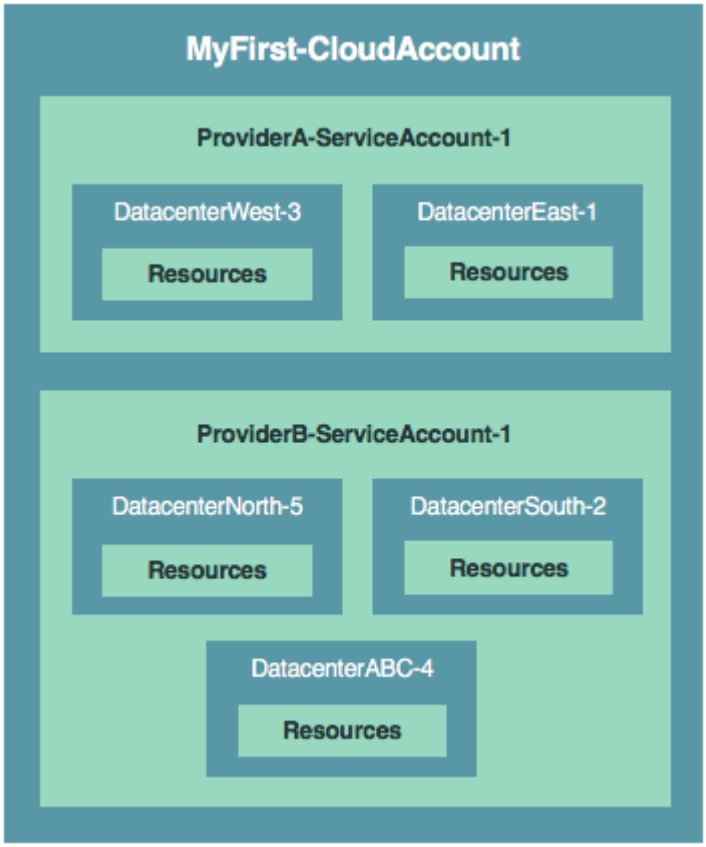
- LZRs hinzufügen. Ein logisches Rechenzentrum (LZR) ist eine regionsspezifische virtuelle Cloud, die einem Servicekonto zugeordnet ist. Das Rechenzentrum hostet Ihre Cloud-Ressourcen.
- Discovery auf LZRs ausführen, um die CMDB mit Konfigurationsänderungen oder Lebenszyklusänderungen (Erstellen/Ändern/Beenden) für jede Ressource in jedem logischen Rechenzentrum zu aktualisieren, das dem Cloud-Konto zugeordnet ist.
- Kapazitätsgrenzen für Cloud-Services wie virtuelle Computer, virtuelle CPUs, virtuelle Netzwerke, Gesamtgröße des Speichervolume und andere Services festlegen. Legen Sie Grenzwerte fest, um sicherzustellen, dass Cloud-Ressourcen in angemessenem Umfang bereitgestellt werden. Grenzwerte sind besonders wichtig für kapazitätsbeschränkte Umgebungen wie private Clouds.
- Einen Cloud-Konto veröffentlichen, damit Geschäftsteams Stapel bereitstellen können.

Struktur eines Cloud-Accounts

Ein Vorteil von Cloud-Accounts ist, dass Sie angegebene Servicekonten nur mit den Regionen (Rechenzentren) gruppieren können, in denen Sie Cloud-Ressourcen zulassen möchten. Beispielsweise kann Ihr AWS-Konto global mehr als ein Dutzend Rechenzentren haben. Sie verwenden vielleicht jedoch nur eine oder zwei Regionen. Um Ihre Sicherheits- und

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Compliance-Regeln zu erfüllen, möchten Sie möglicherweise, dass keine Ressourcen für zusätzliche Regionen auf der ganzen Welt bereitgestellt werden.



Ein Cloud-Konto kann in den folgenden Szenarien beliebig viele Servicekonten enthalten:

Mögliche Cloud-Accountstrukturen

Struktur	Unterstützt	Nicht unterstützt
Fügen Sie dasselbe Servicekonto so oft wie erforderlich hinzu, sofern jeder Eintrag einem anderen LZR zugeordnet ist.	X	
Fügen Sie dasselbe LZR über verschiedene Servicekonten in einem Cloud-Konto hinzu.		X
Fügen Sie einem bestimmten Cloud-Konto verschiedene LZRs aus verschiedenen Servicekonten hinzu, sofern die Regionen nicht identisch sind. Beispiel: Sie haben „us-west-1“ in „serviceaccount1“ und „us-west-2“ in „serviceaccount2“. Beide können „cloudaccount1“ hinzugefügt werden. „us-west-1“ in „serviceaccount1“ und „us-west-1“ in „serviceaccount2“ können jedoch nicht zu „cloudaccount1“ hinzugefügt werden.	X	

Aktualisiert einen Cloud-Account

Belassen Sie einen Cloud-Konto im Status **Entwurf**, bis Sie bereit sind, die Rechenzentren und Kapazitätsgrenzen verfügbar zu machen – z. B. in Blaupausen und dem Cloudbenutzerportal. Sie können den Status nach der Ausführung von Discovery in **Veröffentlicht** ändern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusätzliches Cloud-Konto einrichten

Weitere Informationen finden Sie unter Zusätzliches Cloud-Konto einrichten.

Einem Cloud-Konto ein Rechenzentrum hinzufügen

Sie können der Cloud-Infrastruktur jederzeit ein logisches Rechenzentrum hinzufügen, das durch einen Cloud-Konto dargestellt wird. Siehe Fügen Sie ein Rechenzentrum zu einem hinzu Cloud-Konto.

Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

Kapazitätsgrenzen schränken die Attribute von Cloud-Ressourcen wie die Anzahl der virtuellen Computer, virtuellen CPUs oder des zusammengefassten Speichers ein. Sie können Grenzwerte für Ressourcen für jedes logische Rechenzentrum in einem Cloud-Konto separat festlegen.

Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen

In AWS erkannte Servicekategorien

Der Discovery-Prozess erkennt AWS-Services.

In AWS erkannte Servicekategorien

Servicekategorie	Name	CI-Klasse	Muste
Berechnen	AWS::CloudFormation::Stack	cmdb_ci_aws_cloudformation_stack	
Datenbank	AWS::Datacenter	cmdb_ci_aws_datacenter	
Sicherheit	AWS::DirectoryService		
Berechnen	AWS::EC2::EIP	cmdb_ci_cloud_ip_address	
Berechnen	AWS::EC2::Image	cmdb_ci_os_template	
Berechnen	AWS::EC2::Instance	cmdb_ci_vm_instance	
Berechnen	AWS::EC2::InstanceType	cmdb_ci_compute_template	
Sicherheit	AWS::EC2::Keypair	cmdb_ci_cloud_key_pair	
Netzwerk	AWS::EC2::NetworkInterface	cmdb_ci_nic	
Berechnen	AWS::EC2::SecurityGroup	cmdb_ci_compute_security_group	
Netzwerk	AWS::EC2::Subnet	cmdb_ci_cloud_subnet	
Speicher	AWS::EC2::Volume	cmdb_ci_storage_volume	

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicekategorie	Name	CI-Klasse	Muste
Netzwerk	AWS::EC2::VPC	cmdb_ci_network	
Lastenausgleich	AWS::ElasticLoadBalancing::LoadBalancer	cmdb_ci_cloud_load_balancer	Amaz AWS Elasti Load Balan Servic
Lastenausgleich	AWS::ElasticLoadBalancingV2::LoadBalancer	cmdb_ci_cloud_load_balancer	Amaz AWS Elasti Load Balan Servic
Datenbank	AWS::RDS::DBEvent		
Datenbank	AWS::RDS::DBInstance	cmdb_ci_cloud_database	Amaz AWS Relati Datal Servic
	Verfügbarkeitszone	cmdb_ci_availability_zone	

Hinweis: Die vollständige Liste der übereinstimmenden Klassen/Ressourcen finden Sie in der Tabelle „Cloud-Ressourcentypen“ [sn_capi_resource_type].

In Azure erkannte Servicekategorien

Der Discovery-Prozess erkennt Microsoft Azure-Services.

In erkannte Servicekategorien Azure

Hinweis:

Die CAPI-basierte Discovery-Methode ist veraltet. Folgen Sie Migrieren Sie von CAPI zu Mustern, um weitere Informationen zu erhalten.

Servicekategorie	Name	CI-Klasse	Muster	Produkt
	Azure-Rechenzentrum	cmdb_ci_azure_datacenter		
	Azure-Abonnement	cmdb_ci_cloud_service_account		
	Cloud-Ressource	cmdb_ci_cmp_resource		
Applikationsservices	Microsoft (Unknown Resource Type)			Micros Produc
Applikationsservices	Microsoft.ApiManagement/ service			Micros
Applikationsservices	Microsoft.Cache			Micros

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicekategorie	Name	CI-Klasse	Muster	Produkt
Anwendungsservices	Microsoft.Web/serverFarms			Micros
Applikationsservices	Microsoft.Web/sites	cmdb_ci_cloud_webserver		Micros
Berechnen	Microsoft.Compute/ availabilitySets	cmdb_ci_availability_zone		Micros
Berechnen	Microsoft.Compute/images	cmdb_ci_os_template		Micros
Berechnen	Microsoft.Compute/ virtualMachines	cmdb_ci_vm_instance		Micros
Berechnen	Microsoft.Compute/ virtualMachineScaleSets			Micros
Berechnen	Microsoft.ServiceFabric/ clusters			Micros
Berechnen	Microsoft.Compute/vmSize	cmdb_ci_compute_template		Micros
Berechnen	Microsoft.Resources/ deployments	cmdb_ci_azure_deployment		Micros
Berechnen	Microsoft.Resources/ resourceGroups	cmdb_ci_resource_group		Micros
Datenbank	Microsoft.DocumentDB			Micros
Datenbank	Microsoft.Sql/servers	cmdb_ci_cloud_database	Azure-Datenbank	Micros
Datenbank	Microsoft.sql/ managedInstances	cmdb_ci_cloud_database	Azure-Datenbank	Micros
Datenbank	Microsoft.dbformysql	cmdb_ci_cloud_database	Azure-Datenbank	Micros
Datenbank	Microsoft.documentdb/ databaseaccounts	cmdb_ci_cloud_database	Azure-Datenbank	Micros
Datenbank	Microsoft.cache/redis	cmdb_ci_cloud_database	Azure-Datenbank	Micros
Datenbank	Microsoft.dbfürpostgresql/ servers	cmdb_ci_cloud_database	Azure-Datenbank	Micros
Datenbank	Microsoft.dbformysql/server	cmdb_ci_cloud_database	Azure-Datenbank	Micros
Datenbank	Microsoft.Sql/servers/ databases	cmdb_ci_database	Azure-Datenbank	Micros
Load Balancer	Microsoft.Network/ loadBalancers	cmdb_ci_cloud_load_balancer		Micros
Netzwerk	Microsoft.Network/ applicationGateways			Micros
Netzwerk	Microsoft.Network/ networkInterfaces	cmdb_ci_nic		Micros
Netzwerk	Microsoft.Network/ networkSecurityGroups	cmdb_ci_compute_security_group		Micros

Automatische Übersetzung

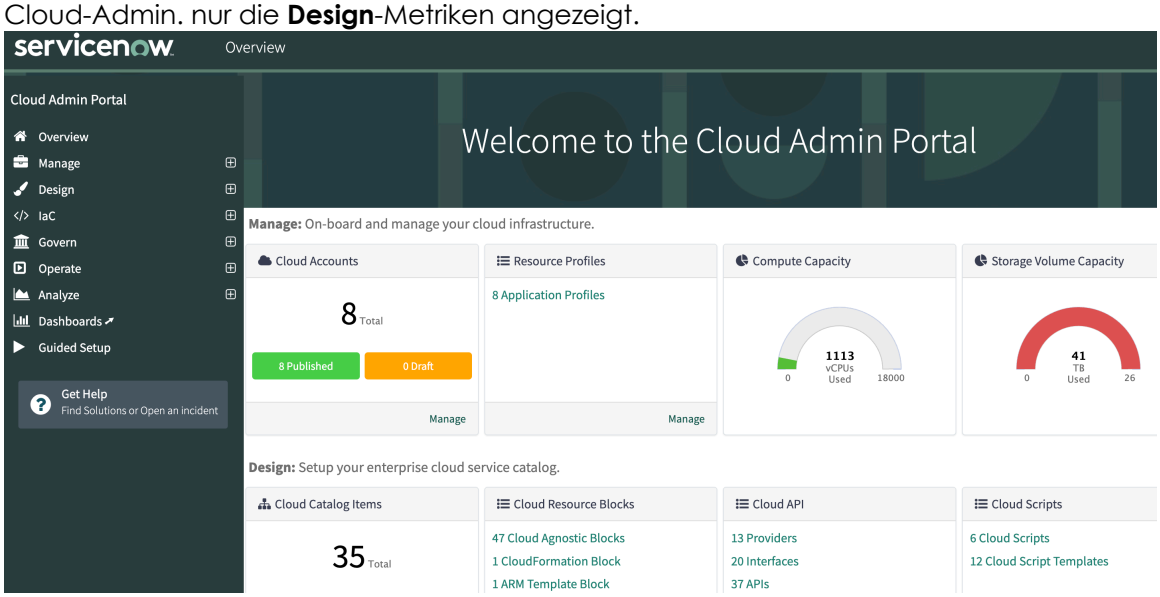
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Servicekategorie	Name	CI-Klasse	Muster	Produkt
Netzwerk	Microsoft.Network/ publicIPAddresses	cmdb_ci_cloud_public_ipaddress		Micros
Netzwerk	Microsoft.Network/ routeTables	cmdb_ci_route_table		Micros
Netzwerk	Microsoft.Network/subnets	cmdb_ci_cloud_subnet		Micros
Netzwerk	Microsoft.Network/ virtualNetworks	cmdb_ci_network		Micros
Sicherheit	Microsoft.Security			Micros
Speicher	Microsoft.Storage/blobs	cmdb_ci_storage_volume		Micros
Speicher	Microsoft.Storage/ storageAccounts	cmdb_ci_cloud_storage_account		Micros
Tools	Microsoft.Insights/ components			Micros
Tools	Microsoft.ServiceBus			Micros

Cloud-Adminportal

Das Portal für Cloud-Admin. ist ein rollenbasiertes Portal. Sie können alle Ihre Cloud-Ressourcen von einer einheitlichen Basis aus verwalten, entwerfen, steuern, betreiben und analysieren.

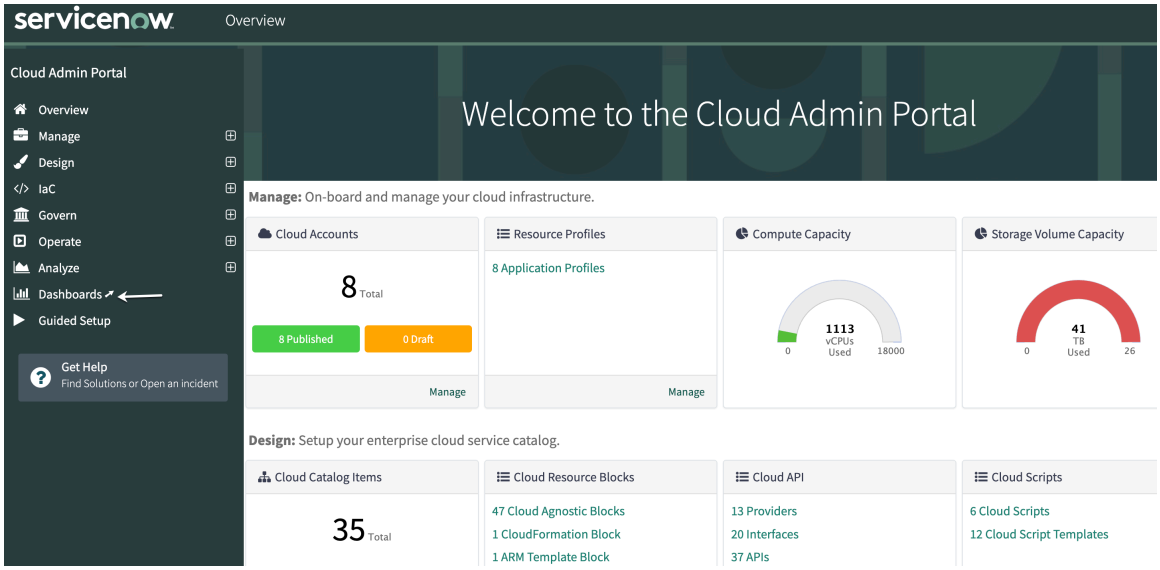
Je nachdem, mit welcher Rolle Sie angemeldet sind, zeigt das Portal für Cloud-Admin. unterschiedliche Metriken an. Wenn Sie beispielsweise bei der Cloud Provisioning and Governance-Anwendung als Cloud Service Designer angemeldet sind, werden im Portal für Cloud-Admin. nur die **Design**-Metriken angezeigt.



Ab diesem Release können Sie jetzt über den Link **Dashboards** im linken Navigationsbereich des Cloud-Adminportals auf diese Next Experience Dashboard-Seiten zugreifen:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Den Link zu diesen Dashboards finden Sie auf einer neuen Registerkarte basierend auf Ihrer Anwenderrolle:

- Cloud-Ursachenanalyse-Dashboard
- Dashboard für Cloud-Vorgänge
- Cloud-Tag-Werte-Dashboard

Folgen Sie Die Anwendung Cloud Provisioning and Governance anfordern, um mehr über die Installation von Cloud Provisioning and Governance für den Zugriff auf die Administrator- und Anwenderseiten zu erfahren. Melden Sie sich beim Portal mit den folgenden Cloud Provisioning and Governance-Rollen an, um die zugehörigen Metriken anzuzeigen oder zu verwalten:

Beschreibender Name und Rollenname	**Zugriff auf die Metriken in** Portal für Cloud-Admin.
Root-Administrator `[sn_cmp.cmp_root_admin]`	Alle Metriken. • Übersicht • Verwalten • Entwurf • LAC • Bedingungen • Betreiben • Analysieren • Geführtes Setup
Cloud-Administrator `[sn_cmp.cloud_admin]`	Verwalten Siedie Metriken. • Übersicht • Verwalten
Systemadministrator	Alle Metriken.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beschreibender Name und Rollenname	Zugriff auf die Metriken in Portal für Cloud-Admin.
`[admin]`	• Übersicht • Verwalten • Entwurf • LAC • Bedingungen • Betreiben • Analysieren • Geführtes Setup
Kontrolle `[sn_cmp.cloud_governor]`	• Steuern • Analysieren
Service Designer `[sn.cmp.cloud_service_designer]`	Design
Operator `[sn_cmp.cloud_operator]`	Betreiben

Nur die Rollen Root-Administrator, Cloud-Administrator und Systemadministrator können alle Metriken im Portal für Cloud-Admin. anzeigen und verwalten.

Klicken Sie auf **Guided Setup**, um die Cloud Provisioning and Governance-Anwendung auf Ihrer ServiceNow-Instanz zu konfigurieren. Sie werden durch das Abschließen verschiedener Konfigurationsaufgaben geleitet. Der Prozentsatz der Aufgaben, die Sie abgeschlossen haben, wird angezeigt, damit Sie Ihren Fortschritt überwachen können.

Klicken Sie auf **Hilfe**, um eine Frage zu stellen, einen Incident zu öffnen, zur Produktdokumentation oder zur Knowledge Base-Website zu wechseln.

Ressourcenprofile

Ressourcen-Profile sind vom Cloud Provider unabhängige Definitionen, die die zulässigen Attributwerte für eine Ressource angeben. Ressourcen-Profile ermöglichen Ihnen die Steuerung der Auswahlmöglichkeiten, die dem Benutzer beim Anfordern einer Cloud-Ressource angezeigt werden. Daher müssen Sie nicht für jede Variation der Ressource eine eindeutige Blaupause definieren.

Hinweis: Zusätzlich zu den Cloud-unabhängigen Profilen können Sie öffentliche Images von Providern zum Cloud Provisioning and Governance-Katalog hinzufügen. Siehe Öffentliches AWS-Image zu Cloud Provisioning and Governance hinzufügen und Öffentliches Azure-Image zu Cloud Provisioning and Governance hinzufügen.

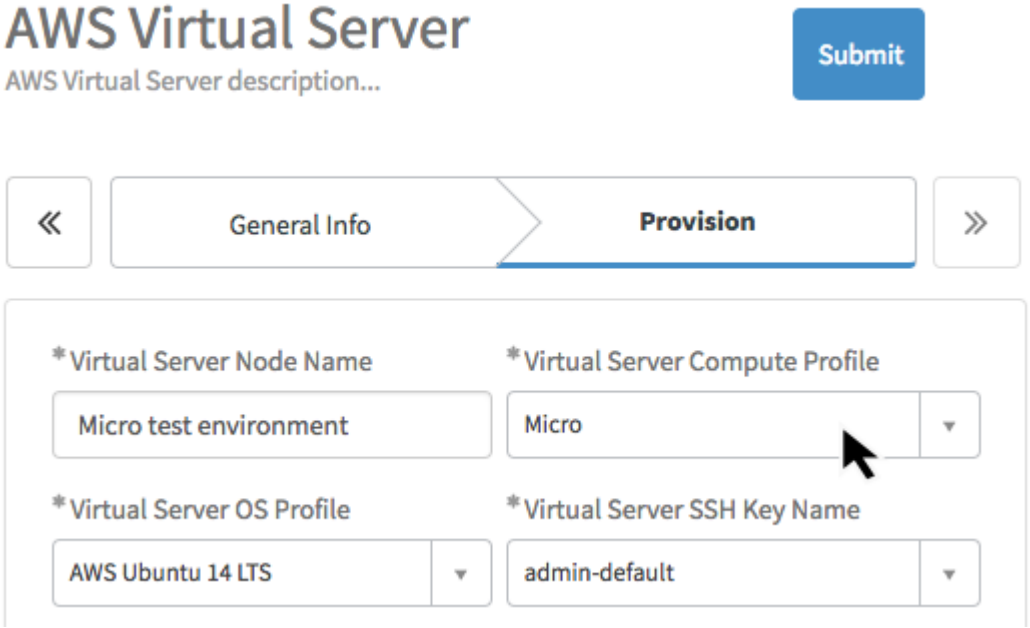
Beispiel: Computing-Profil

Sie können ein Computing-Profil mit dem Namen *Micro* erstellen und einem Hardwaretyp „micro“ mit angegebenen Werten für Arbeitsspeicher und CPU zuordnen. Später, wenn ein Benutzer beim Anfordern eines virtuellen Servers eine Computing-Ressource auswählt, wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Micro als Option in der Liste der verfügbaren Computing-Ressourcen angezeigt. Der Benutzer muss keine Werte für Arbeitsspeicher und CPU angeben – die Werte stammen aus dem Profil.

Computing-Profil im Anforderungsformular



Zuordnungen von Ressourcenprofilen

Ressourcen-Profile erstellen Zuordnungen zwischen den folgenden Elementen:

- Cloud-Konto.
- Logisches Rechenzentrum im Cloud-Konto.
- Bestimmter Ressourcentyp in der CMDB, die die Attribute bereitstellt.
- Optional: Preiswert, der Benutzern angezeigt wird, wenn sie eine Ressource anfordern, die das Ressourcenprofil verwendet.

Standardmäßig ordnet Cloud Provisioning and Governance für AWS und Azure Profile nach der Ausführung von Discovery Vorlagen zu. Bei anderen Providern, z. B. Google Cloud, müssen Sie das Profil manuell der richtigen Vorlage und dem richtigen Rechenzentrum zuordnen.

Ressourcentypen

Jedem Ressourcenprofil sind Attribute zugeordnet. Die Attribute hängen von den Ressourcentypen ab, die nach der Ausführung von Discovery für ein Cloud-Konto ausgefüllt werden.

Ressourcen-Profil **Typ**	**Beschreibung und Attribute**	**Ressourcentyp und Vorlage**
Anwendungsprofil	Ein Anwendungsprofil gibt Anwendungssoftware an, die auf neu bereitgestellten Ressourcen installiert werden soll. Benutzer können Anwendungen auswählen, wenn sie einen Stapel anfordern. Verwenden Sie Anwendungsprofile bei der Integration in	Applikationsvorlage [sn_cmp_application_template]

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen-Profil **Typ**	**Beschreibung und Attribute**	**Ressourcentyp und Vorlage**
	Konfigurationsverwaltung (kontinuierliche Bereitstellung) von Providern wie Ansible Playbooks. Attribute: Anwendungen, die auf virtuellen Computern ausgeführt werden.	
Computing-Profil	In einem Computing-Profil wird die Hardware für neu bereitgestellte virtuelle Computer angegeben. Attribute: Die Größe der Computing-Ressourcen, einschließlich virtueller CPUs, Arbeitsspeicher und lokalem Speicher.	Hardwaretyp [cmdb_ci_compute_template]
Computing-Sicherheitsgruppenprofil	Ein Computing-Sicherheitsgruppenprofil wendet bestimmte Sicherheitsregeln auf neu bereitgestellte Ressourcen an. Sie ordnen ein Compute-Sicherheitsgruppenprofil einem Cloud-Konto, einem Rechenzentrum, einer Compute-Sicherheitsgruppenvorlage und Sicherheitsregeln für die Vorlage zu. Attribute: Firewallregeln, z. B. Aktivieren von HTTP und HTTPS.	Sicherheitsgruppenvorlage berechnen [cmdb_ci_security_grp_template]
BS-Profil	Mit einem BS-Profil wird ein bestimmtes Image auf einem neu bereitgestellten virtuellen Computer installiert. Sie ordnen ein BS-Profil einem Cloud-Konto, einem Standort (Rechenzentrum), einer Bildvorlage und einem Cloud-Skript zu. Attribute: Betriebssystem-Images, einschließlich BS-Typ und -Version, Root-Gerätetyp und Image-Quelle.	Bild [cmdb_ci_os_template]
Zeitplanprofil	Sie ordnen einem Instanzzeitplan ein Zeitplanprofil zu. Das Zeitplanprofil gilt für alle neu bereitgestellten Ressourcen, die das Profil verwenden. Beispielsweise können in einem Zeitplanprofil die Wochentage und Tageszeiten angegeben werden, zu denen ein Stapel gestartet und gestoppt werden soll.	N/V

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen-Profil **Typ**	**Beschreibung und Attribute**	**Ressourcentyp und Vorlage**
	Attribute: Zeitplanattribute, z. B. wann ein Stapel gestartet, gestoppt oder die Bereitstellung aufgehoben werden soll.	

Zugehörige Informationen

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

Anwendungsprofil erstellen

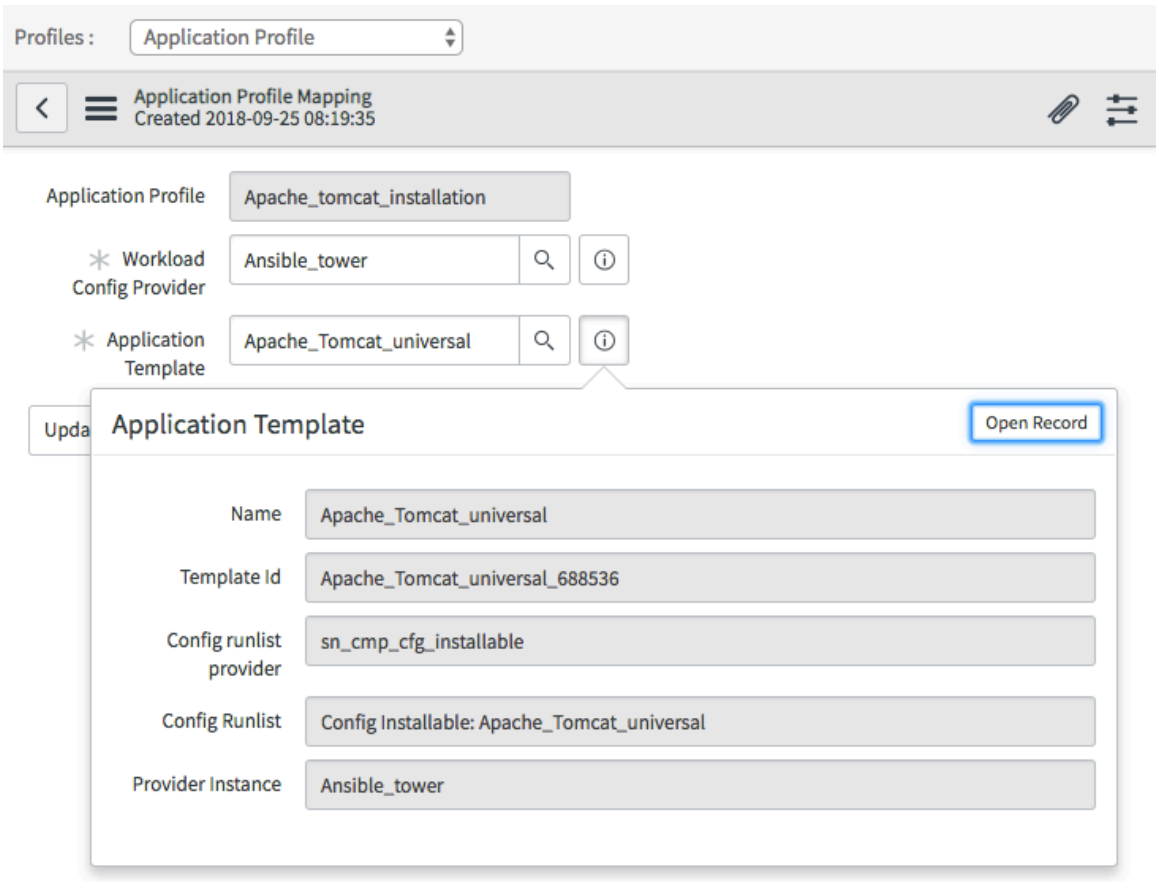
Ein Anwendungsprofil gibt Anwendungssoftware an, die auf neu bereitgestellten Ressourcen installiert werden soll. Benutzer können Anwendungen auswählen, wenn sie einen Stapel anfordern. Verwenden Sie Anwendungsprofile bei der Integration in Konfigurationsverwaltung (kontinuierliche Bereitstellung) von Providern wie Ansible Playbooks.

Vorbereitungen

- Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.
- Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

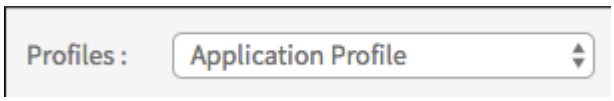
Dieses Beispiel zeigt eine Anwendungsprofilzuordnung für einen Tomcat-Server in Ansible.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Ressourcenprofile**.
2. Wählen Sie in der Liste **Profile** die Option **Anwendungsprofil** aus, und klicken Sie dann auf **Neu**.



3. Geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** für das Profil ein, und klicken Sie dann auf **Absenden**.
   Das Profil wird erstellt.
4. Ordnen Sie das Profil einer Vorlage zu.

   a. Klicken Sie in der Liste auf das von Ihnen erstellte Profil.

   b. Klicken Sie in der zugehörigen Liste **Anwendungsprofilzuordnungen** auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
Workload-Konfigurations-Provider	Wählen Sie einen Provider für Konfigurationsverwaltung aus, der dem Profil zugeordnet werden soll.
Applikationsvorlage [sn_cmp_application_template]	Wählen Sie eine Vorlage aus, der das Profil zugeordnet werden soll. Wenn Sie Discovery für den Konfigurations-Provider ausgeführt haben, sind die Vorlagen bereits ausgefüllt. Der einem Anwendungsprofil zugeordnete Ressourcentyp ist `sn_cmp_application_template`. Klicken Sie auf das Referenzsymbol ( ), um die Details der Vorlage anzuzeigen. So erstellen Sie eine neue Vorlage: **i.** Klicken Sie auf das Referenzsymbol ( ), um die Liste der Anwendungsvorlagen zu öffnen. **ii.** Klicken Sie auf **Neu**, und füllen Sie das Formular der Anwendungsvorlage aus: ▪ **Name**: Geben Sie einen beschreibenden Namen für die Vorlage ein. ▪ **Vorlagen-ID**: Geben Sie eine ID für die Vorlage ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ **Provider der Konfig-Ausführungsliste**: Klicken Sie auf die Liste, wählen Sie eine Tabelle aus der Liste **Tabellenname** aus, und wählen Sie dann Datensätze für die Tabelle aus der Liste **Dokument** aus. ▪ **Konfig-Ausführungsliste**: Geben Sie eine Konfigurations-Ausführungsliste an. ▪ **Provider-Instanz**: Wählen Sie eine Provider-Instanz aus.

5. Erstellen Sie so viele Zuordnungen wie nötig.

Zugehörige Informationen

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

Computing-Profil erstellen

In einem Computing-Profil wird die Hardware für neu bereitgestellte virtuelle Computer angegeben. Ein Computing-Profil wird einem Cloud-Konto, einem Rechenzentrum und einer Hardwarevorlage zugeordnet.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.

Prozedur

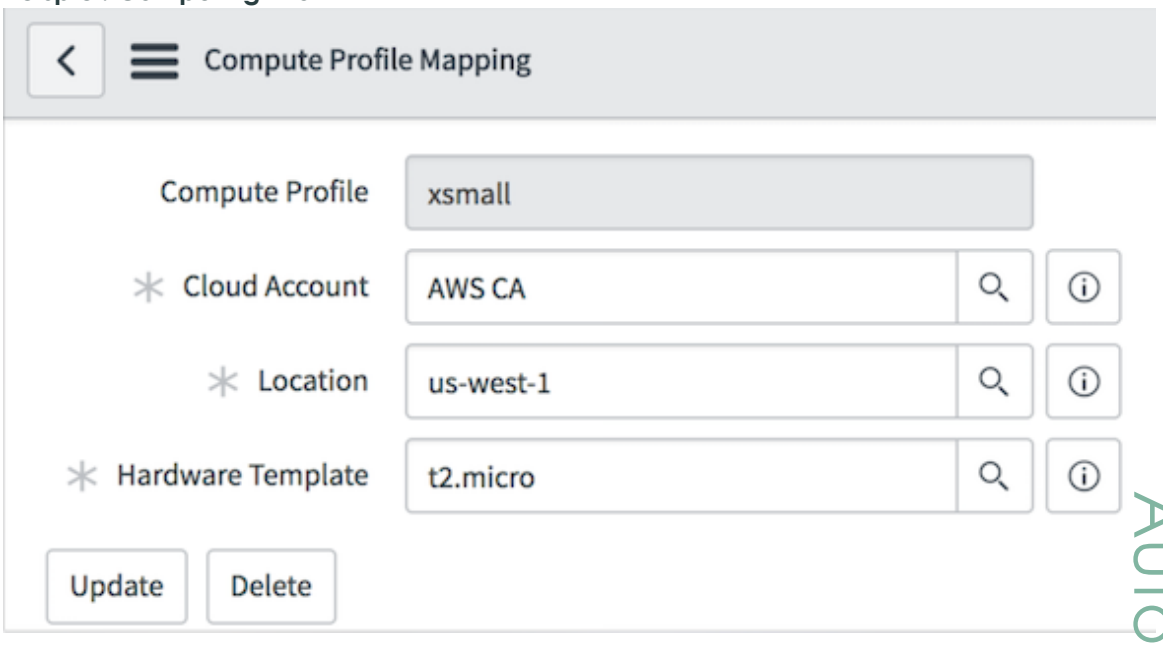
1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Ressourcenprofile**.
2. Wählen Sie in der Liste **Profile** die Option **Anwendungsprofil** aus, und klicken Sie dann auf **Neu**.
3. Geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** für das Profil ein, und klicken Sie dann auf **Absenden**.
   Das Profil wird erstellt.
4. Klicken Sie auf das von Ihnen erstellte Ressourcenprofil.
5. Ordnen Sie das Profil einer Vorlage zu.

   a. Klicken Sie in der Liste auf das von Ihnen erstellte Profil.

   b. Klicken Sie in der zugehörigen Liste **Profilzuordnungen** auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: Computing-Profil



Feld	Beschreibung
Cloud-Konto	Wählen Sie einen Cloud-Konto aus, für den das Profil gültig ist.
Standort	Wählen Sie das Rechenzentrum aus, für das das Profil gültig ist.
Hardwarevorlage [cmdb_ci_compute_template]	Wählen Sie einen Hardwaretyp aus, dem das Profil zugeordnet werden soll. Klicken Sie auf das Referenzsymbol ( ), um die Details der Vorlage anzuzeigen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

Computing-Sicherheitsgruppenprofil erstellen

Ein Computing-Sicherheitsgruppenprofil wendet bestimmte Sicherheitsregeln auf neu bereitgestellte Ressourcen an. Sie ordnen ein Compute-Sicherheitsgruppenprofil einem Cloud-Konto, einem Rechenzentrum, einer Compute-Sicherheitsgruppenvorlage und Sicherheitsregeln für die Vorlage zu.

Vorbereitungen

Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.

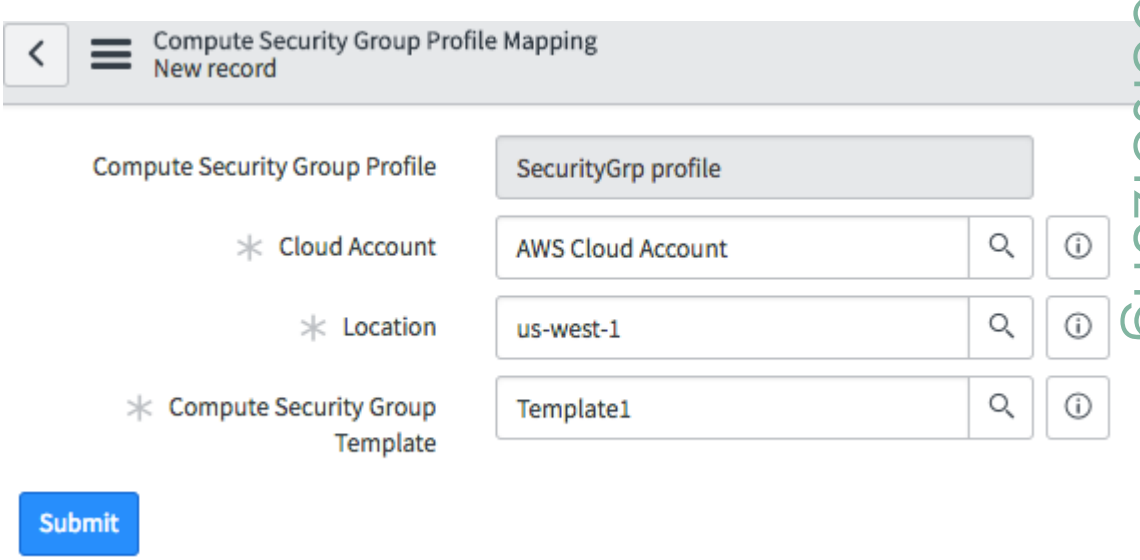
Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Ressourcenprofile**.
2. Wählen Sie in der Liste **Profile** die Option **Computing-Sicherheitsprofil** aus, und klicken Sie dann auf **Neu**.
3. Geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** für das Profil ein, und klicken Sie dann auf **Absenden**.
   Das Profil wird erstellt.
4. Ordnen Sie das Profil einer Vorlage zu.

   a. Klicken Sie in der Liste auf das von Ihnen erstellte Profil.

   b. Klicken Sie in der zugehörigen Liste **Computing-Sicherheitsgruppen-Profilzuordnungen** auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.



Feld	Beschreibung
Cloud-Konto	Wählen Sie einen Cloud-Konto für das Profil aus.
Standort	Wählen Sie das Rechenzentrum aus, das zum Cloud-Konto gehört.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Sicherheitsgruppenvorlage berechnen [cmdb_ci_security_grp_template]	Wählen Sie eine Vorlage aus, der das Profil zugeordnet werden soll, oder erstellen Sie eine. Zum Erstellen einer neuen Vorlage klicken Sie auf das Listensymbol und dann auf **Neu**. Geben Sie einen Namen und eine Vorlagen-ID ein, und klicken Sie auf **Absenden**. Klicken Sie auf das Referenzsymbol ( ), um die Details der Vorlage anzuzeigen.

5. Fügen Sie der Vorlage Regeln hinzu.
Sie können pro Vorlage mehrere Regeln erstellen.

a. Klicken Sie in der zugehörigen Liste **Sicherheitsgruppen-Profilzuordnungen** unter der Überschrift **Computing-Sicherheitsgruppenvorlage** auf den Vorlagennamen.

b. Klicken Sie in der zugehörigen Liste **Regelvorlage der Computing-Sicherheitsgruppen** auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
CIDR-Bereich	Geben Sie einen CIDR-Bereich an. Beispiel: 10.0.0.0/24
IP-Protokoll	Wählen Sie ein IP-Protokoll aus. In Azure werden die Protokolle TDP und UDP unterstützt. ICMP wird nicht unterstützt.
Von Port	Geben Sie die Quellportnummer an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Ist ausgehend	Geben Sie `0` für eingehend und `1` für ausgehend ein.
Name	Geben Sie einen Namen für die Regel an.
Netzwerktyp	Wählen Sie den Typ des Netzwerks aus.
An Port	Geben Sie die Zielportnummer an.

Zugehörige Informationen

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

BS-Profil erstellen

Mit einem BS-Profil wird ein bestimmtes Image auf einem neu bereitgestellten virtuellen Computer installiert. Sie ordnen ein BS-Profil einem Cloud-Konto, einem Standort (Rechenzentrum), einer Bildvorlage und einem Cloud-Skript zu. BS-Profile sind anbieterunabhängig, und Sie können dasselbe Profil für mehrere Cloud-Accounts verwenden.

Vorbereitungen

- Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.
- Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Hinweis: Profilzuordnungen, in denen mehr Details angegeben sind, werden zuerst ausgeführt. Beispielsweise hat eine Zuordnung, in der eine Blaupause, ein Betriebssystemprofil und ein Ressourcenalias angegeben sind, Vorrang vor einer Zuordnung, in der nur ein Betriebssystemprofil angegeben ist.

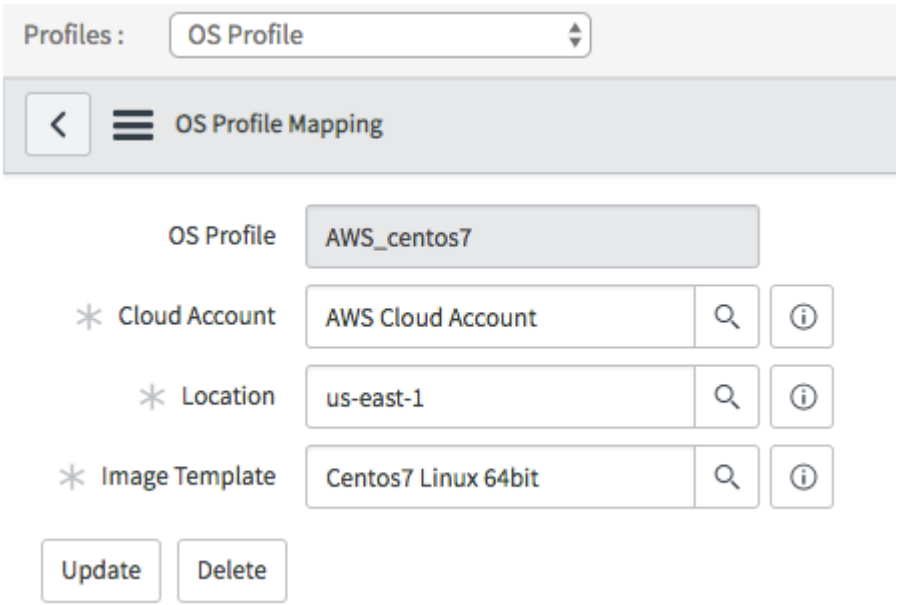
Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Ressourcenprofile**.
2. Wählen Sie in der Liste **Profile** die Option **BS-Profil** aus, und klicken Sie dann auf **Neu**.
3. Geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** für das Profil ein, und klicken Sie dann auf **Absenden**.
   Das Profil wird erstellt.
4. Ordnen Sie das Profil einer Vorlage zu.

   a. Klicken Sie in der Liste auf das von Ihnen erstellte Profil.

   b. Klicken Sie in der zugehörigen Liste **BS-Profilzuordnungen** auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
Cloud-Konto	Wählen Sie den Cloud-Konto aus, dem das BS-Profil zugeordnet werden soll.
Standort	Wählen Sie ein Rechenzentrum im Cloud-Konto aus.
Bildvorlage [cmdb_ci_os_template]	Wählen Sie eine Bildvorlage aus, der das Profil zugeordnet werden soll. Klicken Sie auf das Referenzsymbol ( ), um die Details der Vorlage anzuzeigen. **Wichtig:** Kein neues Bildvorlageerstellen. Bildvorlagen muss auf der Seite „Cloud-Accounts“ im Portal für Cloud-Admin. () erkannt werden.**Verwalten** > **Cloud-Accounts**) an. Wenn Sie einer Bildvorlage Anmeldeinformationen hinzufügen, werden die Anmeldeinformationen von allen VMs geerbt, die mithilfe der Vorlage bereitgestellt werden. Siehe Bildvorlagen Anmeldeinformationen hinzufügen.

5. Ordnen Sie das Profil einem Cloud-Skript zu. In diesem Verfahren geben Sie ein vorhandenes Skript an. Siehe Skriptvorlagen und Skript für die Cloud-Initialisierung erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der zugehörigen Liste „Cloud-Skript – BS-Profilzuordnungen“ auf **Neu**, und füllen Sie das Formular aus.

Feld	Beschreibung
Plan [Optional]	Wählen Sie eine Blaupause, um das Skript auf einen bestimmten, in der Blaupause verwendeten Ressourcenblock zu beschränken.
Cloud-Skript	Wählen Sie ein Cloud-Skript aus, dem das Betriebssystemprofil zugeordnet werden soll.
Aktiv	Aktivieren Sie das Kontrollkästchen, wenn das Cloud-Skript nach der Bereitstellung des virtuellen Computers ausgeführt werden soll.
Applikation	Cloud Provisioning and Governance ist automatisch ausgewählt.
BS-Profil	Wenn Sie eine Blaupause angeben, wird das Cloud-Skript ausgeführt, wenn die Blaupause bereitgestellt wird.
Ressourcen-Alias [Optional]	Wenn Sie einen Ressourcenalias für die Blaupause angeben, wird das Cloud-Skript ausgeführt, wenn die Blaupause mit dem angegebenen Ressourcenalias bereitgestellt wird.

b. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
Das **Namensattribut** `[scriptName]` wird in der Liste „Überschreibungen der BS-Profilzuordnung“ aufgeführt.

c. Geben Sie in der Liste „Überschreibungen der BS-Profilzuordnung“ einen Attributnamen und einen Wert ein, die bei der Bereitstellung der Ressource verwendet werden.

Zeitplanprofil erstellen

Sie ordnen einem Instanzzeitplan ein Zeitplanprofil zu. Das Zeitplanprofil gilt für alle neu bereitgestellten Ressourcen, die das Profil verwenden. Beispielsweise können in einem Zeitplanprofil die Wochentage und Tageszeiten angegeben werden, zu denen ein Stapel gestartet und gestoppt werden soll.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Ressourcenprofile**.
2. Wählen Sie in der Liste **Profile** die Option **Zeitplanprofil** aus.
3. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** ein, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Zeitplan	Wählen Sie einen vorhandenen Zeitplan aus, oder definieren Sie einen benutzerdefinierten Zeitplan. Ein Zeitplan ist eine Regel, die bestimmte Zeiträume für Aktionen einschließt oder ausschließt. Verwenden Sie zum Definieren eines Zeitplans das **Systemzeitplaner**-Modul. Siehe Zeitplan definieren
Multiplikator	Automatisch ausgefüllter Wert zwischen `0` und `1`: Der Bruchteil der Zeit, in dem erwartet wird, dass ein Stapel mit diesem Zeitplan eingeschaltet ist.

Zugehörige Informationen

Bei Bedarf alle Rechenzentren in einem Servicekonto erkennen

Bildvorlagen Anmeldeinformationen hinzufügen

Wenn Sie einer Bildvorlage Anmeldeinformationen hinzufügen, werden die Anmeldeinformationen von allen VMs geerbt, die mithilfe der Vorlage bereitgestellt werden.

Vorbereitungen

- Erforderliche Rolle: cloud_admin
- Eine Reihe von Anmeldeinformationen für die Standardauthentifizierung muss vorhanden sein.

Prozedur

1. Führen Sie eine der folgenden Aktionen aus:
   - Wenn der VM-Vorlage ein BS-Profil zugeordnet ist:
     a. Öffnen Sie das BS-Profil (**Verwalten** > **Ressourcenprofile**) an.
     b. Klicken Sie in der zugehörigen Liste „BS-Profilzuordnungen“ auf den **Namen** der Vorlage in der Spalte **Bildvorlage**.
   - Navigieren Sie für VMware-Vorlagen zu **Alle** > **Konfiguration** > **VMware** > **VM-Vorlagen**.
2. Wählen Sie auf dem Formular „Image“ die **Anmeldeinformationen** der Standardauthentifizierung aus.
3. Klicken Sie auf **Aktualisieren**.

Öffentliches AWS-Image zu Cloud Provisioning and Governance hinzufügen

Sie können jedes AWS-Image in einem BS-Profil auswählbar machen.

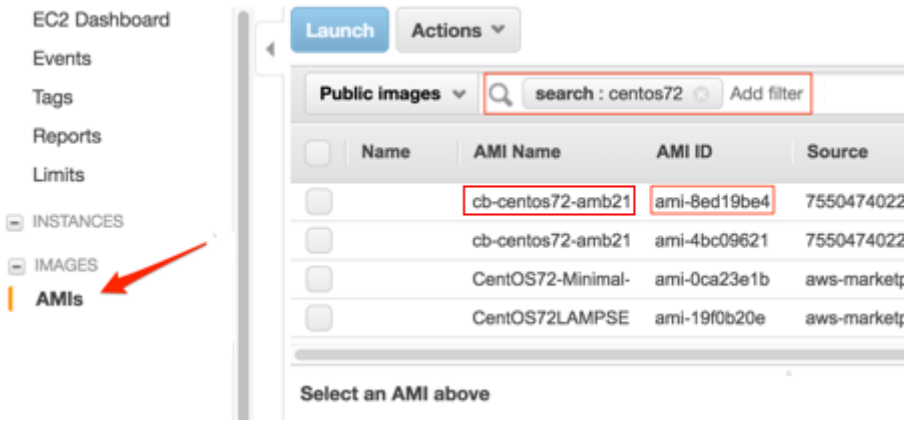
Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wählen Sie in der AWS-Konsole den EC2-Service aus, und klicken Sie dann auf **BILDER** > **AMIs**.



2. Filtern Sie die Liste der Images, und notieren Sie sich die Werte für **AMI Name** und **AMI ID** für das gewünschte Image.
3. Geben Sie in der Instanz `cmdb_ci_os_template.list` in dem Textfeld **Filternavigator** zum Öffnen der Tabellen-Images [cmdb_ci_os_template] ein, und klicken Sie dann auf **Neu** .
4. Tragen Sie auf dem Formular **Image** die folgenden Werte ein:

Feld	Wert
Objekt-ID	**AMI ID**-Wert von AWS.
Name	Ein aussagekräftiger Name, der auf dem **AMI Name**-Wert von AWS basiert.
Gast-BS	Betriebssystem.

5. Im Feld **Berechtigungsnachweise** klicken Sie auf die Lupe und dann auf **Neu** auf der Berechtigungsnachweis-Seite.
6. Klicken Sie in der Liste auf **Grundlegende Berechtigungsnachweise**.
7. Geben Sie im Formular „Standard-Berechtigungsnachweise“ einen aussagekräftigen **Namen** für den Berechtigungsnachweis ein.
8. Geben Sie einen **Benutzernamen** ein, den Sie für Instanzen verwenden, die aus diesem Image bereitgestellt werden.

   In AWS werden SSH-Schlüssel verwendet, weswegen kein Passwort erforderlich ist.

   Hinweis: Wenn der Name `ec2-user` oder `root` nicht funktioniert, wenden Sie sich an Ihren AMI-Provider.

Richtlinien für Benutzernamen

Typ	Name
Amazon Linux	`ec2-user`
RHEL	`ec2-user` oder `root`
Ubuntu	`ubuntu` oder `root`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Name
Centos	`centos`
Fedora	`ec2-user`
SUSE	`ec2-user` oder `root`

9. Klicken Sie auf **Senden**, um das Formular „Basic Auth Credentials“ zu schließen.
10. Klicken Sie mit der rechten Maustaste auf den Header, und klicken Sie auf **Speichern**, um die aktuelle Konfiguration des neuen Image-Datensatzes zu speichern.
    In der Liste „zugehörige Elemente“ können Sie sehen, dass das Image dem angegebenen Datencenter zugeordnet ist.
11. Klicken Sie auf **Aktualisieren**, um das öffentliche Image in einem OS-Profil auswählbar zu machen.
    Dieser Schritt erstellt auch eine Beziehung zwischen dem öffentlichen Image und dem logischen Datencenter (LDC) in der CMDB.

Öffentliches Azure-Image zu Cloud Provisioning and Governance hinzufügen

Sie können jedes Azure-Image in einem BS-Profil auswählbar machen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Notieren Sie sich in der Azure-Befehlszeilenschnittstelle (CLI) die Werte für **Offer**, **Publisher**, **Sku** und **Version**.

   In der Befehlszeile können Sie nach „offer“ (Angebot) oder nach „publisher“ (Herausgeber) oder nach beidem suchen, wie im Beispiel gezeigt. Jeder Einzelposten ist ein Image einer bestimmten Version von CentOS von OpenLogic.

   Sie können den folgenden Beispielbefehl in der CLI verwenden, um die Werte abzurufen:
   `az vm image list -f Windows --output table`

```
:~ jsher.able$ az vm image list --offer CentOS --publisher OpenLogic --all --output table
Offer     Publisher    Sku    Urn                Version
--------  -----------  -----  -----------------  -----------
CentOS    OpenLogic    6.5    OpenLogic:CentOS   6.5.201501
CentOS    OpenLogic    6.5    OpenLogic:CentOS   6.5.201503
CentOS    OpenLogic    6.5    OpenLogic:CentOS   6.5.201506
CentOS    OpenLogic    6.5    OpenLogic:CentOS   6.5.20150904
CentOS    OpenLogic    6.5    OpenLogic:CentOS   6.5.20160309
CentOS    OpenLogic    6.5    OpenLogic:CentOS   6.5.20170207
```

2. Geben Sie in der Instanz `cmdb_ci_os_template.list` in dem Textfeld **Filternavigator** zum Öffnen der Tabellen-Images [cmdb_ci_os_template] ein, und klicken Sie dann auf **Neu** .
3. Konfigurieren Sie das Formularlayout, um **Offer** (Angebot), **Serial number** (Seriennummer), **Version** und **Vendor** (Lieferant) anzuzeigen.
4. Tragen Sie auf dem Formular Image die folgenden Werte ein:

Feld	Wert
Objekt-ID	Geben Sie `/Herausgeber/Angebot/SKU/Version` ein. Sie können diese Werte von der Azure-Befehlszeilenschnittstelle abrufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Wert
	Beispiel: `/OpenLogic/CentOS/6.5/6.5.201501`.
Name	Aussagekräftiger Name, der die Version des Betriebssystems darstellt, `CentOS 6.5` im Beispiel.
Gast-BS	Betriebssystem.
Angebot	Wert **Offer** (Angebot) von Azure.
Seriennummer	Wert **Sku** von Azure.
Version	Wert **Version** von Azure.
Lieferant	**a.** Klicken Sie auf die Lupe und dann auf **Neu**. **b.** Geben Sie im Feld **Name** den Wert für **Publisher** (Herausgeber) von Azure ein. **c.** Klicken Sie auf **Absenden**.

5. Im Feld **Berechtigungsnachweise** klicken Sie auf die Lupe und dann auf **Neu** auf der Berechtigungsnachweis-Seite.
6. Klicken Sie in der Liste auf **Grundlegende Berechtigungsnachweise**.
7. Geben Sie im Formular „Standard-Berechtigungsnachweise“ einen aussagekräftigen **Namen** für den Berechtigungsnachweis ein.
8. Geben Sie einen **Benutzernamen** und ein **Passwort** zum Nutzen von Instanzen ein, die aus diesem Image bereitgestellt werden.
9. Klicken Sie auf **Senden**, um das Formular „Basic Auth Credentials“ zu schließen.
10. Klicken Sie mit der rechten Maustaste auf den Header, und klicken Sie auf **Speichern**, um die aktuelle Konfiguration des neuen Image-Datensatzes zu speichern.
    In der Liste „zugehörige Elemente“ können Sie sehen, dass das Image dem angegebenen Datencenter zugeordnet ist.
11. Klicken Sie auf **Aktualisieren**, um das öffentliche Image in einem OS-Profil auswählbar zu machen.
    Dieser Schritt erstellt auch eine Beziehung zwischen dem öffentlichen Image und dem logischen Datencenter (LDC) in der CMDB.

IPAM-Integration

Verwenden Sie ein IP-Adressverwaltungstool (IPAM) wie Infoblox, um Cloud-IP-Adressen, Netzwerke und Subnetze in Ihren Cloud-Katalogangeboten zu verwalten. Es ist jedoch zu beachten, dass diese Funktionalität von unseren vorlagenbasierten Cloud-Katalogen nicht unterstützt wird.

Infoblox-Integration

Standardmäßig unterstützt Cloud Provisioning and Governance die Infoblox-Integration. Sie können Infoblox-Anmeldeinformationen erstellen und dann einen Infoblox-Instanzdatensatz einrichten. Siehe Infoblox-Server registrieren für Anweisungen.

Hinweis: Die IPAM-Integration wird für vorlagenbasierte Cloud-Katalogelemente nicht unterstützt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Diese Integration wird nur mit Legacy-Blueprints unterstützt. Weitere Informationen finden Sie in diesem Knowledge Base -Artikel.

Subnetze

Wenn Sie Subnetze in Ihren AWS- und Azure-Clouds haben, findet Cloud Provisioning and Governance diese, wenn Discovery für ein Servicekonto oder Cloud-Konto ausgeführt wird.

Hinweis: Wenn Sie Netzwerke und Subnetze in einer VMware vSphere-Plattform haben, erstellt Discovery keine Subnetzdatensätze in der CMDB und kann das Subnetz nicht dem entsprechenden Netzwerk zuordnen. Sie müssen die Datensätze manuell erstellen.

Infoblox-Server registrieren

Für die Integration von Infoblox müssen Sie einen Infoblox-Datensatz erstellen und ihn den entsprechenden Anmeldeinformationen zuordnen, um Ihren Infoblox-Server bei der Instanz zu registrieren.

Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_admin
- Erstellen Sie Infoblox-Anmeldeinformationen .

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Netzwerke und IPAM** > **IPAM-Anbieter** > **Infoblox**.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Namen** ein, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Feld	Beschreibung
URL	Geben Sie die URL des Infoblox-Servers ein.
Anmeldeinformationen	Wählen Sie die Infoblox-Anmeldeinformationen aus.

IP-Pool erstellen

Erstellen Sie einen IP-Pool, um ein Cloud-Subnetz einer IPAM-Provider-Instanz zuzuordnen.

Vorbereitungen

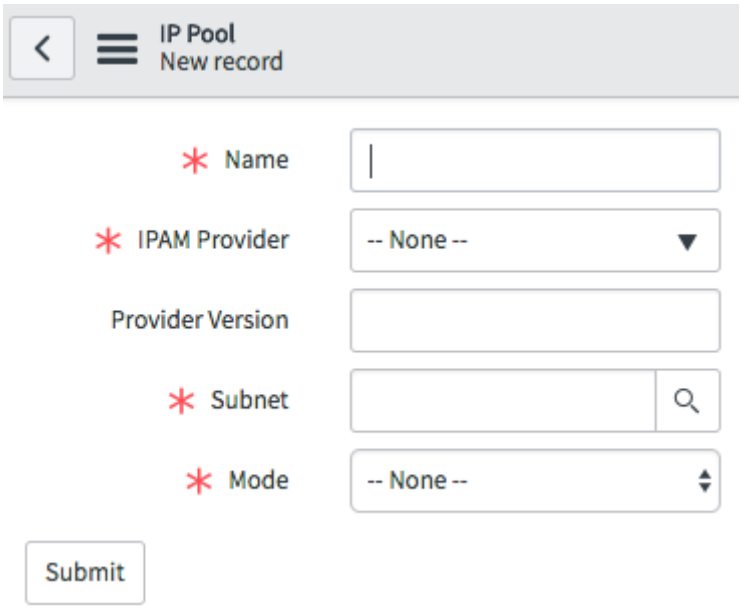
- Erforderliche Rolle: sn_cmp.cloud_admin
- Erstellen Sie Infoblox-Anmeldeinformationen , und registrieren Sie einen Infoblox-Server.
- Führen Sie Discovery für den Cloud-Konto aus, um Subnetze zu finden, oder erstellen Sie Cloud-Subnetze manuell.

Hinweis: Diese Funktionalität wird für unsere vorlagenbasierten Cloud-Kataloge nicht unterstützt.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Netzwerke und IPAM**.
2. Klicken Sie auf der Registerkarte **IP-Pools** auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Namen** ein, und füllen Sie dann das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
IPAM-Anbieter	Wählen Sie einen IPAM-Provider aus.
Provider-Instanz	Wählen Sie eine Instanz für den Provider aus.
Providerversion	Geben Sie eine Version für den Provider ein.
Subnetz	Wählen Sie ein Subnetz aus. Wählen Sie für AWS oder Azure ein erkanntes Subnetz aus, das in AWS oder Azure konfiguriert wurde. Für VMware kopieren Sie den CIDR-Bereich aus dem IPAM-Tool, und fügen Sie den CIDR-Bereich in dieses Feld ein. Weitere Informationen finden Sie unter Cloud-Subnetz erstellen.
Modus	Wählen Sie basierend auf dem Provider, für den Sie diesen IP-Pool erstellen, einen Modus aus. Der Modus hängt vom Provider ab.

3. Klicken Sie auf **Absenden**.

Ergebnisse
Das zugehörige Subnetz wird in der zugehörigen Liste **Subnetz** am unteren Rand des Formulars angezeigt.

Cloud-Subnetz erstellen

Wenn Ihr VMware vSphere-Konto über Subnetze verfügt, erstellen Sie in der Instanz einen Cloud-Subnetz-Datensatz.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Netzwerke und IPAM**.
2. Klicken Sie auf der Registerkarte **IP-Pools** auf **Neu**, um einen neuen Datensatz zu erstellen.
3. Klicken Sie im Feld **Subnetz** auf das Suchsymbol.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Liste der Cloud-Subnetze wird angezeigt.

4. Klicken Sie auf **Neu**.
5. Füllen Sie die Formularfelder aus (siehe Tabelle).

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.
Status	Behalten Sie den Statuswert **Installiert** bei.
CIDR/ Gateway/ Subnetzmaske	Geben Sie die dem Subnetz zugeordnete CIDR, die IP-Adresse des Gateways und die Subnetzmaske ein. Für VMware sind die Felder „CIDR“, „Gateway“ und „Subnetzmaske“ obligatorisch.
Primäres und sekundäres DNS	Geben Sie die DNS-Werte ein. Für VMware, ist das Feld „Primäre DNS“ obligatorisch.

6. Klicken Sie auf **Absenden**.

Beziehung zwischen einem VMware-Netzwerk und einem Subnetz erstellen

Wenn Sie VMware-Netzwerke und Subnetze erkennen, müssen Sie manuell eine Beziehung zwischen beiden erstellen.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn keine Beziehung vorhanden ist und ein Benutzer ein virtuelles Netzwerk und Subnetz im Cloudbenutzerportal auswählen muss, kann ein Fehler auftreten.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Service-Accounts**.
2. Öffnen Sie das Rechenzentrum, das das VMware-Cloud-Netzwerk enthält.

   Hinweis: VMware-Cloud-Netzwerke werden in der Tabelle „VMware vCenter-Netzwerk“ [cmdb_ci_vcenter_network] gespeichert. AWS- und Azure-Cloud-Netzwerke werden in der Tabelle „Cloud-Netzwerke“ `[cmdb_ci_network]` gespeichert.

3. Klicken Sie unter **Zugehörige Elemente** auf das Pluszeichen, um eine neue Beziehung hinzuzufügen.
4. Stellen Sie sicher, dass das Kontrollkästchen **Vorgeschlagene Beziehungen verwenden** aktiviert ist, und wählen Sie dann die Beziehung **Enthält (Übergeordnet)** aus.
5. Erstellen Sie unter **Filter** den erforderlichen Filter, um das Subnetz zu finden.
6. Aktivieren Sie unter **Konfigurationselemente** das Kontrollkästchen neben dem Subnetz.
7. Klicken Sie im Abschnitt **Beziehungen** auf das Pluszeichen.
   Die Beziehung wird der Liste hinzugefügt.
8. Klicken Sie auf **Speichern und Beenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Adressen für VMware vSphere-VMs in InfoBlox reservieren

Erstellen Sie zum Zeitpunkt der Bereitstellung der virtuellen Computer eine Richtlinie zum Reservieren von IP-Adressen für VMware vSphere-VMs in Infoblox.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Sie können eine Richtlinie erstellen, die aufgerufen wird, wenn eine VMware-VM bereitgestellt wird, um eine IP-Adresse von Infoblox zu erhalten. Vor der Bereitstellung des virtuellen Computers ruft die Instanz Infoblox auf, das einen Hostdatensatz mit der IP-Adresse erstellt.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

Feld	Beschreibung
Richtlinienname	Geben Sie einen beschreibenden Namen ein.
Richtlinienauslöser	Wählen Sie **Bei Ressourcenvorgang** aus.
Ressourcenblock	Wählen Sie **ResourceBlock Virtual Server** (ResourceBlock Virtueller Server) aus.
Vorgang	Wählen Sie die **Virtual Server interface provision** (Schnittstellenbereitstellung für virtuellen Server) aus.
Moment	Wählen Sie **Vor dem Vorgang** aus.

3. Klicken Sie auf **Absenden**, um die Richtlinie zu veröffentlichen.
4. Erstellen Sie eine Richtlinienregel für die Richtlinie.
5. Geben Sie im Bedingungsgenerator eine Bedingung für die Suche nach der vSphere-VM an.
6. Auswahlvorgang **Anforderung von** > **beginnt mit** und geben Sie `vSphere`ein.
7. Klicken Sie auf **Aktualisieren**.
8. Klicken Sie in der zugehörigen Liste **Richtlinienregelaktion** auf **Neu**, um eine Richtlinienaktion zu erstellen.
9. Wählen Sie **IP-Adressverwaltung** im Dialogfeld **Create Policy Rule Action** (Richtlinienregelaktion erstellen) aus.
10. Geben Sie einen Namen in das Feld **Aktionsname** ein, wählen Sie **Infoblox** in der Liste **Provider-Typ** und dann in der Liste **IPAM-Methodenname** die Option **IP-Adresse reservieren** aus.
11. Klicken Sie auf **Absenden**.
12. Geben Sie im Abschnitt **Richtlinienregel-Aktionsattribute** den Domänennamen Ihres Netzwerks im Feld **DNSSuffix** ein.
    Beispiel: `corp.servicenow.com`. Die Werte für alle anderen Eigenschaften sind bereits ausgefüllt.
13. Klicken Sie auf **Aktualisieren**, und veröffentlichen Sie die Richtlinie erneut.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

IP-Adressen für AWS- und Azure-VMs in Infoblox registrieren

Erstellen Sie eine Richtlinie zum Reservieren von IP-Adressen für AWS- und Azure-VMs in Infoblox, nachdem diese virtuellen Computer bereitgestellt wurden.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Wenn AWS- und Azure-VMs bereitgestellt werden, werden ihnen automatisch IP-Adressen zugewiesen. Sie können eine Richtlinie erstellen. Die Richtlinie wird aufgerufen, sobald diese virtuellen Computer bereitgestellt wurden, um ihre IP-Adressen abzurufen und diese IP-Adressen in Infoblox zu registrieren.

Hinweis: Diese Funktionalität wird für unsere vorlagenbasierten Cloud-Kataloge nicht unterstützt.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

Feld	Beschreibung
Richtlinienname	Geben Sie einen beschreibenden Namen ein.
Richtlinienauslöser	Wählen Sie **Bei Ressourcenvorgang** aus.
Ressourcenblock	Wählen Sie **ResourceBlock Virtual Server** (ResourceBlock Virtueller Server) aus.
Vorgang	Wählen Sie die **Virtual Server interface provision** (Schnittstellenbereitstellung für virtuellen Server) aus.
Moment	Wählen Sie **Vor dem Vorgang** aus.

3. Klicken Sie auf **Absenden**, um die Richtlinie zu veröffentlichen.
4. Erstellen Sie eine Richtlinienregel für die Richtlinie.
   Geben Sie im Bedingungsgenerator zwei Bedingungen für die Suche nach AWS- und Azure-VMs an. Auswahlvorgang **Anforderungsformular** > **beginnt mit** und geben Sie `AWS`ein. Geben Sie eine andere Bedingung für Azure an.
5. Klicken Sie auf **Aktualisieren**.
6. Klicken Sie in der zugehörigen Liste **Richtlinienregelaktion** auf **Neu**, um eine Richtlinienaktion zu erstellen.
7. Wählen Sie **IP-Adressverwaltung** im Dialogfeld **Create Policy Rule Action** (Richtlinienregelaktion erstellen) aus.
   Geben Sie einen Namen in das Feld **Aktionsname** ein, wählen Sie **Infoblox** in der Liste **Provider-Typ** und dann in der Liste **IPAM-Methodenname** die Option **IP-Adresse registrieren** aus.
8. Klicken Sie auf **Absenden**.
9. Geben Sie im Abschnitt **Richtlinienregel-Aktionsattribute** den Domänennamen des Netzwerks Ihres Unternehmens im Feld **DNSSuffix** ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel: `corp.servicenow.com`. Die Werte für alle anderen Eigenschaften sind bereits ausgefüllt.

10. Klicken Sie auf **Aktualisieren**, und veröffentlichen Sie die Richtlinie erneut.

Hostdatensatz in Infoblox löschen

Wenn die Bereitstellung eines virtuellen Computers aufgehoben wird, löschen Sie den Hostdatensatz aus Infoblox. Durch das Löschen des Hostdatensatzes kann diese IP-Adresse für andere virtuelle Computer verfügbar sein und verwendet werden.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Bedingungen** > **Richtlinien**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder im Formular „Richtlinie“ aus (siehe Tabelle).

Feld	Wert
Richtlinienname	Geben Sie einen beschreibenden Namen ein.
Richtlinienauslöser	Wählen Sie **Bei Ressourcenvorgang** aus.
Ressourcenblock	Wählen Sie **ResourceBlock Virtual Server** (ResourceBlock Virtueller Server) aus.
Vorgang	Wählen Sie die **Virtual Server interface De-provision** (Schnittstellenbereitstellung für virtuellen Server aufheben) aus.
Moment	Wählen Sie **Nach dem Vorgang** aus.

4. Klicken Sie auf **Absenden**, um die Richtlinie zu veröffentlichen.
5. Erstellen Sie eine Richtlinienregel für die Richtlinie, und klicken Sie auf **Aktualisieren**.
6. Klicken Sie in der zugehörigen Liste **Richtlinienregelaktion** auf **Neu**, um eine Richtlinienaktion zu erstellen.
7. Wählen Sie **IP-Adressverwaltung** im Dialogfeld **Create Policy Rule Action** (Richtlinienregelaktion erstellen) aus.
   Geben Sie einen Namen in das Feld **Aktionsname** ein, wählen Sie **Infoblox** in der Liste **Provider-Typ** und dann in der Liste **IPAM-Methodenname** die Option **IP-Adresse freigeben** aus.
8. Klicken Sie auf **Absenden**.
9. Geben Sie im Abschnitt **Richtlinienregel-Aktionsattribute** den Domänennamen des Netzwerks Ihres Unternehmens im Feld **DNSSuffix** ein.
   Beispiel: `corp.servicenow.com`. Die Werte für alle anderen Eigenschaften sind bereits ausgefüllt.
10. Klicken Sie auf **Aktualisieren**, und veröffentlichen Sie die Richtlinie erneut.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Support für kontinuierliche Bereitstellung (Konfigurationsverwaltung)

Die Cloud Provisioning and Governance-Anwendung unterstützt die Integration in Lösungen zur kontinuierlichen Bereitstellung (auch bekannt als Konfigurationsverwaltung). Ansible wird als Standard-Provider für Konfigurationsverwaltung unterstützt.

Die Anwendung Cloud Provisioning and Governance unterstützt Konfigurationsverwaltungs-Provider auf zwei Arten:

- **Ansatz auf Basis des Anwendungsprofils**: Erstellen Sie ein Anwendungsprofil für eine Entität, und wählen Sie im Bestellkatalogformular dieses Profil aus, um diese Entität bereitzustellen. Jedes Profil verfügt über eine installierbare Konfiguration. Sie können mehrere Anwendungsprofile erstellen, z. B. eines für PostgreSQL und eines für Apache. Jedes Profil kann einem Konfigurationsverwaltungs-Provider zugeordnet werden. Im Cloudbenutzerportal wird basierend auf dem von Ihnen ausgewählten Profil ein Konfigurationsraster mit Attributen und Werten für den jeweiligen Konfigurationsverwaltungs-Provider angezeigt. Sie können alle Werte im Bestellformular ändern und die Entität bereitstellen.
- **Ansatz auf Basis des Ressourcenblocks**: Verwenden Sie einen Ressourcenblock wie Apache2 in einer Blaupause, um eine Entität darzustellen, die von einem Konfigurationsverwaltung-Provider verwaltet wird. Derselbe Ressourcenblock kann zur Unterstützung von mehr als einer Entität derselben Art verwendet werden. Beispielsweise kann ein Apache2-Ressourcenblock zur Unterstützung mehrerer Apache2-Server verwendet werden. Wählen Sie im Bestellkatalogformular einen Provider-Typ aus, und wählen Sie dann einen Provider aus. Basierend auf dem spezifischen Provider werden Konfigurationsverwaltungsattribute und -werte angezeigt. Sobald Sie die Entität bereitgestellt haben, können Sie die Konfiguration des Ressourcenblocks speichern und in der CMDB für die zukünftige Verwendung ablegen.
- **Aktionen nach der Bereitstellung während der Katalogbereitstellung**: Anwender können in jedem Katalog, der eine VM bereitstellt, einen Ansible-Auftrag als Schritt nach der Bereitstellung aufrufen. Dies wird als Tag-2-Vorgang ausgeführt, sobald die VM-Installation abgeschlossen ist. Weitere Informationen zu den Prozessen finden Sie unter https://www.servicenow.com/community/itom-blog/cpg-calling-ansible-job-as-post-provision-step-for-cloud-catalog/ba-p/2271552 und https://www.servicenow.com/community/itom-blog/cpg-calling-ansible-job-as-day2-operation/ba-p/2270969 .

Wichtig: Beginnend mit dem Release Orlando sind Blaupausen für die Cloud-Bereitstellung in Instanzen verfügbar, für die ein Upgrade von einem früheren Release durchgeführt wurde. Sie können jedoch keine neuen Blaupausen erstellen. Vorhandene Blaupausen und Katalogelemente aus diesen Blaupausen bleiben davon unberührt und funktionieren weiterhin.

Beschreibung

Schritt	Ziel	Siehe diese Themen
1. Erstellen Sie Anmeldeinformationen für Ansible.	Aktivieren Sie Cloud Provisioning and Governance, um auf den Konfigurations-Provider mit den erforderlichen Anmeldeinformationen zuzugreifen.	Ansible Tower-Benutzernamen und -Passwort konfigurieren
2. Erstellen Sie den Workload-Provider-Typ und dann den Provider.	Konfigurieren Sie Cloud Provisioning and Governance, mit dem Konfigurationsverwaltungs-Provider Ihrer Wahl zu arbeiten. Führen Sie dann Discovery für den Provider	Erstellen Sie einen Workload-Provider-Typ und Ansible-Konfigurationsverwaltungs-

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritt	Ziel	Siehe diese Themen
	mit den von Ihnen angegebenen Anmeldeinformationen aus, um die Ressourcen zu finden, die der Provider bereits besitzt.	Provider erstellen und Discovery ausführen
3. Erstellen Sie ein Anwendungsprofil mit einer Zuordnung.	Erstellen Sie das Profil, das die Anwendung definiert, die vom Konfigurationsverwaltungs-Provider verwaltet wird. Das Profil basiert auf den erkannten Beständen beim Provider.	Anwendungsprofil erstellen
4. Erstellen Sie eine Blaupause.	Erstellen Sie eine Blaupause mit den Vorgängen *BootstrapNode*, *Register Node* und *ExecuteConfigPackages* für die virtuelle Ressource, die der Konfigurations-Provider verwaltet. Sie können auch die Eingabeparameter im Formular anpassen, damit der Benutzer wichtige Eingaben auswählen kann, z. B. die Anwendungsprofilvorlage, die Organisation und die Anmeldeinformations-ID.	
5. Stellen Sie im Cloudbenutzerportal eine Ressource bereit.	Die Ressource muss bereitgestellt werden, wobei der Stapelstatus die Schritte *BootstrapNode*, *Register Node* und *ExecuteConfigPackages* angibt.	

Ansible Tower-Benutzernamen und -Passwort konfigurieren

Konfigurieren Sie Ansible Tower-Anmeldeinformationen, um über Ihre Instanz auf die Ansible Automation Engine zuzugreifen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Navigieren zu **Alle** > **Orchestration** > **Anmeldeinformationen**und klicken Sie dann auf **Neu**.
2. Klicken Sie auf **Ansible Tower-Anmeldeinformationen**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle):

   Zur Integration von Cloud Provisioning and Governance mit dem Ansible-Konfigurationsverwaltungskonto müssen Benutzername und Passwort für das Administratorkonto in Ansible konfiguriert werden.

Formularfelder für Ansible Tower-Anmeldeinformationen

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Benutzername/ Passwort	Geben Sie die Authentifizierungsinformationen für den Ansible Tower-Benutzer mit Administratorrechten ein.

Hinweis: Sie müssen keine anderen Felder konfigurieren

Erstellen Sie einen Workload-Provider-Typ

Erstellen Sie einen Workload-Provider-Typ für jeden neuen Konfigurationsverwaltungs-Provider. Diese Informationen werden im Bestellkatalogformular als Verwaltungsattribute angezeigt, die Ihre Benutzer auswählen können, wenn sie eine virtuelle Ressource über einen Konfigurationsverwaltungs-Provider bereitstellen.

Vorbereitungen

Erforderliche Rolle: cloud_admin

Prozedur

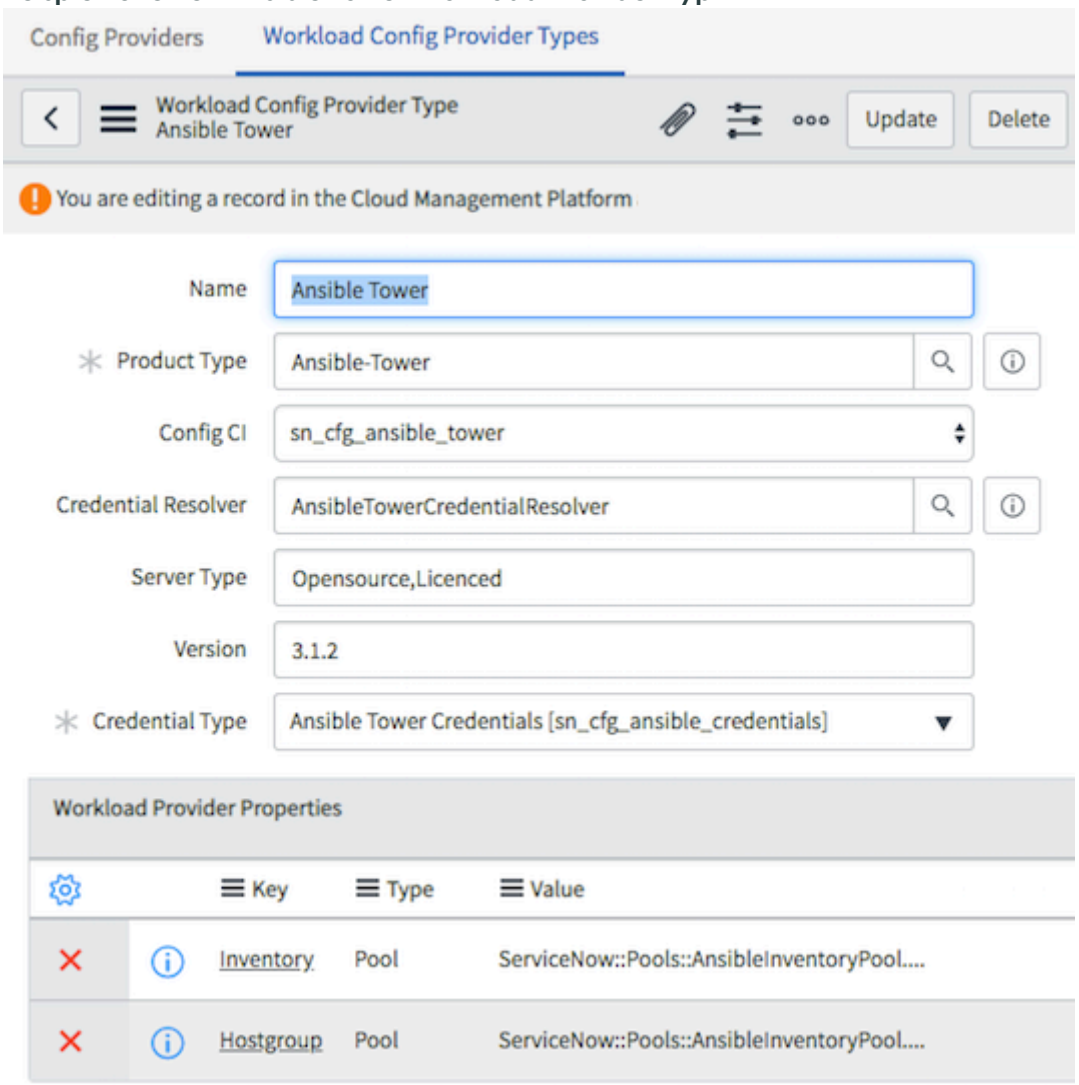
1. Navigieren Sie im Cloud-Administrationsportal zu **Verwalten** > **Konfigurationsverwaltung**.
2. Klicken Sie auf **Workload-Konfigurations-Provider-Typen** und dann auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).

Formular „Workload-Konfigurations-Provider-Typ“

Feld	Beschreibung
Name	Geben Sie einen Namen für den Workload-Provider-Typ ein.
Produkttyp	Ein Cloud-Produkttyp aus der Liste
Konfigurations-CI	Wählen Sie die für den Provider erstellte Konfigurationstabelle aus der Liste aus, die die erkannten Ressourcen anzeigt.
Resolver für Anmeldeinformationen	Wählen Sie einen Anmeldeinformations-Resolver aus der Liste aus.
Servertyp	Wählen Sie den Servertyp für den Provider aus, z. B. „OpenSource“, „Enterprise“ usw.
Version	Geben Sie eine Version für den Provider ein.
Anmeldeinformationstyp	Wählen Sie die Tabelle aus, in der die Anmeldeinformationen für diesen Provider gespeichert sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für einen Ansible Tower-Workload-Provider-Typ



4. Fügen Sie im Abschnitt **Workload-Provider-Eigenschaften** Eigenschaften für den Workload-Typ hinzu.
   Zusätzlich zu den vorhandenen Eigenschaften können Sie weitere Eigenschaften hinzufügen. Workload-Provider-Eigenschaften werden im Bestellkatalogformular (im Cloudbenutzerportal) als Verwaltungsattribute angezeigt.

   Für einen Ansible-Anbietertyp sind beispielsweise **Bestand**und **Hostgruppe** obligatorisch. Die Werte für diese Eigenschaften stammen aus Ressourcenpools.

5. Klicken Sie auf **Absenden**.

Ansible-Konfigurationsverwaltungs-Provider erstellen und Discovery ausführen

Erstellen Sie einen Ansible-Konfigurationsverwaltungsanbieter, und führen Sie dann Discovery für den Anbieter aus, um seine Ressourcen zu finden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Stellen Sie sicher, dass Sie einen Ansible-Server und Ansible-Anmeldeinformationenhaben.
- Wenn Sie Ansible Tower Version 3.6.x oder höher verwenden möchten, müssen Sie die Eigenschaft mid.cmp.ansible.api_version auf V2 festlegen. Sie können auf diese Eigenschaft im Abschnitt „Eigenschaften“ des Moduls „MID-Server“ zugreifen.
- Erforderliche Rolle: cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Wichtig: Ab Release Orlando sind die Cloud Provisioning Blueprints für Instanzen verfügbar, die von einem früheren Release aktualisiert wurden. Sie können jedoch keine Blueprints erstellen. Vorhandene Blueprints und aus diesen Blueprints erstellte Katalogelemente sind davon nicht betroffen und funktionieren weiterhin.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Verwalten** > **Konfigurationsverwaltung**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder des Formulars aus.

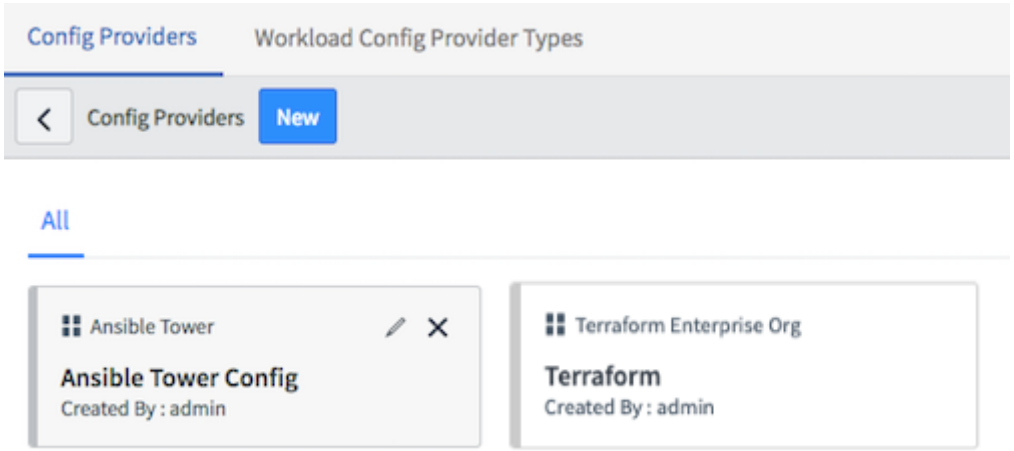
   Hinweis: Die meisten Informationen, die zum Erstellen eines Ansible-Konfigurationsverwaltungs-Providers erforderlich sind, stammen aus den Ansible Tower -Servereinstellungen.

Feld	Beschreibung
Name	Beschreibender Name für den Konfigurationsanbieter.
Organisation	Ansible Tower Organisation für die Zugriffssteuerung Sie können diese Informationen über die Konsole des Konfigurationsverwaltungs-Providers abrufen.
URL	URL von Ansible Tower. Geben Sie die vollständige URL von Ansible Tower einschließlich `https://` ein.<IP> protocol.
Anbieter	Konfigurationsanbietertyp. Wählen Sie in der Dropdown-Liste **Ansible Tower** aus.
Servertyp	Ansible Tower-Servertyp.
Referenz	Anmeldeinformationen für den Zugriff auf den Ansible-Server. Weitere Informationen zum Erstellen von Anmeldeinformationen für den Ansible-Server finden Sie unter Ansible-Anmeldeinformationen.
Version	Version des Konfigurationsanbieters, den Sie erstellen. **Hinweis:** Für Ansible Tower-Versionen über 3.1.2 wählen Sie 3.4.0 aus der Liste aus.

4. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie die Karte Provider für Ansible Tower-Konfiguration.



6. Wählen Sie **Jetzt erkennen aus**, um die Ressourcen im Anbieter für die Ansible-Konfigurationsverwaltung zu finden.

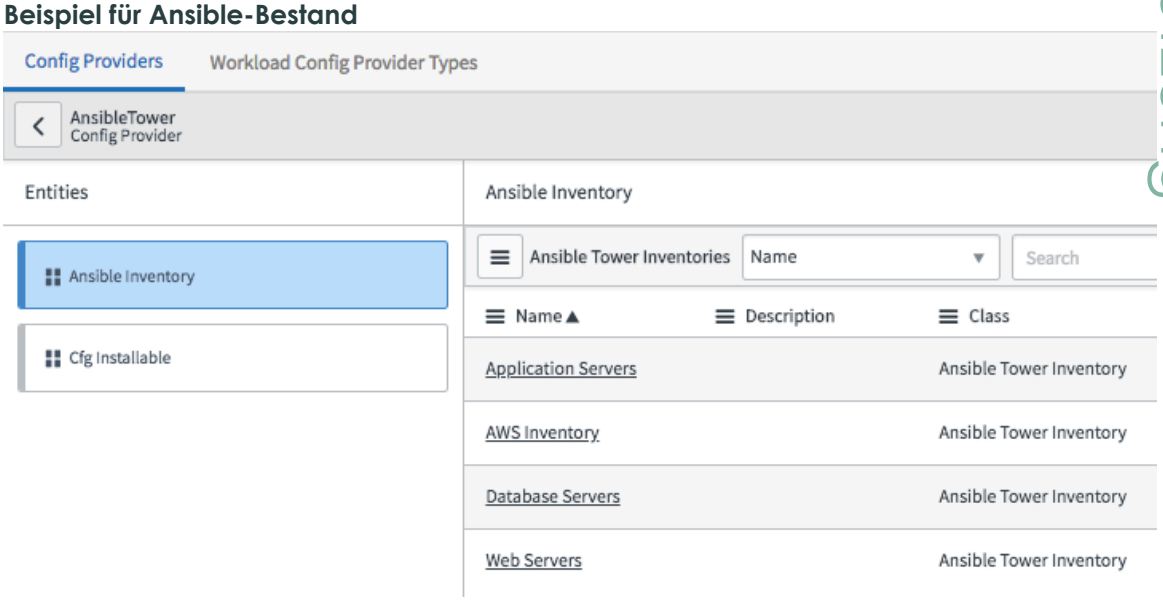
   Hinweis: Wenn Sie Ressourcen über die Schnittstelle des Konfigurationsverwaltungs-Providers bereitstellen oder anderweitig ändern, müssen Sie die Discovery manuell über die Seite „Konfigurations-Provider“ ausführen. Sie können keine geplante Discovery für Konfigurationsverwaltungs-Provider erstellen.

   Die erkannten Ressourcen werden unter **Entitäten** angezeigt.

   Die folgenden Ansible Tower-Ressourcen werden erkannt:

   - **Ansible-Bestand**: Zeigt die erkannten Anwendungen und virtuellen Ressourcen an.
   - **Installierbare Konfiguration**: Zeigt die tatsächlichen Komponenten an, die bei der Installation der Anwendungen ausgeführt werden. Für Ansible sind die Elemente in dieser Liste Auftragsvorlagen, die in diesem Formular auch als Ausführungslisten bezeichnet werden.

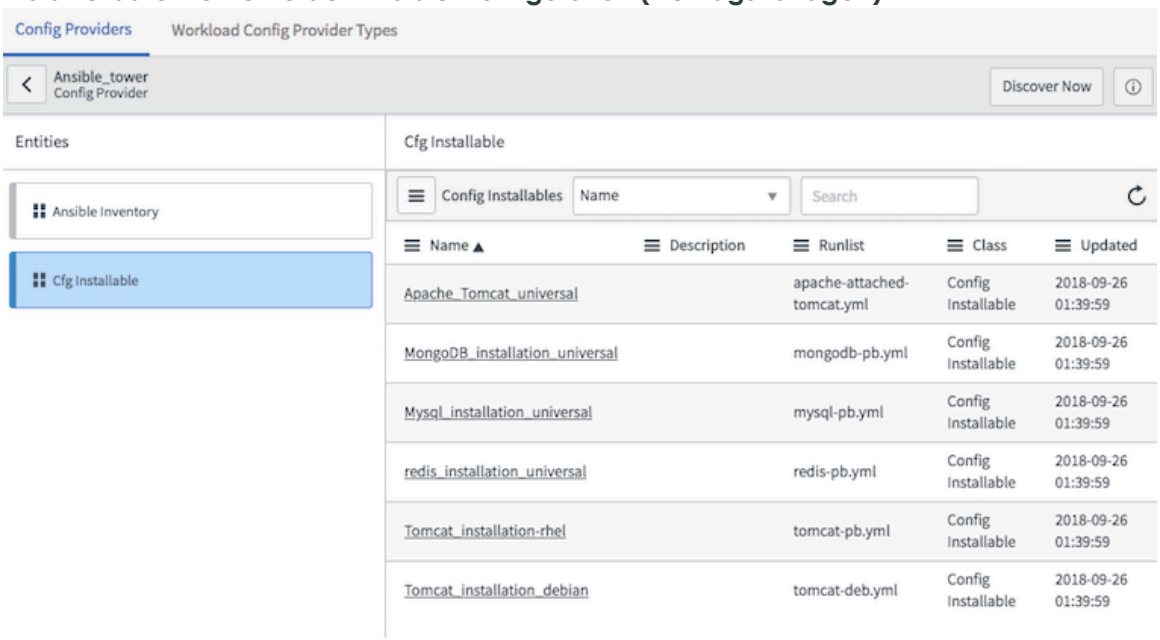
Beispiel für Ansible-Bestand



Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

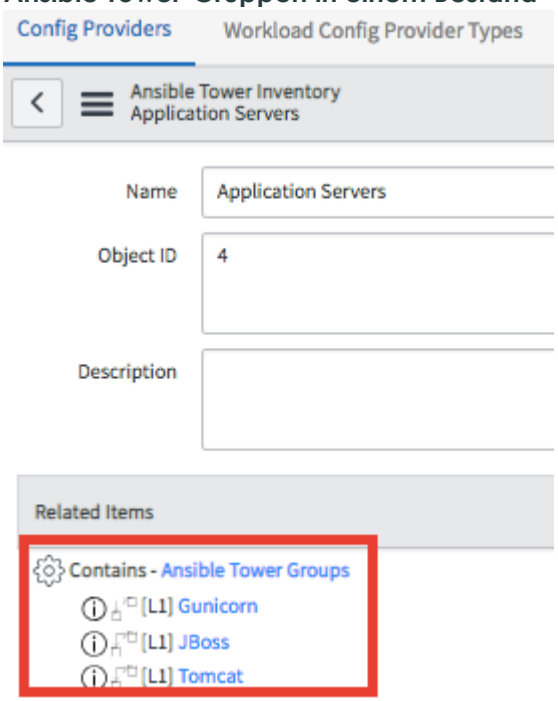
Installierbare Elemente der Ansible-Konfiguration (Auftragsvorlagen)



7. Wählen Sie **Ansible-Bestand** aus, um den Inhalt zu erkunden.

Hinweis: Teilen Sie Benutzern die unterstützten Anwendungen mit, damit sie die richtige Anwendung aus dem Feld **Hostgruppe** im Cloudbenutzerportal auswählen können. Das Feld **Hostgruppe** zeigt alle möglichen Anwendungen (in Ansible Gruppen genannt), nicht nur die, die der Konfigurationsverwaltungs-Provider unterstützt. Daher schlägt die Bereitstellung fehl, wenn der Benutzer eine nicht unterstützte Anwendung auswählt.

Ansible Tower-Gruppen in einem Bestand



Nächste Maßnahme

Nachdem ein Benutzer eine Ressourcebereitgestellt hat, zeigt der Stapelstatus an, wie das System die Schritte „Knoten erstellen“, „Bootstrap“ und „ExecuteConfigPackage“ durchläuft.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können die IP-Adresse einer virtuellen Maschine im Benutzerportal abrufen, indem Sie zu navigieren **Stapel** > **{Kategorie}** und Auswahl der neuen virtuellen Maschine. Öffnen Sie den Konfigurationsverwaltungs-Provider-Server, um die neu bereitgestellte Ressource auf dem vom Benutzer angegebenen Knoten anzuzeigen.

Cloud Provisioning and Governance: Terraform Connector

Verwenden Sie ServiceNow® Cloud Provisioning and Governance: Terraform Connector, um Katalogelemente aus den Terraform -Vorlagen zu generieren und sie zum Bereitstellen und Verwalten von Ressourcen in verschiedenen -Clouds zu verwenden.

Erste Schritte

Untersuchen	Konfigurieren
Erfahren Sie mehr über die Anwendung Cloud Provisioning and Governance: Terraform Connector.	Planen und konfigurieren Sie Ihre Implementierung.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Verwenden

Verwenden Sie die App Cloud Provisioning and Governance: Terraform Connector, um Ressourcen in der Umgebung Terraform zu erkennen, Katalogelemente zu erstellen und zu verwalten.

Referenz

Rufen Sie Details zu Komponenten wie Feldern, Tabellen und Eigenschaften ab.

Problembehandlung und Hilfe

- Cloud Provisioning and Governance Forum auf ServiceNow Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Cloud Provisioning and Governance: Terraform Connector erkunden

Unabhängig davon, ob Sie die Implementierung von Cloud Provisioning and Governance: Terraform Connectorstarten oder erweitern, erfahren Sie mehr über die verfügbaren Funktionen, die bei der Bereitstellung und Verwaltung von Cloud-Ressourcen in verschiedenen Public und Private Clouds helfen.

Cloud Provisioning and Governance: Terraform Connector ist in die Anwendung Cloud Provisioning and Governance integriert und hilft Ihnen, Katalogelemente aus den Terraform -Vorlagen zu erstellen oder zu aktualisieren. Anschließend können Sie die -Katalogelemente verwenden, um die Cloud-Ressourcen bereitzustellen.

Schlüsselfunktionen von Cloud Provisioning and Governance: Terraform Connector

- Erkennen Sie die Terraform -Vorlagen und -Arbeitsbereiche in der Terraform -Umgebung.
- Erstellen Sie Katalogelemente aus den Terraform -Vorlagen.
- Erkennen Sie Änderungen in der Vorlage Terraform, und verwenden Sie den Workflow für IaC-Change-Aufgaben, um das Katalogelement zu aktualisieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Automatische Übersetzung

- Nutzen Sie die Multi-Repository-Unterstützung.
- Geben Sie Metadaten an, um die Formularfelder und Werte des Katalogelements zu füllen.
- Reduzieren Sie die Terraform Cloud -Lizenzkosten, indem Sie die erkannten Terraform -Arbeitsbereiche zur Bereitstellung der Cloud-Infrastruktur verwenden.

Verwenden Sie Terraform als Konfigurationsanbieter

Verwenden Sie den Konfigurations-Provider Terraform Open Source, Terraform Enterpriseund Terraform Cloud, um Ressourcen in den folgenden Clouds bereitzustellen.

Ab diesem Release können Sie OpenTofu mit Cloud Provisioning and Governanceverwenden. Sie müssen über Administratorrechte verfügen, um den Aliasnamen für Terraform Open Source auf VM-Hostebene zu konfigurieren.

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud-Anbieter
- VMware vSphere
- IBM Cloud Platform (Veraltet)

Darüber hinaus können Sie Cloud Provisioning and Governance: Terraform Connector verwenden, um Ressourcen für die Cloud Infrastructure (OCI) Oracle über die App Cloud Provisioning and Governance: Oracle Cloud (OCI) Add-on for Terraform Connector bereitzustellen. Weitere Informationen finden Sie unter Cloud Provisioning and Governance: Oracle Cloud-Add-on (OCI) für Terraform Connector .

Ab Cloud Provisioning and Governance: Terraform Connector Version 1.5.2 unterstützt die App die Bereitstellung von Ressourcen für IBM Cloud Platformnicht mehr.

Erkennen Sie die IaC-Vorlagen (Infrastructure as Code).

Verwenden Sie Cloud Provisioning and Governance: Terraform Connector, um die IaC-Vorlagen (Terraform) in der Umgebung Terraform zu erkennen. Die Organisationen Terraform Enterprise oder Terraform Cloud verwenden unterschiedliche Versionskontrollsysteme, um die Terraform -Vorlagen zu speichern. Cloud Provisioning and Governance: Terraform Connector kann die in den folgenden VCS gespeicherten Vorlagen erkennen:

- Öffentlich und selbst gehostet GitHub
- Öffentlich und selbst gehostet GitLab
- Öffentlich und selbst gehostet Microsoft Azure DevOps

Weitere Informationen finden Sie unter Führen Sie den IaC aus Discovery.

Nutzen Sie die hierarchische Struktur mehrerer Repositorys mit Unterstützung der Discovery-Fähigkeiten des Terraform Connector IaC.

Erstellen Sie Katalogelemente aus den Terraform -Vorlagen

Verwenden Sie die App Cloud Provisioning and Governance: Terraform Connector, um Katalogelemente aus den erkannten Terraform -Vorlagen zu erstellen und sie zur Bereitstellung von Ressourcen in verschiedenen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Clouds zu verwenden. Weitere Informationen finden Sie unter Erstellen Sie ein Katalogelement aus der Vorlage Terraform ..

Erkennen Sie Änderungen in den Terraform -Vorlagen

Verwenden Sie IaC Discovery, um Changes in den Terraform -Vorlagen zu erkennen, die in vorhandenen Katalogelementen verwendet werden. Wenn Cloud Provisioning and Governance: Terraform Connector eine Änderung in der Vorlage Terraform erkennt, wird eine IaC-Change-Aufgabe erstellt. Sie können die IaC-Change-Aufgabe verwenden, um das betroffene Katalogelement zu aktualisieren oder zu deaktivieren und dann ein anderes Katalogelement aus der aktualisierten Vorlage Terraform zu erstellen. Weitere Informationen zur Change-Aufgabe für Katalogelemente finden Sie unter Verwalten Sie die Terraform vorlagenbasierten Katalogelemente.

Terraform Cloud Lizenzkosten reduzieren

Verwenden Sie die erkannten Terraform -Arbeitsbereiche, um die Katalogelemente aus den Terraform -Vorlagen bereitzustellen. Durch die Wiederverwendung des Arbeitsbereichs können Sie die Lizenzkosten Terraform Cloud verwalten, indem Sie die Erstellung von Arbeitsbereichen vermeiden.

Cloud Provisioning and Governance: Terraform Connector konfigurieren

Machen Sie sich mit dem allgemeinen Workflow zum Konfigurieren der Anwendung Cloud Provisioning and Governance: Terraform Connector vertraut.

Führen Sie die folgenden Schritte aus, um die Anwendung Cloud Provisioning and Governance: Terraform Connector zu konfigurieren:

1. Installieren Sie Cloud Provisioning and Governance: Terraform Connector. Weitere Informationen finden Sie unter Cloud Provisioning and Governance: Terraform Connector installieren.
2. Wenn Sie eine Neben- oder Patch-Version von Terraform Open Source, Terraform Enterpriseoder Terraform Cloudverwenden möchten, fügen Sie die Neben- oder Patch-Version dem Workload-Konfigurationsanbieter-Datensatz hinzu. Weitere Informationen finden Sie unter Fügen Sie Unterstützung für kleinere Versionen oder Patch-Versionen von hinzu Terraform.
3. Um Terraform Open Source als Konfigurations-Provider für Cloud Provisioning and Governancezu verwenden, gehen Sie wie folgt vor:
   a. Weisen Sie die Fähigkeit Terraform zu MID-Serverzu. Weitere Informationen finden Sie unter MID-Server-Fähigkeiten konfigurieren .
   b. Erstellen Sie einen Konfigurations-Provider Terraform Open Source. Weitere Informationen finden Sie unter Erstellen Sie einen Konfigurations-Provider Terraform Open Source ..
4. Um Terraform Enterprise oder Terraform Cloud als Konfigurations-Provider für Cloud Provisioning and Governancezu verwenden, gehen Sie wie folgt vor:
   a. Weisen Sie Terraform Enterprise und REST-Fähigkeiten MID-Serverzu. Weitere Informationen finden Sie unter MID-Server-Fähigkeiten konfigurieren .
   b. Erstellen Sie einen Terraform Enterprise - oder Terraform Cloud -Konfigurations-Provider. Weitere Informationen finden Sie unter Erstellen Sie einen Terraform Enterprise - oder Terraform Cloud -Konfigurations-Provider.
5. Erkennen Sie Ressourcen in der Umgebung Terraform. Weitere Informationen finden Sie unter Führen Sie den IaC aus Discovery.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance: Terraform Connector installieren

Mit der Administratorrolle können Sie die Anwendung Cloud Provisioning and Governance: Terraform Connector (com.sn_cmp_ Terraform) installieren.

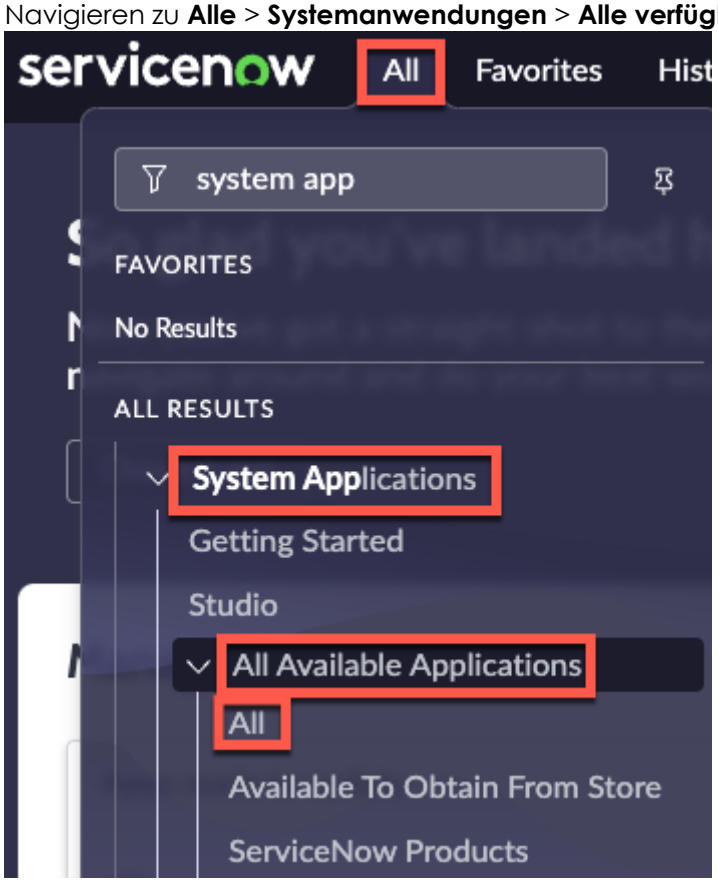
Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung und alle zugehörigen ServiceNow Store-Anwendungen über gültige Berechtigungen für ServiceNow verfügen. Weitere Informationen finden Sie unter Rufen Sie eine Berechtigung für ab ServiceNow Produkt oder Anwendung .
- Überprüfung des folgenden Elements: Cloud Provisioning and Governance: Terraform Connector Anwendungsliste in ServiceNow Store, um Informationen zu Abhängigkeiten, Lizenzierungs- oder Abonnementanforderungen und Releasekompatibilität zu erhalten.
- Stellen Sie sicher, dass die Anwendung Cloud Provisioning and Governance (com.snc.cloud.mgmt) in Now Platforminstalliert und aktiviert ist. Weitere Informationen finden Sie unter Die Anwendung Cloud Provisioning and Governance anfordern.

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren zu **Alle** > **Systemanwendungen** > **Alle verfügbaren Anwendungen** > **Alle**.



2. Suchen Sie mithilfe der Filterkriterien und der Suchleiste nach der Anwendung Cloud Provisioning and Governance: Terraform Connector (com.sn_cmp_ Terraform).

   Sie können nach der Anwendung anhand ihres Namens oder ihrer ID suchen. Wenn Sie die Anwendung nicht finden können, müssen Sie sie möglicherweise über den ServiceNow Store anfordern.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In der Liste neben der Schaltfläche **Installieren** werden die für Sie verfügbaren Versionen angezeigt.

3. Wählen Sie eine Version aus der Liste und dann **Installieren** aus.

   Im angezeigten Dialogfeld „Installieren“ werden alle Abhängigkeiten aufgelistet, die zusammen mit der Anwendung installiert werden.

4. Wenn Sie dazu aufgefordert werden, folgen Sie den Links zum ServiceNow Store, um zusätzliche Berechtigungen für Abhängigkeiten zu erhalten.
5. Wählen Sie **Installieren** aus.

Nächste Maßnahme

- Wenn Sie Cloud Provisioning and Governance: Terraform Connector mit Terraform Open Sourceverwenden möchten, Erstellen Sie einen Konfigurations-Provider Terraform Open Source ..
- Wenn Sie Cloud Provisioning and Governance: Terraform Connector mit Terraform Enterpriseverwenden möchten, Erstellen Sie einen Terraform Enterprise - oder Terraform Cloud -Konfigurations-Provider.

Fügen Sie Unterstützung für kleinere Versionen oder Patch-Versionen von hinzu Terraform

Fügen Sie dem Workload-Provider-Typ-Datensatz Nebenversionen oder Patch-Versionen von Terraform (Terraform Open Source, Terraform Enterpriseoder Terraform Cloud) hinzu.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

Das Basissystem Cloud Provisioning and Governance: Terraform Connector unterstützt die folgenden Terraform -Versionen:

- Terraform Open Source Versionen 1.1.0 bis 1.1.9 und 1.2.0.
- Terraform Enterprise die Versionen 1.1.9 und 1.2.0.
- Terraform Cloud die Versionen 1.1.9 und 1.2.0

Um Vorlagen zu verwenden, die von einer Neben- oder Patch-Version (z. B. Version 0.12.29) unterstützt werden, fügen Sie die Versionsnummer zum Datensatz des Typs des Arbeitsauslastungs-Providers hinzu. Verwenden Sie dann die Nebenversion oder die Patch-Version, um Konfigurationsanbieter in Cloud Provisioning and Governancezu erstellen.

Prozedur

1. Zu `https://`navigieren<instance-name> /sn_cmp_workload_provider_type_list.do
2. Wählen Sie den Typ Terraform aus, dessen Neben- oder Patch-Version Sie verwenden möchten.
3. Ändern Sie den Anwendungsbereich in **Cloud Provisioning and Governance: Terraform Connector**.
4. Geben Sie im Formular „Workload-Konfigurations-Provider-Typ“ im Feld **Version** die Neben- oder Patchversionen als kommagetrennte Werte ein.
5. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erstellen Sie einen Konfigurations-Provider Terraform Open Source .

Erstellen Sie einen Terraform Open Source -Konfigurations-Provider in Cloud Provisioning and Governance. Mit dem Konfigurations-Provider Terraform Open Source kann Cloud Provisioning and Governance die Terraform Open Source -Konfigurationsinstallationselemente (Terraform -Vorlagen) erkennen und Änderungen daran erkennen.

Warum und wann dieser Vorgang ausgeführt wird

Ab diesem Release können Sie OpenTofu mit Cloud Provisioning and Governanceverwenden. Sie müssen über Administratorrechte verfügen, um den Aliasnamen für auf der VM-Hostebene zu konfigurieren. Stellen Sie sicher, dass der Server unter dem Betriebssystem Windows oder Linux ausgeführt wird.

Vorbereitungen

- Stellen Sie sicher, dass eine unterstützte Version Terraform Open Source auf dem Server installiert ist. Cloud Provisioning and Governance: Terraform Connector unterstützt Terraform Open Source Versionen 1.1.0 bis 1.1.9 und 1.2.0.
- Wenn Sie eine Neben- oder Patch-Version der Terraform Open Source CLI verwenden möchten, stellen Sie sicher, dass die Neben- oder Patch-Version dem Workload-Konfigurations-Provider hinzugefügt wird. Weitere Informationen finden Sie unter Fügen Sie Unterstützung für kleinere Versionen oder Patch-Versionen von hinzu Terraform.
- Stellen Sie sicher, dass MID-Server auf den Server Terraform zugreifen kann.
- Stellen Sie sicher, dass MID-Server die Fähigkeit Terraform hat.
- Fügen Sie als neuer Benutzer die Terraform MID-Fähigkeit hinzu, um Ressourcen mit dem Terraform Open-Source-Host (VM) bereitzustellen. Fügen Sie eine für den Cloud-Provider spezifische MID-Fähigkeit (AWS, Azure, VMware, Google) hinzu, um Ressourcen aus der Cloud nach der Bereitstellung von Terraform Open Source-Katalogelementen zu erkennen. Beispiel: Wenn Sie eine VM mit Terraform Open-Source in Google bereitstellen, benötigen Sie MID mit Terraform- und Google-Funktionen. Beide Fähigkeiten können auf dieselben oder verschiedene MIDs festgelegt werden. MID-Server mit Terraform-Fähigkeit sollten in der Lage sein, eine Verbindung zum Terraform-Host (VM) herzustellen, und MID-Server mit Google-Fähigkeit müssen Google Cloud erreichen können. Weitere Informationen finden Sie unter MID-Server-Fähigkeiten konfigurieren .
- Stellen Sie sicher, dass alle Vorlagen in separaten Verzeichnissen gespeichert sind und dass sich alle Vorlagenverzeichnisse im selben Basisverzeichnis befinden.
- Stellen Sie sicher, dass der Terraform-Connector Zugriff auf die Terraform-Registrierung (registry.hshicorp.com) hat.

Erforderliche Rolle: cloud_admin

Prozedur

1. Wahlweise: Wenn Sie Terraform Open Source auf einem Server Linux vom Typ bereitgestellt haben, erstellen Sie Anmeldeinformationen für den privaten SSH-Schlüssel für den Server im Now Platform.

   a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**.
   Das Cloud-Adminportal wird in einer neuen Browserregisterkarte geöffnet.

   b. Navigieren Sie im Cloud-Adminportal zu **Verwalten** > **Anmeldeinformationen**.

   c. Wählen Sie **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Wählen Sie **Anmeldeinformationen für Privater SSH-Schlüssel**aus.

e. Füllen Sie die Felder des Formulars aus.
Eine Beschreibung der Formularfelder finden Sie unter Cloud Provisioning and Governance: Terraform Connector Formularreferenz für Anmeldeinformationen des privaten SSH-Schlüssels.

f. Wählen Sie den zugehörigen Link Anmeldeinformationen testen aus.

g. Füllen Sie die Felder des Formulars aus.

Formular zum Testen von Anmeldeinformationen

Feld	Beschreibung
Ziel	IP-Adresse des Servers Terraform, für den Sie die Anmeldeinformationen erstellen.
MID-Server	MID-Server, der zum Herstellen einer Verbindung mit dem Server Terraform verwendet werden kann.

h. Wählen Sie **OK**.

i. Wählen Sie **Absenden**.

2. Wahlweise: Wenn Sie Terraform Open Source auf einem Windows -Server bereitgestellt haben, erstellen Sie Windows -Anmeldeinformationen für den Server im Now Platform.

a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**.
Das Cloud-Adminportal wird in einer neuen Browserregisterkarte geöffnet.

b. Navigieren Sie im Cloud-Adminportal zu **Verwalten** > **Anmeldeinformationen**.

c. Wählen Sie **Neu**.

d. Wählen Sie **die Windows-Anmeldeinformationen**aus.

e. Füllen Sie die Felder des Formulars aus.
Eine Beschreibung der Formularfelder finden Sie unter Cloud Provisioning and Governance: Terraform Connector Windows Formularreferenz für Anmeldeinformationen.

f. Wählen Sie den zugehörigen Link Anmeldeinformationen testen aus.

g. Füllen Sie die Felder des Formulars aus.

Formular zum Testen von Anmeldeinformationen

Feld	Beschreibung
Ziel	IP-Adresse des Servers Terraform, für den Sie die Anmeldeinformationen erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
MID-Server	MID-Server, der zum Herstellen einer Verbindung mit dem Server Terraform verwendet werden kann.

h. Wählen Sie **OK**.

i. Wählen Sie **Absenden**.

3. Erstellen Sie einen Konfigurations-Provider für Terraform Open Source.

a. Navigieren Sie im Cloud-Adminportal zu **Verwalten** > **Konfigurationsverwaltung**.

b. Wählen Sie **Neu**.

c. Füllen Sie die Felder des Formulars aus.
Eine Beschreibung der Formularfelder finden Sie unter Cloud Provisioning and Governance: Terraform Connector Formularreferenz „Konfigurations-Provider erstellen“..

d. Wählen Sie **Absenden**.

Nächste Maßnahme

Erkennen Sie die Terraform -Vorlagen auf dem Server Terraform Open Source. Weitere Informationen finden Sie unter Führen Sie den IaC aus Discovery.

Erstellen Sie einen Terraform Enterprise - oder Terraform Cloud -Konfigurations-Provider

Erstellen Sie den Konfigurations-Provider Terraform Enterprise oder Terraform Cloud in Cloud Provisioning and Governance. Mit dem Konfigurations-Provider kann Cloud Provisioning and Governance die Arbeitsbereiche und VCS-Repositorys (Version Control System) erkennen, die an die Organisation Terraform angehängt sind.

Vorbereitungen

- Stellen Sie sicher, dass eine unterstützte Version Terraform Enterprise oder Terraform Cloud verwendet wird. Cloud Provisioning and Governance: Terraform Connector unterstützt die folgenden Terraform -Versionen:
  - Terraform Enterprise die Versionen 1.1.9 und 1.2.0
  - Terraform Cloud die Versionen 1.1.9 und 1.2.0
- Um eine Neben- oder Patch-Version von Terraform Enterprise oder Terraform Cloudzu verwenden, stellen Sie sicher, dass die Neben- oder Patch-Version dem Workload-Konfigurations-Provider hinzugefügt wird. Weitere Informationen finden Sie unter Fügen Sie Unterstützung für kleinere Versionen oder Patch-Versionen von hinzu Terraform.
- Stellen Sie sicher, dass die folgenden Eigenschaften in MID-Serverrichtig konfiguriert sind. MID-Server verwendet diese Eigenschaften, um eine Verbindung zu Terraform Enterprise oder Terraform Cloudherzustellen.
  - *glide.http.proxy_host*
  - *glide.http.proxy_port*
  - *glide.http.proxy_username*
  - *glide.http.proxy_password*

  Weitere Informationen finden Sie im Knowledge Base -Artikel KB0754247 .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass MID-Server über die Fähigkeiten Terraform Enterprise und REST verfügt. Weitere Informationen finden Sie unter MID-Server-Fähigkeiten konfigurieren .
- Stellen Sie sicher, dass MID-Server mit den VCS-Konten kommunizieren kann, die in der Organisation Terraform Enterprise oder Terraform Cloud bereitgestellt werden.

Erforderliche Rolle: Administrator

Prozedur

1. Erstellen Sie API-Schlüssel-Anmeldeinformationen für den Account Terraform Enterprise oder Terraform Cloud.
   Weitere Informationen finden Sie unter Erstellen Sie API Key-Anmeldeinformationen für den Account Terraform und den unterstützten VCS-Account.
2. Erstellen Sie einen Konfigurations-Provider für Terraform Enterprise oder Terraform Cloud.
   a. Navigieren Sie im Cloud-Adminportal zu **Verwalten** > **Konfigurationsverwaltung**.
   b. Wählen Sie **Neu**.
   c. Füllen Sie die Felder des Formulars aus.
      Eine Beschreibung der Formularfelder finden Sie unter Cloud Provisioning and Governance: Terraform Connector Formularreferenz „Konfigurations-Provider erstellen“..
   d. Wählen Sie **Absenden**.

Nächste Maßnahme

Erkennen Sie die Arbeitsbereiche und VCS-Repositorys (Version Control System), die an die Organisation Terraform angehängt sind, die im Konfigurations-Provider angegeben ist. Weitere Informationen finden Sie unter Führen Sie den IaC aus Discovery.

Erstellen Sie API Key-Anmeldeinformationen für den Account Terraform und den unterstützten VCS-Account

Erstellen Sie API-Schlüssel-Anmeldeinformationen für den Account Terraform und unterstützte VCS-Accounts (Version Control System), die die Vorlagen-Repositorys Terraform enthalten.

Vorbereitungen

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird

API-Schlüssel-Anmeldeinformationen sind ein gesicherter Datensatz in Now Platform, in dem ein API-Schlüssel wie Terraform Enterprise, Terraform Cloudoder ein VCS-Konto-API-Schlüssel gespeichert wird. Cloud Provisioning and Governance: Terraform Connector verwendet die API-Schlüssel-Anmeldeinformationen, um eine Verbindung zum Account herzustellen und dessen Ressourcen zu erkennen.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**.
   Das Cloud-Adminportal wird in einer neuen Browserregisterkarte geöffnet.
2. Navigieren Sie im Cloud-Adminportal zu **Verwalten** > **Anmeldeinformationen**.
3. Wählen Sie **Neu**.
4. Wählen Sie **API Key-Anmeldeinformationen**aus.
5. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Beschreibung der Formularfelder finden Sie unter Cloud Provisioning and Governance: Terraform Connector Formularreferenz für API-Schlüssel-Anmeldeinformationen.

6. Wählen Sie **Absenden**.

Verwenden Sie die Struktur aus mehreren Repositorys mit der App Terraform Connector .

Mit dem Konfigurations-Provider Terraform Enterprise können Sie jetzt auf jeder Ordnerebene mehrere Terraform -Konfigurationen aus einem Repository erkennen.

Vorbereitungen

Erforderliche Rolle: Administrator

Führen Sie die Schritte Führen Sie den IaC aus Discovery aus, und geben Sie an, welche Repositorys, Verzweigungen und Ordnerpfade für die Erkennung von Terraform -Konfigurationen mit diesen Schritten berücksichtigt werden müssen.

Prozedur

1. Fügen Sie Repositorys und Verzweigungen hinzu, die Sie beim Erkennen von Terraform -Konfigurationen berücksichtigen möchten.
2. Verwenden<Repository-Name> **::** <Branch-Name> -Format, um eine Verzweigung aus einem Repository einzubeziehen.
3. Um mehrere Repository- und Verzweigungszuordnungen anzugeben, verwenden Sie ein Komma (,).

   Beispiel: Repo1::Branch1, Repo2::Branch2.

   Verlassen Sie den Feldpool, wenn Sie alle Repositorys und Verzweigungen in diesem VCS erkennen möchten.
4. Wählen **Sie Möchten Sie Unterordnerpfade für Discovery angeben,** wenn Sie Terraform -Konfigurationen aus bestimmten Ordnerpfaden des Repositorys erkennen möchten.
5. Fügen Sie in der **Ordnerpfadliste**die Liste der Ordnerpfade hinzu, getrennt durch ein Komma (,), um daraus Terraform-Konfigurationen zu erkennen.
   - Der Ordnerpfadfilter gilt für alle Repository-Verzweigungen, die in der „Aufnahmeliste für Repository und Verzweigung“ enthalten sind.
   - Alle Terraform -Konfigurationen, die Sie aus einem bestimmten Ordnerpfad erkennen möchten, müssen sich in Unterordnern befinden, die sich nur eine Ebene unterhalb der Ordnerhierarchie befinden. Beispiel: Ordnerpfad**„/gcp/vm“** hat eine Konfiguration Terraform für VM,
   - Geben Sie **„/gcp“** in der Ordnerpfadliste an, um die VM-Konfiguration Terraform zu erkennen.

Führen Sie den IaC aus Discovery

Führen Sie die IaC-Erkennung (Infrastructure as Code) aus, um die Ressourcen der -Umgebung Terraform zu identifizieren.

Vorbereitungen

- Stellen Sie sicher, dass Sie über die entsprechenden API-Anmeldeinformationen für die VCS-Konten (Version Control System) verfügen, die in den Organisationen Terraform Enterprise oder Terraform Cloud bereitgestellt werden. Weitere Informationen finden Sie unter Erstellen Sie API Key-Anmeldeinformationen für den Account Terraform und den unterstützten VCS-Account.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass die Ordner Terraform Open Source, die die Vorlagen Terraform enthalten, eindeutige Namen haben. Wenn mehrere Terraform -Vorlagenordner denselben Namen haben, werden mehrere Change-Aufgaben erstellt, auch wenn nicht alle Vorlagen Variablenänderungen enthalten.

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Je nach Konfigurationsanbieter erkennt Cloud Provisioning and Governance: Terraform Connector die folgenden Ressourcen aus der Umgebung Terraform :

Terraform Open Source

Das IaC Discovery erkennt die installierbaren Konfigurationselemente (Terraform Vorlagen) auf dem Server Terraform Open Source.

Terraform Enterprise oder Terraform Cloud

Das IaC Discovery erkennt die folgenden Elemente:

- Arbeitsbereiche: Terraform Arbeitsbereiche, die in der Organisation Terraform bereitgestellt werden.
- VCS: VCS-Repositorys und -Verzweigungen, die in der Organisation Terraform bereitgestellt werden.
- Agent-Pools:

  Terraform Cloud verwendet für die Kommunikation mit der lokalen Infrastruktur Agents und Agent-Pools. Stellen Sie Agents im selben Netzwerk wie Ihre Infrastruktur bereit, um eine Verbindung zwischen der -Infrastruktur und Terraform Cloudherzustellen. Weitere Informationen zu Agenten und Agent-Pools finden Sie unter Terraform Cloud Agents .

  Cloud Provisioning and Governance: Terraform Connector erkennt die in Terraform Clouderstellten Agent-Pools. Die erkannten Agents können Sie im Konfigurationsverwaltungsmodul für Ihren Konfigurations-Provider anzeigen. Auf dem Katalogbestellformular können Sie mit einem Agent-Pool-Filter einen aktiven Agent für die Kommunikation mit der privaten Infrastruktur VMware auswählen.

  Hinweis: Sie können die Option „Agent-Pools“ im Konfigurationsverwaltungsformular und im Katalogbestellformular anzeigen, wenn die folgenden Bedingungen erfüllt sind:

  - Sie haben die Mitarbeiterpools VMware in der Organisation Terraform Cloud erstellt.
  - Sie haben VMware Vorlagen für Terraform Enterprise.

- Cfg installables: Terraform Vorlagen, die in den Repositorys des VCS-Accounts gespeichert sind, der von der Organisation Terraform bereitgestellt wurde.

  Hinweis: Um die Terraform -Vorlagen aus dem VCS zu erkennen, benötigt Cloud Provisioning and Governance: Terraform Connector die API-Schlüssel-Anmeldeinformationen des VCS-Kontos.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**.
   Das Cloud-Adminportal wird in einer neuen Browserregisterkarte geöffnet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Navigieren Sie im Cloud-Adminportal zu **Verwalten** > **Konfigurationsverwaltung**.
3. Wählen Sie die Anbieterkarte Terraform aus.
4. Wählen Sie **Jetzt erkennen aus**.

   Hinweis: Sie können den IaC-Auftrag Discovery nicht abbrechen, nachdem Sie ihn ausgelöst haben.

5. Wahlweise: Zur Verwendung Cloud Provisioning and Governance: Terraform Connector von mit Terraform Enterprise oder Terraform Clouderkennen Sie die im bereitgestellten VCS gespeicherten Terraform -Vorlagen.
   a. Wählen Sie die Registerkarte **Tfe Vcs** aus.
   b. Wählen Sie in der Liste Tfe Vcs das VCS-Konto aus, das die Terraform -Vorlagen enthält, die Sie für die Erstellung Cloud Provisioning and Governance von -Katalogelementen verwenden möchten.
   c. Wählen Sie in der Dropdown-Liste Anmeldeinformationen die API-Anmeldeinformationen des ausgewählten VCS-Kontos aus.
   d. Wählen Sie unter „Zugehörige Links“ **die Option Verzweigungen und Repositorys suchen**aus.
   e. Wiederholen Sie Schritt 5.b bis 5.d für alle VCS-Konten, die die Terraform -Vorlagen enthalten, die Sie für die Erstellung von Cloud Provisioning and Governance -Katalogelementen verwenden möchten.
6. Erstellt einen IAC-Discovery-Zeitplan (Infrastructure as Code).
   Der IaC-Discovery-Zeitplan hilft bei der Erkennung neuer Terraform -Vorlagen, Arbeitsbereiche, Agent-Pools und VCS-Verzweigungen für den angegebenen Konfigurations-Provider. Erkennt auch Changes an bereits erkannten Terraform -Vorlagen. Wenn Cloud Provisioning and Governance: Terraform Connector eine Änderung an der Vorlagenvariablen oder den Vorlagenmetadaten erkennt, werden automatisch IaC-Change-Aufgaben für die betroffenen Katalogelemente erstellt.

   a. Navigieren Sie im Cloud-Adminportal zu **Verwalten** > **IaC-Discovery**.

   b. Wählen Sie **Neu**.

   c. Füllen Sie die Felder des Formulars aus.

Formular „IaC-Discovery-Planer“.

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name des IaC-Zeitplans Discovery.
Anbieter	Konfigurationsverwaltungs-Provider, für den Sie den Discovery-Zeitplan erstellen.
Aktiv	Option zum Aktivieren oder Deaktivieren des Zeitplans
Ausführen	Häufigkeit der Zeitplanausführung. Konfigurieren Sie die Häufigkeit der Zeitplanausführung im Feld Ausführen und in den zugehörigen Formularfeldern.

   d. Wählen Sie **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Verwenden Sie die Struktur aus mehreren Repositorys mit der App Terraform Connector . mit IaC-Discovery
- Wenn Cloud Provisioning and Governance: Terraform Connector neue Terraform -Vorlagen erkennt, die Sie für die Cloud-Ressourcenbereitstellung verwenden möchten, erstellen Sie ein Katalogelement aus der erkannten Vorlage. Weitere Informationen finden Sie unter Erstellen Sie ein Katalogelement aus der Vorlage Terraform ..
- Wenn Cloud Provisioning and Governance: Terraform Connector Changes in einer vorhandenen Vorlage erkannt hat, führen Sie eine der folgenden Aktionen aus, um die zugehörige IaC-Change-Aufgabe zu lösen:
  - Aktualisiert das betroffene Katalogelement gemäß der aktualisierten Vorlage Terraform.
  - Deaktivieren Sie das betroffene Katalogelement, und erstellen Sie dann ein Katalogelement gemäß der aktualisierten Vorlage.

  Weitere Informationen finden Sie unter Verwalten Sie die Terraform vorlagenbasierten Katalogelemente.

Domänentrennung und Cloud Provisioning and Governance: Terraform Connector

Domänentrennung wird für Cloud Provisioning and Governance: Terraform Connector unterstützt. Mit der Domain Separation können Sie Daten, Prozesse und Verwaltungsaufgaben in logische Gruppierungen, sogenannte Domänen, aufteilen. Sie können verschiedene Aspekte dieser Trennung steuern, einschließlich der Benutzer, die Daten sehen und darauf zugreifen können.

Cloud Provisioning and Governance: Terraform Connector lässt sich in Cloud Provisioning and Governance integrieren und entspricht der Cloud Provisioning and Governance Domain Separation. Weitere Informationen finden Sie unter Domain Separation und Cloud Provisioning and Governance.

Die Terraform -Umgebung wird aktualisiert

Machen Sie sich mit den allgemeinen Workflows für das Upgrade der Umgebung Terraform vertraut.

Wird aktualisiert Terraform Open Source

Upgrade-Methoden für Terraform Open Source

Upgrade-Methode	Beschreibung
Aktualisieren Sie die vorhandene Terraform Open Source -Installation auf eine neuere unterstützte Version	**Hinweis:** Wenn Sie die vorhandene Terraform Open Source -Installation aktualisieren, kann die Upgrade-Zeit länger dauern. Führen Sie die folgenden Aktionen aus, um die vorhandene Installation Terraform Open Source zu aktualisieren: 1. Aktualisieren Sie den Server Terraform Open Source auf eine Version, die von Cloud Provisioning and Governance: Terraform Connectorunterstützt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upgrade-Methoden für Terraform Open Source (Fortsetzung)

Upgrade-Methode	Beschreibung
	Weitere Informationen zum Upgraden von Terraform finden Sie in den Upgrade-Leitfäden in Terraform Dokumentation . Cloud Provisioning and Governance: Terraform Connector unterstützt Terraform Open Source Versionen 1.1.0 bis 1.1.9 und 1.2.0. **2.** Testen und ändern Sie die vorhandenen Terraform -Vorlagen, um die Kompatibilität mit der Zielversion Terraform Open Source sicherzustellen. **3.** Aktualisieren Sie die im Konfigurations-Provider Terraform Open Source erwähnte Version Terraform Open Source.
Richten Sie einen neuen Terraform -Server mit der gewünschten Terraform Open Source -Version ein	Führen Sie die folgenden Aktionen aus, um einen neuen Terraform -Server mit der gewünschten Terraform Open Source -Version einzurichten: **1.** Erstellen Sie einen Linux - oder Windows -Server für Terraform Open Source die -Installation. **2.** Installieren Sie eine Terraform Open Source -Version, die von Cloud Provisioning and Governance: Terraform Connectorunterstützt wird. Cloud Provisioning and Governance: Terraform Connector unterstützt Terraform Open Source Versionen 1.1.0 bis 1.1.9 und 1.2.0. **3.** Kopieren Sie die vorhandenen Terraform -Vorlagen auf den neuen Terraform -Server. **Hinweis:** Stellen Sie sicher, dass alle Vorlagen in separaten Verzeichnissen gespeichert sind und dass sich alle Vorlagenverzeichnisse im selben Basisverzeichnis befinden. **4.** Testen und ändern Sie die kopierten Terraform -Vorlagen, um die Kompatibilität mit der Zielversion Terraform Open Source sicherzustellen. **5.** Erstellen Sie einen Terraform Open Source-Konfigurations-Provider. Weitere Informationen finden Sie unter Erstellen Sie einen Konfigurations-Provider Terraform Open Source ..

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Upgrade-Methoden für Terraform Open Source (Fortsetzung)

Upgrade-Methode	Beschreibung
	6. Entfernen Sie die alten Katalogelemente gemäß der Geschäftsstrategie Ihrer Organisation, und legen Sie dann den alten Server Terraform still.

Terraform Enterprise und Terraform Cloudwerden aktualisiert

Testen und ändern Sie die vorhandenen Terraform -Vorlagen, um die Kompatibilität mit der neuen Version Terraform Enterprise oder Terraform Cloud sicherzustellen.

Hinweis: Die Stapel und die Arbeitsbereiche Terraform sind an die Version Terraform gebunden, über die sie bereitgestellt wurden. Daher wird dieselbe Version Terraform zum Bereitstellen und Aufheben der Bereitstellung eines Stapels oder eines Terraform -Arbeitsbereichs verwendet.

Cloud Provisioning and Governance: Terraform Connector verwenden

Machen Sie sich mit den allgemeinen Anwendungsfällen und Nutzungs-Workflows für die Anwendung Cloud Provisioning and Governance: Terraform Connector vertraut.

Ordnen Sie die Eingabeparameter Terraform dem Katalogelement Cloud Provisioning and Governance zu

Erstellen Sie eine JSON-Datei, um die in der Vorlagendatei verwendeten Variablen zu speichern, damit Sie sie erkannten Ressourcen, Pools und Filtern zuordnen können. Sie können Variablen oder Parameter aus der Vorlage Terraform verwenden, um Feldern im Formular „Katalogelementbereitstellung“ zuzuordnen.

Vorbereitungen

Erforderliche Rolle: cloud_designer

Warum und wann dieser Vorgang ausgeführt wird

Cloud Provisioning and Governance: Terraform Connector unterstützt diese Fähigkeit für Terraform Open Source, Terraform Enterpriseund Terraform Cloud.

Wichtig: Wenn Sie Terraform -Vorlagen zum Erstellen von Katalogelementen verwenden, gibt der Wert Standort das Rechenzentrum oder die Region an, in der die Konfigurationselemente und Stapel bereitgestellt werden sollen. Verwenden Sie die Metadatendatei, um andere Variablen basierend auf erkannten Ressourcen, Netzwerken, Profilen, Pools und Filtern usw. zuzuordnen.

Um Formularfelder im Katalogerstellungsformular während der Verwendung Terraform von -Vorlagen automatisch auszufüllen, gehen Sie wie folgt vor:

- Geben Sie die Schlüssel-Wert-Paare in der JSON-Datei für Variablen an, die in der Vorlage Terraform definiert sind.
- Konfigurieren Sie Variablen, um Felder und Daten in automatisch zu füllen **Cloud-Anwenderportal** > **Cloud-Katalog** > **Neu** > **Bereitstellung** Seite.

Weitere Informationen zum Binden eines Parameters an einen Ressourcenpool finden Sie unter Binden Sie einen Parameter an einen Ressourcenpool.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie eine JSON-Datei in dem Verzeichnis oder Repository, das die Grundlage für das Katalogelement ist.

   Wichtig: Nennen Sie die JSON-Datei `metadata.snc`, und speichern Sie sie im selben Verzeichnis oder Repository wie die Vorlagendatei (.tf). Diese Namenskonvention ermöglicht die Discovery und Analyse der JSON-Datei `metadata.snc` als Teil der installierbaren Konfiguration.

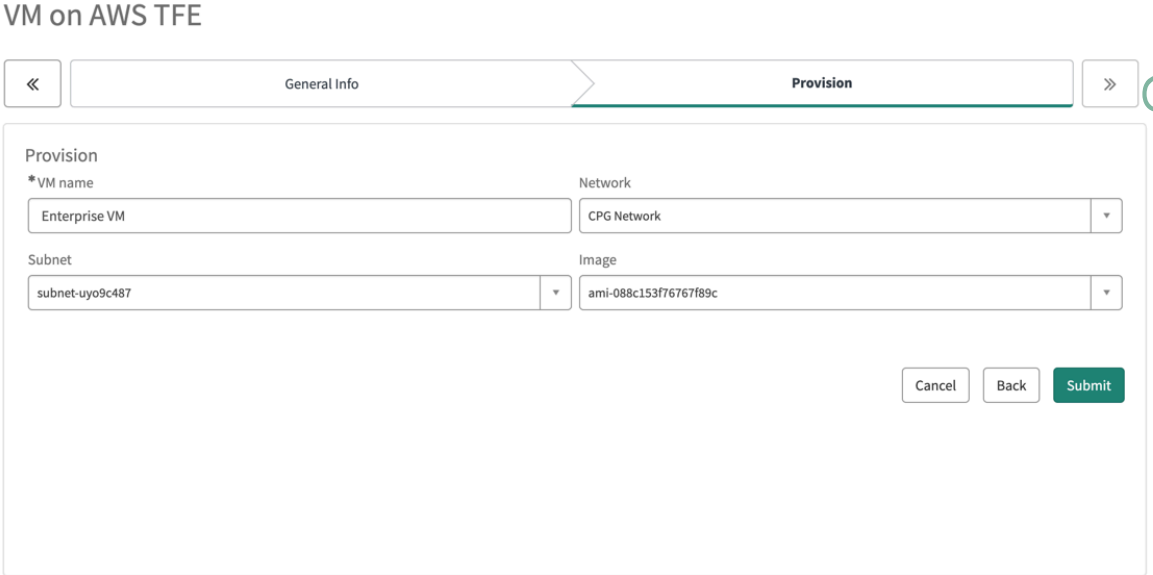
2. Geben Sie den entsprechenden Pool und Filter als Datentyp für die Variable Terraform in der JSON-Datei `metadata.snc` an.

```
 "Metadata": {
   "SNC::Parameter::Metadata": {
     "rgName": {
       "datasource": "ServiceNow::Pools:: ResourceGroupPool.getByLDC"
     },
     "Network": {
       "datasource": "ServiceNow::Pools::NetworkPool.getObjectsByLDC"
     },
     "Subnet": {
       "datasource": "ServiceNow::Pools::
SubnetPool.getObjectsByNetwork",
       "datasourceFilter": { "Network": "Network" }
     }
   }
 }
```

   Der Wert, den Sie im Variablenfeld der Datei `metadata.snc` angeben, wird im Abschnitt „Bereitstellung“ des Formulars „Katalogelement“ ausgefüllt.

   Das folgende Bild zeigt die Felder auf der Registerkarte Bereitstellung des Katalogformulars. Die Werte werden basierend auf den in der Datei `metadata.snc` definierten Variablen automatisch ausgefüllt.

Beispiel: Automatisch gefüllte Werte im Abschnitt „Bereitstellung“ des Katalogerstellungsformulars



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Füllen Sie das Rechenzentrum mit Terraform-basierten Katalogelementen aus

In jeder Anforderung für ein Katalogelement mit Terraform -Vorlagen gibt der erforderliche Standortwert das Rechenzentrum oder die Region an, in der die Konfigurationselemente und Stapel bereitgestellt werden sollen. Sie können eine Variable mit dem Namen *region* in der Vorlage Terraform für die Zuordnung zum Feld Standort im Anforderungsformular verwenden.

Vorbereitungen

Erforderliche Rolle: cloud_designer

Prozedur

Definieren Sie in der Vorlagendatei, die die Grundlage für das Katalogelement darstellt, eine Variable mit dem Namen *region*.

```
variable "region" {
                type="string"
              }
```

- Das für die Variable *region* definierte Feld wird im Abschnitt „Bereitstellung“ des Anforderungsformulars für das Katalogelement nicht angezeigt (diesen Zweck erfüllt das Feld Standort).
- Der Wert, den der Benutzer für das Feld Standort im Anforderungsformular angibt, konfiguriert das Rechenzentrum oder die Region für die Ressource.

Erstellen Sie ein Katalogelement aus der Vorlage Terraform .

Erstellen Sie ein Katalogelement aus der Vorlage Terraform, um die Bereitstellung von Cloud-Ressourcen anzufordern. Aktivierte Katalogelemente werden im Cloud-Benutzerportal angezeigt.

Vorbereitungen

- Stellen Sie sicher, dass ein geeigneter Terraform -Konfigurations-Provider verfügbar ist. Weitere Informationen zum Erstellen des Konfigurations-Providers finden Sie unter Erstellen Sie einen Konfigurations-Provider Terraform Open Source . und Erstellen Sie einen Terraform Enterprise - oder Terraform Cloud -Konfigurations-Provider.
- Stellen Sie sicher, dass die Vorlage Terraform funktioniert (d. h. Sie können die Vorlage direkt mit dem System Terraform verwenden, um die angegebenen Cloud-Ressourcen bereitzustellen). Weitere Informationen zu Terraform -Vorlagen finden Sie unter Terraform Sprachdokumentation .
- Stellen Sie sicher, dass der Anbieterblock der Vorlage Terraform die folgende Syntax einhält:
  - Anbieterblocksyntax für die Cloud Microsoft Azure :

```
provider "azurerm" {

  subscription_id = "${var.subscriptionId}"
  client_id       = "${var.clientId}"
  client_secret   = "${var.clientSecret}"
  tenant_id       = "${var.tenantId}"
}
```

  - Anbieterblocksyntax für die Cloud Amazon Web Services :

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
provider "aws" {
  access_key      = "${var.access_key}"
  secret_key      = "${var.secret_key}"
  region          = "${var.region}"
}
```

◦ Anbieterblocksyntax für Google Cloud Platform

```
terraform {
  required_providers {
    google = {
      source  = "hashicorp/google"
      version = "5.10.0"
    }
  }
}

provider "google" {
  credentials = var.credentials
  project     = var.project
  region      = var.region
}
```

◦ Anbieterblocksyntax für VMware Cloud:

```
provider "vsphere" {
  user                 = "${var.user}"
  password             = "${var.password}"
  vsphere_server       = "${var.vsphere_server}"
}
```

Hinweis: Codieren Sie keine Anmeldeinformationen in der Vorlage Terraform hart. Verwenden Sie entsprechende Terraform Variablen, um die Anmeldeinformationen aus Now Platformabzurufen.

- Stellen Sie sicher, dass die Variablendefinitionsdatei (`variable.tf`, `.tfvars`oder `.tfvars.json`) die Definition der im Anbieterblock verwendeten Variablen enthält.
- Wenn Sie Terraform Enterprise oder Terraform Cloudverwenden, stellen Sie sicher, dass MID-Server eine Verbindung zu Version Control System (VCS) herstellen kann, die in der Organisation Terraform bereitgestellt werden.

  Um die Konnektivität mit den in der Organisation Terraform bereitgestellten VCS-Konten zu überprüfen, führen Sie den entsprechenden Befehl „curl“ auf MID-Serveraus.

  GitHub

  ```
  curl -H "Authorization: <API credential>
   https://<github-api-host>/user/repos?per_page=100&page=1"
  ```

  GitLab

  ```
  curl -H "Authorization: <API credential>"
   https://<gitlab-api-host>/api/v4/projects?visibility=private
  &per_page=100&page=1
  ```

  Microsoft Azure DevOps

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
curl -H "Authorization: <API credential>
 https://<azure-devops-api-host>/<organization>/<project>/_ap
is/git/repositories?api-version=6.0"
```

Wo,

- *organization* ist der Name der Organisation Microsoft Azure DevOps.
- *project* ist der Name des Projekts Microsoft Azure DevOps.

Weitere Informationen zu den API-Anmeldeinformationen finden Sie unter Cloud Provisioning and Governance: Terraform Connector Formularreferenz für API-Schlüssel-Anmeldeinformationen.

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Die App Cloud Provisioning and Governance: Terraform Connector unterstützt die folgenden Terraform -Datentypen:

- Zeichenfolge
- Nummer
- boolescher Wert
- Liste
- Tupel
- Zuordnen
- Objekt

Prozedur

1. Ein Cloud-Katalogelement erstellen.

   a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**.
   Das Cloud-Adminportal wird in einer neuen Browserregisterkarte geöffnet.

   b. Navigieren zu **Entwurf** > **Cloud-Katalogelemente**.

   c. Wählen Sie **Neu**.

   d. Füllen Sie die Felder des Formulars aus.

Formular „Cloud-Katalogelement“

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name des Katalogelements.
Quelle	Quelle des Katalogelements. Wählen Sie in der Dropdown-Liste **Konfigurationsmanagement-Vorlage** aus.
Anbietertyp	Terraform Konfigurationsanbietertyp, den Sie verwenden möchten.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ Um Terraform Enterprise oder Terraform Cloudzu verwenden, wählen Sie **Terraform Enterprise**aus. ▪ Um einen Linux-basierten Terraform Open Source -Server zu verwenden, wählen Sie **Terraform-Umgebung**aus. ▪ Um einen Windows-basierten Terraform Open Source -Server zu verwenden, wählen Sie **Terraform Windows Environment (Terraform-Windows-Umgebung)**aus.
Anbieter	Name des Terraform Konfigurations-Providers, den Sie verwenden möchten.

e. Speichern Sie das Formular „Cloud-Katalogelement“.

2. Ordnen Sie dem Katalogelement eine Terraform -Vorlage zu.

a. Wählen Sie in der zugehörigen Liste Cloud-Vorlagen **Neu**.

b. Wählen Sie in der Dropdown-Liste Konfiguration installierbar die Vorlage Terraform aus, die Sie verwenden möchten.

c. Speichern Sie das Formular ServiceNow Cloud-Vorlagenversionen.

Hinweis: Ein Katalogelement kann mehrere Versionen der Cloud-Vorlage enthalten, aber nur eine Version kann aktiv sein.

d. Wählen Sie **Aktivieren** aus, um die Cloud-Vorlage zu aktivieren.

3. Wahlweise: Um Katalogelement-Formularfelder hinzuzufügen oder zu entfernen, bearbeiten Sie die dem Katalogelement zugeordneten Variablensätze.

4. Aktivieren Sie die Checkbox **Aktiv**, um das Katalogelement zu aktivieren.

5. Wählen Sie **Aktualisieren**.

Nächste Maßnahme
Vergewissern Sie sich, dass das Katalogelement im Cloud-Anwenderportal angezeigt wird.

Verwalten Sie die Terraform vorlagenbasierten Katalogelemente

Verwenden Sie eine IaC-Change-Aufgabe (Infrastructure as Code), um die Terraform vorlagenbasierten Katalogelemente zu erstellen oder zu aktualisieren. Die IaC-Change-Aufgabe trägt dazu bei, dass die -Katalogelemente an den aktuellen Infrastrukturspezifikationen ausgerichtet sind, die in der Vorlage Terraform codiert sind.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Wenn die App Cloud Provisioning and Governance: Terraform Connector eine Änderung der Variablen in der Vorlagendatei (.TF) Terraform oder der Metadatendatei (`metadata.snc`) erkennt, erstellt sie Change-Aufgaben. Die Change-Aufgaben werden Benutzern zugewiesen, die die Katalogelemente erstellt haben (Benutzer mit der Rolle [sn.cmp.cloud_service_designer]). Je nach in den Vorlagenvariablen oder den Metadaten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

erkanntem Change werden Sie von der Katalogelementaufgabe aufgefordert, eine der folgenden Aktionen auszuführen:

- Erstellen Sie ein Katalogelement aus der geänderten Vorlagenversion.

  Ein neues Katalogelement wird erstellt. Dabei wird eine Nummer an den bestehenden Namen des Katalogelements angehängt. Wenn das vorhandene Katalogelement beispielsweise `Linux VM` heißt, wird das neue Katalogelement unter dem Namen `Linux VM1` erstellt.

- Aktualisiert das vorhandene Katalogelement gemäß der aktualisierten Vorlagenversion.

  Wenn Sie das vorhandene Katalogelement gemäß der aktualisierten Vorlagenversion aktualisieren, wird eine neue Version der Vorlage erstellt und aktiviert, während die vorhandene Vorlagenversion außer Kraft gesetzt und deaktiviert wird.

Hinweis: Der Name des Terraform-Konfigurationsanbieters sollte beim Exportieren von Katalogelementen, die auf Terraform-Vorlagen basieren, in den Umgebungen übereinstimmen. Wenn beispielsweise der Konfigurationsanbieter in der Entwicklungsumgebung TFE heißt, sollte er auch in der Zielumgebung (UAT, Prod usw.) als TFE bezeichnet werden.

Bis Sie eine der oben genannten Aktionen ausführen, ist das Katalogelement deaktiviert. Wenn sich das Katalogelement im Status „Deaktiviert“ befindet, können Cloud-Anwender nicht darauf zugreifen.

Cloud Provisioning and Governance: Terraform Connector erstellt eine IaC-Change-Aufgabe für ein vorlagenbasiertes Katalogelement Terraform, wenn eine der folgenden Bedingungen erfüllt ist:

- Der Quellvorlage Terraform wird eine oder mehrere Variablen hinzugefügt.
- Mindestens eine Variable wird aus der Quellvorlage Terraform gelöscht.
- Eine oder mehrere Variablen, die in der Quellvorlage Terraform verwendet werden, erfahren eine Datentypänderung.
- Der Standardwert einer oder mehrerer Variablen ändert sich.

Hinweis: Die Aufhebung der Bereitstellung des betroffenen Stapels löst die Aufhebung der Bereitstellung beim Cloud-Anbieter aus.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**. Das Cloud-Adminportal wird in einer neuen Browserregisterkarte geöffnet.
2. Navigieren zu **IaC** > **Change-Aufgaben**.
3. Öffnen Sie die entsprechende Change-Aufgabe.
4. Wahlweise: Passen Sie die neuen oder aktualisierten Variablen an, die in der Vorlage Terraform erkannt wurden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Wählen Sie den zugehörigen Link **Variablen anpassen** aus.

b. Bearbeiten Sie den Standardwert der neuen oder aktualisierten Variablen Terraform aus der zugehörigen Liste „Metadaten der Terraform-Aufgabe“.

> **Hinweis:** Der im Variablendatensatz der zugehörigen Liste Terraform Aufgaben-Metadaten erwähnte Standardwert überschreibt den in der Vorlage Terraform erwähnten Standardwert.

5. Wahlweise: Wählen Sie den Link **„Änderungen“** in der Empfehlungsnachricht aus, um einen Unterschiedsvergleich im Vorlageninhalt anzuzeigen, der von IaC-Discovery erkannt wurde.
6. Füllen Sie die Felder des Formulars aus.
   Weitere Informationen finden Sie unter Cloud Provisioning and Governance: Terraform Connector Terraform Referenz des Formulars „Katalogelementaufgabe“..
7. Wählen Sie **Aktualisieren**.

Anmeldeinformationen zwischen Cloud Provisioning and Governance und Terraformzuordnen

Ordnen Sie mit der Funktion der Zuordnung von Anmeldeinformationen zwischen Cloud Provisioning and Governance und Terraform mithilfe der Zuordnung von Anmeldeinformationen.

Vorbereitungen

Die neueste Version Cloud Provisioning and Governance: Terraform Connector muss aus installiert werden ServiceNow Store .

Erforderliche Rolle: sn_cmp.cloud_admin, admin

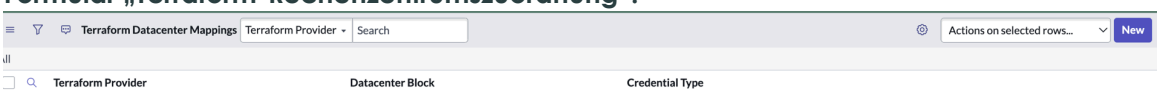
Warum und wann dieser Vorgang ausgeführt wird

Verwenden Sie das Modul „Zuordnung von Anmeldeinformationen, um Zuordnungen von Anmeldeinformationen und Servicekonten für Rechenzentrums-Anmeldeinformationen durchzuführen, die vom Anbieter Terraform zur Bereitstellung von Rechenzentrumsressourcen und Cloud Provisioning and Governance von für die Discovery verwendet werden.

Prozedur

1. Navigieren zu **Alle** > **Entwurf** > **Zuordnung von Anmeldeinformationen**.
2. Wählen Sie **Neu**.

Formular „Terraform-Rechenzentrumszuordnung“.



3. Füllen Sie die Felder des Formulars aus.

Terraform Formular „Rechenzentrumszuordnungen“.

Feld	Beschreibung
Terraform Anbieter	Name des Anbieters Terraform
Rechenzentrumsblock	Der Ressourcenblock, dessen Anmeldeinformationen Sie aus der Suchtabelle zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anmeldeinformationstyp	Der entsprechende Anmeldeinformationstyp aus der Suchtabelle. Beispiel: Azure Serviceprinzipal [azure_service_principal].
Resolver für Anmeldeinformationen	Eine entsprechende MID-Server -Skripteinbindung aus der Suchtabelle. Beispiel: Suchen Sie das TerraformProviderCredentialResolver-Skript und wählen Sie es aus.

4. Wählen Sie **Absenden**.
   Der Datensatz mit den Provider-Anmeldeinformationen Terraform wird erstellt und in der Liste Terraform Rechenzentrumszuordnungen angezeigt.
5. Navigieren Sie in dem von Ihnen erstellten Datensatz zur zugehörigen Liste „ **Zuordnungen der Anmeldeinformationen“**, und wählen Sie **Neu**aus.

   a. Füllen Sie das Formular **Zuordnung von Anmeldeinformationen** aus.

Feld	Beschreibung
Anbieter-Authentifizierungsschlüssel	Feldname des Authentifizierungsschlüssels (Variable), wie vom Provider verwendet. Zum Beispiel verwendet der Anbieterblock Terraform für (Amazon Web Services) AWS das `Feldsecret_key`.
Discovery-Anmeldeinformationsschlüssel	Das entsprechende Feld in den Discovery-Anmeldeinformationen aus der Suchtabelle. Zum Beispiel entspricht das Feld `„access_key“` in Terraform dem Feld `„Geheimer Schlüssel“` in der Instanz ServiceNow.
Terraform Zuordnung des Rechenzentrums	Rechenzentrum, für das Sie die Anmeldeinformationen zuordnen.

   b. Wählen Sie **Absenden**.

6. Wählen Sie die Registerkarte **Service-Account-Zuordnungen** und dann **Neu**aus.

   a. Füllen Sie das Formular **Servicekontozuordnung** aus.

Feld	Beschreibung
Anbieter-Authentifizierungsschlüssel	Feldname des Authentifizierungsschlüssels (Variable), wie vom Provider verwendet. Zum Beispiel verwendet der Provider-Block Terraform für AWS das `Feldsecret_key`.
Feld für Service-Account	Feldname des Servicekontos (Variable) aus der Suchtabelle, dessen Anmeldeinformationen Sie dem Provider-Authentifizierungsschlüssel zuordnen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Terraform Zuordnung des Rechenzentrums	Rechenzentrum, für das Sie die Anmeldeinformationen zuordnen.

b. Wählen Sie **Absenden**.

Sie haben die Feldwerte, die Sie unter den zugehörigen Listen „Anmeldeinformationszuordnung“ und „Service-Account-Zuordnung“ hinzugefügt haben, dem Anbieter Terraform zugeordnet.

Ordnen Sie die Umgebungsvariable Terraform dem Ressourcenblock des Rechenzentrums zu

Ordnen Sie die Umgebungsvariable Terraform dem Ressourcenblock des Rechenzentrums Cloud Provisioning and Governance zu. Nachdem Sie die Umgebungsvariable zugeordnet haben, können Sie sie verwenden, um anwenderdefinierte Eingabeparameter während der Ressourcenbereitstellung über Terraform Enterprisezu übergeben.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Um die Umgebungsvariable Terraform bedingt festzulegen, verwenden Sie einen geskripteten Ausdruck. Weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden.

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal**.
   Das Cloud-Adminportal wird in einer neuen Browserregisterkarte geöffnet.
2. Auswahlvorgang **Entwurf** > **Ressourcenblöcke**.
3. Wählen Sie die entsprechende Karte für das logische Rechenzentrum aus.
4. Versetzen Sie den Ressourcenblock des logischen Rechenzentrums in den Status **Entwurf**.
5. Wählen Sie die Registerkarte **Vorgänge** aus.
6. Wählen Sie in der Dropdown-Liste Schnittstelle die **Option Terraform Orchestration-Schnittstelle**aus.
7. Auswahlvorgang **Schritte** > **Flow.Subflow.TFEBereitstellung**.
8. Legen Sie das Textfeld **„terraform_variables“** auf das Schlüssel-Wert-Paar der Umgebungsvariablen fest.
   Beispiel: **{"USER_AGENT_PROVIDER_NAME":"AgentValue"}**
9. Legen Sie den Ressourcenblock des logischen Rechenzentrums auf den Status **„Veröffentlicht“** fest.

Cloud Provisioning and Governance: Terraform Connector-Referenz

Referenzthemen enthalten zusätzliche Informationen zur Anwendung Cloud Provisioning and Governance: Terraform Connector.

Cloud Provisioning and Governance: Terraform Connector Formularreferenz „Konfigurations-Provider erstellen“.

Cloud Provisioning and Governance verwendet den Konfigurations-Provider für die Interaktion mit der Bereitstellung Terraform.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Name des Konfigurationsanbieters.
Anbieter	Konfigurationsanbietertyp. • Terraform Enterprise: Wählen Sie diesen Wert aus, um einen Terraform Enterprise -Konfigurations-Provider zu erstellen. • Terraform Umgebung: Wählen Sie diesen Wert aus, um einen Linux-basierten Konfigurations-Provider Terraform Open Source zu erstellen. • Terraform Windows Umgebung: Wählen Sie diesen Wert aus, um einen Windows-basierten Konfigurations-Provider Terraform Open Source zu erstellen.
Organisation	OrganisationTerraform, die die Arbeitsbereiche und Vorlagen-Repositorys Terraform enthält. Dieses Feld erscheint, wenn Sie Terraform Enterprise in der Dropdown-Liste Anbieter auswählen.
URL	Basis-URL des API-Servers Terraform oder IP-Adresse des Servers Terraform. • Um einen Konfigurations-Provider für Terraform Open Sourcezu erstellen, geben Sie den IP-Port des Servers Terraform ein. • Um einen Konfigurations-Provider für Terraform Enterprisezu erstellen, geben Sie die Basis-URL des Terraform Enterprise -API-Servers ein. • Um einen Konfigurations-Provider für Terraform Cloudzu erstellen, geben Sie `https://app. Terraform.io/api/v2`ein
Basisverzeichnis	Verzeichnis, in dem sich alle einzelnen Terraform -Vorlagenverzeichnisse befinden. Dieses Feld wird angezeigt, wenn Sie Terraform Umgebung oder Terraform Windows Umgebung in der Dropdown-Liste Anbieter auswählen.
Servertyp	Servertyp der Terraform -Bereitstellung.
Referenz	Anmeldeinformationen für den Zugriff auf Terraform. • Wählen Sie für den Linux-basierten Server Terraform Open Source die entsprechenden Anmeldeinformationen für den privaten SSH-Schlüssel aus. • Wählen Sie für den Windows-basierten Server Terraform Open Source die entsprechenden RDP-Anmeldeinformationen (Remote Desktop Protocol) aus. • Wählen Sie für Terraform Enterprise oder Terraform Clouddie entsprechenden Terraform API-Schlüssel-Anmeldeinformationen aus.
Version	Unterstützte Terraform Open Source CLI-Version, die auf dem Server Terraform installiert ist. Weitere Informationen zu den unterstützten Versionen Terraform Open Source finden Sie im Abschnitt über die Voraussetzungen von Erstellen Sie einen Konfigurations-Provider Terraform Open Source ..

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Weitere Informationen zu den unterstützten Versionen Terraform Enterprise und Terraform Cloud finden Sie im Abschnitt über die Voraussetzungen in Erstellen Sie einen Terraform Enterprise - oder Terraform Cloud -Konfigurations-Provider. Ab Cloud Provisioning and Governance: Terraform Connector Version 1.5.2, Version 1.0.0 ist veraltet. Die veraltete Version entspricht Terraform Open Source CLI Version 0.11 und 0.12.

Cloud Provisioning and Governance: Terraform Connector Formularreferenz für Anmeldeinformationen des privaten SSH-Schlüssels

Cloud Provisioning and Governance: Terraform Connector verwendet die Anmeldeinformationen des privaten SSH-Schlüssels, um eine Verbindung zum Server Linux herzustellen, auf dem Terraform Open Source ausgeführt wird.

Der Server Linux unterstützt die folgenden Authentifizierungsmodi:

- Authentifizierung mit Anwendername und Passwort.
- Authentifizierung nur mit dem privaten Schlüssel.
- Authentifizierung mit privatem Schlüssel und SSH-Passwortsatz.

Feld	Beschreibung
Name	Name des Berechtigungsnachweises
Anwendername	SSH-Anwendername des Servers Linux, auf dem Terraform ausgeführt wird.
Passwort	SSH-Passwort des Servers Linux, auf dem Terraform ausgeführt wird.
SSH-Passwortsatz	SSH-Passwortsatz des Servers Linux, auf dem Terraform ausgeführt wird.
Privater SSH-Schlüssel	Privater SSH-Schlüssel des Servers Linux, auf dem Terraform ausgeführt wird.

Cloud Provisioning and Governance: Terraform Connector Windows Formularreferenz für Anmeldeinformationen

Cloud Provisioning and Governance: Terraform Connector verwendet die Anmeldeinformationen Windows, um eine Verbindung zum Server Windows herzustellen, auf dem Terraform Open Source ausgeführt wird.

Feld	Beschreibung
Name	Name des Berechtigungsnachweises
Anwendername	RDP-Anwendername (Remote Desktop Protocol) für den Server Windows, auf dem Terraform ausgeführt wird.
Passwort	RDP-Passwort für den Server Windows, auf dem Terraform ausgeführt wird.

Cloud Provisioning and Governance: Terraform Connector Formularreferenz für API-Schlüssel-Anmeldeinformationen

Cloud Provisioning and Governance: Terraform Connector verwendet API-Schlüssel-Anmeldeinformationen, um die Anforderungen zu authentifizieren, die an Terraform

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Enterprise und Terraform Cloud und die darin bereitgestellten Versionskontrollsysteme gesendet werden.

Weitere Informationen zu API-Schlüsselberechtigungen und Tokens finden Sie unter https://developer.hashicorp.com/terraform/cloud-docs/users-teams-organizations/api-tokens .

Feld	Beschreibung
Name	Eindeutiger und beschreibender Name der Anmeldeinformationen.
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.

API-Schlüssel	API-Schlüssel, der für den Zugriff auf den Account verwendet werden kann.
	• Terraform Enterprise oder Terraform Cloud API-Schlüssel: Bearer-Token für den Zugriff auf Terraform Enterprise oder Terraform Cloud.
	Stellen Sie sicher, dass der API-Schlüssel der folgenden Syntax entspricht:
	`Bearer <API key>`
	• GitHub API-Schlüssel: API-Token für den Zugriff auf den Unternehmens- oder Community-Account GitHub.
	Stellen Sie sicher, dass das Token der folgenden Syntax entspricht:
	`Token <API key>`
	• GitLab API-Schlüssel: Bearer-Token für den Zugriff auf den Unternehmens- oder Community-Account GitLab.
	Stellen Sie sicher, dass das Token der folgenden Syntax entspricht:
	`Bearer <API key>`
	• Microsoft Azure DevOps API-Schlüssel: base64-codiertes Token für den Zugriff auf den Unternehmens- oder Community-Account Azure DevOps.
	Wichtig: Stellen Sie dem API-Token einen Doppelpunkt (:) voran, und codieren Sie dann die gesamte Zeichenfolge im Base-64-Format.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Stellen Sie sicher, dass das Token der folgenden Syntax entspricht: `Basic <base-64 encoded API key>`
Betrifft	MID-Server, auf den Sie die Anmeldeinformationen anwenden. Wählen Sie **Alle MID-Server**aus
Auftrag	Reihenfolge, in der die Plattform diese Anmeldeinformationen ausführt, wenn versucht wird, sich bei Geräten anzumelden. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist 100.
Anmeldeinformationsalias	Anmeldeinformationsalias, der die Anmeldeinformationen auflösen kann.

Cloud Provisioning and Governance: Terraform Connector Terraform Referenz des Formulars „Katalogelementaufgabe“.

Geben Sie im Formular Terraform Katalogelementaufgabe die Aktion an, die Sie zum Lösen der Change-Aufgabe für das Katalogelement ausführen möchten.

Terraform Formular „Katalogelementaufgabe“.

Feld	Beschreibung
Aktion für Katalogelementaufgabe	Aktion, die Sie ausführen möchten. • Katalogelement mit dieser Vorlagenversion aktualisieren Wählen Sie diese Option aus, um das Katalogelement mit dieser Vorlagenversion zu aktualisieren. Eine neue Version der Vorlage wird erstellt und aktiviert, während die vorhandene Vorlagenversion deaktiviert wird. • Create catalog item with this template (Neues Katalogelement mit dieser Vorlage erstellen) Wählen Sie diese Option aus, um ein Katalogelement mit dem vorhandenen Katalogelementnamen zu erstellen und eine Nummer an den Katalogelementnamen anzuhängen. Wenn Ihr Katalogelement beispielsweise `Linux VM`lautet, wird

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Terraform Formular „Katalogelementaufgabe“. (Fortsetzung)

Feld	Beschreibung
	der neue Katalog mit dem Namen `Linux VM 1`erstellt. Das Katalogelement wird automatisch aktiviert und kann über das Cloud-Benutzerportal bereitgestellt werden.
Zuweisungsgruppe	Die Zuweisungsgruppe, der Sie die Katalogelementaufgabe zuweisen.
Zugewiesen an	Benutzer, dem Sie die Aufgabe zuweisen
Kurzbeschreibung	Kurze Beschreibung der Aufgabe.
Genehmigung	Genehmigungsstatus der Aufgabe
Arbeitsnotizen	Etwaige Notizen, die Sie für den Aufgabendatensatz eingeben möchten

Vorgänge an Tag 2 mit Workflows

Nutzen Sie das Framework der Workflows, um Ihre Vorgänge an Tag 2 zu automatisieren. Schreiben Sie schnell einen Workflow, der mit einer Cloud API oder einer bestimmten Ressource kommuniziert. Verwenden Sie SSH, PowerShell oder ein ähnliches Tool, um auf die Workflow-Fähigkeiten zuzugreifen und sie dann zu erweitern.

Die Tag-1-Vorgänge stellen Ressourcen in einer Cloud als Teil der Bestellung aus dem ServiceNow-Katalog oder dem Cloud-Katalog bereit. Diese Vorgänge führen zu einem Stapel, der eine Liste der bereitgestellten Ressourcen enthält. Tag-2-Vorgänge können für die Ressourcen ausgeführt werden, die Teil des Stapels sind, oder für die vom System erkannten Ressourcen.

Zuvor mussten Sie zum Ausführen von Tag-2-Vorgängen in Cloud Provisioning and Governance direkt mit der Cloud API (CAPI) interagieren. Dies bedeutete häufig, dass Sie neue APIs schreiben mussten, um einen neuen Vorgang zu unterstützen. Mit der Möglichkeit, Tag-2-Vorgänge Workflows zuzuordnen, können Sie die Basissystem-Workflow-Fähigkeiten jetzt noch einfacher nutzen.

Zu den Fähigkeiten gehören:

- SSH/PowerShell zum Herstellen einer Verbindung mit einer VM.
- Verwenden von REST-Endpunkten zum Aufrufen verschiedener Cloud-Provider.
- Aufrufen plattformspezifische Funktionen.

Regeln mit Workflows

Cloud Provisioning and Governance unterstützt die Verwendung von Now Platform-Regeln mit Workflows. Regeln sind Sammlungen von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das System die Aktionen aus. Wenn eine Bedingung als „false“ ausgewertet wird, führt das System die Aktionen nicht aus. Das Erstellen von Regeln hilft Ihnen, Aktivitäten nachzuverfolgen und schneller auf Probleme zu reagieren und sie zu lösen.

Weitere Informationen

Allgemeine Informationen zu Workflows finden Sie unter:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Workflow-Übersicht
- Workflow aus einer Tabelle erstellen

Informationen zum Arbeiten mit Variablen in Workflows finden Sie unter:

- Workflow-Eingabevariablen
- Variablen in einem Workflow verwenden

Anmeldeinformationen verarbeiten

Erweitern Sie das Workflow-Modul, um Prozesse zu verwalten und Dinge außerhalb einer Instanz mit Orchestration zu automatisieren. Verwenden Sie die entsprechenden Anmeldeinformationen, die für Aktivitätselemente von Orchestration SSH und PowerShell erforderlich sind: SSH erfordert SSH und PowerShell erfordert Windows.

Die Cloud Provisioning and Governance-Anwendung generiert Anmeldeinformationen (Knotenanmeldeinformationen), nachdem eine VM bereitgestellt wurde. Knotenanmeldeinformationen werden verwendet, um eine Verbindung zu einer VM herzustellen. Zusätzlich zu den Knotenanmeldeinformationen generiert das System SSH-/Windows-Anmeldeinformationen. Diese Anmeldeinformationen sind für Orchestration erforderlich, was die Automatisierung von Workflows bereitstellt.

Bereits vorhandene VMs

Cloud Provisioning and Governance generiert jetzt SSH-Anmeldeinformationen als private Schlüssel und Windows-Anmeldeinformationen für alle aktiven, bereits vorhandenen VMs, die über Cloud Provisioning and Governance bereitgestellt werden.

Anmeldeinformationen löschen

Wenn Sie die Bereitstellung einer VM aufheben oder sie löschen, werden alle zugehörigen Anmeldeinformationen gelöscht, einschließlich der Knotenanmeldeinformationen und der SSH-Anmeldeinformationen als private Schlüssel bzw. Windows-Anmeldeinformationen sowie des Anmeldeinformationsalias-Tags.

Anmeldeinformationen verwenden

Weitere Detailinformationen finden Sie unter Anmeldeinformationen in SSH-Workflows verwenden.

Anmeldeinformationen in SSH-Workflows verwenden

Fügen Sie einen SSH-Workflow mit einem Anmeldeinformations-Tag hinzu.

Vorbereitungen

- Orchestration muss installiert sein.
- Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Sie können einen Ausdruck verwenden, um das Anmeldeinformationsalias-Tag abzurufen. Anweisungen finden Sie unter SSH-Aktivität erstellen .

In diesem Beispiel wird eine VM verwendet, die in einem AWS LDC-Rechenzentrum bereitgestellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Klicken Sie im Cloudbenutzerportal auf **Einen Stapel starten**, und wählen Sie die AWS-VM aus.
2. Geben Sie auf der Registerkarte „Allgemeine Informationen“ einen eindeutigen und aussagekräftigen **Stapelnamen** ein, wählen Sie **AWS-Rechenzentrum** als **Standort** aus, und klicken Sie dann auf **Weiter**.
3. Geben Sie auf der Registerkarte „Bereitstellung“ einen **Knotennamen für den virtuellen Server** ein (der Name kann mit dem Stapelnamen identisch sein), und klicken Sie dann auf **Absenden**.
   Die Seite „Cloud-Aktivitäten“ zeigt die von Ihnen angeforderte VM und den Status Ihrer Anforderung an. Der Abschnitt „Anforderungsstatus“ zeigt nach Abschluss „Bereitstellung erfolgreich“ an.
4. Sehen Sie sich in Ihrer Instanz den Workflow an:

   a. Filtern Sie nach Workflow, und klicken Sie dann auf **Workflow-Editor**.

   b. Filtern Sie rechts im Workflow-Listenfenster auf der Registerkarte „Workflows“, und wählen Sie den Workflow aus, mit dem Sie arbeiten möchten.
   Wenn der Workflow im Canvas-Bereich angezeigt wird, wird die Aktivitätspille „SSH-Befehl ausführen“ im Workflow angezeigt.

5. Zum Bearbeiten der Aktivitäten im Workflow klicken Sie auf das Symbol für die Workflow-Eigenschaften (Kreis mit einem i), und führen Sie folgende Schritte aus:

   a. Wechseln Sie auf der **Registerkarte** Anwenderdefiniert rechts zu **Anwenderdefinierte Aktivitäten** > **Global** und doppelklicken Sie auf die Aktivität, um sie zu ändern.
   Wenn die neue Aktivität im Activity Designer geöffnet wird, können Sie das Formular verwenden, um eine wiederverwendbare Orchestrierungsaktivität zu erstellen.

   b. Um von der Cloud Provisioning and Governance-Anwendung zur Global-Anwendung zu wechseln und den Datensatz zu bearbeiten, klicken Sie in der Menüleiste auf **Hier**.
   Die Global-Anwendung stellt die Aktivitäten plattformübergreifend zur Verfügung.

6. Bearbeiten Sie die Felder auf den folgenden Aktivitätsregisterkarten.
7. Klicken Sie auf **Fortfahren**, um zur nächsten Registerkarte zu wechseln.
8. Folgen Sie der Feldbeschreibung unten, um **die Aktivitätsdetails** auszufüllen.

Registerkarte „Aktivität“	Feldbeschreibungen
Allgemein	Eindeutiger Name für die Aktivität
Eingaben	Werte für Host, Typ und ob die Aktivität obligatorisch ist.
Ausführungsbefehl	Zum Bilden des auszuführenden Befehls ziehen Sie Eingaben aus der Liste in das Formular. Verfügbare Eingaben: ◦ **Host** ist die IP-Adresse der VM, mit der eine Verbindung hergestellt werden soll. ◦ **Befehl** ist ein beliebiges Skript oder ein einzelner Befehl, der auf der VM ausgeführt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Registerkarte „Aktivität“	Feldbeschreibungen
	◦ **Anmeldeinformations-Tag** ist das Alias für die sys_id der VM. Sie können das Anmeldeinformations-Tag entweder manuell eingeben oder einen Ausdruck im Ressourcenskript bereitstellen, das dann das Anmeldeinformations-Tag-Feld automatisch ausfüllt. Skript: *$(Script:CMPVMUtils.getCredentialAlias[arg=$[parameter.resourceID]])*
Ausgabe	Name der einzelnen Ausgabe und Typ der einzelnen Ausgabe, z. B. Zeichenfolge.
Bedingungen	Alle erforderlichen Bedingungen. Bedingungen sind optional.

Verwenden Sie SSH, um eine VM mithilfe eines Workflow-Typvorgangs herunterzufahren

Verwenden Sie SSH, um eine VM mithilfe eines Workflow-Vorgangs remote herunterzufahren. Folgen Sie diesem Anwendungsfall, um alle erforderlichen Aufgaben für diese Art von Herunterfahren zu durchlaufen.

Vorbereitungen
Erforderliche Rolle: workflow designer oder sn_cmp.cloud_admin

Prozedur

1. Führen Sie die folgenden Schritte aus, um die benutzerdefinierte SSH-Aktivität zu erstellen:

a. Navigieren zu **Administratorportal** > **Workflows** > **Workflow-Editor**.

b. Klicken Sie auf die Registerkarte **Anwenderdefiniert** und dann auf **+** (Pluszeichen), um eine neue anwenderdefinierte Aktivität zu erstellen.

c. Wählen Sie **SSH** aus der Liste der Aktivitätstypen aus.

d. Der Aktivitätsdesigner wird mit der angezeigten Registerkarte Allgemein geöffnet Geben Sie einen eindeutigen Namen für die Aktivität ein, und klicken Sie dann auf **Fortfahren**.

e. Fügen Sie auf der Registerkarte „Eingaben“ die Eingabevariablen mit den folgenden Schritten hinzu, und klicken Sie dann auf **Fortfahren**:

f. Klicken Sie in der Eingabetabelle auf das **+ in einem Kreis**, um eine neue Eingabevariable zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

g. Klicken Sie rechts neben ABC in der Spalte **Name**, und geben Sie den Eingabenamen ein.

Eingaben variieren je nach betroffenem Objekt. Sie können eine Aktivität anhalten, um eine VM anzuhalten, sodass die Eingaben die Werte widerspiegeln, die zum Ausführen dieser Aktion erforderlich sind.

Die Spalten **Typ** und **Obligatorisch** werden gemäß den von Ihnen angegebenen Eingaben automatisch ausgefüllt.

h. Erstellen Sie für jede Eingabe in der folgenden Tabelle ein neues Eingabeobjekt, und klicken Sie dann auf **Fortfahren**:

Eingabevariablen	Typ	Obligatorisch
Host	Zeichenfolge	Nein
Befehl	Zeichenfolge	Nein
CredentialTag	Zeichenfolge	Nein

i. Führen Sie auf der Registerkarte „Ausführungsbefehl“ Folgendes aus:

j. Klicken Sie in der Ausgabetabelle auf das **+ in einem Kreis**, um eine neue Ausgabevariable zu erstellen.

k. Klicken Sie rechts neben ABC in der Spalte **Name**, und geben Sie den Ausgabenamen ein.
Die Ausgabevariablen geben die möglichen Ergebnisse an, wenn der Workflow versucht, SSH-Verbindungen zur VM herzustellen. Die Spalte **Typ** wird automatisch ausgefüllt.

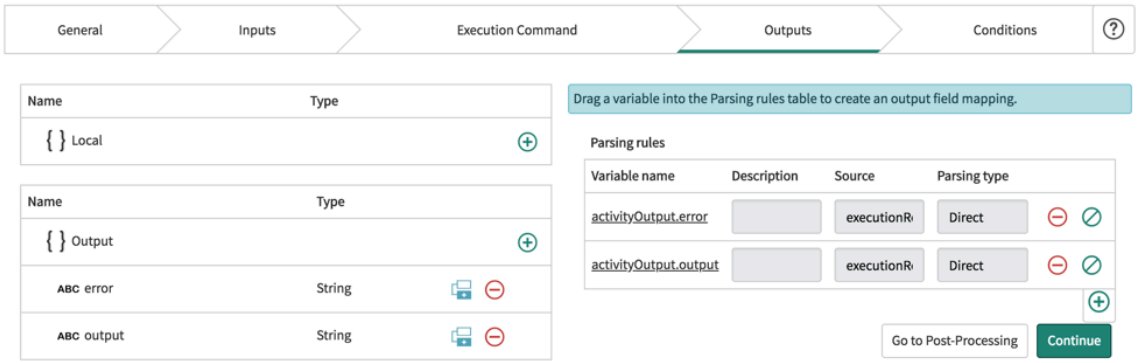
Ausgaben	Typ
Fehler	Zeichenfolge
Ausgabe	Zeichenfolge

l. Klicken Sie auf die **Fehlervariable**, und ziehen Sie sie in das Feld für den Variablennamen in der Tabelle mit Analyseregeln.

m. Wählen Sie im Dialogfeld der Analyseregel für Fehler in der Dropdown-Liste der Analysequellen die entsprechende Quelle aus. In diesem Fall „executionResult.errorMessages“.

n. Wiederholen Sie den Vorgang für die Ausgabevariable, wählen Sie „executionResult.output“ als Analysequelle aus, und klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



o. Klicken Sie auf **Fortsetzen**.
Bedingungen sind optional.

p. Klicken Sie auf **Speichern**und dann auf **Veröffentlichen**, um die Aktivität zur Verwendung im Workflow verfügbar zu machen.

2. Führen Sie zum Erstellen des SSH-Workflows zum Herunterfahren der VM die folgenden Schritte aus:

Wenn Sie einen Workflow erstellen, ordnen Sie ihn einer Tabelle und einer Aktivität zu.

- Sie können den Workflow in einer Tabelle auf globaler Ebene oder in einer Tabelle auf Anwendungsebene erstellen. Verwenden Sie die globale Tabelle, um den Workflow für alle ServiceNow-Anwendungen verfügbar zu machen. Hier verwenden wir eine Tabelle für Cloud Provisioning and Governance, sodass dieser Workflow nur für die Verwendung mit dieser Anwendung verfügbar ist.
- Sie können den Workflow im Workflow-Editor oder im Activity Designer erstellen. Hier wird der Activity Designer verwendet.

a. Wählen Sie im Activity Designer rechts die Registerkarte **Workflows** aus, und klicken Sie dann auf das Pluszeichen (**+**), um einen neuen Workflow hinzuzufügen.

b. Geben Sie im Fenster „Neuer Workflow“ einen eindeutigen Namen für den Workflow ein.

c. Wählen Sie aus dem Dropdown-Menü **Tabelle** die zu verwendende Tabelle aus.
Suchen Sie nach der **VM-Instanz cmdb_ci_vm_instance,** und verwenden Sie sie, um mit dem Workflow eine VM auszuschalten.

d. Klicken Sie auf **Absenden**.

e. Wenn der Workflow im Canvas-Bereich angezeigt wird, löschen Sie die Verbindungslinie zwischen Start- und Endpunkt des Workflows.

f. Löschen Sie die Verbindungslinie zwischen Start- und Endpunkt des Workflows.

g. Klicken Sie mit der rechten Maustaste auf die Canvas mit weiteren Informationen, und wählen Sie **Eingaben bearbeiten** aus.

h. Erstellen Sie die folgenden Eingaben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Übernehmen Sie die Eingabenamen aus dem Feld „Spalte“, nicht aus dem Feld „Bezeichnung“. Wenn der Workflow einer Tabelle auf globaler Ebene zugeordnet ist, wird dem Eingabenamen im Feld „Spalte“ das Präfix „u_“ vorangestellt, z. B. u_ipaddress. Hier befindet sich die Tabelle auf Anwendungsebene, daher ist kein Präfix erforderlich.

Workflow-Eingaben

Typ	Bezeichnung	Spalte (automatisch hinzugefügt)	Max. Länge
Zeichenfolge	IPAddress	ipaddress	100
Zeichenfolge	CredentialTag	credentialtag	100

i. Klicken Sie auf **Absenden**.

j. Klicken Sie mit der rechten Maustaste auf die Canvas, und wählen Sie **Benutzerdefinierte Aktivität hinzufügen** aus.

k. Suchen Sie im Fenster „Versionen“ nach der Aktivität, die Sie zu Anfang in diesem Anwendungsfall erstellt haben, und wählen Sie sie aus.

l. Geben Sie im Fenster „Neue Aktivität“ für diese Aktivität (Workflow-Aktivität „Neuer Datensatz“ [Diagrammansicht]) einen Namen für die Aktivität ein.

m. Geben Sie im Feld **Host** die von der Aktivität erwartete Eingabezuordnung ein.

Hier ist dies die IP-Adresse des Hosts: *${workflow.inputs.u_ipaddress}*. Verwenden Sie diesen Ausdruck zum Abrufen der IP-Adresse:

$(Script:CMPVMUtils.getReachableIp[arg=$(Stack.items[Virtual Server].attributes[sys_id])])

n. Geben Sie im Feld „Befehl“ *shutdown -h now* ein.

o. Geben Sie im Feld „Anmeldeinformations-Tag“ *${workflow.inputs.u_credentialtag}* ein.

Verwenden Sie diesen Ausdruck, um das Anmeldeinformations-Tag abzurufen:

$(Script:CMPVMUtils.getCredentialAlias[arg=${Stack.items[Virtual Server].attributes[sys_id]}])

p. Klicken Sie auf **Absenden**.
Die Aktivität wird in der Workflow-Canvas angezeigt.

q. Klicken Sie mit der rechten Maustaste auf die Canvas, und wählen Sie **Kernaktivität hinzufügen** aus, um eine Ausführungsskript-Aktivität hinzuzufügen.

r. Suchen Sie im Fenster „Workflow-Aktivitätsdefinitionen“ nach **Skript ausführen** und wählen Sie die Option aus.

s. Geben Sie im Fenster „Neue Aktivität: Skript ausführen“ einen Namen für die Aktivität ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

t. Schneiden Sie ein (für Ihre Umgebung geeignetes) **Skript** aus, und fügen Sie es im Feld „Skript“ ein.
Dieses Skript aktualisiert den Status der VM nach dem Herunterfahren.

Beispielskript:

```
if ( gs.nil(data.get(3).error)) {
                    current.state = 'off';
                    current.setWorkflow(false);
                    current.update();
}
```

u. Klicken Sie auf **Absenden**.

v. Verbinden Sie im Canvas-Bereich die Connectors zwischen dem Anfangspunkt, der Aktivität, dem Ausführungsskript und dem Endpunkt.

w. Validieren Sie den Workflow mithilfe der Workflow-Validierung.

Hinweis: Das System empfiehlt nicht die Verwendung von *`current.update()`*. Dies kann ignoriert werden.

3. Führen Sie die folgenden Schritte aus, um den Vorgang einem Ressourcenblock hinzuzufügen:
Sie können aus den vorhandenen Vorgängen in einem Ressourcenblock auswählen, um mit Ihrem Workflow zu arbeiten, oder Sie können einen benutzerdefinierten Vorgang erstellen.

a. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Ressourcenblöcke**.

b. Wählen Sie einen Ressourcenblock aus, z. B. **Virtueller Server**.

c. Ändern Sie den Status des Ressourcenblocks von **Veröffentlicht** in **Entwurf**, um ihn bearbeitbar zu machen.

d. Wählen Sie die Registerkarte **Vorgänge** und dann im Dropdown-Feld Schnittstelle eine Schnittstelle aus, die dem Benutzer zur Verfügung steht.
Die Standardschnittstelle ist **Virtuelle Serverschnittstelle**.

e. Klicken Sie rechts neben dem Feld „Vorgang“ auf **+**, und geben Sie dann im Dialogfeld „Vorgang hinzufügen“ einen aussagekräftigen und eindeutigen Namen ein.

f. Wählen Sie einen Vorgang aus der Dropdown-Liste „Vorgangstyp“ aus.

g. Wählen Sie im Feld „Zugriffstyp“ die Option **Öffentlich** aus.

h. Füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Vorgangstyp	Wählen Sie den auszuführenden Vorgang aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugriffstyp	Wählen Sie **Öffentlich** aus, damit der Benutzer den Vorgang während der Bereitstellung auf Ressourcenebene sehen kann. Auf **Privat** festgelegte Vorgänge sind während der Bereitstellung nicht sichtbar.

Der Vorgang ist für die Ressource verfügbar, wenn Sie die Ressource für Ihren Workflow auswählen.

i. Um einen Ressourcenvorgangsschritt zum Aufrufen des Workflows hinzuzufügen, klicken Sie noch auf der Registerkarte Vorgänge auf **Schritte** > **Schritt hinzufügen**.
Damit der Workflow als Teil der Update Sets exportiert werden kann, müssen Sie eine Erweiterungsschnittstelle erstellen und den neuen Vorgang hinzufügen. Weitere Detailinformationen finden Sie unter Cloud Provisioning and Governance-Ressourcenblöcke mit einem Überschreibungsvorgang erweitern.

j. Wählen Sie im Popup-Fenster „Vorgangschritte hinzufügen“ die Option **Workflow aufrufen** für **Vorgangstyp** aus.

k. Wählen Sie den **Workflow** aus der Liste der von Ihnen erstellten Workflows aus.
Das System kann die Liste anhand von Tags filtern. So fügen Sie ein Tag hinzu:

i. Navigieren Sie zu **Systemeigenschaften**.

ii. Suchen Sie nach der Systemeigenschaft *sn_cmp.workflow_tag_filter*, und wählen Sie sie aus.

iii. Bearbeiten Sie die Eigenschaft. Fügen Sie ein Tag oder eine kommagetrennte Liste von Tags hinzu.

iv. Klicken Sie auf **Speichern**.

l. So filtern Sie die Workflows:

i. Öffnen Sie in der Workflow-Tabelle den Workflow.

ii. Klicken Sie auf **Tag hinzufügen**.

iii. Geben Sie den Wert ein, den Sie zuvor in der Eigenschaft *sn_cmp.workflow_tag_filter* angegeben haben.

iv. Drücken Sie die **Eingabetaste**, um den Wert als Tag zum Workflow hinzuzufügen. Der neue Schritt wird angezeigt, nachdem die Software den neuen Vorgangskatalog für Tag 2 generiert hat.

m. Es können Workflows vorhanden sein, die in anderen als globalen Tabellen erstellt wurden.
Sie können einen Workflow hinzufügen, der für eine solche Tabelle erstellt wurde. Zum Ausführen von Vorgängen für diese Art von Workflow benötigen Sie die sys_id des Datensatzes, in dem der Workflow ausgeführt wird, um den aktuellen Datensatz zu erstellen. Wenn der Designer einen Workflow hinzufügt, der sich in einer anderen als der globalen Tabelle befindet, erstellt das System einen *wf_current*-Parameter im Vorgangseingabeparameter. Sie können dann einen Ausdruck schreiben, um die sys_id der Ressource zuzuordnen, in der der Vorgang ausgeführt wird. Sobald dies abgeschlossen ist, kann der Designer das Schlüsselwort „aktuell“ in Workflow-Skripts verwenden.

So fügen Sie den Workflow hinzu:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

i. Nachdem Sie den Schritt erstellt haben, fügt das System die Workflow-Eingaben den Vorgangseingabeparametern hinzu. Sie können dann bei Bedarf die Zuordnung für diese Parameter bereitstellen.

ii. Klicken Sie auf die Schaltfläche **Katalog generieren**, um das Katalogelement für den Vorgang zu erstellen.

iii. Nachdem der Katalog generiert wurde, können Sie den Katalogelementen Regeln aus den Lade- und Feldänderungsregeln hinzufügen.

n. Setzen Sie den Ressourcenblock auf den Status **Veröffentlicht**, um den Workflow im Cloudbenutzerportal verfügbar zu machen.

4. Führen Sie die folgenden Schritte aus, um den Vorgang über das Benutzerportal auszuführen:

a. Stellen Sie eine einfache AWS-VM über das Portal bereit.

b. Nach Abschluss der VM-Bereitstellung navigieren Sie zum Stapel > VM-Ressource.

c. Wählen Sie in der Option „Ressourcenvorgang auswählen“ die benutzerdefinierte Stoppaktivität aus, die Sie zuvor in diesem Anwendungsfall erstellt haben, und klicken Sie dann auf OK.
Der Vorgang wird ausgeführt, nachdem das RITM erstellt wurde und sich der VM-Status in der AWS-Konsole ändert.

d. Navigieren zu **Betreiben** > **Pfade** um die Pfadprotokolle anzuzeigen und die Betriebsschritte nachzuverfolgen.

5. Führen Sie bei Bedarf die folgenden Schritte zur Problembehebung aus:

a. Verwenden Sie das Anforderungselement (RITM), und navigieren Sie zum Dashboard „RootCauseAnalysis“.
Das RITM enthält den Link zum Workflow-Kontext des derzeit ausgeführten Vorgangs.

b. Überprüfen Sie diese allgemeinen Fehler:

Fehlerbehandlung

Symptom	Fehlermeldung
VM wird heruntergefahren, aber ein Problem mit der SSH-Verbindung ist aufgetreten	„Fehler; Auftrag mit Status FEHLER beendet: Problem in SSH-Sitzung, Auftrag abgebrochen: Verbindung wurde unerwartet vom SSH-Server geschlossen: \n“
VM ist bereits heruntergefahren/VM ist nicht erreichbar	„Verbindung kann nicht hergestellt werden, der Status ist TCP_CONNECTION_FAILURE. Zeitüberschreitung beim Warten darauf, dass TCP eine Verbindung mit 10.198.252.224:22 herstellt: \n“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Symptom	Fehlermeldung
	Hinweis: Bestätigen Sie, dass die IP-Adresse der VM in „wf_context“ die richtige Adresse ist. Die VM wurde möglicherweise bereits heruntergefahren. Bestätigen Sie, dass die IP-Adresse zugänglich ist.
Root-Zugriff nicht verfügbar	„Fehler beim Ausgeben des Methodenaufrufs: Zugriff verweigert\nMuss root sein.\nExit-Status: 1\n\n“ **Hinweis:** Bestätigen Sie, dass das Kontrollkästchen **Sudo erforderlich** in der SSH-Aktivität zu Beginn dieses Anwendungsfalls aktiviert ist.

Benutzerdefinierte SSH-Aktivität erstellen

Erstellen Sie eine benutzerdefinierte SSH-Aktivität, damit Sie sie in Ihrem Workflow verwenden können.

Vorbereitungen
Erforderliche Rolle: cloud designer oder admin

Prozedur

1. Navigieren zu **Alle** > **Administratorportal** > **Workflows** > **Workflow-Editor**.
2. Klicken Sie auf die Registerkarte **Benutzerdefiniert**, und klicken Sie dann auf „+“ (Pluszeichen), um eine neue benutzerdefinierte Aktivität zu erstellen.
3. Wählen Sie **SSH** aus der Liste der Aktivitätstypen aus.

4. Wenn der Aktivitätsdesigner mit der angezeigten Registerkarte Allgemein geöffnet wird, geben Sie einen eindeutigen Namen für die Aktivität ein, und klicken Sie dann auf **Fortsetzen**.
5. Fügen Sie auf der Registerkarte „Eingaben“ die Eingabevariablen hinzu. Verwenden Sie dazu die folgenden Schritte, und klicken Sie dann auf **Fortfahren**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der Eingabetabelle auf das **+ in einem Kreis**, um eine neue Eingabevariable zu erstellen.

b. Klicken Sie rechts neben ABC in der Spalte **Name**, und geben Sie den Eingabenamen ein.

Eingaben variieren je nach betroffenem Objekt. Hier erstellen wir eine Aktivität zum Stoppen einer VM, sodass die Eingaben die Werte widerspiegeln, die zum Ausführen dieser Aktion erforderlich sind.

Die Spalten **Typ** und **Obligatorisch** werden gemäß den von Ihnen angegebenen Eingaben automatisch ausgefüllt.

c. Erstellen Sie ein neues Eingabeobjekt für jede Eingabe in der folgenden Tabelle, und klicken Sie dann auf **Fortfahren**:

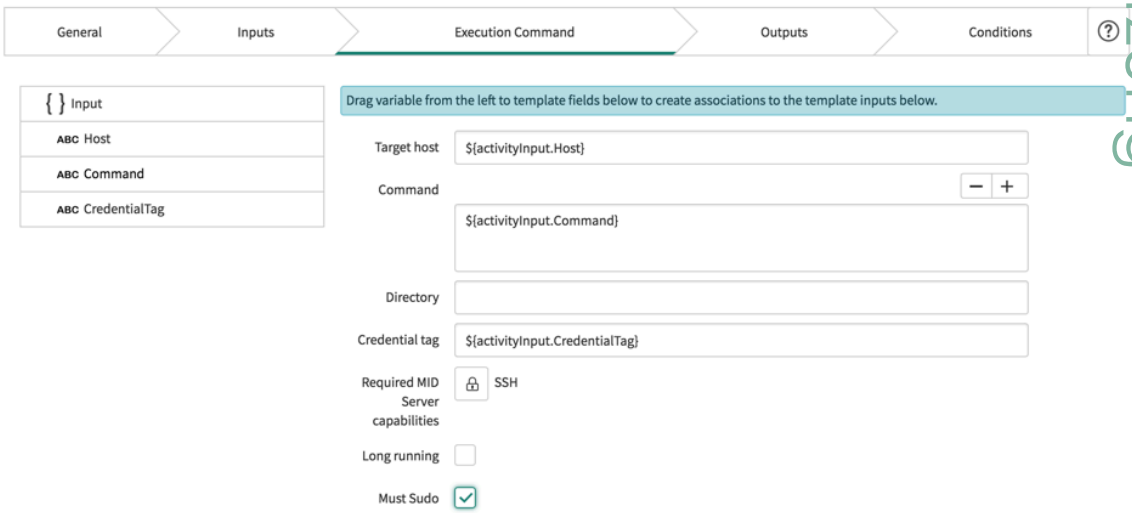
Eingabevariablen	Typ	Obligatorisch
Host	Zeichenfolge	Nein
Befehl	Zeichenfolge	Nein
CredentialTag	Zeichenfolge	Nein

6. Führen Sie auf der Registerkarte „Ausführungsbefehl“ Folgendes aus:

a. Klicken Sie auf die Eingabevariablen, und ziehen Sie sie von links in die Vorlagenfelder auf der rechten Seite.
Dieser Schritt erstellt die Ausdrücke, die verwendet werden.

b. Aktivieren Sie das Kontrollkästchen **Sudo erforderlich**, damit Sie sich später beim virtuellen Server anmelden können.

c. Klicken Sie auf **Fortsetzen**.



7. Fügen Sie auf der Registerkarte „Ausgaben“ die Ausgabevariablen mit den folgenden Schritten hinzu:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der Ausgabetabelle auf das **+ in einem Kreis**, um eine neue Ausgabevariable zu erstellen.

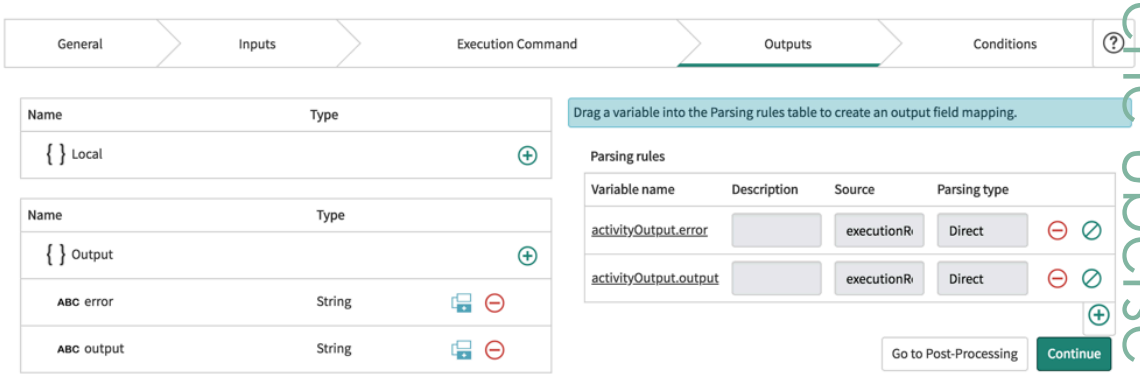
b. Klicken Sie rechts neben ABC in der Spalte **Name**, und geben Sie den Ausgabenamen ein.
Die Ausgabevariablen geben die möglichen Ergebnisse an, wenn der Workflow versucht, SSH-Verbindungen zur VM herzustellen. Die Spalte **Typ** wird automatisch ausgefüllt.

Ausgaben	Typ
Fehler	Zeichenfolge
Ausgabe	Zeichenfolge

c. Klicken Sie auf die **Fehlervariable**, und ziehen Sie sie in das Feld für den Variablennamen in der Tabelle mit Analyseregeln.

d. Wählen Sie im Dialogfeld der Analyseregel für Fehler in der Dropdown-Liste der Analysequellen die entsprechende Quelle aus. In diesem Fall „executionResult.errorMessages“.

e. Wiederholen Sie den Vorgang für die Ausgabevariable, wählen Sie „executionResult.output“ als Analysequelle aus, und klicken Sie auf **Absenden**.



f. Klicken Sie auf **Fortsetzen**.
Bedingungen sind optional.

g. Klicken Sie auf **Speichern** und dann auf **Veröffentlichen**, um die Aktivität für den Workflow verfügbar zu machen.

Nächste Maßnahme

Sie haben jetzt eine benutzerdefinierte Aktivität erstellt, die als Container vorhanden ist, bis Sie ihr die Eingabezuordnungen hinzufügen. Die Zuordnungen teilen der Aktivität mit, woher die benötigten Informationen stammen. Sie geben die Eingabezuordnungen während des Workflow-Erstellungsverfahrens ein. Siehe SSH-Workflow erstellen.

SSH-Workflow erstellen

Erstellen Sie den zum Herunterfahren der VM erforderlichen SSH-Workflow. Verwenden Sie die benutzerdefinierte SSH-Aktivität, die Sie bereits erstellt haben.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Sie müssen bereits eine benutzerdefinierte SSH-Aktivität erstellt haben.
- Erforderliche Rolle: workflow designer oder admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn Sie einen Workflow erstellen, ordnen Sie ihn einer Tabelle und einer Aktivität zu.

- Sie können den Workflow in einer Tabelle auf globaler Ebene oder in einer Tabelle auf Anwendungsebene erstellen. Verwenden Sie die globale Tabelle, um den Workflow für alle ServiceNow-Anwendungen verfügbar zu machen. Hier verwenden wir eine Tabelle für Cloud Provisioning and Governance, sodass dieser Workflow nur für die Verwendung mit dieser Anwendung verfügbar ist.
- Sie können den Workflow im Workflow-Editor oder im Activity Designer erstellen. Hier wird der Activity Designer verwendet.

Prozedur

1. Wählen Sie im Activity Designer rechts die Registerkarte **Workflows** aus, und klicken Sie dann auf das Pluszeichen (**+**), um einen neuen Workflow hinzuzufügen.
2. Führen Sie im Fenster „Neuer Workflow“ die folgenden Schritte aus:

   a. Geben Sie einen eindeutigen Namen für den Workflow ein.

   b. Wählen Sie aus dem Dropdown-Menü **Tabelle** die zu verwendende Tabelle aus. Suchen Sie nach der **VM-Instanz cmdb_ci_vm_instance,** und verwenden Sie sie, da der Workflow zum Ausschalten einer VM verwendet werden soll.

   c. Klicken Sie auf **Absenden**.

3. Wenn der Workflow im Canvas-Bereich angezeigt wird, führen Sie die folgenden Schritte aus:

   a. Löschen Sie die Verbindungslinie zwischen Start- und Endpunkt des Workflows.

   b. Klicken Sie mit der rechten Maustaste auf die Canvas mit weiteren Informationen, und wählen Sie **Eingaben bearbeiten** aus.

   c. Erstellen Sie die folgenden Eingaben:

   Hinweis: Übernehmen Sie die Eingabenamen aus dem Feld „Spalte“, nicht aus dem Feld „Bezeichnung“. Wenn der Workflow einer Tabelle auf globaler Ebene zugeordnet ist, wird dem Eingabenamen im Feld „Spalte“ das Präfix „u_“ vorangestellt, z. B. u_ipaddress. Hier befindet sich die Tabelle auf Anwendungsebene, daher ist kein Präfix erforderlich.

Workflow-Eingaben

Typ	Bezeichnung	Spalte (automatisch hinzugefügt)	Max. Länge
Zeichenfolge	IPAddress	ipaddress	100

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Bezeichnung	Spalte (automatisch hinzugefügt)	Max. Länge
Zeichenfolge	CredentialTag	credentialtag	100

d. Klicken Sie auf **Absenden**.

4. Klicken Sie mit der rechten Maustaste auf die Canvas, und wählen Sie **Benutzerdefinierte Aktivität hinzufügen** aus.
5. Suchen Sie im Fenster „Versionen“ nach der Aktivität, die Sie vorher unter Benutzerdefinierte SSH-Aktivität erstellen erstellt haben, und wählen Sie sie aus.
6. Führen Sie im Fenster „Neue Aktivität“ für diese Aktivität (Workflow-Aktivität „Neuer Datensatz“ [Diagrammansicht]) die folgenden Schritte aus:

   a. Geben Sie einen Namen für die Aktivität ein.

   b. Geben Sie im Feld **Host** die von der Aktivität erwartete Eingabezuordnung ein.

   Das heißt, die IP-Adresse des Hosts: *`${workflow.inputs.u_ipaddress}`*.

   Diesen Ausdruck für die IP-Adresse verwenden:

   $(Script:CMPVMUtils.getReachableIp[arg=$(Stack.items[Virtual Server].attributes[sys_id])])

   c. Geben Sie im Feld „Befehl“ *`shutdown -h now`* ein.

   d. Geben Sie im Feld „Anmeldeinformations-Tag“ *`${workflow.inputs.u_credentialtag}`* ein.

   Verwenden Sie diesen Ausdruck, um das Anmeldeinformations-Tag abzurufen:

   $(Script:CMPVMUtils.getCredentialAlias[arg=${Stack.items[Virtual Server].attributes[sys_id]}])

   e. Klicken Sie auf **Absenden**.
   Die Aktivität wird in der Workflow-Canvas angezeigt.

7. Klicken Sie mit der rechten Maustaste auf die Canvas, und wählen Sie **Kernaktivität hinzufügen** aus, um eine Ausführungsskript-Aktivität hinzuzufügen.
8. Suchen Sie im Fenster „Workflow-Aktivitätsdefinitionen“ nach **Skript ausführen** und wählen Sie die Option aus.
9. Führen Sie im Fenster „Neue Aktivität: Skript ausführen“ die folgenden Schritte aus:

   a. Geben Sie einen Namen für die Aktivität ein.

   b. Schneiden Sie ein (für Ihre Umgebung geeignetes) **Skript** aus, und fügen Sie es im Feld „Skript“ ein.

   Dieses Skript aktualisiert den Status der VM nach dem Herunterfahren.

   Beispielskript:

```
if ( gs.nil(data.get(3).error)) {
                    current.state = 'off';
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                    current.setWorkflow(false);
                    current.update();
}
```

c. Klicken Sie auf **Absenden**.

10. Verbinden Sie im Canvas-Bereich die Connectors zwischen dem Anfangspunkt, der Aktivität, dem Ausführungsskript und dem Endpunkt.
11. Klicken Sie auf **Veröffentlichen**, um den Workflow verfügbar zu machen.
12. Validieren Sie den Workflow mithilfe der Workflow-Validierung.

Hinweis: Das System empfiehlt nicht die Verwendung von current.update(). Dies kann ignoriert werden.

Antwortaktion für Cloud Provisioning and Governance erstellen

Erstellen Sie einen Subflow mit den erforderlichen Eingabeparametern, der Cloud Provisioning and Governance benachrichtigt, ob der Flow erfolgreich abgeschlossen wurde oder nicht.

Vorbereitungen

- Stellen Sie sicher, dass Sie mit den Konzepten von , Subflows und Aktionsdesigner vertraut sind.
- Erstellen Sie einen Subflow, den Sie für die Vor- oder Nachbereitstellung aufrufen möchten.

Erforderliche Rolle: flow_designer, action_designer oder admin

Warum und wann dieser Vorgang ausgeführt wird

Informieren Sie die Cloud Provisioning and Governance-Anwendung über den Ausführungsstatus von Schritten im Subflow, indem Sie für jeden Schritt eine Antwort ausfüllen.

- Erstellen Sie eine Aktion mit relevanten Eingabeparametern.
- Fügen Sie der Aktion ein Skript hinzu.
- Übergeben Sie eine Korrelations-ID an die Aktion im Subflow.

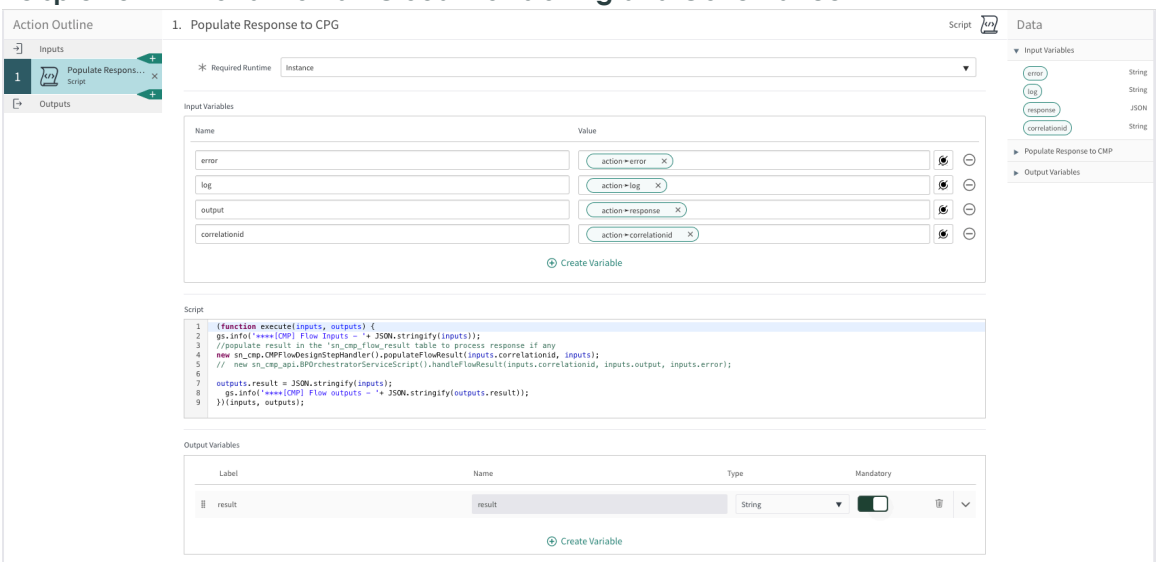
Die Antwortaktion teilt der Cloud Provisioning and Governance-Anwendung mit, ob ein Schritt im Subflow erfolgreich ausgeführt wird oder ob die Bedingung des Schritts fehlschlägt und zu einem Fehler führt.

Prozedur

1. Navigieren zu **Alle** > **Flow Designer** > **Aktionen** Wählen Sie auf der Registerkarte **Neue Aktion**aus.
   Weitere Informationen finden Sie unter Aktionen erstellen .
2. Füllen Sie die Aktionseigenschaften aus.
3. Definieren Sie Aktionseingaben und erstellen Sie sie, um Daten für die Aktionsschritte und Ausgaben verfügbar zu machen.
   Erstellen Sie die folgenden Eingabevariablen: Fehler, Protokoll, Ausgabe und Korrelations-ID.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Antwortaktion an Cloud Provisioning and Governance



4. Wählen Sie einen Skriptaktionsschritt aus, um einen Vorgang für die Aktionseingaben durchzuführen.
5. **Speichern** und **Veröffentlichen** Sie die Aktion.
6. Öffnen Sie im **Flow Designer** den Subflow, den Sie aufrufen.

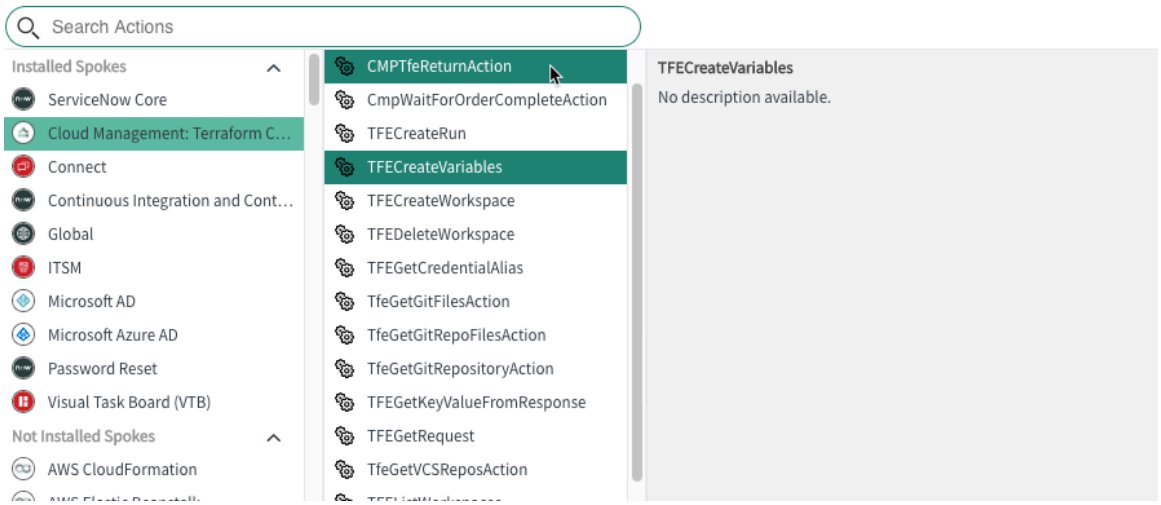
   Hinweis: Stellen Sie sicher, dass die Subflow-Eingabe `flowcorrelationid` im Subflow vorhanden ist.

7. Klicken Sie auf derselben Subflow-Seite auf **Aktionen**, um zu erweitern und **Aktionen**, **Subflow** oder **Flow-Logik**zu suchen.
8. Wählen Sie Cloud Provisioning and Governance aus, suchen Sie die Antwortaktion und fügen Sie sie aus der Dropdown-Liste hinzu.
9. Wählen Sie für die Eingaben in der Aktion relevante Werte aus der **Datenpillenauswahl** aus.

   Hinweis: Verwenden Sie die Eingabe `flowcorrelationid` aus dem **Datenbereich** für jede Aktion im Subflow, die einen logischen Endschritt aufweist, wieder.

10. Wahlweise: Wenn Sie den Terraform Connector für Terraform Enterprise verwenden, führen Sie diese Schritte aus.
    a. Zum Hinzufügen von Aktionen, Flows, Subflows oder Flow-Logik klicken Sie auf **Zum Hinzufügen einer Aktion, einer Flow-Logik oder eines Subflow auswählen**.
    b. Auswahlvorgang **Aktion** > **Cloud-Management: Terraform-Connector**, und wählen Sie eine Standardaktion aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Die von Ihnen erstellte Aktion sendet eine Antwort an die Cloud Provisioning and Governance-Anwendung und aktualisiert die Reihenfolge mit dem Status des Schritts des Subflows.

Nächste Maßnahme

Testen Sie den Subflow und veröffentlichen Sie ihn, wenn er zum Hinzufügen zu einem Flow oder zum Aufrufen aus einem Skript bereit ist.

Hinweis: Sie können nur Subflows testen oder veröffentlichen, die mindestens eine Aktion enthalten.

Cloud-Katalogelement erstellen

Erstellen Sie, basierend auf einer Vorlage oder einer vorhandenen Blaupause, ein Cloud-Katalogelement für die Bereitstellung und veröffentlichen Sie das Katalogelement, um einen Service bereitzustellen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Beim Erstellen eines Katalogelements können Sie das Katalogelement mit einer Vorlage verknüpfen, die entweder nativ für den Cloud-Anbieter ist (z. B. CFT, ARM, GDM) oder bei der es sich um eine Terraform-IaC-Vorlage handelt. Nachdem Sie ein Katalogelement generiert haben, generiert das System automatisch Komponenten wie Variablensätze, Lebenszyklusvorgänge, Regeln sowie Vor- und Nachbereitstellungsvorgänge. Sie können alle diese Komponenten auf der Seite „Katalogelement erstellen“ verwalten.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Cloud-Katalogelemente**.
   Alle von Ihnen erstellten Katalogelemente werden in einer Kartenlayoutansicht aufgelistet. Sie können auf ein inaktives Katalogelement klicken, um es bereitzustellen.
2. Klicken Sie auf **Neu**.
   Der Bildschirm „Cloud-Katalogelemente“ wird angezeigt.
3. Füllen Sie die Felder des Formulars aus.

Formular „Cloud-Katalogelement“

Feld	Beschreibung
Name	Name des Katalogelements.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Aktiv	Option zur Bereitstellung des Katalogelements. Dieses Kontrollkästchen kann erst aktiviert werden, nachdem Sie eine Blaupause ausgewählt haben.
Symbol	Das Bild wird neben dem Artikelnamen im Katalog als Symbol angezeigt. Sie können Sie ein 16x16-Pixel-Bild hochladen. Wenn kein Bild hochgeladen wird, wird neben diesem Element das Standardsymbol angezeigt. Das hochgeladene Bild überschreibt das Standardbild. Das von Ihnen hochgeladene Bild wird im Servicekatalog angezeigt, nicht in der ServiceNow® Cloud Provisioning and Governance-Anwendung.
Bild	Bild für das Katalogelement. Das von Ihnen ausgewählte Bild wird im Cloudbenutzerportal für das Katalogelement angezeigt (nachdem Sie auf **Einen Stapel starten** geklickt haben).
Kataloge	Namen der Kataloge.
Kategorie	Die Kategorie für das Element wird standardmäßig angezeigt. Sie können die Kategorie ändern. Katalogsuchen finden nur Elemente, die einer Kategorie zugewiesen sind. Die Kategorien werden im Servicekatalog angezeigt. Das Katalogelement kann in mehreren Kategorien angezeigt werden. Zum Hinzufügen von Kategorien klicken Sie auf die Registerkarte **Kategorien**, und dann auf **Neu** oder **Bearbeiten**.
Quelle	Quelltyp (Cloud-Vorlage oder Benutzerdefiniert), mit dem das Katalogelement verknüpft werden soll.
Vorlagentyp	◦ Wählen Sie **Cloud-Vorlage** aus, und wählen Sie dann den Vorlagentyp (**ARM-Vorlage** oder **CloudFormation-Vorlage** zum Importieren Cloud-nativer Vorlagen) aus. ◦ Wählen Sie **Konfigurationsverwaltungsvorlage** aus, um die Vorlagen der Konfigurationsverwaltungs-Provider Ansible oder Terraform zu verwenden.
Blaupause	Wenn Sie im Feld **Quelle** die Option **Benutzerdefiniert** ausgewählt haben, wählen Sie eine Blaupause aus, die dem Katalogelement zugeordnet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Planvorgang	Nachdem Sie das Katalogelement generiert haben, wird der Wert in diesem Feld automatisch eingetragen. Dieses Feld wird nur angezeigt, wenn Sie eine Blaupause auswählen.
Kurzbeschreibung	Kurzbeschreibung des Katalogelements. Diese Beschreibung wird im Cloudbenutzerportal neben dem Katalogelement angezeigt.
Beschreibung	Vollständige Beschreibung des Katalogelements. Diese Beschreibung wird im Servicekatalog angezeigt, nicht in der Cloud Provisioning and Governance-Anwendung. Sie können Videos, Bilder, Links zu Artikeln der internen Knowledge Base (KB) und Links zu externen Informationsquellen und Anleitungen einbetten.

4. Klicken Sie auf **Absenden**.
   Das Katalogelement und alle zugehörigen Komponenten wie Variablensätze, Lebenszyklusvorgänge und Regeln werden generiert und als Registerkarten auf der Seite „Cloud-Katalogelement“ angezeigt.

   Hinweis: Wenn Sie **Vorlage** aus der Liste „Quelltyp“ ausgewählt haben, müssen Sie eine Vorlage erstellen und die Vorlage dem Katalogelement zuordnen.

   Die zugehörigen Links sind Aktionen, die Sie für das Katalogelement ausführen können.

Aktion	Beschreibung
Katalogelement exportieren	Exportiert alle Komponenten (z. B. Blaupausen, Ressourcenblöcke, Regeln) des Katalogelements aus einer Umgebung in die andere. Weitere Informationen finden Sie unter Verschieben von Cloud Provisioning and Governance-Inhalten zwischen Umgebungen.
Elementdiagnose	Identifiziert mögliche Probleme mit den Katalogelementdaten und der Konfiguration. Siehe Elementdiagnosebericht
Attribute verwalten	Weitere Informationen finden Sie unter Vorgangsattribute verwalten.
Katalogelement zurücksetzen	Setzt alle Anpassungen zurück, die Sie am Katalogelement vorgenommen haben (bis zur letzten von Ihnen vorgenommenen Änderung).

Nächste Maßnahme

Auf Cloud-Vorlage basierendes Katalogelement erstellenan.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zugehörige Informationen

Katalogelement aus einer Terraform-Vorlage erstellen

Katalogelement aus einer GCP-Vorlage erstellen

Veröffentlichen Sie einen Blueprint als Cloud-Katalogelement

Sie können ein Katalogelement direkt aus einer Blaupause erstellen und veröffentlichen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

- Beginnend mit Orlando sind Cloud Provisioning-Blaupausen für Instanzen verfügbar, die von einem früheren Release aktualisiert wurden. Sie können jedoch keine neuen Blaupausen erstellen. Vorhandene Blaupausen und Katalogelemente aus diesen Blaupausen bleiben davon unberührt und funktionieren weiterhin.
- Verwenden Sie Cloud-Vorlagen für Cloud Provisioning, um Katalogelemente anstelle von Blaupausen zu erstellen. Mithilfe von Cloud Provisioning Cloud-Vorlagen können Sie die Spezifikationssyntax für Azure ARM, AWS CFT, Google Deployment Manager (GDM) und Terraform in Cloud-Katalogelemente zur Ausführung Ihrer Cloud-Bereitstellungsorchestrierung einbinden.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Blueprints**.
2. Öffnen Sie eine Blaupause (im Entwurfsmodus), klicken Sie auf die Registerkarte **Katalog**, und klicken Sie dann auf **Katalogelement erstellen**.
   Das Dialogfeld „Blaupausenkatalog erstellen“ wird angezeigt.
3. Geben Sie einen Namen für das Katalogelement in das Feld **Name** ein, und klicken Sie auf **Speichern**.
   Das Katalogelement wird generiert und auf der Registerkarte **Katalog** angezeigt.
4. Klicken Sie auf das Katalogelement, um Aktualisierungen am Katalogelement vorzunehmen.
   Der Bildschirm „Cloud-Katalogelement“ wird angezeigt.
5. Klicken Sie auf **Aktualisieren**, um die Änderungen zu speichern.

Auf Cloud-Vorlage basierendes Katalogelement erstellen

Erstellen Sie eine Cloud-Vorlage, und ordnen Sie die Vorlage einem Katalogelement zu. Sobald Sie eine Vorlage erstellt haben, können Sie die Vorlage erneut verwenden, um zusätzliche Katalogelemente für die Services zu erstellen, die Sie bereitstellen möchten.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Vorlage erstellen, indem Sie eine generische Vorlagendatei hochladen, eine Vorlage von einer öffentlichen URL importieren oder den Inhalt einer vorhandenen Vorlage kopieren und einfügen. AWS CloudFormation-Vorlagen (CFT) bieten Unterstützung für JSON und YAML. Azure Resource Manager-Vorlagen (ARM) bieten Unterstützung für JSON. Die folgenden Inhaltstypen für URLs öffentlicher Vorlagen werden unterstützt:

- Text/Plain
- Application/JSON
- YAML MIME

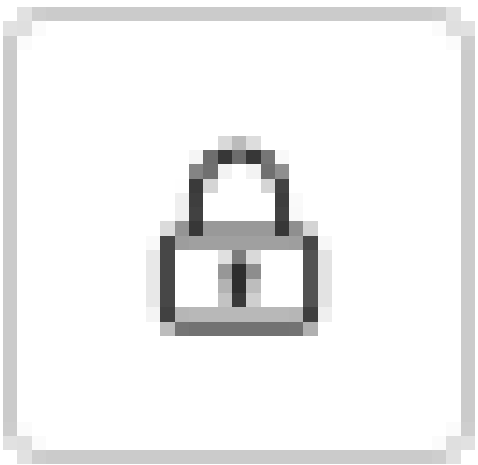
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Katalogelemente, die auf Vorlagen in früheren Releases basierten, werden nun so behandelt, als ob sie auf Blaupausen basieren.

Sie können eine Vorlage beliebig oft aktualisieren. Mit jeder Aktualisierung wird eine neue Version der Vorlage erstellt. Eine Vorlage kann einen von drei Status haben: **Entwurf**, **Aktiv** oder **Verlauf**. Wenn Sie eine Vorlage erstellen und nicht aktivieren, befindet sich die Vorlage im Entwurfsstatus. Sobald Sie die Vorlage aktiviert haben, ändert sich der Status in „Aktiv“. Wenn Sie eine andere Vorlage erstellen und diese aktivieren, wird der Status der vorherigen aktiven Vorlage in „Verlauf“ geändert. Zu jeder Zeit ist nur eine Vorlage im Status „Aktiv“. Jedes Mal, wenn Sie eine Vorlage aktivieren, wird die vorherige aktive Vorlage dem Verlauf zugeordnet.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Cloud-Katalogelemente** und erstellen dann ein Katalogelement, oder öffnen Sie ein vorhandenes Katalogelement.
2. Klicken **Cloud-Vorlagen** > **Neu** und geben Sie dann im Feld **Kurzbeschreibung** eine aussagekräftige Kurzbeschreibung ein.
3. Geben Sie die **Erfassungsmethode** an.

Option	Bezeichnung
Import aus URL	Importieren Sie eine Vorlage, indem Sie eine öffentliche URL angeben, unter der sich die Vorlage befindet. Wählen Sie diese Option aus, und klicken Sie dann auf das Sperrsymbol (), um das Feld **Cloud-Vorlagen-URL** zu entsperren. Geben Sie die öffentliche URL in dieses Feld ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Bezeichnung
	Hinweis: Für die öffentliche URL werden nur die Protokolle HTTP und HTTPS unterstützt. FTP wird nicht unterstützt. Stellen Sie sicher, dass die Größe der Vorlage den Standardwert von 3 MB nicht überschreitet. Sie können den Standardwert der Dateigröße ändern, indem Sie den Wert in der Eigenschaft *sn_cmp.template_content_size_supported_inbyte* in der Tabelle „sys_properties“ ändern. Geben Sie die Dateigröße in Byte ein. Es gibt auch eine Standardzeitüberschreitung von 5 Minuten für eine HTTP-Anforderung. Sie können den Wert für die Zeitüberschreitung in der Eigenschaft *sn_cmp.template_url_import_http_timeout* in der Tabelle „sys_properties“ ändern. Geben Sie den neuen Wert in Millisekunden ein.
Eine Datei hochladen	Laden Sie eine Vorlage von Ihrer lokalen Workstation hoch.
Vorlagen-Textkörper verwenden	Fügen Sie den Inhalt der Vorlagendatei in das Feld **Text** ein.

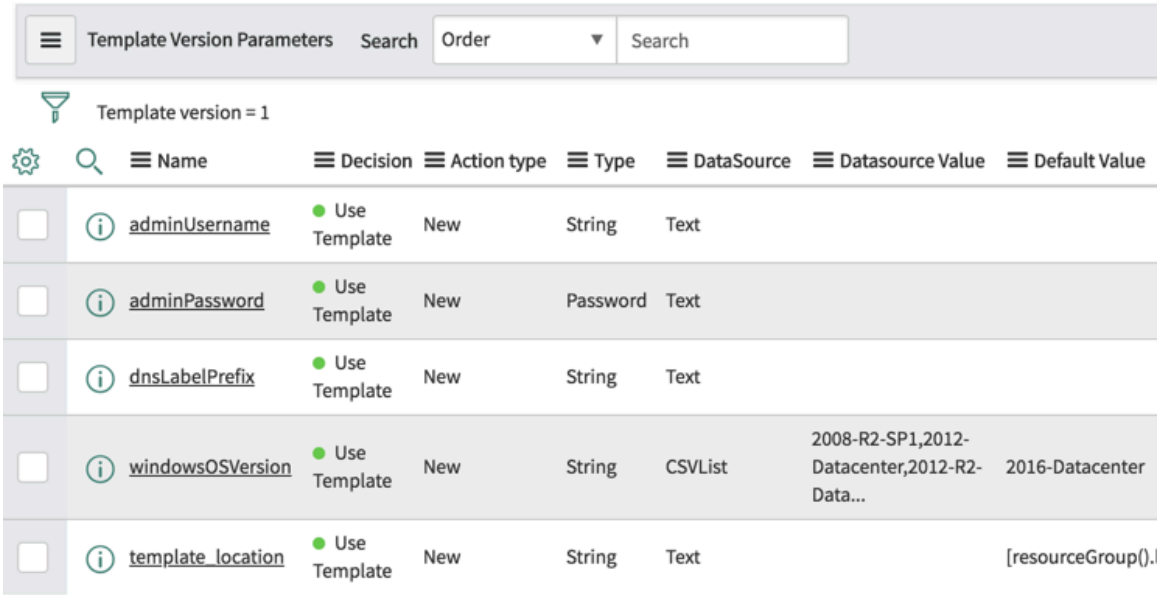
Nachdem Sie die **Erfassungsmethode** angegeben haben, wird die Vorlage validiert, und die Ergebnisse werden in den Feldern **Validierungsstatus** und **Validierungsnachricht** angezeigt.

4. Klicken Sie auf **Absenden**.
   Die Vorlage wird erstellt, und die Seite „Cloud-Katalogelement“ wird geöffnet.
5. Wenn dies die erste Version der Vorlage ist, überspringen Sie diesen Schritt. Andernfalls öffnen Sie auf der Registerkarte **„Cloud-Vorlagen“** die Vorlage (derzeit im Status Entwurf), um die Parameter der Vorlagenversion anzuzeigen.

Hinweis: Die erste Version einer Vorlage, die Sie erstellen und veröffentlichen, weist keine Konfliktprobleme auf. Wenn Sie die Vorlage aktualisieren, kann ein Konflikt auftreten. Wenn ein Parameter **Aktionstyp** den Wert **Aktualisieren** hat, dann geben Sie einen Wert für **Entscheidung** an.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Öffnen Sie jeden Parameter, der für **Entscheidung** einen Wert von **Ausstehend** hat, wählen Sie einen Wert aus, und klicken Sie dann auf das Häkchen .

Option	Bezeichnung
Aktualisierung überspringen	Die Aktualisierungen der Vorlage werden verworfen.
Vorlage verwenden	Die Aktualisierungen der Vorlage werden angewendet.

7. Nachdem Sie alle **ausstehenden** Entscheidungen aktualisiert haben, klicken Sie auf **Aktivieren**.
Der Status der Vorlage ändert sich von **Entwurf** in **Aktiv**, und das System generiert das Katalogelement.

CloudFormation-JSON-Codebeispiel zum Erstellen einer AWS EC2-Instanz

Referenz-Codebeispiel zum Bereitstellen einer Amazon AWS Cloud EC2-Instanz

AWS EC2-Instanzen mit CloudFormation bereitstellen

- Überprüfen Sie beim Entwerfen eines Katalogelements die CloudFormation-Vorlage, um die Services zu identifizieren, die bereitgestellt werden. Vergewissern Sie sich, dass entsprechende Berechtigungen für die Services gewährt werden können, damit keine Fehler aufgrund fehlender Berechtigungen auftreten, wenn der Stapel bestellt wird. Weitere Informationen finden Sie unter Berechtigungen für die AWS-Konsole konfigurieren
- Nehmen Sie die erforderlichen Änderungen vor, indem Sie dieses Codebeispiel als Referenz verwenden.

```
{
   "AWSTemplateFormatVersion":"2010-09-09",
   "Description":"AWS CloudFormation Sample Template
 EC2InstanceWithSecurityGroupSample: Create an Amazon EC2 instance
 running the Amazon Linux AMI. The AMI is chosen based on the region in
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
which the stack is run. This example creates an EC2 security group for
the instance to give you SSH access. **WARNING** This template creates
an Amazon EC2 instance. You will be billed for the AWS resources used if
you create a stack from this template.",
  "Parameters":{
     "KeyName":{
        "Description":"Name of an existing EC2 KeyPair to enable SSH
access to the instance",
        "Type":"AWS::EC2::KeyPair::KeyName",
        "Default":"admin-Default",
        "ConstraintDescription":"must be the name of an existing EC2
KeyPair."
     },
     "InstanceType":{
        "Description":"WebServer EC2 instance type",
        "Type":"String",
        "Default":"t2.micro",
        "AllowedValues":[
           "t1.micro",
           "t2.nano",
           "t2.micro",
           "t2.small",
           "t2.medium",
           "t2.large",
           "m1.small",
           "m1.medium",
           "m1.large",
           "m1.xlarge",
           "m2.xlarge",
           "m2.2xlarge",
           "m2.4xlarge",
           "m3.medium",
           "m3.large",
           "m3.xlarge",
           "m3.2xlarge",
           "m4.large",
           "m4.xlarge",
           "m4.2xlarge",
           "m4.4xlarge",
           "m4.10xlarge",
           "c1.medium",
           "c1.xlarge",
           "c3.large",
           "c3.xlarge",
           "c3.2xlarge",
           "c3.4xlarge",
           "c3.8xlarge",
           "c4.large",
           "c4.xlarge",
           "c4.2xlarge",
           "c4.4xlarge",
           "c4.8xlarge",
           "g2.2xlarge",
           "g2.8xlarge",
           "r3.large",
           "r3.xlarge",
           "r3.2xlarge",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "r3.4xlarge",
            "r3.8xlarge",
            "i2.xlarge",
            "i2.2xlarge",
            "i2.4xlarge",
            "i2.8xlarge",
            "d2.xlarge",
            "d2.2xlarge",
            "d2.4xlarge",
            "d2.8xlarge",
            "hi1.4xlarge",
            "hs1.8xlarge",
            "cr1.8xlarge",
            "cc2.8xlarge",
            "cg1.4xlarge"
         ],
         "ConstraintDescription":"must be a valid EC2 instance type."
      },
      "SSHLocation":{
         "Description":"The IP address range that can be used to SSH to
 the EC2 instances",
         "Type":"String",
         "MinLength":"9",
         "MaxLength":"18",
         "Default":"0.0.0.0/0",

 "AllowedPattern":"(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})/(\
\d{1,2})",
         "ConstraintDescription":"must be a valid IP CIDR range of the
 form x.x.x.x/x."
      },
      "Network":{
         "Description":"The Network to the EC2 instances",
         "Type":"String"
      },
      "AvailabilityZone":{
         "Description":"The AZ of the EC2 instance",
         "Type":"String"
      },
      "SubnetPool":{
         "Description":"The IP address range that can be used to SSH to
 the EC2 instances",
         "Type":"String"
      }
   },
   "Metadata":{
      "SNC::Parameter::Metadata":{
         "SubnetPool":{

 "datasource":"ServiceNow::Pools::SubnetPool.getObjectsByNetwork",
            "datasourceFilter":{
               "Network":"Network"
            }
         },
         "Network":{
            "datasource":"ServiceNow::Pools::NetworkPool.getObjectsByLDC"
         },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        "KeyName":{

"datasource":"ServiceNow::Pools::CloudKeyPairPool.getObjectsByLDC"
        }
     }
  },
  "Mappings":{
     "AWSInstanceType2Arch":{
        "t1.micro":{
           "Arch":"PV64"
        },
        "t2.nano":{
           "Arch":"HVM64"
        },
        "t2.micro":{
           "Arch":"HVM64"
        },
        "t2.small":{
           "Arch":"HVM64"
        },
        "t2.medium":{
           "Arch":"HVM64"
        },
        "t2.large":{
           "Arch":"HVM64"
        },
        "m1.small":{
           "Arch":"PV64"
        },
        "m1.medium":{
           "Arch":"PV64"
        },
        "m1.large":{
           "Arch":"PV64"
        },
        "m1.xlarge":{
           "Arch":"PV64"
        },
        "m2.xlarge":{
           "Arch":"PV64"
        },
        "m2.2xlarge":{
           "Arch":"PV64"
        },
        "m2.4xlarge":{
           "Arch":"PV64"
        },
        "m3.medium":{
           "Arch":"HVM64"
        },
        "m3.large":{
           "Arch":"HVM64"
        },
        "m3.xlarge":{
           "Arch":"HVM64"
        },
        "m3.2xlarge":{
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "Arch":"HVM64"
         },
         "m4.large":{
            "Arch":"HVM64"
         },
         "m4.xlarge":{
            "Arch":"HVM64"
         },
         "m4.2xlarge":{
            "Arch":"HVM64"
         },
         "m4.4xlarge":{
            "Arch":"HVM64"
         },
         "m4.10xlarge":{
            "Arch":"HVM64"
         },
         "c1.medium":{
            "Arch":"PV64"
         },
         "c1.xlarge":{
            "Arch":"PV64"
         },
         "c3.large":{
            "Arch":"HVM64"
         },
         "c3.xlarge":{
            "Arch":"HVM64"
         },
         "c3.2xlarge":{
            "Arch":"HVM64"
         },
         "c3.4xlarge":{
            "Arch":"HVM64"
         },
         "c3.8xlarge":{
            "Arch":"HVM64"
         },
         "c4.large":{
            "Arch":"HVM64"
         },
         "c4.xlarge":{
            "Arch":"HVM64"
         },
         "c4.2xlarge":{
            "Arch":"HVM64"
         },
         "c4.4xlarge":{
            "Arch":"HVM64"
         },
         "c4.8xlarge":{
            "Arch":"HVM64"
         },
         "g2.2xlarge":{
            "Arch":"HVMG2"
         },
         "g2.8xlarge":{
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "Arch":"HVMG2"
         },
         "r3.large":{
            "Arch":"HVM64"
         },
         "r3.xlarge":{
            "Arch":"HVM64"
         },
         "r3.2xlarge":{
            "Arch":"HVM64"
         },
         "r3.4xlarge":{
            "Arch":"HVM64"
         },
         "r3.8xlarge":{
            "Arch":"HVM64"
         },
         "i2.xlarge":{
            "Arch":"HVM64"
         },
         "i2.2xlarge":{
            "Arch":"HVM64"
         },
         "i2.4xlarge":{
            "Arch":"HVM64"
         },
         "i2.8xlarge":{
            "Arch":"HVM64"
         },
         "d2.xlarge":{
            "Arch":"HVM64"
         },
         "d2.2xlarge":{
            "Arch":"HVM64"
         },
         "d2.4xlarge":{
            "Arch":"HVM64"
         },
         "d2.8xlarge":{
            "Arch":"HVM64"
         },
         "hi1.4xlarge":{
            "Arch":"HVM64"
         },
         "hs1.8xlarge":{
            "Arch":"HVM64"
         },
         "cr1.8xlarge":{
            "Arch":"HVM64"
         },
         "cc2.8xlarge":{
            "Arch":"HVM64"
         }
      },
      "AWSRegionArch2AMI":{
         "us-east-1":{
            "PV64":"ami-2a69aa47",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "HVM64":"ami-6869aa05",
            "HVMG2":"ami-a41a3fb3"
         },
         "us-west-2":{
            "PV64":"ami-7f77b31f",
            "HVM64":"ami-7172b611",
            "HVMG2":"ami-caf253aa"
         },
         "us-west-1":{
            "PV64":"ami-a2490dc2",
            "HVM64":"ami-31490d51",
            "HVMG2":"ami-00347e60"
         },
         "eu-west-1":{
            "PV64":"ami-4cdd453f",
            "HVM64":"ami-f9dd458a",
            "HVMG2":"ami-e2f7bd91"
         },
         "eu-central-1":{
            "PV64":"ami-6527cf0a",
            "HVM64":"ami-ea26ce85",
            "HVMG2":"ami-d2ff04bd"
         },
         "ap-northeast-1":{
            "PV64":"ami-3e42b65f",
            "HVM64":"ami-374db956",
            "HVMG2":"ami-4c78d52d"
         },
         "ap-northeast-2":{
            "PV64":"NOT_SUPPORTED",
            "HVM64":"ami-2b408b45",
            "HVMG2":"NOT_SUPPORTED"
         },
         "ap-southeast-1":{
            "PV64":"ami-df9e4cbc",
            "HVM64":"ami-a59b49c6",
            "HVMG2":"ami-f3f95990"
         },
         "ap-southeast-2":{
            "PV64":"ami-63351d00",
            "HVM64":"ami-dc361ebf",
            "HVMG2":"ami-3a122e59"
         },
         "ap-south-1":{
            "PV64":"NOT_SUPPORTED",
            "HVM64":"ami-ffbdd790",
            "HVMG2":"ami-21a7d34e"
         },
         "us-east-2":{
            "PV64":"NOT_SUPPORTED",
            "HVM64":"ami-f6035893",
            "HVMG2":"NOT_SUPPORTED"
         },
         "sa-east-1":{
            "PV64":"ami-1ad34676",
            "HVM64":"ami-6dd04501",
            "HVMG2":"NOT_SUPPORTED"
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        },
        "cn-north-1":{
           "PV64":"ami-77559f1a",
           "HVM64":"ami-8e6aa0e3",
           "HVMG2":"NOT_SUPPORTED"
        }
     }
  },
  "Resources":{
     "EC2Instance":{
        "Type":"AWS::EC2::Instance",
        "Properties":{
           "InstanceType":{
              "Ref":"InstanceType"
           },
           "KeyName":{
              "Ref":"KeyName"
           },
           "SubnetId":{
              "Ref":"SubnetPool"
           },
           "ImageId":{
              "Fn::FindInMap":[
                 "AWSRegionArch2AMI",
                 {
                    "Ref":"AWS::Region"
                 },
                 {
                    "Fn::FindInMap":[
                       "AWSInstanceType2Arch",
                       {
                          "Ref":"InstanceType"
                       },
                       "Arch"
                    ]
                 }
              ]
           }
        }
     },
     "InstanceSecurityGroup":{
        "Type":"AWS::EC2::SecurityGroup",
        "Properties":{
           "GroupDescription":"Enable SSH access via port 22",
           "SecurityGroupIngress":[
              {
                 "IpProtocol":"tcp",
                 "FromPort":"22",
                 "ToPort":"22",
                 "CidrIp":{
                    "Ref":"SSHLocation"
                 }
              }
           ]
        }
     }
  },
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
   "Outputs":{
      "InstanceId":{
         "Description":"InstanceId of the newly created EC2 instance",
         "Value":{
            "Ref":"EC2Instance"
         }
      },
      "AZ":{
         "Description":"Availability Zone of the newly created EC2
 instance",
         "Value":{
            "Fn::GetAtt":[
               "EC2Instance",
               "AvailabilityZone"
            ]
         }
      }
   }
}
```

Vorbereitstellungsvorgänge erstellen

Vorgänge vor der Bereitstellung optimieren die Bereitstellung von Katalogelementen durch die Automatisierung von Aufgaben wie Benachrichtigungen, Workflows oder Skripts vor der Bereitstellung. Durch die Konfiguration dieser Vorgänge werden manuelle Schritte vermieden, was Zeit und Aufwand spart, da das System automatisch bestimmte Aktionen ausführt, wenn eine Bereitstellungsanforderung übermittelt wird, z. B. die Benachrichtigung von Anwendern über die bevorstehende Elementbereitstellung.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Sie können Vorbereitstellungsaufgaben nur für Katalogelemente erstellen, die auf Vorlagen basieren.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Cloud-Katalogelemente**.
2. Öffnen Sie ein Katalogelement, klicken Sie auf die Registerkarte **Pre Provisioning Operation** (Vorbereitstellungsvorgang), klicken Sie auf **Neu**, und füllen Sie das Formular aus.

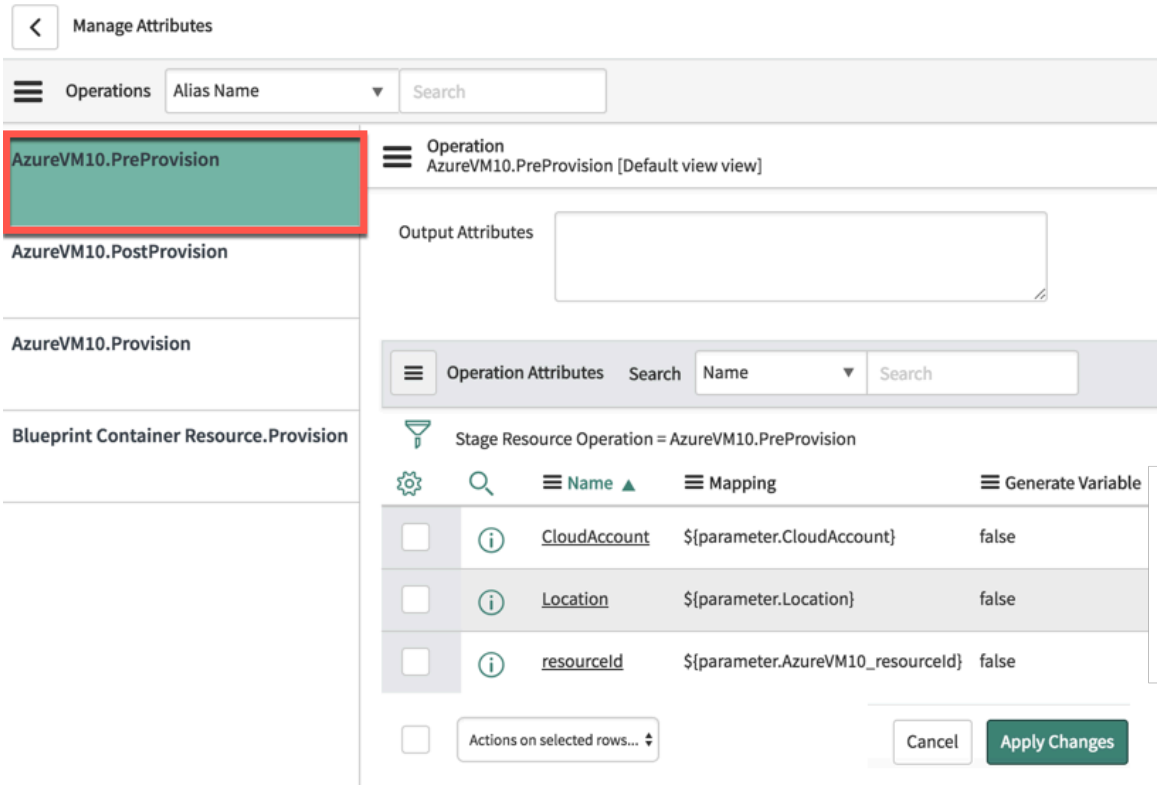
Feld	Beschreibung
Schritttyp	Vorbereitstellungsvorgänge. Abhängig vom Typ des ausgewählten Vorbereitstellungsvorgangs werden zusätzliche Felder angezeigt. ◦ CAPI: ▪ CAPI-Provider ▪ CAPI-Methode ▪ CAPI-Version ◦ InstanceScript:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Skript: Geben Sie den Namen des Skripts ein. ◦ Ressource: ▪ Ressourcenschnittstelle ▪ Schnittstellenvorgang ◦ Workflow Flow: Wählen Sie einen Workflow aus. Alle in der Instanz erstellten Workflows werden aufgelistet. ◦ Flow: Wählen Sie einen Subflow aus. Alle aktiven Subflows in der Instanz werden aufgelistet. **Hinweis:** Weitere Informationen finden Sie unter Subflows .
Auftrag	Reihenfolge der Vorbereitstellungsvorgänge. Geben Sie die Reihenfolge ein, in der der Vorbereitstellungsvorgang aufgerufen werden soll. Niedrigere Zahlen werden zuerst aufgerufen. Wenn Sie beispielsweise 2 für CAPI und 3 für InstanceScript eingeben, wird zuerst CAPI und dann das InstanceScript aufgerufen. Wenn Sie keinen Wert in dieses Feld eingeben, gibt das System automatisch einen Wert in Schritten von 20 ein.
Aktiviert	Option zum Aktivieren des Vorbereitstellungsvorgangs, der aufgerufen werden soll.

3. Klicken Sie auf **Absenden**.
   Parameter für Vorbereitstellungsvorgänge werden als Vorgangsattribute auf der Seite „Attribute verwalten“ erstellt.
4. Klicken Sie zum Hinzufügen von Werten für die Attribute des Vorbereitstellungsvorgangs auf **Attribute verwalten**.
   Der Bildschirm „Attribute verwalten“ wird angezeigt.
5. Klicken Sie auf **PreProvision**.
   Alle Attribute für den Vorbereitstellungsvorgang werden aufgelistet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Erstellen Sie entweder Ausdruckszuordnungen für ein Attribut (im Feld **„Zuordnung“**), oder generieren Sie Variablen für ein Attribut.
   Weitere Informationen finden Sie unter Vorgangsattribute verwalten.
7. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.
   Alle Konfigurationen, die Sie an den Attributen vorgenommen haben, werden gespeichert, und Sie kehren zum Bildschirm „Cloud-Katalogelemente“ zurück.

Katalogelement aus einer GDM-Vorlage (Google Cloud Deployment Manager) erstellen oder aktualisieren

Anstatt ein Katalogelement basierend auf einer Blaupause zu generieren, können Sie ein Katalogelement basierend auf einer Vorlage im GDM Configuration Management System generieren. Das System analysiert die Attribute sowohl in der Vorlagendatei als auch in optionalen unterstützenden Dateien und generiert dann eine Blaupause und ein Katalogelement.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird
Cloud Provisioning and Governance unterstützt Google Cloud Platform-Vorlagen, die vom Cloud Deployment Manager (GDM) verwaltet werden und in YAML, Python oder Jinja2 erstellt wurden.

Das Verfahren zum Erstellen eines Katalogelements aus einer Vorlage umfasst die folgenden Schritte:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

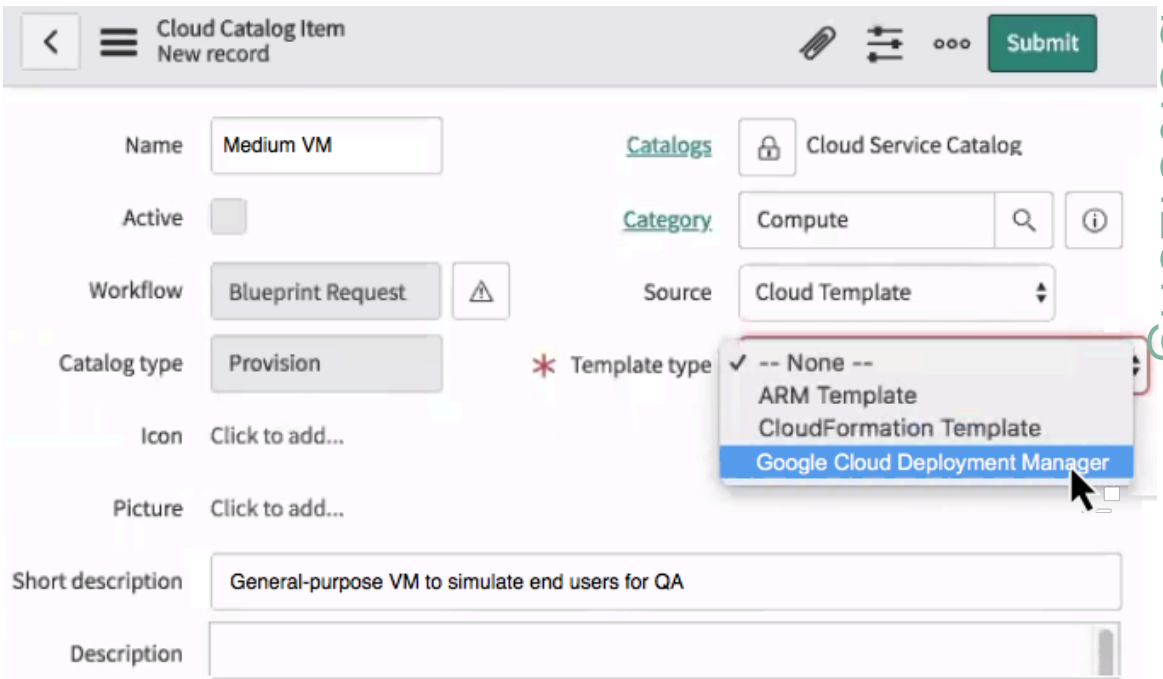
1. Erstellen und speichern Sie einen Katalogelement-Datensatz, in dem auf die Vorlage verwiesen wird. Das Katalogelement befindet sich im Status **Entwurf**. In einem späteren Schritt aktivieren Sie das Katalogelement, um es für Cloud-Benutzer verfügbar zu machen.
2. Erstellen Sie einen Datensatz vom Typ Cloud-Vorlage. In der Cloud-Vorlage wird eine installierbare Konfiguration (eine Verzeichnisstruktur, die die Vorlagendatei enthält,) angegeben, die als Quelle für das Katalogelement verwendet werden soll.

   Hinweis: Sie können den Datensatz der Cloud-Vorlage später aktualisieren, indem Sie auf eine aktualisierte, installierbare Konfiguration verweisen. Anweisungen sind in diesem Verfahren enthalten.

3. Nur Google Cloud Platform: Wenn die Vorlagendatei von unterstützenden Dateien abhängt (typischerweise Updates oder Vorlagencode, in dem Attribut-Einstellungen angegeben sind), fügen Sie die Dateien der zugehörigen Liste **Abhängige Vorlagen** hinzu.
4. Aktivieren Sie die Cloud-Vorlage, um einen Ressourcenblock und eine Blaupause zu erzeugen, die mit dem Katalogobjekt verknüpft sind, und um die Cloud-Vorlage für die Verwendung durch das Katalogelement verfügbar zu machen.
5. Aktivieren Sie das Katalogelement, sodass es Cloud-Benutzer im Cloudbenutzerportal zur Bereitstellung von Ressourcen verwenden können.

Prozedur

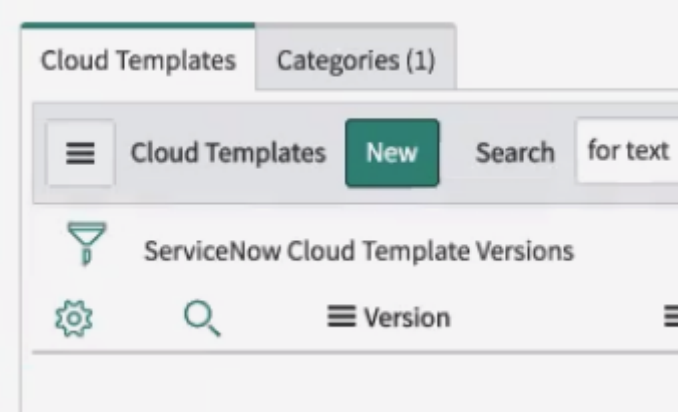
1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Cloud-Katalogelemente**.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen**, eine **Kurzbeschreibung** und eine **Beschreibung** ein.
3. Geben Sie die **Quelle** als **Cloud-Vorlage** und den **Vorlagentyp** als **Google Cloud Deployment Manager** an.



4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.
5. Klicken Sie in der zugehörigen Liste „Cloud-Vorlagen“ auf **Neu**, und geben Sie einen eindeutigen **Namen** und eine **Kurzbeschreibung** ein.

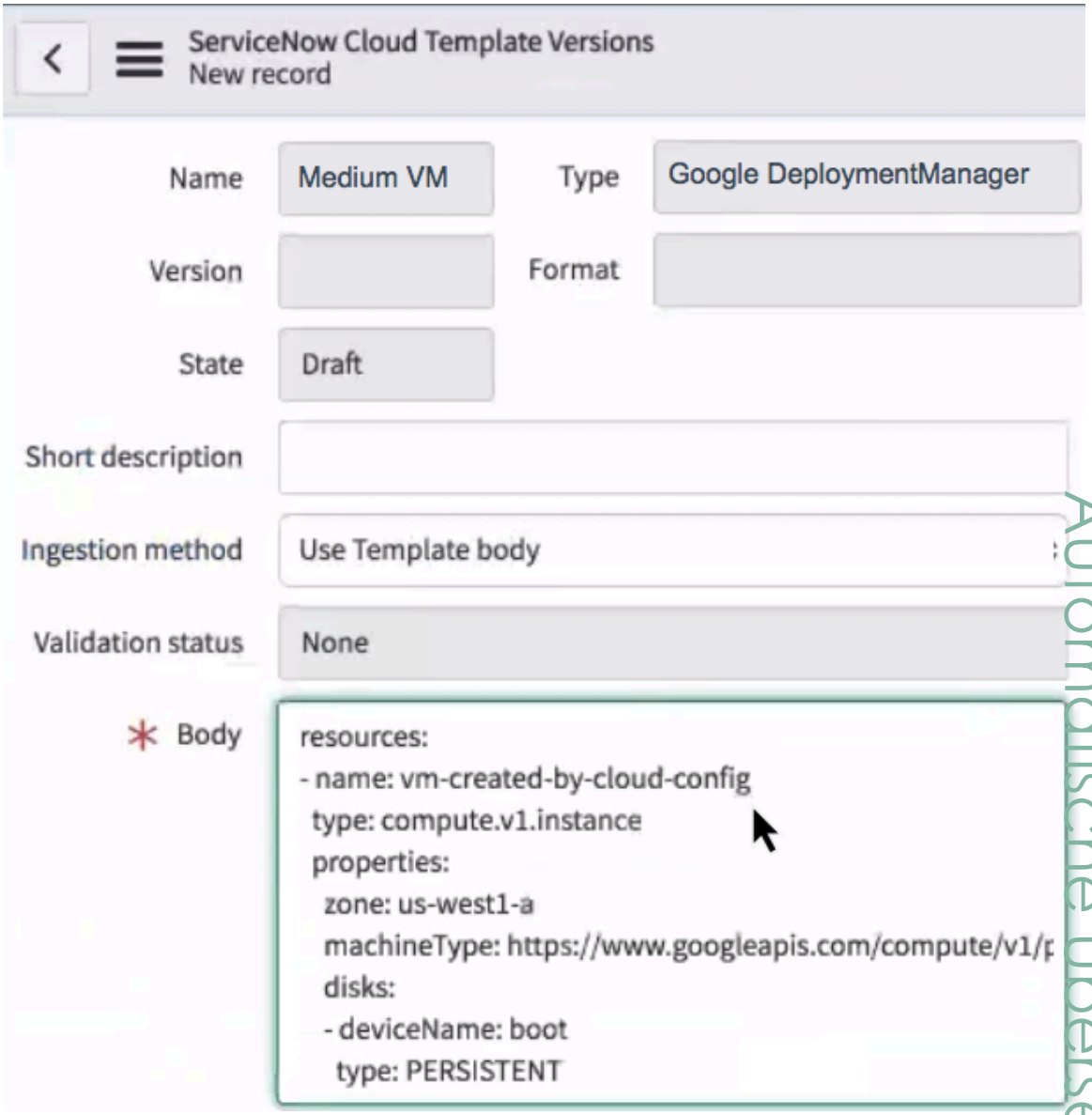
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



6. Geben Sie den Inhalt der Vorlage an, und wählen Sie eine von drei Optionen aus.
   - Fügen Sie den Text der Vorlagendatei in das Formular ein:
     a. Legen Sie die **Erfassungsmethode** auf **Vorlagentext verwenden** fest.
     b. Normalerweise verwenden Sie entweder eine von Ihnen erstellte benutzerdefinierte Vorlage oder eine Vorlage in einem öffentlichen GitHub- oder Bitbucket-Repository. Öffnen Sie die Vorlagendatei in einem Texteditor, und kopieren Sie den vollständigen Text der Datei.
     c. Fügen Sie im Formular „Cloud-Vorlagenversionen“ den Text in das Textfeld **Text** ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



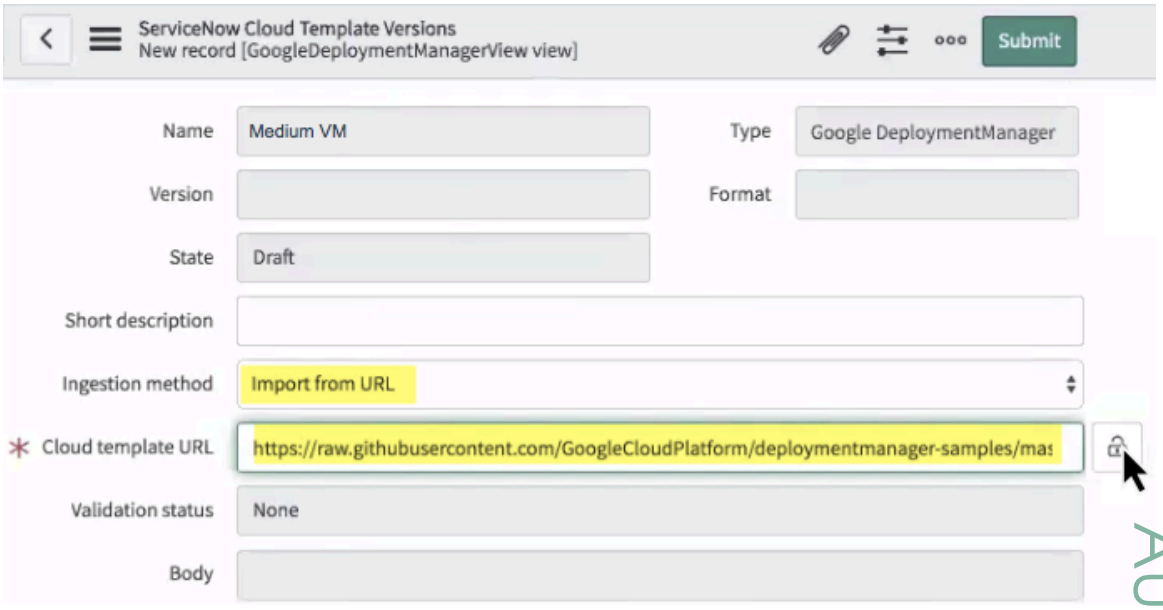
◦ Geben Sie die URL der Vorlagendatei an:

a. Legen Sie die **Erfassungsmethode** auf **Aus URL importieren** fest.

b. Wechseln Sie in einem Browser zur Vorlagendatei. Kopieren Sie die vollständige URL der Vorlage in das Textfeld **Cloud-Vorlagen-URL**.

Automatische Übersetzung

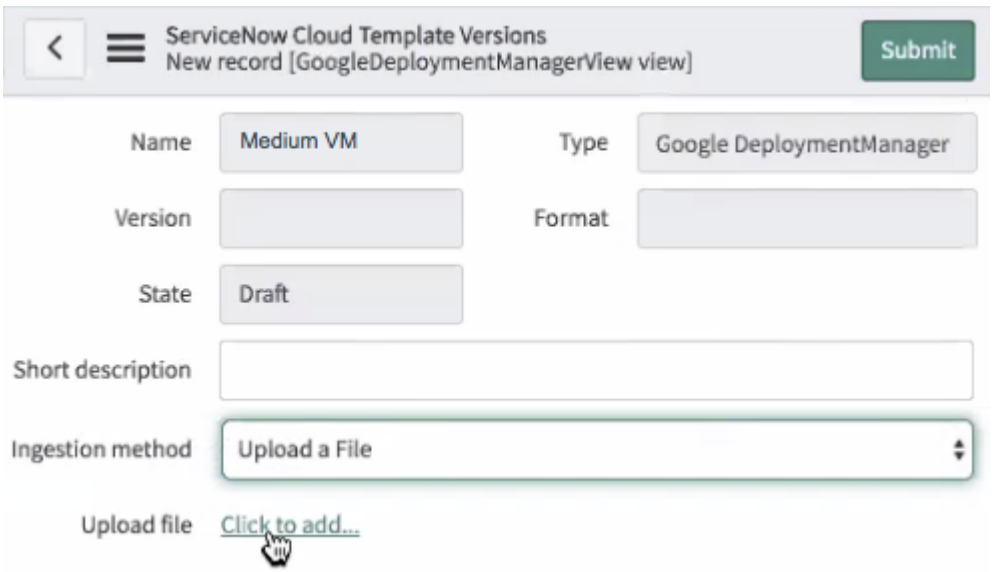
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



◦ Laden Sie die Vorlagendatei hoch:

a. Legen Sie die **Erfassungsmethode** auf **Datei hochladen** fest.

b. Klicken Sie beim Feld **Datei hochladen** auf den Link **Zum Hinzufügen klicken**.



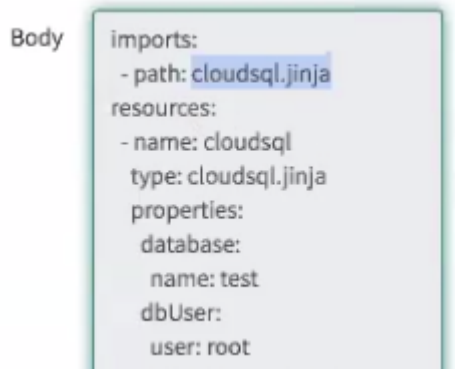
c. Klicken Sie auf **Datei wählen**, wählen Sie die Datei aus, und klicken Sie auf **OK**. Das System fügt die Vorlage hinzu, und der Dateiname wird im Feld **Datei hochladen** angezeigt. Die Ergebnisse des Importprozesses werden in den Feldern **Validierungsstatus** und **Validierungsnachricht** angezeigt.

7. Der Vorlagencode erscheint im Textfeld **Text**.

Wenn die Datei unter `imports:` keinen Eintrag für `path:` enthält, überspringen Sie diesen Schritt. Wenn die Datei einen Eintrag enthält, ist die Vorlagendatei von mindestens einer anderen Datei abhängig (in der Regel Aktualisierungen oder Dateien, die Attributeinstellungen festlegen). Führen Sie das folgende Verfahren für jede abhängige Datei aus (im Beispiel `cloudsql.jinja`):

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



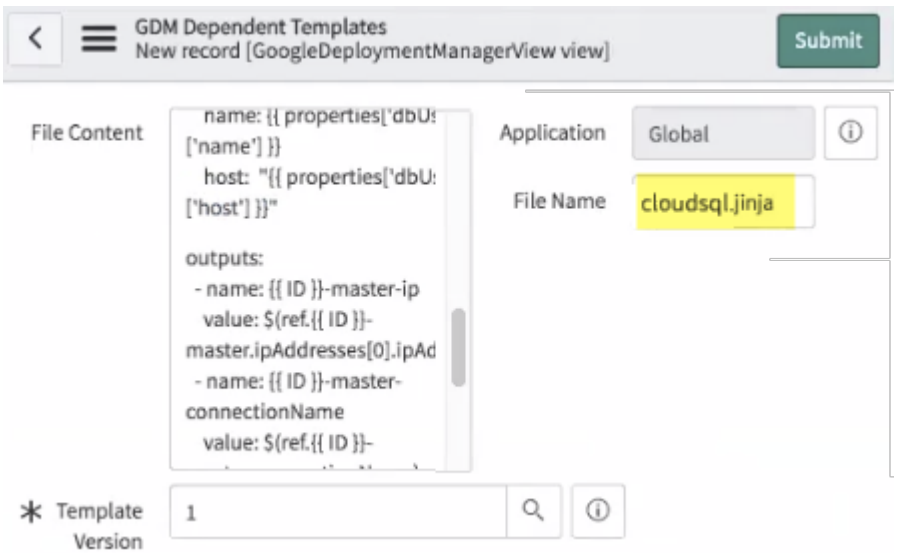
a. Öffnen Sie in einem Texteditor die abhängige Vorlagendatei (im Beispiel„`cloudsql.ginja` “).

b. Kopieren Sie den vollständigen Text der Datei.

c. Klicken Sie in der zugehörigen Liste **Abhängige GDM-Vorlagen** auf **Neu**.

d. Fügen Sie den vollständigen Text der abhängigen Vorlagendatei in das Textfeld **Dateiinhalt** ein.

e. Geben Sie den exakten Namen der abhängigen Vorlagendatei in das Textfeld **Dateiname** ein.



f. Klicken Sie auf **Absenden**.
Die Datei wird in der zugehörigen Liste der **Abhängige GDM-Vorlagen** angezeigt.

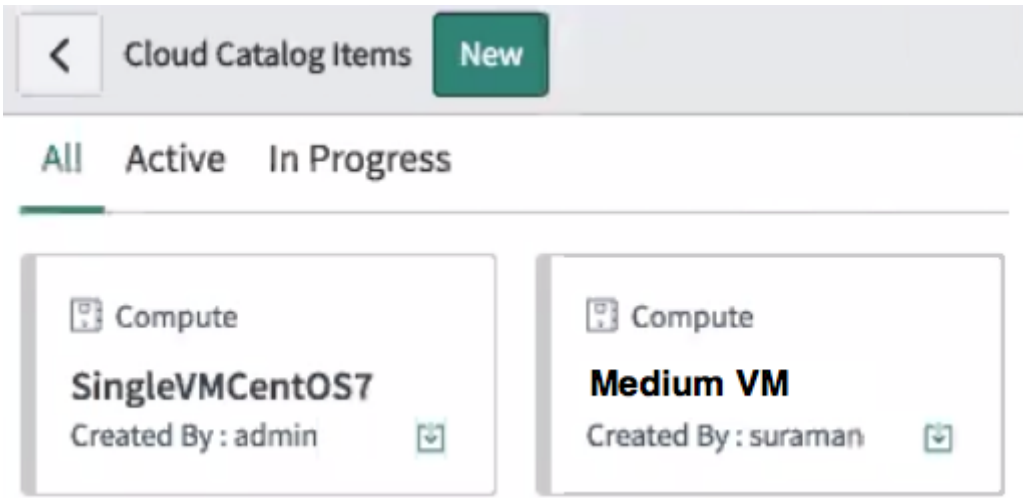
g. Wiederholen Sie den Vorgang für jede abhängige Vorlagendatei.

8. Klicken Sie im Formular „Cloud-Vorlagenversionen“ auf **Aktivieren**.
Das System generiert das Katalogelement und eine Blaupause mit dem Namen, den Sie für das Katalogelement angegeben haben.

9. Aktivieren Sie im Formular „Cloud-Katalogelement“ das Kontrollkästchen **Aktiv**, und klicken Sie dann auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das System zeigt das Katalogelement auf der Seite „Cloud-Katalogelemente“ an und veröffentlicht das Katalogelement im Cloud Service Catalog zur Verwendung durch Endbenutzer.



Hinweis: Wie bei jedem Katalogelement können Sie ein für Benutzer sichtbares Feld hinzufügen oder entfernen. Klicken Sie auf die Karte, um das Katalogelementformular zu öffnen. Bearbeiten Sie auf der Registerkarte **Variablensätze** die Variablen.

Nächste Maßnahme
Vergewissern Sie sich, dass das Katalogelement im Cloudbenutzerportal angezeigt wird.

Post-Bereitstellungsvorgänge erstellen

Erstellen Sie Aufgaben nach der Bereitstellung für neu bereitgestellte Katalogelemente, indem Sie Workflows, Skripts, CAPI-Aufrufe oder Ressourcenvorgänge definieren. Richten Sie aus Effizienzgründen einen Vorgang nach der Bereitstellung ein, um einen manuellen Aufruf zu vermeiden. Dieser Ansatz verbessert das Zeitmanagement und stellt nach der Ressourcenbereitstellung eine nahtlose Ausführung der gewünschten Aktionen für das Katalogelement sicher.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird
Sie können Post-Bereitstellungsvorgänge nur für Katalogelemente erstellen, die auf Vorlagen basieren.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Cloud-Katalogelemente**.
2. Öffnen Sie ein Katalogelement, klicken Sie auf die Registerkarte **Post-Bereitstellungsvorgang**, und klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

Formular zur Vorgangseinrichtung

Feld	Beschreibung
Schritttyp	Post-Bereitstellungsvorgang. Abhängig vom Typ des ausgewählten Post-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Bereitstellungsvorgangs werden zusätzliche Felder angezeigt. ◦ CAPI: ▪ CAPI-Provider ▪ CAPI-Schnittstelle ▪ CAPI-Methode ▪ CAPI-Version ◦ InstanceScript: Skript: Geben Sie den Namen des Skripts ein. ◦ Ressource: ▪ Ressourcenschnittstelle ▪ Schnittstellenvorgang ◦ Workflow Flow: Wählen Sie einen Workflow aus. Alle in der Instanz erstellten Workflows werden aufgelistet. **Hinweis:** Während Sie einen Ressourcenvorgangsschritt hinzufügen, können Sie keine Flows aufrufen. Dies ist eine bekannte Einschränkung. ◦ Flow: Wählen Sie einen Subflow aus. Alle aktiven Subflows in der Instanz werden aufgelistet. **Hinweis:** Weitere Informationen finden Sie unter Subflows .
Auftrag	Reihenfolge von Post-Bereitstellungsvorgängen. Geben Sie die Reihenfolge (in Zahlen) ein, in der der Post-Bereitstellungsvorgang aufgerufen werden soll. Wenn Sie beispielsweise den Wert 2 für CAPI und den Wert 3 für InstanceScript eingeben, wird zuerst CAPI und dann das InstanceScript aufgerufen. Wenn Sie keinen Wert in dieses Feld eingeben, gibt das System automatisch einen Wert in Schritten von 20 ein.
Aktiviert	Option zum Aktivieren des Post-Bereitstellungsvorgangs, der aufgerufen werden soll.

4. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Parameter für den Post-Bereitstellungsvorgang werden automatisch als Vorgangsattribute im Formular „Attribute verwalten“ erstellt.

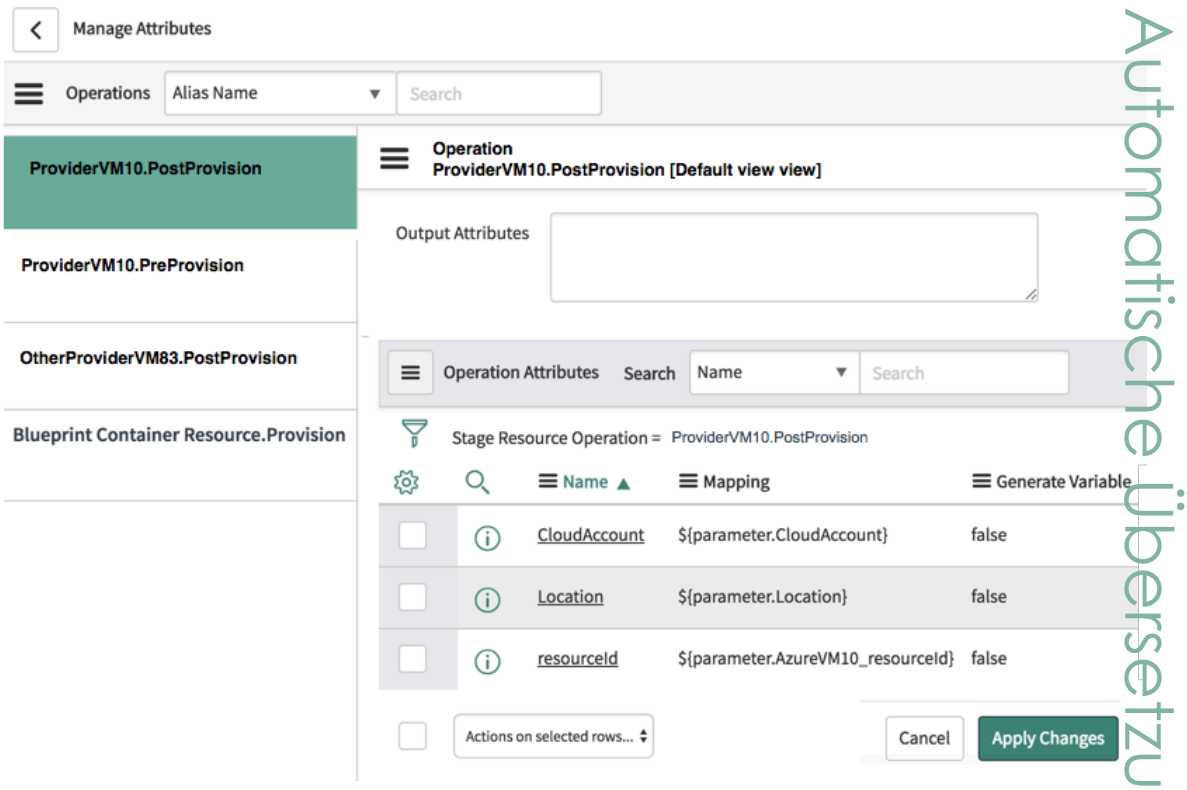
5. So legen Sie Attributwerte für einen Post-Bereitstellungsvorgang fest:

   a. Klicken Sie auf den zugehörigen Link **Attribute verwalten**.

      Das Formular „Attribute verwalten“ wird geöffnet.

   b. Wählen Sie den zu aktualisierenden Post-Bereitstellungsvorgang aus.

      Alle Attribute für den ausgewählten Vorgang werden in der Liste der Vorgänge angezeigt. Sie können entweder Ausdruckszuordnungen (wie in der Spalte **Zuordnung**) für ein Attribut erstellen oder Variablen für ein Attribut generieren. Weitere Informationen finden Sie unter Vorgangsattribute verwalten.



   c. Bearbeiten Sie im Formular „Vorgangsattribute“ die Werte im Feld **Zuordnung** nach Bedarf.

   d. Um einen Wert festzulegen und das Feld nicht für Cloud-Benutzer anzuzeigen, setzen Sie **Variable generieren** auf „false“.

      Für Post-Bereitstellungsvorgänge für VMware können Sie die folgenden Attributwerte festlegen:

Post-Bereitstellungsvorgangsattribute für VMware

Attributname	Im Zuordnungsausdruck festzulegendes <Wertfeld>
NodeCredential	$(capiResolver.NodeCredentialResolver#nodeCredentialIdSysID>)

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Attributname	Im Zuordnungsausdruck festzulegendes <Wertfeld>
	Hinweis: Sie müssen die Anmeldeinformationen manuell erstellen, um die sys_id im Ausdruck angeben zu können.
NodeAddress	$(Script:CMPVMUtils.getReachableIp[arg=$(Stack.items[<VM-Name>].attributes[sys_id])])
ScriptExpression	${CloudScript.scripts <![CDATA[<Script Name>]] >}

e. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.
Alle Konfigurationen werden gespeichert, und die Seite „Cloud-Katalogelemente“ wird geöffnet.

Auf Cloud Formation-Vorlage basierendem Katalogelement Post-Bereitstellung hinzufügen

Erstellen Sie einen Post-Bereitstellungsvorgang als Workflow für ein Katalogelement, das auf einer Cloud Formation-Vorlage (Cloud Formation Template, CFT) basiert.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird
In diesem Beispiel erstellen Sie ein Schlüsselpaar in der AWS-Konsole, wählen dann die entsprechenden Anmeldeinformationen aus, erkennen Cloud-Konten, erstellen ein CFT-basiertes Katalogelement, fügen dem Katalogelement einen Post-Bereitstellungsvorgang als Workflow hinzu und stellen zuletzt das Katalogelement bereit.
Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind, bevor Sie mit der Bearbeitung dieses Beispiels beginnen:

- Das Cloud Provisioning and Governance-Plugin ist aktiviert.
- AWS-Anmeldeinformationen und Servicekonto sind eingerichtet.
- Das Cloud-Konto für AWS Logical Data Center ist erstellt.
- Das Schlüsselpaar ist in AWS konfiguriert und in CMP als „cmdb_ci_cloud_key_pair“ verfügbar.
- Ein Workflow ist auf einer Instanz verfügbar. In diesem Beispiel wird der Workflow `SSH_Workflow_New` verwendet.
- Eine Skripteinbindung zum Abrufen der privaten und öffentlichen IP ist verfügbar.

Prozedur

1. Erstellen Sie in der AWS-Konsole ein neues Schlüsselpaar.
   Geben Sie dem Schlüsselpaar einen Namen, z. B. `ItappWOP`.
   Wenn Sie ein Schlüsselpaar erstellen, wird automatisch eine PEM-Datei auf Ihr System heruntergeladen.
2. Öffnen Sie die PEM-Datei, und kopieren Sie den gesamten Inhalt der Datei.
3. Navigieren Sie mithilfe des Filternavigators in Ihrer Instanz zur Anwendung „Anmeldeinformationen“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Klicken Sie auf **Neu**, und wählen Sie dann **Private SSH-Schlüsselanmeldeinformationen** aus.
5. Geben Sie im Feld **Name** einen Namen (`Itappwop`) ein.
6. Fügen Sie im Feld **Privater SSH-Schlüssel** den Inhalt der PEM-Datei ein.
7. Geben Sie im Feld **Anmeldeinformationsalias** einen Aliasnamen (`Itappwop`) ein.
   Der Aliasname muss mit dem Namen übereinstimmen, den Sie im Feld **Name** eingegeben haben.
8. Klicken Sie auf **Absenden**.
9. Führen Sie ServiceNow® Discovery aus, um Cloud-Konten zum Synchronisieren von Daten aus AWS zu erkennen.
10. Erstellen Sie ein Cloud-Katalogelement basierend auf AWS CFT, um einen Stapel bereitzustellen.

    a. Navigieren zu **Cloud-Adminportal** > **Entwurf** > **Cloud-Katalogelemente**

    b. Klicken Sie auf **Neu**.
    Der Bildschirm „Cloud-Katalogelement“ wird angezeigt.

11. Geben Sie einen eindeutigen Namen für das Katalogelement in das Feld **Name** ein, wählen Sie **Cloud-Vorlage** im Feld **Quelle** und **Cloud Formation-Vorlage** im Feld **Vorlagentyp** aus.
12. Klicken Sie auf **Absenden**.
    Das Katalogelement wird generiert.
13. Erstellen Sie eine Cloud-Vorlage, und ordnen Sie die Vorlage dem Katalogelement zu.

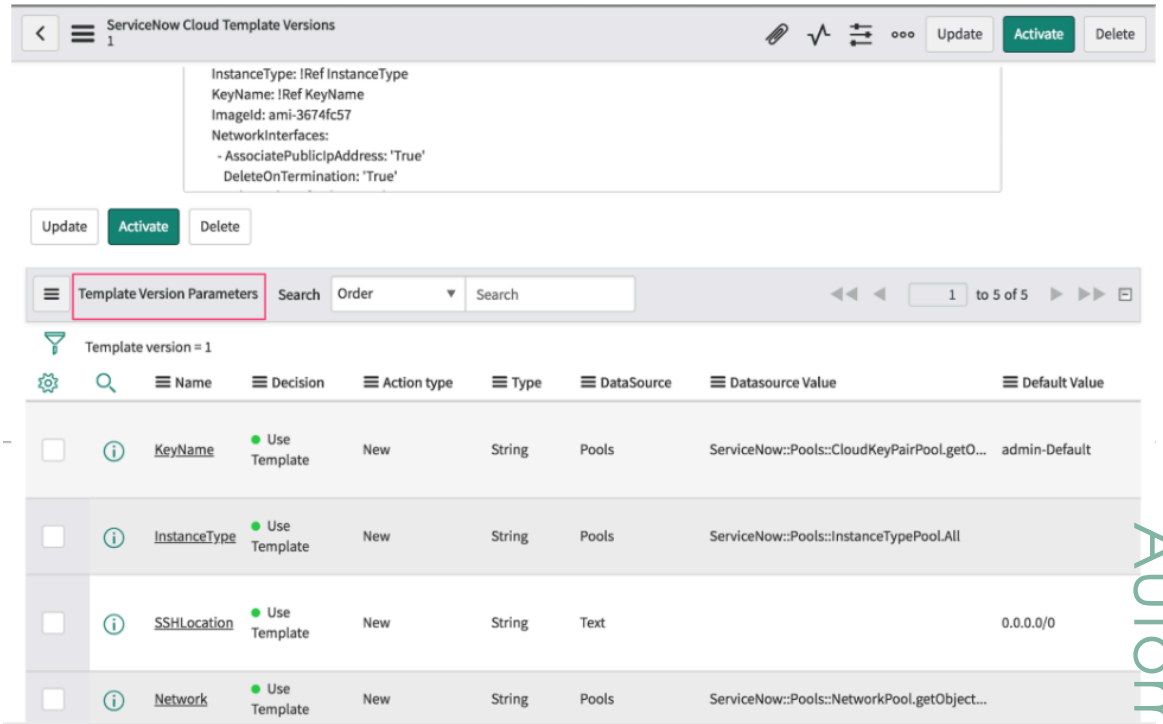
    a. Navigieren zu **Cloud-Adminportal** > **Entwurf** > **Cloud-Katalogelemente**.

    b. Öffnen Sie den Katalogelementdatensatz, für den Sie eine Cloud-Vorlage erstellen möchten, und klicken Sie auf **Cloud-Vorlagen** > **Neu**.
    Der Bildschirm „Cloud-Vorlagenversionen“ wird angezeigt.

    c. Wählen Sie in der Liste „Erfassungsmethode“ die Option **Vorlagentext verwenden** aus, und fügen Sie den Inhalt der AWS CFT in das Feld **Text** ein.

    d. Klicken Sie auf **Speichern**.
    Alle aus der AWS CFT extrahierten Variablen werden im Abschnitt „Versionsparameter der Vorlage“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



e. Klicken Sie auf **Aktivieren**.
Das Katalogelement wird generiert.

14. Wechseln Sie zum Cloud-Benutzerportal, und öffnen Sie das Katalogelement, das Sie gerade generiert haben.
Auf der Registerkarte **Bereitstellung** sehen Sie alle aus der Vorlage extrahierten Variablen. Sie können dem Katalogelement einen Post-Bereitstellungsvorgang als Workflow hinzufügen.
15. Navigieren zu **Cloud-Adminportal** > **Entwurf** > **Cloud-Katalogelemente**.
16. Öffnen Sie den Katalogelementdatensatz, für den Sie den Post-Bereitstellungsvorgang als Workflow erstellen möchten.
17. Klicken Sie auf die Unterregisterkarte **Post Provisioning Operation** Post-Bereitstellungsvorgang, und klicken Sie auf **Neu**.
Das Formular „Vorgangsschritt“ wird angezeigt.
18. Wählen Sie **Workflow** in der Liste **Setup-Typ** aus, und wählen Sie **SSH_Workflow_New** in der Liste **Flow** aus.
19. Klicken Sie auf **Absenden**.
Parameter für den Workflow-Vorgang werden automatisch als Vorgangsattribute auf dem Bildschirm „Attribute verwalten“ erstellt.
20. Klicken Sie auf **Attribute verwalten**.
Der Bildschirm **Attribute verwalten** wird angezeigt.
21. Klicken Sie auf **EC2-Instanz mit SSH-Skript.Post-Bereitstellung bereitstellen**.
22. Klicken Sie auf das Attribut **key_name**, und geben Sie entweder den Wert des Anmeldeinformationsalias (`Itappwop`) ein, oder geben Sie eine Ausdruckszuordnung in das Feld **Zuordnung** ein.
Zuordnungen geben an, wo die Informationen im System abgerufen werden. Weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

23. Klicken Sie auf das Attribut **Stapel-ID**, und geben Sie die Ausdruckszuordnung `$(context.order.stack)` ein.
24. Klicken Sie auf **Apply Changes (Änderungen übernehmen)**.
    Workflow wird dem Katalogelement, das Sie generiert haben, als ein Vorgang nach der Bereitstellung zugeordnet.
25. Stellen Sie das CFT-basierte Katalogelement im Cloud-Benutzerportal bereit.
    a. Navigieren Sie zum **Cloud-Benutzerportal**, und klicken Sie auf **Einen Stapel starten**.
    b. Öffnen Sie das Katalogelement, das Sie bereitstellen möchten, und geben Sie Werte in alle Pflichtfelder auf den Registerkarten **Allgemeine Informationen** und **Bereitstellung** ein.
26. Klicken Sie auf **Absenden**, um das Katalogelement bereitzustellen.
27. Validieren Sie das bereitgestellte Katalogelement nach Abschluss.

Prä- oder Post-Bereitstellungsvorgänge mit Subflows einem vorlagebasierten Katalogelement hinzufügen

Sie können einen Vorgang nach der Bereitstellung mithilfe von Subflows für ein vorlagenbasiertes Katalogelement erstellen.

Vorbereitungen

- Die Anwendung Orchestration wurde installiert.

Erforderliche Rolle: Cloud-Benutzer, -Designer, -Admin, sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

In diesem Beispiel fügen Sie einem vorhandenen Katalogelement, das Sie durch Erfassen einer Vorlage erstellen, einen Subflow als Prä- oder Post-Bereitstellungsvorgang hinzu.

Prozedur

1. Navigieren Sie im Cloud-Adminportal zu **Entwurf** > **Cloud-Katalogelemente**.
2. Öffnen Sie ein Katalogelement, klicken Sie auf die Registerkarte **Prä-Bereitstellungsvorgang** oder **Post-Bereitstellungsvorgang**, und klicken Sie auf **Neu**.
3. Geben Sie im Formular die folgenden Feldwerte ein oder wählen Sie sie aus.
4. Wählen Sie in der Liste **Schritttyp** als Vorgangsschritttyp **Flow** aus.
5. Klicken Sie auf das Lupensymbol beim Feld **Flow**.
6. Wählen Sie in der Nachschlageliste **Subflow** einen aktiven Subflow aus.
   In der Suchtabelle sind alle aktiven Flows und Subflows in der Instanz aufgelistet.

   Hinweis: Während Sie einen Ressourcenvorgangsschritt hinzufügen, können Sie keine Flows aufrufen. Dies ist eine bekannte Einschränkung.

7. Geben Sie im Feld **Reihenfolge** eine Reihenfolge für diesen Vorgang an.
8. Aktivieren Sie das Kontrollkästchen **Aktiviert**, um den Vorgang zu aktivieren.
9. Klicken Sie auf **Absenden**.
   Der Schritt des Subflow-Vorgangs wird dem Katalogelement angefügt und in der zugehörigen Liste „Prä-Bereitstellungsvorgang“ oder „Post-Bereitstellungsvorgang“ angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme

- Alle dem von Ihnen ausgewählten Subflow zugeordneten Eingabeparameter werden in der zugehörigen Liste „Schlüsselwerte“ automatisch ausgefüllt.
- Klicken Sie auf den Subflow-Vorgangsschritt in der entsprechenden zugehörigen Liste, um Eingabeparameter hinzuzufügen oder zu ändern.

Hinweis: Stellen Sie sicher, dass der Eingabeparameter `flowcorrelationid` im Subflow mit der folgenden Ausdruckszeichenfolge erstellt wird:

Schlüssel	Wert
`flowcorrelationid`	`$(Script:CMPFlowStepHandler.generateCorrelationId)`

- Alle dem von Ihnen ausgewählten Subflow zugeordneten Eingabeparameter werden in der zugehörigen Liste „Schlüsselwerte“ automatisch ausgefüllt.
- Erstellen Sie einen Schrittantwortprozessor. Weitere Informationen finden Sie unter Antwortprozessor konfigurieren.
- Erstellen Sie eine Antwortaktion für Cloud Provisioning and Governance

Machen Sie das Katalogelement sichtbar

Sie können die in Cloud-Management erstellten Katalogelemente im Standardserviceportal verwenden.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie zu einem Cloud-Katalogelement.
2. Fügen Sie **Servicekatalog** oder Ihren spezifischen Katalog zu hinzu **Katalogelement**.
3. Speichern Sie.
4. Wählen Sie **Kategorien** aus Elementen der zugehörigen Liste aus.
5. Bearbeiten Sie die Kategorien, und fügen Sie eine Kategorie aus **dem Servicekatalog** oder Ihrem spezifischen Katalog hinzu.
6. Rufen Sie die Servicekatalogseite oder Ihre spezifische Katalogseite auf.
   Das neue Katalogelement wird angezeigt.

Variablensatz für Cloud Provisioning and Governance erstellen

Reduzieren Sie die Anzahl der erforderlichen Schritte zum Erstellen und Verwalten mehrerer Katalogelemente und Bestellleitfäden, indem Sie Variablensätze erstellen. Bei Variablensätzen müssen Sie nicht für jedes Katalogelement einzeln Variablen erstellen.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird
Erstellen Sie eine Sammlung strukturierter Variablen, die mithilfe von Variablensätzen für mehrere Katalogelemente und Bestellleitfäden wiederverwendet werden können.

Ein neuer Variablensatz ist zum Hinzufügen relevant, wenn bestimmte Anforderungsformularvariablen zum Ausführen von Aktionen wie Aktionen nach der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bereitstellung oder zum Sammeln zusätzlicher Informationen wie anwenderdefinierter Tags erforderlich sind.

Sie können den Variablensatz ändern, und die Änderungen werden für alle Katalogelemente übernommen, die dem Variablensatz zugeordnet sind. Mit Variablensätzen können Sie auch Katalog-Clientskripts und UI-Richtlinien definieren, die für die Variablen im Satz gelten.

Wenn Sie ein Katalogelement generieren, werden automatisch zwei Variablensätze (**Allgemeine Informationen** und **Bereitstellung**) erstellt. Erstellen Sie so viele Variablensätze wie nötig.

Prozedur

1. Öffnen Sie ein Cloud-Katalogelement, und klicken Sie auf der Registerkarte **Variablensätze** auf **Neu**.
   Der Bildschirm „Variablensatz“ wird angezeigt.
2. Füllen Sie die Formularfelder aus (siehe Tabelle).

Feld	Beschreibung
Titel	Eindeutiger Name für den Variablensatz.
Interner Name	(Eindeutiger) Name des Variablensatzes für die interne Verwendung. **Hinweis:** Wenn dieses Feld leer ist, wird sein Wert basierend auf dem Feld **Titel** für alle Variablentypen mit Ausnahme von Bruch, Containeraufteilung und Container-Ende automatisch ausgefüllt.
Layout	Für das Layout werden folgende Auswahlmöglichkeiten angezeigt: **1 Spalte breit**, **2 Spalten breit, wechselnde Seiten** oder **2 Spalten breit, eine Seite, dann die andere**.
Reihenfolge	Reihenfolgennummer für den Variablensatz.
Beschreibung	Beschreibung des Variablensatzes.

3. Klicken Sie auf **Absenden**.
   Der neue Variablensatz wird erstellt und auf der Registerkarte **Variablensätze** angezeigt. Öffnen Sie den neuen Variablensatz, und klicken Sie auf der Registerkarte **Cloud-Variablen** auf **Neu**, um Variablen für den Satz zu erstellen.

Variable für Cloud Provisioning and Governance bearbeiten

Bearbeiten Sie eine vorhandene Cloud-Variable oder erstellen Sie eine neue Cloud-Variable, um Informationen für die Bestellung eines Katalogelements zu sammeln.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Sie können eine Variable bearbeiten, um ihren Typ zu ändern, z. B. von **Maskiert** in **Auswahlfeld für Suche**. Sie können auch den Variablensatz einer Variable und ihre Reihenfolge ändern, sie aktiv oder inaktiv machen, ihre Berechtigungs- und Verfügbarkeitsoptionen ändern und vieles mehr.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Cloud-Katalogelemente**.
2. Öffnen Sie ein Katalogelement, klicken Sie auf die Unterregisterkarte **Variablensätze**, und klicken Sie auf den Variablensatz, zu dem die zu bearbeitende Variable gehört. Alle Cloud-Variablen für den ausgewählten Variablensatz werden auf der untergeordneten Registerkarte **Cloud-Variablen** angezeigt.
3. Klicken Sie auf den Variablensatz, den Sie bearbeiten möchten.
4. Füllen Sie die Felder des Formulars aus.

Formular „Cloud-Variable“

Feld	Beschreibung
Typ	Zu erstellender Variablentyp. Wenn Sie **Auswahlfeld für die Suche**auswählen, werden auf der Unterregisterkarte **Typspezifikationen** diese Felder angezeigt: ◦ **Poolfilter verwenden**: Aktivieren Sie dieses Kontrollkästchen, um dem Feld einen Poolfilter hinzuzufügen. ◦ **Pool**: Wählen Sie einen Pool aus, um dem Benutzer des Cloud-Service eine Liste von Werten aus einer vorhandenen Tabelle im Katalogbestellformular anzubieten. Beispielsweise können Sie „CloudAccountPool“ auswählen, um eine Liste aller Cloud-Konten zu erhalten. ◦ **Poolfilter**: Wählen Sie einen Filter aus, um die Auswahlmöglichkeiten im Pool weiter einzugrenzen.
Variablensatz	Der Variablensatz, zu dem die Variable gehört.
Obligatorisch	Option, um die Variable als Teil des Bestellvorgangs obligatorisch zu machen.
Aktiv	Option, um die Variable zur Verwendung verfügbar zu machen.
Reihenfolge	Ordnen Sie an, dass die Variable auf der Seite für das Katalogelement platziert wird. Die Variablen sind von oben nach unten vom kleinsten zum größten Reihenfolgenwert organisiert. Zum Beispiel wird eine Variable mit einem Ordnungswert

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	von 1 über anderen Variablen mit Werten höherer Ordnung platziert.

Fragen

Feld	Beschreibung
Frage	Frage an Benutzer, die den Katalogartikel bestellen. **Hinweis:** Wenn Sie im Feld **Typ** die Option **Auswahlfeld** auswählen, wird am Ende des Bildschirms eine Unterregisterkarte **Fragenauswahl** angezeigt. Sie können eine bestimmte Auswahlliste für die Frage eingeben.
Name	Ein Name zur Identifizierung der Frage. **Hinweis:** Wenn dieses Feld leer ist, wird sein Wert basierend auf dem Feld Frage für alle Variablentypen mit Ausnahme von break, container split, container end, HTML, container start, label, UI page und duration automatisch ausgefüllt.
Tooltip	Tooltip-Text, der angezeigt wird, wenn Benutzer auf die Variable zeigen. Geben Sie eine kurze Notiz ein, um den Zweck der Frage zu beschreiben.
Beispieltext	Hinweis, der im Fragefeld angezeigt wird, bevor ein Benutzer einen Wert eingibt. Anwendbar für folgende Variablen: ◦ IP-Adresse ◦ E-Mail ◦ URL ◦ Einzeiliger Text ◦ Mehrzeiliger Text ◦ Datum ◦ Datum/Uhrzeit

Anmerkung

Feld	Beschreibung
Hilfe anzeigen	Wenn diese Option ausgewählt ist, wird der Hilfetext für die Variable angezeigt.
Immer erweitert	Diese Option wird nur angezeigt, wenn das Kontrollkästchen **Hilfe anzeigen** aktiviert ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Wenn diese Option ausgewählt ist, wird der Wert des Felds **Hilfetext** standardmäßig erweitert, wenn die Katalogelementseite geladen wird.
Hilfe-Tag	Wenn das Kontrollkästchen **Immer erweitert** deaktiviert ist, klicken Sie auf den in diesem Feld angegebenen Wert, um den Wert des Feldes **Hilfetext** anzuzeigen.
Hilfetext	Hilfeinformationen für eine Service Catalog-Variable
Anweisungen	Informationen, die Rich-Text-Formatierung erfordern oder Bilder hinzufügen, um Hilfeinformationen zu unterstützen. **Hinweis:** Verwenden Sie für HTML-Tabellen Größen, die innerhalb der Breite der Variablen liegen.

Typspezifikationen (Die Felder in diesem Abschnitt variieren für jeden Variablentyp)

Feld	Beschreibung
Variablenbreite	Breite für die Variable auf der Katalogelementseite, um anzugeben, wie viel Prozent der Bildschirmgröße sie umfassen darf. Dieses Feld wird für alle Variablentypen mit Ausnahme der Zeilenumbrüche, des Containerendes, des Containerstarts, der Containeraufteilung, des Containerlayouts und der Beschriftungsvariablen angezeigt.
Regulärer Ausdruck zur Validierung	Regulärer Ausdruck, der die Benutzereingabe für die Eigenschaft validiert.
Validierungsfehler für regulären Ausdruck	Wenn der Ausdruck nicht gültig ist, wird ein Fehler angezeigt.

Standardwert

Feld	Beschreibung
Standardwert	Standardwert für die Variable
Variablenattribute	Attribute für diese Variable.

Berechtigungen

Feld	Beschreibung
Leserollen	Rollen, die die Variable vor oder nach dem Anfordern des Katalogelements

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	oder Datensatzerstellers anzeigen können. Nur ein Benutzer mit den in diesem Feld angegebenen Rollen kann die Variable anzeigen.
Schreibrollen	Rollen, die die Variable im Variableneditor bearbeiten können, nachdem sie das Katalogelement oder den Datensatzersteller angefordert haben. Wenn ein Benutzer die in diesem Feld angegebenen Rollen nicht besitzt, ist die Variable im Variableneditor schreibgeschützt.
Erstellenrollen	Rollen, die Werte für die Variable erstellen können, bevor sie das Katalogelement oder den Datensatzersteller anfordern. Wenn ein Benutzer die angegebene Rolle nicht besitzt, ist die Variable schreibgeschützt, bevor das Katalogelement oder der Datensatzersteller angefordert wird.

Verfügbarkeitsdiagramm

Sichtbar	Wenn diese Option ausgewählt ist, ist die Variable im Elementformular vor der Bestellung des Elements, im Variableneditor nach der Bestellung des Elements und in der Warenkorbansicht des Elements sichtbar.
Schreibgeschützt	Wenn ausgewählt, ist die Variable im Cloud-Benutzerportal schreibgeschützt und kann nicht bearbeitet werden.

5. Klicken Sie auf **Aktualisieren**, wenn Sie alle Änderungen an der Variablen vorgenommen haben.

Vorgangsattribute verwalten

Sie können Attributwerte für Katalogelemente angeben, damit Cloud-Benutzer Katalogelemente ordnungsgemäß bereitstellen können. Sie können Attribute für Bereitstellungs-, Prä- und Post-Bereitstellungsvorgänge konfigurieren und verwalten.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

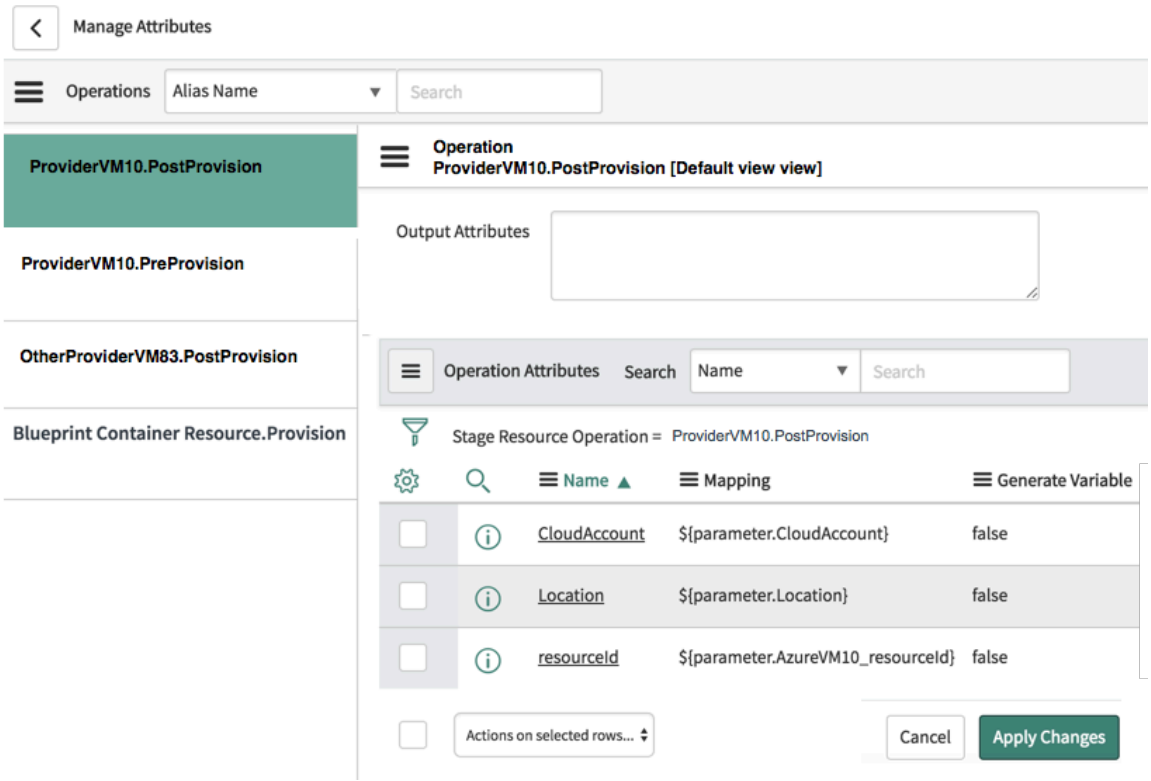
Warum und wann dieser Vorgang ausgeführt wird

Die Attribute für Bereitstellungs-, Prä- und Post-Bereitstellungsvorgänge werden automatisch generiert. Sie können Variablen für diese Attribute generieren und auch neue Attribute für den Ressourcenvorgang erstellen. Sie können auch die zugehörigen Listen „Vorgang vor der Bereitstellung“, „Post-Bereitstellungsvorgang“ und „Lebenszyklusvorgänge“ verwenden, um Variablen für Orchestration-Attribute zu erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Cloud-Katalogelemente**.
2. Öffnen Sie ein Katalogelement, und klicken Sie auf die zugehörige Liste „Vorgang vor der Bereitstellung“ oder „Post-Bereitstellungsvorgang“.
   Auf der Seite „Vorgangsschritt“ werden die Vorgänge aufgelistet.



3. Klicken Sie auf einen Vorgang, um die entsprechenden Attribute anzuzeigen.
4. Konfigurieren Sie die Attribute für jeden Vorgang.
   - **Zuordnung**: Rufen Sie die automatisch generierten Zuordnungswerte für jedes Attribut auf. Zuordnungen geben an, wo die Informationen im System abgerufen werden. Zum Ändern der Ausdruckszuordnungen doppelklicken Sie auf den Zuordnungswert und geben Sie neue Werte ein. Klicken Sie dann auf das Häkchensymbol ( ). Ausdrücke können die Werte für Informationen enthalten, die dynamisch im System generiert werden, z. B. die Werte für die Auswahlen, die Benutzer im Cloudbenutzerportal treffen. Weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden.
   - **Variable generieren**: Generiert eine Variable für ein Attribut. Doppelklicken Sie auf den Wert (*false*), wählen Sie **Wahr** aus, und klicken Sie auf das Häkchensymbol ( ).
5. Klicken Sie auf **Änderungen übernehmen**, nachdem Sie alle erforderlichen Änderungen vorgenommen haben.
   Alle Konfigurationen, die Sie an den Attributen vorgenommen haben, werden gespeichert, und Sie kehren zum Bildschirm „Cloud-Katalogelemente“ zurück.

Blaupausen für die Cloudbereitstellung

Eine Blaupause ist eine spezialisierte Katalogelementvorlage zum Anbieten von Cloud-Services oder Stapeln für Cloud-Benutzer. Blaupausen können mit jedem Service Provider für Cloud-Services verwendet werden, z. B. Amazon AWS Cloud oder Microsoft Azure Cloud. Blaupausen aus dem Orlando-Release können nur eingeschränkt verwendet werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

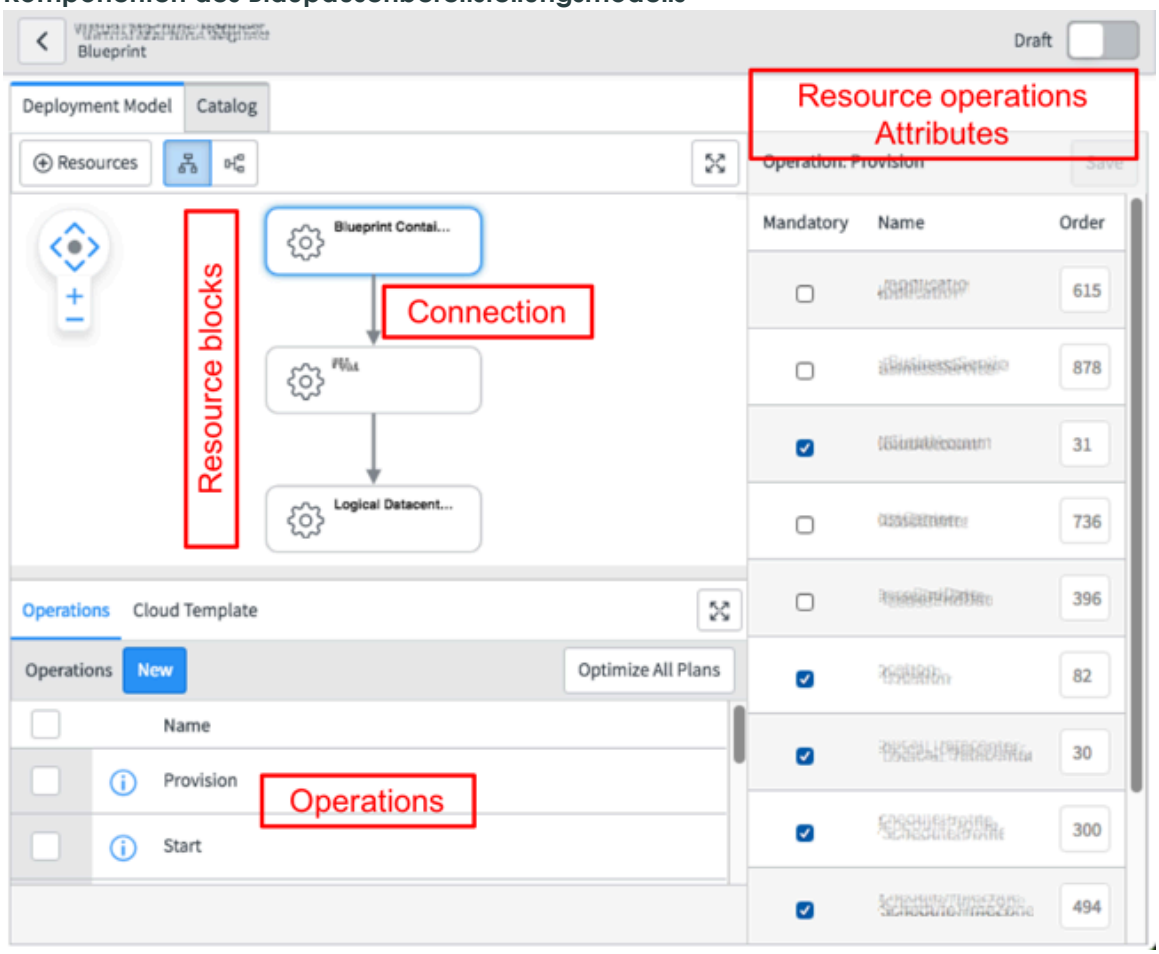
Komponenten von Blaupausen

Hinweis:

- Beginnend mit Orlando sind Cloud Provisioning-Blaupausen für Instanzen verfügbar, die von einem früheren Release aktualisiert wurden. Sie können jedoch keine neuen Blaupausen erstellen. Vorhandene Blaupausen und Katalogelemente aus diesen Blaupausen bleiben davon unberührt und funktionieren weiterhin.
- Verwenden Sie Cloud-Vorlagen für Cloud Provisioning, um Katalogelemente anstelle von Blaupausen zu erstellen. Mithilfe von Cloud Provisioning Cloud-Vorlagen können Sie die Spezifikationssyntax für Azure ARM, AWS CFT, Google Deployment Manager (GDM) und Terraform in Cloud-Katalogelemente zur Ausführung Ihrer Cloud-Bereitstellungsorchestrierung einbinden.

Die Blaupause ist der Mechanismus, der an den Cloud-Provider übergeben wird, um die Cloud-Assets einzurichten. Das Anfordern eines Cloud-Katalogelements wird als Starten eines Stapels bezeichnet. Nachdem das Cloud-Asset abgerufen wurde, kann es erkannt und verwaltet werden.

Komponenten des Blaupausenbereitstellungsmodells



Ressourcenblöcke

Die in der Blaupause (Katalogelement) enthaltenen Cloud-Ressourcen. Beispielsweise kann ein Ressourcenblock einen virtuellen Computer, eine auf der VM ausgeführte App und Informationen über das Rechenzentrum enthalten, das die VM hostet. Auch als Ressourcen bezeichnet.

Verbindungen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Die Beziehung zwischen Ressourcen. Beispielsweise hat die VM eine Hostbeziehung mit der App. Es gibt zwei Arten von Verbindungen: Einschluss und Angehängt.

- Einschluss: Eine Verbindung, bei der der Ressourcenblock einen weiteren enthält. Diese Beziehung wird visuell als Beziehung von oben nach unten dargestellt, wie im Bild gezeigt. Beispielsweise muss der Blaupausencontainer mindestens einen weiteren Ressourcenblock enthalten.
- Angehängt: Eine Verbindung zwischen Ressourcen, die eine Bindung für die direkte Kommunikation untereinander erfordern. Die Beziehung wird visuell nebeneinander dargestellt. Beispielsweise stellt die Bindung zwischen einem virtuellen Computer und einem Speicher eine Angehängt-Beziehung dar.

Betrieb

Die Aktionen, die an Ressourcenblöcken oder am Ressourcenstapel ausgeführt werden, um die Ressourcen zu verwalten. Beispielsweise kann der Cloud-Benutzer eine Ressource bereitstellen, starten und stoppen.

Ressourcenvorgänge

Die Schritte zum Ausführen des Vorgangs für die Ressource. Um beispielsweise das Katalogelement bereitzustellen, muss das System die VM und die darauf ausgeführte App bereitstellen. Klicken Sie auf einen Vorgang, um Detailinformationen für die Ressourcenvorgänge anzuzeigen.

Attribute

Die Details der Ressource. Attribute können im Katalogelementformular als Katalogeigenschaften angezeigt werden. Beispielsweise kann die Blaupause die Version der App bereitstellen, die für die VM bereitgestellt werden soll.

Einschränkungen

Eine Attributoption zur Einschränkung eines cloudunabhängigen Ressourcenblocks, z. B. eines logischen Rechenzentrums, zur Verwendung mit einem bestimmten Cloud-Provider. Beispielsweise kann ein logisches Rechenzentrum auf Amazon AWS Cloud beschränkt werden. Wenn Sie später zu Microsoft Azure Cloud oder einem anderen Cloud-Provider wechseln oder einen solchen hinzufügen, können Sie die Einschränkung nach Bedarf ändern.

Planungsblaupausen

Planen Sie vor dem Erstellen von Blaupausen die Stapel, die Sie im Servicekatalog anbieten möchten. Bereiten Sie die folgenden Informationen vor, bevor Sie mit der Entwicklung beginnen.

Ressourcenblöcke

Planen Sie die Ressourcenblöcke, die Sie in Blaupausen verwenden möchten. Stellen Sie sicher, dass die entsprechenden Ressourcenblöcke für die Verwendung in Blaupausen verfügbar sind, und fügen Sie sie bei Bedarf hinzu.

Serviceangebote (Stapel)

Zum Planen eines Serviceangebots oder Stapel stellen Sie die benötigten Ressourcenblöcke und deren Verbindungen grafisch dar.

Cloud-Konten und Rechenzentren

Rufen Sie eine Liste der Cloud-Konten und Rechenzentren ab, die der Cloud-Administrator konfiguriert hat. Stellen Sie fest, ob welche eingeschränkt sind.

Servicekatalogvariablen und -variablensätze

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Stellen Sie sicher, dass Sie wissen, wie Servicekatalogelemente Variablen und Variablensätze verwenden. Das Verständnis von Servicekatalogelementen und -prozessen hilft Ihnen, Blaupausen besser zu verstehen.

Beginnen Sie hier

Cloud Provisioning-Blaupause erstellen

Cloud Provisioning-Blaupause erstellen

Verwenden Sie den Blaupausendesigner, um benutzerdefinierte Blaupausen für die Cloud Provisioning and Governance-Anwendung zu erstellen. Blaupausen sind im Orlando-Release veraltet.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

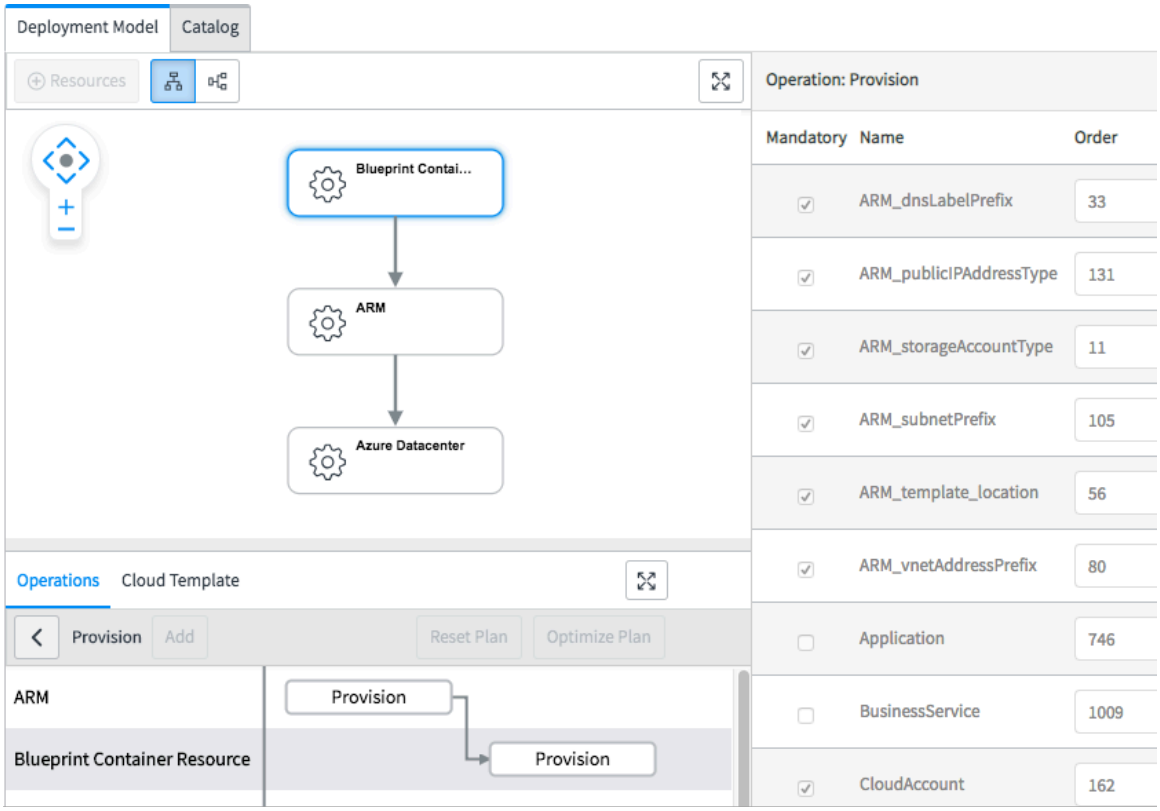
Hinweis:

- Beginnend mit Orlando sind Cloud Provisioning-Blaupausen für Instanzen verfügbar, die von einem früheren Release aktualisiert wurden. Sie können jedoch keine neuen Blaupausen erstellen. Vorhandene Blaupausen und Katalogelemente aus diesen Blaupausen bleiben davon unberührt und funktionieren weiterhin.
- Verwenden Sie Cloud-Vorlagen für Cloud Provisioning, um Katalogelemente anstelle von Blaupausen zu erstellen. Mithilfe von Cloud Provisioning Cloud-Vorlagen können Sie die Spezifikationssyntax für Azure ARM, AWS CFT, Google Deployment Manager (GDM) und Terraform in Cloud-Katalogelemente zur Ausführung Ihrer Cloud-Bereitstellungsorchestrierung einbinden.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Blueprints**.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und sinnvollen **Namen** und eine **Beschreibung** ein, und geben Sie die **Kategorie** des Service an.
   Standardmäßig werden mehrere Kategorien bereitgestellt.
3. Klicken Sie auf **Absenden**.
   Das System erstellt den Blaupausendatensatz und zeigt die Registerkarte „Bereitstellungsmodell“ des Blaupausendesigners an. Die Registerkarte „Bereitstellungsmodell“ ist eine visuelle Canvas, auf der Sie Ressourcenblöcke ablegen. Jeder Ressourcenblock stellt ein CI in einem mehrschichtigen Anwendungsstapel dar. Das Bereitstellungsmodell gibt die Ressourcen und Verbindungen zwischen Ressourcen für die Cloud-Elemente an, die Sie definieren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



4. Zum Hinzufügen einer Ressource zum Bereitstellungsmodell klicken Sie auf **Ressourcen**, und wählen Sie die Ressource aus der Liste aus.
   Die Ressourcen werden auf der Canvas angezeigt. Verschieben Sie die Ressource an eine für das gewünschte Modell geeignete Stelle. Fügen Sie beliebig viele Ressourcen hinzu.
5. Verbinden Sie die Containerressource mit der ersten Ressource, die bereitgestellt werden soll.
   Zum Erstellen einer Verbindung zwischen Ressourcen wählen Sie die übergeordnete Ressource aus, klicken auf das Verbindungsfeld in der Ressource und legen die Verbindung in einer Ressource mit einer gepunkteten Kontur ab. Das System lässt bestimmte Verbindungen nicht zu (z. B. kann ein AWS-Rechenzentrum keine ARM-Ressource hosten).
6. Fügen Sie alle Ressourcen hinzu, die die Blaupause bilden, und verbinden Sie sie.
   Sie müssen alle Ressourcen hinzufügen und verbinden, bevor Sie Vorgänge und Attribute im Abschnitt **Vorgänge** konfigurieren. Während Sie die Ressourcen auf der Registerkarte „Bereitstellungsmodell“ aktualisieren, generiert das System die Cloud-Vorlage: eine vollständige Darstellung der Blaupause als YAML-Skript. Sie können die Darstellung der Cloud-Vorlage für das Bereitstellungsmodell exportieren und später in die Cloud Provisioning and Governance-Anwendung auf einer anderen Instanz importieren.
7. Konfigurieren Sie die Vorgänge, die das System für die Ressourcen durchführt, und die während der Vorgänge zu verwendenden Attribute.
   Standardmäßig werden die Vorgänge **Bereitstellung**, **Stoppen**, **Starten** und **Bereitstellung aufheben** bereitgestellt. Sie können entweder einen vorhandenen Vorgang auswählen oder einen neuen Blaupausenvorgang erstellen.
   - Wählen Sie einen bestehenden Vorgang aus: Wählen Sie im Abschnitt **Vorgänge** das Kontrollkästchen **Bereitstellung** für den Vorgang aus, und klicken Sie auf **Bereitstellung**, um ein Diagramm anzuzeigen. Sie können das Diagramm neu anordnen, indem Sie Vorgänge löschen und hinzufügen. Sie können für die Cloud Provisioning and Governance-Anwendung auf **Alle Pläne optimieren** klicken, um einen für Sie optimierten Vorschlag für einen Plan zu erhalten. Die Cloud Provisioning and Governance-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Anwendung untersucht die von Ihnen erstellte Blaupause und schlägt basierend auf den Attributen, Zuordnungen und Abhängigkeiten der einzelnen Ressourcen einen optimierten Plan zur Ausführung vor. Alle Attribute für den Vorgang **Bereitstellung** werden im Fenster angezeigt. Sie können beliebige Attribute aktivieren oder deaktivieren. Nach der Konfiguration des Vorgangs **Bereitstellung** können Sie den nächsten Vorgang auswählen und seine Attribute nach Bedarf konfigurieren.

- Erstellen Sie einen neuen Blaupausenvorgang: Klicken Sie im Abschnitt **Vorgänge** auf **Neu**. Das Dialogfeld „Neuer Blaupausenvorgang“ wird angezeigt. Geben Sie einen Namen ein, wählen Sie einen Vorgangstyp aus, geben Sie Eingabeparameter für den neuen Vorgang ein, und klicken Sie auf **Speichern**. Der neue Blaupausenvorgang wird im Abschnitt **Vorgänge** angezeigt.

8. Wenn Sie den Entwurf der Blaupause abgeschlossen haben und sie nicht weiter konfigurieren möchten, klicken Sie auf den Umschalter **Entwurf**, um den Plan zu veröffentlichen.
   Eine Nachricht weist darauf hin, dass Ihre Blaupause veröffentlicht wurde. Um mit der Konfiguration der Blaupause fortzufahren, überspringen Sie diesen Schritt.
9. Zum Konfigurieren von Parametern wie Variablensätzen, Regeln und Lebenszyklusvorgängen für das Blaupausenkatalogelement klicken Sie auf die Registerkarte **Katalog** und dann auf den Katalog.
   Der Bildschirm „Cloud-Katalogelement“ wird angezeigt.
10. Klicken Sie auf **Aktualisieren**, wenn Sie Änderungen am Formular vorgenommen haben.
11. Klicken Sie auf **Veröffentlichen**, um die Blaupause zu veröffentlichen.
    Zum Anzeigen aller veröffentlichten Katalogelemente klicken Sie auf der Zielseite der Blaupausen auf **Veröffentlicht**.

Ausführungsplan einen Ressourcenvorgang hinzufügen

Das Basissystem enthält eine große Anzahl vordefinierter Ressourcenvorgänge. In seltenen Fällen können Sie einen benutzerdefinierten Vorgang für eine Ressource hinzufügen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Klicken Sie im Blaupause-Designer auf die Registerkarte **Vorgänge**, und wählen Sie den entsprechenden Blaupausenvorgang aus.
   Beispielsweise können Sie den Vorgang **Bereitstellung** auswählen.
2. Klicken Sie auf **Hinzufügen**.
   Das Dialogfeld „Ressourcenvorgang hinzufügen“ wird angezeigt.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).

Ressource	Wählen Sie eine Ressource für den auszuführenden Vorgang aus.
Schnittstelle	Wählen Sie eine Schnittstelle für die Ressource aus.
Vorgang	Wählen Sie den für den Schritt auszuführenden Vorgang aus. Standardmäßig werden die Vorgänge **Bereitstellung**, **Stoppen**, **Starten** und **Bereitstellung aufheben** bereitgestellt. Sie benötigen mindestens einen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Bereitstellungsvorgang, damit ein Benutzer ein Cloud-Katalogelement bestellen kann.

4. Klicken Sie auf **Absenden**.
   Der neue Vorgang wird dem Vorgangsdiagramm hinzugefügt. Das System fügt die entsprechenden Parameter für den Vorgang hinzu.
5. Klicken Sie auf das Kontrollkästchen **Formularparameter erstellen**, um einen Parameter auszuwählen.
   Die Parameter unterscheiden sich je nach Vorgang. Geben Sie einen Zuordnungsausdruck für den ausgewählten Parameter in das Feld **Zuordnung** ein. Weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden.
6. Klicken Sie auf **Speichern**.

Blaupausenvorgänge parallel ausführen

Sie können Ihre Blaupausenressourcenvorgänge linear oder parallel ausführen.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird
Standardmäßig werden die Vorgänge für Blaupausenressourcen seriell aufgeführt und folgen einer Reihenfolge. Sie können Vorgänge parallel ausführen, indem Sie sie in Verzweigungen anordnen. Identifizieren Sie die in einer Blaupause angegebenen Vorgänge, die keine Abhängigkeiten aufweisen und parallel ausgeführt werden können. Ordnen Sie solche Vorgänge in einer einzelnen Verzweigung an. Der Blaupausendesigner führt diese Vorgänge gemeinsam aus. Wenn in einer Verzweigung ein Fehler auftritt, werden die Vorgänge in der betroffenen Verzweigung nicht mehr ausgeführt. Die Vorgänge in den anderen Verzweigungen, die nicht vom Fehler betroffen sind, werden jedoch weiterhin ausgeführt. Die parallele Art der Ausführung von Vorgängen verkürzt somit die Zeit in Bereitstellungsstapel.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Blueprints**.
2. Klicken Sie auf eine Blaupause, klicken Sie auf die Registerkarte **Modell zur Bereitstellung** und klicken Sie dann auf **Vorgänge**.
   Alle Vorgänge für die Blaupause werden aufgelistet.
3. Klicken Sie auf einen Vorgang, um ein Diagramm anzuzeigen.
   Sie können das Diagramm neu anordnen, indem Sie Vorgänge löschen und hinzufügen.
4. Sie können für die Cloud Provisioning and Governance-Anwendung auf **Plan optimieren** klicken, um einen für Sie optimierten Vorschlag für einen Plan zu erhalten.
   Die Anwendung Cloud Provisioning and Governance betrachtet den von Ihnen erstellten Blueprint. Basierend auf den Attributen, Zuordnungen und Abhängigkeiten der einzelnen Ressourcen schlägt die Anwendung einen optimierten Plan zur Ausführung vor.

Blaupausenattribute

Wenn Sie einer Ressource einen Blaupausenvorgang hinzufügen, fügt das System die entsprechenden Attribute hinzu. Sie können festlegen, ob die Attribute als Katalogeigenschaften im Formular verfügbar gemacht werden sollen, wenn das System den Vorgang ausführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Allgemeine Attribute für den Bereitstellungsvorgang für virtuelle Computer

Attribut	Beschreibung
VmFolderName	Name des Ordners des virtuellen Computers.
ResourceGroupName	Der Name der Ressourcengruppe, zu dem die Ressource gehört.
StackName	Der Name des Stapels, den der Benutzer bereitstellt.
CloudAccount	Das Cloud-Konto, zu dem der Ressourcenstapel gehört.
OSProfile	Das Ressourcenprofil, in diesem Fall das Betriebssystemprofil, auf dem die Cloud-Ressource basiert.
DiscoverAndAttachIP	Sucht nach einer freien elastischen IP-Adresse und weist sie einem virtuellen Computer in AWS zu. Wenn eine VM auf einer VPC in AWS bereitgestellt wird, erhält sie standardmäßig keine öffentliche IP. Wenn keine elastischen IPs verfügbar sind, kann der VM keine IP zugewiesen werden.

⚠ **Warnung:** Es wird empfohlen, *KeyPreference* nicht zu verwenden. Wenn Sie das Attribut verwenden, setzen Sie *KeyPreference* nicht auf `Benutzer`.

Blaupausenregel konfigurieren

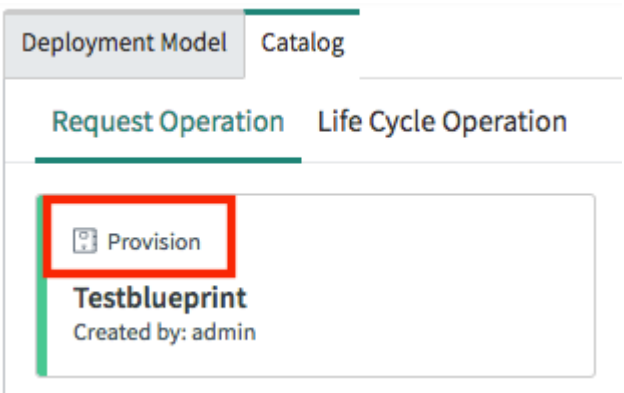
Konfigurieren Sie eine Regel, die Aktionen enthält, die das System für Blaupausenattribute durchführen kann.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Öffnen Sie eine Blaupause, die das Attribut enthält, für das Sie eine Regel erstellen möchten.
2. Klicken Sie auf der Registerkarte **Katalog** auf den Vorgang, der das Attribut enthält, z. B. den Bereitstellungsvorgang.



3. Klicken Sie in der zugehörigen Liste „Variablensätze“ im Formular „Cloud-Katalogelement“ auf den Namen des Variablensatzes, der die Variable enthält.
4. Klicken Sie in der zugehörigen Liste „Cloud-Variablen“ im Formular „Variablensatz“ auf den Namen der Variable, für die Sie eine Regel erstellen möchten.
5. Klicken Sie in der zugehörigen Liste „Regeln“ auf **Neu**, und füllen Sie das Formular aus.

Automatische Übersetzung

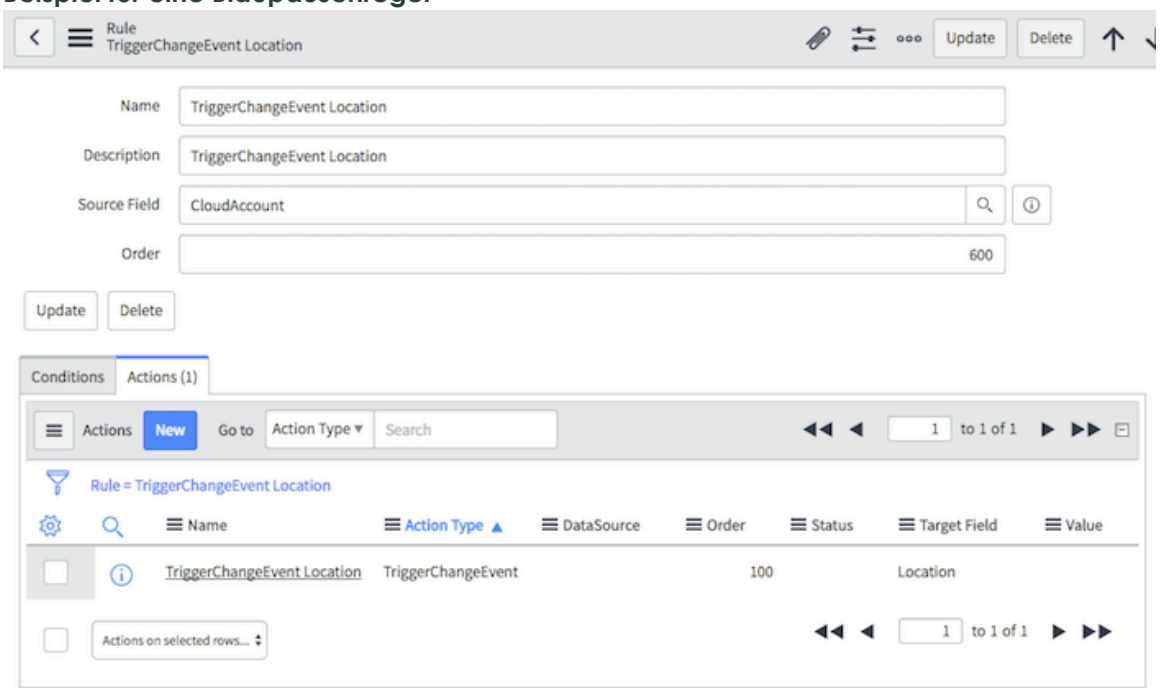
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name Beschreibung	Geben Sie einen Namen und eine Beschreibung ein.
Reihenfolge	Geben Sie eine Nummer ein, die dem System mitteilt, welcher Datensatz zuerst im Verhältnis zu anderen ausgewertet werden soll. Der Datensatz mit der niedrigsten Nummer wird zuerst ausgeführt.

6. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

Example:
Diese Beispielregel basiert auf der Eigenschaft *CloudAccount* und enthält eine Aktion, die das System anweist, die Liste der Standorte zu aktualisieren, wenn der Benutzer das Cloud-Konto ändert.

Beispiel für eine Blaupausenregel



Nächste Maßnahme
Konfigurieren Sie eine optionale Bedingung und eine obligatorische Aktion.

Blaupausenregelbedingung konfigurieren

Konfigurieren Sie die Bedingung für eine Eventregel eines Blaupausenformulars, die bestimmt, wann die Aktionen in der Regel ausgeführt werden können. Bedingungen sind optional.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Öffnen Sie eine Regel für eine Variable in einer Blaupause.
2. Klicken Sie in der zugehörigen Liste „Bedingungen“ auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).

Feld	Beschreibung
Operand	Geben Sie die Eigenschaft ein, für die Sie die Bedingungsauswertung durchführen können. Beispiel: Wenn Ihre Blaupause über eine Eigenschaft verfügt, die den Wert eines Rechenzentrums enthält, geben Sie den Namen der Eigenschaft hier ein.
Operator	Wählen Sie einen Operator aus, der den Operanden auswertet.
Wert	Geben Sie einen Wert ein, dem die ausgewertete Eventregel entsprechen muss.
Bedingungstyp	Wenn Sie mehrere Bedingungen konfigurieren, wählen Sie den logischen Operator aus, der bestimmt, wie das System die Bedingung in Bezug auf die nächste Bedingung auswertet (die nächste Bedingung wird durch das Feld **Auftrag** bestimmt): ◦ **UND**: Diese Bedingung muss die nächste Bedingung erfüllen, bevor die Richtlinie ausgeführt werden kann. ◦ **ODER** : Diese Bedingung oder die nächste Bedingung, die den Kriterien entspricht, kann die Ausführung der Richtlinie ermöglichen. Wenn Sie keine Option auswählen, wird **UND** standardmäßig verwendet.
Reihenfolge	Geben Sie eine Nummer ein, die dem System mitteilt, welcher Datensatz zuerst im Verhältnis zu anderen ausgewertet werden soll. Der Datensatz mit der niedrigsten Nummer wird zuerst ausgeführt.
Status	Behalten Sie den Status „Aktiv“ bei, damit die Bedingung vom System verarbeitet wird. Ändern Sie den Status in „Inaktiv“, wenn Sie nicht möchten, dass das System die Bedingung verarbeitet.

4. Klicken Sie auf **Absenden**.

Example:
Diese Beispielbedingung gilt, wenn der Benutzer das AWS-Rechenzentrum für die Eigenschaft „Logical_Datacenter“ auswählt, die ein Feld im Katalogelementformular ist:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine Blaupausenbedingung

Nächste Maßnahme

Blaupausenaktion konfigurieren

Blaupausenaktion konfigurieren

Konfigurieren Sie Aktionen, die das System ausführt, wenn Attributaktionen von Blaupausenformularen oder Eventaktionen ausgelöst werden. Sie können Aktionen konfigurieren, z. B. ein Feld als Pflichtfeld festlegen, ein Feld anzeigen oder ausblenden oder ein Feld automatisch ausfüllen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Öffnen Sie eine Regel für eine Eigenschaft oder ein Ereignis in einer Blaupause.
2. Klicken Sie in der zugehörigen Liste **Aktionen** auf **Neu**, und füllen Sie das Formular aus.

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name.
Aktionstyp	Wählen Sie einen Aktionstyp aus: ◦ **Neu laden**: ◦ **Anzeigen**: ◦ **Ausblenden**: ◦ **MakeMandatory**: ◦ **MakeNonMandatory**: ◦ **TriggerChangeEvent**: ◦ **SetValue**:
Datenquelle	Wählen Sie einen Aktionstyp aus: ◦ **Cloud-Konto neu laden**: ◦ **Cloud-Standort neu laden**: ◦ **Kontingent prüfen**: ◦ **Ressourcenprofil neu laden**: ◦ **Aus Profil neu laden**:
Zielfeld	Geben Sie den Namen des Felds im Formular ein, für das die Aktion gilt. Wenn Sie beispielsweise **TriggerChangeEvent** für den Aktionstyp ausgewählt haben und sich im Formular

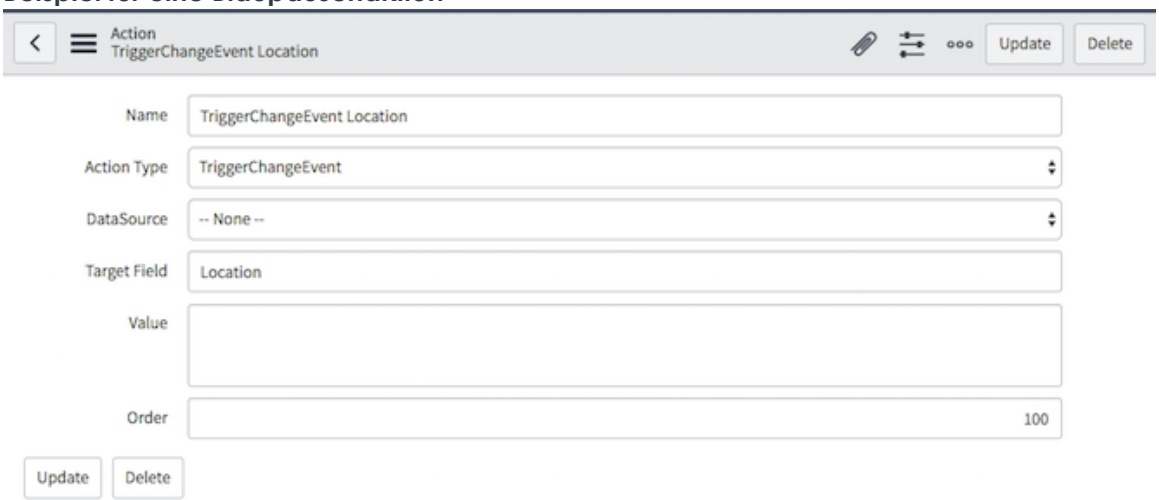
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	etwas ändert, ändert sich der Wert des Feldes, wie in der Blaupausenregel angegeben.
Wert	Geben Sie einen optionalen Wert ein, den Sie dem Zielfeld zuweisen möchten. Wenn Sie beispielsweise **SetValue** für das Feld **Aktionstyp** ausgewählt haben und den **Ressourcengruppennamen** aktualisieren möchten, können Sie den Wert `${ResourceGroup}` verwenden, der die Namen der Ressourcengruppen aus der Blaupause abruft.
Reihenfolge	Geben Sie eine Nummer ein, die dem System mitteilt, welcher Datensatz zuerst im Verhältnis zu anderen ausgewertet werden soll. Der Datensatz mit der niedrigsten Nummer wird zuerst ausgeführt.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.
4. Wahlweise: Geben Sie einen **Schlüssel** und **Wert** in die zugehörige Liste „KeyValues“ ein. Der Wert im Feld **Wert** wird auf das Attribut im Feld **Schlüssel** angewendet.
5. Erstellen Sie so viele Aktionen wie nötig.

Example:
Diese Beispielaktion gilt für das Beispiel einer Blaupausenregel, das auf dem Attribut „CloudAccount“ basiert. Diese Aktion weist das System an, die Liste der Standorte zu aktualisieren, wenn der Benutzer das Cloud-Konto ändert.

Beispiel für eine Blaupausenaktion



Nächste Maßnahme
Veröffentlichen Sie einen Blueprint als Cloud-Katalogelement.

Formularkonfiguration mit Blaupausen

Blaupausen steuern, was dem Benutzer auf dem Katalogbestellformular angezeigt wird. Sie können das Formular so konfigurieren, dass Felder ein- oder ausgeblendet werden, Felder mit Standardwerten ausgefüllt werden und andernfalls basierend auf Kriterien ein eindeutiges Formular für den Benutzer erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis:

- Beginnend mit Orlando sind Cloud Provisioning-Blaupausen für Instanzen verfügbar, die von einem früheren Release aktualisiert wurden. Sie können jedoch keine neuen Blaupausen erstellen. Vorhandene Blaupausen und Katalogelemente aus diesen Blaupausen bleiben davon unberührt und funktionieren weiterhin.
- Verwenden Sie Cloud-Vorlagen für Cloud Provisioning, um Katalogelemente anstelle von Blaupausen zu erstellen. Mithilfe von Cloud Provisioning Cloud-Vorlagen können Sie die Spezifikationssyntax für Azure ARM, AWS CFT, Google Deployment Manager (GDM) und Terraform in Cloud-Katalogelemente zur Ausführung Ihrer Cloud-Bereitstellungsorchestrierung einbinden.

Sie können außerdem die Werte in Formularfeldern mithilfe von Richtlinien ändern. Beispiele finden Sie unter Cloud-Richtlinie erstellen und Richtlinienaktionsskript erstellen.

Komponenten der Blaupausenformularkonfiguration

Blaupausen verwenden diese Komponenten, um zu steuern, wie das System Katalogformularfelder verwendet:

- Katalogvariablen definieren die grundlegende Struktur jedes Felds in Katalogbestellformularen.
- Regeln geben eine Aktion an, die das System für ein Feld ausführt, wenn eine Bedingung erfüllt ist.
- Skripts fragen Informationen aus dem System ab, die Sie benötigen, um den Kataloganforderer anzuzeigen, Formularfelder auszufüllen und die von Benutzern übermittelten Daten zu verarbeiten.
- UI-Gruppen fassen zugehörige Felder auf einer Registerkarte zusammen. Benutzer können Registerkarten durchlaufen, um alle Formularfelder auszufüllen.

Beginnen Sie hier

Diese Aufgaben zeigen Ihnen die Grundlagen der Formularkonfiguration mit Blaupausen:

- Bestellformular für Cloud-Katalogelement Felder hinzufügen
- Standardwerte für die Sichtbarkeit von Cloud-Katalogelementen steuern
- Variablensatz für Cloud Provisioning and Governance erstellen

Beispiele

Diese Beispiele führen Sie durch die Formularkonfiguration basierend auf einem bestimmten Ziel: Konfigurationsbeispiele für das Cloud-Katalogformular.

Bestellformular für Cloud-Katalogelement Felder hinzufügen

Sie können einem Cloud-Katalogformular Felder hinzufügen, wenn der Benutzer zusätzliche Informationen eingeben soll, die über das hinausgehen, was ein Standard-Blueprint bereitstellt.

Vorbereitungen

- Sie benötigen eine Blaupause, die Sie im Katalog veröffentlicht haben. Die Blaupause sollte im Entwurfsstatus vorliegen. Lesen Sie Cloud Provisioning-Blaupause erstellen, wenn Sie diese Voraussetzung nicht erfüllt haben.
- Standardmäßig werden Cloud-Elemente im Cloud-Katalog anstatt im Standardservicekatalog Ihrer Instanz angezeigt. Blaupausen verwenden jedoch

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

mehrere Funktionen aus dem Standardservicekatalog. Es wird empfohlen, sich mit der Funktionsweise des Servicekatalogs vertraut zu machen. Informationen zu den ersten Schritten finden Sie unter Servicekatalog .

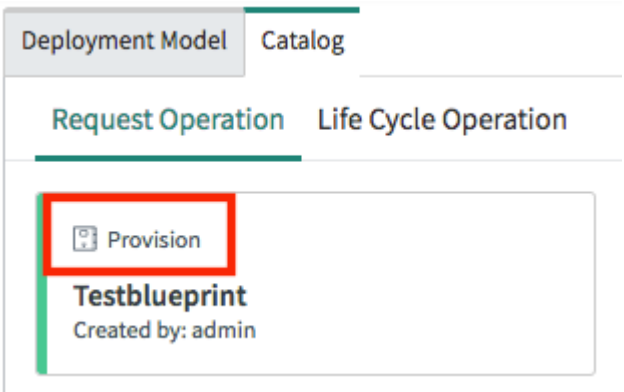
- Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Felder werden in Blaupausen als Variablen dargestellt. Zum Hinzufügen eines Felds fügen Sie einem Vorgang in einer Blaupause eine Variable hinzu.

Prozedur

1. Öffnen Sie eine Blaupause, die Sie bereits erstellt haben.
2. Klicken Sie auf die Registerkarte **Katalog**, und klicken Sie dann auf den Vorgang, dem Sie die Variable hinzufügen möchten, z. B. Bereitstellung.



Das Formular „Cloud-Katalogelement“ wird geöffnet.

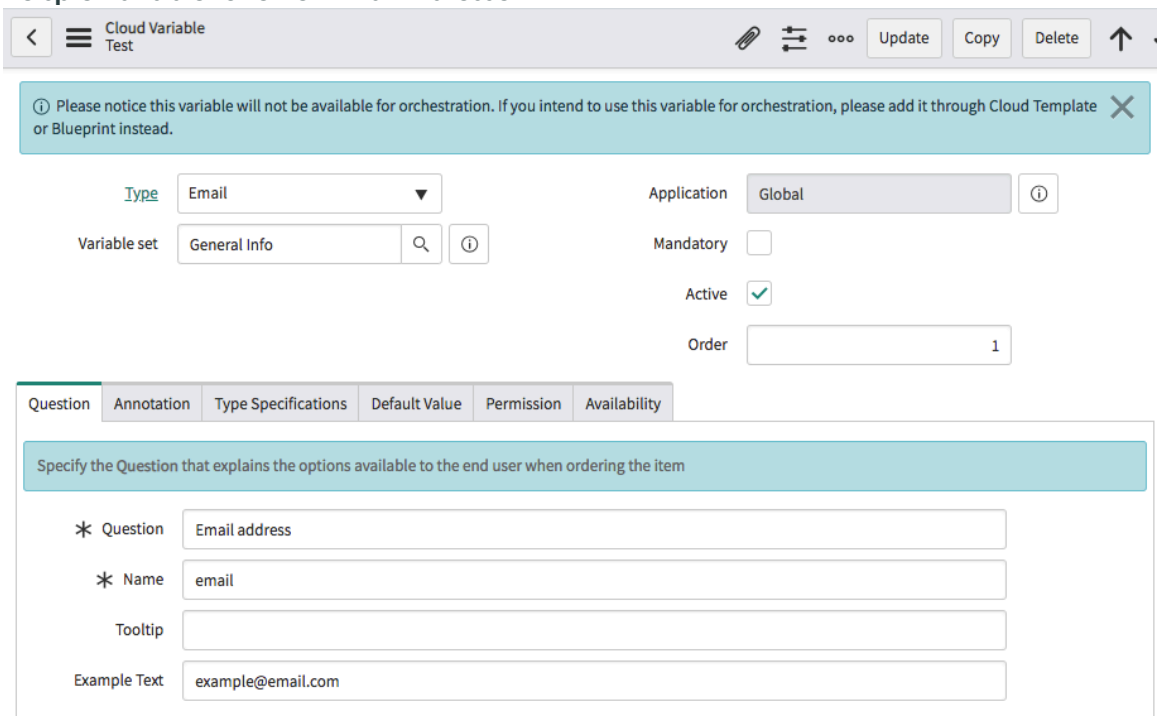
3. Klicken Sie in der zugehörigen Liste „Variablensätze“ unten auf den Satz, zu dem die Variable gehören soll.
Klicken Sie beispielsweise auf „Allgemeine Informationen“, ein Standardvariablensatz für alle Blaupausen, damit das Feld auf der ersten Registerkarte des Katalogbestellformulars angezeigt wird.
Das Formular „Variablensatz“ wird geöffnet.
4. Klicken Sie in der zugehörigen Liste „Cloud-Variablen“ unten auf **Neu**.
5. Füllen Sie die wichtigen Formularfelder aus, z. B.:

Feld	Beschreibung
Typ	Wählen Sie den Typ der Variable aus, z. B. **Einzeiliger Text** für ein Textfeld, **Kontrollkästchen** oder **Datum**.
Registerkarte „Frage“	Geben Sie unter **Frage** einen Namen ein. Dies ist der Wert, den der Benutzer auf dem Katalogbestellformular für das Feld sieht. Das Feld **Name**, das der tatsächliche Name der Variable ist, wird automatisch mit dem gleichen Wert in Kleinbuchstaben ausgefüllt.
Andere Registerkarten	Füllen Sie andere Felder auf den verbleibenden Registerkarten aus, um die Sichtbarkeit des Felds, den Formularhilfetext, den Standardwert und die Zugriffsrechte zu steuern.

Hinweis: Diese Variable ist nicht für die Orchestrierung verfügbar. Wenn Sie diese Variable für die Orchestrierung verwenden möchten, fügen Sie sie stattdessen über Cloud-Vorlage oder Blaupause hinzu.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispielvariable für eine E-Mail-Adresse

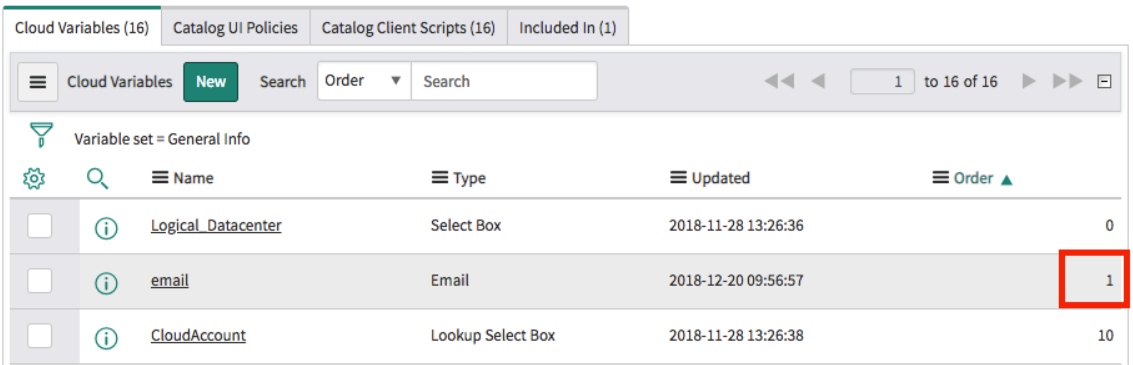


6. Klicken Sie auf **Absenden**.

   Das Formular „Variablensatz“ wird geöffnet und zeigt die neue Variable in der zugehörigen Liste „Cloud-Variablen“ an.

7. Ändern Sie den Wert in der Spalte **Reihenfolge**, um die Position des Felds auf dem Formular zu steuern.

   Hinweis: Ein niedrigerer Wert für die Reihenfolge verschiebt das Feld im Formular nach oben und umgekehrt.

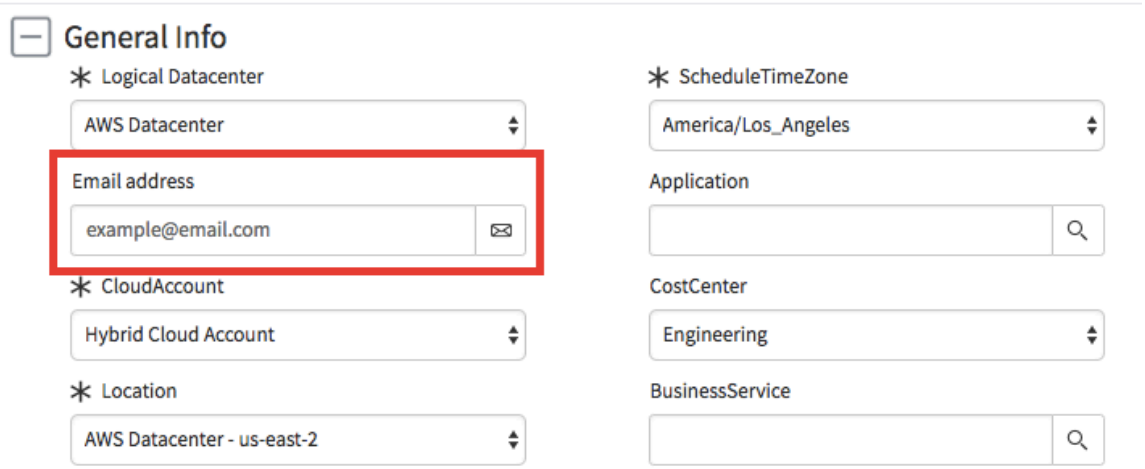


   In diesem Beispiel ist die Reihenfolge auf **1** festgelegt, was bedeutet, dass das Feld „E-Mail-Adresse“ nach dem Feld „Logisches Rechenzentrum“ und vor dem Feld „Cloud-Konto“ angezeigt wird.

8. Klicken Sie im Formularbanner oben links auf **Testen**, um sich eine Vorschau des Bestellformulars anzusehen, wie es einem Benutzer im Cloud-Katalog angezeigt würde. Das Formular wird mit dem von Ihnen erstellten neuen Feld angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Klicken Sie oben links im Formular auf den Zurück-Pfeil.
10. Schalten Sie das Katalogelement auf **Veröffentlichen** um.

Standardwerte für die Sichtbarkeit von Cloud-Katalogelementen steuern

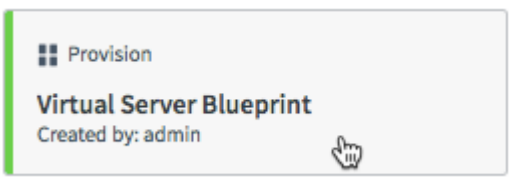
Mithilfe von Blaupausen können Sie steuern, wie Formularfelder Benutzern im Cloud-Katalog angezeigt werden. Beispielsweise können Sie steuern, wo die Felder Benutzern im Katalogelementformular angezeigt werden und ob sie schreibgeschützt oder obligatorisch sind.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Öffnen Sie die zu ändernde Blaupause, und schalten Sie sie von **Veröffentlicht** auf **Entwurf** um.
2. Klicken Sie auf die Registerkarte **Katalog**.
   Die Unterregisterkarte „Anforderungsvorgang“ wird geöffnet und zeigt die veröffentlichten Katalogelemente für den Bereitstellungsvorgang an.
3. Klicken Sie auf die Kachel **Bereitstellung** für das Katalogelement.
   Die Einstellungen im Bereitstellungsvorgang steuern das Formular, das dem Benutzer bei der ersten Anforderung des Elements angezeigt wird, bevor es bereitgestellt wird.



   Das Formular „Cloud-Katalogelement“ wird geöffnet.
4. Klicken Sie in der zugehörigen Liste „Variablensätze“ unten auf den Satz, zu dem die Variable gehören soll.
   Klicken Sie beispielsweise auf **Allgemeine Informationen**, ein Standardvariablensatz für alle Blueprints, damit das Feld auf der ersten Registerkarte des Katalogbestellformulars angezeigt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Wählen Sie im Formular „Variablensatz“ die Variable aus, die Sie ändern möchten.
6. Führen Sie im Formular „Cloud-Variable“ eine der folgenden Aktionen aus.

An	Aktion
Feld zum Pflichtfeld machen	Markieren Sie die Checkbox **Pflichtfeld**. Entfernen Sie das Häkchen aus dem Kontrollkästchen, um das Feld optional zu machen.
Feld schreibgeschützt machen	Klicken Sie auf die Registerkarte **Verfügbarkeit**, und aktivieren Sie dann das Kontrollkästchen **Schreibgeschützt**. Entfernen Sie das Häkchen aus dem Kontrollkästchen, um das Feld bearbeitbar zu machen. Verwenden Sie diese Option, um automatisch einen Wert im Feld auszufüllen, den der Benutzer nicht ändern kann.
Feld ein- oder ausblenden	Klicken Sie auf die Registerkarte **Verfügbarkeit**, und aktivieren Sie dann das Kontrollkästchen **Sichtbar**.
Feld auf eine andere Registerkarte verschieben	Wählen Sie einen anderen **Variablensatz** aus. **Allgemeine Informationen** und **Bereitstellung** werden im Basissystem bereitgestellt, und Sie können zusätzliche Formular-UI-Gruppen konfigurieren. Informationen zum Hinzufügen einer neuen Registerkarte für die Organisation von Feldern im Katalogelement finden Sie unter Variablensatz für Cloud Provisioning and Governance erstellen.
Standardwert festlegen	Klicken Sie auf die Registerkarte **Standardwert**, und geben Sie den Wert unter **Standardwert** ein. Wenn das Feld nicht schreibgeschützt ist, können Benutzer den Wert im Cloud-Katalogformular ändern. Referenzfelder müssen die Sys-ID des Datensatzes verwenden, der den Standardwert darstellt.
Hilfe für den Benutzer hinzufügen	Führen Sie einen der folgenden Schritte aus: ◦ Klicken Sie auf die Registerkarte **Frage**, und fügen Sie im Feld **Tooltip** einen Wert hinzu, um eine Blase mit dem Text anzuzeigen, wenn der Benutzer den Mauszeiger über das Feld bewegt. ◦ Klicken Sie auf die Registerkarte **Anmerkung**, wählen Sie **Hilfe anzeigen** aus, und geben Sie dann Werte in den Feldern **Hilfetext** oder **Anweisungen** ein, um über dem Feld zusätzlichen Text für den Benutzer anzuzeigen.

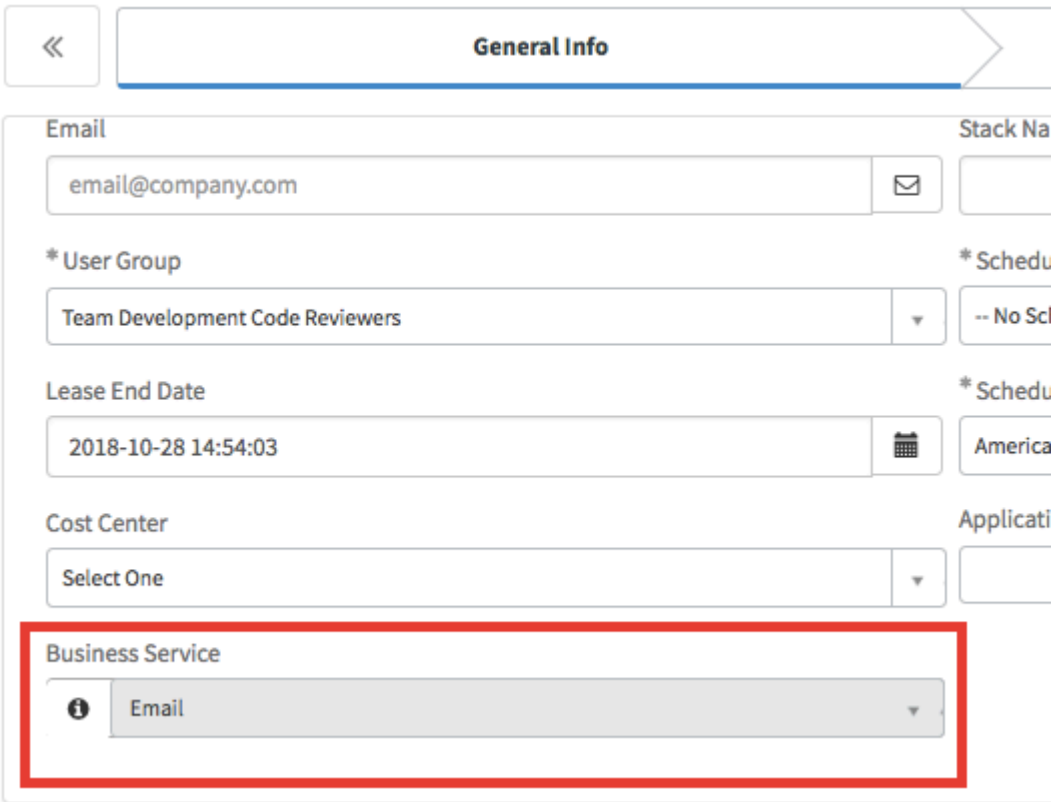
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Aktualisieren**.
8. Schalten Sie das Katalogelement auf **Veröffentlichen** um.

Example:
In diesem Beispiel gilt für das Feld „Business Service“ Folgendes:

- Es wird basierend auf der Sys-ID des Datensatzes mit dem im Datensatz des Business Service „E-Mail“ in der Tabelle „cmdb_ci_service“ ausgefüllt.
- Es ist schreibgeschützt, sodass Benutzer es nicht ändern können.
- Es ist obligatorisch, da es als erforderlich erachtet wird, bevor das System die virtuelle Ressource bereitstellen kann.
- Es enthält Hilfetext, der dem Benutzer mitteilt, dass die Standardauswahl „E-Mail“ ist.

Auf dem Katalogbestellformular wird das Feld wie in der folgende Grafik angezeigt:



Konfigurationsbeispiele für das Cloud-Katalogformular

Mehrere Beispiele werden bereitgestellt, um Ihnen das Verständnis zu erleichtern, wie Bestellformulare des Cloud-Katalogs bearbeitet werden. Diese Beispiele decken Blaupausenregeln, Blaupausenvariablen und Blaupausenformular-UI-Gruppen ab.

Beispiel	Ziel	Verwendete Blaupausenkomponenten
Standort basierend auf dem Cloud-Konto ausfüllen	Verwenden Sie vorhandene Blaupausenregeln, um zu veranschaulichen, wie das Feld	Dieses Beispiel veranschaulicht die Regeln.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel	Ziel	Verwendete Blaupausenkomponenten
	„Standort“ basierend auf dem vom Benutzer ausgewählten Cloud-Konto ausgefüllt wird.	
Feld aus einem Cloud-Katalogformular entfernen	Blenden Sie das Feld „Kostenstelle“ im Katalogformular aus, wenn der Kataloganforderer zur Datenbankgruppe gehört.	Dieses Beispiel veranschaulicht Folgendes: • Regeln • Ressourcenpools
Stapelnamen mit einem Skript ausfüllen	Geben Sie dem Kataloganforderer einen vordefinierten Stapelnamen, der die ID des Kataloganforderers enthält. Das Feld kann weiterhin vom Benutzer bearbeitet werden, damit er es bei Bedarf ändern kann.	Dieses Beispiel veranschaulicht Folgendes: • Regeln • Ressourcenpools • Geskriptete Werte
Bestellformular für Cloud-Katalogelement Felder hinzufügen	Erstellen Sie eine Katalogvariable und -eigenschaft, und verwenden Sie diese zum Veröffentlichen eines neuen Felds in einem Formular.	Dieses Beispiel veranschaulicht Folgendes: • Katalogvariablen • Feldreihenfolge • Regeln • Ressourcenpools • Geskriptete Werte
Standardwerte für Cloud-Katalogformularfelder festlegen	Legen Sie einen Standardwert für eine Eigenschaft und eine Blaupausenregel fest.	Dieses Beispiel veranschaulicht Folgendes: • Standardvariablen • Regeln
UI-Gruppe mit zusätzlichen Feldern hinzufügen	Gruppieren Sie Katalogformularfelder in Registerkarten, um das Formular besser zu organisieren und den Benutzer von einem Einstellungssatz zu einem anderen zu führen.	Dieses Beispiel veranschaulicht die UI-Gruppen (Registerkarten).

Standort basierend auf dem Cloud-Konto ausfüllen

Dieses Beispiel führt Sie durch einen vorhandenen Satz von Blaupausenregeln, der standardmäßig von Cloud Provisioning and Governance bereitgestellt wird.

Vorbereitungen

Bevor Sie diesem Beispiel folgen können, müssen Sie mit dem Erstellen von Blaupausen und Blaupausenregeln vertraut sein. Sehen Sie sich folgende Ressourcen an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

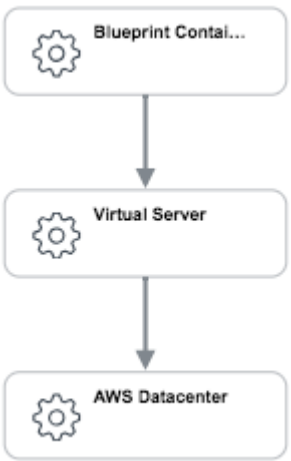
- Blaupausen für die Cloudbereitstellung
- Cloud Provisioning-Blaupause erstellen
- Blaupausenregel konfigurieren

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

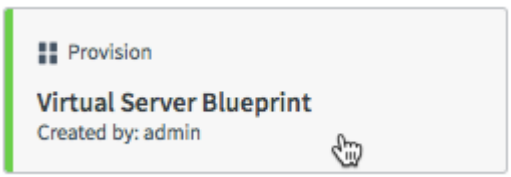
Das Ziel dieses Beispiels ist es, Ihnen zu zeigen, wie ein Standardsatz von Blaupausenregeln die Aufgabe erfüllt, das Feld „Standort“ basierend auf dem Cloud-Konto auszufüllen. Da dieses Beispiel Sie durch die Standarddaten führt, müssen Sie keine Datensätze erstellen, wenn Sie diese Schritte ausführen.

Diese Blaupause, die einen virtuellen Server umfasst, der in einem AWS-Rechenzentrum bereitgestellt werden kann, wird zur Illustration des Beispiels verwendet:



Prozedur

1. Öffnen Sie eine ähnliche Blaupause mit einem virtuellen Server oder ähnlichem.
2. Klicken Sie auf dem Blaupausenformular auf die Registerkarte **Katalog**, und klicken Sie dann auf die Kachel, die den Vorgang **Bereitstellung** darstellt.



3. Klicken Sie auf die Schaltfläche **Allgemeine Informationen** Variablensatz in der zugehörigen Liste „Variablensätze“.
4. Klicken Sie auf die Variable **CloudAccount**, um das Cloud-Variablenformular zu öffnen.

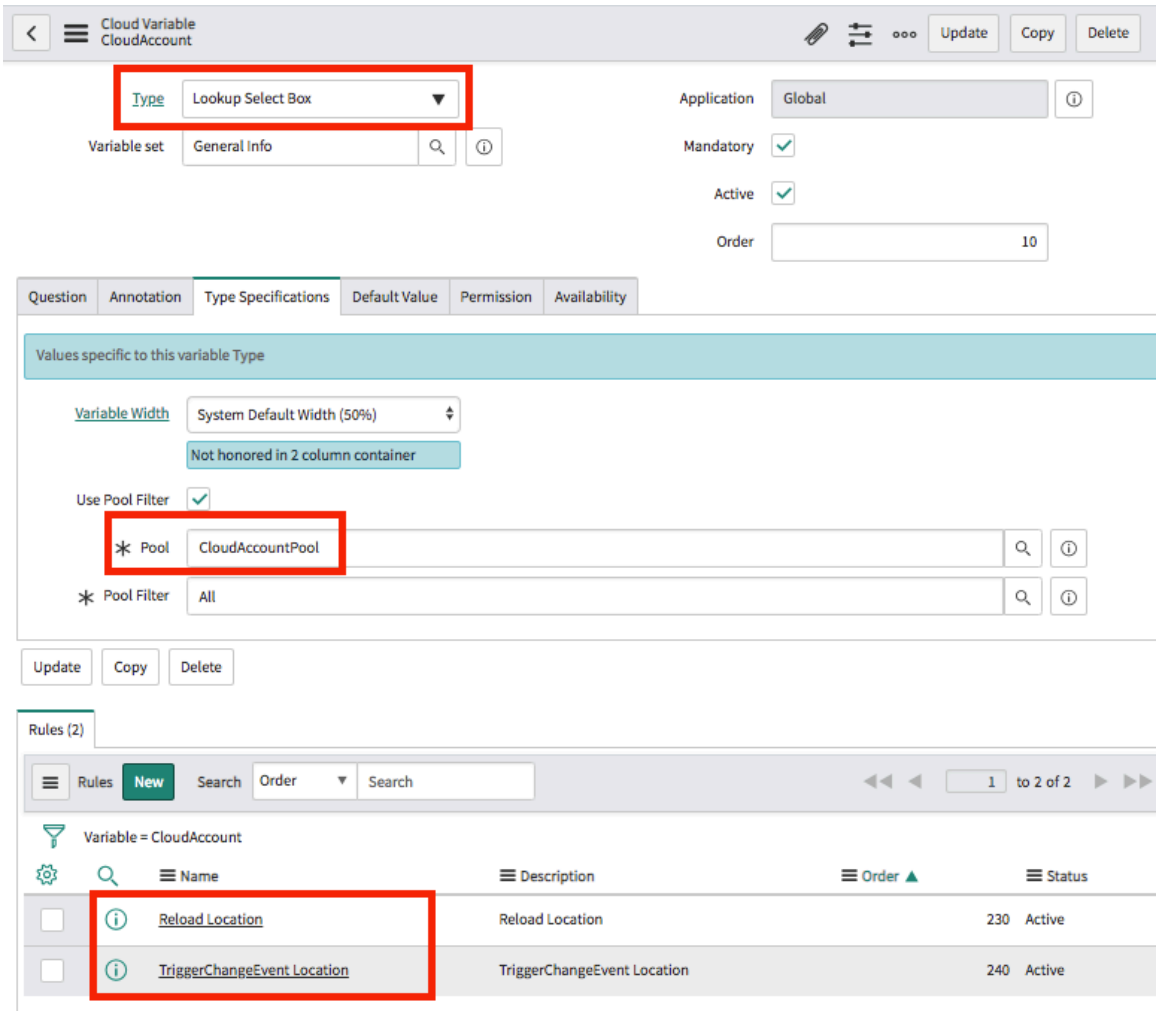
   Beachten Sie folgende Elemente:

   - In der zugehörigen Liste „Regeln“ unten werden zwei Regeln bereitgestellt:
     - „ReloadLocation“ lädt den Wert im Feld „Umzug“ neu. Diese Regel wird zuerst ausgeführt, da sie eine niedrigere Reihenfolgennummer als die andere Regel hat.
     - „TriggerChangeEvent Location“ weist das System an, die Aktionen für die Regeln auszulösen, die bereits für die Standortvariable konfiguriert sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Das Feld **Auswahlfeld für Suche** gibt an, dass das Feld „Cloud-Konto“ eine Auswahl für den Benutzer bietet. Die Optionen, die der Benutzer auswählen kann, stammen aus dem CloudAccountPool im Feld **Typspezifikationen**.

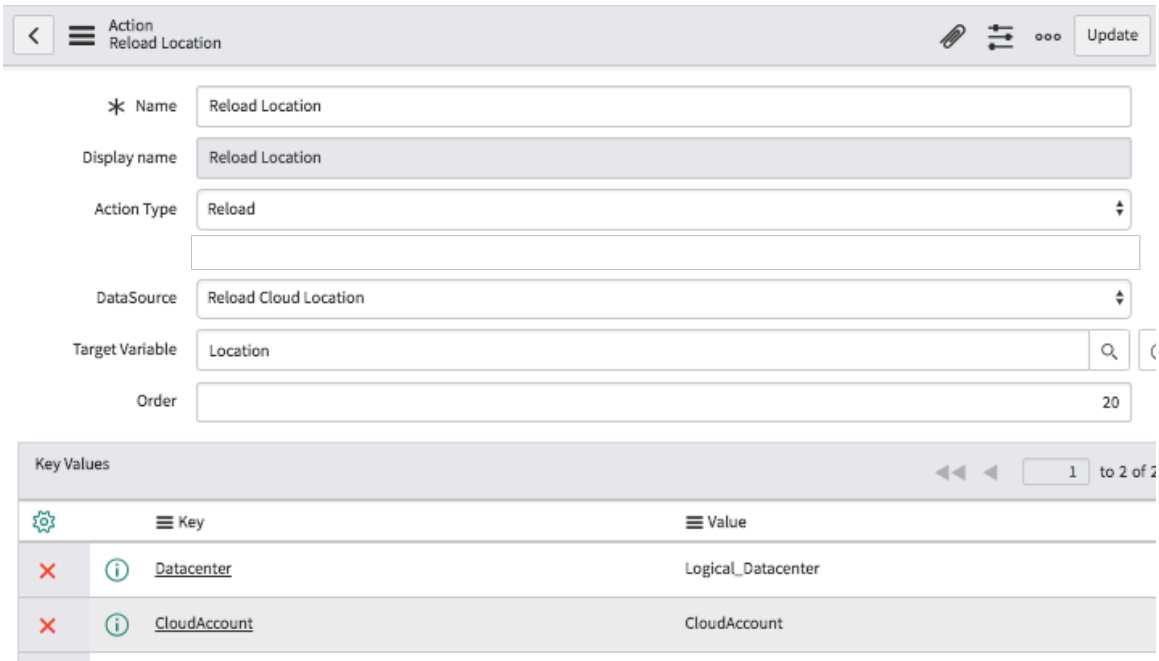


5. Klicken Sie auf die Regel **Standort neu laden**, und klicken Sie dann in der zugehörigen Liste „Aktionen“ auf die Aktion **Standort neu laden**.

   Beachten Sie folgende Elemente:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der **Aktionstyp** ist **Neu laden**, was das System anweist, das Katalogelementformular neu zu laden, sodass ein neuer Wert für das in der **Zielvariable** angegebene Feld (der**Standort**), ausgefüllt werden kann.



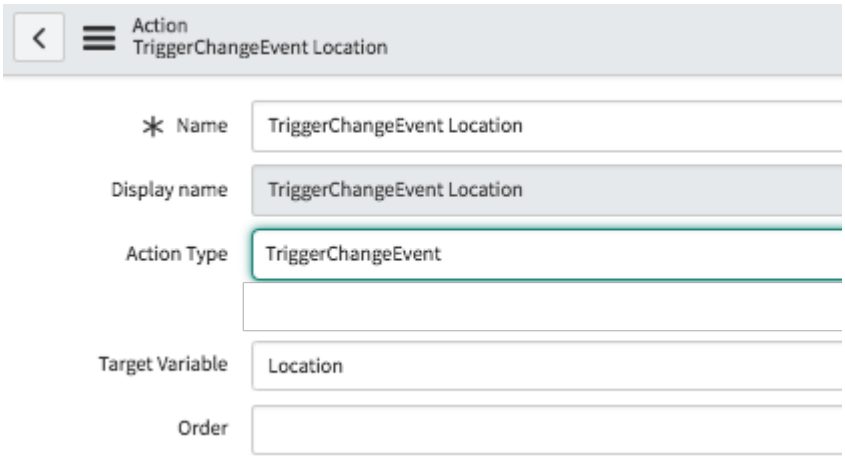
- Das Feld **DataSource** weist das System an, den Standort neu zu laden.
- Die Liste **KeyValues**, die nur verwendet wird, wenn Sie einen Aktionstyp **Neu laden** angeben, legt fest, dass der Benutzer über das Formular das Cloud-Konto übergibt. Das Cloud-Konto ist erforderlich, um den richtigen Wert für den Standort neu zu laden, da der Standort aus einem Pool geladen wird. Dieser Pool verfügt über einen Filter, der die Eingabe des Cloud-Kontos erfordert, um die richtigen Standortoptionen zurückzugeben.

6. Navigieren Sie zurück zum Katalogeigenschaftsformular „CloudAccount“, und öffnen Sie die andere Regel: **TriggerChangeEvent Location**.
7. Klicken Sie auf die zugehörige Liste **Aktionen**, öffnen Sie die Aktion **TriggerChangeEvent Location**, und klicken Sie dann in der zugehörigen Liste „Aktionen“ auf die Aktion **TriggerChangeEvent Location**.

   Beachten Sie folgende Elemente:

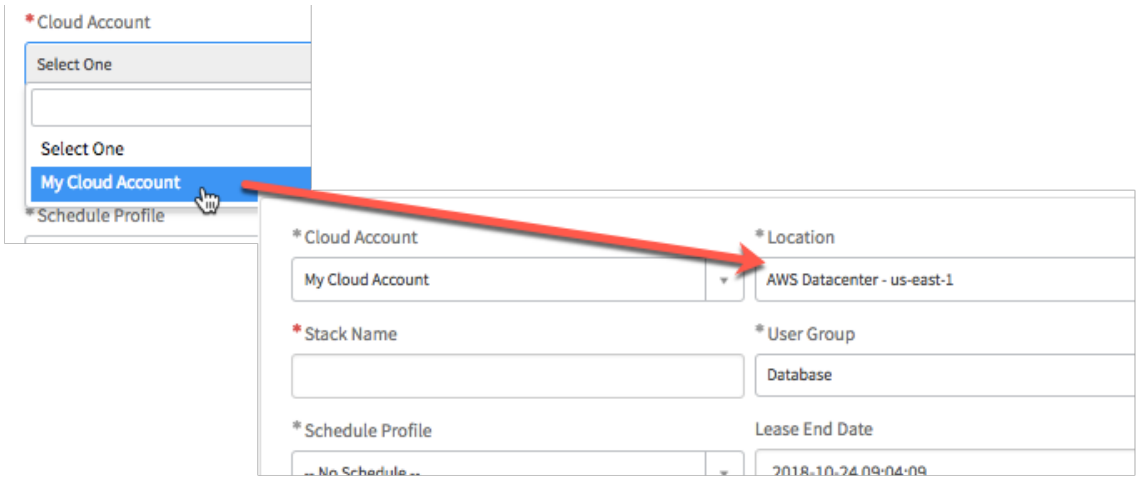
   - Der **Aktionstyp** ist **TriggerChangeEvent**, was das System anweist, die Aktionen für die Regeln auszulösen, die bereits für die Standorteigenschaft konfiguriert sind. Standardmäßig sind bereits mehrere Regeln für die Standorteigenschaft konfiguriert. Dazu gehören Regeln, die andere Felder wie **BS-Profil**, **Netzwerk** usw. neu laden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Es sind keine **KeyValues** erforderlich, da diese Aktion keine Aktion zum erneuten Laden ist.

Das Ergebnis dieser beiden Regeln für das Attribut „CloudAccount“ wird im folgenden Beispiel veranschaulicht:



8. Führen Sie diese Schritte aus, um zu sehen, warum das System den Wert **AWS-Rechenzentrum – us-east-1** im Feld **Standort** ausgefüllt hat und wie das System bestimmt, welcher Standort mit dem Wert von **Mein Cloud-Konto** verknüpft ist:

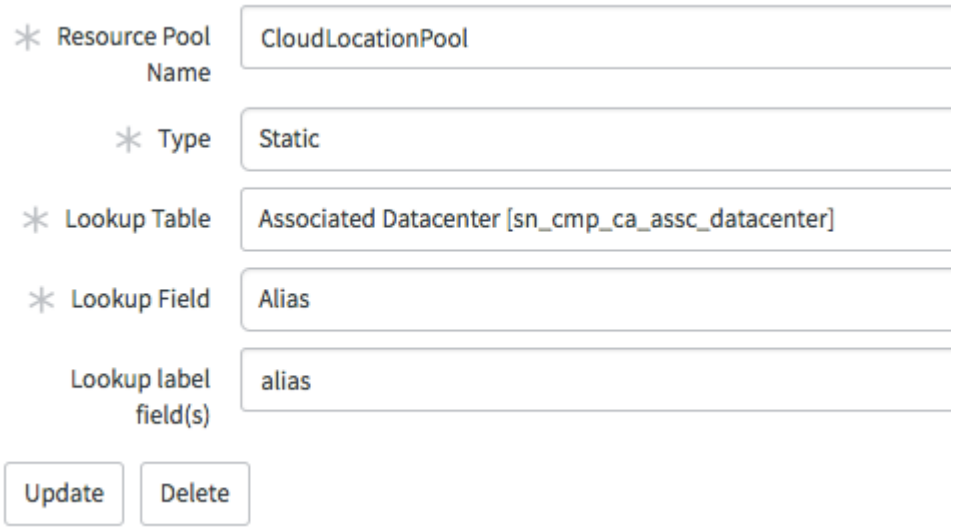
   a. Öffnen Sie in der gleichen Blaupause den Variablensatz **Allgemeine Informationen** und dann den Parameter **Standort**.

   b. Klicken Sie auf die Registerkarte **Typspezifikationen**.

      Beachten Sie die Werte, die für das Feld **Standort** aus dem *CloudLocationPool*-Ressourcenpool ausgefüllt werden können.

   c. Navigieren zu **Verwalten** > **Ressourcenpools**, öffnen Sie **CloudLocationPool**, und beachten Sie die folgenden Elemente:

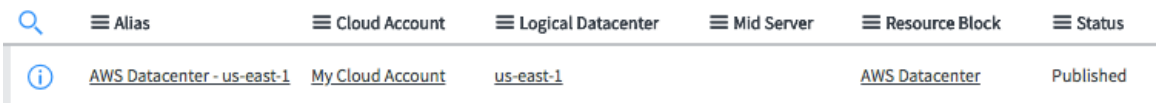
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



- Die Standorte stammen aus den Datensätzen in der **Suchtabelle**, die in diesem Beispiel die Tabelle **Zugeordnetes Rechenzentrum [sn_cmp_ca_assc_datacenter]** ist.
- Der tatsächliche Wert, der Benutzern im Feld „Standort“ auf dem Katalogelementformular angezeigt wird, stammt aus dem **Suchfeld**. In diesem Beispiel gibt das **Suchfeld** die Spalte „Alias“ aus der Tabelle „Zugeordnetes Rechenzentrum“ [sn_cmp_ca_assc_datacenter] an. Die Spalte **Alias** enthält die tatsächlichen, vom Benutzer lesbaren Namen für alle Standorte.

d. Wechseln Sie zur Standardoberfläche Ihrer Instanz, nicht zum Adminportal, und geben Sie `sn_cmp_ca_assc_datacenter.list` in den Navigationsfilter ein.

Die Liste der Rechenzentren, die bereits Cloud-Konten zugeordnet sind, wird angezeigt.



Beachten Sie, dass das Cloud-Konto **Mein Cloud-Konto** bereits **AWS-Rechenzentrum – us-east-1** zugeordnet ist. Dies ist der Wert, den der Benutzer im Feld „Standort“ sieht. Das System konnte diesen Wert aufgrund der Zuordnung in der Tabelle „Zugeordnetes Rechenzentrum“ anzeigen. Das System hat diese Zuordnung erstellt, als Ihr Cloud Provisioning and Governance-Administrator das Cloud-Konto für AWS erstellt und dann Discovery für das Rechenzentrum „us-east-1“ in diesem Cloud-Konto ausgeführt hat.

Es ist möglich, dass mehrere Rechenzentren mit **Mein Cloud-Konto** verknüpft sind. In diesem Fall werden im Feld „Standort“ alle zugehörigen Rechenzentren neu geladen. Da das Feld „Standort“ vom Typ „Auswählen“ ist, kann der Benutzer im Feld den gewünschten Standort auswählen.

Feld aus einem Cloud-Katalogformular entfernen

Entfernen Sie ein Feld aus dem Katalogformular Cloud Provisioning and Governance, wenn der Benutzer zu einer bestimmten Gruppe gehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Bevor Sie diesem Beispiel folgen können, müssen Sie mit dem Erstellen von Blaupausen und Blaupausenregeln vertraut sein. Sehen Sie sich folgende Ressourcen an:

- Blaupausen für die Cloudbereitstellung
- Cloud Provisioning-Blaupause erstellen
- Blaupausenregel konfigurieren

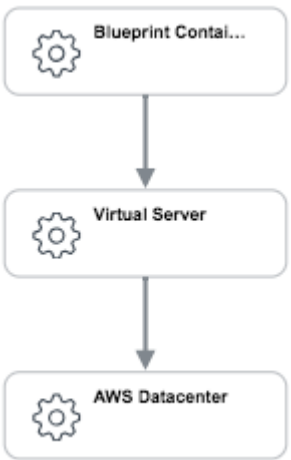
Warum und wann dieser Vorgang ausgeführt wird

Das Ziel dieses Beispiels ist, das Feld „Kostenstelle“ im Katalogformular auszublenden, wenn der Kataloganforderer zur Datenbankgruppe gehört. Sie können einem Beispiel wie diesem folgen, wenn Sie Katalogelementfelder basierend auf Werten in anderen Feldern ein- oder ausblenden möchten.

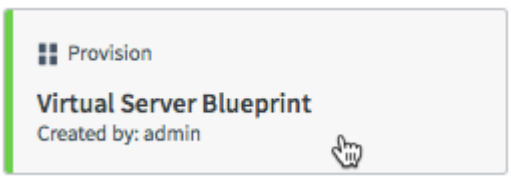
Prozedur

1. Blaupause mit einem virtuellen Server erstellen

   In diesem Beispiel wird eine Blaupause mit einem virtuellen Server in einem AWS-Rechenzentrum verwendet.



2. Klicken Sie auf dem Blaupausenformular auf die Registerkarte **Katalog**, und klicken Sie dann auf die Kachel, die den Vorgang **Bereitstellung** darstellt.



3. Klicken Sie auf die Schaltfläche **Allgemeine Informationen** Variablensatz in der zugehörigen Liste „Variablensätze“.
4. Klicken Sie auf die Variable **CostCenter**, um das Cloud-Variablenformular zu öffnen.
5. Konfigurieren Sie die Regel, die die Kostenstelle basierend auf der Benutzergruppe entfernt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der zugehörigen Liste **Regeln** auf **Neu**.

b. Füllen Sie die Felder **Name** und **Beschreibung** aus.

c. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

6. Konfigurieren Sie die Bedingung, die erfordert, dass die Benutzergruppe „Datenbank“ ist:

a. Klicken Sie in der zugehörigen Liste **Bedingungen** auf **Neu**.

b. Füllen Sie die Felder des Formulars aus.

Feld	Einzugebender oder auszuwählender Wert	Beschreibung
Operand	UserGroup	Dieser Wert ist das Feld „Benutzergruppe“, das der Benutzer auswählt.
Operator	--Keine--	Behalten Sie den Wert **--Keine--** bei, da diese Bedingung die einzige Bedingung ist, die Sie konfigurieren müssen. Wenn Sie weitere Bedingungen hinzufügen, können Sie einen anderen Operator auswählen, um zu bestimmen, wie das System diese Bedingung im Verhältnis zu den anderen auswertet.
Wert	287ee6fea9fe198100ada7950d0b1b73	Dieser Wert ist die Sys-ID der Benutzergruppe „Datenbank“, die als Teil der Demodaten in Ihrer Instanz bereitgestellt wird. Weitere Informationen finden Sie unter Sys-ID .

c. Klicken Sie auf **Absenden**.

7. Um zu verstehen, warum die Sys-ID der Benutzergruppe für das System erforderlich ist, führen Sie die folgenden Schritte aus:

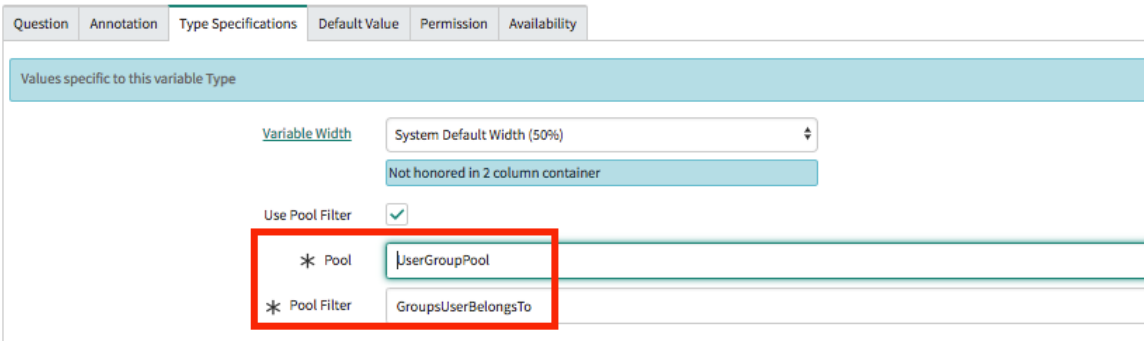
a. Öffnen Sie die Blaupause erneut, und klicken Sie erneut auf den Vorgang „Bereitstellung“.

b. Klicken Sie in der zugehörigen Liste **Variablensätze** auf **Allgemeine Informationen**.

c. Klicken Sie auf die Variable **UserGroup**.

Beachten Sie, dass das System auf der Registerkarte **Typspezifikationen** Benutzergruppen aus **UserGroupPool** ausfüllt. Das System führt den geskripteten Poolfilter mit dem Namen **GroupsUserBelongsTo** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Navigieren Sie im Cloud-Administrationsportal zu **Verwalten** > **Ressourcenpools**.

e. Suchen und öffnen Sie **UserGroupPool**.

Beachten Sie, dass die Werte für den Pool aus der Tabelle im Feld **Suchtabelle** abgeleitet sind, das in diesem Fall ist die Gruppentabelle [sys_user_group] ist.

Beachten Sie auch, dass die zugehörige Liste „Ressourcenpoolfilter“ zwei Abfragen enthält:

- **All** ist eine generische Abfrage, die die Liste aller Datensätze aus der **Suchtabelle** zurückgibt. Der von dieser Tabelle zurückgegebene Wert stammt aus dem **Suchfeld**, in diesem Fall der Sys-ID. Das System ignoriert jedoch die Abfrage *ALL* in diesem Fall, da die geskriptete Abfrage vorhanden ist.
- **GroupsUserBelongsTo** ist eine geskriptete Abfrage, die die Sys-ID der Datensätze in der **Suchtabelle** zurückgibt.

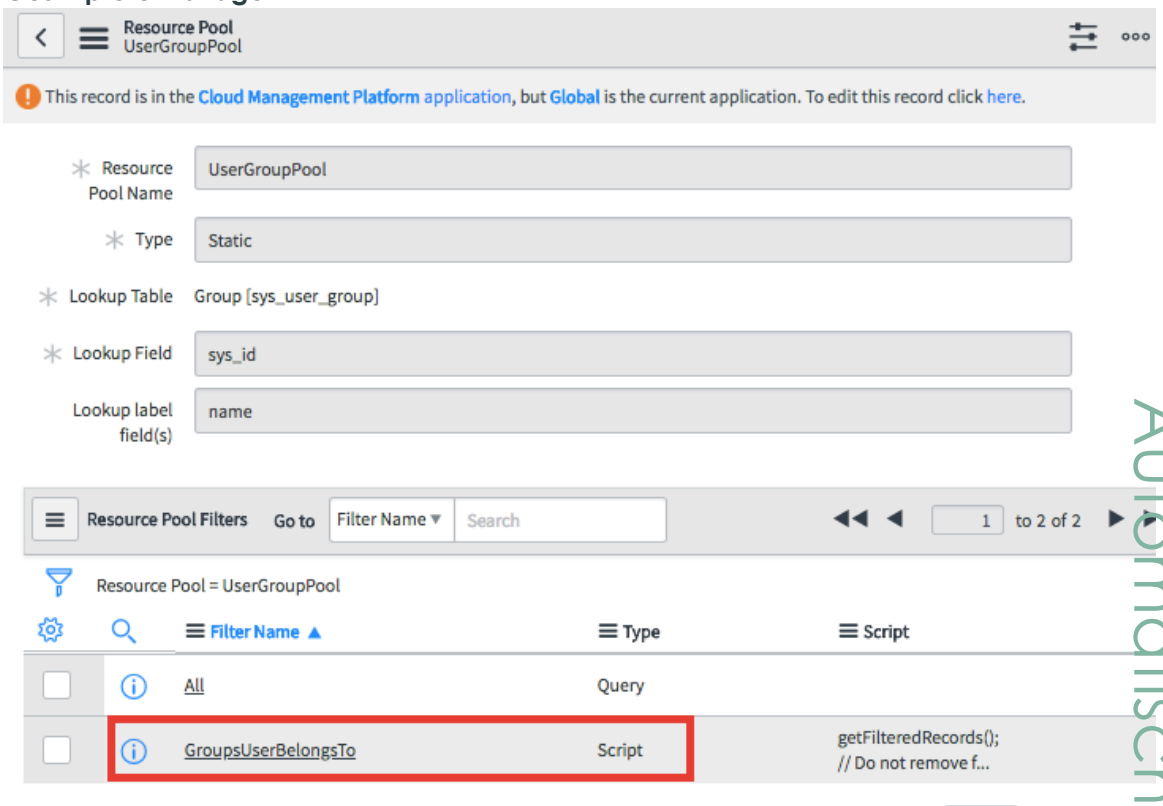
Wichtig: Wenn eine geskriptete Abfrage vorhanden ist, verwendet das System diese anstelle der generischen *ALL*-Abfrage.

Sowohl die generische Abfrage als auch die geskriptete Abfrage geben die Sys-ID des Datensatzes in der Suchtabelle zurück. Tatsächlich ignoriert hier das System aber

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die **All**-Abfrage und den im **Suchfeld** angegebenen Wert und verwendet das Skript **GroupsUserBelongsTo**.

Geskriptete Abfrage



Stapelnamen mit einem Skript ausfüllen

Dieses Beispiel zeigt, wie der Name des Stapels, den ein Benutzer im Cloud Provisioning and Governance-Katalog anfordert, mithilfe der Benutzer-ID ausgefüllt wird. Im Beispiel wird eine Skripteinbindung verwendet, die Sie über eine Blaupausenregelaktion aufrufen können.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Bevor Sie diesem Beispiel folgen können, müssen Sie mit dem Erstellen von Blaupausen und Blaupausenregeln vertraut sein. Sehen Sie sich folgende Ressourcen an:

- Blaupausen für die Cloudbereitstellung
- Cloud Provisioning-Blaupause erstellen
- Blaupausenregel konfigurieren

In diesem Beispiel wird eine Skripteinbindung verwendet. Wenn Sie ähnliche Skripteinbindungen erstellen möchten, machen Sie sich mit den Glide System APIs vertraut, die Teil Ihrer Instanz sind. Auf der Entwicklerwebsite finden Sie eine umfassende Liste aller APIs. Unter Skripteinbindungen finden Sie weitere Informationen darüber, wie das System diese Skripts verwendet.

Warum und wann dieser Vorgang ausgeführt wird

Das Ziel dieses Beispiels besteht darin, die ID des Kataloganforderers zu verwenden und im Feld „Stapelname“ auszufüllen. Das Feld kann weiterhin bearbeitet werden. Folgen Sie einem Beispiel wie diesem, wenn Sie eine Benennungs- oder Bezeichnungskonvention für bestimmte Werte locker erzwingen möchten, dem Benutzer aber dennoch erlauben möchten, den gewünschten Text einzugeben.

Automatische Übersetzung

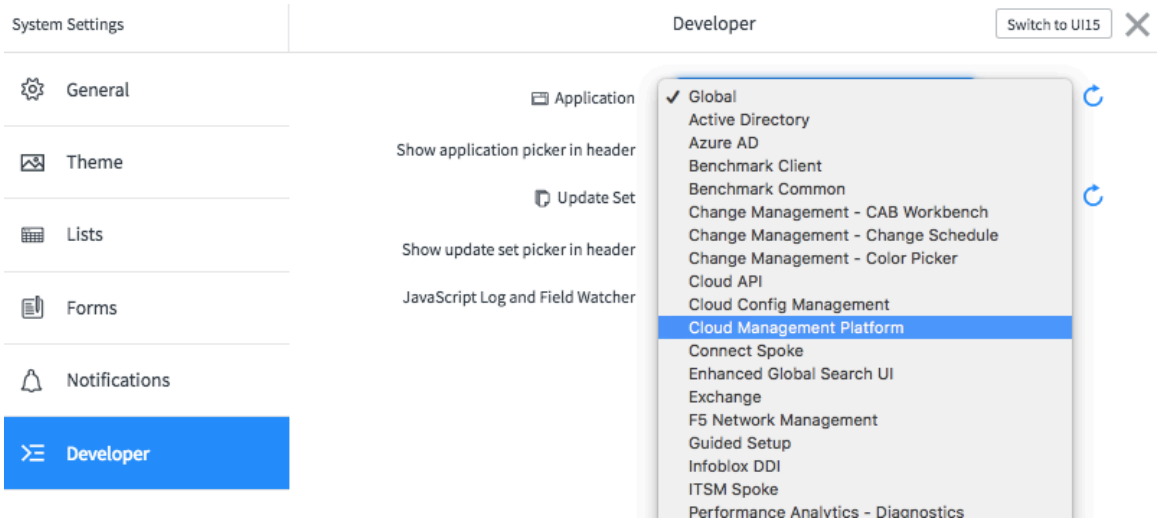
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Erstellen Sie eine Skripteinbindung, die die Benutzer-ID der das Katalogelement anfordernden Person zurückgibt:

   a. Klicken Sie auf der Standardoberfläche für die Instanz (nicht im Cloud-Adminportal) oben links auf das Zahnradsymbol ( ), und klicken Sie dann auf **Entwickler**.

   b. Wählen Sie im Feld **Anwendung** die Option **Cloud Provisioning and Governance** aus.



   Der Anwendungsbereich Ihrer Instanz ändert sich in **Cloud Provisioning and Governance**. Diese Auswahl bedeutet, dass die Cloud Provisioning and Governance-Anwendung die Skripteinbindung finden kann.

   c. Schließen Sie das Fenster „Systemeinstellungen“.

   d. Navigieren zu **Systemdefinition** > **Skripteinbindungen**.

   e. Klicken Sie auf **Neu**.

   f. Füllen Sie die Formularfelder aus (siehe Tabelle):

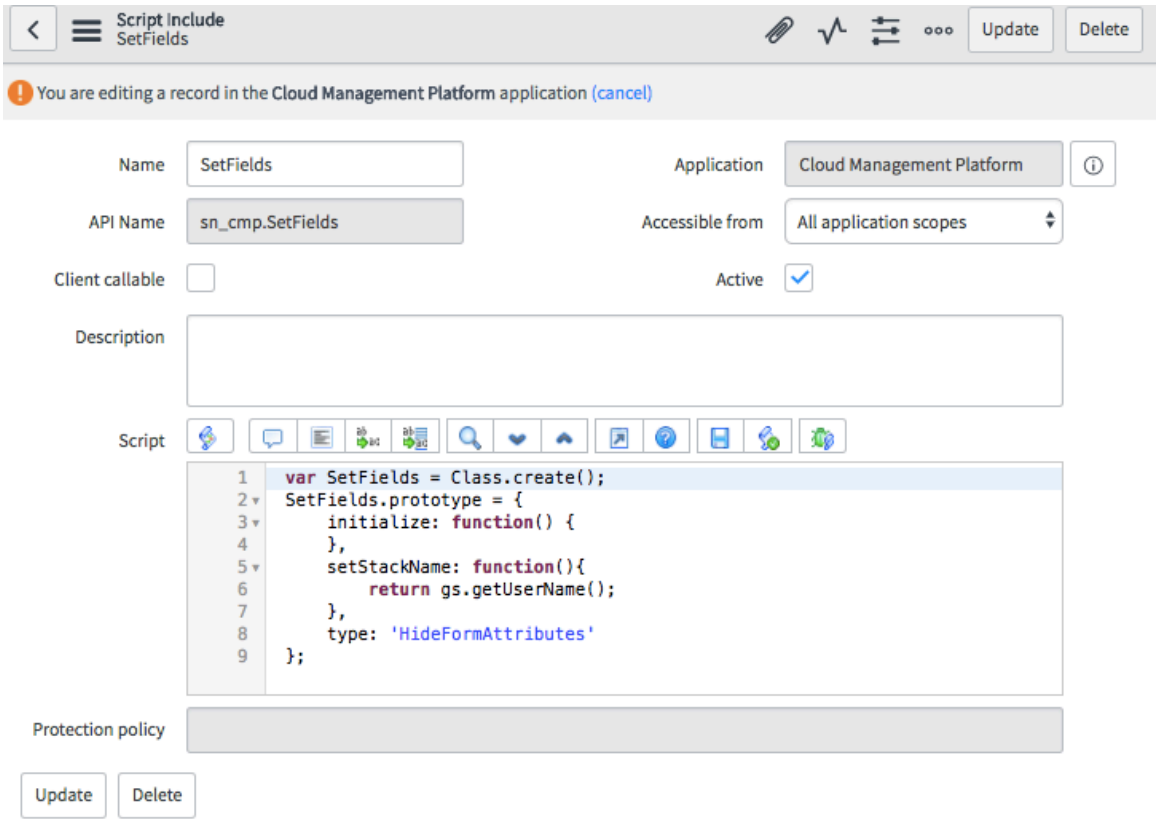
Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen ohne Leerzeichen an.
Zugänglich von	Wählen Sie **Alle Anwendungsbereiche** aus.
Skript	Geben Sie dieses Skript ein:

```
var SetFields = Class.create();
SetFields.prototype = {
 initialize: function() {
 },
 setStackName: function(){
  return gs.getUserName();
 },
 type: 'HideFormAttributes'
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
`};`	
Die Funktion `setStackName ()` gibt den Benutzernamen des Katalogelementanforderers zurück. Sie können diese Funktion über eine Blaupausenregelaktion aufrufen.	

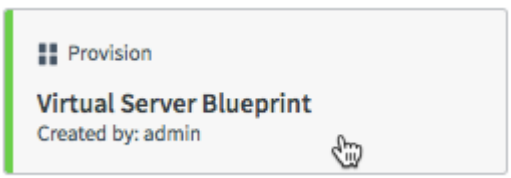


g. Klicken Sie auf **Absenden**.

h. Klicken Sie erneut oben links auf das Zahnradsymbol ( ), und ändern Sie die **Anwendung** wieder in **Global**.

2. Navigieren Sie im Cloud-Adminportal zu **Entwurf** > **Blueprints** und öffnen Sie den entsprechenden Blueprint.

3. Klicken Sie auf dem Blaupausenformular auf die Registerkarte **Katalog**, und klicken Sie dann auf die Kachel, die den Vorgang **Bereitstellung** darstellt.



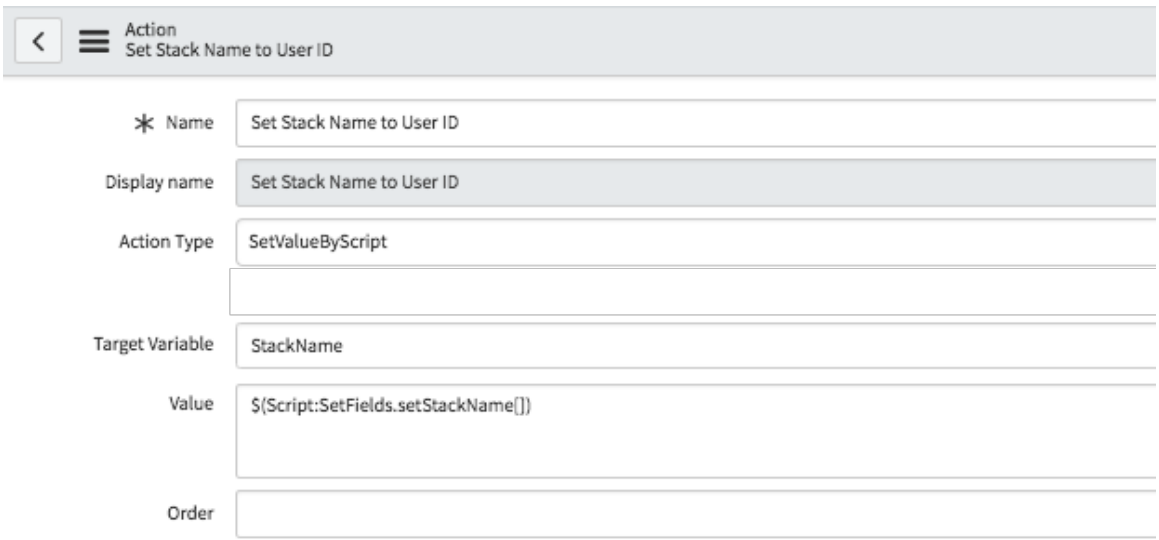
4. Klicken Sie auf die Schaltfläche **Stapelname** Variablensatz in der zugehörigen Liste „Variablensätze“.

Beachten Sie, dass Stapelname ein einzeiliges Textfeld ist, das Texteingaben akzeptiert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Erstellen Sie eine Regel zum Ausfüllen des Stapelnamens:
   a. Scrollen Sie nach unten zum Ende des Formulars, und klicken Sie in der zugehörigen Liste **Regeln** auf **Neu**.
   b. Geben Sie einen Namen und eine Beschreibung ein.
   c. Klicken Sie auf **Absenden**.
6. Konfigurieren Sie die Aktion wie folgt:
   a. Scrollen Sie nach unten zum Ende des Formulars „Regel“, und klicken Sie in der zugehörigen Liste **Aktion** auf **Neu**.
   b. Konfigurieren Sie die Regel wie folgt:

Feld	Beschreibung
Name	Geben Sie einen aussagekräftigen Namen und eine Beschreibung an, z. B. `Stapelnamen auf Benutzer-ID festlegen`.
Aktionstyp	Wählen Sie **SetValueByScript** aus, um das System anzuweisen, die im Feld **Wert** angegebene Skripteinbindung aufzurufen.
Zielvariable	Wählen Sie **Stapelname** aus, um das System anzuweisen, den Wert des Felds „Stapelname“ festzulegen.
Wert	Rufen Sie die Methode in der Skripteinbindung auf, die die Benutzer-ID zurückgibt. Der Aufruf muss die folgende Syntax haben: `$(Script:ScriptIncludeName.methodName[])` Verwenden Sie in diesem Beispiel `$(Script:SetFields.setStackName[])`.

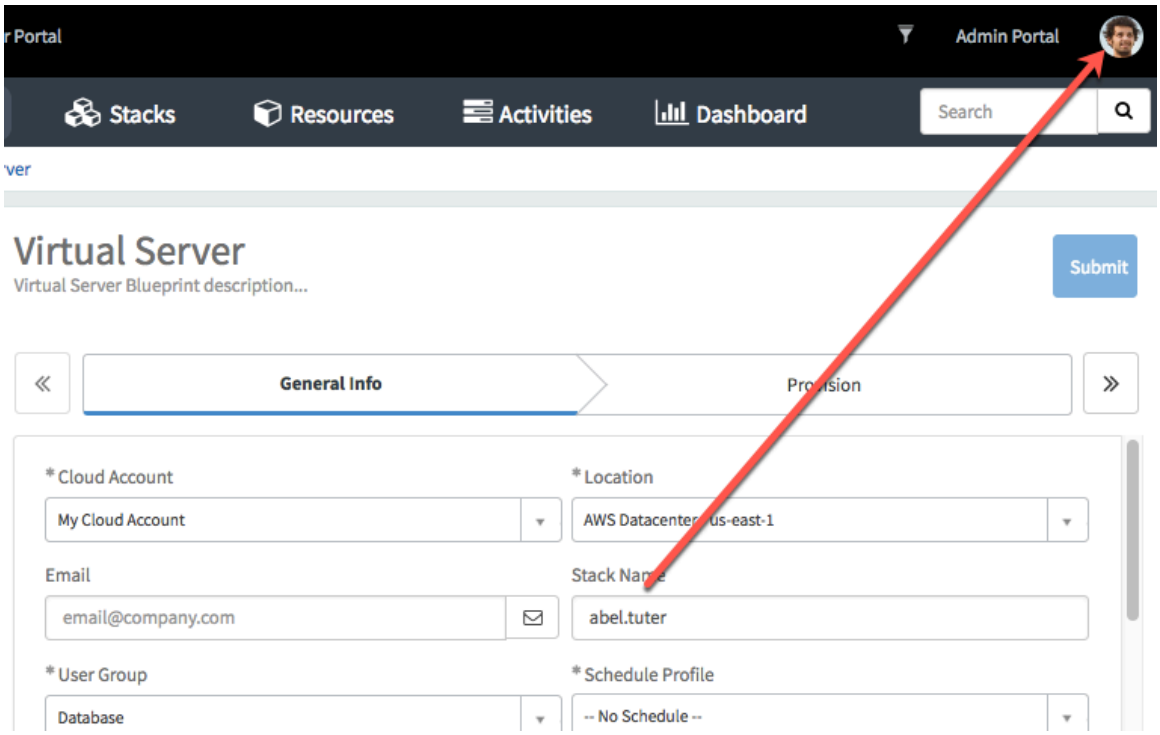


   c. Klicken Sie auf **Absenden**.

Ergebnisse
Im Cloud-Benutzerportal wird im Katalogbestellformular für den Bereitstellungsvorgang die Benutzer-ID des angemeldeten Benutzers angezeigt. In diesem Beispiel wird der Benutzer „Able Tutor“ verwendet, der im Basissystem als Demodaten bereitgestellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Wert im Feld **Stapelname** ist der gleiche Wert wie im Feld „Benutzer-ID“ der Tabelle „Benutzer“ [sys_user]. Das Profilsymbol für denselben angemeldeten Benutzer wird auch oben rechts im Cloud-Benutzerportal angezeigt.



Standardwerte für Cloud-Katalogformularfelder festlegen

Sie können Standardwerte für alle Benutzer festlegen oder Felder basierend auf Bedingungen mit Standardwerten ausfüllen. Dieses Beispiel zeigt, wie ein Zeitplanprofil und ein Business Service als Standards festgelegt werden.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Bevor Sie diesem Beispiel folgen können, müssen Sie mit dem Erstellen von Blaupausen und Blaupausenregeln vertraut sein. Sehen Sie sich folgende Ressourcen an:

- Blaupausen für die Cloudbereitstellung
- Cloud Provisioning-Blaupause erstellen
- Blaupausenregel konfigurieren

Warum und wann dieser Vorgang ausgeführt wird

Das Ziel dieses Beispiels ist die Anzeige eines Standardwerts für das Zeitplanprofil und den Business Service. Jedes Feld leitet seine Werte unterschiedlich ab:

- Das Zeitplanprofil leitet seine Werte von einem Poolfilter ab, der einen Textwert zurückgibt. Daher müssen Sie den Standardwert festlegen, indem Sie den richtigen, übereinstimmenden Text für eine der Zeitplanprofiloptionen anwenden, die dem Benutzer in einer Liste angezeigt werden.
- Der Business Service leitet seine Werte aus einer Referenz auf die Tabelle „Service“ [cmdb_ci_service] ab. Daher müssen Sie den Wert festlegen, indem Sie die Sys-ID des Datensatzes angeben, den Sie anzeigen möchten.

Im Beispiel in diesem Thema werden die Werte auf verschiedene Arten festgelegt:

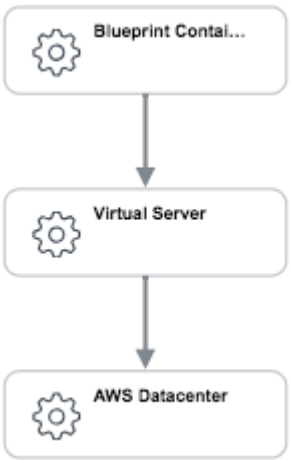
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Standardwert für das Zeitplanprofil wird direkt in der Eigenschaft „Zeitplanprofil“ festgelegt und gilt für alle Benutzer ohne Bedingungen. Sie können dies tun, um die Verwendung virtueller Ressourcen für alle Benutzer auf einen bestimmten Zeitplan zu beschränken, z. B. nur während der Geschäftszeiten.
- Der Standardwert für den Business Service wird mithilfe einer Aktion in einer Blaupausenregel festgelegt. Sie können eine Regel zum Festlegen eines Standardwerts verwenden, wenn der Wert nur dann als Standard festgelegt werden soll, wenn bestimmte Bedingungen erfüllt sind. Wenn der Benutzer beispielsweise zu einer Benutzergruppe gehört, die nur einen Business Service verwendet, legen Sie den Wert für den Benutzer so fest, dass er nicht eine lange Liste aller Business Services in Ihrer Organisation durchsuchen muss.

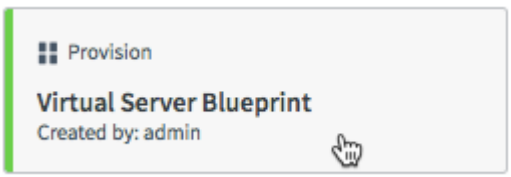
Prozedur

1. Blaupause mit einem virtuellen Server erstellen

   In diesem Beispiel wird eine Blaupause mit einem virtuellen Server in einem AWS-Rechenzentrum verwendet.



2. Klicken Sie auf dem Blaupausenformular auf die Registerkarte **Katalog**, und klicken Sie dann auf die Kachel, die den Vorgang **Bereitstellung** darstellt.



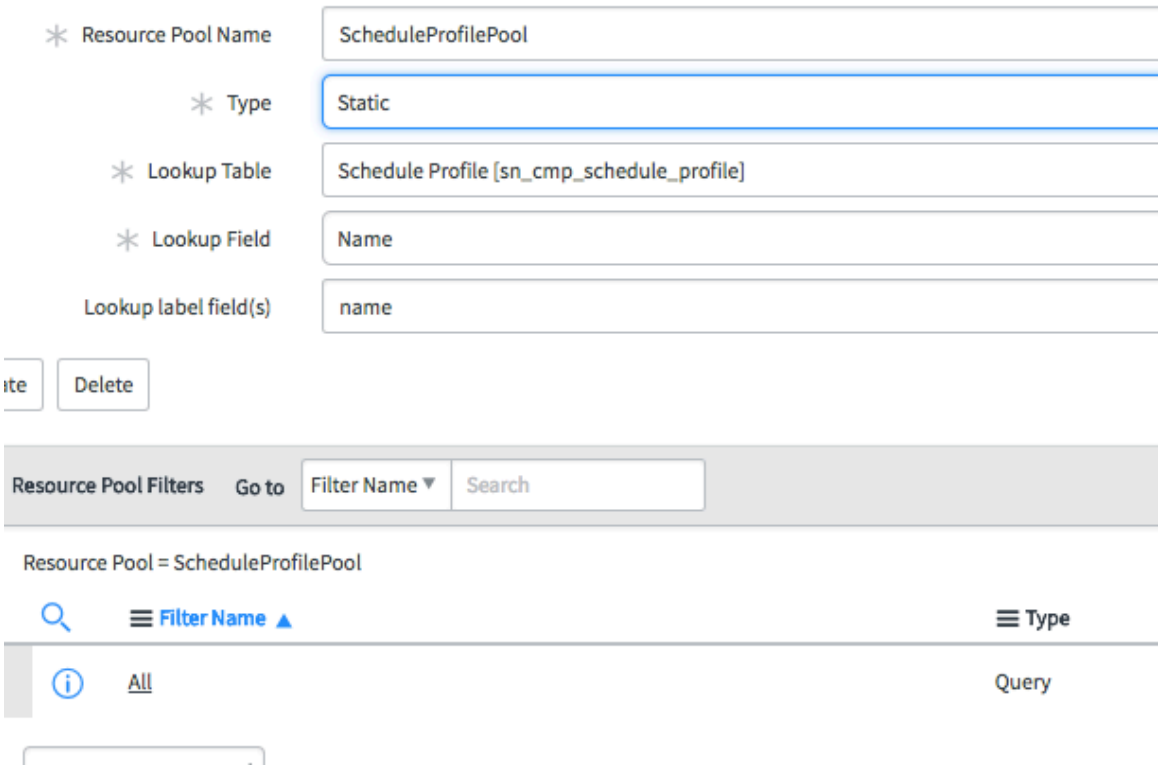
3. Klicken Sie auf die Schaltfläche **Allgemeine Informationen** Variablensatz in der zugehörigen Liste „Variablensätze“.
4. Klicken Sie auf die Variable **ScheduleProfile**.

   Beachten Sie, dass das Feld **Pool** auf der Registerkarte **Typspezifikationen** den Pool angibt, aus dem die Werte für das Zeitplanprofil abgeleitet werden: ScheduleProfilePool.

   Der Pool **ScheduleProfilePool** gibt den Filter **Alle** an, der die Werte im Feld „Name“ der Tabelle „Zeitplanprofil“ [sn_cmp_schedule_profile] zurückgibt. Diese Werte sind statische Textwerte, was bedeutet, dass Sie den genauen Textwert für den Namen

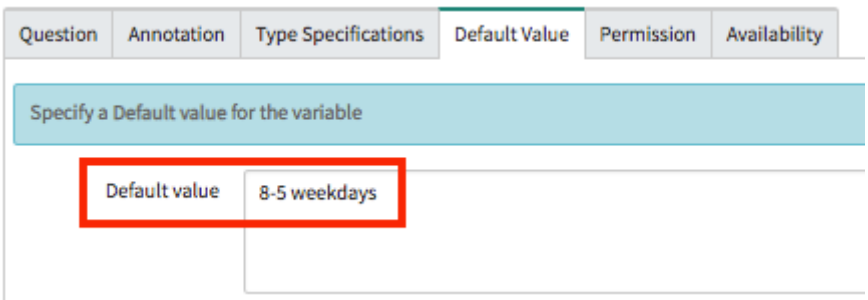
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

des Zeitplanprofils angeben können, das Sie als Standard festlegen möchten.



5. Geben Sie auf der Registerkarte **Standardwert** des Eigenschaftsformulars „ScheduleProfile“ den Text ein, der dem Wert im Feld „Name“ aus der Tabelle „Zeitplanprofil“ [sn_cmp_schedule_profile] entspricht.

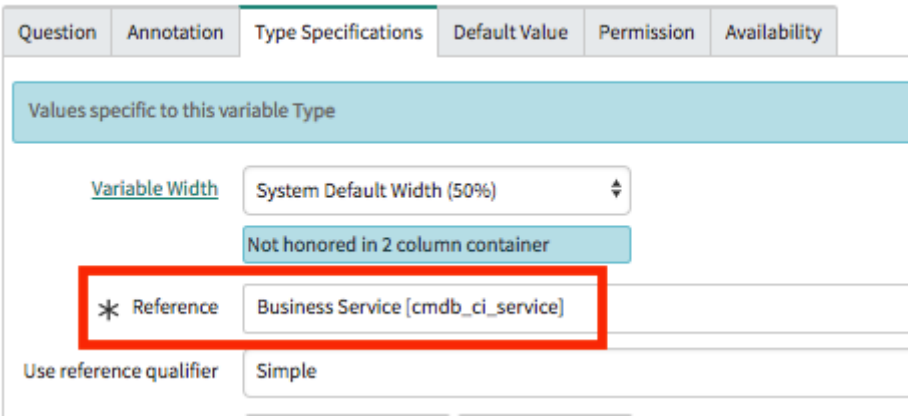
   In diesem Beispiel beträgt dieser Wert `Wochentage von 8-17.00 Uhr`.



6. Klicken Sie auf **Aktualisieren**.
7. Klicken Sie auf die Variable **BusinessService**.

   Beachten Sie, dass das Feld **Referenz** auf der Registerkarte **Typspezifikationen** die Tabelle „Service“ [cmdb_ci_service] angibt, aus der die Werte für den Business Service abgeleitet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Standardmäßig müssen Sie zum Verweisen auf einen bestimmten Datensatz in einer Tabelle die Sys-ID des Datensatzes kennen.

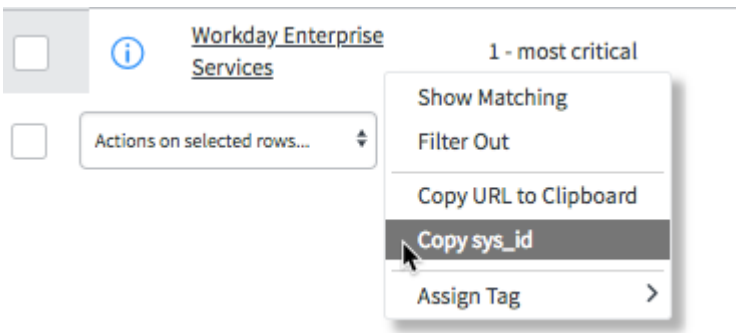
8. So rufen Sie die Sys-ID eines Business Service ab:

a. Geben Sie in der Hauptoberfläche für die Instanz (nicht im Cloud-Adminportal) `cmdb_ci_service.list` im Anwendungsfilter ein.

b. Suchen Sie den Business Service, den Sie als Standard festlegen möchten.

c. Klicken Sie mit der rechten Maustaste auf den Datensatz, und wählen Sie **sys_id kopieren** aus.

In diesem Beispiel wird **Workday Enterprise Services** verwendet.



9. Erstellen Sie im Variablenformular **BusinessService** eine Regel, eine Aktion und eine Bedingung mit diesen Werten:

a. Klicken Sie in der zugehörigen Liste **Regel** auf **Neu**.

b. Geben Sie einen Namen und eine Beschreibung ein.

c. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.

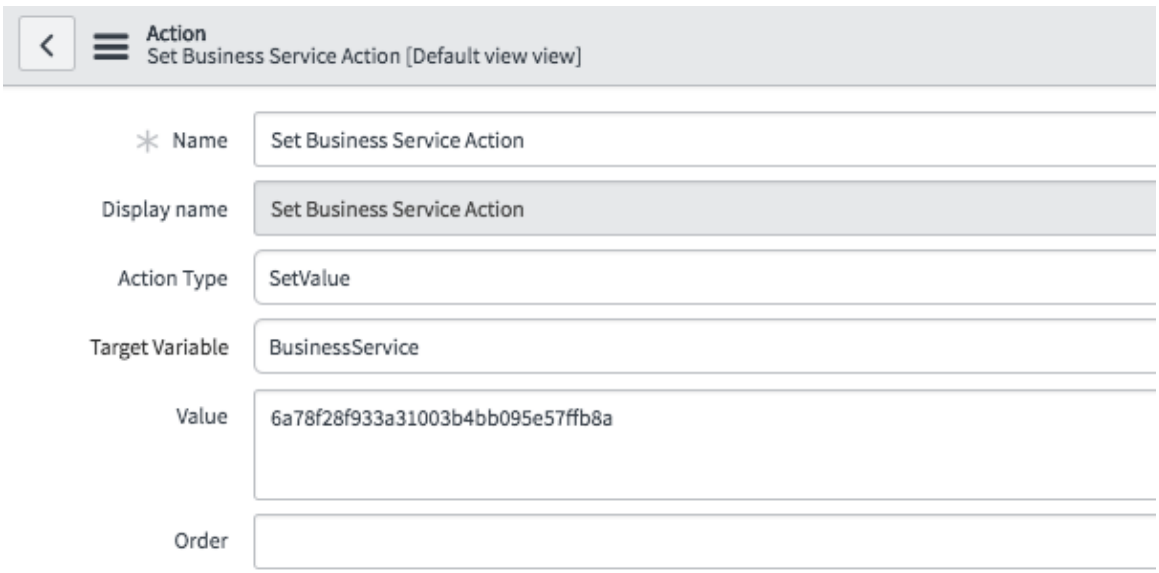
d. Klicken Sie in der zugehörigen Liste **Aktion** für die Regel auf **Neu**.

e. Geben Sie einen Namen an, und konfigurieren Sie dann diese Felder wie angegeben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

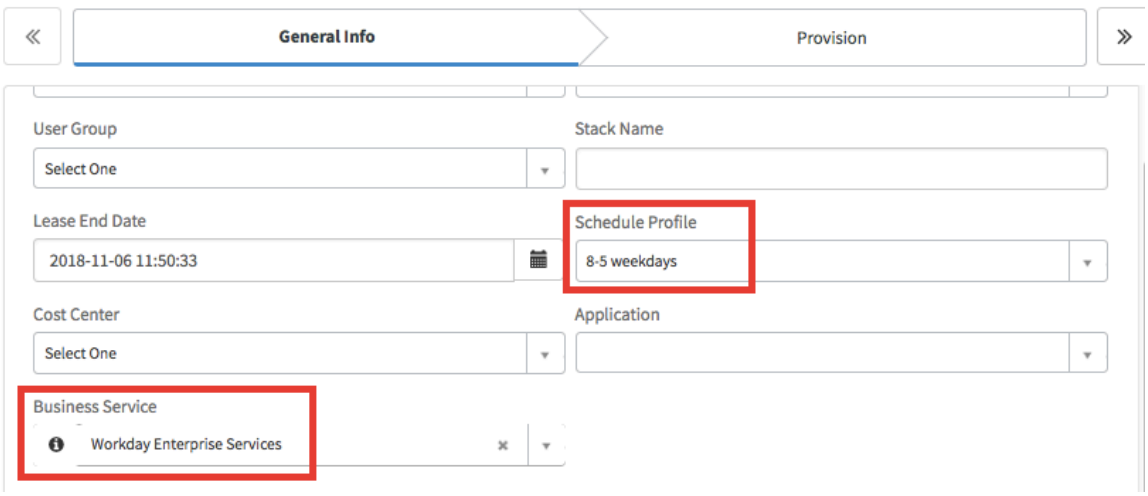
Feld	Wert
Aktionstyp	**SetValue** Diese Option weist das System an, das Feld in den von Ihnen angegebenen Wert zu ändern. Die Auswahl dieser Option entspricht der Eingabe eines Standardwerts im Eigenschaftsformular.
Zielfeld	**BusinessService**
Wert	Die Sys-ID des Business Service, den Sie kopiert haben.

In diesem Beispiel ist der Business Service standardmäßig auf „Workday Enterprise Services“ festgelegt, was im System mit der Sys-ID dargestellt wird, die Sie bereits kopiert haben.



f. Klicken Sie auf **Absenden**.

Ergebnisse



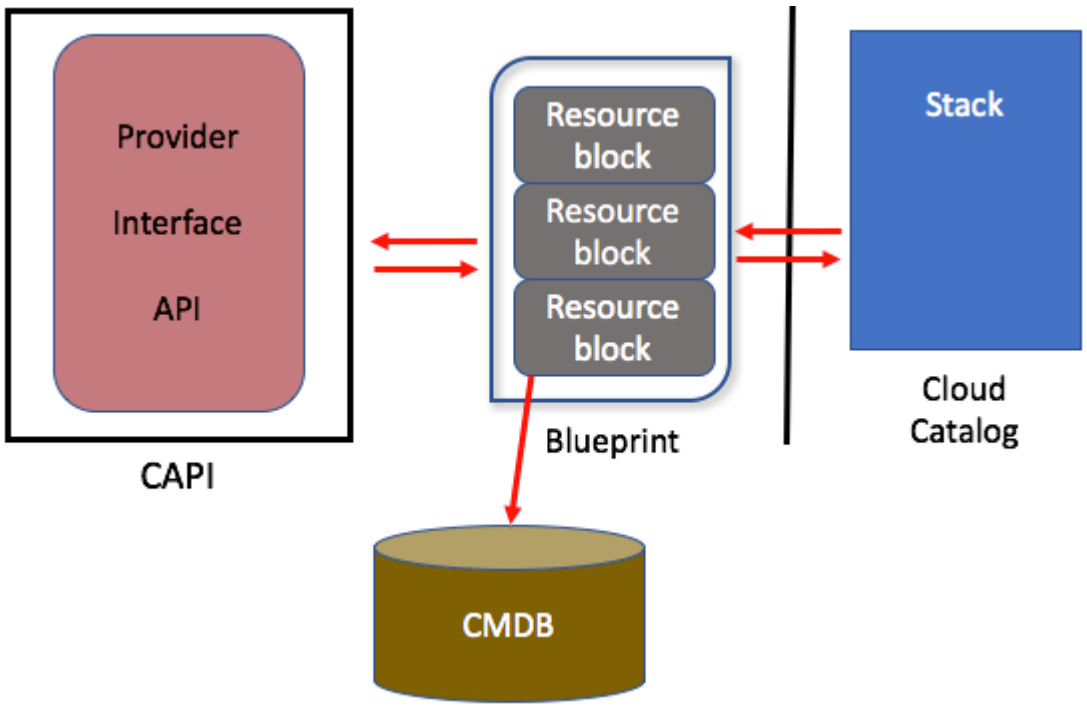
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nächste Maßnahme
Sie können eine Bedingung oder mehrere Bedingungen erstellen, die erfüllt sein müssen, bevor das System den Standardwert für den Business Service festlegt. Beispiel: Sie möchten den Standardwert des Business Service nur dann in „Workday Enterprise Services“ ändern, wenn die Gruppe, der der Benutzer angehört, die Gruppe „Workday Admins“ ist.

Ressourcenblöcke in Cloud Provisioning and Governance

Ressourcenblöcke fungieren als eine Art Middleware-Komponente zwischen Katalogelementen, der Cloud API (CAPI) und der CMDB.

Die folgende Grafik zeigt, wie Ressourcenblöcke zwischen andere Komponenten im System passen:



Blaupausen

Jeder Ressourcenblock wird zu einem Baustein innerhalb einer Blaupause. Die Blaupause wird schließlich zu einem Katalogelement (auch Stapel genannt), das ein Benutzer aus dem Cloud-Katalog bereitstellt.

Cloud-API (CAPI)

Jeder Ressourcenblock definiert zulässige Vorgänge wie „Bereitstellung“ und „Bereitstellung aufheben“. Diese Vorgänge rufen verschiedene Komponenten in der CAPI auf, um den vom Stapel empfangenen Vorgang auszuführen.

Die CMDB

Jeder Ressourcenblock basiert auf einem CI-Typ der CMDB. Ressourcenblöcke haben auch einen Antwortprozessor, der Antworten vom Cloud-Provider verarbeitet, um eine Art von Aktion in der CMDB durchzuführen, z. B. das Erstellen oder Aktualisieren eines CI.

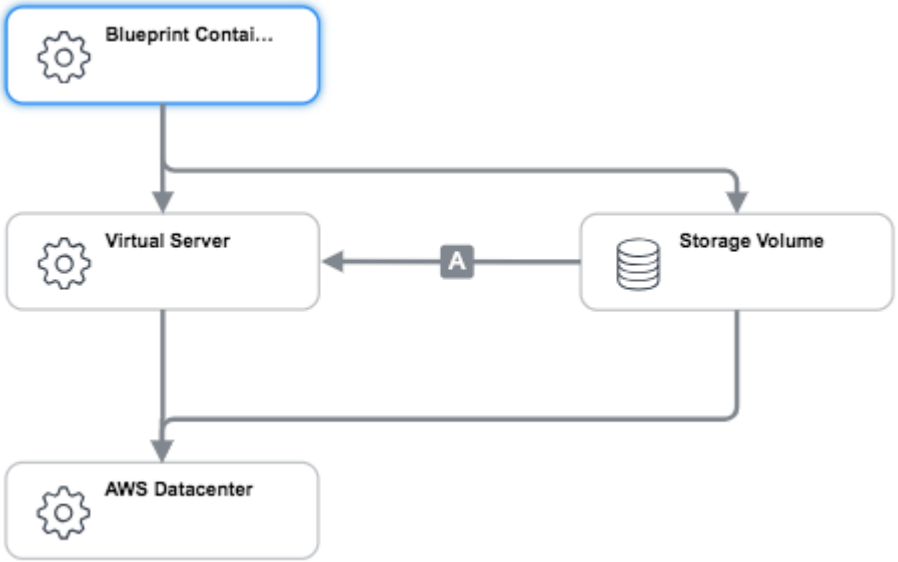
Verbindungen von Ressourcenblöcken

Ressourcenblöcke sind in Blaupausen miteinander verbunden. Beispielsweise ist in dieser Blaupause ein Ressourcenblock eines virtuellen Servers mit Speicher verbunden. Der virtuelle Server und der Speicher sind beide mit einem AWS-Rechenzentrum-Ressourcenblock verbunden.

Automatische Übersetzung

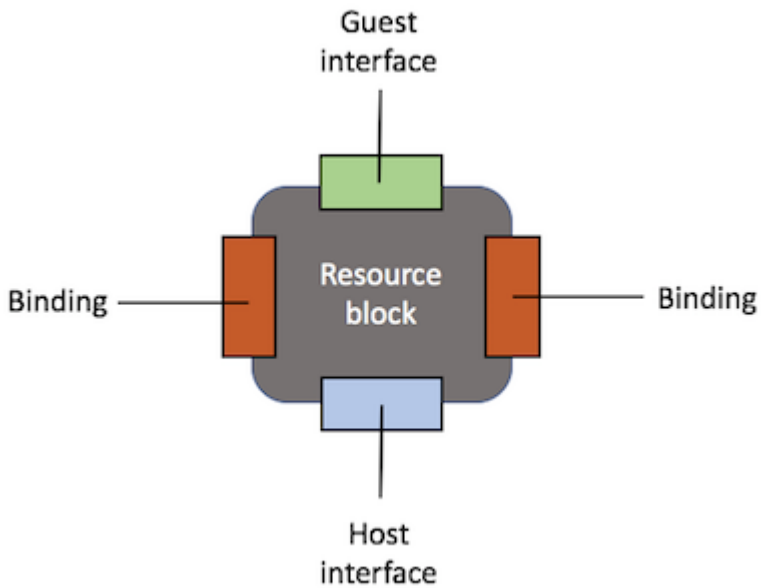
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Blaupause: Server mit Speicher



Damit diese Verbindungen erfolgreich hergestellt werden können, muss jeder Ressourcenblock einen Schnittstellentyp angeben. Diese Grafik veranschaulicht diese Schnittstellen:

Schnittstellentypen für Ressourcenblöcke



- Die Gastschnittstelle stellt eine Verbindung mit der darüber befindlichen Ressource her. Die Gastschnittstelle enthält die Vorgänge (auch Vorgangssignaturen genannt), mit denen Benutzer Aktionen für ihre Ressource ausführen können.
- Die Hostschnittstelle stellt eine Verbindung mit der Ressource unter dem Ressourcenblock in der Blaupause her. Die Hostschnittstelle enthält auch Vorgangssignaturen.
- Die Bindungen verbinden angrenzende Ressourcen.

Ressourcenblöcke können beliebig viele Gastschnittstellen, Hostschnittstellen und Bindungen aufweisen. Verbindungen können in verschiedene Richtungen hergestellt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Vertikale Verbindungen erfordern, dass die Hostschnittstelle des oberen Ressourcenblocks der Gastschnittstelle des unteren Ressourcenblocks entspricht.

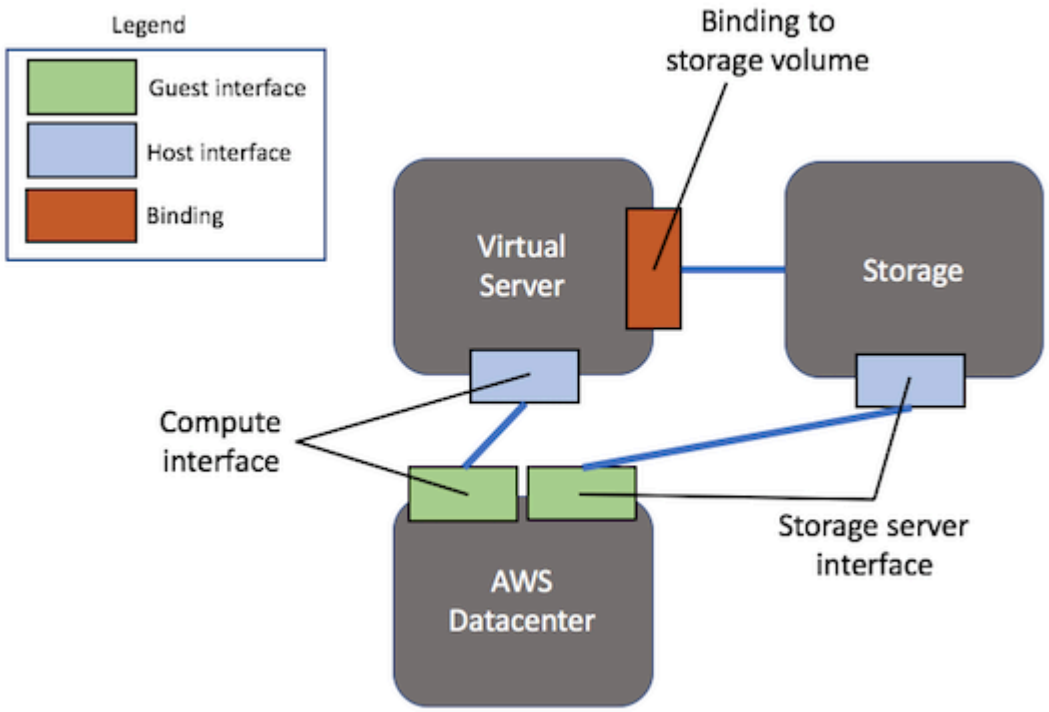
  Hinweis: In Blaupausen wird diese vertikale Verbindung als Containment-Verbindung bezeichnet.

- Horizontale Verbindungen binden eine Ressource an eine andere, aber beide Ressourcen müssen sich über demselben Ressourcenblock befinden.

  Hinweis: In Blaupausen wird diese horizontale Verbindung als Angehängt-Verbindung bezeichnet.

Wenn in dieser Beispielblaupause ein virtueller Server mit angehängtem Speicher in einem AWS-Rechenzentrum verbunden ist, sind die Ressourcenblöcke wie folgt konfiguriert:

Schnittstellen für Ressourcenblöcke



Ressourcenblock	Schnittstellen und Bindungen
Virtueller Server	• Hostschnittstelle: Computing • Bindung: an Speichervolume
AWS-Rechenzentrum	• Gastschnittstelle: Computing • Gastschnittstelle: Speicherserverschnittstelle
Speicher	Hostschnittstelle: Speicherserverschnittstelle Die Bindung zwischen dem virtuellen Server und dem Speicher ist unidirektional. Sie konfigurieren die Bindung für

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcenblock	Schnittstellen und Bindungen
	den virtuellen Speicherressourcenblock nur, indem Sie den Speicherressourcenblock angeben. Sie müssen keine weitere Bindung für den Speicherressourcenblock konfigurieren.

Gastschnittstellen und Vorgänge

Jede Gastschnittstelle bietet einen Standardsatz von Vorgängen (auch Vorgangssignaturen genannt), mit denen der Benutzer auswählen kann, was er mit einer virtuellen Ressource tun möchte. Der häufigste Vorgang ist die Bereitstellung, was bedeutet, dass eine virtuelle Ressource erstellt wird. Viele Gastschnittstellen und entsprechende Vorgänge werden standardmäßig mit der Cloud Provisioning and Governance-Anwendung bereitgestellt. Sie können diese standardmäßigen Gastschnittstellen für viele Ihrer Ressourcenblöcke verwenden.

Wenn Sie eine neue Gastschnittstelle erstellen müssen, werden diese Vorgänge standardmäßig bereitgestellt:

- Start
- Stoppen
- Bereitstellung
- Aufheben der Bereitstellung
- Bereinigung
- ModifySchedule
- ModifyLease

Details der Ressourcenblockkomponenten

Jeder Ressourcenblock enthält diese Komponenten:

Ebenen

Die logische Ebene im Stapel, zu der dieser Ressourcenblock gehört. Standardmäßig stellt Cloud Provisioning and Governance die Ebenen bereit. Beim Konfigurieren von Ressourcenblöcken können Sie die für Sie relevante auswählen.

Vorgänge für jede Gastschnittstelle

Wie bereits erwähnt, bietet jede Gastschnittstelle Vorgänge. Die häufigsten Vorgänge für einen virtuellen Server sind beispielsweise **Bereitstellung**, **Bereitstellung aufheben**, **Starten**, **Stoppen**.

Eingabeparameter für die einzelnen Vorgänge

Die Eingabeparameter enthalten Werte, die der Cloud-Provider bei der Ausführung von Vorgängen über CAPI verwendet. Diese Parameter enthalten die Informationen, die der Benutzer beim Ausführen eines Vorgangs, z. B. Bereitstellung, für einen Stapel auswählt.

Beispielsweise muss ein Benutzer normalerweise den Standort angeben, bei dem es sich um ein Rechenzentrum handelt, zu dem ein Stapel gehört. Der Wert, den der Benutzer im Feld **Standort** auswählt, wird im Standortparameter gespeichert. Das System verwendet diesen Parameter, der standardmäßig für den Ressourcenblock des virtuellen Servers verfügbar ist, und übergibt ihn an den CAPI-Schnittstellenvorgang *CreateNode*. Der Schnittstellenvorgang

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

`CreateNode` weist den Cloud-Provider an, den tatsächlichen virtuellen Server zu erstellen (oder bereitzustellen).

Schritte für die einzelnen Vorgänge

Jeder Vorgang erfordert einen Schritt, um die tatsächliche Arbeit auszuführen. Jeder Schritt ruft eine bestimmte Schnittstelle und Methode in CAPI auf und übergibt die für diese Methode erforderlichen Eingabeparameter. Beispielsweise stellt der Vorgang **Bereitstellung** für einen virtuellen Server einen Schritt zum Herstellen einer Verbindung und zum Erstellen eines virtuellen Computers sowie einen weiteren Schritt zum Erstellen des Knotens im Cloud-Provider bereit. Jeder Schritt bietet andere Eingabeparameter. Zum Herstellen einer Verbindung und Erstellen eines virtuellen Computers ist neben vielen anderen Parametern das Cloud-Konto erforderlich. Zum Erstellen des Knotens ist kein Cloud-Konto erforderlich.

Sie können jedem Vorgang beliebig viele Schritte hinzufügen. Sie können auch Ausgabeattribute verwenden, um Werte in Attributen von einem Schritt an einen anderen Schritt zu übergeben oder Werte von Schritten in einem Vorgang an Schritte in einem nachfolgenden Vorgang zu übergeben. Beispielsweise kann der Vorgang der **Bereitstellung** für einen virtuellen Server ein Ausgabeattribut für die Netzwerkschnittstellen-ID und ein anderes für die Knoten-ID bereitstellen. Wenn der Cloud-Provider die Antwort sendet, werden die tatsächliche ID des Netzwerks und die des Knotens aus der Antwort analysiert und in den Ausgabeattributen gespeichert. Nachfolgende Schritte können dann die IDs zum Ausführen von Aktionen verwenden.

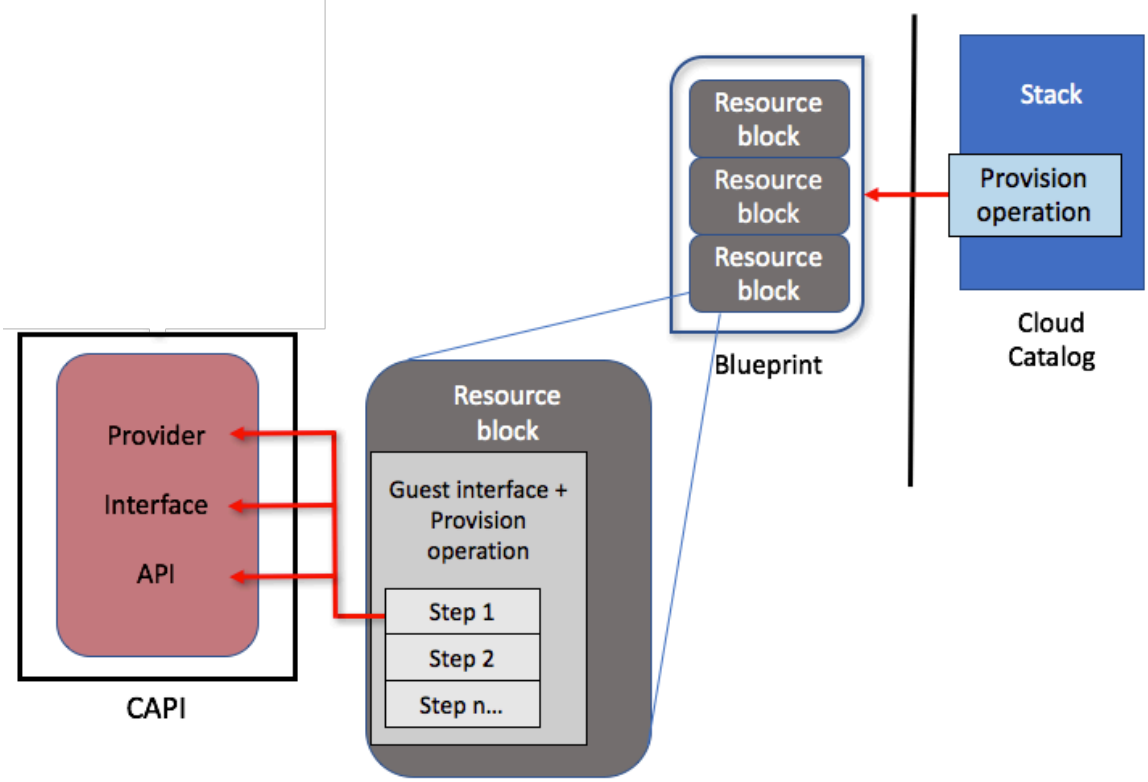
Antwortprozessoren

Antwortprozessoren teilen dem System mit, was in der CMDB zu tun ist. Wenn der Cloud-Provider eine Antwort sendet, nachdem ein Vorgang ausgeführt wurde, verarbeitet der Prozessor die Antwort.

Hinweis: Diese Prozessoren sind Skripts, die im System eingeschlossen sind. Sie sind keine MID Server-Skripteinbindungen wie die CAPI-Skripts, die Sie zur Integration des Cloud-Providers erstellen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Zusammenarbeit von Komponenten



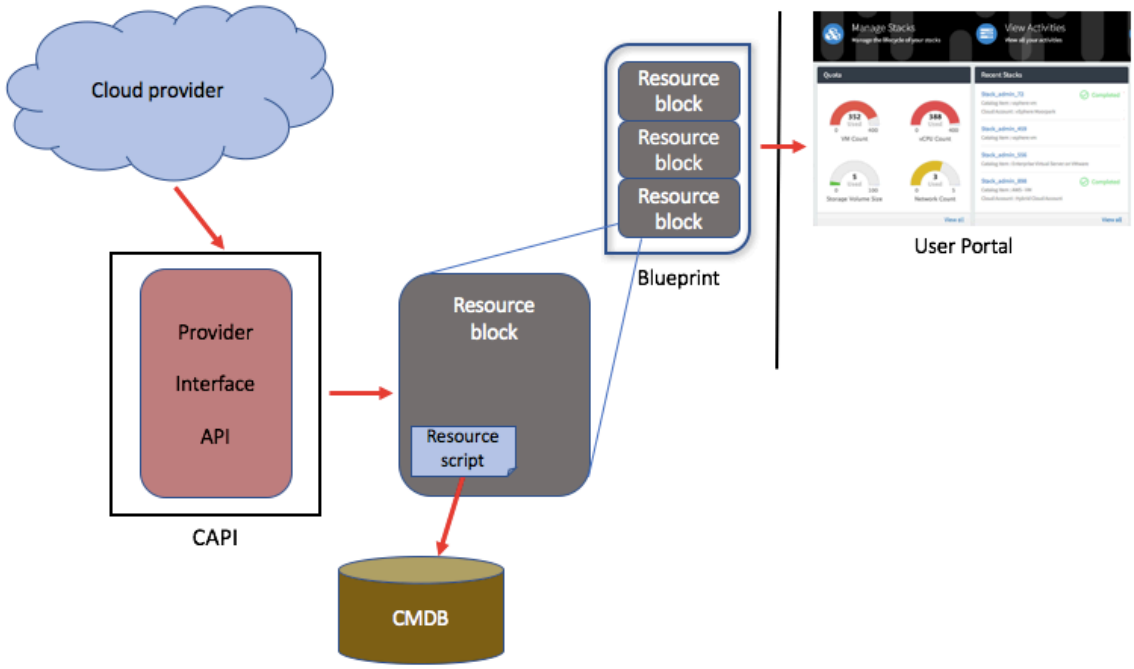
Benutzer können Katalogelemente, auch Stapel genannt, im Cloud-Katalog sehen. Ein Katalogelement basiert auf einer Blaupause, die wiederum aus miteinander verbundenen Ressourcenblöcken besteht.

1. Der Benutzer startet den Prozess, indem er einen Stapel anfordert. Die Anforderung ist der Vorgang **Bereitstellung** im System.
2. Das System führt die Schritte in der angegebenen Reihenfolge für den Vorgang **Bereitstellung** für die Ressourcenblöcke aus, die den Stapel bilden.
3. Jeder Schritt ruft CAPI auf, um die auszuführende Methode zu bestimmen und gleichzeitig Werte für erforderliche Parameter zu übergeben.
4. CAPI arbeitet mit der API des Cloud-Providers zusammen, um die tatsächliche Ressource bereitzustellen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozess-Flow beim Erstellen einer Ressource im Cloud-Provider



1. Der Cloud-Provider stellt die Ressource bereit und antwortet mit JSON.
2. Das System analysiert die Antwort im Ressourcenskript im Ressourcenblock.
3. Das System aktualisiert die CMDB. Beim Bereitstellen einer neuen Ressource erstellt das System ein CI in der richtigen Tabelle.
4. Der neue Stapel wird im Cloud-Benutzerportal für den zu verwaltenden Benutzer angezeigt.

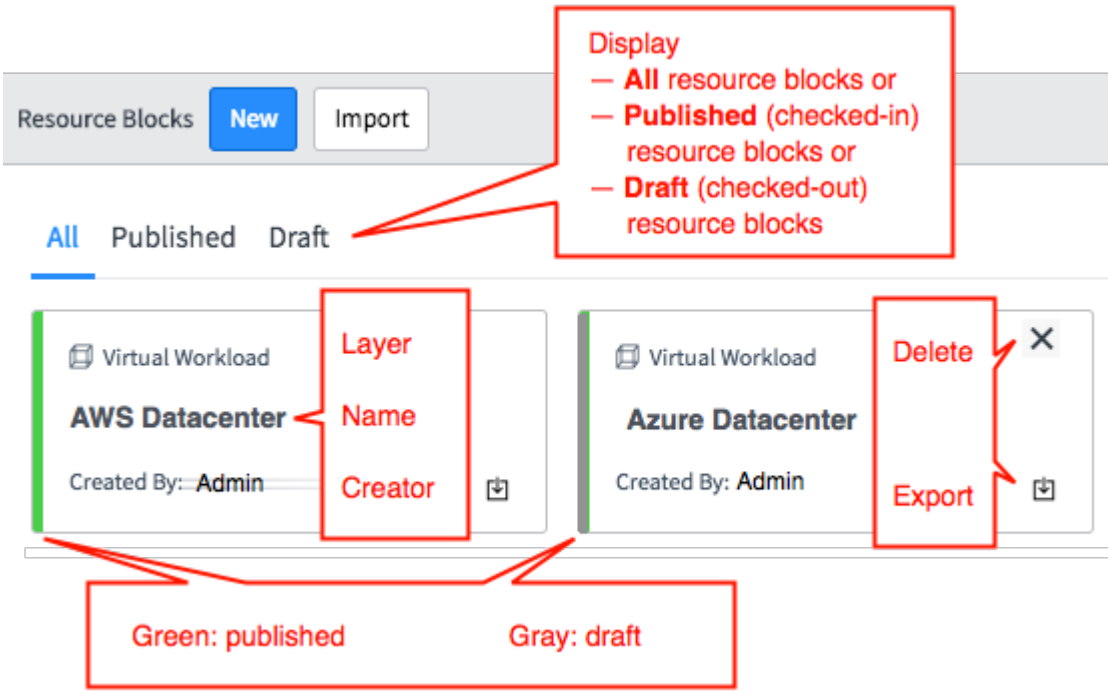
Die Seite „Ressourcenblöcke“

Verwalten Sie Ressourcenblöcke auf der Seite „Ressourcenblöcke“. Öffnen Sie das Cloud-Adminportal, und navigieren Sie dann zu **Entwurf** > **Ressourcenblöcke**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Komponenten der Seite „Ressourcenblöcke“



Benutzerdefinierten Ressourcenblock erstellen

Wenn die Blöcke im Basissystem nicht die erforderlichen Cloud-Ressourcen bereitstellen, können Sie einen benutzerdefinierten Ressourcenblock erstellen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Cloud-Adminportal** > **Entwurf** > **Ressourcenblöcke** und klicken Sie auf **Neu**.
2. Geben Sie einen eindeutigen und aussagekräftigen **Namen** und eine **Beschreibung** für den Ressourcenblock ein, und geben Sie dann die folgenden Einstellungen ein:

Ebene	Wählen Sie die Ebene aus, die den Typ des Ressourcenblocks darstellt: ◦ **Anwendung**: Ressourcen, die Anwendungen sind. Beispielsweise könnte die Anwendung PetStore auf einer Tomcat- oder WebLogic-Plattform vorhanden sein. ◦ **Plattform**: Ressourcen, die in der Regel auf einem virtuellen Server wie MySQL, Tomcat oder Apache gehostet werden. ◦ **Logisches Rechenzentrum**: Ressourcen, die Rechenzentren wie AWS, Azure oder vSphere sind. ◦ **Virtuelle Infrastruktur**: Ressourcen, die virtuell sind und dennoch eine Infrastruktur für die virtuelle Welt bieten, z. B.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	NetApp SVM, NetApp CDOT, CISCO ICF Cloud oder VMware NSX. ◦ **Virtueller Workload**: Ressourcen, die in einem Rechenzentrum gehostet werden. Beispielsweise virtueller Server, Speichervolume, Netzwerk oder Gateway. **Hinweis:** ◦ Anwendungen werden auf Plattformen bereitgestellt. ◦ Plattformen werden in logischen Rechenzentren oder virtuellen Infrastrukturen bereitgestellt.
CI-Typ	Wählen Sie den CI-Typ in Ihrer CMDB aus, der den Ressourcenblock darstellt. Wenn der Benutzer einen Stapel startet, werden die Cloud-Ressourcen bereitgestellt und tatsächliche CIs für die Ressourcen werden in der CMDB in diesem CI-Typ erstellt. Wenn Sie beispielsweise „Speichervolume“ auswählen, erstellt das System einen Datensatz in der Tabelle „Speichervolume“ [cmdb_ci_storage_volume], wenn der Benutzer ein neues Volume bereitstellt. **Hinweis:** Jeder Ressourcenblock basiert auf einem CI-Typ der CMDB. Stellen Sie sicher, dass nicht mehr als ein Ressourcenblock an einen CI-Typ gebunden ist.
Standardgastschnittstelle Schnittstelle erstellen	Wählen Sie die Gastschnittstelle aus, die die für die Ressource erforderlichen Vorgänge enthält. Später können Sie die für diese standardmäßige Gastschnittstelle zu verwendenden Vorgänge weiter definieren und auswählen. Das System bietet Ihnen eine Reihe von Standardvorgängen für jede Schnittstelle. Wenn ein anderer Ressourcenblock eine **Hostschnittstelle** spezifiziert (siehe die Beschreibung zum Feld „Hostschnittstelle“), die dem entspricht, was Sie hier im Feld **Gastschnittstelle** angeben, kann dieser Ressourcenblock ein potentieller Host für diesen Ressourcenblock sein. Wenn Sie das Kontrollkästchen **Schnittstelle erstellen** aktivieren, geben Sie einen Namen für die Gastschnittstelle ein. Das System erstellt die Gastschnittstelle, öffnet den Ressourcenblock, den Sie konfigurieren, im Ressourcenblockformular und listet die neue Schnittstelle in der zugehörigen Liste **Gastschnittstelle der Ressource** auf. Eine Beschreibung der Gastschnittstelle der Ressource finden Sie in den folgenden Schritten. Wenn Sie eine neue Gastschnittstelle erstellen, beachten Sie auch, dass andere Ressourcenblöcke die Schnittstelle verwenden können.
Hostschnittstelle	Wählen Sie die Schnittstelle aus, die der potenzielle Host dieses Ressourcenblocks anbieten muss. Jeder andere

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Ressourcenblock, der eine standardmäßige Gastschnittstelle desselben Typs bietet, den Sie hier angeben, kann ein Host dieser Ressource werden. Später können Sie eine oder mehrere tatsächliche Hostressourcen auswählen. Beispielsweise gibt der standardmäßige Ressourcenblock „AWS-Rechenzentrum“ die **Computing**-Schnittstelle als eine Standardgastschnittstelle an. Das bedeutet, dass das AWS-Rechenzentrum die **Computing**-Hostschnittstelle anderen Ressourcenblöcken anbietet, über die eine Verbindung mit dem AWS-Rechenzentrum hergestellt werden kann. Geben Sie die **Computing**-Schnittstelle hier als Hostschnittstelle des Ressourcenblocks an, damit der Ressourcenblock nach anderen Ressourcenblöcken suchen kann, die die **Computing**-Schnittstelle als Gastschnittstelle verwendet. Da das AWS-Rechenzentrum die **Computing**-Schnittstelle als Gastschnittstelle verwendet, können Sie das AWS-Rechenzentrum später in der zugehörigen Liste „Hostressource“ als tatsächlichen Host auswählen. Andere Ressourcenblöcke, die die **Computing**-Schnittstelle anbieten, indem **Computing** als Gastschnittstelle angegeben wird, sind ebenfalls potenzielle Hosts für diesen Ressourcenblock. Sie müssen wissen, welche Schnittstellen die potenziellen Hostressourcen als Gastschnittstellen anbieten. Und bestimmen Sie, welche Vorgänge Teil dieser Gastschnittstellen sind.

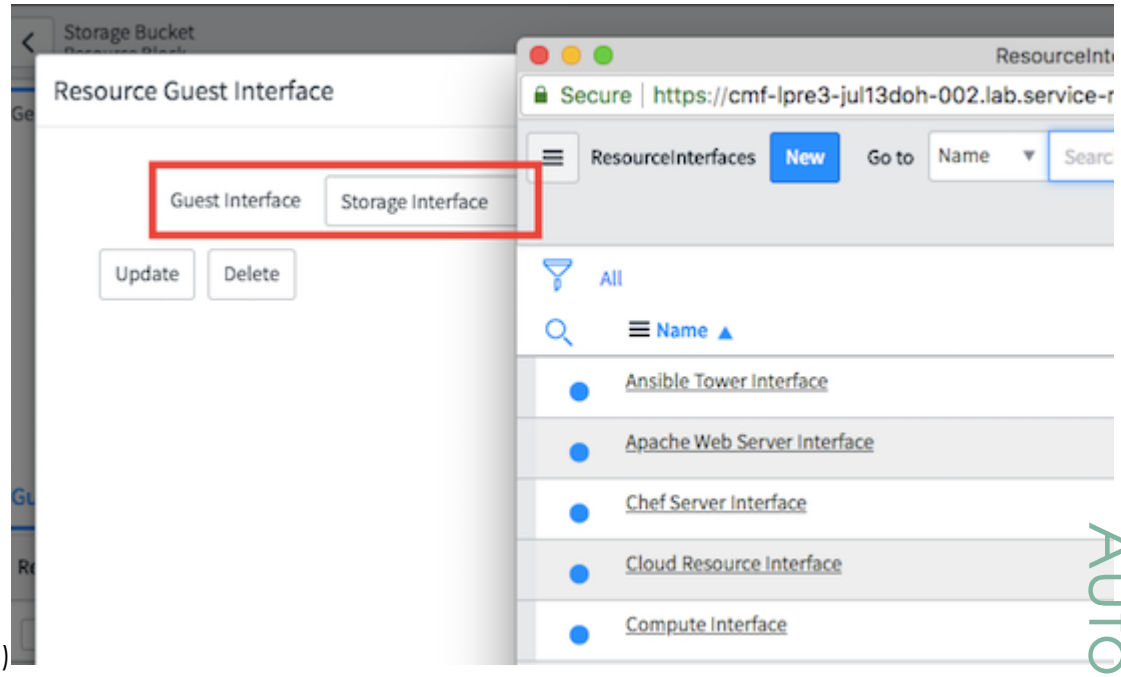
3. Klicken Sie auf **Absenden**.
   Setzen Sie die Aktualisierung der Einstellungen in den zugehörigen Listen bei Bedarf fort.
4. Wahlweise: Führen Sie die folgenden Schritte aus, um eine weitere Gastschnittstelle hinzuzufügen.
   Sie können eine zusätzliche Gastschnittstelle angeben, die anderen Ressourcenblöcken angeboten wird. Beispielsweise kann ein Ressourcenblock „Rechenzentrum“ eine **Computing**-Schnittstelle, eine **Netzwerkservicecontainer**-Schnittstelle und eine **Firewall**-Schnittstelle zur Verwendung durch andere Ressourcenblöcke bieten.

   a. Klicken Sie bei **Gastschnittstelle** auf **Neu**.

   b. Wählen Sie im Feld **Gastschnittstelle** eine Schnittstelle aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

(Optional)

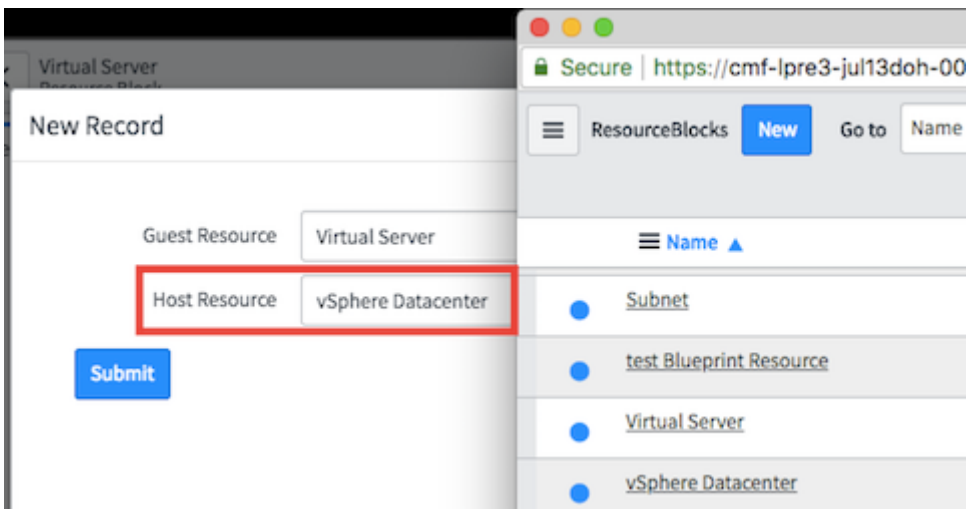


c. Klicken Sie auf **Absenden** oder **Aktualisieren**.

5. Geben Sie bei „Hostressource“ die Ressource an, die diesem Ressourcenblock als Host dienen kann, in der Regel diejenige, die die Schnittstelle anbietet, die Sie im Feld **Hostschnittstelle** angegeben.
Der ausgewählte Hostressourcenblock übernimmt die Bereitstellung dieses Ressourcenblocks. Beispiel: Die Hostressource ist ein Ressourcenblock „Virtueller Computer“, der einen Apache-Webserver hosten kann. Die Auswahl der Hostressource beschränkt die Optionen, die Benutzern bei der Auswahl eines Hosts angezeigt werden.

Example

Wählen Sie zum Beispiel **vSphere-Rechenzentrum** im Feld **Hostressource** aus, damit diese Ressource in einer VMWare Cloud gehostet werden kann.



Hinweis: Sie können nur die Hostressourcen auswählen, die die **Hostschnittstelle** unterstützen, die zuvor für diesen Ressourcenblock angegebenen wurden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wahlweise: Führen Sie die folgenden Schritte aus, um Bindungen hinzuzufügen.
   Eine Bindung ist ein weiterer Ressourcenblock, zu dem dieser Ressourcenblock eine Verbindung herstellen kann. Wählen Sie Ressourcenblöcke aus, die die gleiche **Gastschnittstelle** unterstützen, wie für diesen Ressourcenblock konfiguriert wurde.

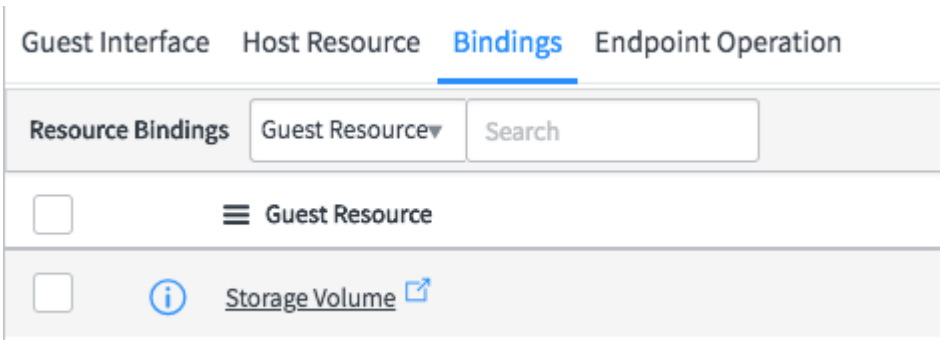
   Beim Erstellen einer Blaupause können Sie eine Angehängt-Verbindung zwischen zwei Ressourcenblöcken hinzufügen, die mit dieser Bindung verbunden sind. Für die Konfiguration des Ressourcenblocks ist es wichtig, die Richtung der Bindung zu verstehen. Sie hängen einen virtuellen Server einem Netzwerk an, oder Sie hängen Speicher einem virtuellen Server an. Sie können diese Richtungen nicht umkehren.

   a. Klicken Sie unter **Bindungen** auf **Neu**.

   b. Wählen Sie im Feld **Hostressource** eine Ressource im Feld **Gastressource** aus.
      Die Gastressource ist der Ressourcenblock, den Sie dem aktuellen Ressourcenblock anhängen.

   c. Klicken Sie auf **Absenden** oder **Aktualisieren**.

   Example
   Beispielsweise kann ein virtueller Server eine Verbindung mit virtuellem Speicher herstellen. Standardmäßig stellt das Basissystem einen Ressourcenblock „Virtueller Server“ mit einer Bindung zum Ressourcenblock „Speichervolume“ bereit, um diese Verbindung zu aktivieren.

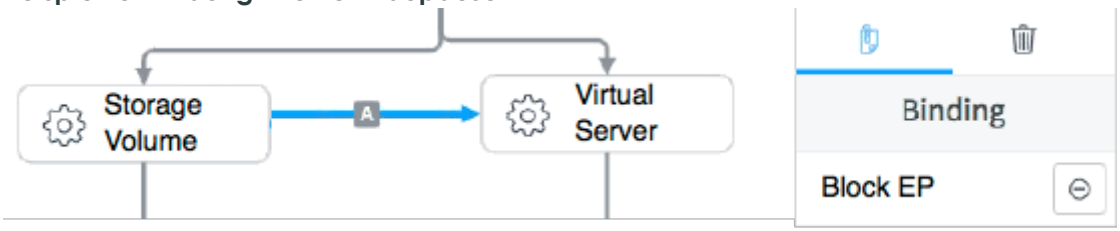
   (Optional)

7. Führen Sie die folgenden Schritte aus, um Endpunktvorgänge zwischen den beiden zu bindenden Ressourcen zu konfigurieren.
   Die Endpunkte rufen Vorgänge während der Bindung auf. Beispielsweise kann ein Speichervolume einen Endpunkt mit den erforderlichen Bedingungen und den auszuführenden Vorgängen angeben, um eine Verbindung zu einem virtuellen Server herzustellen. Der virtuelle Server muss auch eine Bindungsschnittstelle für das Speichervolume unterstützen.

   Implementieren Sie einen Endpunkttyp wie **Block-EP**, damit der virtuelle Server den Endpunkt verwendet. Später, wenn Sie Blaupausen erstellen, erstellen Sie die Bindung zwischen dem Speichervolume und dem virtuellen Server.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für Bindung in einer Blaupause



a. Klicken Sie unter **Endpunktvorgänge**auf **Neu**.

b. Wählen Sie unter **Bindungsressource** den Ressourcenblock aus, der den Endpunkt dieses Ressourcenblocks verwendet.

c. Wählen Sie den Endpunkttyp aus, den die **Quellressource** darstellt.

d. Wählen Sie unter **Vorgangsimplementierung** die Implementierung aus, die den Vorgang ausführt, den Sie in dieser Endpunktzuordnung definieren.

e. Wählen Sie den **Typ** des Vorgangs aus, der für die Zuordnung ausgeführt werden soll. Nur Vorgänge, die für den angegebenen **Endpunkt** geeignet sind, werden in der Liste angezeigt.

Ändern Sie nicht die Einstellungen in der **Quellressource**.

f. Klicken Sie auf **Absenden** oder **Aktualisieren**.

Hostressource für einen Ressourcenblock angeben

Hosts, die die **Hostschnittstelle** eines Ressourcenblocks unterstützen, sind potenzielle Hosts für den Ressourcenblock. Sie verwenden die Einstellung **Hostschnittstelle**, um die Optionen, die dem Anforderer des Stapels bei der Auswahl eines Hosttyps angezeigt werden, weiter einzuschränken.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Ressourcenblöcke**.
2. Wählen Sie den Ressourcenblock aus, und wählen Sie dann **Entwurf** im Formular **Ressourcenblöcke** aus:

3. Klicken Sie in der zugehörigen Liste **Hostressource** auf **Neu**.
   Auf dem Formular **Ressourcenhost** sind die **Anwendung** und die **Gastressource** (der Ressourcenblock, den Sie derzeit konfigurieren) bereits angegeben.
4. Geben Sie die **Hostressource** an.
   Beispielsweise können Sie für einen virtuellen Server **AWS-Rechenzentrum** oder **Azure-Rechenzentrum** als potenzielle Hosttypen auswählen.
5. Klicken Sie auf **Absenden**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geben Sie die Bindungen für Ressourcenblöcke an

Bindungen stellen Endpunktbeziehungen dar. Beispielsweise kann ein Speichervolume einen Endpunkttyp „Block-EP“ (cmdb_ci_endpoint_block) implementieren. Ein virtueller Server verwendet möglicherweise einen Endpunkt dieses Typs. Bindungen müssen die Gastschnittstelle unterstützen, die für den Ressourcenblock angegeben ist.

Vorbereitungen
Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Ressourcenblöcke**.
2. Wählen Sie den Ressourcenblock aus, und wählen Sie dann **Entwurf** im Formular **Ressourcenblöcke** aus:

3. Klicken Sie in der zugehörigen Liste **Ressourcenbindungen** auf **Neu**.
4. Auf dem Formular **Ressourcenbindung** sind die **Anwendung** und die **Gastressource** (der Ressourcenblock, den Sie derzeit konfigurieren) bereits angegeben.
   Geben Sie die **Bindungsressource** an.
5. Klicken Sie auf **Absenden**.

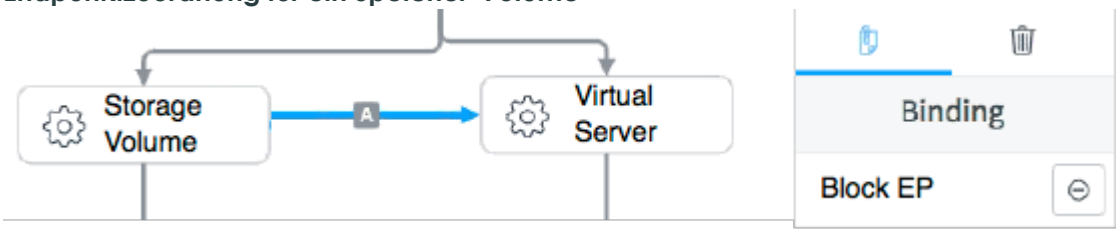
Endpunkt-Vorgangszuordnung konfigurieren

Sie können die Endpunktzuordnung eines Speichervolume konfigurieren, um eine Verbindung zu einer Ressource herzustellen.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Im folgenden Beispiel gibt die für ein Speichervolume konfigurierte Endpunktzuordnung die Bedingungen, die erfüllt sein müssen, und den Vorgang, der ausgeführt werden soll, an, um eine Verbindung zu einer Ressource herzustellen (im Beispiel ein virtueller Server), die eine Bindungsschnittstelle zu einem Speichervolume unterstützt. Das Speichervolume implementiert den Endpunkt (im Beispiel vom Typ „Block-EP“), und der virtuelle Server verwendet den Endpunkt:

Endpunktzuordnung für ein Speicher-Volume



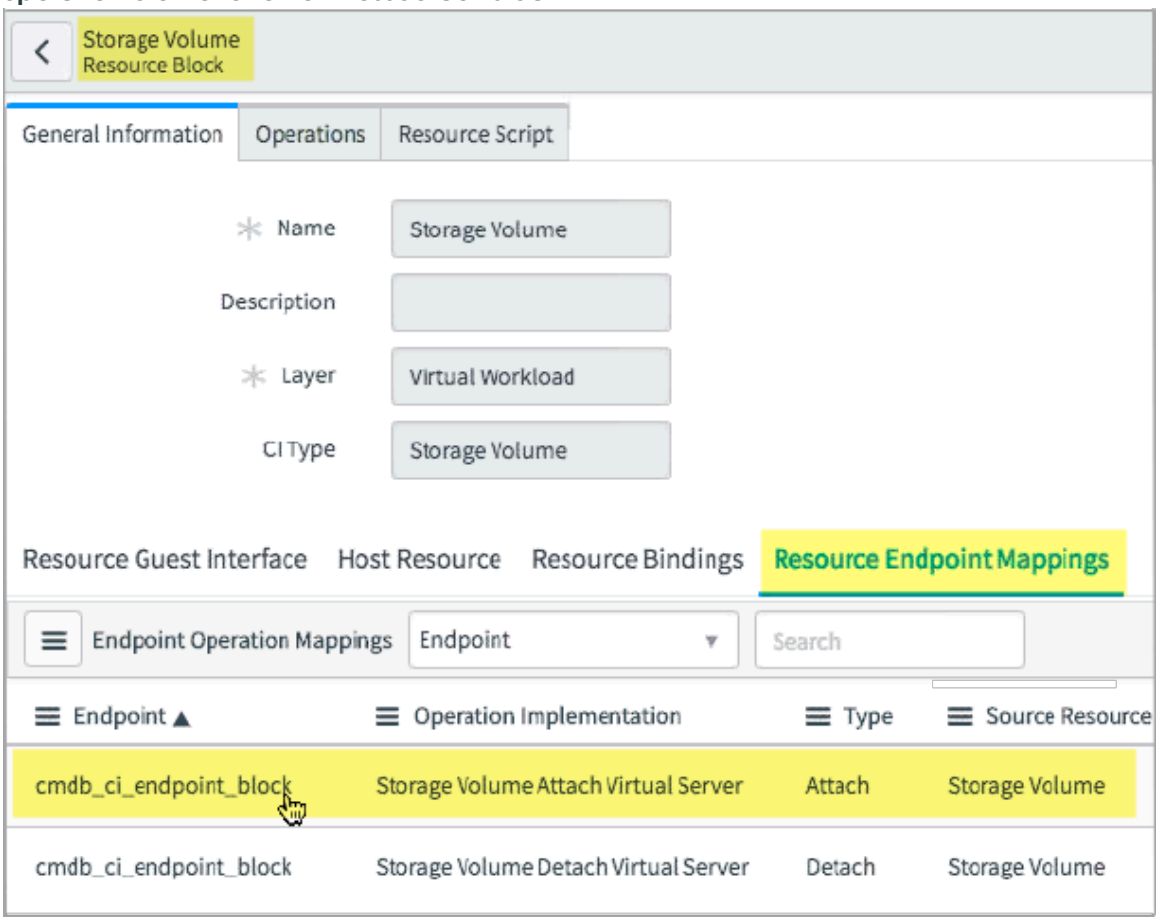
Die Einstellungen in der zugehörigen Liste **Ressourcenendpunkt-Zuordnungen** im Beispiel geben die Bedingungen und eine Aktion an:

- Für einen Ressourcenblock, der eine Bindungsschnittstelle für ein **Speichervolume** unterstützt
- Für eine **Quellressource** mit einem **CI-Typ** von **Speichervolume**
- Mit einem **Endpunkt** vom Typ **Block-EP** (cmdb_ci_endpoint_block)

Verwenden Sie den Vorgang **Anhängen**, um die Verbindung zu implementieren. Verwenden Sie die angegebene **Vorgangsimplementierung**, um den Vorgang **Anhängen** auszuführen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Speichervolume für einen Ressourcenblock



Prozedur

1. Öffnen Sie beim Konfigurieren eines Ressourcenblocks die zugehörige Liste **Ressourcenendpunkt-Zuordnung**, klicken Sie auf **Neu**, und geben Sie dann die folgenden Einstellungen an:

Bindungsressource	Ressourcenblock, der den **Endpunkt** verwendet, den die **Quellressource** darstellt.
Endpunkt	Endpunkttyp, den die **Quellressource** darstellt.
Typ	Typ des Vorgangs, der für die Zuordnung ausgeführt werden soll. Nur Vorgänge, die für den angegebenen **Endpunkt** geeignet sind, werden in der Liste angezeigt.
Vorgangsimplementierung	Implementierung, die zum Ausführen des Vorgangs aufgerufen wird, den Sie in dieser Zuordnung definieren.
Applikation	Schreibgeschützt. Cloud Provisioning and Governance-Anwendung.
Quellressource	Ressourcenblock, der einen **Endpunkt** des von Ihnen angegebenen Typs darstellen kann. Üblicherweise muss diese Einstellung nicht geändert werden.

2. Wiederholen Sie diese Vorgehensweise für die erforderliche Anzahl an Zuordnungen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eingabeparameter für Ressourcenblöcke konfigurieren

Sie können Vorgänge für jede Schnittstelle eines Ressourcenblocks konfigurieren, indem Sie Eingabeparameter, Schritte und Ausgabeattribute angeben. Eingabeparameter enthalten Werte, die das System zum Identifizieren und Verwalten einer virtuellen Ressource benötigt, z. B. das Rechenzentrum und die Ressourcengruppe, in der sich die Ressource befindet.

Vorbereitungen

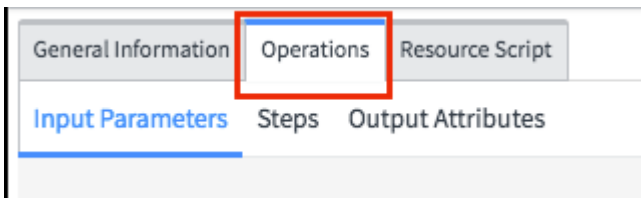
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Das System ordnet dem Ressourcenblock automatisch Standardvorgänge aus der Cloud API (CAPI) zu, wenn Sie ihm Schnittstellen hinzufügen. Es stellt auch Standardeingabeparameter für die einzelnen Vorgänge bereit.

Prozedur

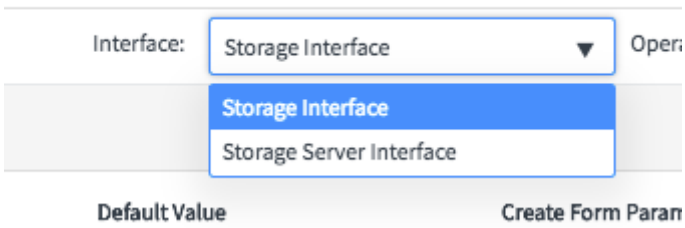
1. Öffnen Sie einen Ressourcenblock, und klicken Sie dann auf die Registerkarte **Vorgänge**.



   Die Unterregisterkarte **Eingabeparameter** wird standardmäßig angezeigt.

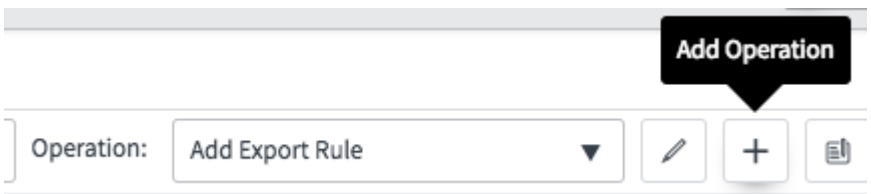
2. Wählen Sie die Schnittstelle aus der Auswahlliste **Schnittstelle** aus.

   Die Schnittstellen in dieser Auswahlliste sind von der Liste **Gastschnittstelle der Ressource** auf der Registerkarte **Allgemeine Informationen** abgeleitet, die Sie bereits beim Erstellen eines Ressourcenblocks konfiguriert haben.



3. Wählen Sie den Vorgang aus, für den Sie die Eingabeparameter ändern möchten. Sie können auch einen neuen Vorgang erstellen.

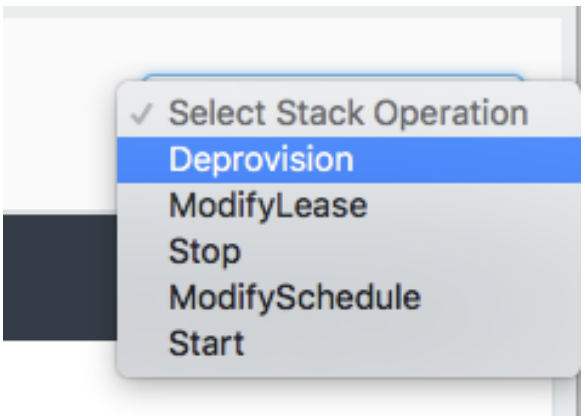
   a. Klicken Sie auf das Symbol **Vorgang hinzufügen**.



   b. Füllen Sie das Formular aus (siehe Tabelle):

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Name	Geben Sie einen beschreibenden Namen ein.
Vorgangstyp	Wählen Sie den Vorgangstyp aus der Auswahlliste aus.
Zugriffstyp	Wählen Sie **Öffentlich** aus, um den Ressourcenblockvorgang über das Katalogbestellformular verfügbar zu machen, wenn ein Benutzer einen Stapel verwaltet, dessen Besitzer er ist. Die tatsächlichen Vorgänge werden in einer Liste auf dem Katalogbestellformular angezeigt:  Wählen Sie **Privat** aus, um zu verhindern, dass der Vorgang verwendet wird, wenn ein Benutzer einen Stapel startet. Diese Einstellung gilt auf Katalogelementebene und nicht auf der Ebene des gesamten Stapel. Sie können den Zugriffstyp für den gesamten Stapel beim Konfigurieren von Blaupausen steuern. Beispiel: Sie möchten den Vorgang `Bereitstellung aufheben` für eine einzelne VM als privat markieren, aber nicht für den gesamten Stapel. Dies ermöglicht dem Benutzer, die Bereitstellung aller Elemente auf einmal aufzuheben, und verhindert, dass der Benutzer nur die Bereitstellung der VM aufhebt.

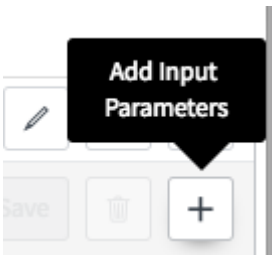
c. Klicken Sie auf **Absenden**.

4. Konfigurieren Sie die Eingabeparameter, um eine Möglichkeit zur Eingabe der Elemente bereitzustellen, die Sie zum Ausführen des ausgewählten Vorgangs benötigen.

Wenn Sie beispielsweise einen Bereitstellungsvorgang für eine AWS-Ressource hinzufügen, benötigen Sie mindestens den Parameter „CloudAccount“ und den Parameter „Standort“, um den Vorgang auszuführen. Sie müssen die Provider API kennen, um zu wissen, was an sie übergeben werden soll. Wenn Sie beispielsweise einen Bereitstellungsvorgang für einen S3-Bucket in AWS hinzufügen möchten, müssen Sie die zulässigen AWS-Vorgänge für Buckets und die Anforderungselemente für Dinge wie das Erstellen eines Bucket (den PUT-Bucket-Vorgang) kennen. Sie finden diese Ressourcen normalerweise in der AWS- und der Azure-Dokumentation.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf das Symbol **Eingabeparameter hinzufügen**.



b. Fügen Sie den **Namen** des Parameters hinzu, den Sie von der Cloud-Provider API erhalten haben.
In diesem Beispiel können Sie `CreateBucketConfiguration` für einen AWS S3-Bucket hinzufügen.

c. Wählen Sie in der Spalte **Datenquelle** den Typ des Eingabeparameters aus, den Sie konfigurieren.
Dieser Wert gibt die Quelle oder den Standort an, aus dem der Parameterwert stammt:

- **Text**: Ein Textwert, den der Benutzer übergibt.
- **Pools**: Die Abfrage, die für einen Pool ausgeführt werden soll, um einen Wert zu erhalten. Der Pool **Datenquellenwert** muss der folgenden Konvention entsprechen: `ServiceNow::Pools::PoolName.Pool-Filter-Name`. Weitere Informationen zu Pools finden Sie unter Pools und Filter für Cloud Provisioning.
- **CSVList**: Werte aus einer kommagetrennten Werteliste, die Sie in den **Datenquellenwert** eingeben.
- **Array**: Ein Array von Werten. Sie können ihm programmgesteuert ein Array in JavaScript senden. Das Format ist wie folgt: `['abc','def']`.
- **FormData**: Daten, die von dem in der Blaupause konfigurierten Formular übermittelt wurden.
- **ResourceScript**: Ein Ausdruck, der einen Wert übergibt. Der Ausdruck muss im Feld **Zuordnung** dieser Konvention entsprechen:

  ```
  $(Script:script-name.function[arg1=${Übergabewert},arg2=
  ${Übergabewert}])
  ```

- **TLR**: Der Wert, der vom Ressourcencontainer der obersten Ebene über diesem Ressourcenblock in der Blaupause geerbt wurde.

d. Klicken Sie auf **Speichern**.

e. In der Spalte **Zuordnung** können Sie sich die automatisch generierten Zuordnungswerte ansehen.
Zuordnungen geben an, wo die Informationen im System abgerufen werden. Sie müssen die Zuordnungswerte nur für Parameter des Typs **ResourceScript** ändern, wo Sie den Ausdruck eingeben müssen.

f. Geben Sie in der Spalte **Standardwert** einen Wert ein, den das System verwenden soll, wenn der Benutzer keinen Wert übergibt oder wenn Sie nichts in den **Datenquellenwert** eingegeben haben.

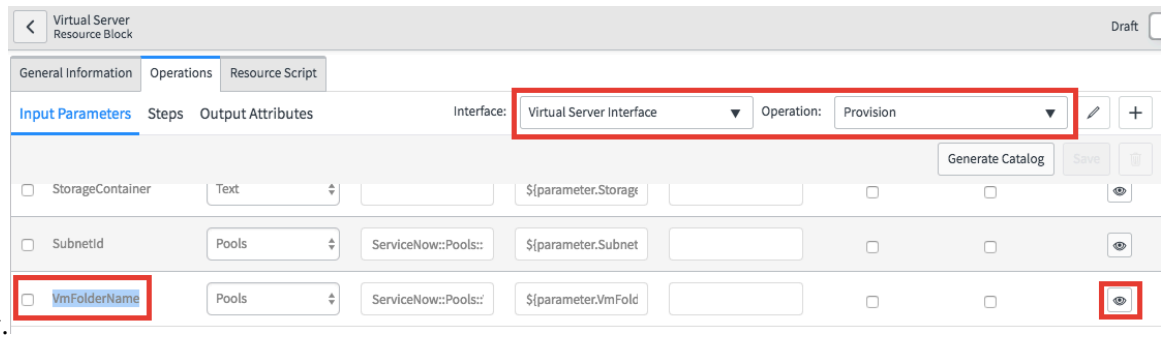
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

g. Wählen Sie **Formular erstellen** aus, um dieses Attribut im Bestellformular verfügbar zu machen, das dem Benutzer beim Bereitstellen des Stapelelements angezeigt wird. Sie können auch **Obligatorisch** auswählen, um die Eingabe des Benutzers zu erzwingen.

h. Klicken Sie in der Spalte **Eingeschränkt auf** auf das Eingeschränkt-Symbol ( ), und wählen Sie dann einen Ressourcenblock aus, um das Attribut einzuschränken, das an einen bestimmten Host übergeben werden soll.

In diesem Beispiel konfigurieren Sie einen Ressourcenblock für einen virtuellen Server in vSphere, für den der Name des VM-Ordners (dargestellt durch das Attribut `VmFolderName`) erforderlich ist. Für andere Rechenzentrumstypen ist der Name des VM-Ordners nicht erforderlich. Daher können Sie `VmFolderName` auf den Ressourcenblock des vSphere-Rechenzentrums beschränken.

Dieses Bild zeigt, wie das Attribut „VMFolderName“ auf das vSphere-Rechenzentrum beschränkt ist.



Vorgangsschritte einem Ressourcenblock hinzufügen

Nachdem Sie Vorgänge und Eingabeparameter für Ihren Ressourcenblock konfiguriert haben, fügen Sie für jeden Vorgang Schritte hinzu, um dem System mitzuteilen, welche Cloud API (CAPI) aufgerufen werden soll. Jeder Schritt ist ein eigener Aufruf von CAPI.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur

1. Klicken Sie im Ressourcenblock unter **Vorgänge** auf die Unterregisterkarte **Schritte**.
2. Klicken Sie auf **Schritt hinzufügen**.
3. Füllen Sie die Formularfelder aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Vorgangstyp	Wählen Sie die Art des Vorgangs aus: ◦ **Cloud API aufrufen**: Wählen Sie diese Option aus, um einen Provider, eine Schnittstelle und eine Methode aus der CAPI auszuwählen. ◦ **Hostressourcenvorgang aufrufen**: Wählen Sie diese Option aus, um einen Vorgang (auch Vorgangssignatur genannt) aus der Hostschnittstelle zu verwenden, die Sie bereits für diesen Ressourcenblock angegeben haben. ◦ **Skript aufrufen**: Wählen Sie diese Option aus, um eine Methode aus einer vorhandenen MID Server-Skripteinbindung aufzurufen. ◦ **Workflow aufrufen**: Wählen Sie diese Option aus, um einen vorhandenen Workflow aufzurufen, durch den Vorgänge für diesen Ressourcenblock ausgelöst werden. ◦ **Flow aufrufen**: Wählen Sie diese Option aus, um Subflows aus einer Liste aktiver Subflows aufzurufen.
API-Anbieter [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die API aus, die die erforderlichen Schnittstellen bereitstellt. Die Provider sind Teil der Cloud API (CAPI). Beispielsweise stellt CAPI den AWS-Provider bereit, der über Produkte verfügt, von denen einige Provider-Namen aufweisen. Dieser Wert wird angezeigt, wenn Sie den Vorgangstyp „Cloud API aufrufen“ auswählen.
API-Schnittstelle [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die Schnittstelle mit den Methoden aus, die Sie verwenden möchten. Beispielsweise stellt die **Blob-Speicher-Schnittstelle** die **CreateContainer**-Schnittstelle bereit, die das System während der Bereitstellung verwendet.
API-Methode [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die Methode aus, mit der der Vorgang ausgeführt werden soll. In diesem Beispiel ist **CreateContainer** erforderlich, um Speicher bereitzustellen.
CAPI-Version [Vorgangstyp = Cloud API aufrufen]	Geben Sie eine Version für die CAPI API ein.
Hostschnittstelle [Vorgangstyp = Hostressourcenvorgang aufrufen]	Wählen Sie die Schnittstelle aus, über die ein Vorgang aufgerufen werden soll. Sie können nur die Schnittstelle auswählen, die Sie auf der Registerkarte **Allgemeine Informationen** des Ressourcenblocks konfiguriert haben. Um die Schnittstelle zu ändern, navigieren Sie zurück zur Registerkarte **Allgemeine Informationen** und wählen Sie einen anderen Wert im Feld **Hostschnittstelle** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Schnittstellenvorgang [Vorgangstyp = Hostressourcenvorgang aufrufen]	Wählen Sie den Vorgang der Hostschnittstelle aus. Wenn Sie beispielsweise die Schnittstelle **Speicherserver** auswählen, können Sie alle Vorgänge in dieser Schnittstelle aufrufen, z. B. *`CreateStorageVolume`*.
Skripts [Vorgangstyp = Skript aufrufen]	Geben Sie das Skript ein, das Sie aufrufen möchten, und geben Sie auch die Methode im Skript an. Verwenden Sie folgende Syntax: `Skriptname.Methode`.
Workflow [Vorgangstyp = Skript aufrufen]	Verwenden Sie keinen Workflow.
Fluss [Vorgangstyp = Flow aufrufen > Subflow]	Wählen Sie den Subflow aus der Liste „Subflows“ aus. Wenn Sie beispielsweise einen Subflow für die Terraform Enterprise-Bereitstellung auswählen, können Sie den vorhandenen Subflow einfach wiederverwenden, um die Eingaben und Ausgaben entsprechend zu füllen.
Bedingung	Geben Sie eine optionale Bedingung ein, die erfüllt sein muss, bevor das System diesen Schritt verwendet.

Bei der Azure-API und der Methodenzuordnung „CreateNode“ können Sie sehen, dass der Endpunktvorgang ein Skript ist. Es ruft die MID Server-Skripteinbindung auf, die Ihnen die Funktion *`createNode()`* anzeigt. Diese Funktion verwendet die Skripteinbindung *`AzureComputeVirtualMachine`*. Nehmen Sie sich Zeit, um sich diese Skripteinbindung anzusehen und sie zu verstehen.

4. Klicken Sie auf **Absenden**.

   Die Registerkarten **Eingabe** und **Antwortprozessor** werden für den Schritt angezeigt.

5. Konfigurieren Sie auf der Registerkarte **Eingabe** die CAPI-Vorgangseingaben.

   Öffnen Sie auf der CAPI-Schnittstelle (in diesem Fall die Schnittstelle **Blob-Speicher**) die Methode *`CreateContainer`*. Die Eingaben von CAPI werden auf der Registerkarte „Eingabe“ angezeigt, auf der Sie Parameter erstellen.

   Denken Sie daran, dass die Parameter auf der Registerkarte **Eingabeparameter** durch Benutzer ausgefüllt werden. Sie können diese Eingabeparameter den Parametern auf der Registerkarte **Eingabe** zuordnen. Kopieren Sie dazu den **Zuordnungswert** von der **Registerkarte Eingabeparameter** in das Feld **Wert** in **Schritte** > **Eingabe** Registerkarte

   Wenn dieser Schritt ein Skript aufruft und dieses Skript Argumente zur Rückgabe von Werten erfordert, können Sie für jedes Argument einen neuen Eingabeparameter hinzufügen. Verwenden Sie diese Syntax im Feld **Wert**: `${parameter.arg1}`.

6. Wenn für nachfolgende Schritte in diesem Vorgang oder nachfolgenden Vorgängen die Übergabe von Parameterwerten aus diesem Schritt erforderlich ist, konfigurieren Sie Ausgabeattribute.

   Beispielsweise kann der Vorgang der Bereitstellung für einen virtuellen Server ein Ausgabeattribut für die Netzwerkschnittstellen-ID und ein anderes für die Knoten-ID bereitstellen. Wenn der Cloud-Provider die Antwort sendet, werden die tatsächliche ID des

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerks und die des Knotens aus der Antwort analysiert und in den Ausgabeattributen gespeichert. Nachfolgende Schritte können dann die IDs zum Ausführen von Aktionen verwenden.

a. Klicken Sie auf die Registerkarte **Ausgabeattribute**.

b. Geben Sie Code in der folgenden Schreibweise ein:

```
{
  "Attribute": "${Value}"
}
```

Der Wert stammt dabei aus einer Zuordnung zur Schnittstelle und zum Vorgang.

Sehen Sie sich als Beispiel das folgende Ausgabeattribut an:

```
{
  "NodeId": "${Compute Interface.CreateNode.Output.resp.nodeId}"
}
```

- `NodeId` ist das Attribut.
- `Compute Interface` gibt die Schnittstelle an.
- `CreateNode` ist der Name der Methode, die den Knoten erstellt.
- `Output.resp` ist ein obligatorischer Teil der Syntax.
- `nodeId`

Vorgang einem Ressourcenblock zur Verwendung mit einem Workflow hinzufügen

Sie können aus den vorhandenen Vorgängen in einem Ressourcenblock auswählen, um mit Ihrem Workflow zu arbeiten, oder Sie können einen benutzerdefinierten Vorgang erstellen.

Vorbereitungen

Erforderliche Rolle: cloud designer oder admin

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Ressourcenblöcke**.
2. Wählen Sie einen Ressourcenblock aus, z. B. **Virtueller Server**.
3. Ändern Sie den Status des Ressourcenblocks von **Veröffentlicht** in **Entwurf**, um ihn bearbeitbar zu machen.
4. Wählen Sie die Registerkarte **Vorgänge** aus.
5. Wählen Sie im Dropdown-Feld „Schnittstelle“ eine Schnittstelle aus, die dem Benutzer zur Verfügung steht.
   Die Standardschnittstelle ist **Virtuelle Serverschnittstelle**.
6. Klicken Sie rechts neben dem Feld „Vorgang“ auf **+**, und führen Sie diese Schritte im Dialogfeld „Vorgang hinzufügen“ aus:
   a. Geben Sie einen aussagekräftigen und eindeutigen Namen ein.
   b. Wählen Sie einen Vorgang aus der Dropdown-Liste „Vorgangstyp“ aus.
   c. Wählen Sie im Feld „Zugriffstyp“ die Option **Öffentlich** aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.

Vorgangstyp	Wählen Sie den auszuführenden Vorgang aus.
Zugriffstyp	Wählen Sie **Öffentlich** aus, damit der Benutzer den Vorgang während der Bereitstellung auf Ressourcenebene sehen kann. Auf **Privat** festgelegte Vorgänge sind während der Bereitstellung nicht sichtbar.

Der Vorgang ist für die Ressource verfügbar, wenn Sie die Ressource für Ihren Workflow auswählen.

Nächste Maßnahme

Ressourcenvorgangsschritt zum Aufrufen eines Workflows hinzufügen

Ressourcenvorgangsschritt zum Aufrufen eines Workflows hinzufügen

Sie können einen Workflow aufrufen, indem Sie einer Ressource einen Vorgangsschritt hinzufügen und die Ressource dann einem Workflow zuordnen.

Vorbereitungen

- Die Orchestration-Anwendung ist installiert.
- Erforderliche Rolle: Cloud-Benutzer, -Designer oder Administrator

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Ressourcenblöcke**.
2. Klicken Sie auf den Ressourcenblock, dem ein Vorgangsschritt hinzugefügt werden soll.
3. Setzen Sie den Ressourcenblock auf den Status **Entwurf**, und klicken Sie dann auf **Vorgänge** > **Schritte** > **Schritt hinzufügen**.
   Damit der Workflow als Teil der Update Sets exportiert werden kann, müssen Sie eine Erweiterungsschnittstelle erstellen und den neuen Vorgang hinzufügen. Weitere Detailinformationen finden Sie unter Cloud Provisioning and Governance-Ressourcenblöcke mit einem Überschreibungsvorgang erweitern.
4. Wählen Sie im Popup-Fenster „Vorgangschritte hinzufügen“ für **Vorgangstyp** die Option **Workflow aufrufen** aus.
5. Wählen Sie den **Workflow** aus der Liste der von Ihnen erstellten Workflows aus.
   Das System kann die Liste anhand von Tags filtern. So fügen Sie ein Tag hinzu:
   a. Navigieren Sie zu **Systemeigenschaften**.
   b. Suchen Sie nach der Systemeigenschaft *sn_cmp.workflow_tag_filter*, und wählen Sie sie aus.
   c. Bearbeiten Sie die Eigenschaft. Fügen Sie ein Tag oder eine kommagetrennte Liste von Tags hinzu.
   d. Klicken Sie auf **Speichern**.
6. Filtern Sie die Workflows.
   a. Öffnen Sie in der Workflow-Tabelle den Workflow.
   b. Klicken Sie auf **Tag hinzufügen**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Geben Sie den Wert ein, den Sie zuvor in der Eigenschaft *sn_cmp.workflow_tag_filter* angegeben haben.

d. Klicken Sie auf **Eingeben**.
Der Wert wird dem Workflow als Tag hinzugefügt.

Der neue Schritt wird angezeigt, nachdem die Software den neuen Vorgangskatalog für Tag 2 generiert hat.

7. Fügen Sie einen Workflow hinzu.
   a. Nachdem Sie den Schritt erstellt haben, fügt das System die Workflow-Eingaben den Vorgangseingabeparametern hinzu.
   b. Geben Sie bei Bedarf die Zuordnung für diese Parameter an.
   c. Klicken Sie auf die Schaltfläche **Katalog generieren**, um das Katalogelement für den Vorgang zu erstellen.
   d. Nachdem der Katalog generiert wurde, können Sie den Katalogelementen Regeln aus den Lade- und Feldänderungsregeln hinzufügen.
   Es können Workflows vorhanden sein, die in anderen als globalen Tabellen erstellt wurden. Sie können einen Workflow hinzufügen, der für eine solche Tabelle erstellt wurde. Zum Ausführen von Vorgängen für diese Art von Workflow benötigen Sie die sys_id des Datensatzes, in dem der Workflow ausgeführt wird, um den aktuellen Datensatz zu erstellen. Wenn der Designer einen Workflow hinzufügt, der sich in einer anderen als der globalen Tabelle befindet, erstellt das System einen *wf_current*-Parameter im Vorgangseingabeparameter. Sie können dann einen Ausdruck schreiben, um die sys_id der Ressource zuzuordnen, in der der Vorgang ausgeführt wird. Sobald dies abgeschlossen ist, kann der Designer das Schlüsselwort „aktuell“ in Workflow-Skripts verwenden.
8. Setzen Sie den Ressourcenblock auf den Status **Veröffentlicht**, um den Workflow im Cloudbenutzerportal verfügbar zu machen.

Ressourcenvorgangsschritt zum Aufrufen eines Subflows hinzufügen

Rufen Sie einen Subflow auf, indem Sie einer Ressource einen Vorgangsschritt hinzufügen und dann die Ressource einem neuen oder vorhandenen Subflow zuordnen.

Vorbereitungen

- Die Orchestration-Anwendung ist installiert.

Erforderliche Rolle: Cloud-Benutzer, -Designer oder Administrator

Warum und wann dieser Vorgang ausgeführt wird

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Ressourcenblöcke**.
2. Klicken Sie auf den Ressourcenblock, dem ein Vorgangsschritt hinzugefügt werden soll.
3. Setzen Sie den Ressourcenblock auf den Status **Entwurf**, und klicken Sie dann auf **Vorgänge** > **Schritte** > **Schritt hinzufügen**.
   Das Formular „Vorgangsschritt“ wird angezeigt.
4. Wählen Sie **Flow aufrufen** aus der Liste **Vorgangstyp** aus.
5. Wählen Sie **Subflow** aus der Liste **Flow-Typ** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Während Sie einen Ressourcenvorgangsschritt hinzufügen, können Sie keine Flows aufrufen. Dies ist eine bekannte Einschränkung.

6. Wählen Sie in der Nachschlageliste **Flow/Subflow** einen aktiven Subflow aus.
7. Wahlweise: Geben Sie eine Bedingung im Feld **Bedingung** an.
8. Klicken Sie auf **Absenden**.
   Der Subflow-Vorgangsschritt wird dem Ressourcenblock angefügt und auf der Seite angezeigt. Alle dem von Ihnen ausgewählten Subflow zugeordneten Eingabeparameter werden auf der Registerkarte **Eingabe** automatisch ausgefüllt.
9. Klicken Sie auf der Unterregisterkarte **Eingaben** auf das Symbol , um einen neuen Schrittparameter hinzuzufügen.

   a. Fügen Sie dem Subflow das folgende Schlüssel-Wert-Paar hinzu.

Schlüssel	Wert
flowcorrelationid	$(Script:CMPFlowStepHandler.generateCorrelation

10. Klicken Sie auf die Registerkarte **Antwortprozessor**, und klicken Sie dann auf das Pluszeichen.
    Das Dialogfeld „Antwortprozessor hinzufügen“ wird angezeigt.
11. Wählen Sie in der Liste **Skriptname** ein Skript für den Antwortprozessor aus.
    Damit ein Skript in der Liste **Skriptname** angezeigt wird, muss es bereits auf der Registerkarte **Ressourcenskript** erstellt worden sein. Weitere Informationen finden Sie unter Antwortprozessor konfigurieren.
12. Klicken Sie auf **Absenden**.
13. Setzen Sie den Ressourcenblock auf den Status **Veröffentlichen**, um Ihre Änderungen zu übernehmen und den Ressourcenblock zu veröffentlichen.

Nächste Maßnahme
Erstellen Sie eine Antwortaktion für Cloud Provisioning and Governance

Cloud Provisioning and Governance-Ressourcenblöcke mit einem Überschreibungsvorgang erweitern

Sie können Ihre vorhandene Gastschnittstelle erweitern, um einen neuen Vorgang zu erstellen. Sie können auch eine neue Gastschnittstelle mit eigenen Vorgängen, Parametern und Eingaben erstellen.

Vorbereitungen
Machen Sie sich mit den Eingabeparametern, Vorgängen und Schritten für Ressourcenblöcke vertraut. Weitere Informationen finden Sie unter Eingabeparameter für Ressourcenblöcke konfigurieren und Vorgangsschritte einem Ressourcenblock hinzufügen.

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird
Die Cloud Provisioning and Governance-Anwendung ist mit mehreren nützlichen Ressourcenblöcken gebündelt. Erstellen Sie Erweiterungen für die Schnittstellen vorhandener Ressourcenblöcke, um diesen Ressourcenblöcken mehr Funktionalität hinzuzufügen. Nachdem Sie eine Schnittstellenerweiterung erstellt haben, verwenden Sie sie in

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

einer Blaupause, um einen benutzerdefinierten Vorgang auszuführen. Wenn Ihnen beispielsweise die Art der Bereitstellung eines virtuellen Servers nicht gefällt, erweitern Sie die Ressourcenblockschnittstelle des virtuellen Servers, indem Sie Vorgänge hinzufügen oder vorhandene Vorgänge überschreiben.

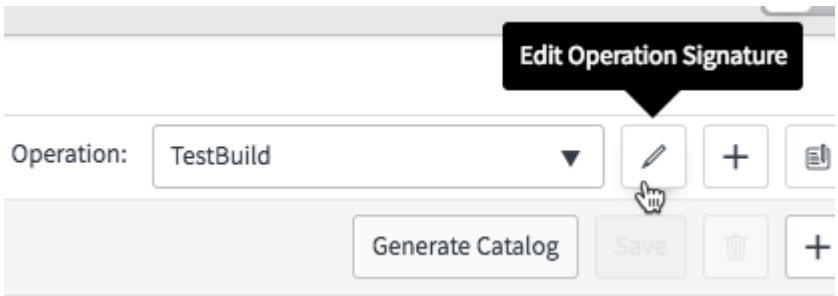
Hinweis: Vorgänge in Ressourcenblöcken werden auch Vorgangssignaturen genannt.

Prozedur

1. Öffnen Sie einen Ressourcenblock.
2. Ändern Sie den Status des Ressourcenblocks von **Veröffentlicht** in **Entwurf**.
3. Klicken Sie auf die Registerkarte **Vorgänge**.
4. Klicken Sie auf das Symbol **Vorgang überschreiben**.

5. Wählen Sie eine vorhandene Gastschnittstelle aus, oder aktivieren Sie das Kontrollkästchen **Neu erstellen**, um eine neue Gastschnittstelle zu erstellen.
6. Wahlweise: Wenn Sie eine Schnittstelle erstellen, geben Sie einen Namen in das Feld **Schnittstelle** ein.
7. Klicken Sie auf **Absenden** oder **Aktualisieren**.
   Der neue Vorgang wird in der Liste **Vorgang** angezeigt. Wenn Sie eine neue Schnittstelle erstellen, wird sie in der Liste **Schnittstelle** angezeigt.
8. Konfigurieren Sie die erforderlichen Eingabeparameter, Schritte und Ausgabeattribute für Ihre neue Gastschnittstelle.
9. So bearbeiten Sie den Vorgang oder ändern den Zugriffstyp:

   a. Klicken Sie auf das Symbol **Vorgangssignatur bearbeiten**.



   b. Ändern Sie bei Bedarf den **Vorgangstyp**, und fügen Sie unten Eingabeparameter hinzu, bearbeiten oder entfernen sie.

   c. Wenn der Blaupausendesigner den Vorgang nur dann direkt an der Ressource ausführen soll, wenn sie instanziiert wird, wählen Sie **Privat** als **Zugriffstyp** aus.

   d. Klicken Sie auf **Aktualisieren**.

10. Nach Abschluss der Anpassungen stellen Sie den Umschalter auf **Veröffentlicht**.
11. Navigieren zu **Cloud-Adminportal** > **Entwurf** > **Blueprints**.
12. Führen Sie die Schritte in Cloud Provisioning-Blaupause erstellen aus, um eine Blaupause hinzuzufügen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

13. Klicken Sie auf **Vorgänge**, und klicken Sie im Ressourcenblock auf den Vorgang, den Sie ändern möchten.
    Die Standardschnittstelle des Ressourcenblocks wird in der rechten Spalte angezeigt.
14. Klicken Sie auf das Symbol **Ressourcenvorgang bearbeiten** (Bleistift), um die von Ihnen erstellte Schnittstellenerweiterung anzuwenden.
15. Klicken Sie auf **Absenden**.
    Die Blaupause wird mit der benutzerdefinierten Schnittstellenerweiterung ausgeführt.

Ergebnisse
Nachdem Sie diesen Ressourcenblock einer Blaupause hinzugefügt haben, können Sie die hinzugefügten Parameter anpassen.

Ressourcenblock ein Ressourcenskript hinzufügen

Ein Ressourcenskript wird während der Bereitstellung auf einer Ressource ausgeführt oder gibt Daten an die CMDB zurück, nachdem eine Ressource bereitgestellt wurde.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Prozedur
1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Ressourcenblöcke**.
2. Öffnen Sie den Ressourcenblock, und legen Sie ihn auf den Status **Entwurf**

   fest.
3. Geben Sie auf der Registerkarte **Ressourcenskript** einen eindeutigen und aussagekräftigen **Namen** ein, und definieren Sie dann das Skript:

Skript	Skriptcode.
Typ	Skripttyp: ◦ Instanzskript: Javascript, das einen Vorgang für die Instanz ausführt (z. B. einen Workflow). ◦ PowerShell-Skript ◦ Python-Skript ◦ Antwortprozessor: Konvertiert Rückgabedaten von der externen Cloud API an die Vorgangsimplementierung in ein Format, das von der CMDB akzeptiert wird. ◦ Shell-Skript

4. Klicken Sie auf **Absenden**.
   Fügen Sie so viele Skripts wie nötig hinzu.

Antwortprozessor konfigurieren

Konfigurieren Sie einen Antwortprozessor für die Verarbeitung von Antworten von Rechenzentren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Die CI-Klassentypen für Ihre Ressourcen müssen bereits in der CMDB vorhanden sein. Wenn Sie benutzerdefinierte Produkte oder Provider in CAPI erstellt haben, müssen Sie auch benutzerdefinierte CI-Typen erstellen, damit der Antwortprozessor CIs identifizieren kann. Informationen zum Erstellen von CI-Typen finden Sie unter Eine CI-Klasse für eine virtuelle Cloud-Ressource erstellen.

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Nachdem jeder Schritt abgeschlossen ist, sendet das Rechenzentrum eine Antwort an die ECC-Warteschlange für den MID-Server. Beispiel: Wenn ein Benutzer einen virtuellen Server in einem AWS-Rechenzentrum bereitstellt, sendet AWS Informationen über den neuen virtuellen Server an die ECC-Warteschlange. Das System muss in der CMDB ein CI für den virtuellen Server erstellen. Dazu wird ein Antwortprozessor verwendet.

Alternativ dazu können Sie die musterbasierte gezielte Erkennung verwenden, um Antworten aus den Rechenzentren zu verarbeiten. Weitere Informationen finden Sie unter Musterbasierte gezielte Erkennung.

Hinweis: Der Ressourcentyp, für den Sie das Antwortprozessorskript hinzufügen, muss in der Tabelle [sn_capi_resource_type] vorhanden sein.

Prozedur

1. Öffnen Sie einen Ressourcenblock, und klicken Sie auf die Registerkarte **Ressourcenskript**. Stellen Sie sicher, dass sich der Ressourcenblock nicht im Status „Veröffentlicht“ befindet.
2. Klicken Sie auf **Neu**.
3. Geben Sie im Feld **Name** den Namen für das Ressourcenskript ein.
4. Geben Sie ein Skript in das Feld **Skript** ein.
5. Klicken Sie auf **Absenden**.
6. Klicken Sie im Ressourcenblock auf die Registerkarte **Vorgänge**.
7. Klicken Sie auf die Unterregisterkarte **Schritte**.
8. Klicken Sie auf einen Schritt.
9. Klicken Sie bei dem Schritt auf die Registerkarte **Antwortprozessor**.
10. Klicken Sie auf das Hinzufügen-Symbol (+).
11. Wählen Sie im Feld **Skriptname** den Prozessor aus, den Sie gerade erstellt haben.
12. Klicken Sie auf **Absenden**.
    Das Antwortprozessorskript kann die Antwort des Cloud-Providers für den CI-Typ des Ressourcenblocks verarbeiten.

Antwortprozessor für Workflow ausführen

Führen Sie einen Antwortprozessor für einen Workflow aus, um die Workflow-Daten wieder in ein Configuration Item (CI) abzurufen. Der Antwortprozessor nimmt die Daten auf und sendet sie an die CMDB, die die Daten wiederum in ein CI einfügt.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Bevor Sie einen Antwortprozessor für einen Workflow ausführen, müssen Sie einen Workflow erstellen, den Workflow an einen Vorgangsschritt eines Ressourcenblocks anhängen und dann den Katalog generieren. Um die Antwort aus dem Workflow an die Cloud Provisioning and Governance-Anwendung zurückzugeben, muss der Workflow-Designer die Aktivität *Cloud Return Response* zum Workflow hinzufügen. Eine Variable muss in der Aktivität *Cloud Return Response* für die Antwort erwähnt werden. Siehe Workflow .

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Ressourcenblöcke**.
2. Öffnen Sie einen Ressourcenblock, der sich im Entwurfsstatus befindet, und navigieren Sie zu **Vorgänge Schritte**.
3. Klicken Sie auf **Schritt hinzufügen**.
   Das Dialogfeld „Vorgangsschritte hinzufügen“ wird angezeigt.
4. Fügen Sie einen Workflow-Vorgangsschritt hinzu.
   Weitere Informationen finden Sie unter Vorgangsschritte einem Ressourcenblock hinzufügen.
   Der Workflow-Vorgangsschritt wird dem Ressourcenblock angefügt und auf der Seite angezeigt. Alle dem Workflow zugeordneten Eingabeparameter werden auf der Registerkarte **Eingabe** angezeigt.
5. Klicken Sie auf **Katalog generieren**.
   Der Workflow wird im Cloudbenutzerportal als Vorgang angezeigt. Wählen Sie den Workflow in der Auswahl **Vorgang auswählen** aus, um den Vorgang auszuführen. Der Status des Vorgangs wird auf der Unterregisterkarte „Vorgang nachverfolgen“ angezeigt.
6. Klicken Sie auf die Registerkarte **Antwortprozessor**, und klicken Sie dann auf das Pluszeichen.
   Das Dialogfeld „Antwortprozessor hinzufügen“ wird angezeigt.

7. Wählen Sie in der Liste **Skriptname** ein Skript für den Antwortprozessor aus.
   Damit ein Skript in der Liste **Skriptname** angezeigt wird, muss es bereits auf der Registerkarte **Ressourcenskript** erstellt worden sein.
8. Klicken Sie auf **Absenden**.
   Das Skript wird auf der Registerkarte **Antwortprozessor** angezeigt. Sie können das Skript öffnen und Änderungen daran vornehmen.

Beispiel für einen Antwortprozessor für einen virtuellen Server

Das Skript *Create_Virtual_Server_Response_Processor*, das standardmäßig in Cloud Provisioning and Governance verfügbar ist, ist der Antwortprozessor, der die Erstellung von AWS-VM-CIs verarbeitet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Virtuellen Server erstellen

Das Ressourcenprozessorskript „Create_Virtual_Server_Response_Processor“ ist standardmäßig im Ressourcenblock „Virtueller Server“ verfügbar. Seine Aufgabe besteht darin, einen Datensatz für einen virtuellen Server in der Tabelle „VM-Instanz“ [cmdb_ci_vm_instance] zu erstellen, wenn ein neuer virtueller Server bereitgestellt wird.

Alle Antwortprozessoren haben diese erste Zeile mit diesen allgemeinen Parametern:

```
function processResponse(response, cloudServiceAccountId, ldc,
 correlationId,step, requestorContext) {
```

Dadurch werden die Antwort des Cloud-Providers und die wichtigen Informationen, wie z. B. die Konto-ID, abgerufen, die erforderlich sind, damit das System das neue CI erstellen kann. Alle diese Parameter sind für alle Antwortprozessoren erforderlich.

Zeile 10 wandelt die Antwort in JSON um, damit sie vom System verarbeitet werden kann. Die Informationen werden in der Variablen „vmResponse“ gespeichert:

```

var vmResponse = global.JSON.parse(response);
```

Immer wenn Sie einen Antwortprozessor erstellen oder bearbeiten, müssen Sie wissen, welche Eingaben für den CI-Typ erforderlich sind. Zeile 11 verarbeitet eine der erforderlichen Eingaben, die Hardware-ID, die für den CMDB-Datensatz erforderlich ist:

```

var hardwareId = vmResponse.hardwareId;
```

Zeile 39 zeigt die Informationen an, die das System benötigt, um den neuen virtuellen Server und zugehörige CIs zu identifizieren, damit die Informationen in der CMDB abgelegt werden können. In diesem Fall identifiziert die Objekt-ID des Servicekontos das dem virtuellen Server zugeordnete Konto, die Objekt-ID des Rechenzentrums das Rechenzentrum, in dem der virtuelle Server ausgeführt wird, und die Objekt-ID der VM-Instanz den virtuellen Server selbst. Dieser Block mit Identifizierungscode verhindert die Erstellung doppelter CIs.

```

var vmInfo = {
    "cmdb_ci_vm_instance": {
      "validator": "virtual_machine_create_update_validator",
      "validator_overrides": {},
      "identification": {
        "cmdb_ci_cloud_service_account": {
          "criterion": {
            "object_id": cloudServiceAccountId
          }
        },
        "cmdb_ci_aws_datacenter": {
          "criterion": {
            "object_id": ldc
          }
        },
        "cmdb_ci_vm_instance": {
          "criterion": {
            "object_id": vmResponse.nodeId
          }
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
        }
      },
```

Attribute werden in die Felder in der Tabelle „cmdb_ci_vm_instance“ eingetragen. Diese Attribute werden in Zeile 61 definiert:

```
"attributes": {
  "name": vmResponse.nodeName,
  "object_id": vmResponse.nodeId,
  "state": status_map[vmResponse.state],
  "dns_suffix": vmResponse.dnsSuffix,
  "cpus": vmCPUs,
  "memory": vmMemory,
  "disks": vmResponse.volumes.length,
  "disks_size": "",
  "nics": vmResponse.networkInterfaces.length,
  "terminated_on": "",
  "termination_protection": "",
  "ip_address": vmPubIPAddr,
  "assigned_to": reqContext.userId,
  "assignment_group": reqContext.groupId
},
```

Auch Verweise auf andere CIs können im Antwortprozessor enthalten sein. In diesem Fall wird die BS-Vorlage, auf der der virtuelle Server basiert, identifiziert, indem zuerst die Objekt-ID des Servicekontos, dann die des Rechenzentrums und schließlich die der tatsächlichen BS-Vorlage identifiziert wird.

```
"references": {
  "cmdb_ci_os_template": {
    "identification": {
      "cmdb_ci_cloud_service_account": {
        "criterion": {
          "object_id": cloudServiceAccountId
        }
      },
      "cmdb_ci_aws_datacenter": {
        "criterion": {
          "object_id": ldc
        }
      },
      "cmdb_ci_os_template": {
        "criterion": {
          "object_id": imageIdTrim
        }
      }
    },
```

Der folgende Codeblock fügt die Objekt-ID des BS-Images der Attributliste hinzu, damit diese Informationen in den CMDB-Datensatz des virtuellen Servers eingefügt werden können.

```
"attributes": {
  "object_id": imageIdTrim
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Codeblock führt eine zusätzliche Identifizierung für die Computing-Vorlage (den Hardwaretyp) durch und fügt das Ergebnis dann den Attributen hinzu:

```
"cmdb_ci_compute_template": {
  "identification": {
    "cmdb_ci_cloud_service_account": {
      "criterion": {
        "object_id": cloudServiceAccountId
      }
    },
    "cmdb_ci_aws_datacenter": {
      "criterion": {
        "object_id": ldc
      }
    },
    "cmdb_ci_compute_template": {
      "criterion": {
        "object_id": vmResponse.hardwareId
      }
    }
  },
  "attributes": {
    "object_id": vmResponse.hardwareId,
    "name": vmResponse.hardwareId
  }
}
```

Zusätzliche Codeabschnitte stellen die Beziehung zu Netzwerkschnittstellen her und identifizieren jeden an den virtuellen Server angehängten Speicher.

Dieser obligatorische Codeblock verschiebt die Daten in die CMDB und gibt die JSON-Zeichenfolge zurück:

```
cloudModelString.push(vmInfo);
return global.JSON.stringify(cloudModelString);
```

Ressourcenblock die Terraform Orchestration-Schnittstelle hinzufügen

Nachdem Sie die Terraform-App im Store für Cloud Provisioning and Governance aktiviert haben, werden cloudbasierte Vorgänge für Cloud-Provider unterstützt, die die Terraform Open Source-Edition verwenden. Fügen Sie die Terraform Orchestration-Schnittstelle zum Ressourcenblock hinzu, um cloudbasierte Vorgänge über Terraform-Vorlagen auszuführen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cmp_root_admin, sn_cmp.cloud_service_designer

Prozedur

1. Navigieren Sie im Cloud-Adminportal zu **Entwurf** > **Ressourcenblock**.
2. Klicken Sie auf den Ressourcenblock, z. B. **Azure-Rechenzentrum**.
3. Ändern Sie den Status des Ressourcenblocks von **Veröffentlicht** in **Entwurf**, um ihn bearbeitbar zu machen.
4. Navigieren zu **Allgemeine Informationen** > **Gastschnittstelle**und klicken Sie dann auf **Neu**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Suchen Sie die **Terraform Orchestration-Schnittstelle** in der Liste „Gastschnittstelle“, wählen Sie sie aus, und klicken Sie auf **Absenden**.
6. Klicken Sie auf die Registerkarte **Vorgänge**.
7. Navigieren Sie auf der Registerkarte **Eingabeparameter** zu **Schnittstelle** und wählen Sie **Terraform Orchestration Interface** (Terraform Orchestration-Schnittstelle) aus.
8. Konfigurieren Sie auf der Registerkarte **Eingabeparameter** die CAPI-Vorgangseingaben.

   Öffnen Sie bei der CAPI-Schnittstelle (in diesem Fall die Schnittstelle **Terraform Orchestration-Schnittstelle**) die Methode *`CreateStack`*. Die Eingaben von CAPI werden auf der Registerkarte „Eingabe“ angezeigt, auf der Sie Parameter erstellen.

   Die Registerkarte **Eingabeparameter** wird durch Benutzer ausgefüllt werden. Sie können diese Eingabeparameter den Parametern auf der Registerkarte **Eingabe** zuordnen. Kopieren Sie dazu den **Zuordnungswert** von der **Registerkarte Eingabeparameter** in das Feld **Wert** in **Schritte** > **Eingabe** Registerkarte

   Wenn dieser Schritt ein Skript aufruft und dieses Skript Argumente zur Rückgabe von Werten erfordert, können Sie für jedes Argument einen neuen Eingabeparameter hinzufügen. Verwenden Sie diese Syntax im Feld **Wert**: `${parameter.arg1}`.
9. Klicken Sie unter **Vorgänge** auf die Unterregisterkarte **Schritte**.
10. Klicken Sie auf **Schritt hinzufügen**.
11. Füllen Sie die Formularfelder aus.

Feld	Beschreibung
Vorgangstyp	Wählen Sie die Art des Vorgangs aus. **Cloud API aufrufen**: Wählen Sie diese Option aus, um einen Provider, eine Schnittstelle und eine Methode aus der CAPI auszuwählen.
API-Anbieter	Wählen Sie die API aus, die die erforderlichen Schnittstellen bereitstellt. Die Provider sind Teil der Cloud API (CAPI). Beispielsweise stellt CAPI den Provider **Terraform OpenSource** bereit, der die **Configuration Orchestration-Schnittstelle** bereitstellt. Dieser Wert wird angezeigt, wenn Sie den Vorgangstyp „Cloud API aufrufen“ auswählen.
API-Schnittstelle	Wählen Sie die Schnittstelle mit den Methoden aus, die Sie verwenden möchten. In diesem Beispiel stellt die **Configuration Orchestration-Schnittstelle** mehrere Schnittstellen oder Methoden bereit, die das System während der Bereitstellung verwendet.
API-Methode	Wählen Sie die Methode aus, mit der der Vorgang ausgeführt werden soll. In diesem Beispiel ist **ExecuteCommand** erforderlich, um Terraform-Vorlagen bereitzustellen.
CAPI-Version	Geben Sie eine Version für die CAPI API ein.
Bedingung	Geben Sie eine optionale Bedingung ein, die erfüllt sein muss, bevor das System diesen Schritt verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Klicken Sie auf **Absenden**.

    Die Registerkarten **Eingabe** und **Antwortprozessor** werden für den Schritt angezeigt.

13. Konfigurieren Sie auf der Registerkarte **Eingabe** die CAPI-Vorgangseingaben.

    Öffnen Sie bei der CAPI-Schnittstelle (in diesem Fall die **Configuration Orchestration-Schnittstelle**) die Methode *ExecuteCommand*. Die Eingaben von CAPI werden auf der Registerkarte „Eingabe“ angezeigt, auf der Sie Parameter erstellen.

    Denken Sie daran, dass die Parameter auf der Registerkarte **Eingabeparameter** durch Benutzer ausgefüllt werden. Sie können diese Eingabeparameter den Parametern auf der Registerkarte **Eingabe** zuordnen. Kopieren Sie den **Zuordnungswert** von der **Registerkarte Eingabeparameter** in das Feld **Wert** im **Schritte** > **Eingabe** Registerkarte

    Wenn dieser Schritt ein Skript aufruft und dieses Skript Argumente zur Rückgabe von Werten erfordert, können Sie für jedes Argument einen neuen Eingabeparameter hinzufügen. Verwenden Sie diese Syntax im Feld **Wert**: `${parameter.arg1}`.

    Hinweis: Ordnen Sie die Werte für die folgenden Parameter wie in der folgenden Tabelle erläutert zu:

Parameter	Wert
AdditionalParameters	Geben Sie das folgende Skript ein: `{"ServerType":"$(Script:sn_cmp_terraform.TerraformCommandUtils.getConfigProviderServerTypeByName[arg=${parameter.WorkloadConfigProvider}])"}`
ConfigMgmtProviderInfo	`$(capiResolver.NodeCredentialResolver#nodeCredentialId=$(ci.sn_cmp_wl_cfg_mgmt_provider[name=${parameter.WorkloadConfigProvider}].credential))`
Knotenadresse	`$(ci.cmdb_ci_workload_config_provider[name=${parameter.WorkloadConfigProvider}].url)`
Skript Für CreateStapelvorgang	`${CloudScript.scripts.TerraformDeploy}`
Skript Für DeleteStapelvorgang	`${CloudScript.scripts.DestroyTerraform}`

14. Auf der Registerkarte **Antwortprozessor** konfigurieren Sie die Antwortprozessoren, indem Sie Ressourcenskripts anhängen.
    Sie haben dem Ressourcenblock beim Erstellen des Ressourcenblocks Ressourcenskripts hinzugefügt.

15. Wählen Sie in der Liste „Vorgang“ den Vorgang **CreateStack** oder **DeleteStack** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

16. Klicken Sie bei **Antwortprozessor hinzufügen** auf das Hinzufügen-Symbol +.
17. Klicken Sie auf die Unterregisterkarte **Ressourcenskript**, und klicken Sie dann auf **Neu**.
18. Füllen Sie das Formular aus.

Neuer Datensatz

Feld	Beschreibung
Name	Geben Sie einen Namen (z. B. **Create_AzureTF_Stack_Response_Processor**) für das Ressourcenskript ein.
Typ	Wählen Sie einen Typ (**Antwortprozessor**) für das Skript aus.
Skript Ressourcenskript zum Erstellen	Geben Sie das folgende Skript ein: `function processResponse (response, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId) { var responseObject = global.JSON.parse(response); var tfState = global.JSON.parse(responseObject.terraform.state); var processor = new sn_cmp_terraform.TerraformResponseProcessor(); var processedResponses = processor.processResponse(tfState, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId); return global.JSON.stringify(processedResponses); }`
Skript Ressourcenskript zum Löschen	Geben Sie das folgende Skript ein: `function processResponse (response, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId) { var responseObject = global.JSON.parse(response); var tfState = global.JSON.parse(responseObject.terraform.state); var processor = new sn_cmp_terraform.TerraformResponseProcessor();`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	`var processedResponses = processor.processResponse(tfState, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId); return global.JSON.stringify(processedResponses); }`

19. Wählen Sie in der Liste **Skriptname** das Skript aus, das dem ausgewählten Vorgang entspricht, und klicken Sie auf **Absenden**.
20. Ändern Sie den Status des Ressourcenblocks von **Entwurf** in **Veröffentlicht**.
    Der Ressourcenblock „Rechenzentrum“ wird vom Status „Entwurf“ in den Status „Veröffentlicht“ verschoben, und Sie können keine weiteren Änderungen am Ressourcenblock vornehmen. Sie können einen Ressourcenblock nur ändern, nachdem Sie den Status auf **Entwurf** festgelegt haben.

Ressourcenblock für Microsoft Azure Cloud erstellen

Ressourcenblöcke sind die Bausteine von Cloud-Katalogelementen. Erstellen Sie einen Ressourcenblock für den Microsoft Azure Cloud Platform-Provider basierend auf einem CI-Typ aus der CMDB.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cmp_root_admin

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Ressourcenblöcke**.
2. Klicken Sie auf **Neu**, um das Dialogfeld „Ressourcenblock erstellen“ zu öffnen, und füllen Sie dann das Formular aus.

   Eine detaillierte Beschreibung der einzelnen Felder finden Sie unter Benutzerdefinierten Ressourcenblock erstellen.

Feld	Beschreibung
Name	Geben Sie einen Namen (**Azure-Rechenzentrum**) für den Ressourcenblock ein.
Beschreibung	Geben Sie eine gültige Beschreibung ein.
Ebene	Wählen Sie den Typ des Ressourcenblocks (**Logisches Rechenzentrum**) aus.
CI-Typ	Wählen Sie den CI-Typ (**Azure-Rechenzentrum**) aus, der den Ressourcenblock darstellt.
Gastschnittstelle	Wählen Sie eine Standardgastschnittstelle (**Computing-Schnittstelle**) aus, die beim Hinzufügen eines Ressourcenblocks zu einer Vorlage verwendet werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Absenden**.
   Die Ressourcenblockinformationen werden angezeigt.
4. Klicken Sie auf die Unterregisterkarte **Ressourcenskript**, und klicken Sie dann auf **Neu**.

Feld	Beschreibung
Name	Geben Sie einen Namen (z. B. **Create_AzureTF_Stack_Response_Processor**) für das Ressourcenskript ein.
Typ	Wählen Sie einen Typ (**Antwortprozessor**) für das Skript aus.
Skript Ressourcenskript zum Erstellen	Geben Sie das folgende Skript ein: `function processResponse (response, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId) { var responseObject = global.JSON.parse(response); var tfState = global.JSON.parse(responseObject.terraform.state); var processor = new sn_cmp_terraform.TerraformResponseProcessor(); var processedResponses = processor.processResponse(tfState, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId); return global.JSON.stringify(processedResponses); }`
Skript Ressourcenskript zum Löschen	Geben Sie das folgende Skript ein: `function processResponse (response, cloudServiceAccountId, ldc, correlationId, step, requestorContext, stackId) { var responseObject = global.JSON.parse(response); var tfState = global.JSON.parse(responseObject.terraform.state); var processor = new sn_cmp_terraform.TerraformResponseProcessor(); var processedResponses = processor.processResponse(tfState, cloudServiceAccountId, ldc,`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung

	correlationId, step,
	requestorContext, stackId);
	return
	global.JSON.stringify(processedResponses);
	}

5. Klicken Sie auf **Absenden**.
6. Klicken Sie auf die Unterregisterkarte **Vorgänge**, und klicken Sie dann auf **Schritte**.
7. Wählen Sie **CreateStack** in der Liste **Vorgänge** aus.
8. Klicken Sie auf das Pluszeichen **Schritt hinzufügen**, um das Dialogfeld „Vorgangsschritte hinzufügen“ zu öffnen, und füllen Sie dann das Formular aus.

Feld	Beschreibung
Vorgangstyp	Wählen Sie die Art des Vorgangs aus. **Cloud API aufrufen**: Wählen Sie diese Option aus, um einen Provider, eine Schnittstelle und eine Methode aus der CAPI auszuwählen.
API-Anbieter [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die API aus, die die erforderlichen Schnittstellen bereitstellt. Die Provider sind Teil der Cloud API (CAPI). Beispielsweise stellt CAPI den Provider **Terraform OpenSource** bereit, der die **Configuration Orchestration-Schnittstelle** bereitstellt. Dieser Wert wird angezeigt, wenn Sie den Vorgangstyp „Cloud API aufrufen“ auswählen.
API-Schnittstelle [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die Schnittstelle mit den Methoden aus, die Sie verwenden möchten. In diesem Beispiel stellt die **Configuration Orchestration-Schnittstelle** mehrere Schnittstellen oder Methoden bereit, die das System während der Bereitstellung verwendet.
API-Methode [Vorgangstyp = Cloud API aufrufen]	Wählen Sie die Methode aus, mit der der Vorgang ausgeführt werden soll. In diesem Beispiel ist **ExecuteCommand** erforderlich, um Terraform-Vorlagen bereitzustellen.
CAPI-Version [Vorgangstyp = Cloud API aufrufen]	Geben Sie eine Version für die CAPI API ein.
Bedingung	Geben Sie eine optionale Bedingung ein, die erfüllt sein muss, bevor das System diesen Schritt verwendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

9. Klicken Sie auf **Absenden**.
10. Klicken Sie auf **Antwortprozessor**, und klicken Sie dann auf das Pluszeichen. Das Dialogfeld „Antwortprozessor hinzufügen“ wird angezeigt.
11. Wählen Sie **Create_AzureTF_Stack_Response_Processor** aus der Liste **Skriptname** aus, und klicken Sie auf **Absenden**.
12. Ändern Sie den Status des Ressourcenblocks von **Entwurf** in **Veröffentlicht**. Der Ressourcenblock „Azure-Rechenzentrum“ wird vom Status „Entwurf“ in den Status „Veröffentlicht“ verschoben, und Sie können keine weiteren Änderungen am Ressourcenblock vornehmen. Änderungen an einem Ressourcenblock können nur vorgenommen werden, wenn der Status auf **Entwurf** festgelegt ist.

Cloud-Skripts und Cloud-Skriptvorlagen

In der Cloud Provisioning and Governance-Anwendung ist die Skriptausführung in Cloud-Skripts und Cloud-Skriptvorlagen unterteilt. Verwenden Sie Skripts in Blaupausen, Ressourcenblöcken, BS-Profilen, und verwenden Sie Richtlinienskripts, um Anforderungsformularattribute festzulegen. Richtlinienskripts können Benutzerdaten nicht überschreiben.

Cloud-Skripts

Cloud-Skripts sind einfache Java-Skripts, die Plattformfunktionen verwenden. Beispiel für ein Cloud-Skript:

```
function evaluateTemplate() {
 // Template Resolver is a helper function which we will use to fetch a
 template and replace its parameters,
 // var templateResolver=new TemplateResolver(); this comes inbuild
 // templateAttributes below will passed from the user.
 var listDir=templateResolver.getTemplate('Install',templateAttributes);
 return listDir;
}
```

Jedes Cloud-Skript enthält bestimmte Parameter. Parameter sind die Attribute, auf die Sie zugreifen möchten. Ein Parameter enthält einen Namen, einen Standardwert und einen Überschreibungswert. Der Standardwert kann ein Zeichenfolgenliteral, ein Ressourcenblockparameter oder ein komplexer Skriptausdruck sein, der in Ressourcenblöcken verwendet wird.

Ein Cloud-Skript hat standardmäßig Zugriff auf das Objekt *templateResolver*. Das Objekt *templateResolver* verfügt standardmäßig über eine getTemplate-Methode, deren erster Parameter der Name der Cloud-Skriptvorlage ist. *templateAttributes* sind die Cloud-Skriptparameter, die als Teil eines Cloud-Skripts erstellt werden. Bei Bedarf können in *templateAttributes* Anpassungen vorgenommen werden. Sehen Sie sich beispielsweise das folgende Codefragment an, wenn der Wert des Parameters *DevName* von „John“ in „Emily“ geändert werden muss.

```
function evaluateTemplate() {
 // Template Resolver is a helper function which we will use to fetch a
 template and replace its parameters,
 // var templateResolver=new TemplateResolver(); this comes inbuild
 // templateAttributes below will passed from the user.
 templateAttributes['DevName'] = 'Emily';
 var customNodeName;
 var now_GR = new GlideRecord('some_custom_table_to_query');
 gr.addQuery('some_parameter','some_value');
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 gr.query();
 if(gr.next())
   customNodeName=gr.getValue('some_custom_node_name');

 templateAttributes['NodeName'] = customNodeName;
 var listDir=templateResolver.getTemplate('Install',templateAttributes);
 return listDir;
}
evaluateTemplate();
```

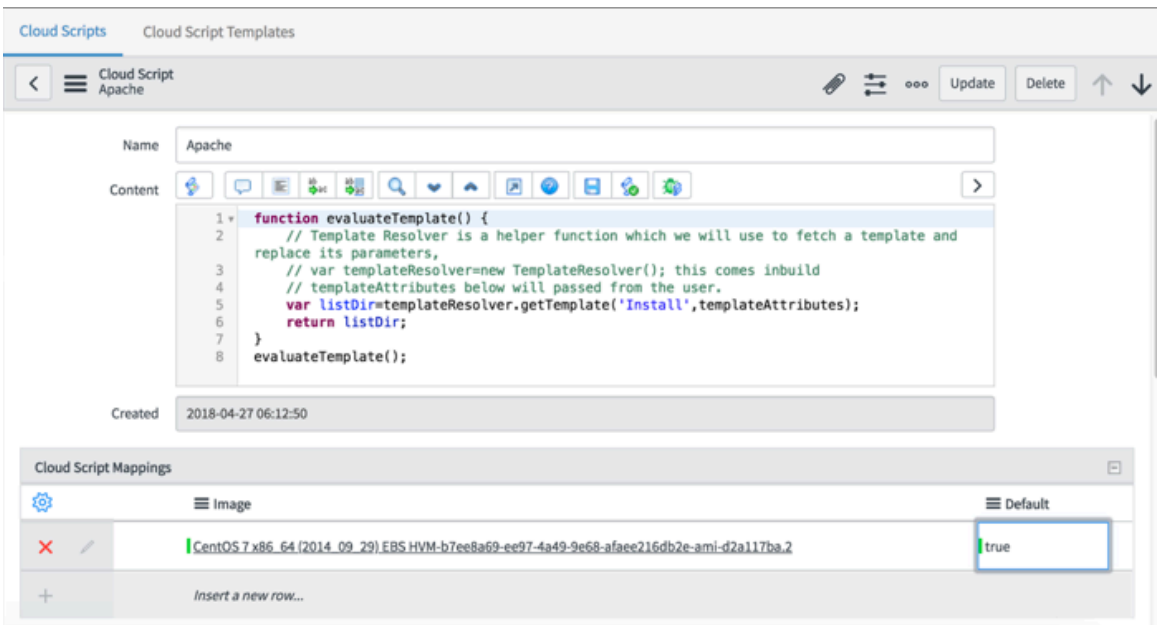
Cloud-Skriptvorlagen

Cloud-Skriptvorlagen sind tatsächliche ausführbare Dateien, die zur Ausführung an einen virtuellen Computer übergeben werden. Cloud-Vorlagen können je nach Ausführungskontext einen beliebigen Typ (Shell/PowerShell/CloudInit) haben. Erstellen Sie zuerst eine Cloud-Vorlage, und ordnen Sie sie dann einem Cloud-Skript zu.

Cloud-Skripts als CloudInit

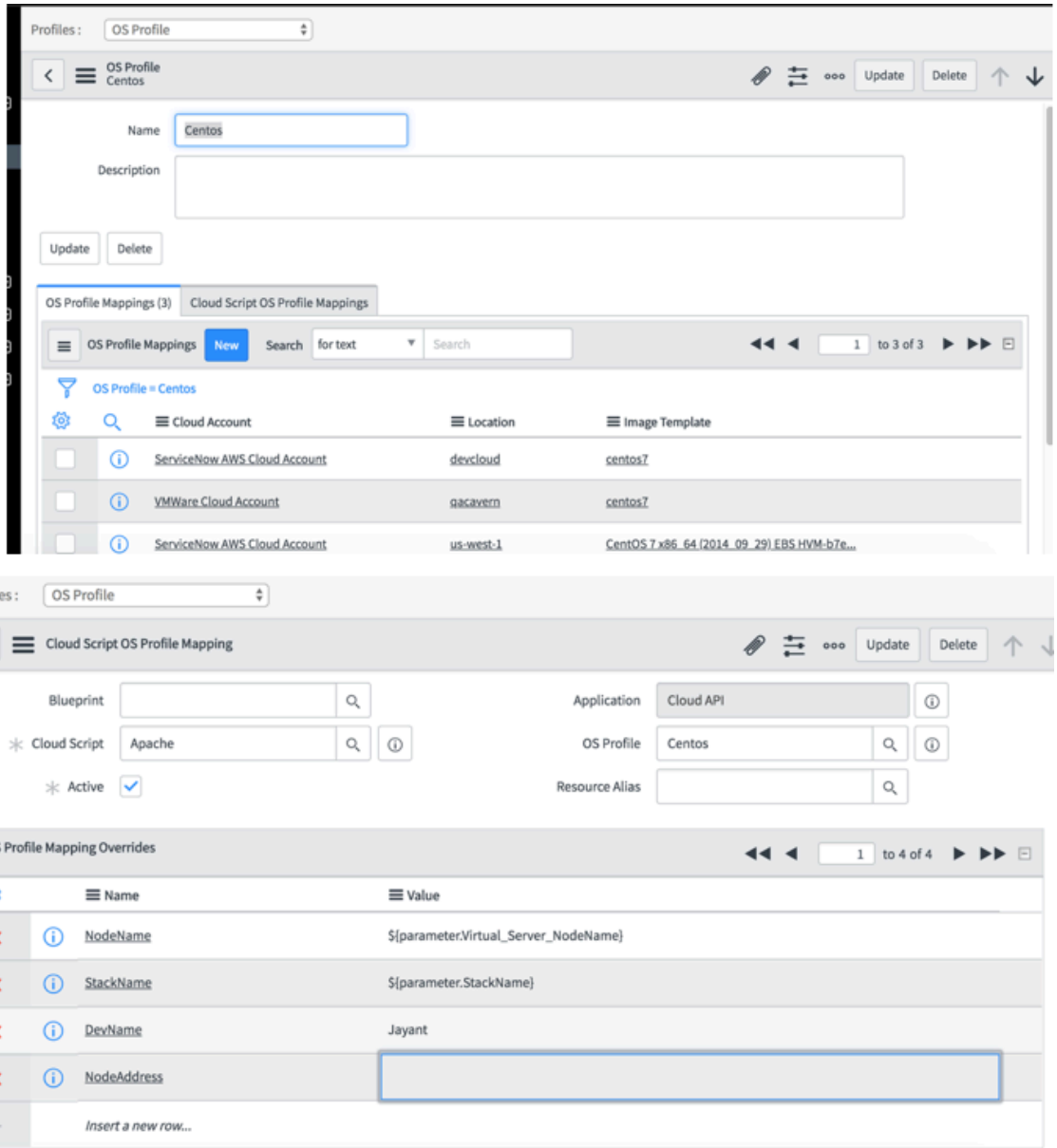
Cloud-Provider bieten eine Möglichkeit, Skripts beim Start von virtuellen Computern auszuführen. In der Cloud-Management-Anwendung können Sie ein cloudinit-Skript auf verschiedenen Ebenen angeben:

- Image-Ebene: Zum Zeitpunkt der Erstellung eines Cloud-Skripts können Sie ein Image angeben, für das dieses Skript ausgeführt werden soll. Sobald ein BS-Profil ausgewählt wird, das dieses bestimmte Image enthält, wird das standardmäßige Cloud-Skript für dieses Image ausgeführt. Im folgenden Beispiel ist ein Apache-Cloud-Skript einem bestimmten Image zugeordnet.



- BS-Profilebene: Sie können ein cloudinit-Skript für einen bestimmten Cloud-Provider und für ein bestimmtes AMI/Image ausführen. Sie können auch generisch einem BS-Profil ein cloudinit-Skript zuordnen, unabhängig vom zugrunde liegenden Image. Im folgenden Beispiel sind dem BS-Profil mehrere Images zugeordnet. Sie können auf der Registerkarte „Cloud-Skript – BS-Profilzuordnungen“ dem BS-Profil ein beliebiges Cloud-Skript zuordnen. Die Zuordnung eines Cloudskripts zu einem BS-Profil hat Vorrang vor der Cloud-Skriptzuordnung auf Image-Ebene.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



In diesem Beispiel wird das Apache-Cloud-Skript dem Centos-BS-Profil zugeordnet. Bei Bedarf können Sie die Skriptparameter im Abschnitt „Überschreibungen der BS-Profilzuordnung“ überschreiben.

- Ressourcenblöcke: Bei der Zuordnung eines Cloud-Skripts zu einem BS-Profil können Sie wählen, ob das Cloud-Skript für einen bestimmten in einer Blaupause verwendeten Ressourcenblock und für einen bestimmten Ressourcenalias ausgeführt werden soll. Weitere Informationen finden Sie unter BS-Profil erstellen.

Cloud-Skripts als Postinit

Sie können Cloud-Skripts als Postinit-Skripts in einem Ressourcenblock verwenden. Sobald Sie einen Ressourcenblock mit einem virtuellen Computer erstellt haben, der bereitgestellt werden soll, können Sie einen ExecuteScript-Vorgang hinzufügen. Der ExecuteScript-Vorgang verwendet einen Skriptparameter (einen Pool von Cloud-Skripts), und Sie können ein beliebiges auszuführendes Skript auswählen. Verwenden Sie das Attribut *`ScriptParameters`* im ExecuteScript-Vorgang, um beliebige Skriptparameter zu überschreiben. Sie können eine JSON-Zuordnung der Skriptparameter und ihrer Überschreibungswerte bereitstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Alle Ausdrücke, die von Cloud-Management unterstützt werden, sind im Attribut `ScriptParamters` anwendbar.

Skriptvorlagen und Skript für die Cloud-Initialisierung erstellen

Erstellen Sie Vorlagen und Skript für die Cloud-Initialisierung, um sie zur VM-Bereitstellung zu verwenden.

Vorbereitungen
Erforderliche Rolle: cloud_admin

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Cloud-Skripts** > **Cloud-Skriptvorlagen**.
2. Klicken Sie auf **Neu**, geben Sie den Namen und Inhalt des Skripts ein, und klicken Sie dann auf **Absenden**.

   Erstellen Sie so viele Skriptvorlagen wie nötig.
3. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Cloud-Skripts**.
4. Klicken Sie auf **Neu**.
5. Geben Sie einen beschreibenden Namen ein, und erstellen Sie ein Skript, das den Vorlagennamen in der folgenden Codezeile verwendet (`scriptName` ist der Name der Vorlage):

   ```
   templateResolver.getTemplate(scriptName);
   ```

   Hinweis: Weitere Informationen finden Sie unter Cloud-Skripts und Cloud-Skriptvorlagen.
6. Klicken Sie auf **Absenden**.

Nächste Maßnahme
Um ein Skript zum Zeitpunkt der Bereitstellung einer virtuellen Ressource auszuführen, ordnen Sie das Skript einem BS-Profil zu. Zum Ausführen eines Post-Bereitstellungsskripts erstellen Sie eine Blaupause, und geben Sie das Skript im Vorgang „Skript ausführen“ an. Ein Beispiel finden Sie unter Beispiel: Cloud-Skript für nach der Bereitstellung.

BS-Profil ein Skript zuordnen

Um geskriptete Aktionen während der VM-Bereitstellung auszuführen, können Sie einem BS-Profil ein Skript zuordnen. Das Skript wird auf VMs ausgeführt, die basierend auf der Bildvorlage im BS-Profil erstellt werden.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_admin

Sie müssen über ein Cloud-Konto mit Rechenzentren verfügen. Sie müssen Discovery für die Servicekonten ausführen, um die Rechenzentren auszufüllen.

Warum und wann dieser Vorgang ausgeführt wird
In diesem Verfahren geben Sie ein vorhandenes Skript an. Siehe Skriptvorlagen und Skript für die Cloud-Initialisierung erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Profilzuordnungen, in denen mehr Details angegeben sind, werden zuerst ausgeführt. Beispielsweise hat eine Zuordnung, in der eine Blaupause, ein Betriebssystemprofil und ein Ressourcenalias angegeben sind, Vorrang vor einer Zuordnung, in der nur ein Betriebssystemprofil angegeben ist.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Verwalten** > **Ressourcenprofile**.
2. Wählen Sie in der Liste **Profile** die Option **BS-Profil** aus, und öffnen Sie dann das Profil.
3. Klicken Sie in der zugehörigen Liste „Cloud-Skript – BS-Profilzuordnungen“ auf **Neu**, und füllen Sie das Formular aus.

Feld	Beschreibung
Plan [Optional]	Wählen Sie eine Blaupause, um das Skript auf einen bestimmten, in der Blaupause verwendeten Ressourcenblock zu beschränken.
Cloud-Skript	Wählen Sie ein Cloud-Skript aus, dem das Betriebssystemprofil zugeordnet werden soll.
Aktiv	Aktivieren Sie das Kontrollkästchen, wenn das Cloud-Skript nach der Bereitstellung des virtuellen Computers ausgeführt werden soll.
Applikation	Cloud Provisioning and Governance ist automatisch ausgewählt.
BS-Profil	Wenn Sie eine Blaupause angeben, wird das Cloud-Skript ausgeführt, wenn die Blaupause bereitgestellt wird.
Ressourcen-Alias [Optional]	Wenn Sie einen Ressourcenalias für die Blaupause angeben, wird das Cloud-Skript ausgeführt, wenn die Blaupause mit dem angegebenen Ressourcenalias bereitgestellt wird.

4. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
   Das **Namensattribut** `[scriptName]` wird in der Liste „Überschreibungen der BS-Profilzuordnung“ aufgeführt.
5. Geben Sie in der Liste „Überschreibungen der BS-Profilzuordnung“ einen Attributnamen und einen Wert ein, die bei der Bereitstellung der Ressource verwendet werden.

Zugehörige Informationen

BS-Profil erstellen

Beispiel: Cloud-Skript für nach der Bereitstellung

Dieses Beispiel zeigt ein Cloud-Skript, das ausgeführt wird, nachdem ein Benutzer einen virtuellen Computer bereitgestellt hat.

Vorbereitungen

- Erforderliche Rolle: cloud_admin
- BS-Ressourcenprofil, das einer Bildvorlage zugeordnet ist. Der Benutzer stellt eine Ressource mithilfe des Profils bereit. Sie müssen dem Bild Anmeldeinformationen für die Standardauthentifizierung hinzufügen.
- Computing-Ressourcenprofil, das einem Hardwaretyp zugeordnet ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

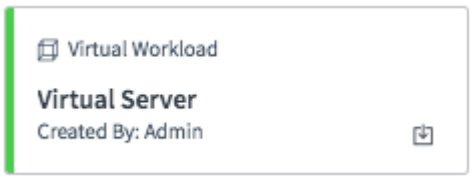
Warum und wann dieser Vorgang ausgeführt wird

In diesem Beispiel erstellen Sie ein Cloud-Init-Skript, passen einen Ressourcenblock an und stellen eine VM über das Cloudbenutzerportal bereit.

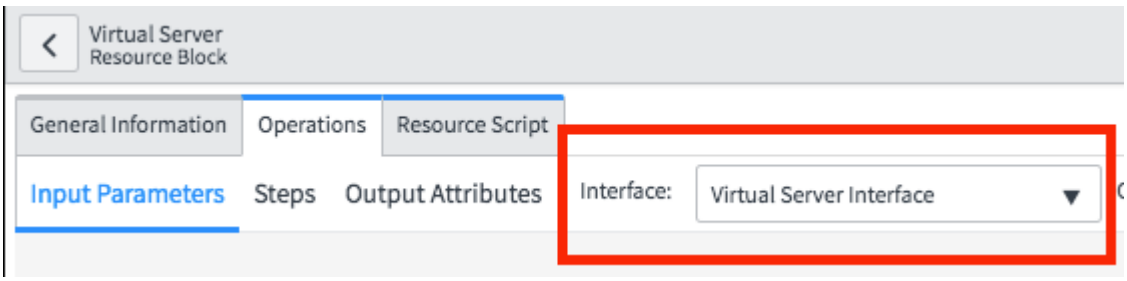
Prozedur

1. Erstellen Sie eine Cloud-Skriptvorlage und ein Cloud-Skript, das auf die Vorlage verweist.
2. Öffnen Sie den Ressourcenblock des virtuellen Servers, und führen Sie die folgenden Schritte aus:

   a. Legen Sie den Umschalter **Entwurf/Veröffentlicht** auf **Entwurf** fest.

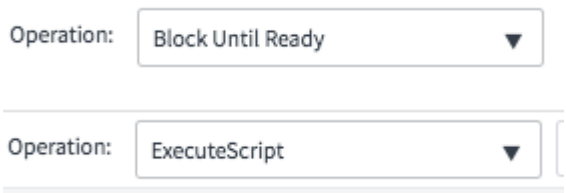


   b. Wählen Sie auf der Registerkarte **Vorgänge** die Option **Virtuelle Serverschnittstelle** aus der Liste **Schnittstelle** aus.



   c. Überprüfen Sie im Feld **Vorgang**, ob diese Vorgänge vorhanden sind:

   - **Blockieren bis bereit**
   - **Skript ausführen**: Dieser Vorgang weist die Blaupause an, ein Skript auszuführen.



   d. Klicken Sie auf die Registerkarte **Eingabeparameter**, um sich die Eingaben für jeden Vorgang anzusehen.

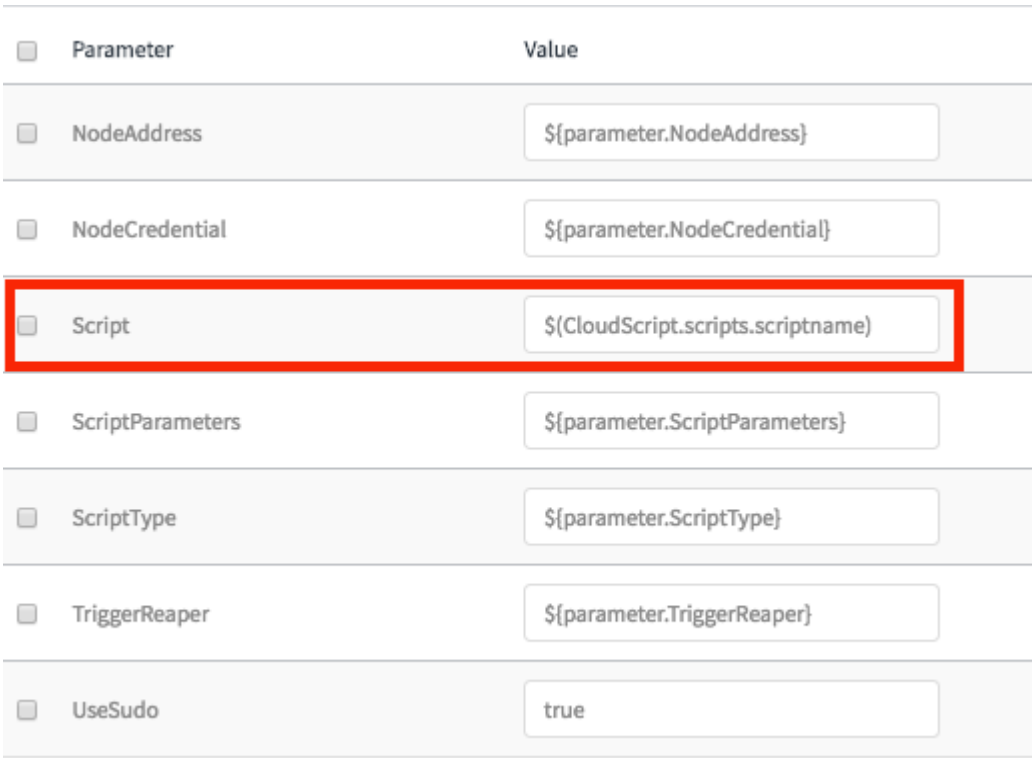
   e. Fügen Sie auf der Registerkarte **Schritte** nach Bedarf Schritte hinzu.

   f. Deaktivieren Sie beim Parameter **Skript** in jedem Schritt das Kontrollkästchen **Skript** und ändern Sie den Ausdruck in der Spalte **Zuordnung** zu dem folgenden Text:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

`$(CloudScript.scripts.scriptname)`, wobei `scriptname` der Name des Skripts ist, nicht die Skriptvorlage, die Sie zuvor erstellt haben.



3. Veröffentlichen Sie den Ressourcenblock des virtuellen Servers, und verwenden Sie ihn in einer Blaupause, die ihrerseits in einem Katalogelement veröffentlicht wird.
4. Starten Sie einen neuen Stapel, um eine VM bereitzustellen, und geben Sie das BS-Profil und das Computing-Profil an, die Sie als Voraussetzung erstellt haben.

Ergebnisse
Auf der Seite „Stapelstatus“ sehen Sie, wie die Vorgänge *`CreateNode`*, *`BlockUntilReady`* und *`ExecuteShellScript`* durchlaufen werden. Der letzte Vorgang hat das von Ihnen erstellte Skript ausgelöst.

Antwortzuordnungen

Die Antwortzuordnung ist der Mechanismus, den CMP verwendet, um alle Ereignisse und Vorgänge in CMDB zurückzuschreiben.

Antwortzuordnungsmechanismus

CMP (Cloud Management Platform) wurde für die aktive Interaktion mit der Cloud-Umgebung in verschiedenen kritischen Phasen entwickelt, einschließlich Discovery, Bereitstellung, Tag-2-Vorgängen und Lebenszyklus-Ereignisse. Während dieser Prozesse ist CMP erforderlich, um Daten effektiv aufzuzeichnen und in der Configuration Management Database (CMDB) zu speichern. Diese Daten können verschiedene Informationen enthalten, von Systemstatus bis zu umfassenden Datensätzen.

Um dies zu erreichen, nutzt CMP seinen Antwortverarbeitungsmechanismus, um die nahtlose und genaue Übertragung von Daten zurück in die CMDB sicherzustellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Funktionen von Response Mapping

- Ordnet das externe Datenformat dem ServiceNow-Format für den IRE-Verbrauch zu.
- Unterstützt einfache und komplexe Zuordnungen, geskriptete Zuordnungen, Bindungszuordnungen und Beziehungszuordnungen.
- Signifikantes Element zum Hinzufügen neuer/Ändern von Zuordnungen.
- Leistungsstark, in CMP für die letzten Releases verwendet.

Weitere Informationen finden Sie unter https://www.servicenow.com/community/itom-articles/cmp-using-response-mapping-how-to-populate-cmdb-using-cmp/ta-p/2323213 .

Parameterwert mit der AllowedPattern-Eigenschaft validieren

Die Eigenschaft *AllowedPattern* in einer Vorlage von Azure Resource Manager (ARM) oder CloudFormation (CF) führt vor dem Senden einer Bereitstellungsanforderung eine Eingabevalidierung durch.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird

Sie können Regeln bereitstellen, um einen Parameterwert zu validieren, bevor die Bereitstellungsanforderung an die Cloud gesendet wird. Um bei einer fehlgeschlagenen Validierung mit einer Fehlermeldung benachrichtigt zu werden, geben Sie die Eigenschaft *ConstraintDescription* in der Vorlage an. Sie können die Fehlermeldung in der Eigenschaft *ConstraintDescription* anpassen, um die Nachricht klar und eindeutig zu formulieren. Normalerweise verfügen die CF-Vorlagen bereits über die Eigenschaften *AllowedPattern* und *ConstraintDescription*. Wenn diese Eigenschaften nicht vorhanden sind, können Sie sie wie im folgenden Verfahren erwähnt hinzufügen:

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Cloud-Vorlagen**.
2. Wählen Sie eine Vorlage aus, oder klicken Sie auf **Neu**, um eine neue Cloud-Vorlage zu erstellen.
   Wenn Sie eine vorhandene Vorlage auswählen, benennen Sie die Vorlage um.
3. Nehmen Sie in einer ARM- oder einer CF-Vorlage im Textfeld **Text** die folgenden Änderungen vor.

   a. Nehmen Sie in einer ARM-Vorlage die folgenden Änderungen vor:
      - Geben Sie im Abschnitt „parameters“ unter „metadata“ *SNC::Parameter::Metadata* ein.
      - Fügen Sie den Schlüssel *AllowedPattern* hinzu, und geben Sie einen gültigen Wertebereich ein.
      - Fügen Sie den Schlüssel *ConstraintDescription* hinzu, und geben Sie eine Fehlermeldung ein.

```
"parameters": {
        "newStorageAccountName": {
            "type": "string",
             "metadata": {
                 "description": "Unique DNS Name for the Storage
 Account where the Virtual Machine's disks will be placed.",
                  "SNC::Parameter::Metadata": {
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                        "allowedPattern": "[0-9a-z]{1,11}",
                         "ConstraintDescription": "must be an
alphanumeric "

                            }}}
```

b. Nehmen Sie in einer CF-Vorlage die folgenden Änderungen vor:

- Fügen Sie den Schlüssel *AllowedPattern* hinzu, und geben Sie einen gültigen Wertebereich ein.
- Fügen Sie den Schlüssel *ConstraintDescription* hinzu, und geben Sie eine Fehlermeldung ein.

```
"Parameters" : {
                 "SSHLocation" : {
                 "Description" : "The IP address range that can be used
 to SSH to the EC2 instances",
                 "Type": "String",
                 "MinLength": "9",
                 "MaxLength": "18",
                 "Default": "0.0.0.0/0",
                  "AllowedPattern":
 "(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})\\.(\\d{1,3})/(\\d{1,2})",
                  "ConstraintDescription": "must be a valid IP CIDR
 range of the form x.x.x.x/x."

    }
  }
```

4. Klicken Sie auf **Absenden**.

Cloud-Governance

Governance bezieht sich auf die Einschränkungen, die Sie für verfügbare Cloud-Ressourcen festlegen können.

Governance-Typen

Typ	Beschreibung
Kontingente	Kontingente sind für Konfigurationselemente oder Cloud-Ressourcen geltende Einschränkungen oder Anforderungen für Gruppen und Benutzer. Verwenden Sie Kontingente, um eine verschwenderische Ressourcennutzung in Ihrer Cloud-Umgebung zu verhindern.
Richtlinien	Eine Cloud-Richtlinie kann einen von einem Benutzer festgelegten Eigenschaftswert überschreiben, eine Genehmigungsaufgabe erstellen, eine IP-Adresse reservieren, Formularfelder vorausfüllen oder ausblenden, benutzerdefinierte Skripts ausführen, die Cloud-API aufrufen oder Workflows starten oder abbrechen. Eine Cloud-Richtlinie gibt Ihnen eine systemweite Kontrolle über Genehmigungen, Ressourcenvorgänge, Blaupausenvorgänge oder Katalogelementeinstellungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Typ	Beschreibung
Pools	Ein Ressourcenpool ist eine Abfrage oder ein Skript zur Filterung einer Tabelle. Sie konfigurieren einen Ressourcenpool, um die Werte zu beschränken, die Benutzern bei der Anforderung eines Katalogelements zur Verfügung stehen.
Berechtigungen	Berechtigungen sind Zugriffsrechte auf Benutzergruppenebene für verschiedene Funktionen in der Cloud Provisioning and Governance-Anwendung und für bestimmte Datensätze in der Instanz, wie beispielsweise Blaupausen oder Cloud-Accounts.

Berechtigungsverwaltung für Cloud-Governance-Rollen

Berechtigungen sind Zugriffsrechte auf Benutzergruppenebene für verschiedene Funktionen in der Cloud Provisioning and Governance-Anwendung und für bestimmte Datensätze in der Instanz, wie beispielsweise Blaupausen oder Cloud-Accounts.

Sie können basierend auf der Benutzergruppe detailliert festlegen, welche Aktionen für Benutzer zulässig oder verboten sind. Standardmäßig umfasst jede Rolle Zugriffsrechte, aber nicht alle Benutzer mit der gleichen Rolle können die Datensätze der anderen Benutzer anzeigen oder bearbeiten. Beispielsweise verfügen Benutzer mit der Rolle „cloud_designer“ standardmäßig über vollständigen Lese- und Schreibzugriff auf ihre eigenen Blaupausen, sie haben jedoch keinen Lese- oder Schreibzugriff auf Blaupausen, die von anderen Cloud-Designern erstellt wurden. Wenn Sie möchten, dass sie Zugriff haben, müssen Sie die Benutzer in eine Gruppe mit der Rolle „cloud_designer“ einordnen und dieser Gruppe dann Lese- und Schreibzugriff auf bestimmte Blaupausen geben.

Berechtigungstypen

Zugriff [Lesen]
: Benutzer können den Datensatz anzeigen, aber nicht bearbeiten oder löschen.

Verwalten [Erstellen und aktualisieren]
: Benutzer können den Datensatz anzeigen und neue Datensätze in derselben Tabelle erstellen und aktualisieren, aber keine Datensätze löschen.

Löschen
: Benutzer können angegebene Datensätze oder alle Datensätze in der Tabelle löschen.

Ausführen
: Benutzer können eine Aktion für Datensätze in der Tabelle ausführen.

Alle
: Benutzer haben Berechtigungen für alle Datensätze in der Tabelle.

Berechtigungsvorschläge

Erwägen Sie, diese Berechtigungen in Ihrer Organisation zu gewähren:

Vorgeschlagene Gruppe und Rolle	Benutzertyp in der Gruppe	Berechtigungsvorschläge	Beschreibung
Katalogbenutzergruppe Cloud-Benutzer `[sn_cmp.cloud_service_user]`	Benutzer, die ähnliche Elemente aus dem Katalog im	Zugreifen [lesen] oder ausführen	Katalogelemente können auch nach der Veröffentlichung von Benutzern im

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgeschlagene Gruppe und Rolle	Benutzertyp in der Gruppe	Berechtigungsvorschläge	Beschreibung
	Cloudbenutzerportal bestellen.		Cloudbenutzerportal erst angezeigt werden, nachdem Sie einer Benutzergruppe, der diese Benutzer angehören, Lesezugriff auf die Elemente gewähren. Gewähren Sie Cloud-Benutzern Zugriffs- und Ausführungsberechtigungen für die Tabellen „Blaupausenkatalogelement“ und „Cloud-Konto“.
Blaupausendesigner Servicedesigner [sn.cmp.cloud_service_designer]	Benutzer, die Blaupausen entwerfen.	Verwalten [Erstellen und aktualisieren]	Blaupausendesigner können andere Blaupausen oder Katalogelemente standardmäßig nicht anzeigen oder bearbeiten. Zur Zusammenarbeit oder zur Wiederverwendung vorhandener Blaupausen und Katalogelemente benötigen Blaupause-Designer über die Berechtigung „Verwalten“ Zugriff auf die Blaupausen anderer Benutzer.
Cloud-Administratoren Cloud-Administrator `[sn_cmp.cloud_admin]`	Benutzer, die Cloud-Accounts erstellen und verwalten.	Verwalten [Erstellen und aktualisieren]	Cloud-Administratoren müssen Vorlagen entsprechenden Ressourcenprofile zuordnen. Zur Zusammenarbeit oder zur Wiederverwendung vorhandener Ressourcenprofile und Vorlagen.

Cloud-Berechtigung zuweisen

Weisen Sie eine Berechtigung zu, um basierend auf der jeweiligen Benutzergruppe detailliert festzulegen, welche Aktionen für Benutzer zulässig oder verboten sind.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

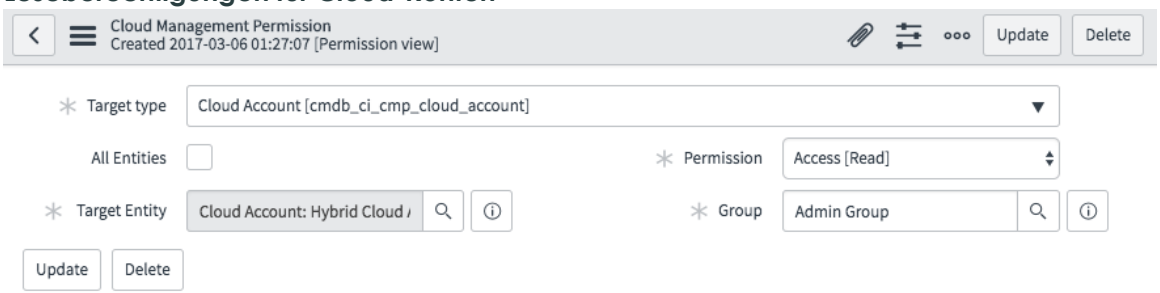
Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor
- Die Anwendergruppe , auf die die Berechtigung angewendet werden soll.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Adminportal** > **Governance** > **Berechtigung**.
2. Füllen Sie die Formularfelder aus (siehe Tabelle).

Leseberechtigungen für Cloud-Konten



Feld	Beschreibung
Zieltyp	Wählen Sie die Cloud-Tabelle aus, zu der der Zieldatensatz gehört.
Alle Entitäten	Wählen Sie diese Option aus, um die Berechtigung auf alle Datensätze in der Tabelle anzuwenden.
Berechtigung	Wählen Sie den Berechtigungstyp aus.
Zielentität	Wählen Sie den Datensatz aus, auf dem die Berechtigung basiert.
Gruppe	Wählen Sie die Benutzergruppe aus.

3. Klicken Sie auf **Absenden**.

Richtlinien für Cloud Provisioning

Eine Cloud-Richtlinie kann einen von einem Benutzer festgelegten Eigenschaftswert überschreiben, eine Genehmigungsaufgabe erstellen, eine IP-Adresse reservieren, Formularfelder vorausfüllen oder ausblenden, benutzerdefinierte Skripts ausführen, die Cloud-API aufrufen oder Workflows starten oder abbrechen. Eine Cloud-Richtlinie gibt Ihnen eine systemweite Kontrolle über Genehmigungen, Ressourcenvorgänge, Blaupausenvorgänge oder Katalogelementeinstellungen.

Example: Ein Benutzer fordert einen Stapel an, mit dem eine Genehmigungsrichtlinie ausgelöst wird

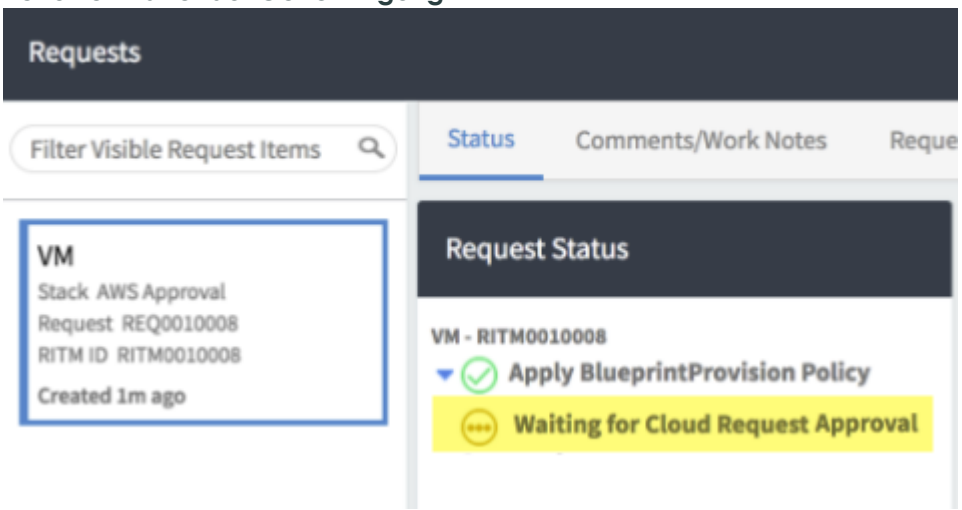
1. Ein Benutzer sendet im Cloudbenutzerportal eine Anforderung zur Bereitstellung einer bestimmten Blaupause. Der Prozess der Bereitstellung der Blaupause ist der Auslöser, mit dem das Richtlinienmodul zur Anwendung einer Genehmigungsrichtlinie veranlasst wird. Eine Cloud-Genehmigungsrichtlinie gibt die Benutzer an, die eine angegebene Cloud-Aktivität genehmigen müssen, bevor die Aktivität fortgesetzt werden kann.
2. Vom Richtlinienmodul wird festgestellt, dass die Anforderung die in der Regel für die Richtlinie angegebene Bedingung erfüllt. In diesem Beispiel wird die Bedingung immer dann als „true“ (wahr) bewertet, wenn eine bestimmte Blaupause bereitgestellt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Da die Bedingung erfüllt ist, wird vom Richtlinienmodul die Aktion ausgeführt, die auch in der Regel angegeben ist. In diesem Beispiel besteht die Aktion darin, eine Genehmigungsaktion für den Manager anzulegen.
4. Während der Genehmiger (der Manager) die Genehmigungsanforderung überprüft, wird dem Benutzer im Cloudbenutzerportal die Statusmeldung „Warte auf Genehmigung“ angezeigt.
5. Die Blaupause wird nach Genehmigung durch den Manager bereitgestellt.

Benutzer wartet auf Genehmigung



Hinweis: Während Sie einen Ressourcenvorgangsschritt hinzufügen, können Sie keine Flows aufrufen. Dies ist eine bekannte Einschränkung.

Richtlinienauslöser

Auslöser sind Ereignisse, die das Richtlinienmodul in Gang setzen. Beispielsweise wird der Auslöser *`bei Ende der Katalogelementanforderung`* ausgelöst, nachdem ein Benutzer ein Anforderungsformular übermittelt hat. Wenn Sie eine Richtlinie definieren möchten, sollten Sie zuerst darüber nachdenken, wie die Richtlinie ausgelöst wird. Beispiele:

- Ein Benutzer fordert einen Vorgang *`Stoppen`* für einen virtuellen Server an (was den Auslöser *`bei Stapelressourcenvorgang`* auslöst).
- Eine Ressource erreicht das Ende ihres Leasings (was den Auslöser *`bei Leasingende`* auslöst).
- Ein Benutzer fordert einen bestimmten Stapel an (was den Auslöser *`bei Blaupausenbereitstellung`* auslöst).

Sie verweisen normalerweise auf eine Richtlinie anhand des Namens des Auslösers der Richtlinie. Beispielsweise können Sie eine Richtlinie, die durch den Auslöser *`bei Leasingende`* ausgelöst wird, als „Richtlinie für Leasingende“ bezeichnen. Weitere Informationen zu den Typen von Auslösern, die Sie implementieren können, finden Sie unter Auslöser für Cloud-Richtlinien.

Funktionsweise von Richtlinien

Für jede Richtlinie konfigurieren Sie normalerweise einen Auslöser, der die Richtlinien-Engine startet. Die Richtlinien-Engine setzt die Richtlinie durch, indem sie alle Regeln ausführt, die für die Richtlinie definiert sind. Eine Richtlinienregel ist eine Sammlung von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das Richtlinienmodul

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

die Aktionen aus. Wird eine Bedingung als „false“ ausgewertet, führt das Richtlinienmodul die Aktionen nicht aus.

- Einige Richtlinientypen gelten nur für bestimmte Typen von Cloud-Vorgängen, z. B. „Starten“, „Stoppen“, „Bereitstellung“ oder „Bereitstellung aufheben“, oder für ein bestimmtes Ziel, z. B. „bei Bereitstellungsvorgang für Blaupause123“ oder „bei Start von Katalogelement ABC“.
- Sie können eine Richtlinie konfigurieren, die kein Ziel angibt, z. B. „bei jedem Bereitstellungsvorgang für eine Blaupause“ oder „bei jedem Start eines Katalogelements“. Fehler in Richtlinien, die für ein beliebiges Objekt gelten, werden ignoriert.
- Wenn mehrere Richtlinien gelten, können Sie die Reihenfolge angeben, in der die Richtlinien angewendet werden (mit einer Ausnahme, die im folgenden Abschnitt beschrieben wird).
- Richtlinien können mit dynamischen Formularen zusammenarbeiten, damit Sie Formularfelder für Endbenutzer ein- oder ausblenden können. Benutzer sehen nur Informationen, die sie Ihrer Entscheidung nach für das Verständnis und die Erfüllung ihrer Aufgaben benötigen.

Richtliniengruppen

Eine Cloud-Richtliniengruppe ist ein Container für zugehörige Richtlinien. Es empfiehlt sich, Richtlinien, die häufig zusammen verwendet werden oder zusammen betrachtet werden sollen, zu gruppieren. Durch die Gruppierung von Richtlinien können Sie Richtlinien konsistent in Ihrer Organisation anwenden.

Reihenfolge der Ausführung, wenn mehrere Richtlinien gelten

Reihenfolge der Ausführung, wenn mehrere Richtlinien vom Typ „Genehmigung“ gelten:

Wenn mehrere „Genehmigungsrichtlinien“ gelten, werden die Richtlinien in der folgenden Reihenfolge angewendet. (Die Genehmigungsrichtlinien sind *`bei Blueprint-Bereitstellung (Genehmigung)`*, *`bei Stapelvorgang (Genehmigung)`*, *`bei Stapelressourcenvorgang (Genehmigung)`*und *`bei Aufgabenkorrektur`*):

1. Nur die erste erfolgreiche Genehmigungsrichtlinie wird angewendet. Es werden keine weiteren Genehmigungsrichtlinien angewendet.
2. Wenn die angewendete Genehmigungsrichtlinie mehrere Regeln aufweist, wird nur die erste erfolgreiche Regel verwendet.
3. Wenn eine Regel über mehrere Aktionen verfügt, wird nur die erste erfolgreiche Aktion ausgeführt.
4. Wenn die angewendete Genehmigungsrichtlinie sowohl eine benutzerdefinierte Genehmigung als auch eine ServiceNow-Genehmigung enthält, wird nur der benutzerdefinierte Genehmigungsprozess ausgeführt.

Reihenfolge der Ausführung für alle anderen Richtlinientypen:

- Richtlinien werden in der Reihenfolge angewendet, die durch die Eigenschaftseinstellung **Reihenfolge der Ausführung** angegeben ist.
- Wenn mehrere Richtlinien dieselbe Einstellung **Reihenfolge der Ausführung** aufweisen, wird die Reihenfolge nicht garantiert.

Vorgänge in Richtlinien

Auslöser basieren häufig auf Benutzeranforderungen und den Vorgängen (Starten, Anhalten, Bereitstellen oder Bereitstellung aufheben), die für einen Blueprint, ein Katalogelement, eine

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressource oder einen Stapel ausgeführt werden können. Einige Auslösertypen geben keinen Cloud-Vorgang an. Zum Beispiel erfolgt die Auslösung des Auslösers *bei Leasingende* unabhängig von jedem Vorgang.

Richtlinienregeln

Eine Richtlinienregel ist eine Sammlung von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das Richtlinienmodul die Aktionen aus. Wird eine Bedingung als „false“ ausgewertet, führt das Richtlinienmodul die Aktionen nicht aus.

- Bedingungen: Bedingungen können Anforderungsformulardaten, Ressourcenaktivitäten oder Benutzeraktivitäten berücksichtigen. Beispiele:
  - Ist die angeforderte CPU größer als 32?
  - Handelt es sich um einen Vorgang *Stoppen*?
  - Endet das Leasing für diese Ressource in den nächsten 7 Tagen?
- Aktionen: Wenn alle Bedingungen als „true“ ausgewertet werden, führt die Richtlinien-Engine die in der Regel angegebenen Aktionen aus. Ausdrücke in Richtlinienaktionen können Werte festlegen oder überschreiben. Beispiele:
  - Der vom Benutzer angegebenen Wert wird überschrieben, indem die CPU-Größe auf 16 geändert wird, dann wird der Genehmigungsprozess gestartet (da die Bedingung erfüllt war, dass die angeforderte CPU größer als 32 ist).
  - Eine Genehmigungsaufgabe für den Manager wird erstellt (da die Bedingung erfüllt war, dass ein Vorgang *Stoppen* angefordert wurde).
  - Benachrichtigungen werden an alle Benutzer in der Gruppe „ABC“ gesendet (da die Bedingung erfüllt war, dass der Leasingvertrag in 7 Tagen endet).

Richtlinien-Aktionsskripts

- Verwenden Sie Richtlinienaktionsskripts, um Werte in Cloud-Anforderungen abzurufen, zu aktualisieren oder festzulegen.
- Ihre Instanz verfolgt für Abrechnung und Berichterstellung getaggte Ressourcen nach. Richtlinienaktionsskripts können Ressourcen-Tags hinzufügen und ändern.

Cloud-Richtlinienbeispiel

Eine Basissystem-Cloud-Richtlinie *Leasingende ServiceNow* verwendet den Auslöser *bei Leasingende*, der ausgelöst wird, wenn sich eine virtuelle Ressource dem Enddatum des Leasingvertrags nähert. Wenn die Bedingungen in der Richtlinienregel erfüllt sind, sendet die Richtlinien-Engine eine Benachrichtigung an den Besitzer der Ressource und führt Vorgänge für die Ressource aus.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

In diesem Beispiel arbeiten Sie mit der Richtlinie *Leasingende ServiceNow*. Die Richtlinie führt die folgenden Aktionen aus, wenn die Bedingungen in der Richtlinienregel erfüllt sind:

- Senden einer Benachrichtigung an den Besitzer einer Cloud-Ressource, wenn der Leasingvertrag für die Ressourcen in Kürze ausläuft.
- Ausführen eines Vorgangs *Stoppen* für die Ressource.
- Ausführen eines Vorgangs *Bereitstellung aufheben* für die Ressource.

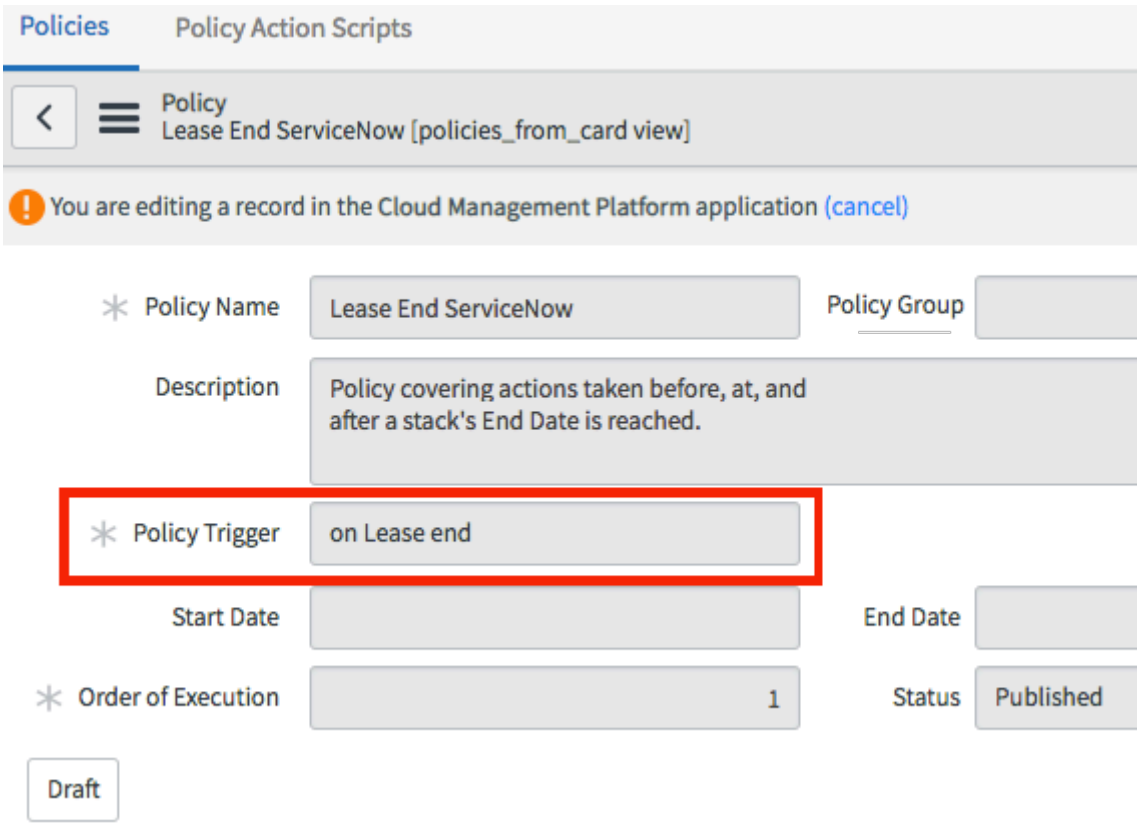
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können jede Basissystem-Richtlinie ändern, indem Sie Einstellungen ändern oder die Richtlinie aktivieren oder deaktivieren.

Hinweis: Geplante Start-/Stopp-Vorgänge werden für die Terraform-Vorlage und die Google Deployment Manager-(GDM-)Stapel nicht unterstützt.

Prozedur

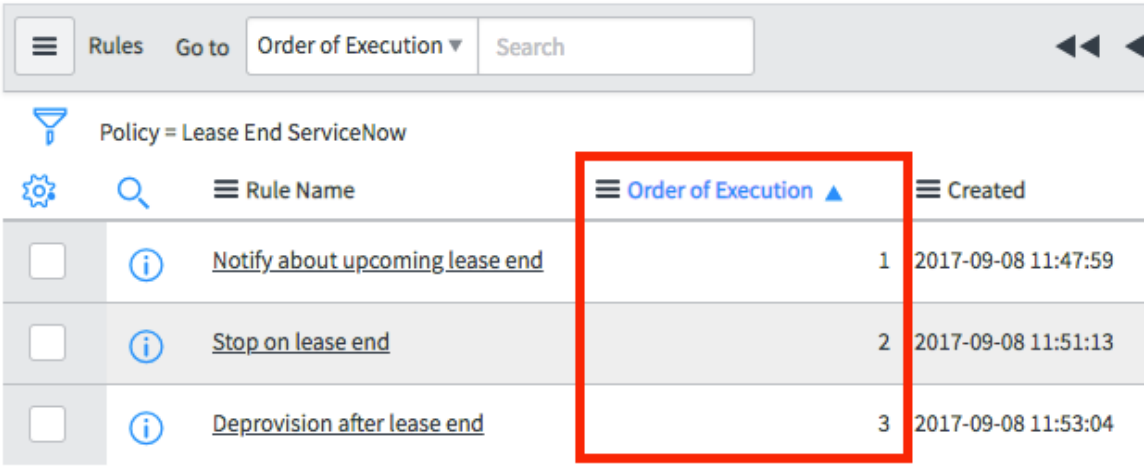
1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Suchen Sie nach der Richtlinie **Leasingende ServiceNow**, und öffnen Sie sie.
3. Beachten Sie, dass der Auslöser **bei Leasingsende** lautet, was bedeutet, dass die Richtlinie ausgelöst wird, wenn der Leasingvertrag für die Ressource fast abgelaufen ist.



4. Sortieren Sie die zugehörige Liste „Regeln“ nach **Reihenfolge der Ausführung**. Die Regel mit der niedrigsten Nummer wird zuerst ausgeführt.

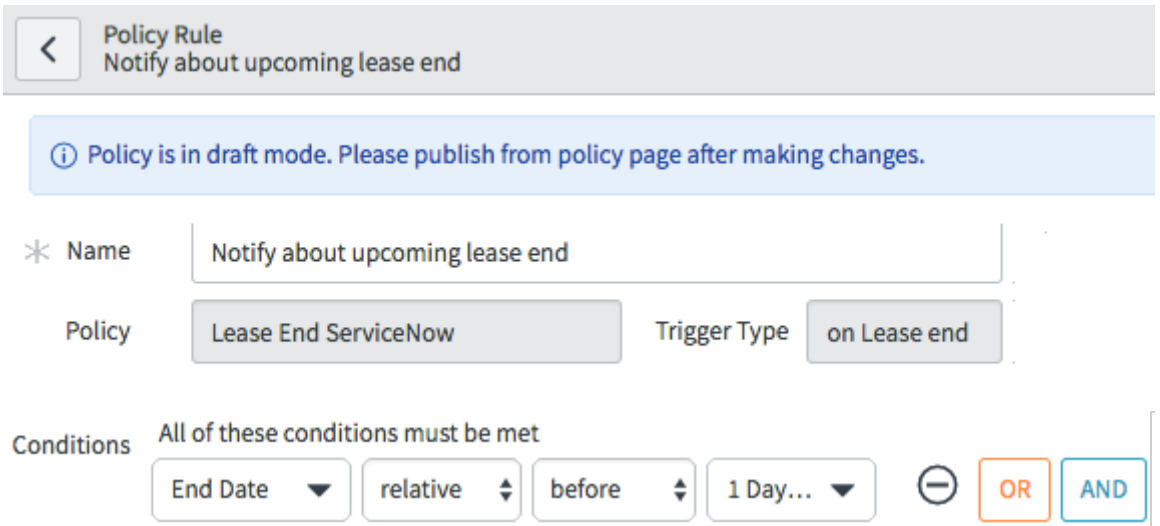
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beachten Sie, dass eine Benachrichtigungsregel zuerst ausgeführt wird, gefolgt von den Vorgängen *`Stoppen`* und *`Bereitstellung aufheben`* für die Ressource.

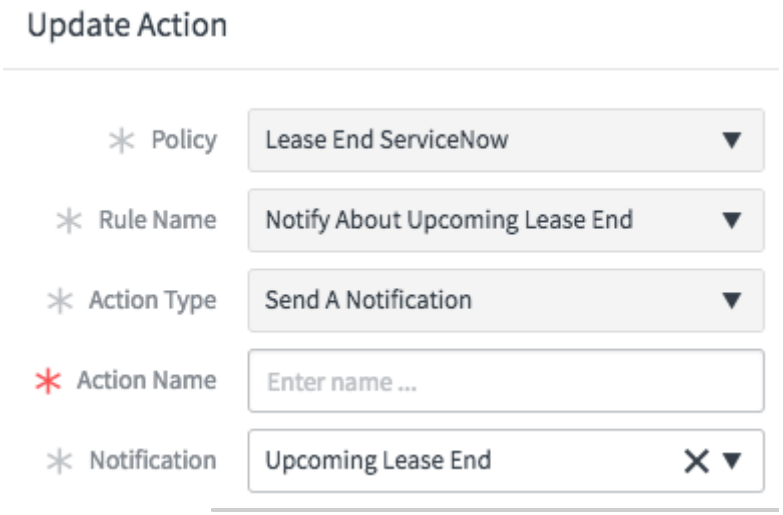
5. Klicken Sie auf die Regel **bei bevorstehendem Leasingende benachrichtigen**.
6. Beachten Sie, dass die Regel eine Bedingung angibt: Wenn das aktuelle Datum einen Tag vor dem Enddatum liegt, wird `true` zurückgegeben.



7. Klicken Sie in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf den (leeren) **Namen** der Aktion.
8. Geben Sie im Popup-Fenster Update Action (Aktion aktualisieren) einen **Aktionsnamen** ein (der Wert ist erforderlich), beachten Sie den Wert der **Benachrichtigung** (Sie werden ihn im nächsten Schritt verwenden), und schließen Sie das Popup-Fenster.

Automatische Übersetzung

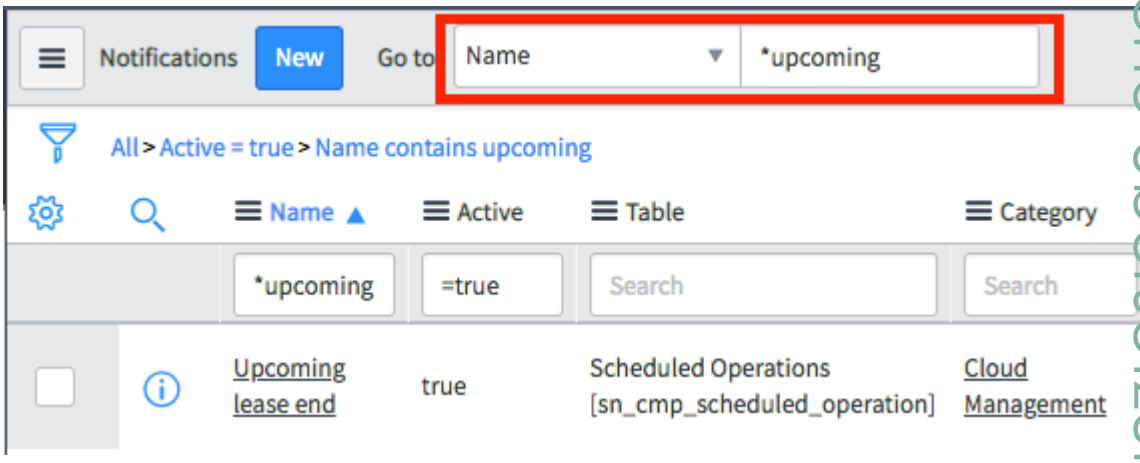
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Überprüfen Sie die anderen Einstellungen der Benachrichtigungsnachricht:

a. Navigieren Sie in der -Instanz (nicht Portal für Cloud-Admin.) zu **Systembenachrichtigung** > **E-Mail** > **Benachrichtigungen**.

b. Suchen Sie nach der in der Aktion angegebenen Benachrichtigung, indem Sie den Filtertext `*Bevorstehendes Leasingende` für **Name** eingeben, und öffnen Sie sie:



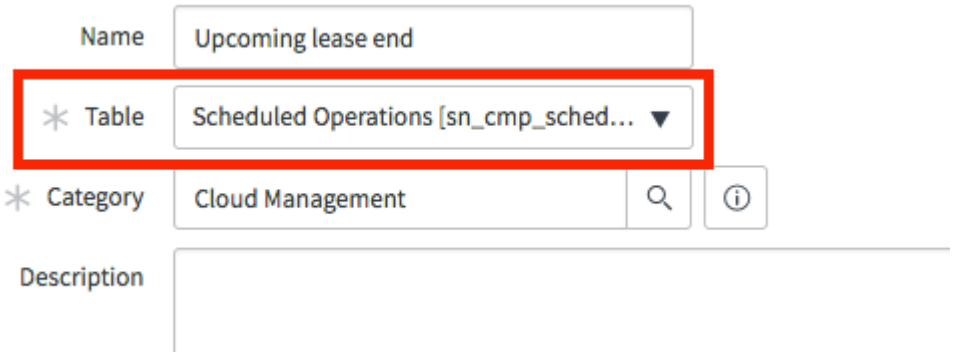
c. Klicken Sie auf **Bevorstehendes Leasingende**, um das Benachrichtigungsformular zu öffnen.

Beachten Sie, dass die Tabelle **Geplante Vorgänge [sn_cmp_scheduled_operation]** angegeben ist.

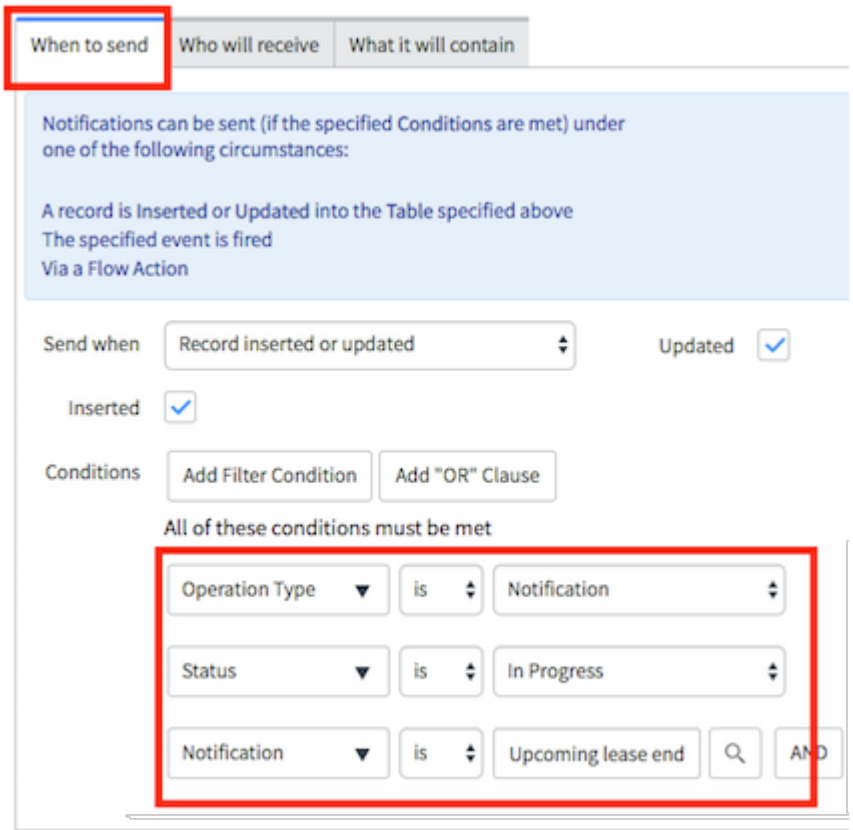
Hinweis: Sie basieren alle Benachrichtigungen für Cloud Provisioning and Governance auf dieser Tabelle.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Beachten Sie auf der Registerkarte **Absendezeitpunkt** die geltenden Bedingungen:



Bedingung	Beschreibung
Vorgangstyp ist „Benachrichtigung“	Gibt an, dass das Feld **Vorgangstyp** in der Tabelle „Geplante Vorgänge“ **Benachrichtigung** lauten muss.
Status	Gibt an, dass das System die Benachrichtigung auslösen soll, wenn der Status des Datensatzes des geplanten Vorgangs in Bearbeitung ist, anstatt zu warten, bis er abgeschlossen ist.
Benachrichtigung	Gibt an, dass die Benachrichtigung *`Upcoming lease end`* angegeben werden muss.

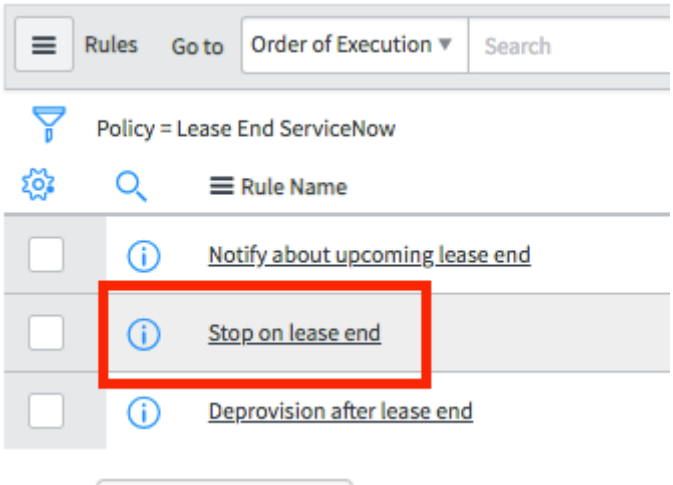
Hinweis: Wenn Sie eine benutzerdefinierte Benachrichtigung erstellen, verwenden Sie die Standardbedingungen, ändern Sie jedoch die Bedingung **Benachrichtigung** in den Namen Ihrer Benachrichtigung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

e. Klicken Sie auf die Registerkarte **Empfänger**.

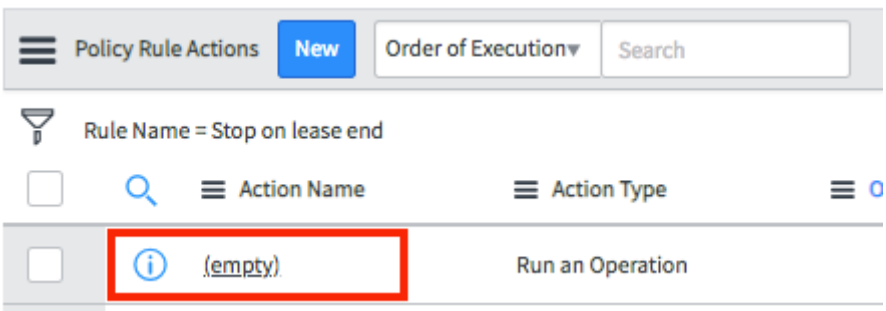
Beachten Sie, dass der Wert für **Benutzer/Gruppen in Feldern** auf `Target.Assigned to`, `Target.Owned` festgelegt ist. Verwenden Sie diese Einstellungen, um die Benachrichtigung an den Besitzer der virtuellen Ressource zu senden.

10. Öffnen Sie im Portal für Cloud-Admin. die Richtlinie „Leasingende ServiceNow“ erneut, und öffnen Sie dann die Regel **bei Leasingende stoppen**.



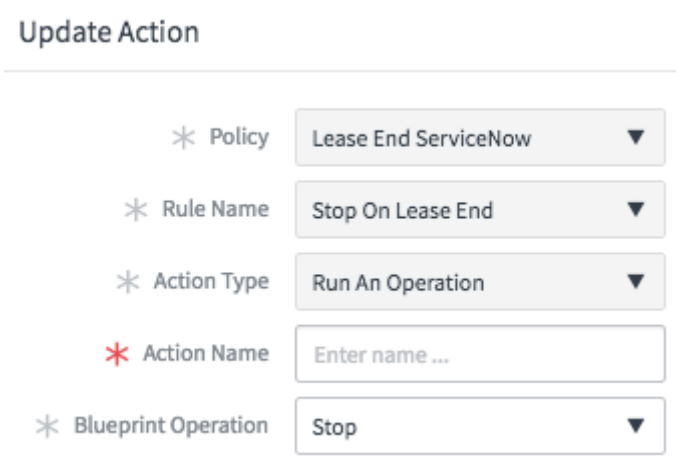
Die Regel hat zwei Aktionen: eine Aktion zum Senden einer Benachrichtigung und die andere Aktion zum Ausführen des Vorgangs *`Stoppen`* für die virtuelle Ressource.

11. Klicken Sie bei dem Vorgang *`Stoppen`* auf den (leeren) **Aktionsnamen** der Aktion.



12. Beachten Sie im Popup-Fenster „Aktualisierungsaktion“ die Einstellungen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
Richtlinien- und Regelname	Die Richtlinie und die Regel, zu denen diese Aktion gehört, werden standardmäßig in diesen Feldern angegeben.
Aktionstyp	**Vorgang ausführen** weist die Richtlinien-Engine an, einen Standardvorgang (*Starten*, *Stoppen*, *Bereitstellung aufheben* usw.) für die Ressource auszulösen.
Planvorgang	Das System führt den Vorgang *STOPPEN* für die Ressource aus.

Die andere Regel, **Bereitstellung nach Leasingende aufheben**, führt den Vorgang *Bereitstellung aufheben* für die Ressource aus, damit sie nach dem Leasingenddatum nicht mehr aktiv bleibt.

Nächste Maßnahme

In diesem Beispiel werden die über die Formularkonfiguration verfügbaren Einstellungen verwendet. Beispielskripts, die Sie zusätzlich verwenden könnten, finden Sie unter Richtlinienaktionsskript erstellen.

Auslöser für Cloud-Richtlinien

Auslöser sind Ereignisse, die das Richtlinienmodul in Gang setzen. Beispielsweise wird der Auslöser *bei Ende der Katalogelementanforderung* ausgelöst, nachdem ein Benutzer ein Anforderungsformular übermittelt hat. Wenn der Auslöser für eine Richtlinie ausgelöst wird, testet die Richtlinien-Engine die in der Richtlinienregel angegebenen Bedingungen und führt die in der Regel angegebenen Aktionen aus, wenn die Bedingungen erfüllt sind.

Auslöser

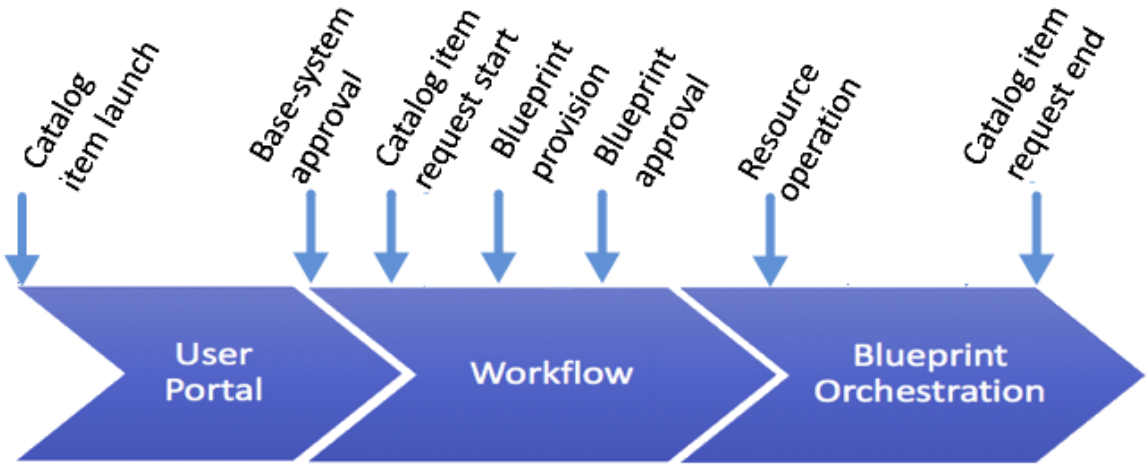
- Sie verweisen normalerweise auf eine Richtlinie anhand des Namens des Auslösers der Richtlinie. Beispielsweise können Sie eine Richtlinie, die durch den Auslöser *bei Leasingende* ausgelöst wird, als „Richtlinie für Leasingende“ bezeichnen.
- Auslöser basieren häufig auf Benutzeranforderungen und den Vorgängen (Starten, Anhalten, Bereitstellen oder Bereitstellung aufheben), die für einen Blueprint, ein Katalogelement, eine Ressource oder einen Stapel ausgeführt werden können. Einige Auslösertypen geben keinen Cloud-Vorgang an. Zum Beispiel erfolgt die Auslösung des Auslösers *bei Leasingende* unabhängig von jedem Vorgang.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Um die Leistung zu optimieren, beschränken Sie die Anzahl der Richtlinien mit allgemeinen Auslösern wie den Auslösern *bei Katalogelement*.
- Ein Auslöser, der kein Ziel (eine Blaupause, ein Katalogelement, einen Stapel oder eine Ressource) angibt, wird immer ausgeführt. Um die Leistung zu optimieren, minimieren Sie daher die Verwendung solcher Richtlinien.

Wichtig: Blueprints sind veraltet. Die Auslöserbeschreibungen, die dem Zeitleistenschema unten folgen, gelten auch für die Erstellung von Katalogen, die auf Cloud-Vorlagen basieren.

Zeitleiste für Bereitstellungsauslöser



Richtlinienauslöser

Arten von Richtlinienauslösern und die Aktionen, die für die zugehörigen Richtlinienregeln verfügbar sind

Auslösername und -aktionen	Beschreibung
on Blueprint provision (bei Blaupausenbereitstellung) Aktionen: • Skript ausführen • Eigenschaft außer Kraft setzen • Prozess abbrechen	Der Auslöser *bei Blaupausenbereitstellung* wird nach der Ausführung der Richtlinien *bei Beginn der Katalogelementanforderung* ausgelöst. Durch eine Richtlinie, die durch den Auslöser *bei Blaupausenbereitstellung* ausgelöst wird, kann ein Skript ausgeführt, ein vom Benutzer angeforderter Attributwert außer Kraft gesetzt oder ein Bereitstellungsvorgang abgebrochen und eine entsprechende Nachricht gesendet werden. Verwenden Sie diesen Auslöser, um einen vom Benutzer eingegebenen Wert außer Kraft zu setzen. Wenn ein Benutzer beispielsweise für ein Attribut einen Wert wie den Stapelnamen auswählt, kann der Name des Stapels durch eine Richtlinie mit diesem Auslöser geändert werden. Darüber hinaus kann durch eine weitere Aktion der Name wieder geändert werden, wenn der Benutzer die Ressource schließlich bereitstellt. Der Benutzer sieht den endgültigen Wert nicht im Formular des Katalogelements, da die Änderung zur Bereitstellungszeit vorgenommen wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten von Richtlinienauslösern und die Aktionen, die für die zugehörigen Richtlinienregeln verfügbar sind (Fortsetzung)

Auslösername und -aktionen	Beschreibung
	Aktion für eine Richtlinie „bei Blaupausenbereitstellung“ erstellen
Genehmigungsauslöser • **bei Genehmigung des Stapelvorgangs**: Wird während eines beliebigen Stapelvorgangs im Cloudbenutzerportal ausgelöst. • **bei Genehmigung des Stapelressourcenvorgangs**: Wird während eines Ressourcenvorgangs (Starten, Stoppen, Bereitstellung usw.) im Cloudbenutzerportal ausgelöst. • **bei Aufgabenremediation**: Wird ausgelöst, wenn ein Benutzer eine fehlgeschlagene Anforderung erneut übermittelt. Aktionen: • ServiceNow Genehmigung • Benutzerdefinierte Genehmigung	Eine Cloud-Genehmigungsrichtlinie gibt die Benutzer an, die eine angegebene Cloud-Aktivität genehmigen müssen, bevor die Aktivität fortgesetzt werden kann. Genehmiger können den Manager des Benutzers, der eine Anforderung sendet, einen angegebenen Benutzer oder eine bestimmte Gruppe oder Benutzer mit einer bestimmten Rolle einschließen. Sie können mehrere Genehmiger angeben. Genehmigungen erfolgen in der von Ihnen angegebenen Reihenfolge. Eine Richtlinie, die von einem der Genehmigungsauslöser ausgelöst wird, kann Genehmigungs-Workflows starten. Die gezielten Genehmigungsrichtlinien ergänzen die Basissystem-Genehmigungsvorgänge. **Hinweis:** Der Genehmigungsprozess wird ausgeführt, nachdem die Eigenschaften festgelegt wurden, da überschriebene Eigenschaftswerte zu einer Änderung der Kosten führen könnten. `on Blueprint provision (approval)` (bei Blaupausenbereitstellung (Genehmigung)) wird angewendet, bevor die Blaupause bereitgestellt wird. Da durch den Bereitstellungsprozess jedoch Anforderungsdaten (und möglicherweise auch Kosten) geändert werden können, werden Genehmigungsprozesse nach der Bereitstellung der Blaupause ausgeführt. Verwenden Sie `on Stack operation (approval)` (bei Stapelvorgang (Genehmigung)) zum Ausführen eines Genehmigungs-Workflows, wenn ein Vorgang auf einem Stapel ausgeführt wird. Standardmäßig wird eine Change-Anforderung erzeugt, wenn ein Vorgang für einen Stapel ausgeführt wird. Sie erfordert jedoch keine Genehmigung. Durch diesen Auslöser kann eine obligatorische Genehmigung gestartet werden. Verwenden Sie `on Stack operation (approval)` (bei Stapelvorgang (Genehmigung)) zum Ausführen eines Genehmigungs-Workflows, wenn ein Vorgang für eine einzelne Ressource ausgeführt wird, die Teil eines Stapels ist. Standardmäßig wird eine Change-Anforderung erzeugt, wenn ein Vorgang für einen Stapel ausgeführt wird. Sie erfordert jedoch keine Genehmigung. Durch diesen Auslöser kann eine obligatorische Genehmigung gestartet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten von Richtlinienauslösern und die Aktionen, die für die zugehörigen Richtlinienregeln verfügbar sind (Fortsetzung)

Auslösername und -aktionen	Beschreibung
	Eine Richtlinie, die durch den Auslöser *bei Aufgabenkorrektur* ausgelöst wird, kann Genehmigungs-Workflows starten. Aktion für eine Genehmigungsrichtlinie erstellen
beim Starten des Katalogelements Aktionen: • Skript ausführen • Eigenschaft außer Kraft setzen	Der Auslöser *beim Starten des Katalogelements* wird ausgelöst, wenn ein Bestellformular (Stapelanforderungsformular) für ein Katalogelement gestartet wird. Eine Richtlinie, die durch den Auslöser *beim Starten des Katalogelements* ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Wert überschreiben (nur Textwerte). Verwenden Sie diesen Auslöser, um zu steuern, was der Benutzer beim Öffnen des Formulars im Cloudbenutzerportal sieht. Beispielsweise können Sie einen Standardwert außer Kraft setzen, der dem Benutzer zuerst angezeigt wird. Der Benutzer kann diesen Wert im Katalogelementformular sehen. Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Aktion für eine Richtlinie „beim Starten des Katalogelements“ erstellen
bei Beginn der Katalogelementanforderung Aktionen: • Skript ausführen • Workflow ausführen	Der Auslöser *bei Beginn der Katalogelementanforderung* wird ausgelöst, nachdem der Benutzer ein Anforderungsformular geöffnet hat. Eine Richtlinie, die durch den Auslöser *bei Beginn der Katalogelementanforderung* oder *bei Ende der Katalogelementanforderung* ausgelöst wird, kann ein Skript oder einen Workflow ausführen. Sie können diesen Auslöser verwenden, um ein benutzerdefiniertes Skript oder einen Workflow auszuführen, mit dem Unternehmensprozesse wie die benutzerdefinierte Genehmigung abgewickelt werden können, bevor die Anforderung des Katalogelements verarbeitet wird. Aktion für eine Richtlinie „bei Beginn/Ende der Katalogelementanforderung“ erstellen
bei Ende der Katalogelementanforderung Aktionen:	Der Auslöser *bei Ende der Katalogelementanforderung* wird ausgelöst, nachdem ein Benutzer ein Anforderungsformular übermittelt hat.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten von Richtlinienauslösern und die Aktionen, die für die zugehörigen Richtlinienregeln verfügbar sind (Fortsetzung)

Auslösername und -aktionen	Beschreibung
• Skript ausführen • Workflow ausführen	Eine Richtlinie, die durch den Auslöser *bei Beginn der Katalogelementanforderung* oder *bei Ende der Katalogelementanforderung* ausgelöst wird, kann ein Skript oder einen Workflow ausführen. Verwenden Sie diesen Auslöser, um einen Workflow zu starten, nachdem eine Katalogelementanforderung verarbeitet wurde. Erwägen Sie diesen Auslöser als einen Schritt nach der Bereitstellung. Beispielsweise könnten Sie einen Workflow zum Installieren von MySQL auf der bereitgestellten Ressource starten. Aktion für eine Richtlinie „bei Beginn/Ende der Katalogelementanforderung“ erstellen
bei Leasing-Ende Aktionen: • Vorgang ausführen • Benachrichtigung senden	Eine Richtlinie, die durch den Auslöser *bei Leasingende* ausgelöst wird, kann eine Benachrichtigung senden oder einen Lebenszyklusvorgang *Starten*, *Stoppen* oder *Bereitstellung aufheben* ausführen. Aktion für eine Richtlinie „Mietvertragsende“ erstellen
beim Start des Ressourcenvorgangs Aktionen: • Skript ausführen • Eigenschaft außer Kraft setzen	Der Auslöser *beim Start des Ressourcenvorgangs* wird ausgelöst, bevor der Katalog für einen Ressourcenvorgang aus dem Cloudbenutzerportal geladen wird. Eine Richtlinie, die durch den Auslöser *beim Start des Ressourcenvorgangs* ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Wert überschreiben (nur Textwerte). Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Aktion für eine Richtlinie „beim Start des Ressourcenvorgangs“ erstellen
beim Start der Ressourcenvorgangsanforderung Aktionen: • Skript ausführen • Workflow ausführen	Der Auslöser *beim Start der Ressourcenvorgangsanforderung* wird ausgelöst, nachdem ein Benutzer eine Ressourcenvorgangsanforderung (*Starten*, *Stoppen*, *Bereitstellung aufheben*) übermittelt hat. Eine Richtlinie, die durch den Auslöser *beim Start der Ressourcenvorgangsanforderung* oder *bei Ende der Ressourcenvorgangsanforderung* ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Attributwert überschreiben. Aktion für eine Richtlinie „beim Start/bei Ende der Ressourcenvorgangsanforderung“ erstellen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Arten von Richtlinienauslösern und die Aktionen, die für die zugehörigen Richtlinienregeln verfügbar sind (Fortsetzung)

Auslösername und -aktionen	Beschreibung
bei Ende der Ressourcenvorgangsanforderung Aktionen: • Skript ausführen • Workflow ausführen	Der Auslöser *bei Ende der Ressourcenvorgangsanforderung* wird vor Abschluss eines Lebenszyklusvorgangs für eine Ressource (*Starten*, *Stoppen*, *Bereitstellung aufheben*) ausgelöst. Eine Richtlinie, die durch den Auslöser *beim Start der Ressourcenvorgangsanforderung* oder *bei Ende der Ressourcenvorgangsanforderung* ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Attributwert überschreiben. Aktion für eine Richtlinie „beim Start/bei Ende der Ressourcenvorgangsanforderung“ erstellen
bei Ressourcenvorgang Aktionen: • Eigenschaft außer Kraft setzen • Skript ausführen • Cloud-API aufrufen • IP-Adressverwaltung	Der Auslöser *bei Ressourcenvorgang* wird während des Orchestration-Prozesses ausgelöst, wenn ein Benutzer einen Lebenszyklusvorgang *Starten*, *Stoppen* oder *Bereitstellung aufheben* für eine bestimmten Ressource durchführt. Eine Richtlinie, die durch den Auslöser *bei Ressourcenvorgang* ausgelöst wird, kann einen von einem Benutzer angeforderten Attributwert überschreiben, ein Skript ausführen, eine Cloud API aufrufen oder einen IP-Adressenverwaltungsvorgang ausführen. Aktion für eine Richtlinie „bei Ressourcenvorgang“ erstellen

Cloud-Richtlinie erstellen

Eine Cloud-Richtlinie kann einen von einem Benutzer festgelegten Eigenschaftswert überschreiben, eine Genehmigungsaufgabe erstellen, eine IP-Adresse reservieren, Formularfelder vorausfüllen oder ausblenden, benutzerdefinierte Skripts ausführen, die Cloud-API aufrufen oder Workflows starten oder abbrechen. Eine Cloud-Richtlinie gibt Ihnen eine systemweite Kontrolle über Genehmigungen, Ressourcenvorgänge, Blaupausenvorgänge oder Katalogelementeinstellungen.

Vorbereitungen

- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

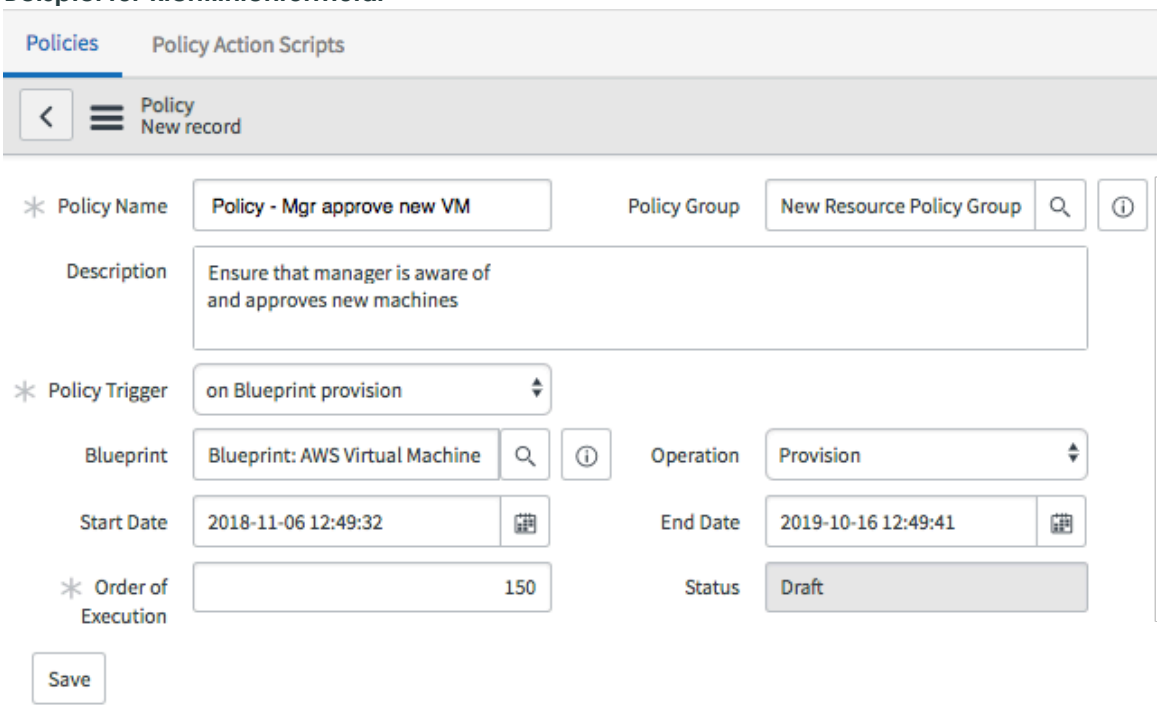
Dieses Verfahren beschreibt alle Richtlinientypen mit Ausnahme von Genehmigungsrichtlinien (*bei Genehmigung der Blaupausenbereitstellung*, *bei Genehmigung des Stapelvorgangs*, *bei Genehmigung des Stapelressourcenvorgangs* und *bei Aufgabenremediation*). Unter Cloud-Genehmigungsrichtlinie erstellen finden Sie Anweisungen zum Erstellen einer Richtlinie mit einem Genehmigungsauslöser.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

Beispiel für Richtlinienformular



Feld	Beschreibung
Richtlinienname	Ein beschreibender Name, der das Wort `Richtlinie` enthält. Beginnen Sie den Namen nicht mit einer Zahl.
Beschreibung	Eine Beschreibung der Absicht der Richtlinie
Richtliniengruppe	Eine Richtliniengruppe, zu der die Richtlinie gehört
Richtlinienauslöser	Auslöser, mit dem festgelegt wird, wann die Richtlinie angewendet werden soll. Zum Beispiel wendet der Auslöser **bei Leasingende** die Richtlinie an, wenn der Leasingvertrag für einen Stapel endet. Weitere Informationen finden Sie unter Auslöser für Cloud-Richtlinien.
Ressourcenblock [wird angezeigt, wenn der Auslöser *`bei Ressourcenvorgang`* ausgewählt ist]	Ressourcenblock, auf den die Richtlinie angewendet wird
Vorgang [wird angezeigt, wenn der Auslöser *`bei Blaupausenbereitstellung`*, *`bei Genehmigung der Blaupausenbereitstellung`*	Wählen Sie den Vorgang aus, für den die Richtlinie gilt. Beispielsweise kann eine Richtlinie nur für den Vorgang *`Bereitstellung aufheben`* oder für alle Vorgänge für die Blaupause oder das Katalogelement gelten.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
oder *bei Ressourcenvorgang* ausgewählt ist]	**Hinweis:** Wenn kein Vorgang angegeben ist, gilt die Richtlinie für alle Vorgänge. Diese Bedingung kann die Leistung beeinträchtigen. ◦ **Alle**: Beliebiger Vorgang wird ausgeführt. ◦ **Starten**: Die Ressource wird gestartet. ◦ **Stoppen**: Die Ressource wird gestoppt. ◦ **Bereitstellung**: Die Ressource wird bereitgestellt. ◦ **Bereitstellung aufheben**: Die Ressource ist für Benutzer nicht mehr verfügbar. ◦ **Skript ausführen**: Ein Skript wird mit der Ressource ausgeführt.
Moment [wird angezeigt, wenn der Auslöser *bei Ressourcenvorgang* ausgewählt ist]	Geben Sie an, wann die Richtlinie durchgesetzt werden soll: ◦ **Vor dem Vorgang**: Vor dem Start des angegebenen Vorgangs. ◦ **Nach dem Vorgang**: Nach Abschluss des angegebenen Vorgangs. **Hinweis:** Wenn Sie Infoblox integriert haben, verwenden Sie **Vor dem Vorgang** für einen virtuellen vSphere-Computer. Verwenden Sie **Nach dem Vorgang** für AWS- und Azure-Clouds, da AWS und Azure die Zuteilung von IP-Adressen steuern. Sie können die mit Infoblox bereitgestellte IP-Adresse registrieren.
Katalogelement [wird angezeigt, wenn ein Auslöser *beim Starten des Katalogelements*, *bei Beginn der Katalogelementanforderung* oder *bei Ende der Katalogelementanforderung* ausgewählt ist]	Wählen Sie das Katalogelement aus, für das die Richtlinie gilt.
Startdatum/Enddatum	Geben Sie das Startdatum an, ab dem die Richtlinie berücksichtigt werden soll, und das Enddatum, ab dem die Richtlinie nicht mehr berücksichtigt werden soll.
Reihenfolge der Ausführung	Geben Sie eine Zahl an, die die Reihenfolge darstellt, in der die Richtlinie angewendet wird. Eine Richtlinie mit einer niedrigeren Nummer wird vor einer Richtlinie mit einer höheren Nummer ausgeführt. Beispielsweise wird eine Richtlinie mit einer **Reihenfolge** von **100** vor einer Richtlinie mit einer **Reihenfolge** von **200** ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Die Eigenschaft **Reihenfolge der Ausführung** gilt nicht für *bei Blueprint-Bereitstellung (Genehmigung)*, *bei Stapelvorgang (Genehmigung)*, *bei Stapelressourcenvorgang (Genehmigung)* und *bei Aufgabenkorrektur* -Richtlinien. Weitere Detailinformationen finden Sie unter Cloud-Genehmigungsrichtlinie erstellen.
Status	◦ **Veröffentlichte** Richtlinien werden erzwungen. Sie können eine Richtlinie im Status **Veröffentlicht** nicht bearbeiten. Zum Bearbeiten einer Richtlinie im Status **Veröffentlicht** klicken Sie im Formularheader auf **Entwurf**. ◦ Sie können Richtlinien im Status **Entwurf** bearbeiten. Richtlinien im Status **Entwurf** werden nicht erzwungen. Zum Durchsetzen einer Richtlinie klicken Sie im Formularheader auf **Veröffentlichen**.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.

Nächste Maßnahme
Konfigurieren Sie eine Cloud-Richtlinienregel für die Richtlinie.

Cloud-Richtlinienregel konfigurieren

Eine Richtlinienregel ist eine Sammlung von Bedingungen und Aktionen. Wenn alle Bedingungen als „true“ ausgewertet werden, führt das Richtlinienmodul die Aktionen aus. Wird eine Bedingung als „false“ ausgewertet, führt das Richtlinienmodul die Aktionen nicht aus.

Vorbereitungen
Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

- Eine Richtlinie kann mehrere Regeln enthalten. Sie können die Reihenfolge konfigurieren, in der Regeln angewendet werden.
- Jede Regel wird vollständig ausgeführt.
- Jeder Regelfehler beendet die Ausführung. Ausnahme: Richtlinien, für die kein Vorgang angegeben ist.

Prozedur

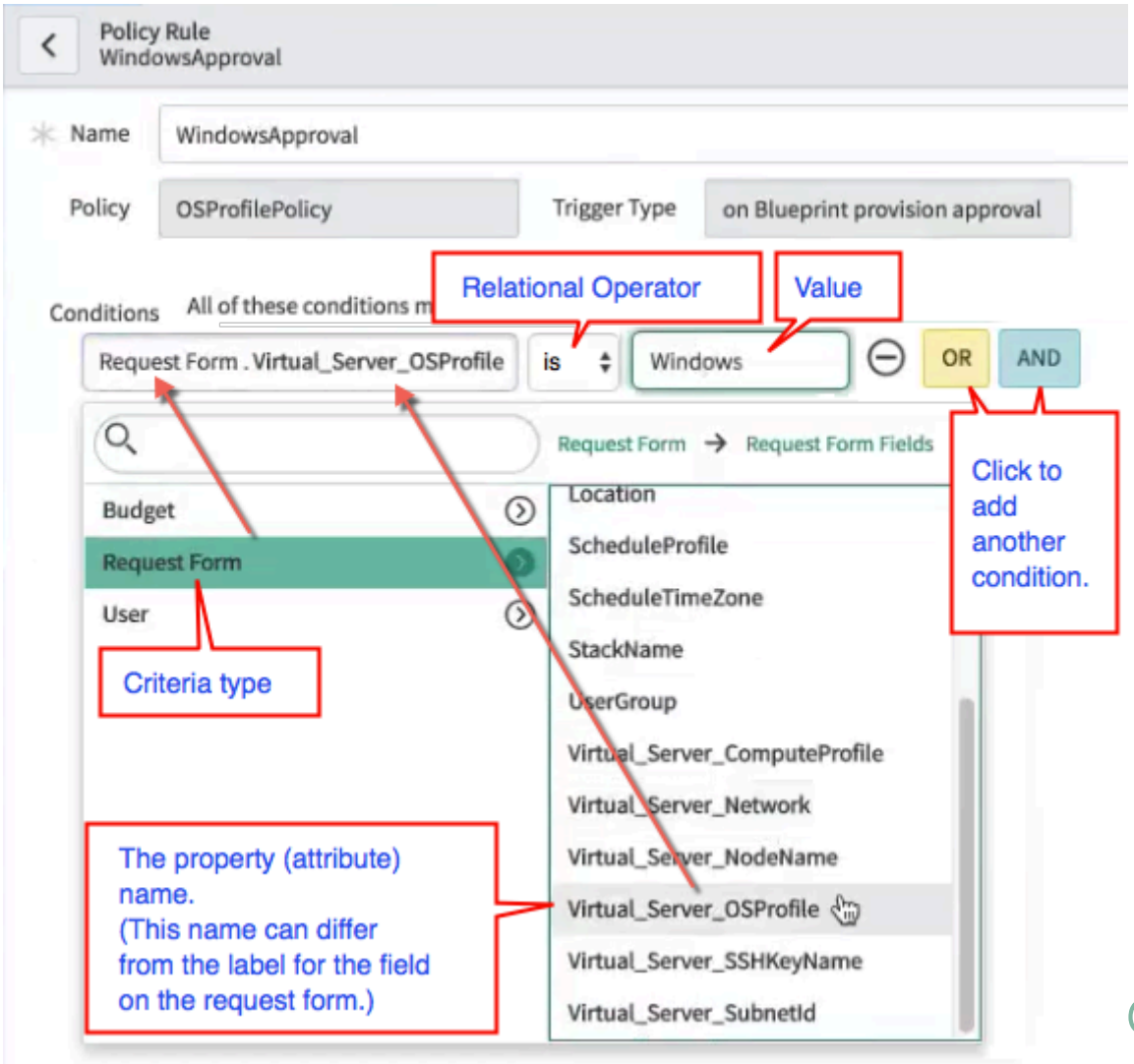
1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und versetzen Sie die Richtlinie bei Bedarf in den Status **Entwurf**.
3. Klicken Sie in der zugehörigen Liste „Regeln“ auf **Neu**, und geben Sie einen beschreibenden **Namen** für die Regel ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Der Regelname darf nicht mit dem Richtliniennamen identisch sein.
- Beginnen Sie den Regelnamen nicht mit einer Zahl.

4. Geben Sie mit dem Condition Builder im Basissystem die **Bedingungen** an, die erfüllt sein müssen, damit die Richtlinien-Engine die Aktionen ausführt.

   Die folgende Beispielregel wird auf eine Genehmigungsrichtlinie für eine Blaupausenbereitstellung angewendet. Die Bedingung ergibt „true“, wenn das Feld **BS-Profil** auf dem Anforderungsformular den Wert „Windows“ aufweist.



Automatische Übersetzung

Feld	Beschreibung
[Kriterientyp]	Wählen Sie eine der folgenden Optionen aus: ◦ **Anforderungsformular**: Basieren Sie die Bedingung auf einem Eigenschaftswert (Attributwert) im Anforderungsformular im Cloudbenutzerportal. Geben Sie an, welche Eigenschaft geprüft werden soll. Im Beispiel prüft die Bedingung, ob das Feld „BS-Profil“ auf dem Anforderungsformular den Wert „Windows“ aufweist. ◦ **Benutzer**: Basieren Sie die Bedingung auf einer Benutzerrolle oder auf der Gruppe, der der Benutzer angehört.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

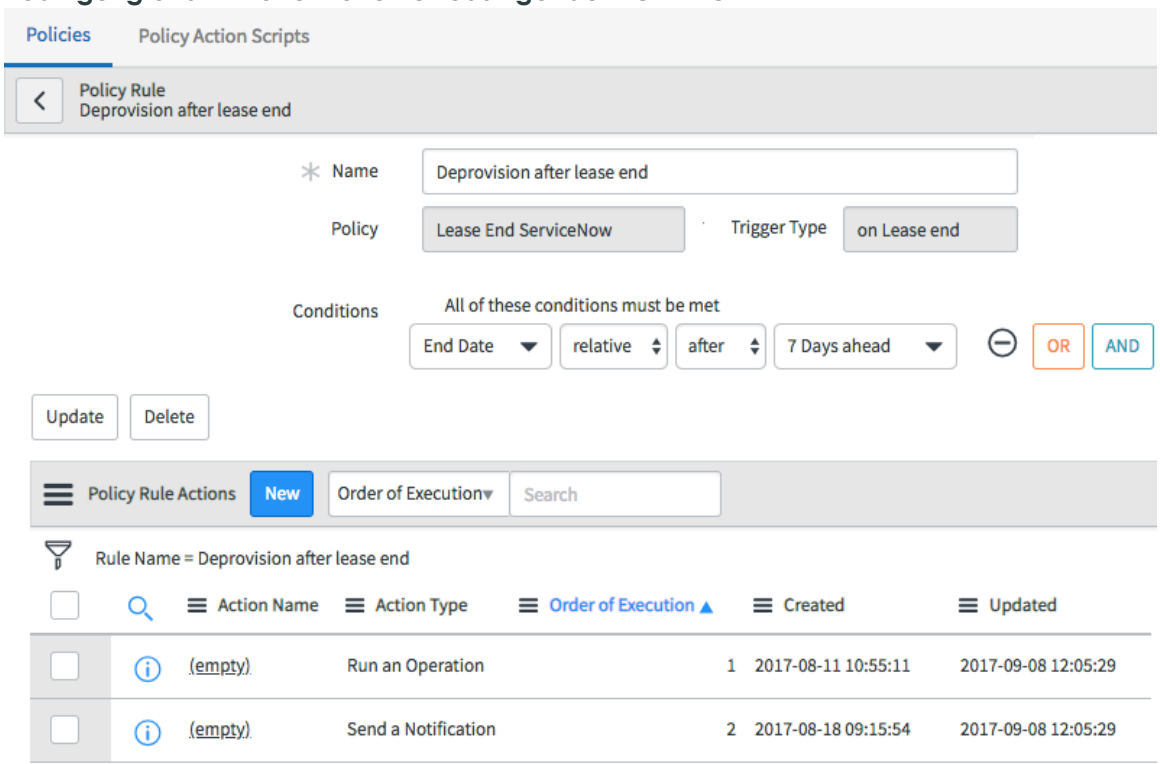
Feld	Beschreibung
	Wählen Sie beispielsweise Folgendes aus, um eine Bedingung zu erstellen, die zutrifft, wenn der Benutzer zur Gruppe „Marketing“ gehört: ▪ [Kriterientyp]: Benutzer ▪ [Benutzerentität]: Gruppe ▪ [Relationale Operatoren]: Entspricht ▪ [Gruppe]: Marketing **Hinweis:** Verwenden Sie verschiedene Kriterien, um eine Bedingung für Richtlinien zu erstellen, die vom Auslöser `bei Leasingende` ausgelöst werden. Sehen Sie sich das Beispiel unter dieser Tabelle an.
[Relationaler Operator]	Wählen Sie einen entsprechenden Operator aus.
[Wert]	Geben Sie je nach ausgewähltem [Kriterientyp] einen Wert ein oder wählen Sie einen aus. ◦ Geben Sie bei **Anforderungsformular** einen Wert für das Attribut ein. ◦ Für **Anwender** > **Gruppe**, wählen Sie eine Gruppe aus. ◦ Für **Anwender** > **Rolle**, wählen Sie eine Rolle aus.
[Logischer Operator]	Wenn Sie mehrere Bedingungen definieren, wählen Sie einen logischen Operator **ODER** oder **UND** aus, der die logische Beziehung zur nächsten Bedingung angibt.

5. Klicken Sie auf **Absenden**.

Example:
Verwenden Sie für Richtlinien, die durch den Auslöser `bei Leasingende` ausgelöst werden, den Datums-Bedingungsgenerator im Basissystem, um die zu prüfende Bedingung zu konfigurieren. Zusätzlich zur Bedingung zeigt das folgende Beispiel die Aktionen, die die Richtlinien-Engine durchführt, wenn die Bedingung erfüllt ist.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Bedingung und Aktionen für eine Leasingende-Richtlinie



Nächste Maßnahme

Erstellen Sie die Richtlinienaktionen, die ausgeführt werden sollen, wenn alle Bedingungen der Regel als „true“ ausgewertet werden.

Ausdrücke in Cloud Provisioning and Governance verwenden

Ausdrücke in Richtlinienaktionen können Werte festlegen oder überschreiben. Ausdrücke in Blaupausen können auf Attribute von Ressourcen zugreifen und Werte Anforderungsformularfeldern zuordnen. Ausdrücke sind in Ressourcenblöcken, Blaupausen, Richtlinien und überall sonst verfügbar, wo Cloud Provisioning and Governance Skripts zulässt.

Ausdrücke verwenden

Ausdrücke können die Werte für Informationen enthalten, die dynamisch im System generiert werden, z. B. die Werte für die Auswahlen, die Benutzer im Cloudbenutzerportal treffen. Ausdrücke sind in Ressourcenblöcken, Blaupausen, Richtlinien und überall sonst verfügbar, wo Cloud Provisioning and Governance Skripts zulässt.

Ausdrücke in Ressourcenblöcken verwenden

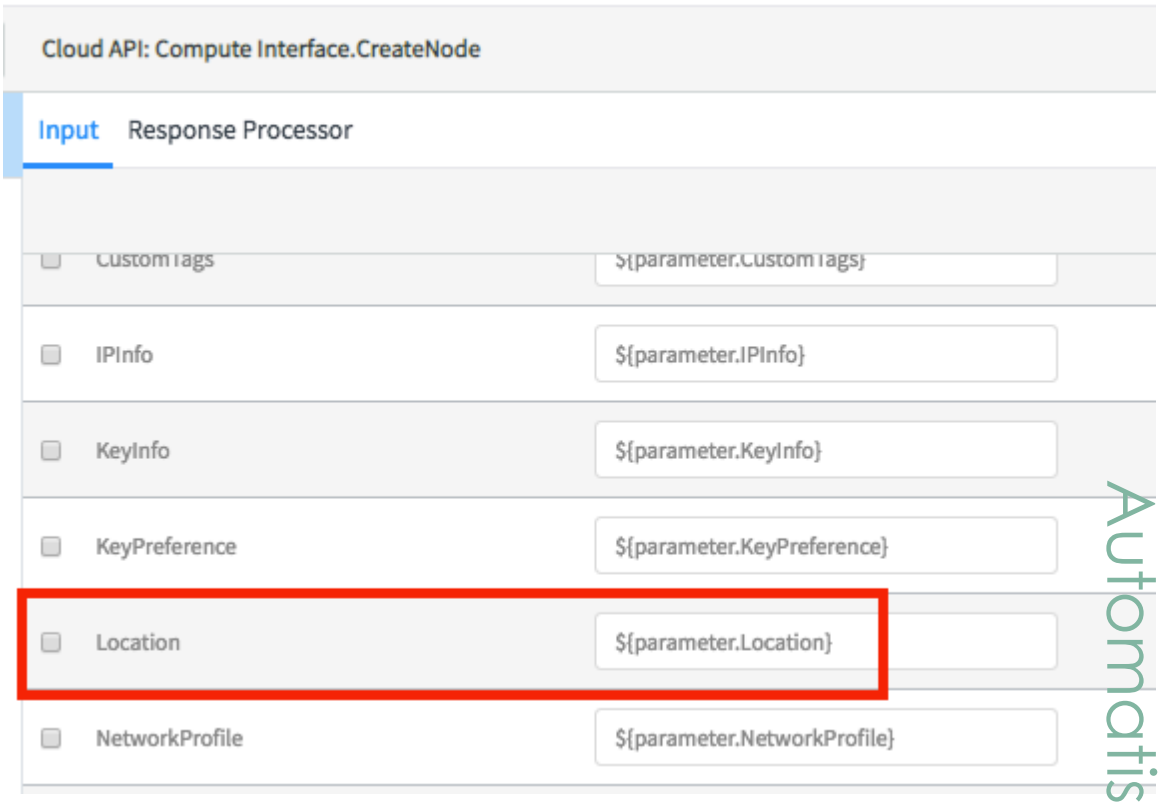
Jeder Ressourcenblockvorgang verwendet einen Ausdruck, der einen Wert für jeden Parameter enthält. Der Ausdruck kann hartcodierte Werte, Daten aus dem Stapel, den der Benutzer im Cloudbenutzerportal bereitstellt, Daten in der CMDB und Daten, die aus Skripts abgeleitet sind, verwenden. Standardmäßig generiert Cloud Provisioning and Governance eine Reihe von Parametern und ihren Ausdrücken für jeden Ressourcenblockvorgang.

Beispiel: Der Parameter *`Location`*, der das Rechenzentrum enthält, zu dem eine Ressource gehört, verwendet den Ausdruck `${parameter.Location}`.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ausdrücke in einem Ressourcenblock



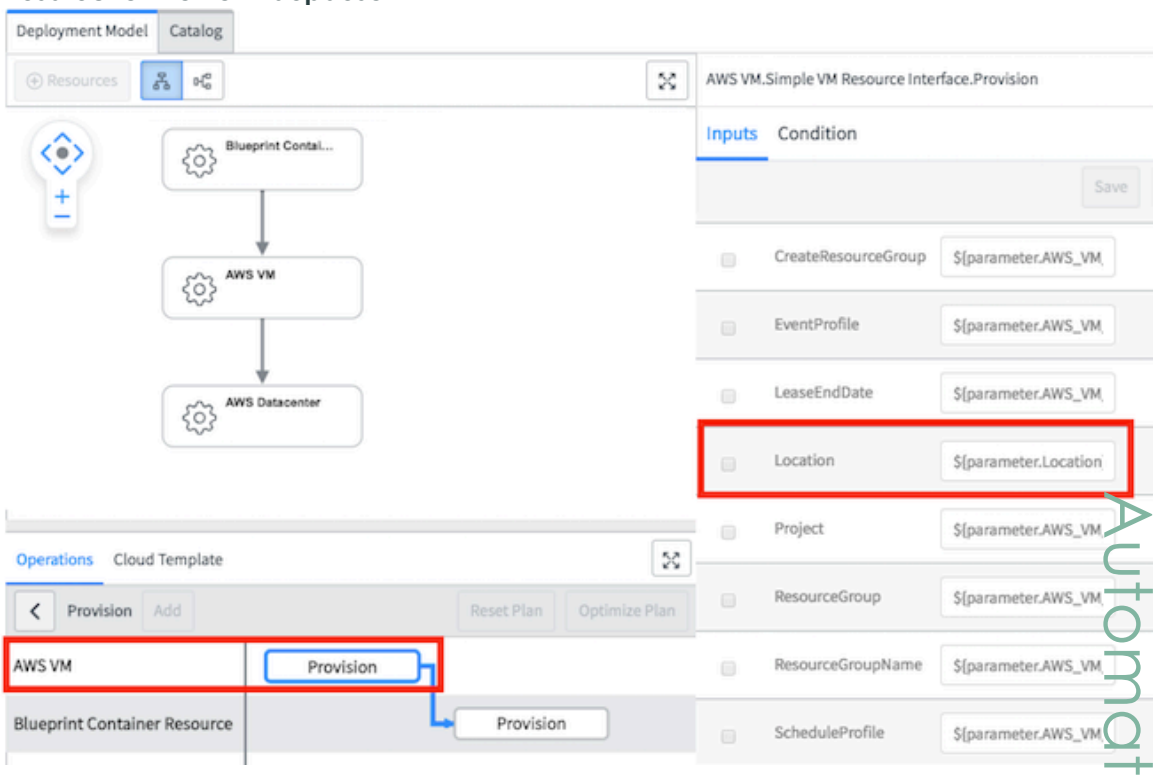
Ausdrücke in Blaupausen verwenden

Blaupausen können Ausdrücke verwenden, um Eingabeparameter für jeden Vorgang in einem Ressourcenblock zuzuordnen. Standardmäßig zeigt die Blaupause die gleichen Parameter und Werte an, die im Ressourcenblock angegeben sind.

Sie können auf Blaupausenattribute mit Ausdrücken zugreifen. Der Ausdruck in der Spalte **Zuordnung** definiert Blaupausenattribute für jeden Vorgang in einem Schritt. Beispielsweise kann auf das Attribut **Standort**, das auf dem Stack-Anforderungsformular angezeigt wird, über den Ausdruck `${parameter.Location}` zugegriffen werden. Der Standortparameter mit dem Wert `${parameter.Location}` wird auf der Registerkarte **Eingaben** angezeigt, wenn Sie einen Blaupausenvorgang auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

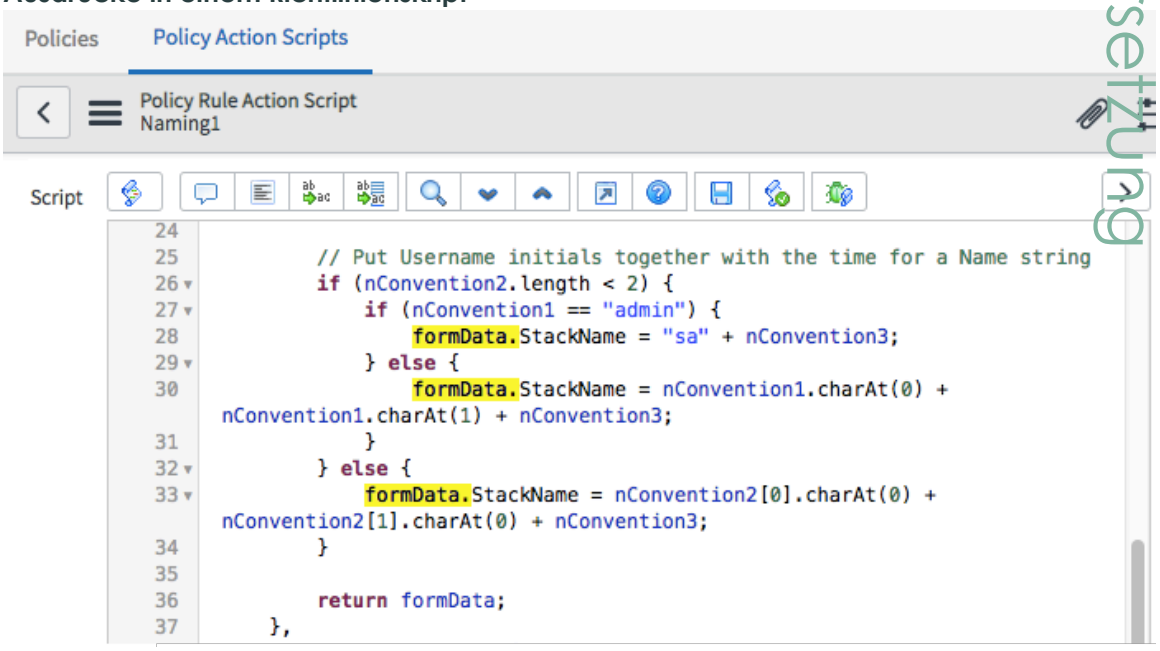
Ausdrücke in einer Blaupause



Ausdrücke in Richtlinienaktionen verwenden

Richtlinienaktionen können Ausdrücke verwenden, um Parameterwerte zu überschreiben, die Benutzer in einem Anforderungsformular im Cloudbenutzerportal übermitteln. Sie können auch in Stack-Vorgängen auf Benutzerdaten zugreifen und diese überschreiben. Verwenden Sie beispielsweise den folgenden Ausdruck, um einen Stapel umzubenennen: `formData.Stackname = "Ihre-Namenskonvention";`.

Ausdrücke in einem Richtlinienskript



Sie können auf Blaupausenattribute mit Ausdrücken zugreifen. Der Ausdruck in der Spalte **Zuordnung** definiert Blaupausenattribute für jeden Vorgang in einem Schritt. Beispielsweise

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

kann auf das Attribut **Standort**, das auf dem Anforderungsformular für einen virtuellen Computer angezeigt wird, über den Ausdruck `${parameter.Location}` zugegriffen werden.

Ausdruckstypen

Definitionsausdrücke

Definitionsausdrücke sind eine Form der frühen Bindung (oder statischen Bindung). Diese Bindungen beziehen sich auf die Bindung zur Kompilierungszeit und werden ausgewertet, wenn der Benutzer das Stapelanforderungsformular übermittelt (wenn die Stapel- oder Ressourcenbereitstellung beginnt). Definitionsausdrücke haben keinen Zugriff auf die Daten, die während Orchestration generiert werden. Definitionsausdrücke werden in geschweifte Klammern eingeschlossen. Beispiel: `${parameter.CloudAccount}`

Laufzeitausdrücke

Laufzeitausdrücke sind eine Form der späten Bindung (oder dynamischen Bindung). Diese Bindungen beziehen sich auf die Bindung zur Laufzeit und haben Zugriff auf die Daten, die während Orchestration erstellt werden (z. B. Stapelelemente). Laufzeitausdrücke werden ausgewertet, wenn sie während einer Ausführung von Orchestration aufgerufen werden. Laufzeitausdrücke werden normalerweise für Dot-Walking mit Daten in Tabellen verwendet. Laufzeitausdrücke sind in Klammern eingeschlossen. Beispiel: `$(Stack.items[VM1].attributes[node_id])`

Definitions-/Laufzeitausdrücke

Einige Ausdrücke enthalten sowohl Definitions- als auch Laufzeitausdrücke.

Komplexe Ausdrücke

Sie können Ausdrücke beliebigen Typs in anderen Ausdrücken verschachteln.

Syntax und Beispiele für Definitionsausdrücke

Die zulässige Syntax verwendet ein Dollarzeichen und geschweifte Klammern. Diese Typen sind verfügbar:

- `${parameter.}`. Verwenden Sie diese Art von Ausdruck, um Werte aus Eingabeattributen von Prozessen wie der Bereitstellung von Blaupausen abzurufen. Daten werden nicht aus Tabellen abgerufen.
- `${Stack.items[]}`. Verwenden Sie diese Syntax für den Zugriff auf Attribute bestimmter Elemente in einem Stapel.
- `${randomNumber}`. Verwenden Sie diese Syntax, um eine Zufallszahl zu generieren. Beispielsweise können Sie eine VM mit einem zufälligen Knotennamen oder Stapelnamen bereitstellen.

Beispiele für Definitionsausdrücke

Beispiel	Beschreibung
${parameter.BillingCode}	Dieser Ausdruck zeigt, wie ein Abrechnungscode-Parameter in einer Blaupause angezeigt wird.
${parameter.formData.CatalogAttributeType}	Dieser Ausdruck verwendet ein Katalogattribut, das von einem Benutzer übermittelt wird, während der Benutzer

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für Definitionsausdrücke (Fortsetzung)

Beispiel	Beschreibung
	das Formular für ein Katalogelement im Cloudbenutzerportal ausfüllt.
${parameter.userData.userId}	Dieser Ausdruck verwendet die ID eines Benutzers, während der Benutzer das Formular für ein Katalogelement im Cloudbenutzerportal ausfüllt.
${Stack.items[Virtueller Server].attributes[sys_id]}	Dieser Ausdruck ruft die sys_id eines virtuellen Servers ab, der Teil eines Stapels ist. „Virtueller Server“ ist der Alias eines Ressourcenblocks, der im Stapel verwendet wird.

Syntax und Beispiele für Laufzeitausdrücke

Die zulässige Syntax verwendet ein Dollarzeichen und Klammern. Diese Typen sind verfügbar:

- `$(ci.tablename)`, wobei `tablename` eine Tabelle im System ist, normalerweise eine CI-Tabelle in der CMDB. Verwenden Sie diese Syntax, um auf Werte von Feldern in der Tabelle zuzugreifen.
- `$(Stack.items[])`. Verwenden Sie diese Syntax für den Zugriff auf Attribute bestimmter Elemente in einem Stapel.

Beispiele für Laufzeitausdrücke

Beispiel	Beschreibung
`$(ci.cmdb_ci_cloud_subnet[ sys_id=12231231231231231231].cidr)`	Dieser Ausdruck führt ein Dot-Walking mit der Tabelle „Cloud-Subnetz“ durch, sucht den spezifischen Datensatz mit der angegebenen sys_id und übernimmt den Wert aus der Spalte `cidr`.
`$(ci.sn_cmp _ip_pool[subnet=${parameter.formData.Subnet Id}])`	Dieser Ausdruck kombiniert Ausdrücke der Typen Laufzeit und Definition. Das Gleichheitszeichen „=“ wird verwendet, um einen Wert für eine Übereinstimmung auszuwerten. Der Ausdruck führt ein Dot-Walking für die Tabelle „IP-Pool“ durch und sucht nach dem Subnetz mit der Subnetz-ID, die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiele für Laufzeitausdrücke (Fortsetzung)

Beispiel	Beschreibung
	der Benutzer übermittelt hat.
`$(ci.cmdb_ci_cloud_subnet[${parameter.formData.SubnetId}].cidr)`	Dieser Ausdruck kombiniert Ausdrücke der Typen Laufzeit und Definition. Der Ausdruck übernimmt den Wert des Felds **cidr** aus einem Subnetz, das der Benutzer bei der Bereitstellung ausgewählt hat. Die eckigen Klammern `[]` geben an, dass der Ausdruck die Tabelle „Cloud-Subnetz" per Dot-Walking auswertet und dann den Wert für „Subnetz" betrachtet, den der Benutzer für eine Blaupausenbereitstellung übermittelt hat. Der Ausdruck erfasst den Wert des Felds **cidr** und geht dann zu dem Wert im Feld **cidr** der sys_id des Subnetzes.
$(Stack.items[Virtueller Server].attributes[sys_id])	Wie auch im Beispiel zum Definitionsausdruck ruft dieser Ausdruck die sys_id eines virtuellen Servers ab, der Teil eines Stapels ist.

Beispielausdruck

```
$(ci.cmdb_ci_nic[$(Script:CMPVMNICs.getNICs[arg=$(Stack.items[Virtueller Server].attributes[sys_id])])].private_ip)
```

- *$(ci*: Laufzeitausdruck zum Abrufen von Daten aus der Tabelle.
- *cmdb_ci_nic*: CI für Netzwerkschnittstellenkarte (NIC).
- *$(Script*: Skriptbasierter Ausdruck.
- *CMPVMNICs*: Skripteinbindung.
- *getNICs*: Funktion in einer Skripteinbindung.
- *arg*: Argumente für die Funktion in der Skripteinbindung. Argumente werden durch Komma (,) getrennt, wenn mehrere Attribute vorhanden sind.
- *$(Stack.items*: Laufzeit-Stapelausdruck zum Abrufen eines Stapelelements aus einem Stapel. Argument ist der in der Blaupause angegebene Alias.
- *Virtual Server*: Alias der in der Blaupause verwendeten Ressource.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- *`$(Stack.items[Virtual Server].attributes[sys_id])`*: Ruft die sys_id der Ressourceninstanz des Stapelelements („Virtueller Server“) in einem Stapel ab.
- *`private_ip`*: Attribut von cmdb_ci_nic. Bei Bedarf durch öffentliche IP-Adresse ersetzen.

Ausdrücke

`Simple parameter mapping expression`

Dieser Ausdruckstyp ruft Werte aus Eingabeattributen von Prozessen ab, z. B. Blaupausenvorgängen, Ressourcenblöcken und Richtlinien. Daten werden nicht aus Tabellen abgerufen. Er ordnet Werte einer Ebene einer anderen zu, z. B. von einer Blaupause zu einer Ressource zur Cloud API.

- Typ: Definition
- Syntax: `${parameter.}`
- Beispiele:
  - `${parameter.BillingCode}` gibt den Abrechnungscode zurück.
  - `${parameter.formData.CatalogAttributeType}` akzeptiert ein Katalogattribut, das auf dem Anforderungsformular im Cloudbenutzerportal übermittelt wird.
  - `${parameter.userData.userId}` verwendet die ID eines Benutzers, der das Anforderungsformular im Cloudbenutzerportal bearbeitet.

`Stack item expression`

Jedes Stapelelement wird durch eine CI-Instanz in der CMDB dargestellt. Verwenden Sie Stapelelementausdrücke, um Eigenschaften der ersten Ebene im CI oder im Stapelelement selbst zu suchen, die das Stapelelement unterstützen.

- Typ: Definition/Laufzeit
- Syntax: `${Stack.items[]}` oder `$(Stack.items[])`
- Beispiele:

  `${Stack.items[VirtualServer1].attributes[sys_id]}` ist ein Ausdruck vom Typ Definition, der die sys_id eines virtuellen Servers in einem Stapel abruft. `VirtualServer1` ist der Alias eines Ressourcenblocks, der im Stapel verwendet wird.

  `$(Stack.items[VirtualServer2].attributes[sys_id])` ist ein Ausdruck vom Typ Laufzeit, der die sys_id eines virtuellen Servers in einem Stapel abruft.

  `${Stack.items[vm1].attributes[node_id]}` liest das Attribut `node_id` des CI, das für die VM erstellt wurde. `vm1` ist der Name des Stapelelements (oder der Alias der Ressource in der Blaupause).

  `$(Stack.items[vm1].status)` liest den Status des Stapelelements.

`Property override expressions in policies`

In Richtlinien können Sie Eigenschaften überschreiben, indem Sie einen Wert aus dem System abrufen oder eine Zufallszahl verwenden. Sie können Daten sowohl aus den

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularen im Cloudbenutzerportal als auch von dem Benutzer verwenden, der den Vorgang auf dem Formular ausgeführt hat.

- Typ: Definition/Laufzeit
- Syntax: `${parameter.formData.xyz}` oder `${this.parameter.userData.xyz}`
- Beispiele:

  Der folgende Wert kann den Stapelnamen auf *Stack_Bob.Smith@company.com* festlegen: `Stack_${parameter.userData.userId}`

  Legen Sie Stapel- oder Tabellenwerte mithilfe von Laufzeitausdrücken fest, indem Sie das Subnetz aus der Tabelle „IP-Pool“ verwenden:

  ```
  $(ci.sn_cmp _ip_pool[subnet=${parameter.formData.Subnet Id}])
  ```

  In Skripts können Sie Werte wie folgt zuweisen:

  ```
  formData.App_Server_NodeName = "MyNodeName";
  ```

  ```
  this.parameter.userData.userId == 'servicenowuserId';
  ```

- Siehe auch Richtlinienaktionsskript erstellen.

Script expression

Im Beispiel ist `VMProperties` eine Skripteinbindung mit einer Funktion namens `getIP`. Ein Skriptausdruck ist auch ein Beispiel für einen komplexen Ausdruck (der Ausdruck ist verschachtelt).

- Typ: Laufzeit
- Syntax: `$(Script:scriptName.function[])`
- Beispiele:

  ```
  $(Script:VMPropertiesUtil.getIP[ arg=
  $(Stack.items[VM1].attributes[object_id])])
  ```

  Ausdruck für private IP:`$(ci.cmdb_ci_nic[$(Script:CMPVMNICs.getNICs[arg=`
  `$(Stack.items[Virtual Server].attributes[sys_id])])].private_ip)`

  Ausdruck für öffentliche IP: `$(ci.cmdb_ci_nic[$(Script:CMPVMNICs.getNICs[arg=`
  `$(Stack.items[Virtual Server].attributes[sys_id])])].public_ip)`

  Ausdruck zum Abrufen des Anmeldeinformationsalias:
  `$(Script:CMPVMUtils.getCredentialAlias[arg=${Stack.items[Virtual Server].attributes[sys_id]}])`

  Ausdruck zum Abrufen der IP-Adresse: `$(Script:CMPVMUtils.getReachableIp[arg=`
  `$(Stack.items[Virtual Server].attributes[sys_id])])`

CI lookup expression

Greift auf Werte von Feldern in einer Tabelle zu, normalerweise eine CI-Tabelle in der CMDB.

- Typ: Definition/Laufzeit
- Syntax: `$(ci.tableName)`

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Beispiele:

  `$(ci.sn_cmp _ip_pool[subnet=${parameter.formData.Subnet Id}])` kombiniert Laufzeit- und Definitionsausdrücke. Der Operator „=“ wertet einen Wert für eine Übereinstimmung aus. Der Ausdruck führt ein Dot-Walking für die Tabelle „IP-Pool“ durch und sucht nach dem Subnetz mit der Subnetz-ID, die der Benutzer übermittelt hat.

  `$(ci.cmdb_ci_cloud_subnet[${parameter.formData.SubnetId}].cidr)` ruft den Wert des Felds `cidr` aus einem Subnetz ab, das der Benutzer während der Bereitstellung angegeben hat. Der Ausdruck führt ein Dot-Walking für die Tabelle „Cloud-Subnetz“ durch, betrachtet den Subnetzwert, den der Benutzer in einer Blaupausenbereitstellung angegeben hat, extrahiert den Wert des Felds `cidr` und geht dann zum Wert im Feld `cidr` der sys_id des Subnetzes.

Random number expression

Generiert eine Zufallszahl. Beispielsweise können Sie eine VM mit einem zufälligen Knotennamen oder Stapelnamen bereitstellen.

- Typ: Laufzeit
- Syntax und Beispiel: `${randomNumber}`

Scratchpad expression/Resource operation output attribute expression

Liest Ausgabeattribute aus einem Vorgang in einen anderen Vorgang.

- Typ: Laufzeit
- Syntax: variiert
- Beispiel: Ausgaben für einen Vorgang festlegen/verfügbar machen:

  `${Compute Interface.CreateNode.Output.resp.nodeId}`

  So lesen Sie die Ausgabeattribute (wobei `VM1.Provision` der Vorgang ist, dessen Ausgabeattribute gelesen werden):

  `$(Outputs[VM1.Provision].NodeId)`

Conditions in expressions

Sie können bedingte Ausdrücke in Blaupausenschritten und Ressourcenvorgangsschritten verwenden, um den Schritt bedingt auszuführen oder zu überspringen. Die bedingten Ausdrücke sind Javascript-Ausdrücke und unterstützen das Ersetzen von Ausdrücken.

- Typ: Definition/Laufzeit
- Syntax: variiert
- Beispiele:

  ‘${parameter.CloudAccount}’==’Amazon Cloud Account’

  ‘$(Stack.items[vm1].attributes[node_id]) ’== ’VM1’

Complex expression

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können Ausdrücke schachteln. Im Beispiel ordnet `${parameter.ServerID}` die sys_id des CI zu und wird ersetzt, bevor der äußere Ausdruck angewendet wird.

- Typ: beliebig
- Syntax: variiert
- Beispiel: `$(ci.cmdb_ci_vm_instance[${parameter.ServerID}].name)`

Order context

Dieser Ausdruck ist für Lebenszyklusvorgänge nützlich und ermöglicht Ihnen das Dot-Walking für die Bestellattribute als Teil der Tabelle *sn_cmp_order*.

- Typ: Laufzeit
- Syntax: `$(context.order.column_name)`
- Beispiele:
  - Anforderungselement: `$(context.order.sc_req_item)`
  - Dot-Walking für Anforderungselementobjekt: `$(context.order.sc_req_item.number)`
  - Gemischter Ausdruck (Konstante + Ausdruck): `"ram $(context.order.sc_req_item.number)"`

Aktion für eine Richtlinie „bei Blaupausenbereitstellung“ erstellen

Der Auslöser *bei Blaupausenbereitstellung* wird nach der Ausführung der Richtlinien *bei Beginn der Katalogelementanforderung* ausgelöst. Durch eine Richtlinie, die durch den Auslöser *bei Blaupausenbereitstellung* ausgelöst wird, kann ein Skript ausgeführt, ein vom Benutzer angeforderter Attributwert außer Kraft gesetzt oder ein Bereitstellungsvorgang abgebrochen und eine entsprechende Nachricht gesendet werden.

Vorbereitungen

Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.

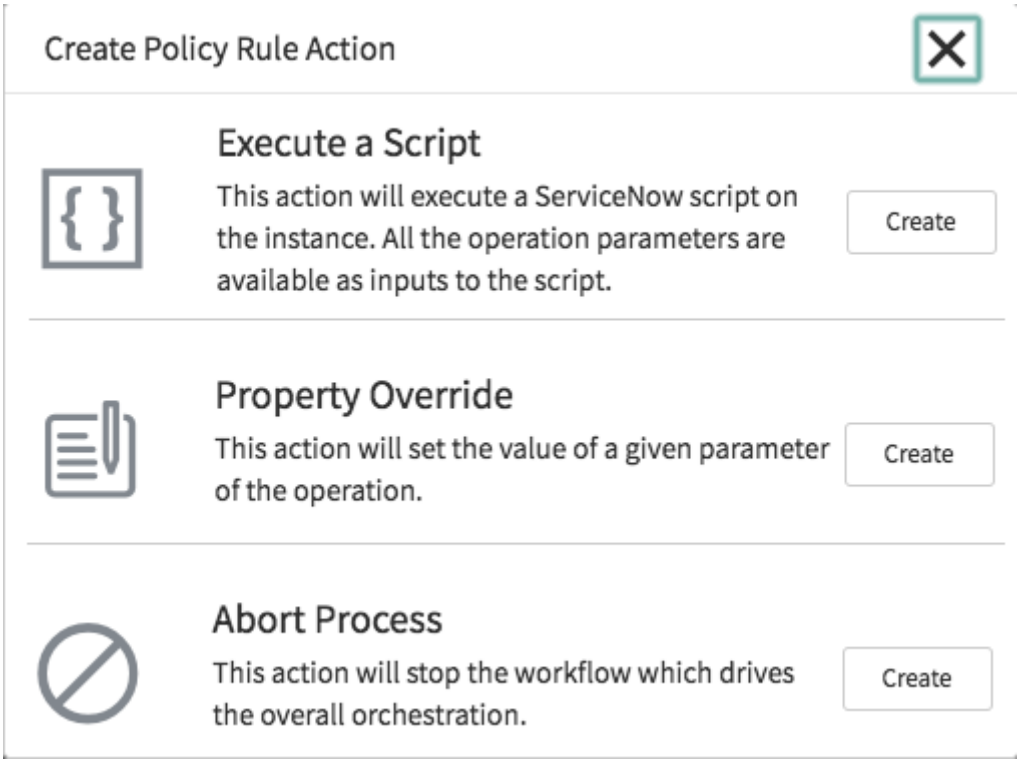
Cloud-Richtlinienregel konfigurieren

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und versetzen Sie die Richtlinie bei Bedarf in den Status **Entwurf**.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



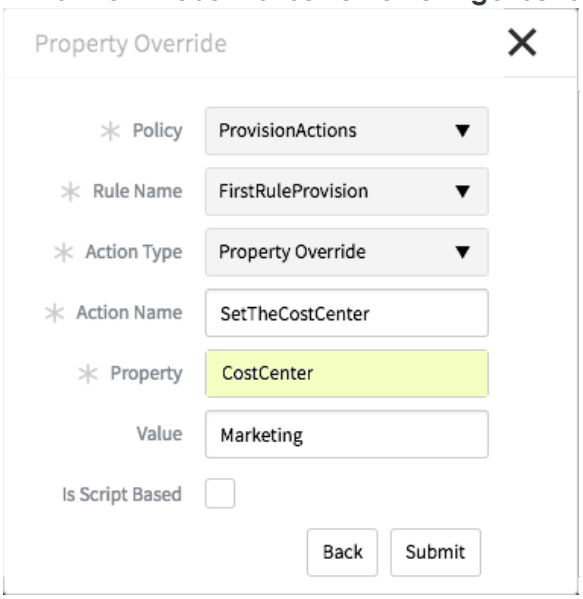
Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

Einstellungen für die Aktion „Eigenschaft außer Kraft setzen“

Feld	Beschreibung
Eigenschaft	Geben Sie den Namen der Eigenschaft (des Attributs), die/das außer Kraft gesetzt werden soll, auf dem Benutzeranfrageformular an.
Wert	Geben Sie einen Wert ein, der den Wert im Feld **Eigenschaften** außer Kraft setzt. Sie können nur Textwerte überschreiben. Sie können einen statischen Wert, einen Ausdruck oder beides angeben. In der Beispielaktion mit dem Namen **SetTheCostCenter** (Kostenstelle festlegen) wird der Wert **Marketing** für die Eigenschaft **CostCenter** (Kostenstelle) angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Aktion zum Außerkraftsetzen einer Eigenschaft konfigurieren  **Hinweis:** Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Folgende Aktionen können mithilfe von Ausdrücken ausgeführt werden (weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden): ◦ Legen Sie Formulardatenwerte mithilfe von Definitionsausdrücken fest. Zum Beispiel: `${parameter.formData.CatalogAttributeType}` ◦ Weisen Sie Benutzerdatenwerte mithilfe von Definitionsausdrücken zu. Beispiel: `${parameter.userData.userId}` Beispielsweise kann mit dem folgenden Wert der Stapelname auf **Stack_Bob.Smith@company.com** gesetzt werden: `Stack_ ${parameter.userData.userId}` ◦ Legen Sie Stapel- oder Tabellenwerte mithilfe von Laufzeitausdrücken fest. Beispiel: `$(ci.sn_cmp_ip_pool[subnet= ${parameter.formData.Subnet Id}])` entnimmt das Subnetz aus der Tabelle „IP-Pools“. ◦ Ordnen Sie einem Feld mithilfe statischer Ausdrücke eine Zufallszahl zu. Verwenden Sie: `${randomNumber}`
Ist skriptbasiert	Aktivieren Sie das Kontrollkästchen, um das Textfeld **Skript** anzuzeigen, und geben Sie dann das Skript an. Sie können den folgenden Beispielskriptausschnitt verwenden, um einen Stapelnamen außer Kraft zu setzen. Mit dem Abschnitt `function (formData)` des Skripts werden die Werte für Felder im Formular geändert. In diesem Beispiel heißt der Stapel `MyStack` (MeinStapel).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	`customScript : function(formData){ // Manipulation of form parameter is only supported here. // Change in any other attributes will be ignored // data available for manipulation are // Form Data - Ex. StackName can be accessed // through formData.StackName // formData.StackName = "MyStack"; // User Data - Ex. User Id can be accessed // through this.parameters.userData // if(this.parameter.userData.userId == 'servicenowuserId') formData.StackName = "MyStack"; return formData; },`

Einstellung für die Aktion „Prozess abbrechen“

Feld	Beschreibung
Nachricht	Geben Sie die Nachricht ein, die der anfordernden Person bei Abbruch des Prozesses angezeigt werden soll.

Aktion für eine Genehmigungsrichtlinie erstellen

Eine Richtlinie, die von einem der Genehmigungsauslöser ausgelöst wird, kann Genehmigungs-Workflows starten. Die Genehmigungsauslöser sind (*bei Blueprint-Bereitstellung (Genehmigung)*, *bei Stapelvorgang (Genehmigung)*, *bei Stapelressourcenvorgang (Genehmigung)*und *bei Aufgabenkorrektur*.

Vorbereitungen

Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.

Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

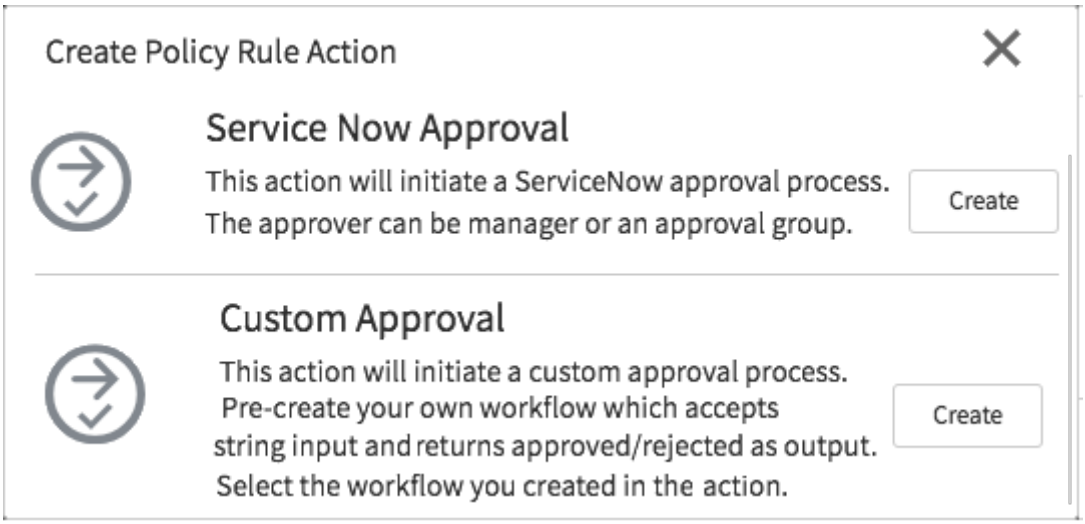
Wenn mehrere „Genehmigungsrichtlinien“ gelten, werden die Richtlinien in der folgenden Reihenfolge angewendet. (Die Genehmigungsrichtlinien sind *bei Blueprint-Bereitstellung (Genehmigung)*, *bei Stapelvorgang (Genehmigung)*, *bei Stapelressourcenvorgang (Genehmigung)*und *bei Aufgabenkorrektur*):

1. Nur die erste erfolgreiche Genehmigungsrichtlinie wird angewendet. Es werden keine weiteren Genehmigungsrichtlinien angewendet.
2. Wenn die angewendete Genehmigungsrichtlinie mehrere Regeln aufweist, wird nur die erste erfolgreiche Regel verwendet.
3. Wenn eine Regel über mehrere Aktionen verfügt, wird nur die erste erfolgreiche Aktion ausgeführt.
4. Wenn die angewendete Genehmigungsrichtlinie sowohl eine benutzerdefinierte Genehmigung als auch eine ServiceNow-Genehmigung enthält, wird nur der benutzerdefinierte Genehmigungsprozess ausgeführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und versetzen Sie die Richtlinie bei Bedarf in den Status **Entwurf**.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben.



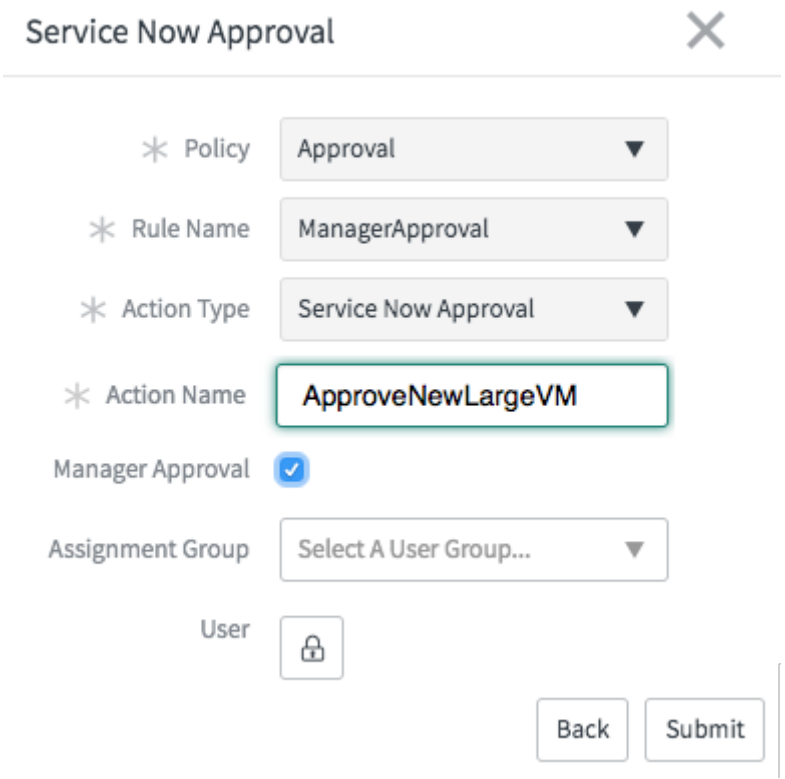
5. Wählen Sie eine der folgenden Aktionen aus.
   - **Benutzerdefinierte Genehmigung** führt den von Ihnen angegebenen Workflow aus. Der Workflow muss den Wert **Genehmigt** zurückgeben, um den Vorgang abzuschließen. Überwachen Sie **die ServiceNow-Genehmigung** für den Anwendungsfall.
   - **Service Now-Genehmigung** unterstützt unterschiedliche Genehmiger basierend auf dem Auslöser für die Richtlinie:

Auslöser	Workflow	Verfügbare Genehmiger
on Blueprint provision (approval) (bei Blaupausenbereitstellung (Genehmigung))	Cloud-Genehmigungsworkflow	▪ Managergenehmigung ▪ Zuweisungsgruppe ▪ Benutzer (Sperre)
bei Genehmigung des Stapelvorgangs	Workflow für Change-Anforderung für Cloud-Vorgang	Zuweisungsgruppe
on Stack resource operation (approval) (bei Stapel-Ressourcenvorgang (Genehmigung))	Workflow für Change-Anforderung für Cloud-Vorgang	Zuweisungsgruppe

6. Geben Sie im Genehmigungsformular einen eindeutigen und aussagekräftigen **Aktionsnamen** an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion in der Regel



7. Wenn Sie **Anwenderdefinierte Genehmigung**auswählen, geben Sie den Workflow an, und klicken Sie dann auf **Absenden.** Wenn Sie **ServiceNow-Genehmigung**auswählen, geben Sie an, wer die Cloud-Aktivität genehmigen soll.

Genehmigungsfelder

Feld	Beschreibung
Managergenehmigung	Eine oder alle der folgenden Optionen: ◦ Aktivieren Sie das Kontrollkästchen **Managergenehmigung**, um festzulegen, dass der Manager des Genehmigers die Anforderung ebenfalls genehmigen muss. Der standardmäßige Genehmigungs-Workflow geht zuerst an den Manager, dann an die Gruppe und schließlich an den Benutzer. ◦ Wählen Sie eine Benutzergruppe aus der Liste **Zuweisungsgruppe** aus. ◦ Deaktivieren Sie die **Benutzer**-Sperre, wählen Sie einen Benutzer aus der Liste aus, und aktivieren Sie die Sperre anschließend wieder.
Zuweisungsgruppe	Wählen Sie die Zuweisungsgruppe zur Genehmigung der Anforderung aus. Jeder Benutzer in der Gruppe kann die Aktion mit dem Standard-Workflow genehmigen. Die Genehmigung wird dann an die im Feld **Benutzer** angegeben Benutzer gesendet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Hinweis: Benutzer in einer Zuweisungsgruppe, die nicht über die Rolle „ITIL“ verfügen, erhalten standardmäßig immer noch einen Genehmigungsdatensatz und eine Benachrichtigung. Sie können die Genehmigung jedoch nicht erteilen. Weisen Sie die Rolle „ITIL“ allen Benutzern oder Benutzergruppen zu, die Vorgänge und Bereitstellungen genehmigen müssen.
Anwender	Wählen Sie mindestens einen Benutzer aus, für den die Genehmigungsaktion gilt. Alle ausgewählten Benutzer müssen die Aktion mit dem Standard-Workflow genehmigen.

Aktion für eine Richtlinie „beim Starten des Katalogelements“ erstellen

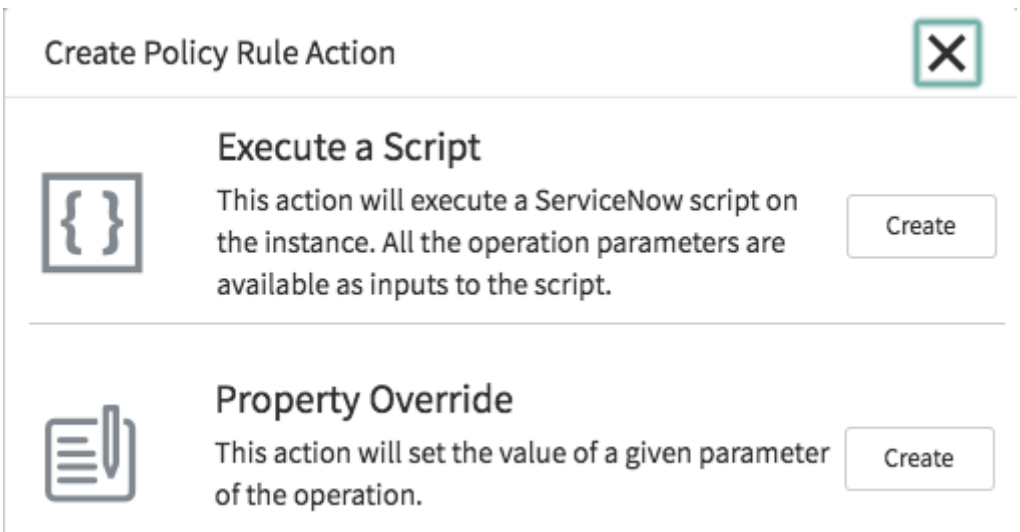
Der Auslöser *beim Starten des Katalogelements* wird ausgelöst, wenn ein Bestellformular (Stapelanforderungsformular) für ein Katalogelement gestartet wird. Eine Richtlinie, die durch den Auslöser *beim Starten des Katalogelements* ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Wert überschreiben (nur Textwerte).

Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und versetzen Sie die Richtlinie bei Bedarf in den Status **Entwurf**.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.

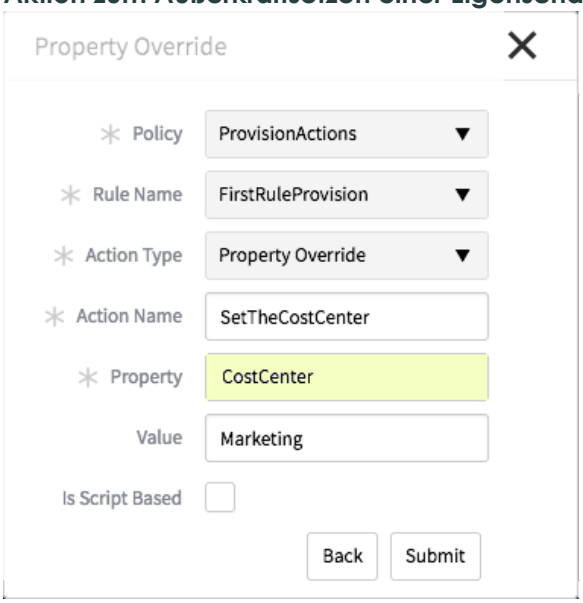


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

Einstellungen für die Aktion „Eigenschaft außer Kraft setzen“

Feld	Beschreibung
Eigenschaft	Geben Sie den Namen der Eigenschaft (des Attributs), die/das außer Kraft gesetzt werden soll, auf dem Benutzeranfrageformular an.
Wert	Geben Sie einen Wert ein, der den Wert im Feld **Eigenschaften** außer Kraft setzt. Sie können nur Textwerte überschreiben. Sie können einen statischen Wert, einen Ausdruck oder beides angeben. In der Beispielaktion mit dem Namen **SetTheCostCenter** (Kostenstelle festlegen) wird der Wert **Marketing** für die Eigenschaft **CostCenter** (Kostenstelle) angegeben. **Aktion zum Außerkraftsetzen einer Eigenschaft konfigurieren**  **Hinweis:** Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Folgende Aktionen können mithilfe von Ausdrücken ausgeführt werden (weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	◦ Legen Sie Formulardatenwerte mithilfe von Definitionsausdrücken fest. Zum Beispiel: `${parameter.formData.CatalogAttributeType}` ◦ Weisen Sie Benutzerdatenwerte mithilfe von Definitionsausdrücken zu. Beispiel: `${parameter.userData.userId}` Beispielsweise kann mit dem folgenden Wert der Stapelname auf **Stack_Bob.Smith@company.com** gesetzt werden: `Stack_ ${parameter.userData.userId}` ◦ Legen Sie Stapel- oder Tabellenwerte mithilfe von Laufzeitausdrücken fest. Beispiel: `$(ci.sn_cmp_ip_pool[subnet= ${parameter.formData.Subnet Id}])` entnimmt das Subnetz aus der Tabelle „IP-Pools“. ◦ Ordnen Sie einem Feld mithilfe statischer Ausdrücke eine Zufallszahl zu. Verwenden Sie: `${randomNumber}`

Ist skriptbasiert	Aktivieren Sie das Kontrollkästchen, um das Textfeld **Skript** anzuzeigen, und geben Sie dann das Skript an.
	
	Sie können den folgenden Beispielskriptausschnitt verwenden, um einen Stapelnamen außer Kraft zu setzen. Mit dem Abschnitt `function (formData)` des Skripts werden die Werte für Felder im Formular geändert. In diesem Beispiel heißt der Stapel `MyStack` (MeinStapel).
	
	`customScript : function( formData){`
	`// Manipulation of form parameter is only supported here.`
	`// Change in any other attributes will be ignored`
	`// data available for manipulation are`
	`// Form Data - Ex. StackName can be accessed`
	`// through formData.StackName`
	`// formData.StackName = "MyStack";`
	`// User Data - Ex. User Id can be accessed`
	`// through this.parameters.userData`
	`// if(this.parameter.userData.userId == 'servicenowuserId')`
	`formData.StackName = "MyStack";`
	`return formData;`
	`},`

Aktion für eine Richtlinie „bei Beginn/Ende der Katalogelementanforderung“ erstellen

Der Auslöser *bei Beginn der Katalogelementanforderung* wird ausgelöst, nachdem der Benutzer ein Anforderungsformular geöffnet hat. Der Auslöser *bei Ende der Katalogelementanforderung* wird ausgelöst, nachdem ein Benutzer ein Anforderungsformular übermittelt hat. Eine Richtlinie, die durch den Auslöser *bei Beginn der Katalogelementanforderung* oder *bei Ende der Katalogelementanforderung* ausgelöst wird, kann ein Skript oder einen Workflow ausführen.

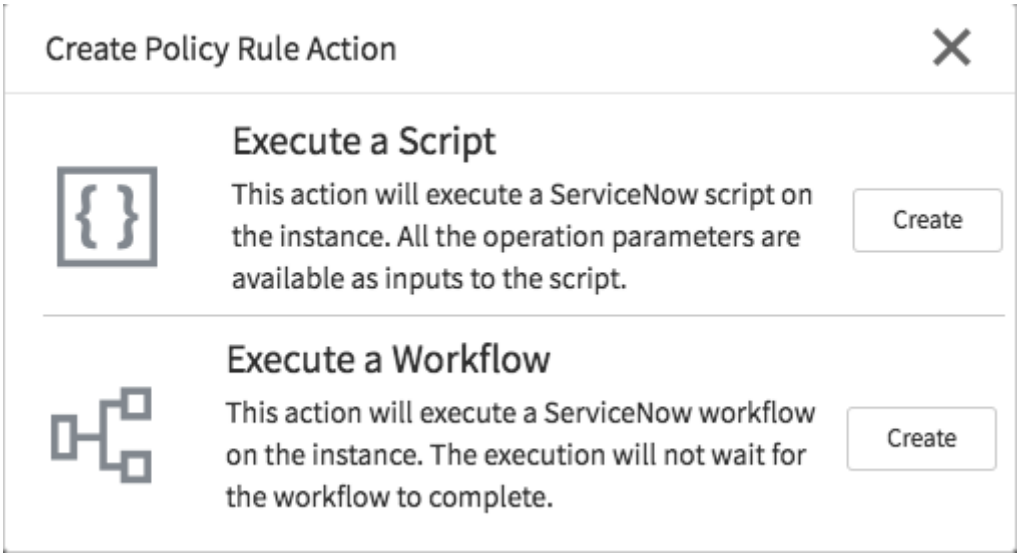
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und versetzen Sie die Richtlinie bei Bedarf in den Status **Entwurf**.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.

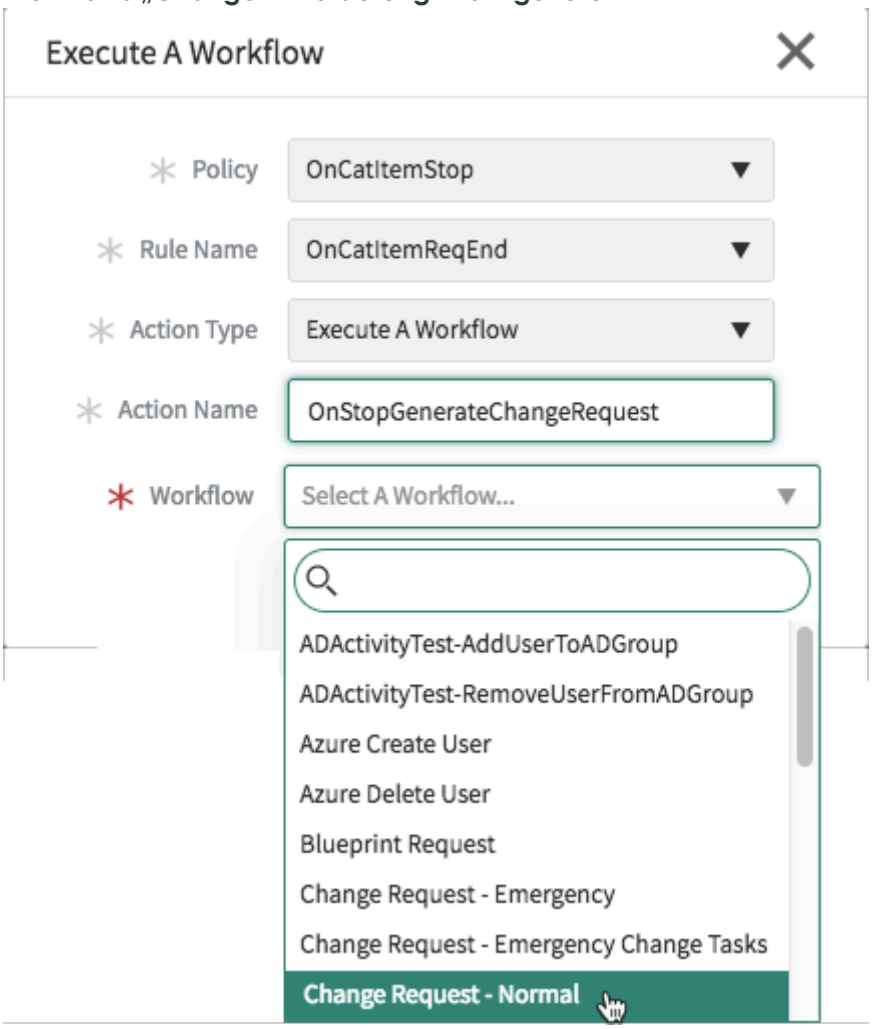


Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aktion vom Typ „Workflow ausführen“ zum Ausführen des Basissystem-Workflows „Change-Anforderung“ konfigurieren



Einstellungen für die Aktion „Workflow ausführen“

Feld	Beschreibung
Aktionsname	Geben Sie einen eindeutigen und aussagekräftigen Namen für die Aktion an, mit der der Workflow gestartet wird.
Workflow	Wählen Sie den auszuführenden Workflow.

Aktion für eine Richtlinie „Mietvertragsende“ erstellen

Eine Richtlinie, die durch den Auslöser *bei Leasingende* ausgelöst wird, kann eine Benachrichtigung senden oder einen Lebenszyklusvorgang *Starten*, *Stoppen* oder *Bereitstellung aufheben* ausführen.

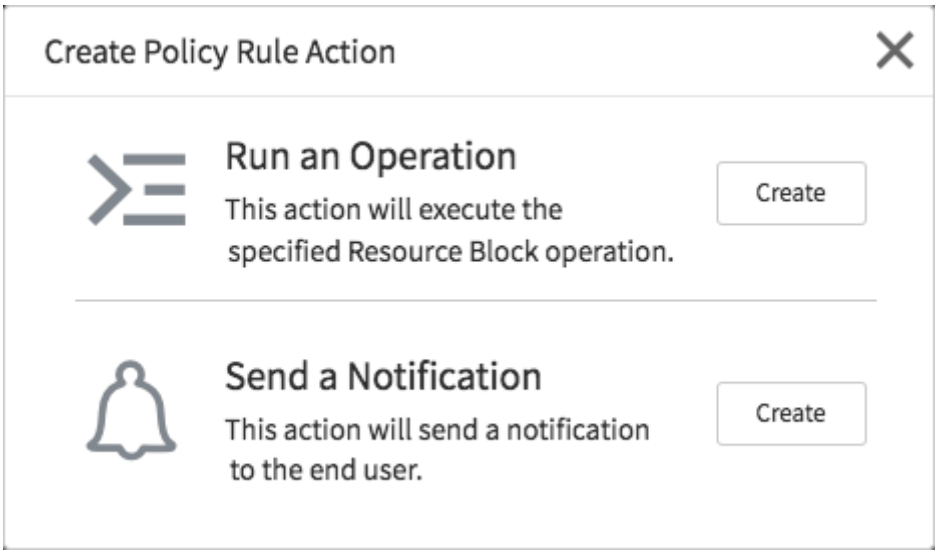
Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und versetzen Sie die Richtlinie bei Bedarf in den Status **Entwurf**.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.



Einstellungen für die Aktion „Vorgang ausführen“

Feld	Beschreibung
Planvorgang	Geben Sie **Start**, **Stopp** oder **Aufheben der Bereitstellung** an.

Einstellungen für die Aktion „Benachrichtigung senden“

Feld	Beschreibung
Benachrichtigung	Wählen Sie den Text der Benachrichtigung aus: ◦ Lease End Date Reached (Mietenddatum erreicht) ◦ Stack Decommissioned (Lease End) (Stapel stillgelegt (Mietende)) ◦ Upcoming Lease End (Bevorstehendes Mietende)

Aktion für eine Richtlinie „bei Ressourcenvorgang“ erstellen

Der Auslöser *bei Ressourcenvorgang* wird während des Orchestration-Prozesses ausgelöst, wenn ein Benutzer einen Lebenszyklusvorgang *Starten*, *Stoppen* oder *Bereitstellung aufheben* für eine bestimmten Ressource durchführt. Eine Richtlinie, die durch den Auslöser *bei Ressourcenvorgang* ausgelöst wird, kann einen von einem Benutzer angeforderten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

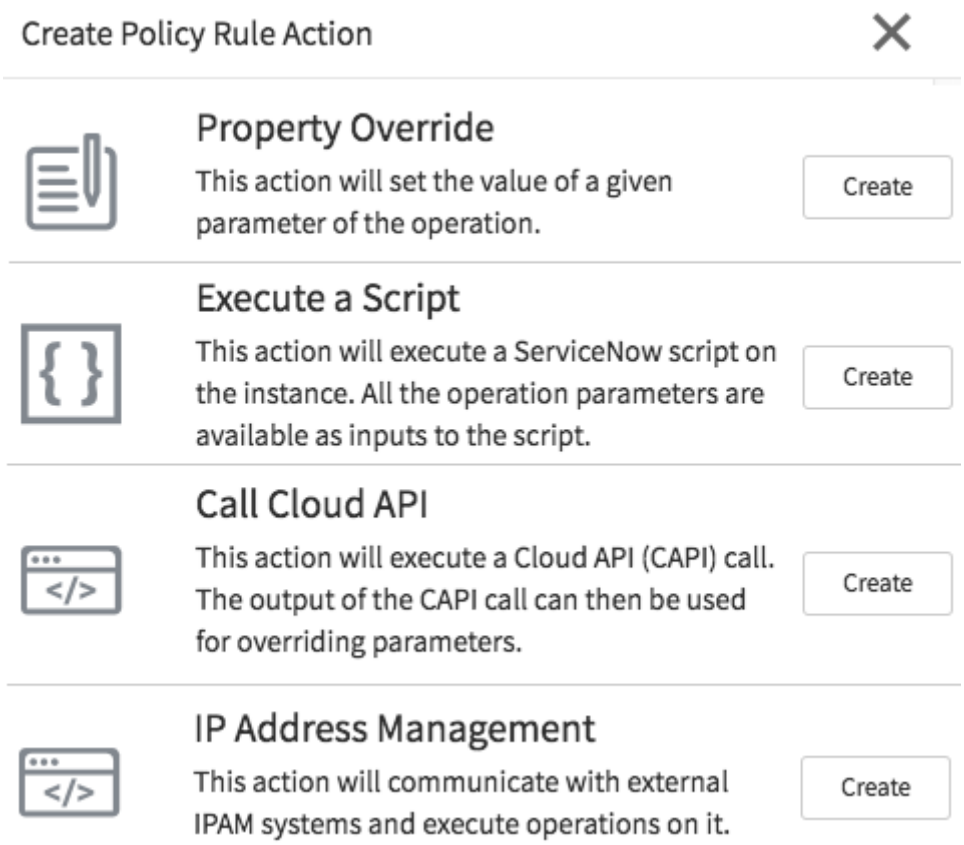
Attributwert überschreiben, ein Skript ausführen, eine Cloud API aufrufen oder einen IP-Adressenverwaltungsvorgang ausführen.

Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Prozedur

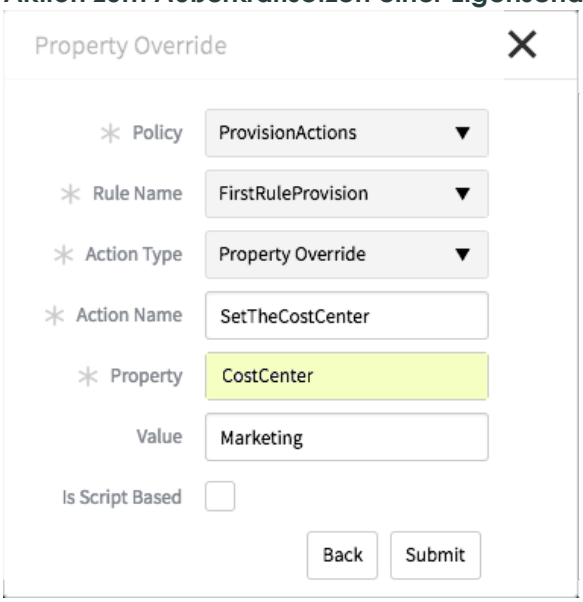
1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und versetzen Sie die Richtlinie bei Bedarf in den Status **Entwurf**.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.



Einstellungen für die Aktion „Eigenschaft außer Kraft setzen“

Feld	Beschreibung
Eigenschaft	Geben Sie den Namen der Eigenschaft (des Attributs), die/das außer Kraft gesetzt werden soll, auf dem Benutzeranfrageformular an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Wert	Geben Sie einen Wert ein, der den Wert im Feld **Eigenschaften** außer Kraft setzt. Sie können nur Textwerte überschreiben. Sie können einen statischen Wert, einen Ausdruck oder beides angeben. In der Beispielaktion mit dem Namen **SetTheCostCenter** (Kostenstelle festlegen) wird der Wert **Marketing** für die Eigenschaft **CostCenter** (Kostenstelle) angegeben. **Aktion zum Außerkraftsetzen einer Eigenschaft konfigurieren**  **Hinweis:** Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Folgende Aktionen können mithilfe von Ausdrücken ausgeführt werden (weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden): ◦ Legen Sie Formulardatenwerte mithilfe von Definitionsausdrücken fest. Zum Beispiel: `${parameter.formData.CatalogAttributeType}` ◦ Weisen Sie Benutzerdatenwerte mithilfe von Definitionsausdrücken zu. Beispiel: `${parameter.userData.userId}` Beispielsweise kann mit dem folgenden Wert der Stapelname auf **Stack_Bob.Smith@company.com** gesetzt werden: `Stack_ ${parameter.userData.userId}` ◦ Legen Sie Stapel- oder Tabellenwerte mithilfe von Laufzeitausdrücken fest. Beispiel: `$(ci.sn_cmp_ip_pool[subnet= ${parameter.formData.Subnet Id}])` entnimmt das Subnetz aus der Tabelle „IP-Pools“. ◦ Ordnen Sie einem Feld mithilfe statischer Ausdrücke eine Zufallszahl zu. Verwenden Sie: `${randomNumber}`
Ist skriptbasiert	Aktivieren Sie das Kontrollkästchen, um das Textfeld **Skript** anzuzeigen, und geben Sie dann das Skript an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung

	Sie können den folgenden Beispielskriptausschnitt verwenden, um einen Stapelnamen außer Kraft zu setzen. Mit dem Abschnitt `function (formData)` des Skripts werden die Werte für Felder im Formular geändert. In diesem Beispiel heißt der Stapel `MyStack` (MeinStapel).
	`customScript : function( formData){`
	`// Manipulation of form parameter is only supported here.`
	`// Change in any other attributes will be ignored`
	`// data available for manipulation are`
	`// Form Data - Ex. StackName can be accessed`
	`// through formData.StackName`
	`// formData.StackName = "MyStack";`
	`// User Data - Ex. User Id can be accessed`
	`// through this.parameters.userData`
	`// if(this.parameter.userData.userId == 'servicenowuserId')`
	`formData.StackName = "MyStack";`
	`return formData;`
	`},`

Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

Wenn Sie den Aktionstyp **Cloud-API aufrufen** auswählen und den Datensatz speichern, wird die zugehörige Liste „Richtlinienregel-Aktionsattribute“ mit den Attributen ausgefüllt, die an den Provider zu übergeben sind. Wenn Sie eine Integration mit Infoblox vornehmen, müssen Sie das Feld **DNSSuffix** konfigurieren. Wenn Sie z. B. einen Host erstellen, wird der Wert im Feld **DNSSuffix** in Infoblox für den neu erstellten virtuellen Computer angezeigt.

Einstellungen für die Aktion „Cloud-API aufrufen“

Feld	Beschreibung
Aktionsname	Geben Sie einen beschreibenden Namen für die Aktion ein. In aufeinander folgenden Richtlinienaktionen für dieselbe Richtlinie können Sie in einem Feld vom Typ **Wert** auf diesen Namen verweisen. Er bezieht sich auf die JSON-Nutzlast, die nach einem API-Aufruf vom Cloud Provider empfangen wird. Um beispielsweise auf eine zugewiesene IP-Adresse zu verweisen, die von der Aktion mit dem Namen *`RefAction`* zurückgegeben wurde, können Sie den folgenden Ausdruck im Feld **Wert** einer anderen Richtlinienaktion verwenden: `$(parameter.RefAction.Allocated_IP}`.
Provider	Geben Sie den Cloud Provider aus der API-Bibliothek ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Version	Geben Sie die Version aus der API-Bibliothek ein.
Schnittstelle	Wählen Sie eine CAPI-Schnittstelle aus. Wählen Sie für Infoblox die **IPAM-Schnittstelle** aus.
Vorgang	Wählen Sie einen durchzuführenden CAPI-Schnittstellenvorgang aus. Für Infoblox wählen Sie **CreateHostRecord** oder **DeleteHostRecord**.
Berechtigungen	Geben Sie die sys_ID der erforderlichen Anmeldeinformationen ein. Sie können auch einen Ausdruck wie den folgenden verwenden: `$(ci.sn_cmp_infoblox_server[$(ci.sn_cmp_ip_pool[subnet=${parameter.formData.SubnetId}].provider_instance)].infoblox_server_credential)`
Endpunkt-URL	Geben Sie die Endpunkt-URL des Connectors aus der API-Bibliothek ein. Bei Infoblox ist dies die IP-Adresse des Infoblox-Servers.

Einstellungen für die Aktion „IP-Adressverwaltung“

Feld	Beschreibung
Name der IPAM-Methode	Wählen Sie den Namen der IPAM-Methode aus. Für Infoblox wählen Sie eine der folgenden Optionen aus: ◦ **IP-Adresse freigeben**: Geben Sie eine IP-Adresse von Infoblox frei, wenn die Bereitstellung eines Computers beendet wird. ◦ **IP-Adresse registrieren**: Registrieren Sie einen neuen virtuellen Computer bei Infoblox. Diese Option wird von AWS- und Azure-Clouds verwendet. ◦ **IP-Adresse reservieren**: Reservieren Sie eine neue IP-Adresse. Diese Option wird von einer vSphere-Cloud verwendet. Siehe IP-Adressen für AWS- und Azure-VMs in Infoblox registrieren, IP-Adressen für VMware vSphere-VMs in InfoBlox reservieren und IPAM-Integration.

Aktion für eine Richtlinie „beim Start des Ressourcenvorgangs“ erstellen

Der Auslöser *beim Start des Ressourcenvorgangs* wird ausgelöst, bevor der Katalog für einen Ressourcenvorgang aus dem Cloudbenutzerportal geladen wird. Eine Richtlinie, die durch den Auslöser *beim Start des Ressourcenvorgangs* ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Wert überschreiben (nur Textwerte).

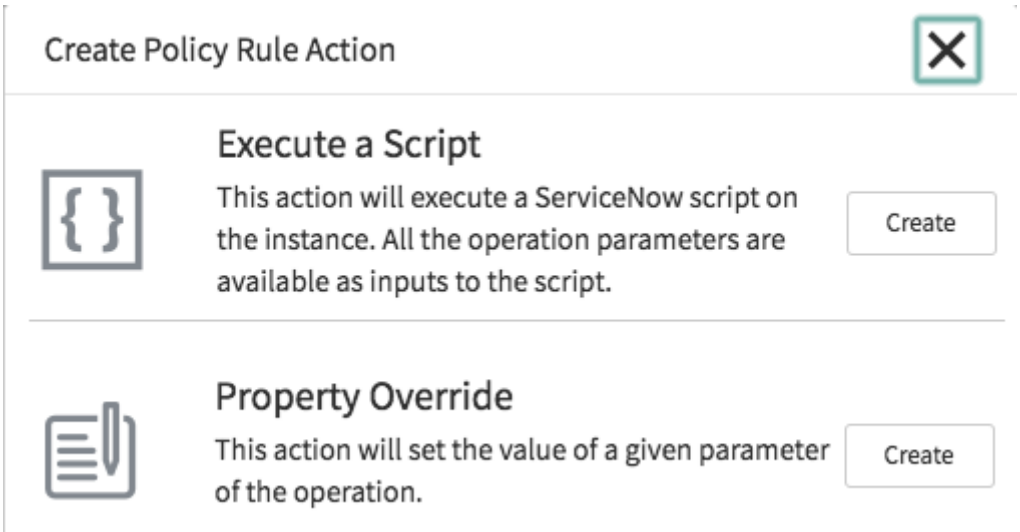
Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und versetzen Sie die Richtlinie bei Bedarf in den Status **Entwurf**.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.



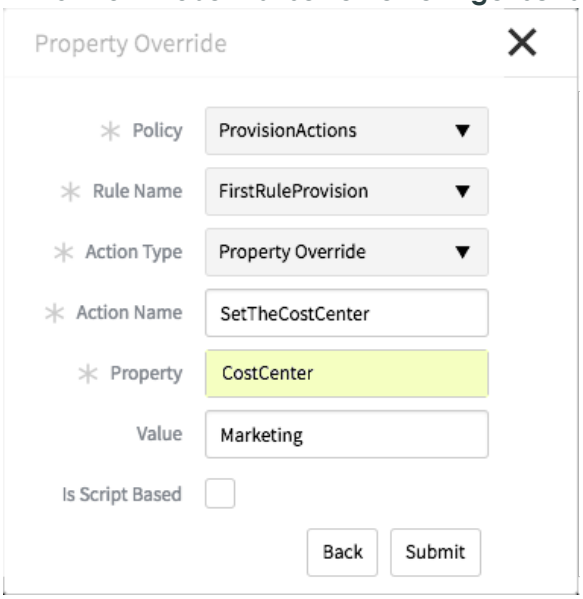
Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

Einstellungen für die Aktion „Eigenschaft außer Kraft setzen“

Feld	Beschreibung
Eigenschaft	Geben Sie den Namen der Eigenschaft (des Attributs), die/das außer Kraft gesetzt werden soll, auf dem Benutzeranfrageformular an.
Wert	Geben Sie einen Wert ein, der den Wert im Feld **Eigenschaften** außer Kraft setzt. Sie können nur Textwerte überschreiben. Sie können einen statischen Wert, einen Ausdruck oder beides angeben. In der Beispielaktion mit dem Namen **SetTheCostCenter** (Kostenstelle festlegen) wird der Wert **Marketing** für die Eigenschaft **CostCenter** (Kostenstelle) angegeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Aktion zum Außerkraftsetzen einer Eigenschaft konfigurieren  **Hinweis:** Wenn ein Wert sowohl von einer Richtlinienregel als auch einer Formularregel außer Kraft gesetzt wird, wird der Wert in der Formularregel verwendet. Folgende Aktionen können mithilfe von Ausdrücken ausgeführt werden (weitere Informationen finden Sie unter Ausdrücke in Cloud Provisioning and Governance verwenden): ◦ Legen Sie Formulardatenwerte mithilfe von Definitionsausdrücken fest. Zum Beispiel: `${parameter.formData.CatalogAttributeType}` ◦ Weisen Sie Benutzerdatenwerte mithilfe von Definitionsausdrücken zu. Beispiel: `${parameter.userData.userId}` Beispielsweise kann mit dem folgenden Wert der Stapelname auf **Stack_Bob.Smith@company.com** gesetzt werden: `Stack_ ${parameter.userData.userId}` ◦ Legen Sie Stapel- oder Tabellenwerte mithilfe von Laufzeitausdrücken fest. Beispiel: `$(ci.sn_cmp_ip_pool[subnet= ${parameter.formData.Subnet Id}])` entnimmt das Subnetz aus der Tabelle „IP-Pools“. ◦ Ordnen Sie einem Feld mithilfe statischer Ausdrücke eine Zufallszahl zu. Verwenden Sie: `${randomNumber}`
Ist skriptbasiert	Aktivieren Sie das Kontrollkästchen, um das Textfeld **Skript** anzuzeigen, und geben Sie dann das Skript an. Sie können den folgenden Beispielskriptausschnitt verwenden, um einen Stapelnamen außer Kraft zu setzen. Mit dem Abschnitt `function (formData)` des Skripts werden die Werte für Felder im Formular geändert. In diesem Beispiel heißt der Stapel `MyStack` (MeinStapel).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	`customScript : function(formData){ // Manipulation of form parameter is only supported here. // Change in any other attributes will be ignored // data available for manipulation are // Form Data - Ex. StackName can be accessed // through formData.StackName // formData.StackName = "MyStack"; // User Data - Ex. User Id can be accessed // through this.parameters.userData // if(this.parameter.userData.userId == 'servicenowuserId') formData.StackName = "MyStack"; return formData; },`

Aktion für eine Richtlinie „beim Start/bei Ende der Ressourcenvorgangsanforderung“ erstellen

Eine Richtlinie, die durch den Auslöser *beim Start der Ressourcenvorgangsanforderung* oder *bei Ende der Ressourcenvorgangsanforderung* ausgelöst wird, kann ein Skript ausführen oder einen vom Benutzer angeforderten Attributwert überschreiben.

Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

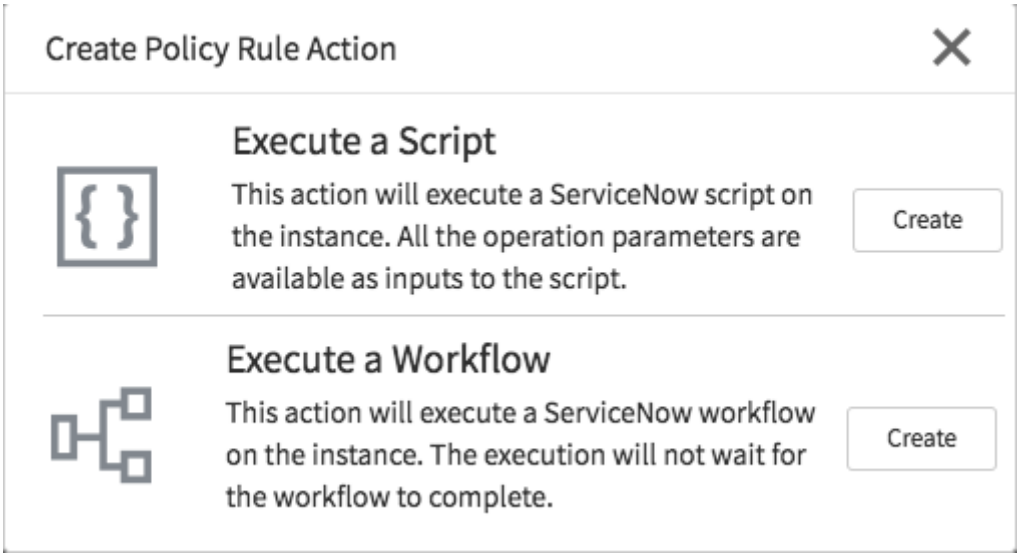
Warum und wann dieser Vorgang ausgeführt wird

- Der Auslöser *beim Start der Ressourcenvorgangsanforderung* wird ausgelöst, nachdem ein Benutzer eine Ressourcenvorgangsanforderung (*Starten*, *Stoppen*, *Bereitstellung aufheben*) übermittelt hat.
- Der Auslöser *bei Ende der Ressourcenvorgangsanforderung* wird vor Abschluss eines Lebenszyklusvorgangs für eine Ressource (*Starten*, *Stoppen*, *Bereitstellung aufheben*) ausgelöst.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und versetzen Sie die Richtlinie bei Bedarf in den Status **Entwurf**.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben, geben Sie einen eindeutigen und aussagekräftigen **Aktionsnamen** ein, und füllen Sie dann das Formular für die Aktion aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Einstellungen für die Aktion „Skript ausführen“

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine Kategorie aus.
Aktionsskriptname	Geben Sie einen eindeutigen und aussagekräftigen Namen für das Skript an.
Aktionsskript	Erstellen Sie das Skript im Textfeld. Details siehe Richtlinienaktionsskript erstellen.

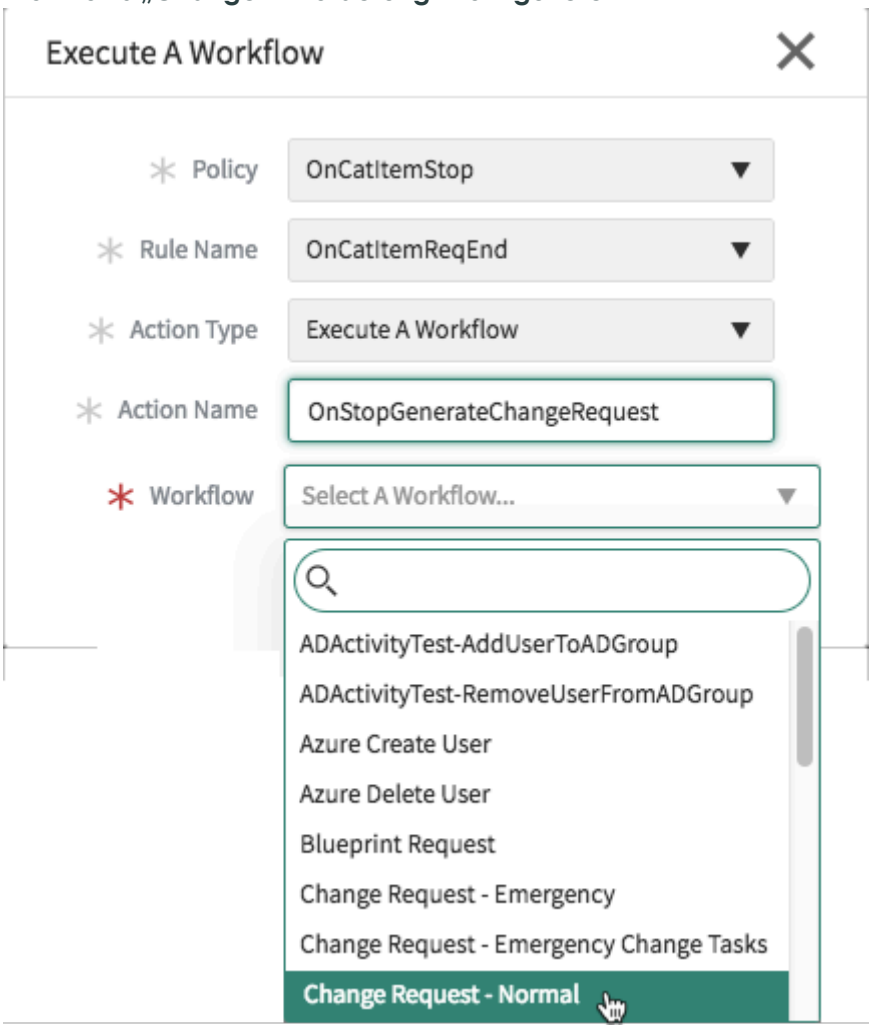
Einstellungen für die Aktion „Workflow ausführen“

Feld	Beschreibung
Aktionsname	Geben Sie einen eindeutigen und aussagekräftigen Namen für die Aktion an, mit der der Workflow gestartet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Workflow	Wählen Sie den auszuführenden Workflow.

Aktion vom Typ „Workflow ausführen“ zum Ausführen des Basissystem-Workflows „Change-Anforderung“ konfigurieren



Aktion für eine Richtlinie „bei Ressourcengrenzen überschritten“ erstellen

Legen Sie die Richtlinie vom Typ *`on Resource limits exceeded`* so fest, dass Genehmigungs-Workflows automatisch ausgeführt oder Benachrichtigungen gesendet werden, wenn ein Bestellformular für ein vorlagenbasiertes Katalogelement übermittelt wird, das die definierten Ressourcengrenzwerte oder Kontingentwerte überschreitet.

Vorbereitungen

Sie müssen die folgenden Elemente konfiguriert haben:

- Mindestens eine Cloud-Richtliniengruppe
- Eine Cloud-Richtlinie
- Eine Genehmigungsrichtlinie
- Eine E-Mail-Benachrichtigung
- Ein Workflow mit dem Workflow-Editor

Erforderliche Rolle: sn_cmp.cloud_governor oder cloud_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Für die Basissystem-Richtlinienaktion *On resource limit exceeded* ist standardmäßig eine ServiceNow-Standardregel für Genehmigungsrichtlinien konfiguriert. Falls Sie andere Aktionen wie Benachrichtigungen oder einen benutzerdefinierten Genehmigungs-Workflow auslösen möchten, wenn die Ressourcengrenze überschritten wird, können Sie entweder die Richtlinienaktion des Basissystems ändern oder eine benutzerdefinierte Richtlinie für Ihre Instanz erstellen.

Prozedur

1. Ändern oder erstellen Sie eine Cloud-Richtlinienaktion, die den Auslöser *on Resource limit exceeded* verwendet.
   a. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
   b. Ändern Sie eine Basissystem-Richtlinie, oder erstellen Sie einen neuen Richtliniendatensatz.
      - a. Öffnen Sie die Basissystem-Richtlinie **Resource Order Control** (Steuerung von Ressourcenbestellungen).
      - b. Ändern Sie den Namen der Richtlinie, das Start- und Enddatum sowie die Reihenfolge der Ausführung.
      - c. Ändern Sie die Bedingungen der Richtlinienregeln.
      - Klicken Sie auf **Neu**, um einen neuen Richtliniendatensatz zu erstellen.

      Weitere Informationen finden Sie unter Cloud-Richtlinien erstellen.
2. Ändern Sie in der zugehörigen Liste „Regeln“ die Basissystemregel, oder erstellen Sie eine neue Regel.
   - Öffnen Sie die Basissystemregel *approveresourcelimit*, mit der die Aktion ausgeführt werden soll, und passen Sie sie an.
   - Erstellen Sie eine Richtlinienregel.

   Weitere Informationen finden Sie unter Cloud-Richtlinienregeln konfigurieren.
3. Geben Sie eine Richtlinienaktion an.
   a. Klicken Sie in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
   b. Klicken Sie neben der Aktion, die ausgeführt werden soll, wenn das Kontingent überschritten wird, auf **Erstellen**.

Optionen	Schritte
ServiceNow-Genehmigungs-Workflow im Basissystem initiieren	a. Geben Sie im Feld **Aktionsname** einen eindeutigen Namen für die Aktion ein. b. Wählen Sie die Option **Managergenehmigung** aus, um den Antrag zur Genehmigung durch den Manager automatisch zu senden. c. Wählen Sie die **Zuweisungsgruppe** aus, für die diese Aktion gilt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Optionen	Schritte
Benutzerdefinierten Genehmigungs-Workflow initiieren	**a.** Geben Sie im Feld **Aktionsname** einen eindeutigen Namen für die Aktion ein. **b.** Wählen Sie im Feld **Workflow** einen vorhandenen benutzerdefinierten Workflow aus.
Senden Sie eine E-Mail-Benachrichtigung an die anfordernde Person des Katalogelements und an den Manager.	**a.** Geben Sie im Feld **Aktionsname** einen eindeutigen Namen für die Aktion ein. **b.** Wählen Sie im Feld **Benachrichtigung** eine Benachrichtigungsvorlage aus. Die Basissystem-Benachrichtigungs-E-Mail für die Richtlinienaktion „bei Ressourcengrenzen überschritten“ wird in der Suchtabelle angezeigt, wenn Sie die Basissystem-Richtlinie verwenden.

4. Klicken Sie auf **Absenden**.

Aktion für eine Richtlinie „bei Aufgabenremediation“ erstellen

Der Auslöser *bei Aufgabenremediation* wird ausgelöst, wenn ein Benutzer eine fehlgeschlagene Anforderung erneut übermittelt. Eine Richtlinie, die durch den Auslöser *bei Aufgabenkorrektur* ausgelöst wird, kann Genehmigungs-Workflows starten.

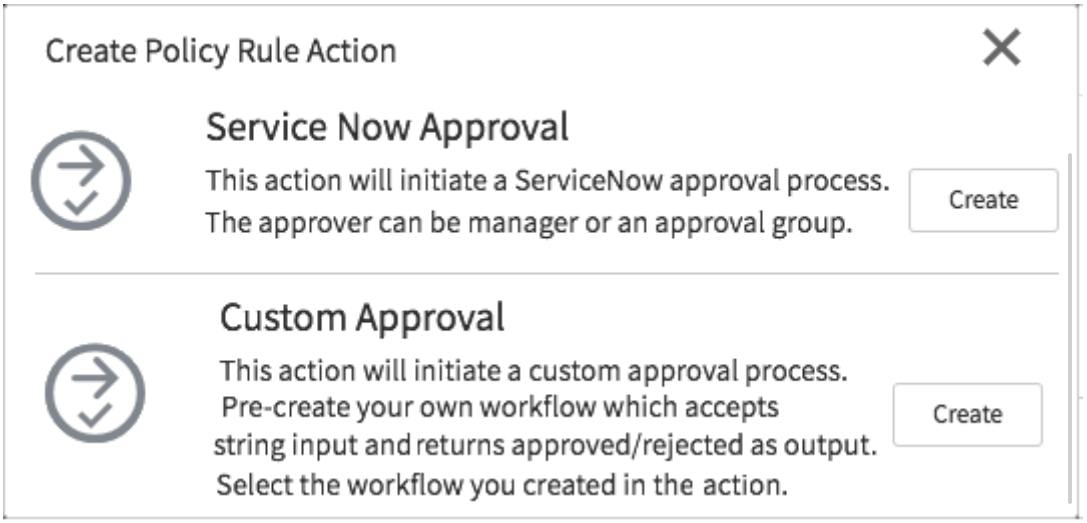
Vorbereitungen

- Erforderliche Rolle: sn_cmp.cloud_governor oder admin
- Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.
- Cloud-Richtlinienregel konfigurieren, sowie zugehörige Bedingungen.

Prozedur

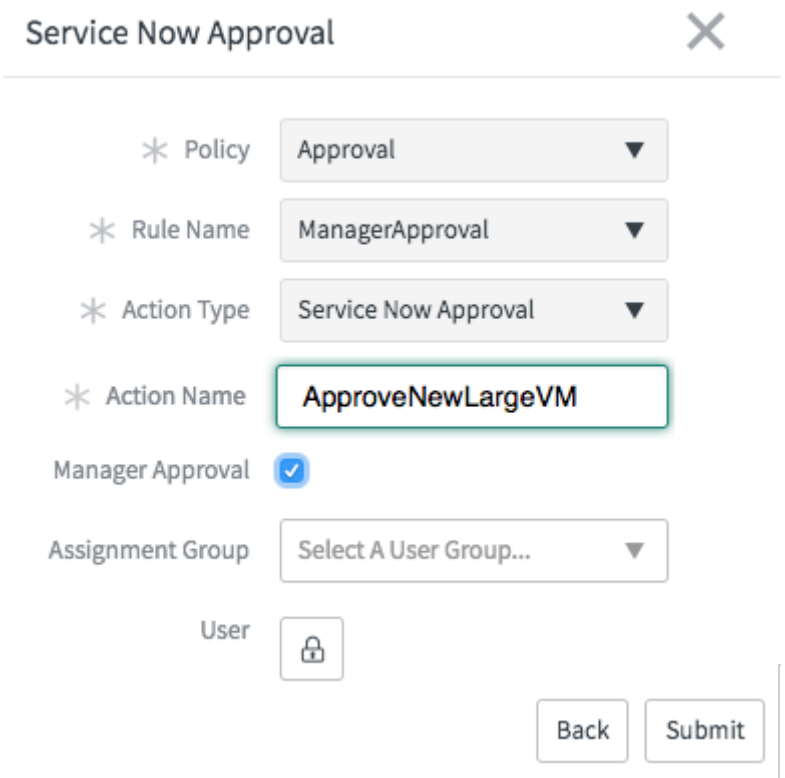
1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und versetzen Sie die Richtlinie bei Bedarf in den Status **Entwurf**.
3. Öffnen Sie die Regel, von der die Aktion ausgeführt werden soll, und klicken Sie dann in der zugehörigen Liste „Richtlinien-Regelaktionen“ auf **Neu**.
4. Klicken Sie im Popup-Fenster auf **Erstellen**, um den Typ der auszuführenden Aktion anzugeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Wählen Sie eine der folgenden Optionen aus.
   - **Benutzerdefinierte Genehmigung** führt den von Ihnen angegebenen Workflow aus. Der Workflow muss den Wert **Genehmigt** zurückgeben, um den Vorgang abzuschließen.
   - **Service Now-Genehmigung** unterstützt unterschiedliche Genehmiger basierend auf dem Auslöser für die Richtlinie:
     - Managergenehmigung
     - Zuweisungsgruppe
     - Benutzer (Sperre)
6. Geben Sie im Genehmigungsformular einen eindeutigen und aussagekräftigen **Aktionsnamen** an.

Aktion in der Regel



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wenn Sie **Anwenderdefinierte Genehmigung**auswählen, geben Sie den Workflow an, und klicken Sie dann auf **Absenden.** Wenn Sie **ServiceNow-Genehmigung**auswählen, geben Sie an, wer die Cloud-Aktivität genehmigen soll.

Genehmigungsfelder

Feld	Beschreibung
Managergenehmigung	Eine oder alle der folgenden Optionen: ◦ Aktivieren Sie das Kontrollkästchen **Managergenehmigung**, um festzulegen, dass der Manager des Genehmigers die Anforderung ebenfalls genehmigen muss. Der standardmäßige Genehmigungs-Workflow geht zuerst an den Manager, dann an die Gruppe und schließlich an den Benutzer. ◦ Wählen Sie eine Benutzergruppe aus der Liste **Zuweisungsgruppe** aus. ◦ Deaktivieren Sie die **Benutzer**-Sperre, wählen Sie einen Benutzer aus der Liste aus, und aktivieren Sie die Sperre anschließend wieder.
Zuweisungsgruppe	Wählen Sie die Zuweisungsgruppe zur Genehmigung der Anforderung aus. Jeder Benutzer in der Gruppe kann die Aktion mit dem Standard-Workflow genehmigen. Die Genehmigung wird dann an die im Feld **Benutzer** angegeben Benutzer gesendet. **Hinweis:** Benutzer in einer Zuweisungsgruppe, die nicht über die Rolle „ITIL“ verfügen, erhalten standardmäßig immer noch einen Genehmigungsdatensatz und eine Benachrichtigung. Sie können die Genehmigung jedoch nicht erteilen. Weisen Sie die Rolle „ITIL“ allen Benutzern oder Benutzergruppen zu, die Vorgänge und Bereitstellungen genehmigen müssen.
Anwender	Wählen Sie mindestens einen Benutzer aus, für den die Genehmigungsaktion gilt. Alle ausgewählten Benutzer müssen die Aktion mit dem Standard-Workflow genehmigen.

Richtlinienaktionsskript erstellen

Verwenden Sie Richtlinienaktionsskripts, um Werte in Cloud-Anforderungen abzurufen, zu aktualisieren oder festzulegen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

Weitere Informationen zum Verwenden von Skripts finden Sie unter Cloud-Skripts und Cloud-Skriptvorlagen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Adminportal zu **Bedingungen** > **Richtlinien**.
2. Klicken Sie auf der Registerkarte **Richtlinien-Aktionsskripts** auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Namen** und eine **Beschreibung** ein, füllen Sie das Formular aus, und klicken Sie dann auf **Absenden**.
   Nachdem Sie einen Namen eingegeben haben, wird ein Skript mit einer Variablen angezeigt, die den von Ihnen eingegebenen Namen verwendet.

Feld	Beschreibung
Aktionsskriptkategorie	Wählen Sie eine andere Kategorie aus, oder behalten Sie die in einem früheren Schritt erstellte Kategorie bei.
Skript	Ändern Sie die Funktion `customScripts` im Skript. Dies ist der einzige Teil des Skripts, den Sie ändern müssen.

Example:
Das folgende Beispielskript ermittelt, ob der Benutzer zu einer Benutzergruppe gehört, und überschreibt dann den benutzerdefinierten Wert des Knotennamens des Anwendungsservers mit dem Wert **MyNodeName**.

```
customScript : function(formData){
  var groups = this.parameters.userData.groups;
    if( groups.length > 0){
      formData.App_Server_NodeName = "MyNodeName";
    }
  return formData;
},
```

Dieses Beispiel gibt eine zufällige Zahl zurück:

```
customScript : function(formData){
  var min = 10000;
  var max = 99999;
  var num = Math.floor(Math.random() * (max - min + 1)) + min;
  formData.randomNumber = num + "";
  return formData;
},
```

Dieses Beispielskript fügt dem Leasingdatum mithilfe der GlideDateTime -Klasse im Basissystem drei Stunden hinzu.

```
var SetLeaseShort = Class.create();
SetLeaseShort.prototype =
 Object.extendsObject(sn_cmp.PolicyExecutionBase, {
 customScript : function(formData){
  // Manipulation of form parameters are supported. Changes in any other
 attributes
              // will be ignored.
  // The data available for manipulation is as follows:
  // Form Data -  for example: StackName can be accessed through
 formData.StackName
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  // formData.StackName = "MyStack";
  // User Data  - for example: User Id can be accessed through
 this.parameters.userData
  // if(this.parameter.userData.userId == 'servicenowuserId')
  // this.info("id = " + formData.StackName);

  // var leaseValue = now();
  // leaseValue = leaseValue.setHours(leaseValue.getHours()+4);
  // formData.LeaseEndDate = leaseValue;

  if (formData.hasOwnProperty("LeaseEndDate")) {
   gdt = new GlideDateTime();
   // 10800 = 3 hours
   gdt.addSeconds(10800);
   formData.LeaseEndDate = gdt.getDisplayValue();
  }
  return formData;
 },
 execute: function() {
  if(this.parameters !=  null && this.parameters.formData != null){
         var inputData =
 JSON.parse(JSON.stringify(this.parameters.formData));
      var outputFormData = this.customScript(inputData);
            if( outputFormData != null){
                this.parameters.formData = outputFormData;
            }
        }
  var output = {};
  output.answer = this.parameters;
  return JSON.stringify(output);
 },
 type : 'SetLeaseShort'
});

var SetLeaseShortObj = new SetLeaseShort(inputAttributes);
var outputParams = SetLeaseShortObj.execute();
gs.info( "Output of script is = " + outputParams);
```

Dieses Beispielskript legt das benutzerdefinierte Namensfeld **Azure Wordpress DNS** im Formular auf denselben Namen wie den Stapelnamen fest:

```
var WordpressFill = Class.create();
WordpressFill.prototype =
 Object.extendsObject(sn_cmp.PolicyExecutionBase, {
 customScript : function(formData){
  // Manipulation of form parameters are supported. Changes in any other
 attributes
        // will be ignored.
  // The data available for manipulation is as follows:
  // Form Data -  for example: StackName can be accessed through
 formData.StackName
  // formData.StackName = "MyStack";
  // User Data  - for example: User Id can be accessed through
 this.parameters.userData
  // if(this.parameter.userData.userId == 'servicenowuserId')
  //this.info("id = " + formData.StackName);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
  formData.Azure_Wordpress_v6_vmDnsName = formData.StackName;

  return formData;
 },
 execute: function() {
  if(this.parameters !=  null && this.parameters.formData != null){
         var inputData =
 JSON.parse(JSON.stringify(this.parameters.formData));
      var outputFormData = this.customScript(inputData);
            if( outputFormData != null){
                this.parameters.formData = outputFormData;
            }
        }
  var output = {};
  output.answer = this.parameters;
  return JSON.stringify(output);
 },
 type : 'WordpressFill'
});

var WordpressFillObj = new WordpressFill(inputAttributes);
var outputParams = WordpressFillObj.execute();
gs.info( "Output of script is = " + outputParams);
```

Zugehörige Informationen

Beispiel für ein Richtlinienaktionsskript zum Kennzeichnen von Ressourcen mit Tags

Beispiel für ein Richtlinienaktionsskript zum Kennzeichnen von Ressourcen mit Tags

Ihre Instanz verfolgt für Abrechnung und Berichterstellung getaggte Ressourcen nach. Richtlinienaktionsskripts können Ressourcen-Tags hinzufügen und ändern. In diesem Beispiel wird eine Speichervolume-Ressource mit Tags versehen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

Warum und wann dieser Vorgang ausgeführt wird

Unter Benutzerdefiniertes Tag für Cloud-Ressourcen erstellen finden Sie Informationen zum Erstellen und Verwenden von Tags in Cloud Provisioning and Governance.

Prozedur

1. Navigieren Sie im Portal für Cloud-Admin.zu **Bedingungen** > **Richtlinien**.
2. Klicken Sie auf der Registerkarte **Richtlinienaktionsskripts** auf **Neu**, und geben Sie einen eindeutigen und beschreibenden **Namen** ein.
3. Klicken Sie auf das Suchsymbol für **Aktionsskriptkategorie**, klicken Sie auf **Neu**, um eine neue Kategorie zu erstellen, und klicken Sie dann auf **Absenden**.
4. Geben Sie auf der Seite „Richtlinienregel-Aktionsskript“ das Skript für die Ressource ein, die Sie mit Tags versehen möchten.
5. Klicken Sie auf **Absenden**, um das Skript zu speichern.
   Das Skript wird in der Liste angezeigt.
6. Klicken Sie auf der Registerkarte „Richtlinien“ auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Namen** für die Richtlinie ein, füllen Sie das Formular mit den folgenden Beispieleinstellungen aus, und klicken Sie dann auf **Speichern** .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richtlinienauslöser	bei Ressourcenvorgang
Ressourcenblock	Speicher-Laufwerk
Vorgang	Storage Volume Interface.Provision
Moment	Vor dem Vorgang

7. Klicken Sie in der zugehörigen Liste „Regeln“ auf **Neu**, geben Sie für den **Namen** den Wert **Add Custom Tags for Storage (Benutzerdefinierte Tags für Speicher hinzufügen)** ein, akzeptieren Sie die Standardeinstellungen, und klicken Sie dann auf **Absenden**.
8. Klicken Sie in der zugehörigen Liste „Richtlinienregelaktionen“ auf **Neu**.
9. Klicken Sie unter „Skript ausführen“ auf **Erstellen**, füllen Sie das Formular mit den folgenden Beispieleinstellungen aus, und klicken Sie dann auf **Absenden**.

Aktionsname	CreateCustomTagsForStorage
Aktionsskriptkategorie	ScriptsForCustomTags
Aktionsskript	AddCustomTagsForStorage

10. Klicken Sie auf der Seite „Richtlinienregel“ auf **Aktualisieren**.
11. Kehren Sie zur Seite „Richtlinie“ zurück, und klicken Sie dann auf **Veröffentlichen**.

Ergebnisse
Starten Sie im Portal für Cloud-Admin. den Stapel, der der Speicherressource zugeordnet ist. Sie können dann bestätigen, dass die Tags angewendet wurden.

Cloud-Genehmigungsrichtlinie erstellen

Eine Cloud-Genehmigungsrichtlinie gibt die Benutzer an, die eine angegebene Cloud-Aktivität genehmigen müssen, bevor die Aktivität fortgesetzt werden kann. Genehmiger können den Manager des Benutzers, der eine Anforderung sendet, einen angegebenen Benutzer oder eine bestimmte Gruppe oder Benutzer mit einer bestimmten Rolle einschließen. Sie können mehrere Genehmiger angeben. Genehmigungen erfolgen in der von Ihnen angegebenen Reihenfolge.

Vorbereitungen
Optional: Erstellen Sie mindestens eine Cloud-Richtliniengruppe.

Erforderliche Rolle: sn_cmp.cloud_governor oder admin

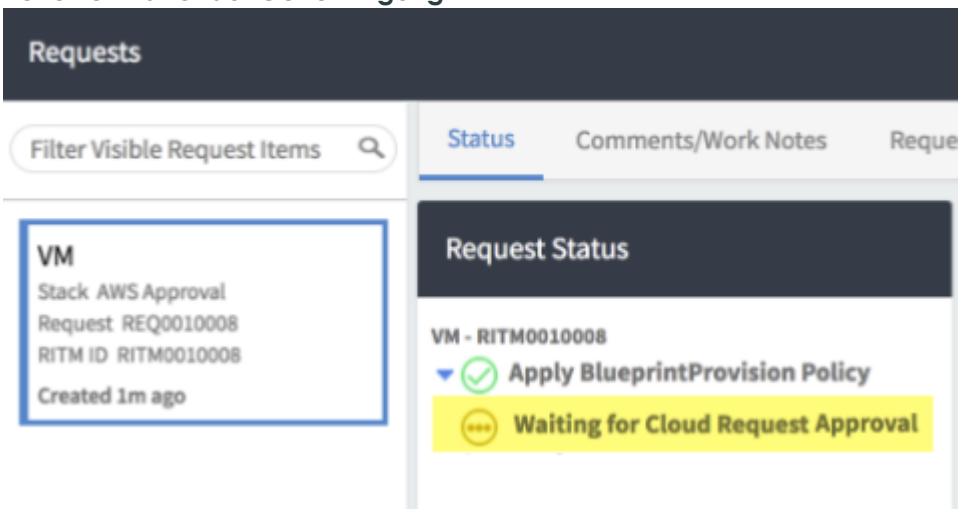
Warum und wann dieser Vorgang ausgeführt wird
In diesem Beispiel fordert ein Benutzer einen Stapel an, der eine Genehmigungsrichtlinie auslöst.

1. Ein Benutzer sendet im Cloudbenutzerportal eine Anforderung zur Bereitstellung einer bestimmten Blaupause. Der Prozess der Bereitstellung der Blaupause ist der Auslöser, mit dem das Richtlinienmodul zur Anwendung einer Genehmigungsrichtlinie veranlasst wird. Eine Cloud-Genehmigungsrichtlinie gibt die Benutzer an, die eine angegebene Cloud-Aktivität genehmigen müssen, bevor die Aktivität fortgesetzt werden kann.
2. Vom Richtlinienmodul wird festgestellt, dass die Anforderung die in der Regel für die Richtlinie angegebene Bedingung erfüllt. In diesem Beispiel wird die Bedingung immer dann als „true“ (wahr) bewertet, wenn eine bestimmte Blaupause bereitgestellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Da die Bedingung erfüllt ist, wird vom Richtlinienmodul die Aktion ausgeführt, die auch in der Regel angegeben ist. In diesem Beispiel besteht die Aktion darin, eine Genehmigungsaktion für den Manager anzulegen.
4. Während der Genehmiger (der Manager) die Genehmigungsanforderung überprüft, wird dem Benutzer im Cloudbenutzerportal die Statusmeldung „Warte auf Genehmigung“ angezeigt.
5. Die Blaupause wird nach Genehmigung durch den Manager bereitgestellt.

Benutzer wartet auf Genehmigung



Die gezielten Genehmigungsrichtlinien ergänzen die anwendungsweite Genehmigung.

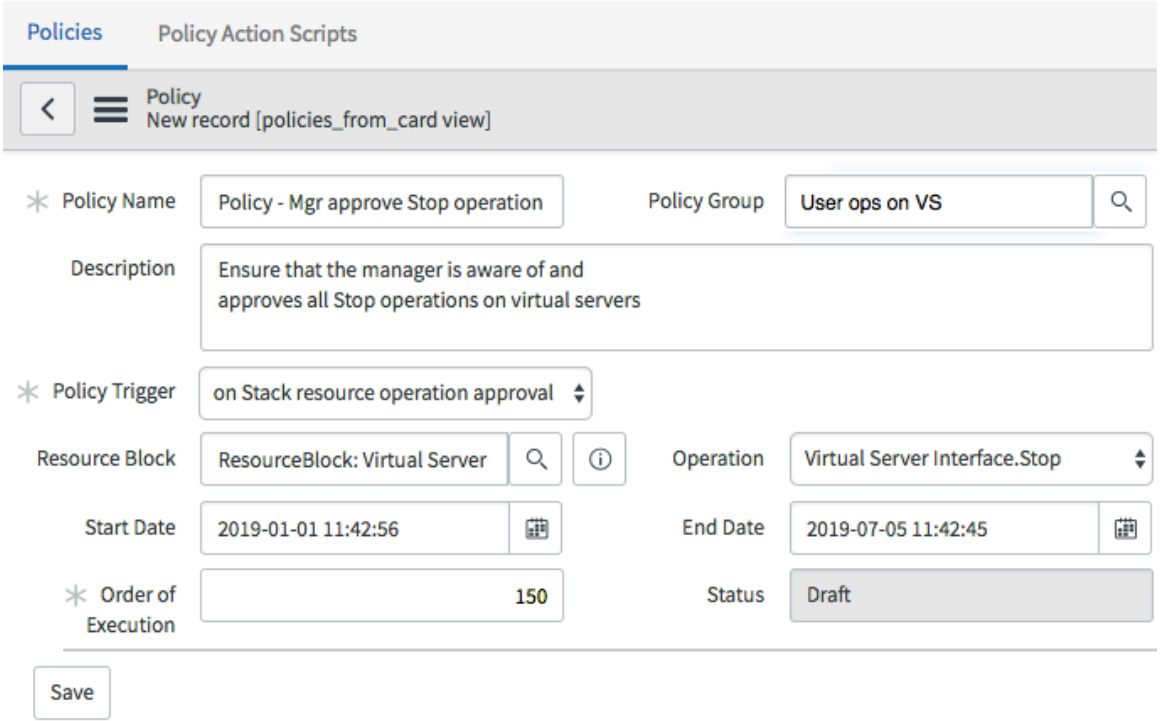
- **bei Genehmigung des Stapelvorgangs**: Wird während eines beliebigen Stapelvorgangs im Cloudbenutzerportal ausgelöst.
- **bei Genehmigung des Stapelressourcenvorgangs**: Wird während eines Ressourcenvorgangs (Starten, Stoppen, Bereitstellung usw.) im Cloudbenutzerportal ausgelöst.
- **bei Aufgabenremediation**: Wird ausgelöst, wenn ein Benutzer eine fehlgeschlagene Anforderung erneut übermittelt.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Klicken Sie auf **Neu**, und füllen Sie das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beispiel für eine Genehmigungsrichtlinie



Feld	Beschreibung
Richtlinienname	Geben Sie einen beschreibenden Namen ein, der das Wort `Richtlinie` enthält. Beginnen Sie den Namen nicht mit einer Zahl.
Beschreibung	Geben Sie eine eindeutige Beschreibung der Absicht der Richtlinie ein.
Richtliniengruppe	Optional: Wählen Sie eine Richtliniengruppe aus. Jede Richtlinie in der Gruppe wird erzwungen.
Richtlinienauslöser	Wählen Sie einen Auslöser aus, der angibt, wann die Richtlinie angewendet werden soll. Die folgenden Auslöser können Genehmigungsrichtlinien starten: ◦ bei Genehmigung der Blaupausenbereitstellung ◦ bei Genehmigung des Stapelvorgangs ◦ bei Genehmigung des Stapelressourcenvorgangs ◦ bei Aufgabenremediation
Blaupause [wird angezeigt, wenn der Auslöser **bei Genehmigung der Blaupausenbereitstellung** oder **bei Genehmigung des Stapelvorgangs** ausgewählt ist]	Wählen Sie die Blaupause aus, für die die Richtlinie gilt. ◦ Wenn keine Blaupause angegeben ist, gilt die Richtlinie für jede Blaupause. Diese Einstellung kann die Leistung beeinträchtigen. ◦ Sie können einer Blaupause mehrere Richtlinien zuweisen. Wenn mehrere Richtlinien gleichzeitig ausgeführt werden, kann die Leistung jedoch beeinträchtigt werden. Veröffentlichen Sie eine Richtlinie nur dann, wenn sie erzwungen werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Vorgang [wird angezeigt, wenn der Auslöser **bei Genehmigung des Stapelressourcenvorgangs** ausgewählt ist] Überprüfer: Wird dies auch für „bei Genehmigung des Stapelvorgangs“ angezeigt?	Wählen Sie den Vorgang aus, für den die Richtlinie gilt. Beispielsweise kann eine Richtlinie nur für den Vorgang *Bereitstellung aufheben* oder für alle Vorgänge für die Blaupause oder das Katalogelement gelten. **Hinweis:** Wenn kein Vorgang angegeben ist, gilt die Richtlinie für alle Vorgänge. Diese Bedingung kann die Leistung beeinträchtigen. ◦ **Alle**: Beliebiger Vorgang wird ausgeführt. ◦ **Starten**: Die Ressource wird gestartet. ◦ **Stoppen**: Die Ressource wird gestoppt. ◦ **Bereitstellung**: Die Ressource wird bereitgestellt. ◦ **Bereitstellung aufheben**: Die Ressource ist für Benutzer nicht mehr verfügbar. ◦ **Skript ausführen**: Ein Skript wird mit der Ressource ausgeführt.
Startdatum/Enddatum	Geben Sie das Startdatum an, ab dem die Richtlinie durchgesetzt werden soll, und das Enddatum, ab dem die Richtlinie nicht mehr durchgesetzt werden soll.
Reihenfolge der Ausführung	Geben Sie eine Zahl an, die die Reihenfolge darstellt, in der die Richtlinie angewendet wird. Eine Richtlinie mit einer niedrigeren Nummer wird vor einer Richtlinie mit einer höheren Nummer ausgeführt. Beispielsweise wird eine Richtlinie mit einer **Reihenfolge** von **100** vor einer Richtlinie mit einer **Reihenfolge** von **200** ausgeführt.
Status	Eine neue Richtlinie befindet sich im Status **Entwurf**. Klicken Sie im Header des Formulars auf **Veröffentlichen**, um die Richtlinie durchzusetzen. Sobald eine Richtlinie veröffentlicht ist, müssen Sie sie auf den Status **Entwurf** setzen, um sie zu aktualisieren.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.
4. Wenn Sie bereit sind, die Richtlinie durchzusetzen, klicken Sie auf **Veröffentlichen**.

Nächste Maßnahme
Konfigurieren Sie mindestens eine Cloud-Richtlinienregel.

Cloud-Richtliniengruppe erstellen

Eine Cloud-Richtliniengruppe ist ein Container für zugehörige Richtlinien. Es empfiehlt sich, Richtlinien, die häufig zusammen verwendet werden oder zusammen betrachtet werden sollen, zu gruppieren. Durch die Gruppierung von Richtlinien können Sie Richtlinien konsistent in Ihrer Organisation anwenden.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_governor oder admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Richtlinien**.
2. Öffnen Sie eine Cloud-Richtlinie, und klicken Sie auf das Suchsymbol für die **Richtliniengruppe**.
3. Wählen Sie die Gruppe aus, der die Richtlinie hinzugefügt werden soll.
   - Um die Richtlinie einer vorhandenen Gruppe hinzuzufügen, wählen Sie die Gruppe aus und klicken Sie dann auf **Absenden**.
   - Zum Erstellen einer Richtliniengruppe, der die Richtlinie hinzugefügt werden soll, klicken Sie in der Liste „Richtliniengruppen“ auf **Neu**, geben Sie einen eindeutigen und aussagekräftigen **Namen** an, und klicken Sie dann auf **Absenden**. Die Richtlinie wird der neuen Gruppe hinzugefügt.

Cloud-Richtlinie exportieren oder importieren

Zum Sichern, Verschieben oder Wiederherstellen einer Richtlinie können Sie die Richtlinie als Update Set exportieren und importieren. Das Update Set enthält Regeln, Bedingungen, Aktionen, Skripts und Skriptkategorien.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin oder admin

Prozedur

1. Navigieren Sie im Cloud-Adminportal zu **Bedingungen** > **Richtlinien**.
2. Führen Sie die folgende Aktion aus, um eine Richtlinie zu exportieren:

   a. Klicken Sie auf das Exportsymbol für die Richtlinie.

   Die Instanz generiert ein Update Set.

3. Zum Importieren einer Richtlinie installieren Sie das Update Set wie folgt:

   a. Navigieren Sie auf der Instanz, in die importiert werden soll, zu **Systemupdate-Sätze** > **Abgerufene Update-Sätze**.

   b. Klicken Sie auf den zugehörigen Link **Update Set aus XML importieren**.

   c. Klicken Sie im Popup-Fenster „XML importieren“ auf **Datei auswählen**, wählen Sie die Datei aus, und klicken Sie dann auf **Hochladen**.

   Wenn eine Richtlinie, die Sie aus der Quellumgebung exportiert haben, in der Zielumgebung vorhanden ist und beide Richtlinien die gleiche sys_id haben, wird die Richtlinie in der Zielumgebung aktualisiert.

Trouble?

Hinweis: Wenn die Richtlinie, die Sie aus der Quellumgebung exportiert haben, in der Zielumgebung vorhanden ist und die Richtlinien unterschiedliche sys_ids aufweisen, tritt während des Importvorgangs ein Fehler auf. Sie müssen eine andere Richtlinie aus der Quellumgebung exportieren oder die gleichnamige Richtlinie in der Zielumgebung löschen.

Zugehörige Informationen

System-Update Sets

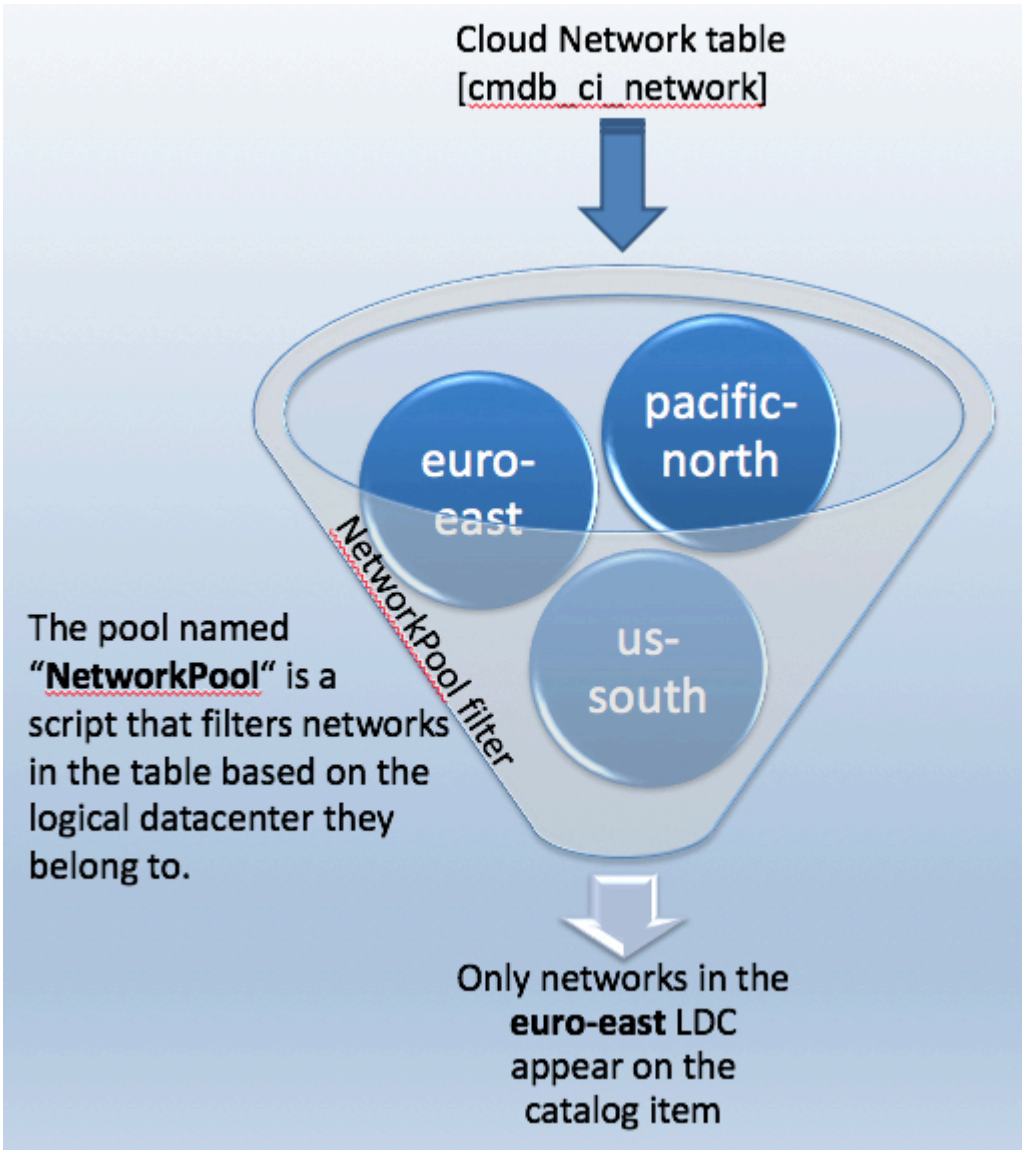
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Pools und Filter für Cloud Provisioning

Ein Ressourcenpool ist eine Abfrage oder ein Skript zur Filterung einer Tabelle. Sie konfigurieren einen Ressourcenpool, um die Werte zu beschränken, die Benutzern bei der Anforderung eines Katalogelements zur Verfügung stehen.

Beispiel für die Verwendung eines Pools

Um einen Benutzer auf die Netzwerke in einem bestimmten logischen Rechenzentrum zu beschränken, verwenden Sie den *`NetworkPool`* genannten Ressourcenpool, der mit der Tabelle „Cloud-Netzwerk“ [cmdb_ci_network] ausgeführt wird. Der Ressourcenpool verwendet ein Skript zum Filtern von Netzwerken basierend auf dem Rechenzentrum, zu dem das Netzwerk gehört.



Funktionsweise von Pools

Die Benennungskonvention für Pools lautet:

```
get<thisItem>By<condition>
```

Dabei ist `condition` die Entität der obersten Ebene, die die Beziehung zwischen den Rückgabewerten bildet. Beispielsweise filtert `getObjectIdByServiceAccount` alle ObjectIDs, die auf dem angegebenen Servicekonto gehostet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abfragetabellen werden nur anhand der angegebenen Bedingung gefiltert. Alle Datensätze, die der Bedingung entsprechen, werden daher zurückgegeben.

Pools und Blaupausen

Beim Konfigurieren von Blaupausen geben Sie Variablen für das Formularverhalten an. Sie können Ressourcenpools als Datenquelle für jede Variable angeben und auswählen, welche Ressourcenpools verwendet werden sollen. Die Variable verwendet dann die gefilterten Werte.

Ressourcenpool im Basissystem

Pool	Basiert auf dieser Tabelle	Filtertyp	Filtername und -beschreibung
AnsibleInventoryPool	Ansible Tower-Bestand [sn_cfg_ansible_inventory]	Skript	Filtert den Namen des Ansible Tower-Bestands.
ApplicationPool	Applikation	Abfrage	Filtert die Namen von Anwendungen.
ApplicationProfilePool	Anwendungsprofil [sn_cmp_application_profile]	Skript	Filtert den Namen von Anwendungsprofilen.
AvailabilityZonePool	Verfügbarkeitszone [cmdb_ci_av availability_zone]	Skript	Filtert Verfügbarkeitszonen basierend auf dem logischen Rechenzentrum, zu dem sie gehören. getNameByLDC: Filtert Verfügbarkeitszonen basierend auf dem logischen Rechenzentrum, zu dem sie gehören. Die Terraform-Vorlage für IBM erfordert den Namen der Verfügbarkeitszone als Eingabe für die Bereitstellung.
AzureDevOpsPipelinePool	Installierbare Konfiguration [sn_cmp_cfg_installable]	Skript	Filtert die installierbaren Konfigurationen.
AzureDevOpsProjectPool	Azure DevOps-Projekt [sn_itom_csc_cp_azure_devops_project]	Skript	Filtert Projekte basierend auf dem Konfigurationsanbieter
BusinessServicePool	Service [cmdb_ci_service]	Abfrage	Filtert die Namen von Business Services.
ChefServerPool	Chef-Server [sn_cfg_chef_server]	Skript	Filtert Chef-Server-Anmeldeinformationen nach Chef-Server.
CloudAccountPool	Cloud-Konto [cmdb_ci_cmp_cloud_account]	Abfrage	Filtert die Namen von Cloud-Accounts.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Pool	Basiert auf dieser Tabelle	Filtertyp	Filtername und -beschreibung
CloudKeyPairPool	[cmdb_ci_cloud_key_pair]	Skript	getObjectIdByServiceAccount: Filtert Cloud-Schlüsselpaare basierend auf dem Servicekonto, zu dem sie gehören.
ComputeProfilePool	Computing-Profil [sn_cmp_compute_profile]	Skript	Filtert Computing-Profile nach dem logischen Rechenzentrum und dem Cloud-Konto, zu denen sie gehören.
ConfigMgmtPool		Skript	Filtert den Workload-Provider für die Konfigurationsverwaltung.
CostCenterPool	Kostenstelle [cmn_cost_center]	Skript	Filtert, um nur die Kostenstellen aufzulisten, zu denen der Benutzer gehört.
DatastorePool	VMware vCenter-Datenspeicher [cmdb_ci_vcenter_datastore]	Skript	Filtert Datenspeicher basierend auf dem logischen Rechenzentrum, zu dem sie gehören.
HardwareTypePool	[cmdb_ci_compute_template]	Skript	getObjectIdByAvailabilityZone: Filtert Hardwarevorlagen basierend auf der Verfügbarkeitszone, zu der sie gehören.
ImagePool	[cmdb_ci_os_template]	Skript	getObjectIdByServiceAccount: Filtert die resourceId des BS-Images nach Servicekonto. In IBM Cloud beziehen sich BS-Images nicht auf ein Rechenzentrum, sondern werden auf der Servicekonto-Ebene gehostet. Terraform erfordert die resourceId als Eingabe für die Bereitstellung.
IPAddressPool	Cloud-IP-Adresse [cmdb_ci_cloud_ip_address]	Abfrage	Filtert die IP-Adresse.
LaunchConfigurationPool	Server-Array-Startkonfiguration [cmdb_ci_sa_launch_config]	Abfrage	Filtert den Konfigurationspool.
NetworkInterfacePool	Cloud Management-Netzwerkschnittstelle [cmdb_ci_nic]	Skript	Filtert den Netzwerkschnittstellen-Pool.
NetworkPool	Cloud-Netzwerk [cmdb_ci_network]	Skript	• Filtert Netzwerke basierend auf dem logischen Rechenzentrum, zu dem sie gehören.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Pool	Basiert auf dieser Tabelle	Filtertyp	Filtername und -beschreibung
			• getObjectIdByLDC: Filtert Netzwerk-IDs basierend auf dem logischen Rechenzentrum, zu dem sie gehören.
OSProfilePool	BS-Profil [sn_cmp_os_profile]	Skript	Filtert Computing-Profile nach dem logischen Rechenzentrum und dem Cloud-Konto, zu denen sie gehören.
ProjectsPool	Projekt [pm_project]	Abfrage	Filtert die Namen von Projekten.
ResourceGroupPool	Ressourcengruppe [cmdb_ci_resource_group]	Skript	Filtert Ressourcengruppen basierend auf dem logischen Rechenzentrum, zu dem sie gehören.
ScheduleTimeZonePool	Auswahl [sys_choice]	Skript	Filtert geplante Zeitzonen.
SecurityGroupPool	Compute-Sicherheitsgruppe [cmdb_ci_compute_security_group]	Skript	• getByNetwork: Filtert die Sicherheitsgruppe nach dem Netzwerk, zu dem sie gehört. • getObjectIdByServiceAccount: Filtert Sicherheitsgruppen-IDs basierend auf dem Servicekonto, zu dem sie gehören.
SecurityGroupProfilePool	Computing-Sicherheitsgruppenprofil [sn_cmp_security_grp_profile]	Abfrage	Filtert die Namen von Sicherheitsgruppenprofilen.
SSHKeyPool	CMP-SSH-Schlüsselpaar [sn_cmp_ssh_credentials]	Skript	Filtert Benutzerschlüssel nach Benutzer.
StorageAccountPool	Cloud-Speicherkonto [cmdb_ci_cloud_storage_account]	Skript	Filtert Cloud-Speicherkonten basierend auf dem logischen Rechenzentrum, zu dem sie gehören.
StorageVolumePool	Speichervolume [cmdb_ci_storage_volume]	Abfrage	Filtert die Namen von Speichervolumes.
SubnetPool	Cloud-Subnetz [cmdb_ci_cloud_subnet]	Skript	• Filtert das Subnetz nach dem Netzwerk, zu dem es gehört. • getObjectIdByNetwork: Filtert Subnetze basierend auf dem Netzwerk, zu dem sie gehören.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Pool	Basiert auf dieser Tabelle	Filtertyp	Filtername und -beschreibung
UserGroupPool	Gruppe [sys_user_group]	Skript	Gibt nur die Gruppen zurück, zu denen der Benutzer gehört.
VirtualMachinePool	[sn_cmp_resource_pool]	Skript	getByAvailabilityZone: Filtert VM-IDs basierend auf der Verfügbarkeitszone, zu der sie gehören.
VmFolderPool	VMware vCenter-Ordner [cmdb_ci_vcenter_folder]	Skript	Filtert VM-Ordner basierend auf dem logischen Rechenzentrum, zu dem sie gehören.

Erstellt einen Ressourcenpool

Ressourcenpools steuern basierend auf Blaupauseneinstellungen die Werte, die einem Benutzer in einem Katalogelement angezeigt werden, wenn er eine Ressource anfordert. Nur Werte, die den Poolfilter oder das Skript passieren, werden als Optionen auf dem Anforderungsformular für Katalogelemente angezeigt.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor

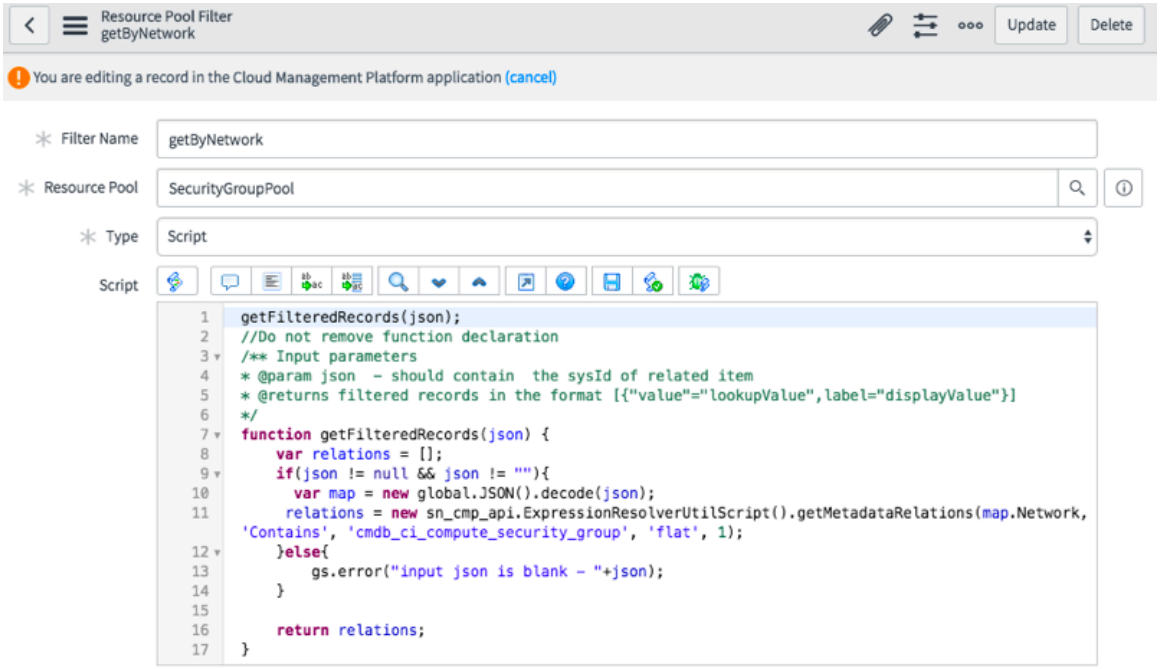
Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Verwalten** > **Ressourcenpools**.
2. Klicken Sie auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Ressourcenpoolnamen** ein, und füllen Sie dann das Formular aus.

Feld	Beschreibung
Typ	Wählen Sie den Typ aus, der festlegt, ob die Gesamtzahl der verfügbaren Werte für die Option, die der Benutzer auswählt, gleich bleibt (Statisch) oder um eins verringert wird (Rückläufig).
Suchtabelle	Wählen Sie die Tabelle aus, die die Datensätze enthält, die als Optionen im Katalogelement für die Ressource angezeigt werden sollen.
Suchfeld [Nicht erforderlich, wenn ein Skript verwendet wird. Dieses Feld wird ignoriert, wenn Sie einen Skriptfilter konfigurieren.]	Wählen Sie das Tabellenfeld aus, das die Werte enthält, die dem Benutzer angezeigt werden sollen. Der Anzeigewert für das Suchfeld wird im Cloudbenutzerportal nicht verwendet. Verwenden Sie stattdessen das/die **Suchbezeichnungsfeld(er)**.
Suchbezeichnungsfelder [Nicht erforderlich, wenn ein Skript verwendet wird. Dieses Feld wird ignoriert, wenn Sie einen Skriptfilter konfigurieren.]	Geben Sie das Suchbezeichnungsfeld ein, das dem Benutzer angezeigt werden soll.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie mit der rechten Maustaste auf die Kopfzeile, und wählen Sie **Speichern** aus.
4. Klicken Sie in der zugehörigen Liste „Ressourcenpoolfilter“ auf **Neu**, geben Sie einen eindeutigen und beschreibenden **Filternamen** ein, und füllen Sie dann das Formular aus.



Feld	Beschreibung
Ressourcenpool	Wählen Sie den Ressourcenpool aus, zu dem der Filter gehört.
Typ	Wählen Sie den Typ des Filters aus: ◦ **Abfrage**: Führen Sie eine Abfrage für die Datensätze in der Tabelle durch, die Sie für die **Suchtabelle** angegeben haben, basierend auf dem von Ihnen angegebenen **Suchfeld**. ◦ **Skript**: Führen Sie ein Skript zum Filtern der Datensätze aus. Geben Sie den Code in das Textfeld **Skript** ein.

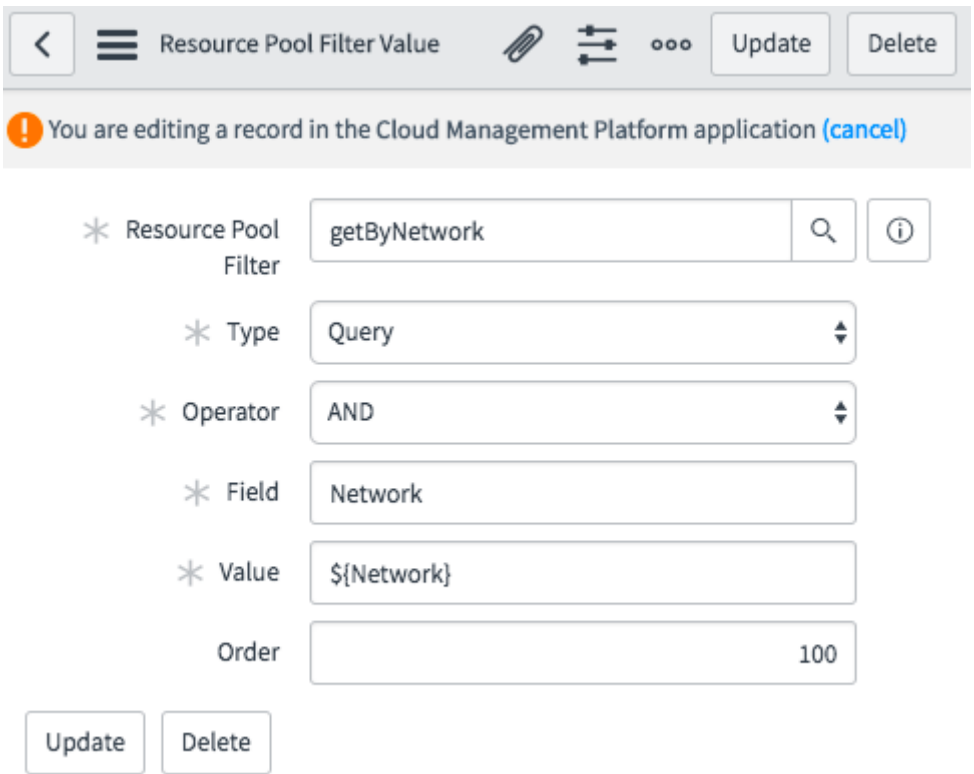
Der Ressourcenpoolfilter wird erstellt.

5. Rechtsklicken Sie auf die Formularüberschrift und wählen Sie **Speichern**.
Wenn Sie einen Filterwert an den Pool zurückgeben müssen und dieser Wert einer anderen Tabelle zugeordnet ist, erstellen Sie einen Datensatz in der zugehörigen Liste „Ressourcenpool-Filterwerte“.
6. Klicken Sie in der zugehörigen Liste „Ressourcenpool-Filterwerte“ auf **Neu**, füllen Sie das Formular aus, und klicken Sie dann auf **Aktualisieren**.

Feld	Beschreibung
Ressourcenpool Filter	Geben Sie den Namen des Filters ein, zu dem der Filterwert gehört.
Typ	Geben Sie den Typ des Filterwerts ein: ◦ **Abfrage**: ◦ **Metadatenregel**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Metadaten-Regelname [Wird angezeigt, wenn Sie als Typ Metadatenregel auswählen]	Geben Sie den Metadaten-Regelnamen ein. Dieses Feld wird nur angezeigt, wenn im Feld **Typ** die Option **Metadatenregel** ausgewählt wird.
Operator	Wählen Sie eine der folgenden Optionen aus: ◦ **UND** ◦ **ODER**
Feld	Geben Sie das Feld in der **Suchtabelle** ein. Beispielsweise **CloudAccount**.
Wert	Geben Sie den Wert, den Sie an den Ressourcenpool zurückgeben, im Format `${feld}` ein, wobei `feld` der Wert im Feld **Feld** ist. Beispielsweise **${CloudAccount}**.
Reihenfolge	Geben Sie eine Reihenfolgennummer ein, die bestimmt, wann der Wert relativ zu anderen Ressourcenpool-Filterwerten angewendet wird. Niedrigere Werte werden zuerst angewendet.



Der Ressourcenpoolfilter wird erstellt.

Binden Sie einen Parameter an einen Ressourcenpool

Um die Fehleranfälligkeit der Katalogbestellung zu verringern, können Sie einen Parameter an einen Ressourcenpool (einen in Basissystembereitgestellten Pool) binden. Parameter, die auf einem Ressourcenpool basieren, führen nur angegebene Werte aus vorhandenen Tabellen im Katalogbestellformular in Cloudbenutzerportalauf.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rolle: sn_cmp.cloud_service_designer

Warum und wann dieser Vorgang ausgeführt wird
Das Katalogbestellformular listet nur Parameterwerte auf, für die die **Datenquelle** angegeben ist. Wenn Sie beispielsweise den Parameter *Resource Group Name* in Ihrer Vorlage verwenden, können Sie das Feld **Ressourcengruppenname** im Metadatenabschnitt an einen vorhandenen SN-Pool (*ResourceGroupPool*) binden.

Wenn Sie einen Ressourcenblock mithilfe einer Cloud-Vorlage erstellen, können Sie einen Parameter im Metadatenabschnitt der Azure Resource Manager- (ARM) oder CloudFormation-Vorlage (CF) an einen SN-Pool binden. Alle SN-Pools werden im Verfahren aufgelistet.

Prozedur
1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Cloud-Katalogelemente**.
2. Wählen Sie eine vorhandene Vorlage aus, oder klicken Sie auf **Neu**, um eine neue Cloud-Vorlage zu erstellen.

   Wenn Sie eine vorhandene Vorlage auswählen, benennen Sie die Vorlage um.

   Im nächsten Schritt ändern Sie die Vorlagendefinition für den entsprechenden Vorlagentyp (wählen Sie ARM oder CloudFormation aus). Sie geben den SN-Poolfilter als Wert für *datasource* an.

SN-Pools, die als Datenquellenwert verwendet werden sollen

SN-Pool	Filter
AvailabilityZonePool	getAllObjects: Ruft alle Verfügbarkeitszonen ab. getObjectsByLDC: Ruft die Verfügbarkeitszone abhängig vom LDC ab.
HardwareTypePool	
ImagePool	
LoadBalancerPool	Alle: Ruft alle Lastenausgleichsmodule ab.
NetworkPool	getAllObjects: Ruft alle Netzwerke ab. getObjectsByLDC: Ruft die Netzwerke abhängig vom LDC ab.
ResourceGroupPool	getObjectsByLDC: Ruft die Ressourcengruppen abhängig vom LDC ab.
SecurityGroupPool	getObjectsByNetwork: Ruft alle Sicherheitsgruppen ab.
SecurityGroupProfilePool	Alle: Ruft alle Sicherheitsgruppenprofile ab.
SSHKeyPool	UserKeys: Ruft alle SSH-Schlüssel ab.
StorageAccountPool	getObjectsByLDC: Ruft die Speicherkonten abhängig vom LDC ab.
StorageVolumePool	Alle: Ruft alle Speichervolumes ab.
SubnetPool	getObjectsByNetwork: Ruft alle Subnetze ab.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

SN-Pool	Filter
VirtualMachinePool	getByAvailabilityZone: Ruft alle virtuellen Computer ab.

3. Ändern Sie eine ARM-Vorlagendefinition:

a. Fügen Sie das Attribut *SNC::Parameter::Metadata* im Metadatenabschnitt *parameters* hinzu.

b. Fügen Sie für das Attribut *SNC::Parameter::Metadatadie Datenquelle* als Schlüssel hinzu, und geben Sie einen SN-Pool-Filter für den Wert ein, z. B. `StorageAccountPool.getObjectsByLDC` (siehe Beispiel).

```
"parameters": {
    "newStorageAccountName": {
      "type": "string",
      "metadata": {
        "description": "Unique DNS Name for the Storage Account where
 the Virtual Machine's disks will be placed.",
         "SNC::Parameter::Metadata": {
         "allowedPattern": "[0-9a-z]{1,11}",
         "ConstraintDescription": "must be a alphanumeric ",

 "datasource":"ServiceNow::Pools::StorageAccountPool.getObjectsByLDC",

        }
      }
    }
```

4. Ändern Sie eine CloudFormation-Vorlagendefinition:

a. Fügen Sie das Attribut *SNC::Parameter::Metadata* hinzu, und definieren Sie den Namen des anwenderdefinierten Attributs (*VpcId*) mit einem *datasource*. Geben Sie für den Wert *datasource* einen SN-Poolfilter ein, wie in diesem Beispiel `NetworkPool.getObjectsByLDC`.

b. Definieren Sie das Zuordnungsattribut *datasourceFilter*, um den benutzerdefinierten Namen (*VpcId*) an den tatsächlichen Attributnamen (*Network*) zu binden.

```
"Parameters" : {

      "VpcId" : {
      "Type" : "AWS::EC2::VPC::Id",
      "Description" : "VpcId of your existing Virtual Private Cloud
 (VPC)",
      "ConstraintDescription" : "must be the VPC Id of an existing
 Virtual Private Cloud."
    },

    "SubnetId" : {
      "Type" : "AWS::EC2::Subnet::Id",
      "Description" : "SubnetId of an existing subnet (for the primary
 network) in your Virtual Private Cloud (VPC)",
      "ConstraintDescription" : "must be an existing subnet in the
 selected Virtual Private Cloud."
    }
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
 },
 "Metadata": {
         "SNC::Parameter::Metadata": {
               "VpcId":{

"datasource":"ServiceNow::Pools::NetworkPool.getObjectsByLDC",
                    "datasourceFilter":{"Network":"VpcId"}
                },
                "SubnetId":{

"datasource":"ServiceNow::Pools::SubnetPool.getObjectsByNetwork",
                    "datasourceFilter":{"Network":"VpcId"}
                }

            }
   }
```

5. Klicken Sie auf **Absenden**.
6. Nachdem der Ressourcenblock, die Blaupause und die Katalogelemente erstellt wurden, sieht der Benutzer des Cloud-Service im Katalogbestellformular nur die Werteliste der Pooldaten für den Parameter.

Beispiel für einen Ressourcenpool, der die Auswahlmöglichkeiten auf Kostenstellen beschränkt

Sie können Ressourcenpools mit Blaupausen verwenden, um die Auswahlmöglichkeiten im Cloud-Kataloganforderungsformular zu beschränken.

Anwendungsfall: Kostenstellenauswahl beschränken

In diesem Beispiel werden die Kosten des Cloud-Assets mit dem Budget der Kostenstelle des Benutzers verrechnet. Basissystem **UserCostCenter** Ressourcenpool stellt sicher, dass ein Benutzer nur Ressourcen in seiner Kostenstelle auswählen kann.

Annahmen

- Das Plugin „Cost Management“ [con.snc.cost_management] ist aktiv.
- Kostenstellen sind definiert, und den Kostenstellen sind Benutzer zugeordnet.
- Mindestens eine Blaupause ist definiert. In diesem Beispiel wird eine Blaupause mit dem Namen **Virtueller AWS-Server** verwendet.
- Ihnen ist die Rolle „sn_cmp_cloud_admin“ zugewiesen, und Sie kennen JavaScript- und JSON-Skripting.

Komponenten

Ressourcenpoolfilter überprüfen

1. Navigieren Sie im Cloud-Adminportal zu **Verwalten** > **Ressourcenpools**.
2. Öffnen Sie den **CostCenterPool**, und überprüfen Sie die zugehörigen Ressourcenpoolfilter.
   - **Alle** ist ein Abfragefilter, der alle Kostenstellen in der Tabelle zurückgibt.
   - **UserCostCenter** ist ein Skriptfilter, der die Kostenstelle sucht, die dem Benutzer zugeordnet ist, der das Element bestellt.

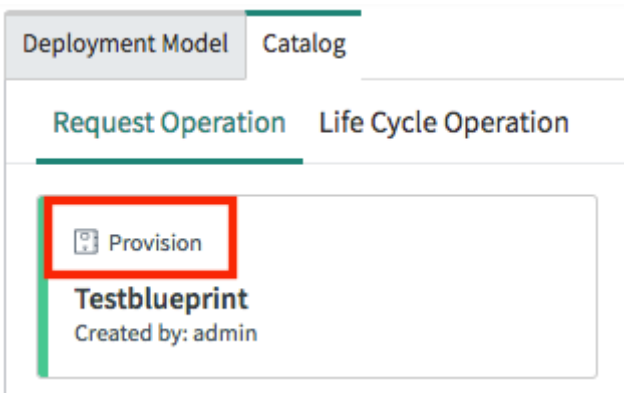
Dies ist das Skript für den Filter **UserCostCenter**:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
getFilteredRecords();
//Do not remove function declaration
/**
* @returns filtered records in the format
 [{"value"="lookupValue",label="displayValue"}]
*/
function getFilteredRecords() {
 var filteredRecords = [];
 var userId = gs.getUserID();
 var userGr = new GlideRecord('sys_user');
 if (userGr.get(userId)){
  var costCenterId = userGr.getValue('cost_center');
  if (costCenterId){
   var costCenterGr = new GlideRecord('cmn_cost_center');
   if (costCenterGr.get(costCenterId)){
    var costCenter = {};
    costCenter.value = costCenterGr.getUniqueValue();
    costCenter.label = costCenterGr.getValue('name');
    filteredRecords.push(costCenter);
   }
  }
 }

 //force to string
 return new global.JSON().encode(filteredRecords);
}
```

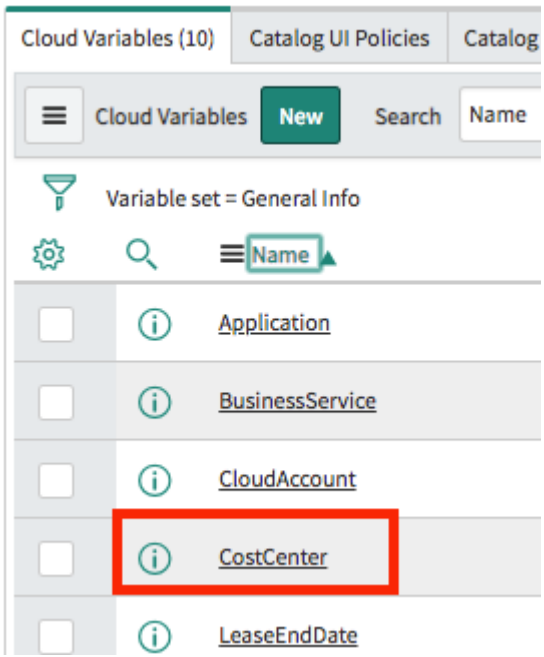
Parameter des Blaupausenkatalogformulars

1. Navigieren zu **Entwurf** > **Blueprints**, und klicken Sie dann auf die Kachel für den Blueprint, den Sie öffnen möchten.
2. Klicken Sie, während sich der Blueprint im Status **Entwurf** befindet, auf die Kachel **Bereitstellungsvorgang** auf **Katalog** > **Anforderungsvorgang** Registerkarte

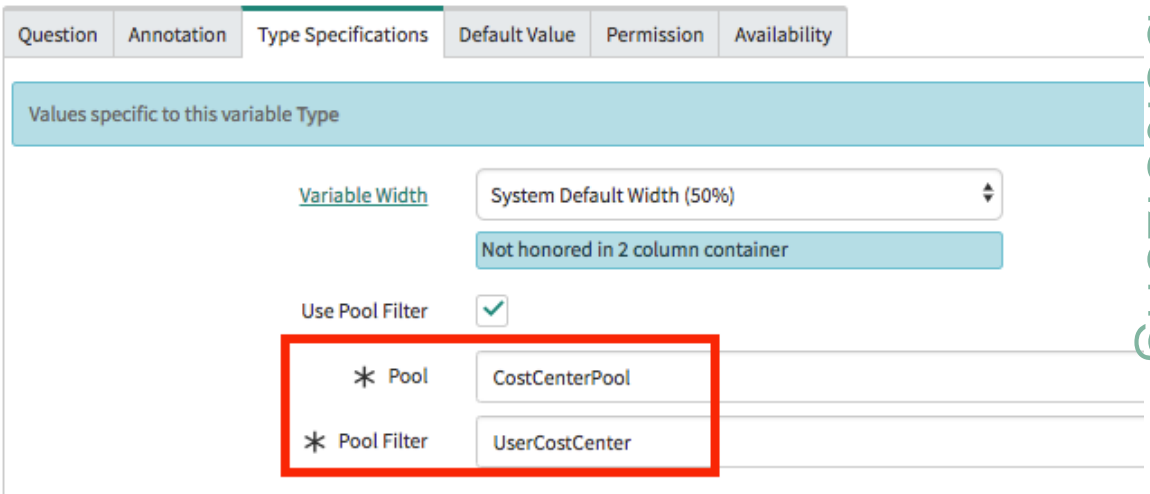


3. Klicken Sie in der zugehörigen Liste „Variablensätze“ auf den Variablensatz **Allgemeine Informationen**. Standardmäßig befindet sich die Variable „CostCenter“ in diesem Variablensatz.
4. Klicken Sie in der zugehörigen Liste „Cloud-Variablen“ im Formular „Variablensatz“ auf die Variable **CostCenter**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf dem Formular „Cloud-Variable“ auf die Registerkarte **Typspezifikationen**.
6. Sehen Sie sich die Felder **Pool** und **Poolfilter** an, die auf den Ressourcenpool und Filter verweisen.
   - *CostCenterPool* ist der Name des Ressourcenpools.
   - *UserCostCenter* ist das Filterskript, das die Kostenstellenoptionen für die Auswahl durch den Benutzer abruft.



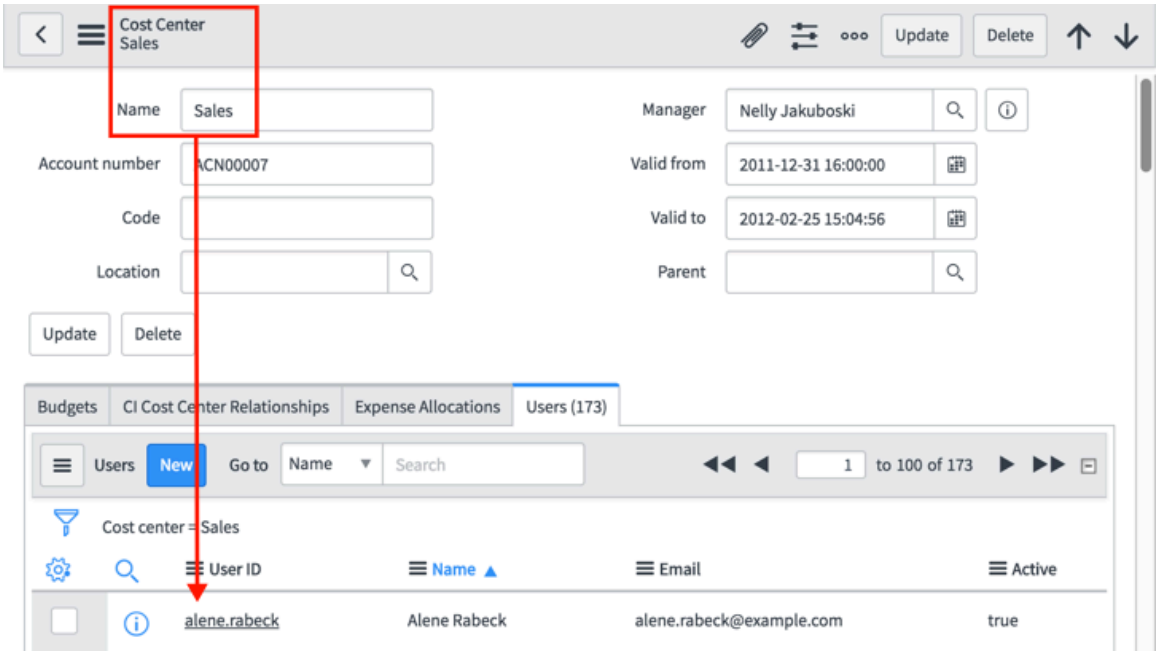
7. Legen Sie die Blaupause auf **Veröffentlicht** fest.

Kostenstellenbenutzer

Identifizieren Sie einen Benutzer, der Mitglied einer Kostenstelle ist und Zugriff auf das Cloudbenutzerportal hat.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Ressourcenpoolfilter testen

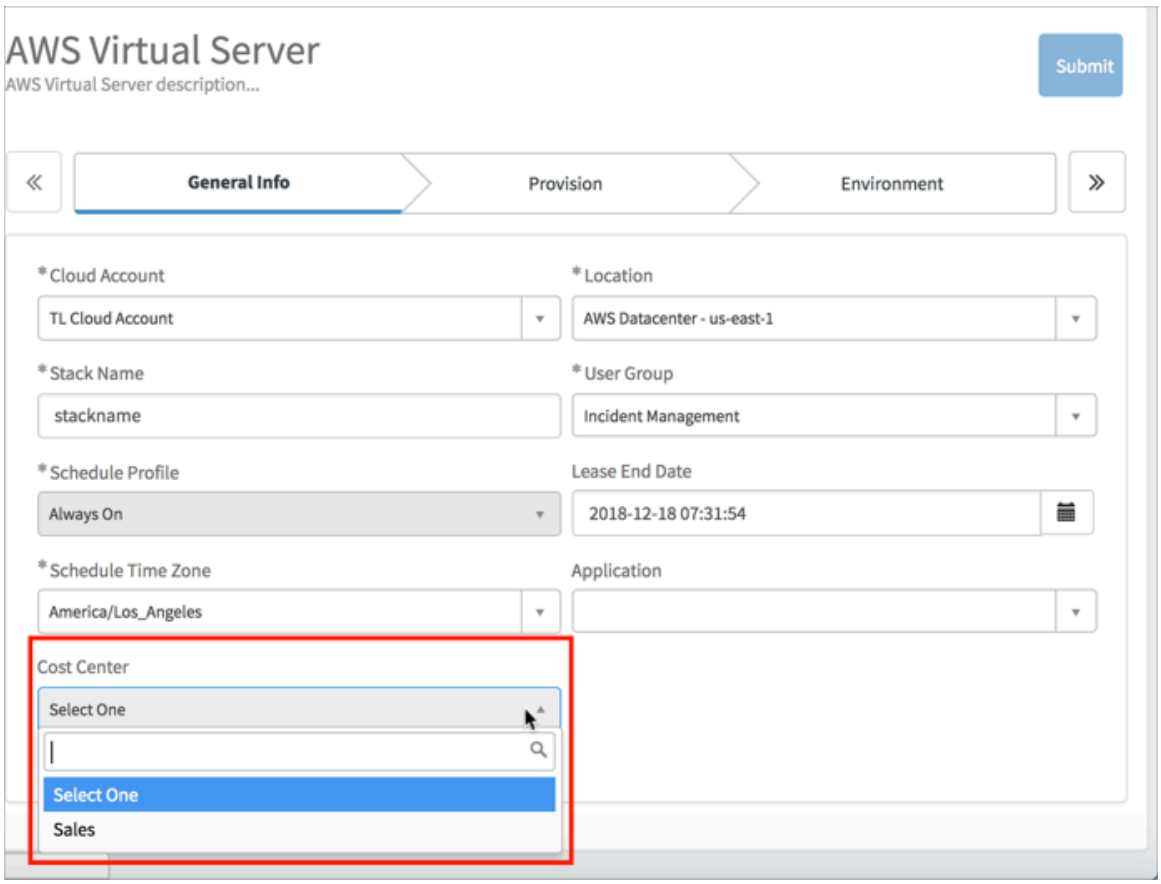
Nach der Überprüfung der Komponenten dieses Anwendungsfalls testen Sie das Cloud-Katalogelement, um sicherzustellen, dass Benutzer nur ihre Kostenstelle auswählen können.

1. Nehmen Sie in diesem Beispiel die Identität der Benutzerin **Alene Rabeck** an.
2. Klicken Sie im Cloudbenutzerportal auf **Einen Stapel starten**, und wählen Sie dann das Cloud-Katalogelement aus (in diesem Beispiel **Virtueller AWS-Server**).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Überprüfen Sie die Auswahlmöglichkeiten in der Liste **Kostenstelle**.



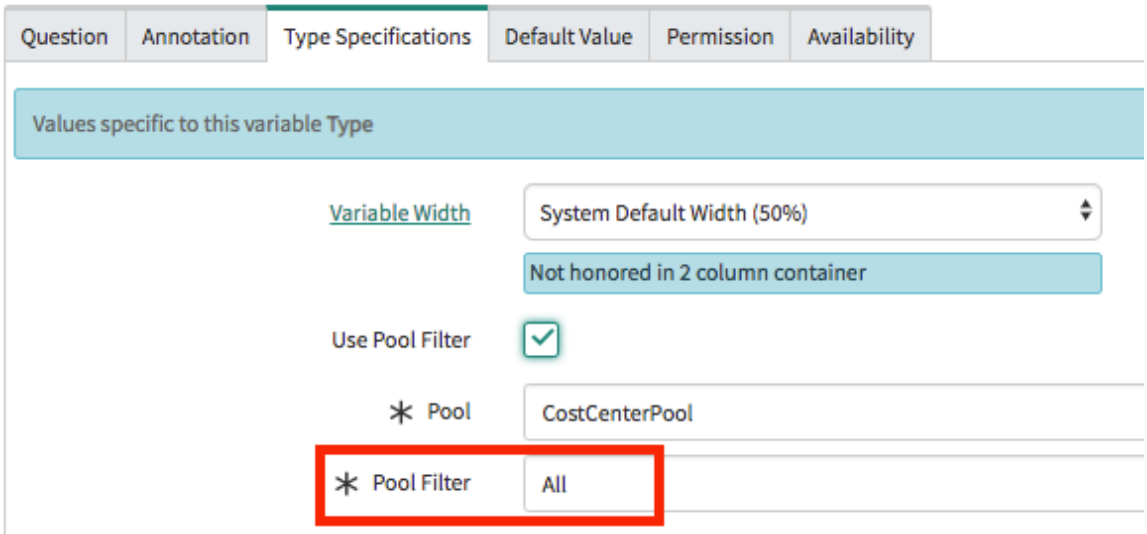
Mit dem Datenquellenwert *CostCenterPool::UserCostCenter* für dieses Katalogelement ist die einzige Option für die **Kostenstelle** die Kostenstelle, bei der der Benutzer Mitglied ist.

Ressourcenpoolfilter ändern

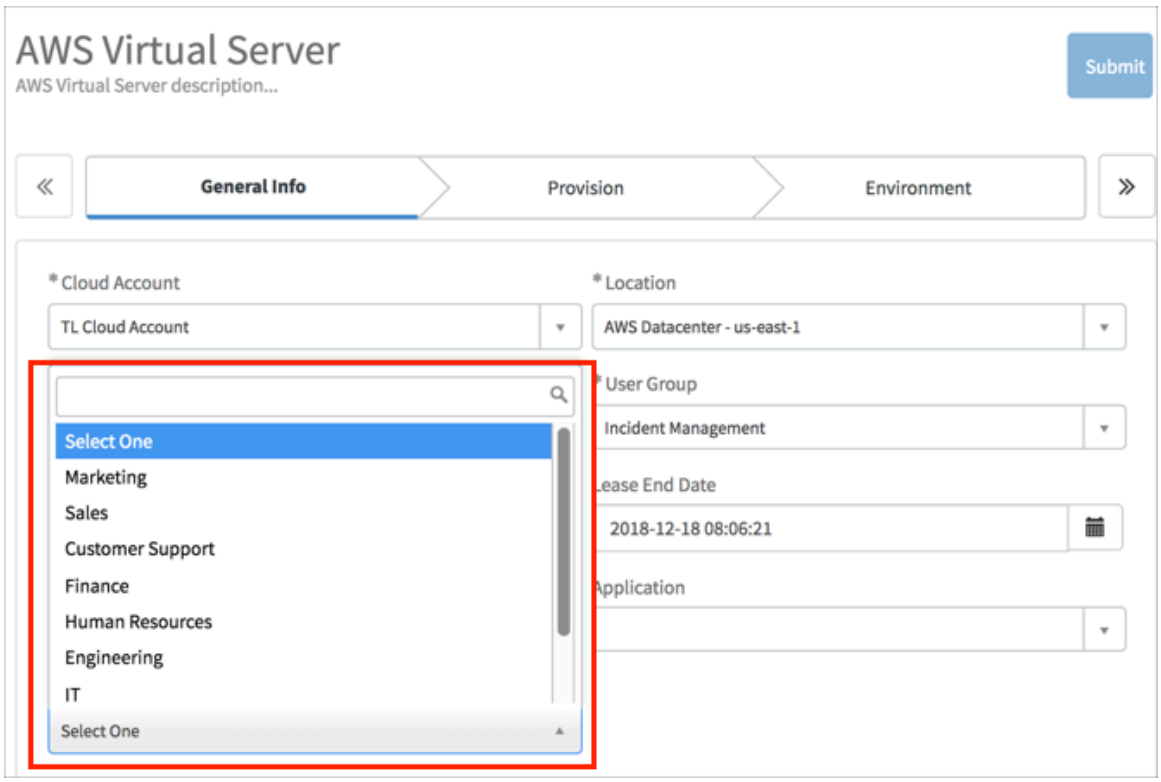
Testen Sie, ob der Ressourcenpoolfilter das Verhalten des Felds **Kostenstelle** steuert, indem Sie ihn ändern und sich die Ergebnisse ansehen.

1. Navigieren Sie im Cloud-Adminportal zu **Entwurf** > **Blueprints** und klicken Sie dann auf **AWS Virtual Server (AWS-Virtual Server)**.
2. Klicken Sie auf die Vorgangskachel **Bereitstellung**.
3. Klicken Sie in der zugehörigen Liste „Variablensätze“ auf den Variablensatz **Allgemeine Informationen**. Standardmäßig befindet sich die Variable „CostCenter“ in diesem Variablensatz.
4. Klicken Sie in der zugehörigen Liste „Cloud-Variablen“ im Formular „Variablensatz“ auf die Variable **CostCenter**.
5. Klicken Sie auf dem Formular „Cloud-Variable“ auf die Registerkarte **Typspezifikationen**.
6. Bearbeiten Sie das Feld **Poolfilter**, um den Filter von *UserCostCenter* in *All* zu ändern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



7. Klicken Sie auf **Aktualisieren** und anschließend auf **Veröffentlichen**.
8. Nehmen Sie in diesem Beispiel die Identität der Benutzerin **Alene Rabeck** an.
9. Starten Sie im Cloudbenutzerportal einen Stapel, und wählen Sie dann **Virtueller AWS-Server** aus.
10. Stellen Sie sicher, dass alle Kostenstellen aufgelistet sind.



Kontingente und Steuerungen für Ressourcenbestellungen

Kontingente sind für Konfigurationselemente oder Cloud-Ressourcen geltende Einschränkungen oder Anforderungen für Gruppen und Benutzer. Verwenden Sie Kontingente, um eine verschwenderische Ressourcennutzung in Ihrer Cloud-Umgebung zu verhindern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie wenden Kontingente auf eine Ressource, z. B. einen virtuellen Server, ein Rechenzentrum oder eine generische Cloud-Ressource sowie auf Benutzer einer bestimmten Gruppe an. Sie können für die Ressource ein Limit pro Benutzer und ein Gesamtlimit für die Gruppe festlegen. Beispielsweise kann ein Kontingent die Anzahl der zulässigen virtuellen Server für Benutzer in der Gruppe **Datenbank** beschränken.

Nachdem diese Art von Kontingent festgelegt wurde, erhalten Benutzer, die versuchen, zusätzliche virtuelle Server bereitzustellen, eine Fehlermeldung und sie können erst mit der Bereitstellung virtueller Server fortfahren, wenn die Ressourcenanzahl wieder unter dem Kontingentgrenzwert liegt. Wenn ein Benutzer zu mehr als einer Gruppe gehört, erhält er als Kontingent das kombinierte Gesamtlimit der beiden Gruppen.

Hinweis: Sie können für Ressourcen auch Beschränkungen pro Rechenzentrum festlegen, indem Sie Kapazitätsgrenzen in Cloud-Accounts verwenden. Weitere Informationen finden Sie unter Kapazitätsgrenzen für Benutzeranforderungen für Ressourcen festlegen.

Ressourcenblocktypen, Kontingenttypen und Attribute

Sie können Benutzern oder Gruppen Kontingente für die folgenden Ressourcenblocktypen zuweisen:

- Virtuelle Server
- Speicherlaufwerkgröße
- Netzwerk
- Stapel

Kontingenttypen enthalten:

Summe

Die Summe aller Attribute für eine Ressource, z. B. die Summe aller virtuellen CPUs.

Anzahl

Die Gesamtanzahl der Attribute für eine Ressource, z. B. die Anzahl der virtuellen Computer.

Cloud-Kontingentdefinition erstellen

In einer Cloud-Kontingentdefinition werden die Einschränkungen für einen Ressourcenblock angegeben. Sie können Vorlagen verwenden oder manuell verschiedene Konfigurationstypen für jede Kontingentdefinition erstellen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_governor

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Quote**.
2. Klicken Sie auf **Neu**.
3. Füllen Sie die Felder des Formulars aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Kontingentdefinition“

Feld	Beschreibung
Kontingentdefinition	Eindeutiger Bezeichner für die Kontingentdefinition. Normalerweise ist dies `Ressourcenname_count` oder `Ressourcenname_size`. Zum Beispiel: Network_Count, VM_Count oder StorageVolume_Size.
Kontingenttyp	Typ der festzulegenden Kontingenteinschränkung: ◦ Anzahl ◦ Größe
Ressourcenname	Der Ressourcenblocktyp, auf den das Kontingent angewendet werden soll. Wählen Sie diesen aus der Nachschlageliste aus. Wählen Sie für vorlagenbasierte Cloud-Ressourcen beispielsweise „Cloud-Ressource“ aus. Weitere Informationen finden Sie unter Ressourcenblöcke in Cloud Provisioning and Governance.
Berechnungseinheit	Einheit, in der dieses Kontingent berechnet wird: ◦ GB ◦ Einzel
CI-Klasse	CMDB-CI-Klasse, die aus der Nachschlageliste ausgewählt werden soll
Attribut	Spaltenname aus dem zugrunde liegenden CI-Typ für den Ressourcenblock, der den Wert enthält, der mit dem Kontingent eingeschränkt werden soll. Beispiel: Wenn Ihr Kontingent die CPU-Anzahl auf einem virtuellen Server begrenzt, lautet die Tabelle des zugrunde liegenden CI-Typs „cmdb_ci_vm_instance“. Die Spalte **cpus** enthält diese CPU-Daten. Geben Sie daher `cpus` ein. Sie können auch `instance` eingeben.
Vorlage [optional]	Tabellenname eines Ressourcentyps, z. B. Hardwaretyp [cmdb_ci_compute_template] oder Image [cmdb_ci_os_template]
Vorlagenattribut [optional]	Spalte aus der Tabelle, die Sie im Feld „Vorlage“ angegeben haben. Dies ist das Attribut, für das das Kontingent festgelegt wird. Beispiel: Wenn Sie die Vorlage [cmdb_ci_compute_template] ausgewählt haben und ein Kontingent für die virtuellen CPUs festlegen möchten, geben Sie `vcpus` ein. In dieser Spalte wird die Anzahl der virtuellen CPUs für alle Datensätze in der Tabelle [cmdb_ci_compute_template] gespeichert.

4. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.
   Die zugehörigen Listen „Kontingentkonfigurationen“, „Standardkontingente“ und „Cloud-Vorlagenressourcen“ werden angezeigt.
5. Klicken Sie in der zugehörigen Liste „Kontingentkonfigurationen“ auf **Neu**.
6. Füllen Sie die Felder im Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formular „Kontingentkonfigurationen“

Feld	Beschreibung
Gruppenname	Eindeutiger Name für die Konfigurationsgruppe
Maximaler Gruppengrenzwert	Maximales Kontingent der Gruppe
Kontingentdefinitionstyp	Der Name der Kontingentdefinition.
Grenzwert pro Benutzer	Maximales Kontingent der einzelnen Benutzer in der Gruppe

7. Klicken Sie auf **Absenden**.
8. Wahlweise: Sie können optionale Standardkontingente angeben, die für den Ressourcenblock festgelegt werden, indem Sie in der zugehörigen Liste „Standardkontingente“ auf **Neu** klicken und dann das Formular ausfüllen.

Formular „Standardkontingente“

Feld	Beschreibung
Maximaler Gruppengrenzwert	Maximales Kontingent der Gruppe
Kontingentdefinition	Die Kontingentdefinition, für die Sie die Standardwerte festlegen.
Grenzwert pro Benutzer	Kontingentgrenze, die für die einzelnen Benutzer in dieser Gruppe gilt

9. Klicken Sie auf **Absenden**.
10. Ordnen Sie das Katalogelement zu, für das das von Ihnen definierte Kontingent gilt, indem Sie in der zugehörigen Liste „Cloud-Vorlagenressourcen“ auf **Neu** klicken.

> **Hinweis:** Wenn Sie einem Katalog kein Kontingent zuordnen, wird für den betreffenden Katalog kein Kontingent berechnet.

11. Füllen Sie die Felder des Formulars aus.

Formular „Cloud-Vorlagenressourcen“

Feld	Beschreibung
Domäne	Domäne, auf die dieses Kontingent angewendet wird
Kontingentdefinition	Name der Kontingentdefinition, die Sie anwenden
Katalogelement	Katalogelement oder Cloud-Ressource, das/die Sie dem Kontingent zuordnen

12. Klicken Sie auf **Absenden**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ergebnisse
Sie haben die Cloud-Kontingentdefinitionen und Kontingentgrenzen für Benutzer und Benutzergruppen festgelegt.

Zugehörige Informationen

Ressourcenblöcke in Cloud Provisioning and Governance

Steuerungen für Ressourcenbestellungen für vorlagenbasierte Cloud-Katalogelemente

Verwenden Sie Steuerungen für Ressourcenbestellungen, um mithilfe von Kontingentdefinitionen und -richtlinien Kontingentprüfungen für vorlagenbasierte Katalogelemente durchzuführen. Mit Kontingentgrenzen können Sie die Bereitstellung oder Bestellung von Ressourcen für Benutzer und Gruppen steuern. Konfigurieren Sie Richtlinienaktionen, um Benachrichtigungen und/oder einen Genehmigungs-Workflow auszulösen.

Steuerungen für Ressourcenbestellungen

Mit Steuerungen für die Ressourcenreihenfolge können Sie das Quotenlimit von Ressourcen steuern, die über vorlagenbasierte Kataloge bereitgestellt werden. Kontingentprüfungen für auf Cloud-Vorlagen basierende Katalogelemente sind ab Release Yokohama verfügbar.

Sie können Kontingentgrenzen jetzt vorlagenbasierten Katalogen zuordnen und Benachrichtigungen oder einen Genehmigungs-Workflow auslösen, wenn die von Ihnen für einen Benutzer oder eine Benutzergruppe angegebenen Ressourcengrenzen oder Kontingentdefinitionen überschritten werden. Weitere Informationen finden Sie unter Ressourcenkontingent.

Verwenden Sie Ressourcensteuerungen, um die folgenden Aktionen auszuführen:

- Berechnen Sie das Kontingent und die Kapazität für vorlagenbasierte Katalogelemente.
- Legen Sie bei der Bereitstellung für Cloud-Benutzer Grenzen für das Stapelkontingent fest.
- Erstellen Sie eine Richtlinie, die ausgelöst werden soll, wenn eine Kontingentgrenze überschritten wird.
- Fügen Sie eine Richtlinienbenachrichtigung und eine Anforderung zur Genehmigung bei Überschreiten einer Kontingentgrenze hinzu.
- Zeigen Sie im Cloud-Benutzerportal Benutzer- und Benutzergruppenkontingente für vorlagenbasierte Kataloge an.

Funktionsweise von Steuerungen für Ressourcenbestellungen

Steuerungen für Ressourcenbestellungen werden nur angewendet, wenn das Kontingent überschritten wurde. Wenn das Kontingent während der Katalogbereitstellung zum ersten Mal überschritten wird, nachdem Steuerelemente für Ressourcenbestellungen konfiguriert wurden, werden die Cloud-Ressourcen weiterhin bereitgestellt. Wenn Cloud-Benutzer jedoch erneut versuchen, eine Ressource bereitzustellen, bei der die konfigurierten Kontingentgrenzen überschritten werden, wird die für die Richtlinie zur Steuerung von Ressourcenbestellungen eingerichtete Richtlinienaktion „bei Ressourcengrenzen überschritten“ ausgelöst.

Hinweis: Wenn einem vorlagenbasierten Katalog kein Kontingent zugeordnet ist, finden für diesen Katalog keine Kontingentberechnungen statt, selbst wenn Benutzer ihre Kontingentgrenzen überschreiten.

Angenommen, Sie geben eine Kontingentgrenze von 20 GB für ein Speichervolume eines Cloud-Benutzers an, und der Benutzer stellt ein Speichervolume mit 40 GB bereit. Beim ersten

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mal wird das Speichervolume bereitgestellt, obwohl die Kontingentgrenze überschritten wird. Die Bereitstellung schlägt jedoch fehl, wenn der Benutzer das nächste Mal versucht, eine Cloud-Ressource mit mehr als 20 GB bereitzustellen.

Stapelanzahl-Kontingent

Mit dem Stapelanzahl-Kontingent wird im Basissystem ein Standardkontingent für vorlagenbasierte Cloud-Katalogelemente eingeführt. Für das Stapelanzahl-Kontingent werden alle aktiven Stapel (identifiziert durch die CI-Klasse *Stack*) gezählt, die von Benutzern und Benutzergruppen bereitgestellt werden. Das Stapelanzahl-Kontingent gilt für alle vorlagenbasierten Cloud-Ressourcen. Sie müssen dabei keine Katalogelemente zu bestehenden Kontingentdefinitionen zuordnen. Sobald das Stapelkontingent aktiviert ist, wird das Kontingent jedes Mal berechnet, wenn ein Benutzer aus der Gruppe, die dem Stapelkontingent zugeordnet ist, eine Cloud-Ressource bereitstellt. Wenn Benutzer aus der zugeordneten Gruppe versuchen, Ressourcen über das festgelegte Stapelkontingent hinaus bereitzustellen, werden die Richtlinie zur Steuerung von Ressourcenbestellungen und die Richtlinienaktion *on Resource Limit exceeded* ausgelöst.

Hinweis: Das im Basissystem bestehende Stapelanzahl-Kontingent beinhaltet keine vordefinierten Standardkontingente, mit denen vor dem Upgrade auf Yokohama erstellte Stapel beibehalten werden. Um das Stapelanzahl-Kontingent zu aktivieren, müssen Sie standardmäßige Kontingentgrenzen für Benutzer und Benutzergruppen festlegen.

Richtlinie zur Steuerung von Ressourcenbestellungen

Die Richtlinie zur Steuerung von Ressourcenbestellungen ist eine Basissystem-Richtlinie, die standardmäßig den Status „Entwurf“ aufweist. Sie können die Standardrichtlinie an Ihre Anforderungen anpassen und sie veröffentlichen oder eine neue Richtlinie erstellen und Kontingente, Regeln und Aktionen definieren, um Steuerungen für Ressourcenbestellungen zu aktivieren. Die Richtlinienaktion „bei Ressourcengrenzen überschritten“ löst die Anwendung der Richtlinie zur Steuerung von Ressourcenbestellungen aus, sobald bei einer Ressource die definierte Kontingentgrenze überschritten wird. Sie können festlegen, ob ein Genehmigungs-Workflow, eine Benachrichtigung oder eine Kombination aus beidem initiiert werden soll, wenn die Richtlinie „Ressourcengrenze überschritten“ ausgelöst wird. Weitere Informationen finden Sie unter Aktion für eine Richtlinie „bei Ressourcengrenzen überschritten“ erstellen.

Hinweis: Sobald das Kontingent des Benutzers oder der Benutzergruppe überschritten wurde, können Sie nur dann Katalogelemente bereitstellen, wenn die Richtlinie veröffentlicht wird. Das liegt daran, dass das aktuelle Systemverhalten von Kontingenten eine weitere Bereitstellung verhindert und die Anforderung nicht weiter verarbeitet.

Nächste Schritte

Steuerungen für Ressourcenbestellungen einrichten

Erstellen Sie Kontingentdefinitionen und Richtlinien, die auf Cloud-Vorlagen basierenden Katalogelementen zugeordnet sind. Verwenden Sie Richtlinienregeln und Aktionen, um einen Genehmigungs-Workflow oder eine Benachrichtigung auszulösen, wenn die für die Gruppe oder den Benutzer definierte Kontingentgrenze überschritten wird.

Vorbereitungen
Voraussetzungen:

- Mindestens eine Cloud-Richtliniengruppe
- Auf Cloud-Vorlagen basierende Katalogelemente

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Stellen Sie sicher, dass Ihre CMDB durch eine ereignisgesteuerte Discovery aktualisiert wird, um eine präzise Durchsetzung des Kontingents zu gewährleisten.
- Stellen Sie sicher, dass Sie beim Konfigurieren von Kontingentdefinitionen einem Katalog in der zugehörigen Liste „Cloud-Vorlagenressourcen“ ein Kontingent zuordnen.

Erforderliche Rolle: sn_cmp.cloud_governor

Warum und wann dieser Vorgang ausgeführt wird

Beachten Sie Folgendes, bevor Sie mit der Einrichtung von Steuerungen für Ressourcenbestellungen beginnen:

- Das Kontingent wird nur für die Ressourcenblöcke berechnet, die an eine CI-Klasse in der CMDB gebunden sind. Wenn Sie benutzerdefinierte Ressourcenblöcke erstellen, die der CI-Klasse in der CMDB nicht zugeordnet sind, findet für diese Ressourcentypen keine Kontingentberechnung statt.
- Wenn Sie sowohl die Richtlinie „Resource Order Control“ (Steuerung von Ressourcenbestellungen) als auch eine Genehmigungsrichtlinie „bei Blaupausenbereitstellung“ konfiguriert haben, hat die Genehmigungsrichtlinie „bei Blaupausenbereitstellung“ Vorrang vor der Genehmigungsrichtlinie zur Steuerung von Ressourcenbestellungen.

Prozedur

1. Definieren Sie das Kontingent, oder verwenden Sie eine Kontingentdefinition des Basissystems für einen Ressourcenblock.

   a. Navigieren Sie im Cloud-Administrationsportal zu **Bedingungen** > **Quote** > **Kontingentdefinition**.

   b. Legen Sie Kontingentdefinitionen fest.

   Für die Basissystem-Richtlinie „Resource Order Control“ (Steuerung von Ressourcenbestellungen) ist standardmäßig die ServiceNow-Standardregel für Genehmigungsrichtlinien konfiguriert. Falls Sie andere Aktionen wie Benachrichtigungen oder einen benutzerdefinierten Genehmigungs-Workflow auslösen möchten, wenn die Ressourcengrenze überschritten wird, können Sie entweder die Richtlinienaktion des Basissystems ändern oder eine benutzerdefinierte Richtlinie für Ihre Instanz erstellen.

   - Ändern Sie eine Kontingentdefinition des Basissystems, indem Sie die Werte der Standardkontingente pro Benutzer und Benutzergruppe und die Benutzergruppen festlegen, für die das jeweils definierte Kontingent gilt.

     Für die folgenden vordefinierten Basissystemkontingente sind Standardkontingente definiert:

     - *VM_Count*
     - *vCPUs Count*
     - *StorageVolume_Size*
     - *Stack_Count*
     - *Network_Count*

     Wichtig: *Stack_Count* gilt nur für vorlagenbasierte Cloud-Ressourcen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Erstellen Sie eine Kontingentdefinition.

  Weitere Informationen finden Sie unter Cloud-Kontingentdefinition erstellen.

2. Ordnen Sie das Kontingent einem vorlagenbasierten Cloud-Katalogelement zu.

   Wichtig: Wenn vorlagenbasierten Katalogen beim Konfigurieren von Kontingentdefinitionen keine Kontingente zugeordnet werden, finden für die betreffenden Kataloge keine Kontingentberechnungen statt, selbst wenn benutzerdefinierte Kontingente überschritten werden. Weitere Informationen finden Sie unter Cloud-Kontingentdefinition erstellen

   a. Klicken Sie in der zugehörigen Liste „Cloud-Vorlagenressourcen“ auf **Neu**.

   b. Wählen Sie im Feld **Katalogelement** das Katalogelement aus, dem Sie diese Kontingentdefinition zuordnen möchten.

   c. Klicken Sie auf **Absenden**.

3. Konfigurieren Sie eine Richtlinienregel.

   a. Navigieren zu **Bedingungen** > **Richtlinien**.

   b. Öffnen Sie die Basissystem-Richtlinie Resource Order Control (Steuerung von Ressourcenbestellungen).
   Die Basissystem-Richtlinie „Resource Order Control“ (Steuerung von Ressourcenbestellungen) weist standardmäßig den Status „Entwurf“ auf.

   c. Navigieren Sie zur zugehörigen Liste „Regeln“, und ändern Sie entweder eine Basissystemregel, oder konfigurieren Sie eine neue Regel, wenn es zahlreiche Anpassungen gibt.

   - Wählen Sie die Basissystemregel *approveresourcelimit* aus, und ändern Sie diese, um eine Richtlinienaktion hinzuzufügen, durch die ein benutzerdefinierter Workflow oder eine Benachrichtigung ausgelöst werden.

     Hinweis: Standardmäßig ist für die Regel *approveresourcelimit* nur die ServiceNow-Genehmigungsaktion konfiguriert.

   - Klicken Sie auf **Neu**, und konfigurieren Sie eine neue Richtlinienregel.

     Weitere Informationen finden Sie unter Cloud-Richtlinienregeln konfigurieren.

4. Konfigurieren Sie eine Richtlinien-Regelaktion.
   - Wählen Sie in der zugehörigen Liste „Richtlinien-Regelaktionen“ die im Basissystem verfügbare Genehmigungsrichtlinien-Regelaktion aus, um eine Benachrichtigung oder einen benutzerdefinierten Genehmigungs-Workflow einzubeziehen.
   - Erstellen Sie in der zugehörigen Liste „Richtlinien-Regelaktionen“ eine Cloud-Richtlinien-Regelaktion, um benutzerdefinierte Genehmigungs-Workflows oder Benachrichtigungen auszulösen, wenn Sie im vorherigen Schritt eine Richtlinienregel erstellt haben.

     Weitere Informationen hierzu finden Sie unter Aktion für Richtlinie „bei überschrittenem Ressourcenlimit“ erstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Vergewissern Sie sich, dass im Feld **Richtliniengruppe** die Richtliniengruppe ausgewählt ist, für die diese Richtlinie gelten soll.

5. Veröffentlichen Sie die Richtlinie, um Steuerungen für Ressourcenbestellungen zu aktivieren, indem Sie auf **Aktualisieren** und dann auf **Veröffentlichen** klicken.

Ergebnisse

Je nach Richtlinien-Regelaktion, die Sie für die Richtlinie zur Steuerung von Ressourcenbestellungen konfiguriert haben, wird bei Überschreiten des festgelegten Kontingents entweder eine E-Mail-Benachrichtigung oder ein Genehmigungs-Workflow oder beides ausgelöst.
Wenn Sie eine Genehmigungsrichtlinie konfiguriert haben, erhält die anfordernde Person eine Benachrichtigung, dass die Genehmigungsanforderung bei Überschreitung des festgelegten Kontingents an einen zuständigen Genehmiger gesendet wurde. In der Regel hat der zugewiesene Genehmiger die Vorlage angelegt, die zum Erstellen der Cloud-Ressource verwendet wird, und verfügt über die Rolle *sn_cmp.cloud_service_designer*.

Dashboard für Cloud-Vorgänge anzeigen

Das Dashboard für Cloud-Vorgänge schlüsselt Cloud-Serviceanforderungen Ihrer Endbenutzer und Cloud-Stapel auf, die Sie im Cloudbenutzerportal anbieten.

Vorbereitungen

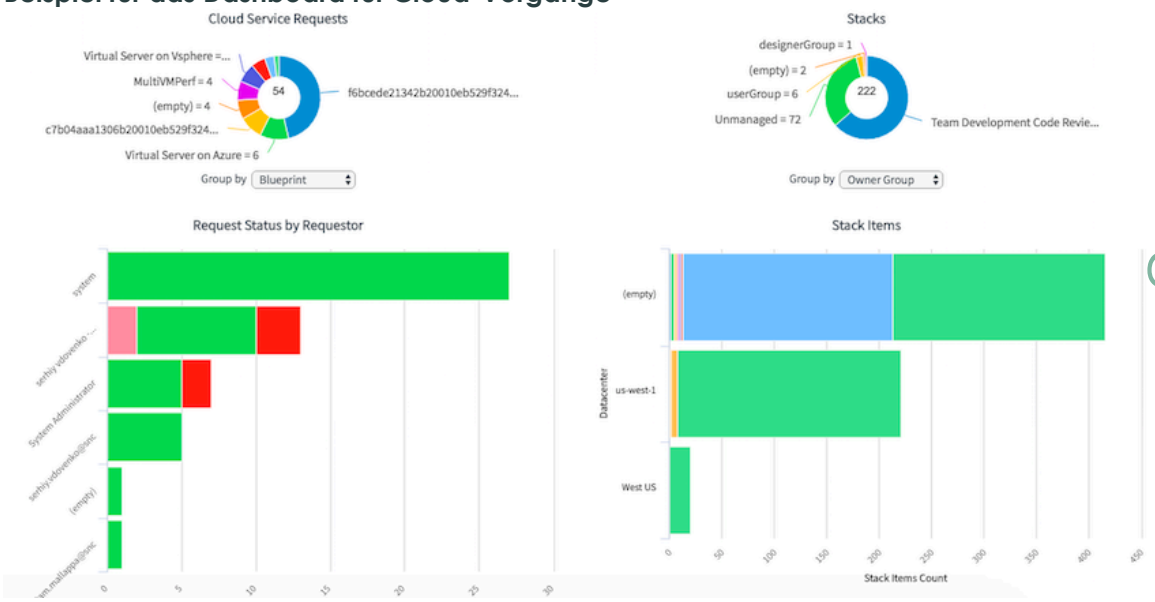
Erforderliche Rolle: sn_cmp.cloud_operator oder sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Betreiben** > **Dashboard für Cloud-Vorgänge**.

   Das Dashboard für Cloud-Vorgänge wird mit Cloud-Serviceanforderungen und Stapeln angezeigt. Anforderungen werden im Balkendiagramm unten auch nach anfordernder Person aufgeschlüsselt. Stapel werden nach Rechenzentren aufgeschlüsselt.

Beispiel für das Dashboard für Cloud-Vorgänge



2. Führen Sie einen der folgenden Schritte aus, um die Tag-Daten zu erhalten, die Sie für den Bericht benötigen:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ziel	Aktion
Daten nach einem anderen Attribut gruppiert anzeigen	Wählen Sie einen Wert in der Auswahlliste **Gruppieren nach** unter einem Diagramm aus.
Aktualisierte Daten anzeigen	Zeigen Sie auf eines der Diagramme, bis das Aktualisierungssymbol ( ) angezeigt wird, und klicken Sie dann auf das Symbol.
Speichern Sie ein Bild eines Diagramms	Zeigen Sie auf eines der Diagramme, bis das Optionssymbol angezeigt wird ( ), und wählen Sie **Als PNG speichern** oder **Als JPEG speichern** aus.

Berichte zur Cloud-Ursachenanalyse verwenden

Berichte zur Ursachenanalyse helfen Ihnen bei der Problembehandlung in Cloud Provisioning and Governance. Verwenden Sie die Berichte, um Details zum Cloud-Orchestrierungspfad und zum Cloud API-Pfad anzuzeigen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_operator oder sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Betreiben** > **Ursachenanalyse-Dashboard**.

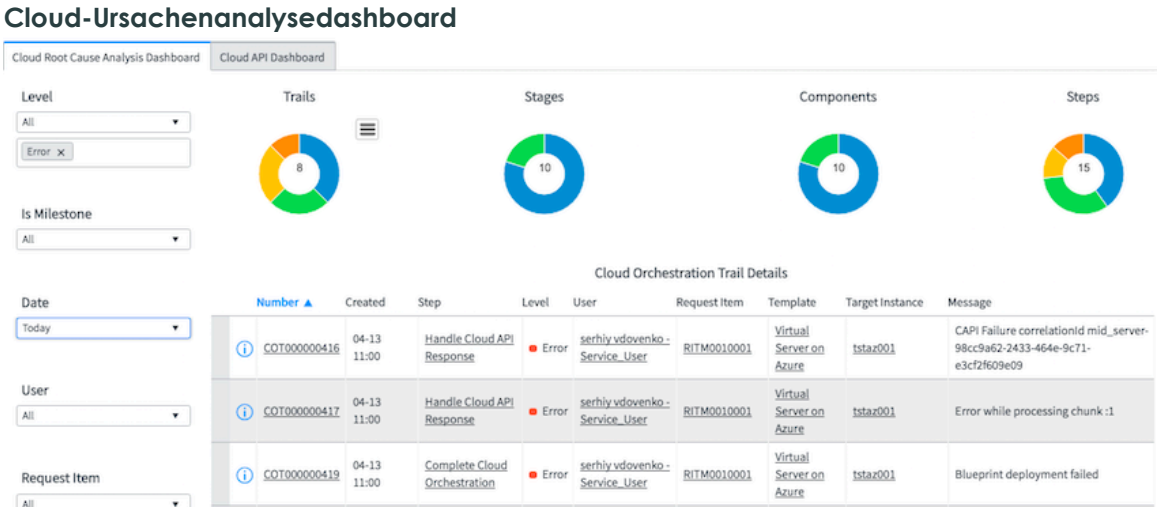
   Das Ursachenanalysedashboard wird standardmäßig mit dem **Cloud-Ursachenanalysedashboard** angezeigt. Dadurch erhalten Sie eine grafische Zusammenfassung des Cloud-Orchestrierungspfads mit Pfaddatensätzen unter den Berichten. In diesen Diagrammen sind Datensätze nach verschiedenen Attributen gruppiert:

   - **Pfade**: Gruppiert Daten nach der Vorlage, der Komponente, z. B. einem Ressourcenblock oder einer Blaupause, für die eine Cloud Provisioning and Governance-Aktion angewendet wurde.
   - **Phasen**: Gruppiert Daten nach der Phase, die angibt, wann die Transaktion stattgefunden hat.
   - **Komponenten**: Gruppiert Daten nach der Komponente im System, die an der Transaktion beteiligt war.
   - **Schritte**: Gruppiert Daten nach dem beschreibenden Schritt, der einer Phase und einer Komponente zugeordnet ist.

   Unter Cloud-Orchestrierungspfad finden Sie eine Liste der möglichen Schritte.

   Anforderungen werden im Balkendiagramm unten auch nach anfordernder Person aufgeschlüsselt. Stapel werden nach Rechenzentren aufgeschlüsselt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



2. Wählen Sie eine Option aus, um die gewünschten Tag-Daten im Bericht zu erhalten.

Ziel	Aktion
Daten filtern	Wählen Sie eine der Optionen aus, z. B. **Ebene**, **Datum** oder **Anforderungselement**.
Aktualisierte Daten anzeigen	Zeigen Sie auf den oberen Rand eines Diagramms, bis das Aktualisierungssymbol ( ) angezeigt wird, und klicken Sie dann auf das Symbol.
Speichern Sie ein Bild eines Diagramms	Zeigen Sie auf eines der Diagramme, bis das Optionssymbol ( ) angezeigt wird, und wählen Sie dann **Als PNG speichern** oder **Als JPEG speichern aus**.

3. Klicken Sie auf die **Nummer** einer beliebigen Cloud-Orchestrierungs-API, um diesen bestimmten Datensatz anzuzeigen.
Siehe Cloud-Orchestrierungspfad für Feldbeschreibungen.

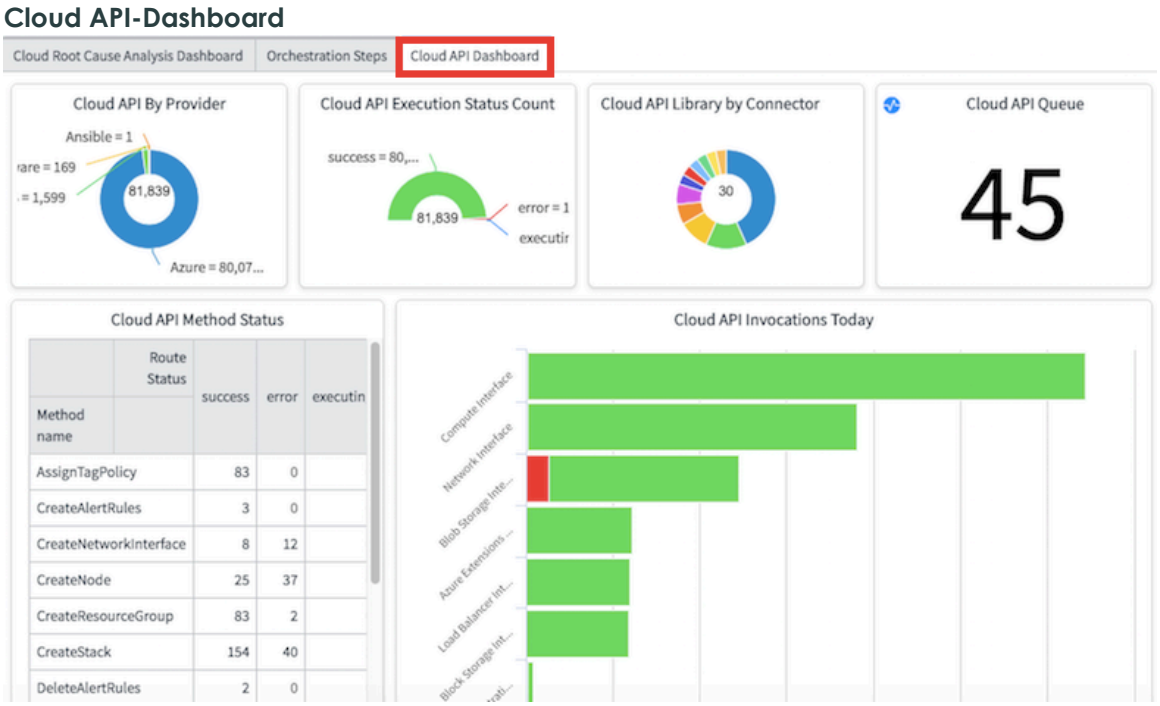
4. Zum Anzeigen von Berichten zum Cloud API-Pfad klicken Sie auf die Registerkarte **Cloud API-Dashboard**.

Dieses Dashboard zeigt Ihnen mehrere Berichte für den Cloud API-Pfad, gruppiert nach Provider, Status und Connectors. Sie können auch Informationen zu den Methoden und APIs sehen, die heute aufgerufen wurden.

Hinweis:

Ab Yokohama wird das Cloud-API-Dashboard ausgeblendet und bei neuen Instanzen nicht mehr aktiviert, es wird jedoch weiterhin unterstützt. Die Anwendung „Cloud-Servicekatalog“ bietet diese Funktionalität jetzt. Die Anwendung wird auf die zukünftige Einstellung vorbereitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf beliebige Daten in den Diagrammen, um die jeweiligen Datensätze des Cloud API-Pfads zu öffnen.
   Unter Cloud API-Pfad finden Sie Beschreibungen der Formularfelder des Cloud API-Pfads.

Cloud API-Pfad

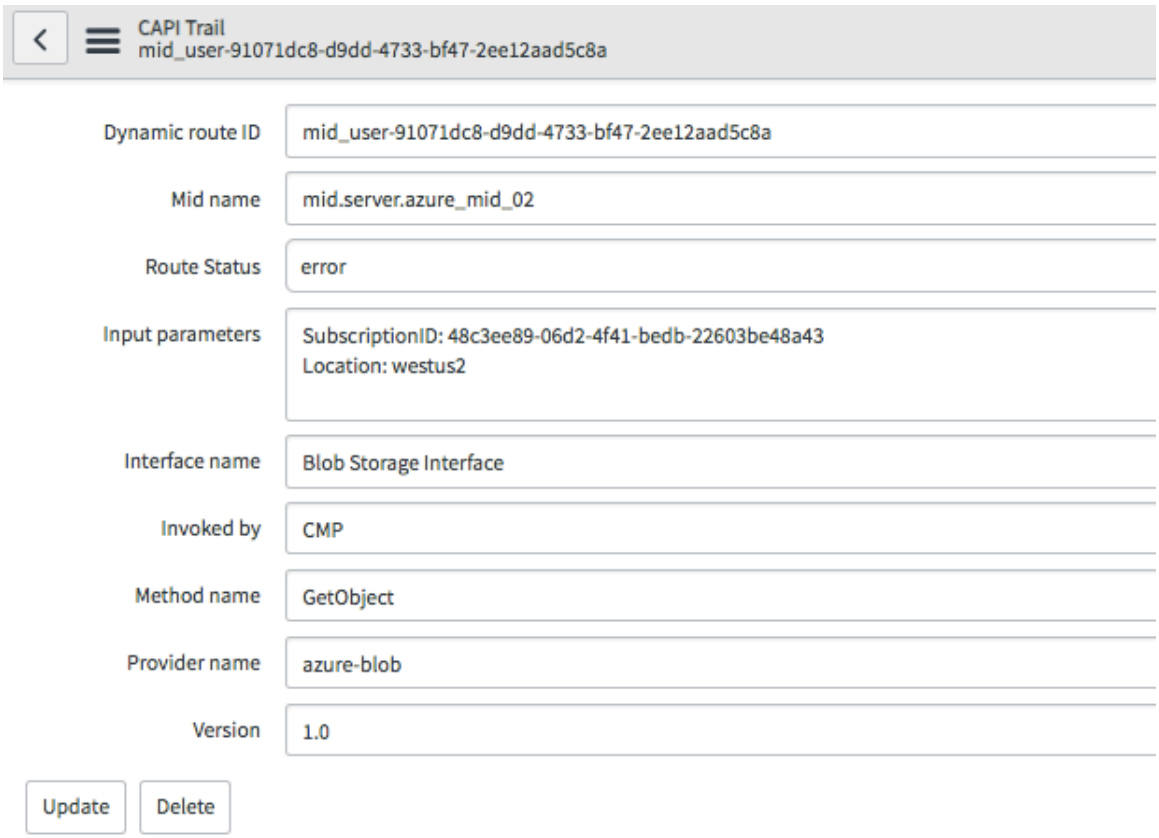
Der Cloud API-Pfad ist ein Aktivitätsprotokoll für alle Aktivitäten, die die Cloud API verwenden und den MID-Server durchlaufen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhalte des Cloud API-Pfads

CAPI-Pfadformular



Feld	Beschreibung
ID der dynamischen Route	Eine automatisch generierte ID-Nummer für den Eintrag.
MID-Name	Der Name des MID-Servers, über den die Discovery ausgeführt wurde.
Routenstatus	Gibt an, ob der von der API ausgeführte Discovery-Vorgang erfolgreich war. Mögliche Werte sind: • **Erfolg** • **Fehler** • **Wird ausgeführt**
Eingabeparameter	Der Eingabeparameter, von dem der API-Pfad-Datensatz generiert wurde. Dieser Wert ist normalerweise das Rechenzentrum, in dem Discovery ausgeführt wurde.
Schnittstellenname	
Aufgerufen durch	Dieser Wert ist immer **CMP**, wenn Discoveryausgeführt wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Methodenname	Der Schnittstellenvorgang von der Cloud-API, von der dieser Datensatz verarbeitet wurde.
Providername	Der Cloud Provider
Version	Die in der Cloud-API angegebene Version

CAPI-Pfadprotokolle

Die zugehörige Liste „CAPI-Pfadprotokolle“ enthält weitere Details zum Eintrag des Cloud API-Pfads. Die folgenden Protokollschlüsseltypen sind verfügbar:

Protokollschlüssel	Beschreibung
route_data	Informationen zu den Cloud-API-Aufrufen
dynamic_route	Informationen über die tatsächliche Route, über die die Daten geflossen sind, einschließlich URIs.
route_result	Die von der Instanz empfangene Nutzlast oder eine Beschreibung des Ergebnisses der Datenübertragung. Die Nutzlast
chunk_number	Die Anzahl der Datenblöcke, die die Instanz empfangen hat
route_status	Gibt an, ob die Routenverbindung und die Übertragung der Nutzlast erfolgreich war
route_error	Der aufgetretene Fehler. Zum Beispiel der Fehler `Failed to list loadbalancer Failed: HTTP-Fehlercode: 403` (Auflistung des Lastenausgleichsmoduls fehlgeschlagen: HTTP-Fehlercode: 403) bedeutet, dass Ihre Anmeldeinformationen falsch waren und Discovery nicht auf die Cloud-Ressource zugreifen konnte.
error_detail	Weitere Details über den Fehler, einschließlich der Cloud Provisioning and Governance-API und des entsprechenden Connectors, der beim Discovery-Versuch verwendet wurde, und die Fehler, die der Cloud Provider ausgegeben hat.

Beispiel für einen „route_error“:

```
Failed to list loadbalancer Failed : HTTP error code : 403
```

Beispiel für den Eintrag „error_detail“ für denselben Fehler:

```
com.snc.cmp.connector.cloud.loadbalancer.component.LoadBalancerException:
 Failed to list loadbalancer Failed : HTTP error code : 403
       at
 com.snc.cmp.connector.cloud.loadbalancer.customizer.impl.AWSLoadBalancer
Customizer.listLoadBalancers(AWSLoadBalancerCustomizer.java:56)
 at
 com.snc.cmp.connector.cloud.loadbalancer.component.LoadBalancerProducer.
process(LoadBalancerProducer.java:46)
 at
 org.apache.camel.util.AsyncProcessorConverterHelper$ProcessorToAsyncProc
essorBridge.process(AsyncProcessorConverterHelper.java:61)
       at
 org.apache.camel.processor.SendProcessor.process(SendProcessor.java:145)
       ...
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesen beiden Einträgen wird angegeben, dass die Anmeldeinformationen falsch waren und Discovery nicht auf die Cloud-Ressource zugreifen konnte. Die Schnittstelle des Lastenausgleichsmoduls gibt den ersten Fehler aus, da das Lastenausgleichsmodul das erste Gerät ist, das Zugriff auf die Cloud-Ressource ermöglicht. Die Fehler `org.apache.camel` weisen auf Weiterleitungsfehler aufseiten von Amazon Web Services hin.

Der entsprechende Fehler auf der Instanzseite wird im Cloud-Orchestrierungspfad erfasst.

Zugehörige Informationen

Cloud-Orchestrierungspfad

Cloud API-Pfad öffnen

Öffnen Sie den Cloud API-Pfad, um Probleme wie fehlgeschlagene Richtlinien oder fehlgeschlagene Discovery von Cloud-Ressourcen zu debuggen und zu beheben.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_operator oder sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Betreiben** > **Pfade**.
2. Auf der Registerkarte **Cloud API-Pfad** filtern und sortieren Sie die Liste der Datensätze aus dem Cloud API-Pfad nach Bedarf.
   Wenn Sie z. B. nach einer fehlgeschlagenen Discovery suchen, filtern Sie die Liste, sodass in der Spalte **Routenstatus** nur Einträge mit **Fehler** anzeigt werden.
3. Klicken Sie auf einen Link in der Spalte „Erstellt“, um den Datensatz des Cloud API-Pfads zu öffnen.
4. Öffnen Sie in der zugehörigen Liste „CAPI-Pfadprotokolle“ den Protokolldatensatz, der die gewünschten Informationen anzeigt.
   Öffnen Sie beispielsweise **route_error** oder **error_detail**, um einen fehlgeschlagenen Vorgang zu debuggen.

Dashboards und Berichte von Cloud Provisioning and Governance

Mit Dashboards können Cloud-Administratoren und Cloud-Benutzer Berichte wie Cloud-Abrechnungsdaten und Cloud Tag-Nutzung anzeigen lassen.

Demonstriert Setup-Optionen für die Abrechnung für Cloud Provisioning and Governance. Folgen Sie diesem kurzen Video, um mehr über Cloud Provisioning and Governance -Dashboards zu erfahren.

Wichtig: Ab Release Yokohama ist das Abrechnungs-Dashboard nicht mehr verfügbar, wenn Sie die App ServiceNow Store Cloud-Einblicke heruntergeladen haben. Folgendes ändert sich

- Sie werden standardmäßig zur Homepage von Cloud-Einblicke weitergeleitet.
- Das Widget „Dashboard anzeigen“ im Cloud-Benutzerportal wird durch das Widget „Ressourcen anzeigen“ ersetzt.
- Im Widget „Aktuelle Monatsausgaben“ und im Widget „Budget“ des Cloud-Benutzerportals werden keine Daten angezeigt, wenn Cloud-Einblicke in der Instanz aktiviert ist.

Cloud-Kosten auf dem Abrechnungsdashboard anzeigen

Das Abrechnungsdashboard bietet eine umfassende Informationsübersicht zur Cloud-Nutzung und zu Kostentrends sowie Kosten-Zusammenfassungen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Wichtig: Auf das **Abrechnungsdashboard** können Sie nur zugreifen, wenn Sie die App ServiceNow Store Cloud-Einblicke nicht heruntergeladen und aktiviert haben. Wenn Sie die App Cloud-Einblicke aktiviert haben, können Sie nur zum Abrechnungsdashboard navigieren, wenn Sie Cloud Provisioning and Governance in einer domänengetrennten Instanz verwenden.

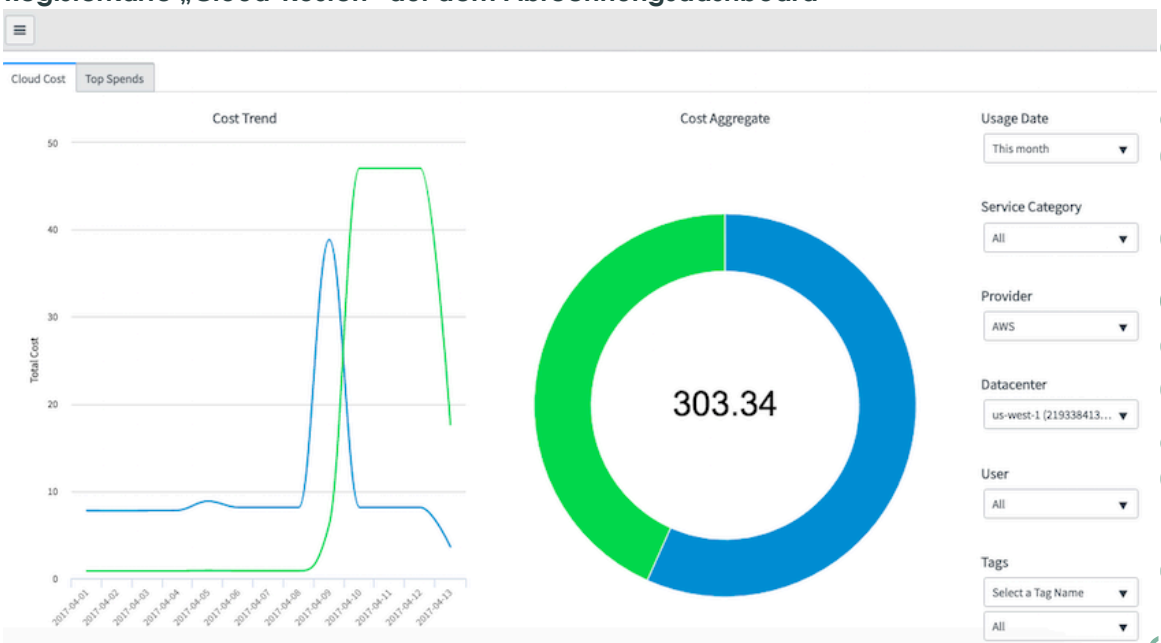
Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Analysieren** > **Abrechnung** > **Abrechungsdashboard**.

   Das Abrechnungsdashboard zeigt standardmäßig die Registerkarte **Cloud-Kosten** an. Auf dieser Registerkarte werden die folgenden zwei Diagramme angezeigt:

   - **Kostentrend**: Ein Liniendiagramm, in dem die täglichen Kosten für das ausgewählte **Nutzungsdatum** dargestellt werden.
   - **Gesamtkosten**: Gesamtkosten für jeden Tag-Wert für das ausgewählte Tag **Gruppieren nach**.

   Registerkarte „Cloud-Kosten“ auf dem Abrechnungsdashboard

2. Führen Sie eine der folgenden Aktionen aus, um die Tag-Daten zu erhalten, die Sie für den Bericht benötigen.

Ziel	Aktion
Aktualisieren Sie den Abrechnungszeitraum	Wählen Sie eine neue Option aus der Auswahlliste Verwendungsdaten.
Siehe Daten, die nach einem anderen Tag gruppiert sind	Wählen Sie einen Wert in der Auswahlliste **Gruppieren nach** unter jedem Diagramm.
Nach Tag-Werten filtern	Wählen Sie in der Liste einen Tag-Wert aus.
Speichern Sie ein Bild eines Diagramms	Zeigen Sie auf eines der Ringdiagramme, bis das Optionssymbol (☰) angezeigt wird,

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ziel	Aktion
	und wählen Sie **Als PNG speichern** oder **Als JPEG speichern** aus.

3. Um die Bereiche mit der höchsten Ausgabenstufe anzuzeigen, klicken Sie auf die Registerkarte **Höchste Ausgaben**.
   Balkendiagramme zeigen standardmäßig die Gesamtkosten für jedes Tag an. Sie können die Daten weiter nach **Servicekategorie**, **Provider** und **Rechenzentrum** filtern.
4. Klicken Sie auf einen beliebigen Teil der Diagramme, um Kostendatensätze für die ausgewählten Kriterien anzuzeigen.
   Die Listenansicht der Kostendatensätze wird angezeigt. Sie können Informationen wie die Nutzungsmenge und spezifische Kosten pro Nutzungsdatum anzeigen.

Beispiel für Kostendatensätze

Usage date	Service Category	Resource	Usage profile	Usage quantity	Cost
2017-04-08	Compute	flow-vm	Data Transfer ($0 / GB)	0.020323	0
2017-04-08	Compute	flow-vm	Data Transfer ($0.08199078 / GB)	0.02444	0.00200385
2017-04-08	Compute	flow-vm	Hourly ($0.06172149 / Hour)	24	1.48131575

Getaggte Ressourcen auf dem Tag-Dashboard anzeigen

Das Tag-Dashboard zeigt alle getaggten Ressourcen an. Verwenden Sie das Tag-Dashboard, um bestimmte Tag-Werte für eine Gruppe von Ressourcen wie Stapel oder virtuelle Computer anzuzeigen.

Vorbereitungen

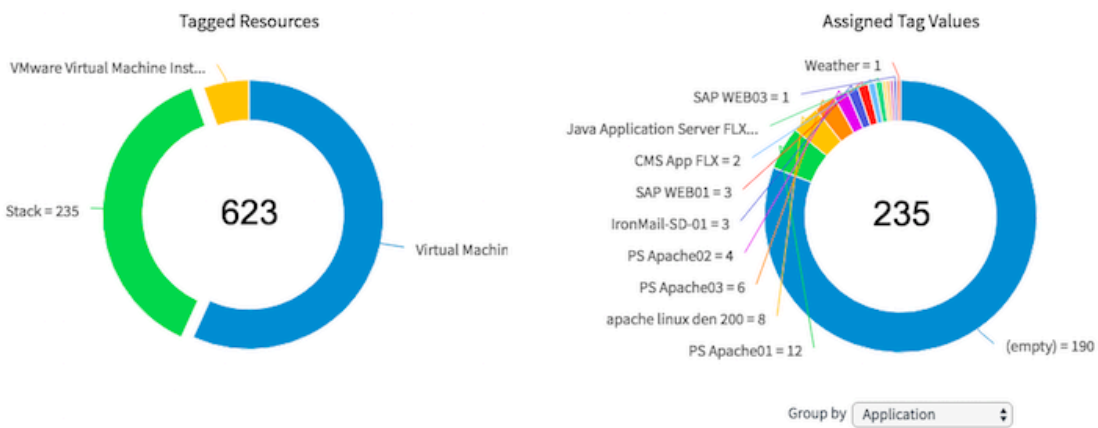
Erforderliche Rolle: sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Analysieren** > **Tag**.

   Die Registerkarte **Tag-Dashboard** zeigt das Tag-Dashboard an, auf dem alle mit Tags gekennzeichneten Ressourcen nach Tags aufgeschlüsselt sind.

Tag-Dashboard



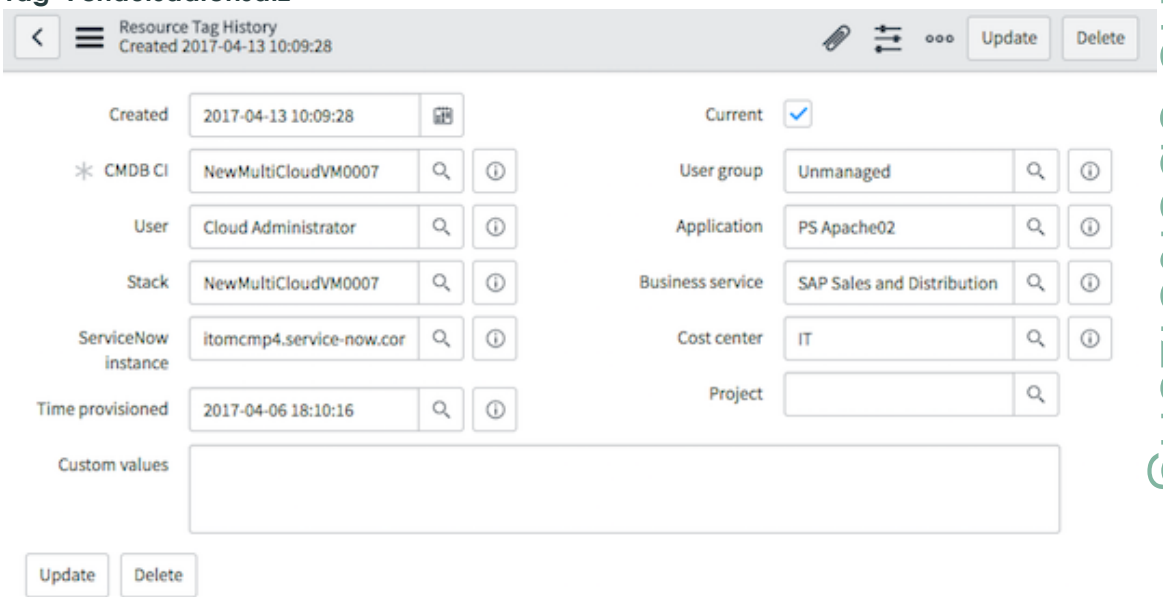
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

2. Führen Sie eine der folgenden Aktionen aus, um die Tag-Daten zu erhalten, die Sie für den Bericht benötigen.

Ziel	Aktion
Tag-Werte für eine bestimmte Ressourcengruppe ansehen	Klicken Sie auf einen Abschnitt des Ringdiagramms **Getaggte Ressourcen**.
Siehe Daten, die nach einem anderen Tag gruppiert sind	Wählen Sie einen Wert in der Auswahlliste **Gruppieren nach** unter dem Ringdiagramm **Zugewiesene Tag-Werte** aus.
Aktualisierte Daten anzeigen	Zeigen Sie auf eines der Diagramme, bis das Aktualisierungssymbol ( ) angezeigt wird, und klicken Sie dann auf das Symbol.
Speichern Sie ein Bild eines Diagramms	Zeigen Sie auf eines der Diagramme, bis das Optionssymbol ( ) angezeigt wird, und wählen Sie **Als PNG speichern** oder **Als JPEG speichern** aus.

3. Klicken Sie zum Anzeigen eines bestimmten Tag-Verlaufsdatensatzes auf einen beliebigen Abschnitt im Diagramm **Zugewiesene Tag-Werte**.
Eine Liste mit Tag-Verläufen wird angezeigt, die der CI-Klasse für den ausgewählten Tag-Wert entsprechen.

Tag-Verlaufsdatensatz



Feld	Beschreibung
Erstellt	Das Datum, an dem der Tag-Verlauf erstellt wurde.
Aktuell	Wenn ausgewählt, gibt dies an, ob der aktuelle Datensatz der aktuellste Datensatz ist.
CMDB CI	Das tatsächliche CI in der CMDB. Klicken Sie auf das Datensatzsymbol, um das CI-Formular anzuzeigen.
Benutzergruppe	Das diesem CI zugeordnete Gruppen-Tag.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Anwender	Das diesem CI zugeordnete Benutzer-Tag.
Applikation	Das diesem CI zugeordnete Anwendungs-Tag.
Stapel	Das diesem CI zugeordnete Stapel-Tag.
Business Service	Das diesem CI zugeordnete Business Service-Tag.
ServiceNow instance	Das diesem CI zugeordnete Instanz-Tag.
Kostenstelle	Das diesem CI zugeordnete Kostenstellen-Tag.
Zeit der Bereitstellung	Das Datum, an dem der Computer bereitgestellt wurde.
Projekt	Das diesem CI zugeordnete Projekt-Tag.
Benutzerdefinierte Werte	Alle diesem CI zugeordneten benutzerdefinierten Werte.

Budgetbasierte Benachrichtigung und Genehmigung

Administratoren können ein Budget für eine Gruppe und einen Benutzer innerhalb der Gruppe zuweisen. Wenn der Benutzer oder die Gruppe den Schwellenwert für das Budgetlimit erreicht, werden sie darüber benachrichtigt.

Wichtig:

- Die budgetbasierte Benachrichtigungs- und Genehmigungsfunktion ist nicht mehr verfügbar, wenn Sie für die Cloud-Abrechnung die App Cloud-Einblicke verwenden.
- Sie können die Funktion „Budgetverbrauch“ nur weiterhin verwenden, wenn Sie Cloud Provisioning and Governance in einer domänengetrennten Instanz verwenden oder wenn Sie die native Abrechnungsfunktion von Cloud Provisioning and Governance erneut aktiviert haben.

Administratoren können ein wöchentliches, monatliches, vierteljährliches oder jährliches Budget (in USD) zuweisen. Das für einen Benutzer und das für eine Gruppe festgelegte Budget sind voneinander unabhängig. Beispielsweise kann eine Gruppe mit fünf Benutzern ein Budget von 100 USD haben, und jedem Benutzer in dieser Gruppe kann ein Limit von 25 USD zugewiesen werden. Eine Organisation entscheidet über die Budgetfrequenz, und alle Gruppen in dieser Organisation folgen derselben Frequenz. Wenn sich eine Organisation beispielsweise für ein monatliches Budget entscheidet, folgen alle Gruppen und Benutzer in dieser Organisation einem monatlichen Budget. Weitere Informationen finden Sie unter Budgets konfigurieren.

Für jede neue Gruppe und jeden neuen Benutzer wird ein Standardbudget angegeben. Eine neue Gruppe erhält ein Standardbudget von 1000 USD, ein neuer Benutzer ein Standardbudget von 100 USD.

Administratoren können das Budget jederzeit erhöhen oder verringern. Wenn der Benutzer oder die Gruppe den Schwellenwert des Budgets erreicht, erfolgt eine Benachrichtigung. Benachrichtigungen werden als Teil des Abrechnungsprozesses ausgelöst. Die Discovery für die Abrechnung wird für jeden Benutzer und jede Gruppe geplant. Am Ende der Abrechnungs-Discovery wird ein Vergleich zwischen dem Budgetlimit und den tatsächlichen Kosten durchgeführt. Wenn der Schwellenwert erreicht oder überschritten wurde, werden Benachrichtigungen ausgelöst.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Administratoren können eine Richtlinie einrichten. Wenn die Budgetgrenze dann einen bestimmten Schwellenwert erreicht oder überschreitet, erteilt der Administrator eine Genehmigung für den Benutzer oder die Gruppe, die Ressourcen weiterhin zu verwenden. Beispielsweise kann der Administrator eine Richtlinie für eine Gruppe erstellen, bei der beim Erreichen von 90 % des Budgetschwellenwerts der Gruppe eine Genehmigung erforderlich ist, damit die Gruppe weiterhin Ressourcen verbrauchen kann. Wenn der Administrator keine Richtlinie für das Budget erstellt, kann der Benutzer oder die Gruppe die Ressourcen weiterhin verwenden.

Sie können die Budgetdetails im unter anzeigen **Analysieren** > **Budgetverbrauch**. Sie können sich die Details zum Budgetverbrauch für einen Benutzer oder auch für eine Gruppe ansehen.

Budgets konfigurieren

Sie können Budgets für Gruppen und für Benutzer in dieser Gruppe konfigurieren. Sie können einen Budgetzeitraum für die Gruppe einrichten und einer Gruppe und jedem Benutzer in dieser Gruppe ein Budgetlimit zuweisen.

Vorbereitungen

Erforderliche Rolle: Administrator

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Bedingungen** > **Budget**.
2. Klicken Sie neben **Budgetkonfiguration** auf **Neu**.
3. Füllen Sie die Formularfelder aus (siehe Tabelle).

Feld	Beschreibung
Gruppenname	Wählen Sie in der Liste eine Gruppe aus.
Budgetzeitraum	Wählen Sie einen Budgetzeitraum für die Gruppe aus: wöchentlich, monatlich, vierteljährlich oder jährlich.
Obergrenze für Gruppe	Geben Sie ein Budgetlimit für die Gruppe ein. Standardmäßig liegt das Budgetlimit für jede neue Gruppe bei 1000 USD.
Grenzwert pro Benutzer	Geben Sie ein Budgetlimit für jeden Benutzer in der Gruppe ein. Standardmäßig liegt das Budgetlimit für jeden neuen Benutzer bei 100 USD.

4. Klicken Sie auf **Absenden**.

Tags für Cloud-Ressourcen

Mithilfe von Tags werden Cloud-Ressourcen kategorisiert, um umfangreichere und detailliertere Nachverfolgungs- und Abrechnungsberichtsdaten bereitzustellen.

Erstellen Sie Tags, damit Cloud Provisioning and Governance Cloud-Ressourcen nach der Bereitstellung automatisch kategorisieren kann. Jedes Tag verknüpft ein bestimmtes `Schlüssel:Wert`-Paar mit einer angeforderten Cloud-Ressource, z. B. `Anwendung=HRMS`.

Nach der Bereitstellung der Cloud-Ressource werden die Schlüssel:Wert-Informationen in Tags Teil der Metadaten der Ressource und zusammen mit allen anderen Parametern der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressource gespeichert. Da eine Cloud-Ressource mehrere Tags haben kann, können Sie Kostenelemente aus mehreren Perspektiven betrachten.

Tag-Definitionen

Tag-Definitionen sind Datensätze, die einen Tag-Namen einem Werttyp zuordnen. Folgende Werttypen sind verfügbar:

Werttyp	Beschreibung
Variable	Ein Wert, den der Benutzer eingibt oder aus einer Auswahlliste auswählt. Dieser Wert wird als Servicekatalogvariable gespeichert. Wenn eine Tabelle einem Variablen-Tag zugeordnet ist, werden die Werte in dem als **Anzeigefeld** markierten Feld dem Benutzer angezeigt, wenn er die Instanz anfordert. In den meisten Fällen ist dies das Feld „Name“. Beispielsweise werden dem Benutzer die Namen der Business Services in der Tabelle „Service“ angezeigt. Wenn in der Tag-Definition keine Tabelle angegeben ist, wird dem Benutzer ein Textfeld angezeigt.
Skript	Ein Skript, das einen Wert von der Instanz abruft, z. B. die aktuelle Zeit auf der Instanz. Das Skript muss den Wert über die Basissystem-API abrufen und den Wert an die `Antwortvariable` zurückgeben. Beispiel: Das Skript zum Abrufen der aktuellen Zeit auf der Instanz lautet: `answer = new GlideDateTime().getValue();`

Standard-Tags

Diese Tags werden standardmäßig bereitgestellt.

Wichtig: Deaktivieren Sie die Standard-Tags nicht, da durch diese Aktion alle entsprechenden Katalogelementvariablen gelöscht werden.

Standard-Cloud-Tags

Bezeichnung	Name	Werttyp	Tabelle mit Auswahloptionen
Applikation	Anwendung	Variable	Anwendung [cmdb_ci_appl]
Business Service	business_service	Variable	Service [cmdb_ci_service]
Kostenstelle	cost_center	Variable	Kostenstelle [cmn_cost_center]
Projekt	Projekt	Variable	N/V
ServiceNow instance	sn_instance	Skript	N/V
Stapel	stack	Variable	Stapel [sn_cmp_stack]
Zeit der Bereitstellung	time_provisioned	Skript	N/V
Anwender	user	Auftragsfeld	Benutzer [sys_user]
Benutzergruppe	user_group	Variable	Gruppe [sys_user_group]

Cloud-Administratoren können auch benutzerdefinierte Tags erstellen, die den spezifischen Anforderungen des Unternehmens entsprechen. Beispielsweise können Sie ein Standort-Tag erstellen, um den Standort der Ressource nachzuverfolgen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Tags

Für Ressourcen in Amazon Web Services (AWS) generierte Tags werden an AWS gesendet und sind auch über die AWS-Konsole verfügbar.

Zugehörige Informationen

Getaggte Ressourcen auf dem Tag-Dashboard anzeigen

Benutzerdefiniertes Tag für Cloud-Ressourcen erstellen

Cloud-Administratoren können zur Kategorisierung von Cloud-Ressourcen zusätzlich zu den Standard-Tags benutzerdefinierte Tags erstellen.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Ressource vor dem Vorhandensein eines bestimmten Tags bereitgestellt wurde, muss dieses Tag dem Datensatz für diese Ressource manuell hinzugefügt werden.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Analysieren** > **Tag** > **Tag-Verwaltung** > **Tag-Definitionen**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder im Formular aus.

Feld	Beschreibung
Bezeichnung	Name, der Cloud-Benutzern auf dem Bildschirm angezeigt werden soll.
Name	Name des Schlüssels. Der Name wird in allen Tabellen zusammen mit dem Wert gespeichert.
Werttyp	Der Typ des Werts für dieses Tag.
Variablenname	Der Name der Variable. Diese Option wird angezeigt, wenn Sie **Variable** als Werttyp auswählen.
Tabelle [optional]	Die Tabelle, die die Auswahlmöglichkeiten für das Werttypfeld **Variable** enthält. Wählen Sie eine Tabelle aus dem System aus. Wenn Sie keine Tabelle auswählen, wird Cloud-Benutzern ein leeres Textfeld für die Variable angezeigt.
Sortierfeld	Das Feld auf dem Anforderungsformular. Klicken Sie neben **Zum Auswählen klicken** auf den Abwärtspfeil, und wählen Sie dann das Feld aus der Tabelle „Aufträge“ [sn_cmp_order] aus.
Aktiv	Ein Indikator, der angibt, ob das Tag verwendet wird. Wählen Sie diese Option aus, um das Tag auf alle neuen Anforderungen anzuwenden.

Zugehörige Informationen

Getaggte Ressourcen auf dem Tag-Dashboard anzeigen

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Abrechnungsdaten mithilfe von benutzerdefinierten Tags aus bereitgestellten Ressourcen gruppieren

Konfigurieren Sie benutzerdefinierte Tags zum Anzeigen und Analysieren von Abrechnungsdaten mithilfe von benutzerdefinierten Tags, die in bereitgestellten Ressourcen vorhanden sind.

Vorbereitungen

- Führen Sie eine Cloud Discovery in Cloud Provisioning and Governance für bereitgestellte Ressourcen durch.
- Führen Sie einen Abrechnungs-Download-Auftrag für das zugeordnete Servicekonto aus.

Erforderliche Rolle: Rolle „Beitragender bei Ressourcenrichtlinien“ im Azure-Servicekonto und sn_cmp.cloud_admin in der Instanz.

Warum und wann dieser Vorgang ausgeführt wird

Bereitgestellte Ressourcen mit vorhandenen Tags werden als Teil der Cloud Discovery erkannt. Vorhandene Tags werden in der Tag-Verwaltung als benutzerdefinierte Tags betrachtet. Standardmäßig werden die importierten (benutzerdefinierten) Tags nicht im Abrechnungsdashboard angezeigt, sodass Sie keine Abrechnungsdaten mithilfe importierter (benutzerdefinierter) Tags filtern und analysieren können.

Wichtig: Ab dem Release Rome werden die Abrechnungs- und Budgetierungsfunktionen nicht mehr unterstützt, wenn Cloud Provisioning and Governance in einer nicht domänengetrennten Instanz ausgeführt wird. Wenn Sie Cloud Provisioning and Governance jedoch in einer domänengetrennten Instanz verwenden, ändert sich die Funktionalität für Abrechnungs- und Budgetierungsfunktionen nicht.

Prozedur

1. Navigieren Sie im **Cloud-Adminportal zu Analysieren** > **Tag** > **Tag-Verwaltung**.

   Die Liste **Tag-Definitionen** zeigt erkannte Ressourcen an, die mit vorhandenen Tags versehen sind, die als „Benutzerdefiniert“ gekennzeichnet sind.

2. Öffnen Sie einen Tag-Datensatz vom Typ **Benutzerdefiniert**.
3. Ändern Sie im Formular „Tag-Definition“ das Tag von „Benutzerdefiniert“ in „ServiceNow (Benutzerdefiniert)“:
   a. Wählen Sie im Feld **Tag-Typ** die Option **ServiceNow (Benutzerdefiniert)** aus.
   b. Kopieren Sie den Wert aus dem Feld **Bezeichnung** in das Feld **Variable**.
   c. Aktivieren Sie die Kontrollkästchen **Aktiv** und **Sichtbar**.
   d. Wählen Sie **Aktualisieren**.
4. Wiederholen Sie die Schritte 2 und 3 für alle benutzerdefinierten Tags, die Sie im Abrechnungsdashboard aktivieren möchten.
5. Führen Sie Cloud Discovery erneut aus, um aktualisierte Tags des Typs „ServiceNow (Benutzerdefiniert)“ anzuzeigen.

   Weitere Informationen finden Sie unter Cloud-Discovery.

6. Führen Sie den Abrechnungszeitplan aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren Sie im **Cloud-Adminportal zu Analysieren** > **Abrechnung** > **Abrechnungszeitplan**.

b. Erstellen Sie einen Zeitplan, oder öffnen Sie einen vorhandenen Zeitplan.

c. Wählen Sie **Jetzt ausführen**.

d. Wählen Sie im Fenster **Abrechnungsdaten abrufen** einen Datumsbereich aus, und klicken Sie dann auf **Herunterladen**.

Die Tags vom Typ ServiceNow (Benutzerdefiniert) werden jetzt im Feld „Tags“ des Abrechnungsdashboards angezeigt.

Nächste Maßnahme

Lassen Sie Cloud-Kosten auf dem Abrechnungsdashboard anzeigen.

Lebenszyklusvorgänge für erkannte Ressourcen konfigurieren und durchführen

Konfigurieren Sie Lebenszyklusvorgänge für Cloud-Ressourcen, die nicht mit ServiceNow® Cloud Provisioning and Governance bereitgestellt wurden. Stellen Sie Ressourcen bereit, und ändern Sie Ressourcenblockvorgänge, um Tag-2-Vorgänge für Cloud-Ressourcen auszuführen, die mit Cloud-Discovery erkannt, aber nicht mit Cloud Provisioning and Governance bereitgestellt wurden.

Vorbereitungen

- Weisen Sie das Configuration Item (CI) einem Benutzer zu, der den Vorgang ausführt.
- Erforderliche Rolle: sn_cmp.cloud_service_user, root_admin, admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Wenn eine Ressource aus dem Cloud Provisioning and Governance-Katalog bereitgestellt wird, können Sie Basissystem-Lebenszyklusvorgänge für einen Stapel oder eine Ressource ausführen. Wenn jedoch eine Ressource als Teil von Cloud-Discovery erkannt und nicht von Cloud Provisioning and Governance bereitgestellt wurde, sind die gleichen Vorgänge (Starten, Stoppen, Bereitstellung aufheben) nicht standardmäßig verfügbar. Das folgende Verfahren gilt für einen Vorgang „Stoppen“ auf einem virtuellen Computer, der nicht von Cloud Provisioning and Governance bereitgestellt wurde.

Prozedur

1. Navigieren zu **Alle** > **Cloud-Adminportal** > **Entwurf** > **Ressourcenblöcke**.
2. Suchen und öffnen Sie die Ressource/das CI, für die/das Sie Lebenszyklusvorgänge ausführen möchten.
3. Stellen Sie den Umschalter auf **Entwurf**, um den Ressourcenblock bearbeitbar zu machen.
4. Im ausgewählten **Ressourcenblock** > **Vorgänge** Wählen Sie auf der Registerkarte die erforderliche **Schnittstelle** und **Operation** aus den jeweiligen Listen aus.

   Hinweis: Die Felder **Schnittstelle** und **Vorgänge** sind nur für Ressourcen verfügbar, die erkannt, aber nicht dem Katalog hinzugefügt oder darin generiert wurden.

5. Klicken Sie auf das Symbol **Vorgang überschreiben**.
6. Geben Sie im Dialogfeld **Vorgang überschreiben** einen Namen für den Schnittstellenvorgang ein.
   Das Kontrollkästchen **Neu erstellen** ist standardmäßig aktiviert.
7. Klicken Sie auf **Absenden**.
   Sie haben den ausgewählten Vorgang für die von Ihnen erstellte Schnittstelle aktiviert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

8. Klicken Sie auf dem Formular **Eingabeparameter** auf das Symbol **Eingabeparameter hinzufügen**.
9. Geben Sie für den Parameter **Name** den Wert `resourceID` ein, und klicken Sie auf **Speichern**.
   Standardmäßig wird ein vom System zugewiesener Ausdruck generiert und im Feld **Zuordnung** angezeigt.
10. Ersetzen Sie für den Parameter `ServerID` den Standardausdruck im Feld **Zuordnung** durch `${parameter.resourceId}`, und klicken Sie auf **Speichern**.
11. Navigieren zu **Vorgänge** > **Schritte** Unterregisterkarte
12. Ändern Sie auf dem Formular **Eingabe** den Wert des Parameters `NodeId` in `${parameter.resourceId}`.
13. Navigieren Sie zurück zum Formular **Eingabeparameter**, und klicken Sie auf **Katalog generieren**.
14. Stellen Sie den Umschalter auf **Veröffentlicht**, um den Ressourcenblock erneut zu veröffentlichen.
    Sie haben den Ressourcenvorgang für diese Ressource/dieses CI konfiguriert.
15. Wahlweise: Navigieren zu **Cloud-Anwenderportal** > **Ressourcen** > **VM-Instanz**, und wählen Sie die VM-Instanz aus, für die Sie den Ressourcenvorgang erstellt haben.
16. Wahlweise: Wählen Sie den neuen Schnittstellenvorgang, den Sie erstellt haben, aus der Liste **Ressourcenvorgänge auswählen** aus.

Nächste Maßnahme

Navigieren Sie zu **Cloud-Anwenderportal** > **Ressourcen** > **VM-Instanz** und wählen Sie in der Liste **Select Resource Operations (Ressourcenvorgänge** auswählen) den neu erstellten Schnittstellenvorgang aus.

Musterbasierte gezielte Erkennung

Erkennen Sie automatisch neu bereitgestellte Cloud-Ressourcen und speichern Sie ihre Informationen mithilfe der musterbasierten gezielten Erkennung in der ServiceNow® ServiceNow® Configuration Management Database (CMDB).

Nachdem die Cloud die in der Ressourcenvorlage genannten Ressourcen bereitgestellt hat, z. B. Azure Resource Manager (ARM) oder CloudFormation Template (CFT), sendet sie eine Antwort an die Anwendung Cloud Provisioning and Governance. Die Antwort enthält Informationen zu den bereitgestellten Ressourcen. Cloud Provisioning and Governance verwendet diese Informationen, um eine Erkennung (gezielte Erkennung) zu starten und so nur die neu bereitgestellten oder geänderten Ressourcen zu erkennen und ihre Attribute in der entsprechenden CI-Klasse in der CMDB zu aktualisieren.

Die musterbasierte gezielte Erkennung bietet eine einfachere Alternative zum vorhandenen CAPI-basierten Ansatz. Cloud Provisioning and Governance verwendet Muster zur Erkennung einzelner Ressourcen, um nur die neu bereitgestellten oder geänderten Ressourcen zu erkennen. Im Gegensatz zu den anderen Mustern durchsucht das Einzelressourcen-Erkennungsmuster nicht die gesamte Cloud-Landschaft nach Änderungen. Es erkennt nur die neu bereitgestellten oder geänderten Ressourcen eines bestimmten Typs.

Die Tabelle „Cloud-Ressourcentypen“ [sn_capi_resource_type] speichert die 1:1-Zuordnung zwischen dem Ressourcentyp und dem Einzelressourcen-Erkennungsmuster, das zum Erkennen der Ressource verwendet wird. Cloud Provisioning and Governance verwendet die Tabelle sn_capi_resource_type, um das entsprechende Muster für den angegebenen Ressourcentyp zu identifizieren. Weitere Informationen zu Mustern finden Sie unter Von der ITOM-Transparenz verwendete Discovery-Muster.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im Basissystem unterstützt Cloud Provisioning and Governance die musterbasierte gezielte Erkennung für eine Vielzahl von Ressourcentypen. Bei Bedarf können Sie benutzerdefinierte Muster verwenden, die Sie für die gezielte Erkennung erstellt haben. Weitere Informationen finden Sie unter Ressourcentyp einem Einzelressourcen-Erkennungsmuster zuordnen.

Cloud Provisioning and Governance überprüft die folgenden Bedingungen, um die musterbasierte gezielte Erkennung aufzurufen:

- Die CAPI-basierte gezielte Erkennung ist für den Ressourcentyp nicht implementiert.
- Die Systemeigenschaft *sn_cmp.targeted.disco.patterns* ist auf **True** festgelegt.
- Die Tabelle sn_capi_resource_type enthält eine 1:1-Zuordnung zwischen dem Ressourcentyp und dem Einzelressourcen-Erkennungsmuster.

Wenn Sie beispielsweise CFT zur Bereitstellung eines Amazon-S3-Buckets verwenden, liest Cloud Provisioning and Governance den Ressourcentyp aus der Cloud-Antwort (AWS::S3::Bucket) und identifiziert dann das entsprechende Muster (AWS S3) aus der Tabelle sn_capi_resource_type. Dann ruft die Anwendung das Muster auf, um nur den neu bereitgestellten Amazon-S3-Bucket zu erkennen und seine Attribute in der entsprechenden CI-Klasse in der CMDB zu aktualisieren (Tabelle „Cloud-Objektspeicher“ [cmbd_ci_cloud_object_storage]).

Wenn für den Ressourcentyp sowohl eine CAPI-basierte gezielte Erkennung als auch eine musterbasierte gezielte Erkennung implementiert ist, verwendet das System die CAPI-basierte gezielte Erkennung.

Wenn für den Ressourcentyp keine CAPI-basierte und musterbasierte gezielte Erkennung implementiert ist, wird der Ressourcentyp in der Tabelle „Cloud-Ressourcen“ [cmdb_ci_cmp_resource] als generische Cloud-Ressource klassifiziert. In solchen Fällen können Sie ein Einzelressourcen-Erkennungsmuster erstellen und es dem Ressourcentyp zuordnen. Weitere Informationen finden Sie unter Muster erstellen oder anpassen und Ressourcentyp einem Einzelressourcen-Erkennungsmuster zuordnen.

Zugehörige Informationen

Antwortprozessor konfigurieren

Eine CAPI-Schnittstelle erstellen oder erweitern

Ressourcentyp einem Einzelressourcen-Erkennungsmuster zuordnen

Definieren Sie eine 1:1-Zuordnung zwischen dem Ressourcentyp und dem Einzelressourcen-Erkennungsmuster in der Tabelle „Cloud-Ressourcentypen“ [sn_capi_resource_type]. Die Funktion der musterbasierten gezielten Erkennung verwendet diese Informationen, um das entsprechende Muster aufzurufen und die bereitgestellte Ressource zu erkennen.

Vorbereitungen

- Vergewissern Sie sich, dass die Anwendung Cloud Provisioning and Governance bereitgestellt wurde.
- Stellen Sie sicher, dass die neuesten Versionen von Discovery und Service-Mapping installiert sind.
- Vergewissern Sie sich, dass der Anwendungsbereich „Cloud-API“ ist.

Erforderliche Rolle: sn_cmp.cloud_service_designer oder sn_cmp.cloud_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Navigieren Sie zur Tabelle sn_capi_resource_type.
2. Wählen Sie den entsprechenden Ressourcentyp-Datensatz aus.
3. Füllen Sie die Felder des Formulars aus.

   Die in dieser Tabelle angegebenen Beispielwerte stellen eine 1:1-Beziehung zwischen dem Ressourcentyp AWS::S3::Bucket und dem entsprechenden Einzelressourcen-Erkennungsmuster (Amazon AWS S3) her.

Feld	Beschreibung
Name	Cloud-Ressourcentyp, den Sie erkennen möchten. Beispiel: AWS::S3::Bucket
Produkt	(Optional) Produktkategorie. Beispiel: AWS Simple Storage Service
CI-Klasse	Name der CI-Tabelle in der CMDB. Das System schreibt die erkannten Informationen in diese Tabelle. Beispiel: Cloud-Objektspeicher [cmdb_ci_cloud_object_storage]
Muster	Ein Einzelressourcen-Erkennungsmuster zum Erkennen der Ressource. Beispiel: Amazon AWS S3
Abhängigkeitssequenz	(Optional) Reihenfolge zum Auslösen des Musters.

4. Wählen Sie **Aktualisieren**.

Tools zur Problembehandlung für Cloud Provisioning and Governance

Die Anwendung Cloud Provisioning and Governance bietet mehrere Tools zur Behebung von Fehlern, die bei der Discovery von Cloud-Konten, der Bereitstellung und Verwaltung von Cloud-Ressourcen und der Aktualisierung der CMDB auftreten können.

Diese Tools zur Problembehandlung sind verfügbar:

Cloud-Orchestrierungspfad

Der Cloud-Orchestrierungspfad ist ein Aktivitätsprotokoll für alle Cloud-Ressourcenaktivitäten auf der Instanz. Verwenden Sie den Cloud-Orchestrierungspfad, um nach Fehlern zu suchen, die bei Cloud-Ressourcen auftreten, wie z. B. Anmeldeinformationsfehler bei Discovery oder API-Ausführungsfehler.

Anweisungen dazu finden Sie unter Cloud-Orchestrierungspfad öffnen.

Cloud-API-Pfad

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Cloud API-Pfad ist ein Aktivitätsprotokoll für alle Aktivitäten, die die Cloud API verwenden und den MID-Server durchlaufen. Verwenden Sie den Cloud API-Pfad, um API-Aufrufe und -Fehler im Zusammenhang mit weitergeleiteten Daten, spezifischen API-Routenfehlern und Java-Laufzeitausnahmen anzuzeigen.

Anweisungen dazu finden Sie unter Cloud API-Pfad öffnen.

Ursachenanalysedashboard

Das Ursachenanalysedashboard fasst Datensätze aus dem Cloud-Orchestrierungspfad und dem Cloud API-Pfad zusammen und stellt sie in nützlichen, filterbaren Listen und Diagrammen dar.

Anweisungen dazu finden Sie unter Berichte zur Cloud-Ursachenanalyse verwenden.

Cloud-Orchestrierungen

Cloud-Orchestrierungen sind die Aufträge, die Ihre Instanz für jeden versuchten Vorgang für einen Stapel verarbeitet hat. Verwenden Sie Datensätze der Cloud-Orchestrierung, um Statusnachrichten zu Vorgängen anzuzeigen, die für Cloud-Ressourcen ausgeführt wurden, und um Details zu jedem API-Schritt abzurufen.

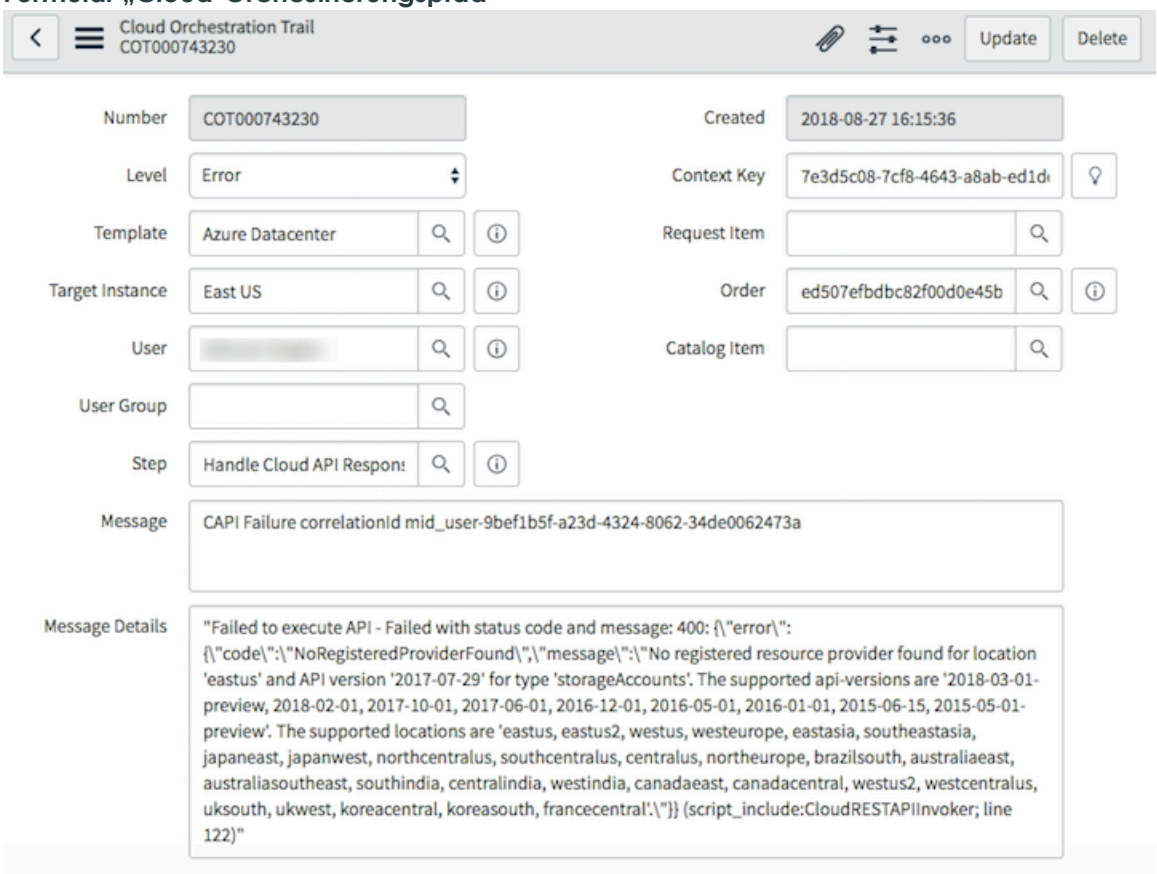
Anweisungen dazu finden Sie unter Cloud-Orchestrierungen öffnen.

Cloud-Orchestrierungspfad

Der Cloud-Orchestrierungspfad ist ein Aktivitätsprotokoll für alle Cloud-Ressourcenaktivitäten auf der Instanz.

Inhalt von Cloud-Orchestrierungspfaden

Formular „Cloud-Orchestrierungspfad“



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Nummer	Eine automatisch generierte Nummer für den Pfadeintrag
Ebene	Eine der folgenden Möglichkeiten: • Debuggen • Info • Warnen • Fehler
Vorlage	Die Komponente, z. B. ein Ressourcenblock oder eine Blaupause, auf die eine Cloud Provisioning and Governance-Aktion angewendet wurde
Vorlageninstanz	Das Rechenzentrum, in dem sich die Cloud-Ressource befindet
Anwender	Der an der Transaktion beteiligte Benutzer
Benutzergruppe	Die Benutzergruppe, zu der der Benutzer gehört
Erstellt	Zeitpunkt (Datum und Uhrzeit), zu dem der Eintrag vom System erstellt wurde
Meilenstein	Gibt an, ob diese Transaktion ein Meilenstein ist. Sie können das Formular so konfigurieren, dass Sie dieses Feld sehen.
Anforderungselement	Die für die Transaktion generierte Service Catalog-Anforderung
Schritt	Der Schritt, bei dem zusätzliche Informationen über die Transaktion identifiziert werden, einschließlich der Komponente und der Phase. Sie können das Formular so konfigurieren, dass Sie dieses Feld sehen.
Katalogelement	Das Katalogelement (sofern vorhanden), das an der Ausführung beteiligt war
Nachricht	Die Fehlermeldung oder die Nachricht über den erfolgreichen Abschluss. Diese kann Elemente wie die ID der entsprechenden Nachricht im Cloud-API-Pfaddatensatz oder die aufgerufene Cloud-API enthalten.
Nachrichtendetails	Details zum Fehler, z. B. HTTP-Fehler

Beispiel für eine Fehlermeldung:

```
Failed to list loadbalancer Failed : HTTP error code : 403
```

Hier wird angegeben, dass die Anmeldeinformationen falsch waren und Discovery nicht auf die Cloud-Ressource zugreifen konnte. Die Schnittstelle des Lastenausgleichsmoduls gibt den ersten Fehler aus, da das Lastenausgleichsmodul das erste Gerät ist, das Zugriff auf die Cloud-Ressource ermöglicht.

Ein entsprechender Fehler auf dem MID Server wird im Cloud API-Pfad erfasst.

Schritte, Phasen und Komponenten

Jeder Eintrag der Cloud-Orchestrierung verfügt über identifizierende Attribute, die erklären, worum es bei der auslösenden Transaktion ging. Schritte gruppieren diese Attribute und identifizieren die Komponente im System, die an der Transaktion beteiligt war, sowie die Phase, in der die Transaktion stattfand.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sie können das Formular „Cloud-Orchestrierungspfad“ so konfigurieren, dass das Feld **Schritt** angezeigt wird, wenn es noch nicht sichtbar ist.

Schritt	Komponente	Phase
API-Parameter anwenden	CAPI-Probe	Cloud-API-Orchestrierung
Konfigurationsparameter anwenden	CAPI-Probe	Cloud-API-Orchestrierung
Endpunktbindung anwenden	CAPI-Probe	Cloud-API-Orchestrierung
Richtlinie anwenden	Richtlinienmodul	Workflow- und Richtlinienausführung
Richtlinienregelaktion anwenden	Richtlinienmodul	Workflow- und Richtlinienausführung
Cloud-API aufrufen	BP-DSL-Executor	Cloud-Orchestrierung
Cloud API-Connector aufrufen	CAPI-Probe	Cloud-API-Orchestrierung
Cloud-Übereinstimmung überprüfen	BP-DSL-Validierung	Cloud-Orchestrierung
Rechenzentrumskapazität überprüfen	BP-DSL-Validierung	Cloud-Orchestrierung
Ressourcenblockrichtlinien überprüfen	BP-DSL-Executor	Cloud-Orchestrierung
Benutzerberechtigungen überprüfen	BP-DSL-Validierung	Cloud-Orchestrierung
Benutzerkontingent überprüfen	BP-DSL-Validierung	Cloud-Orchestrierung
Cloud-Orchestrierung abschließen	BP-DSL-Executor	Cloud-Orchestrierung
Kategorieelementrichtlinie ausführen	Dynamische Formulare	Katalogelementanforderung
Formularregeln ausführen	Dynamische Formulare	Katalogelementanforderung
Ressourcenblockvorgang ausführen	BP-DSL-Executor	Cloud-Orchestrierung
Ressourceninstanzskript ausführen	BP-DSL-Executor	Cloud-Orchestrierung
Kontingentdetails abrufen	Dynamische Formulare	Katalogelementanforderung
Antwort abrufen	CAPI-Orchestrator	Cloud-API-Orchestrierung
Cloud API-Antwort verarbeiten	BP-DSL-Executor	Cloud-Orchestrierung
Antwort der Richtlinienausführung verarbeiten	BP-DSL-Executor	Cloud-Orchestrierung
Antwort und Chunking verarbeiten	CAPI-Probe	Cloud-API-Orchestrierung
Cloud-Orchestrierung aufrufen	Workflow-Engine	Workflow- und Richtlinienausführung
Richtlinien-Engine aufrufen	Workflow-Engine	Workflow- und Richtlinienausführung
Vorprozessualen Workflow aufrufen	Workflow-Engine	Workflow- und Richtlinienausführung
Kategorieelement starten	Katalogelement	Katalogelementanforderung
Aufrufer benachrichtigen	CAPI-Orchestrator	Cloud-API-Orchestrierung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schritt	Komponente	Phase
BP-Ausführungsplan vorbereiten	BP-DSL-Executor	Cloud-Orchestrierung
Ausführbare API vorbereiten	CAPI-Orchestrator	Cloud-API-Orchestrierung
API-Routenanforderung veröffentlichen	CAPI-Orchestrator	Cloud-API-Orchestrierung
Cloud API-Antwort senden	CAPI-Probe	Cloud-API-Orchestrierung
Formular mit Filtern anzeigen	Dynamische Formulare	Katalogelementanforderung
Formular absenden	Katalogelement	Katalogelementanforderung
Eingaben validieren	BP-DSL-Validierung	Cloud-Orchestrierung

Unter Berichte zur Cloud-Ursachenanalyse verwenden finden Sie Anweisungen zum Zugriff auf Berichte im Zusammenhang mit dem Cloud-Orchestrierungspfad.

Zugehörige Informationen

Cloud API-Pfad

Cloud-Orchestrierungspfad öffnen

Öffnen Sie den Cloud-Orchestrierungspfad, um Probleme wie fehlgeschlagene Richtlinien oder fehlgeschlagene Discovery von Cloud-Ressourcen zu debuggen und zu beheben.

Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_operator oder sn_cmp.cloud_admin

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Betreiben** > **Pfade**.
2. Auf der Registerkarte **Cloud-Orchestrierungspfad** filtern und sortieren Sie die Liste der Datensätze aus dem Orchestrierungs-API-Pfad nach Bedarf.
   Wenn Sie z. B. nach einer fehlgeschlagenen Discovery suchen, filtern Sie die Liste, sodass in der Spalte **Ebene** nur Einträge mit **Fehler** anzeigt werden.
3. Klicken Sie auf einen Link in der Spalte **Erstellt**, um den Datensatz des Orchestration-API-Pfads zu öffnen.
4. Öffnen Sie in der zugehörigen Liste „CAPI-Pfadprotokolle“ den Protokolldatensatz, der die gewünschten Informationen anzeigt.
   Öffnen Sie beispielsweise **route_error** oder **error_detail**, um einen fehlgeschlagenen Vorgang zu debuggen.

Cloud-Orchestrierungen öffnen

Cloud-Orchestrierungen zeigen die Aufträge an, die Ihre Instanz für jeden versuchten Vorgang für einen Stapel verarbeitet hat. Sie zeigen auch die Werte der Felder an, die der Benutzer über das Cloudbenutzerportal gesendet hat. Verwenden Sie Cloud-Orchestrierungen zur Behebung von Problemen, die auftreten, wenn ein Benutzer eine Cloud-Ressource bereitstellt oder einen anderen Vorgang für eine vorhandene Cloud-Ressource ausführt.

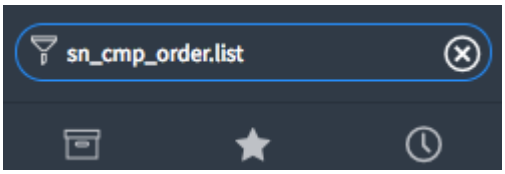
Vorbereitungen

Erforderliche Rolle: sn_cmp.cloud_operator oder sn_cmp.cloud_admin

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie auf der Instanz (nicht im Cloudbenutzerportal) den folgenden Text in den Anwendungsfilter ein:

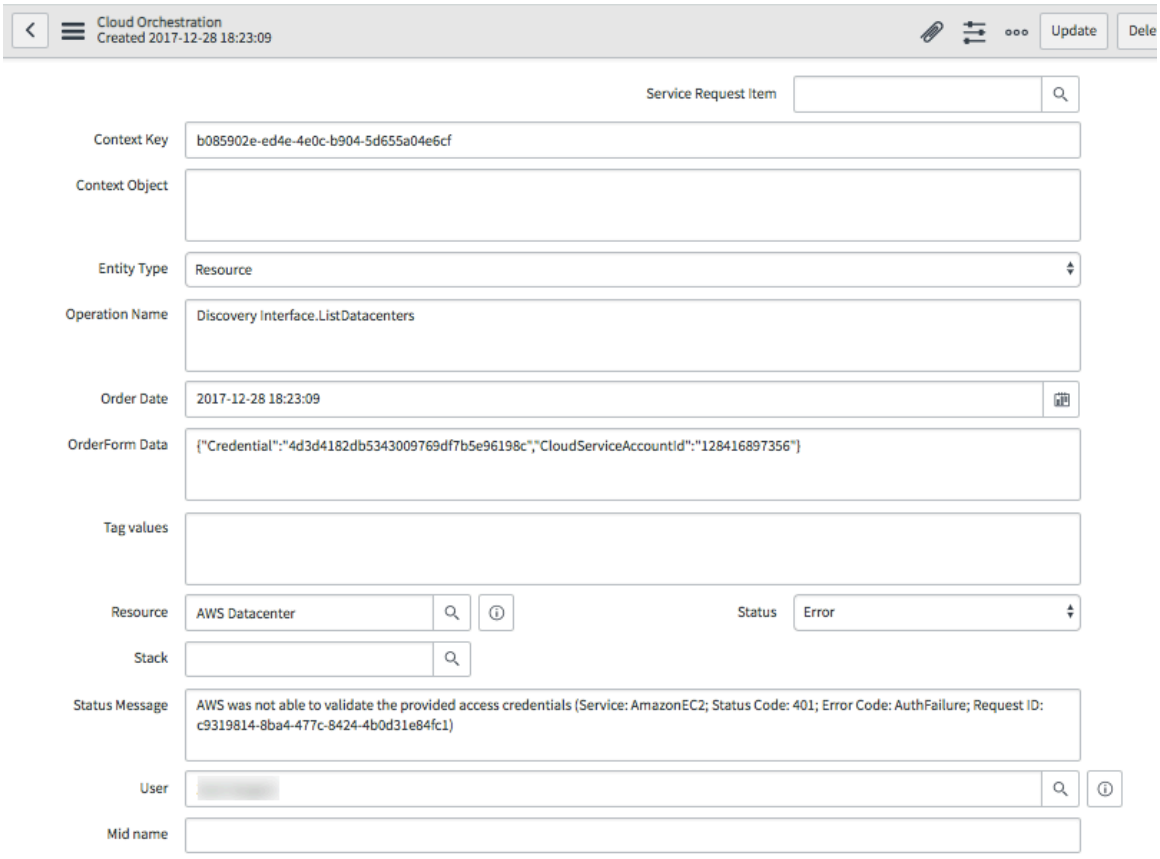


   Die Liste der Cloud-Orchestrierungen wird angezeigt.

2. Sortieren und filtern Sie die Liste, um den gesuchten Fehler oder eine andere Meldung zu finden.

   Um zum Beispiel die Liste nach Datum zu sortieren, klicken Sie auf die Spalte **Auftragsdatum**. Um nur aufgetretene Fehler anzuzeigen, klicken Sie mit der rechten Maustaste in einer Zelle auf **Fehler** und wählen Sie **Übereinstimmungen anzeigen** aus.

3. Öffnen Sie einen Datensatz der Cloud-Orchestrierung, indem Sie auf das Feld **Auftragsdatum** klicken.
4. Überprüfen Sie die Formularfelder:



   Das Beispielformular zeigt den Typ der Nachricht, die Sie sehen können, wenn ein Vorgang aufgrund von falschen Anmeldeinformationen fehlschlägt. Das Feld „OrderForm-Daten“ zeigt die Sys-ID des Anmeldeinformationsdatensatzes und die Servicekonto-ID an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Serviceanforderungselement	Eine Service Catalog-Anforderung (falls vorhanden), die dieser Transaktion zugeordnet ist.
Kontextschlüssel	Ein Schlüsselbezeichner für diese Nachricht.
Kontextobjekt	Dieses Feld ist normalerweise leer.
Kontextinstanz	Die in Transaktionen für einen Stapel verwendete Blaupause oder der in Transaktionen für eine Cloud-Ressource verwendete Ressourcenblock.
Besitzerinstanz Besitzertabelle	Die Besitzerinstanz ist der Ressourcenblock, in dem die Transaktion stattgefunden hat. Dieses Feld wird nur ausgefüllt, wenn der **Entitätstyp** gleich **Ressource** ist. Die Besitzertabelle für die Bereitstellung eines Stapels ist immer „Stapel“ [sn_cmp_stack]. Andernfalls ist die Tabelle der CI-Typ der Ressource, z. B. „VM-Instanz“ [sn_cmp_vm_instance].
Entitätstyp	Gibt an, ob die Transaktion in einer **Blaupause** oder einer **Ressource** (Ressourcenblock) aufgetreten ist.
Vorgangsname	Die Schnittstelle und der Vorgang, der ausgelöst wird.
Auftragsdatum	Das Datum der Transaktion.
OrderForm-Daten	Die über das Benutzerformular übermittelten Daten.
Tag-Werte	Alle an der Transaktion beteiligten Tag-Werte.
Ressource	Der Ressourcenblock, in dem der Vorgang stattgefunden hat. Dieses Feld wird nur ausgefüllt, wenn der Wert des Felds „Entitätstyp“ **Ressource** ist.
Status	Der Status der Nachricht. Wenn Sie einen Fehler anzeigen lassen, wird die Option **Fehler** aufgelistet.
Stapel	Der Stapel, zu dem diese Ressource gehört.
Statusnachricht	Die Statusnachricht, die das Problem erläutert. Durchsuchen Sie die Dokumentation des Cloud-Providers nach den Statuscodes und Nachrichten, die in diesem Feld angezeigt werden. Der Cloud-Provider stellt Ihnen möglicherweise Lösungen zur Verfügung.
Anwender	Der Benutzer, der den Vorgang ausgelöst hat.
MID-Name	Dieses Feld kann den Namen des an der Transaktion beteiligten MID-Servers anzeigen. Es bleibt häufig leer.

Verschieben von Cloud Provisioning and Governance-Inhalten zwischen Umgebungen

Sie können Inhalte in der Cloud Provisioning and Governance-Anwendung aus einer Umgebung in eine andere verschieben. Entwickeln Sie beispielsweise eine Anwendung in einer Umgebung, und verschieben Sie dann die Anwendung und alle zugehörigen Abhängigkeiten zu Test- oder Produktionszwecken in eine andere Umgebung.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Inhaltsentitäten, die verschoben werden können

Die Anwendung Cloud Provisioning and Governance besteht aus Code, Ressourcen, Inhalten und Konfigurationen.

Sie können die folgenden Inhaltsentitäten zwischen Umgebungen verschieben:

- Blaupausen
- Ressourcenblöcke
- Cloud-APIs

Verwenden Sie die Update Sets, um die Inhaltsentitäten zu verschieben. Update Sets sind XML-Dateien, die den gesamten Inhalt in benannte Sets gruppieren und diese Sets dann als Einheit zu Test- oder Bereitstellungszwecken in andere Systeme verschieben. Informationen zur Funktionsweise von System-Update Sets finden Sie unter System-Update Sets .

Abhängigkeiten von Inhaltsentitäten

Jede der Inhaltsentitäten weist einige direkte Abhängigkeiten auf, die automatisch mit dem Inhalt in die neue Umgebung verschoben werden.

Die direkten Abhängigkeiten für jede dieser Inhaltsentitäten sind folgende:

Inhaltsentität	Abhängigkeiten
Blaupause	• Ressourcenblöcke • Cloud-APIs • MID-Skripts • Ressourcenpools • Richtlinien • Skript umfasst Folgendes • Cloud-Skripts
Ressourcenblöcke	• Ressourcenpools • Richtlinien für Ressourcenvorgänge • Skript umfasst Folgendes • Cloud-APIs • Abhängige Ressourcenblöcke • MID-Skripts
Cloud-API	MID-Skripts

Zugehörige Informationen

Eine Blaupause aus einer Umgebung in eine andere verschieben

Einen Ressourcenblock aus einer Umgebung in die andere verschieben

Eine Cloud-API aus einer Umgebung in die andere verschieben

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Blaupause aus einer Umgebung in eine andere verschieben

Mit Update Sets können Sie eine Blaupause und ihre Abhängigkeiten zwischen Umgebungen verschieben. Über Update Sets können Sie eine Blaupause und ihre Abhängigkeiten in einem benannten Set gruppieren und dann als Einheit in andere Systeme verschieben, um sie dort zu testen oder bereitzustellen. Beispielsweise können Sie eine Blaupause aus einer Entwicklungsumgebung in eine Produktionsumgebung verschieben.

Vorbereitungen

Erforderliche Rolle: „sn_cmp.cloud_service_designer“ oder „admin“

- Benutzer mit der Rolle „sn_cmp.cloud_service_designer“ können nur Update Sets exportieren.
- Benutzer mit der Administratorrolle können Update Sets exportieren und importieren.

Warum und wann dieser Vorgang ausgeführt wird

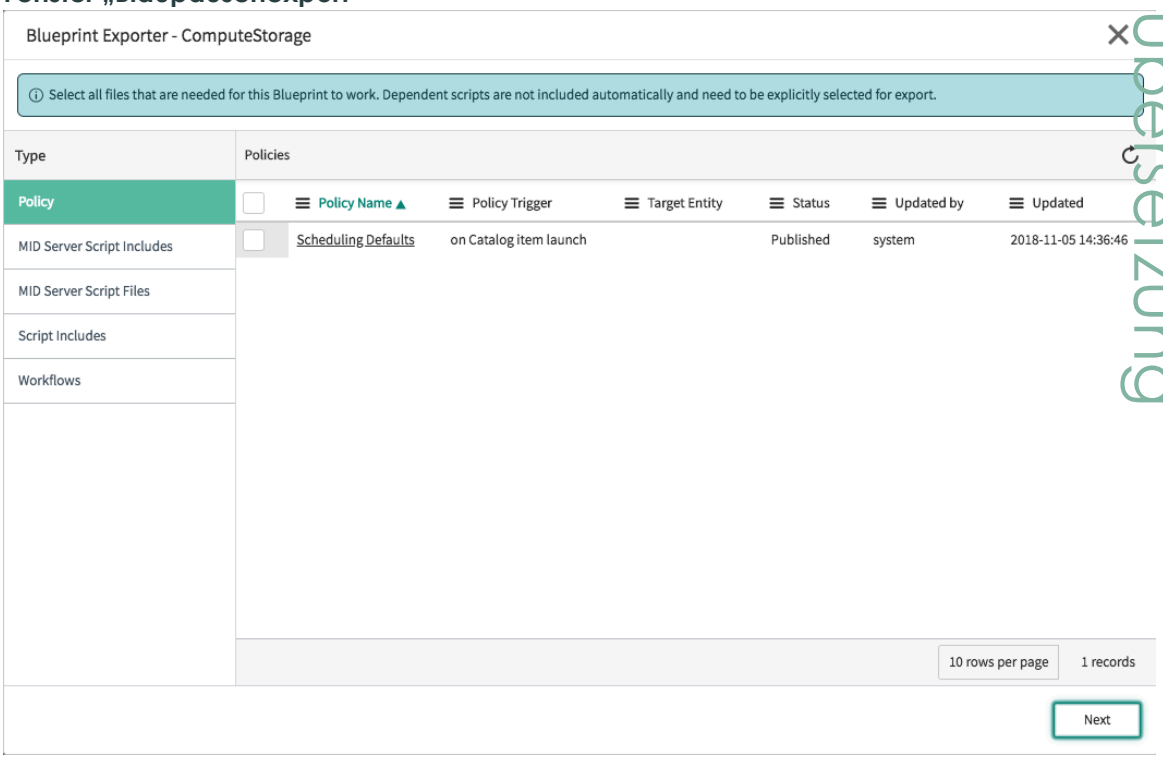
Verpacken Sie die Blaupause als Update Set. Exportieren Sie dann das Update Set aus seiner aktuellen Umgebung, und importieren Sie es in eine andere Umgebung.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Blueprints**.
   Alle Blaupausen, egal ob veröffentlicht oder Entwurf, werden im Fenster „Blueprints“ (Blaupausen) angezeigt.
2. Exportieren Sie die Blaupause.

   a. Klicken Sie für die Blaupause, die Sie exportieren möchten, auf das Symbol „Exportieren“ ( ).

Fenster „Blaupausenexport“



Das Fenster „Blueprint Exporter“ (Blaupausenexporteur) enthält eine Liste aller indirekten Abhängigkeiten (Richtlinie, MID Serverskript-Einbindungen, MID Serverskript-Dateien, Skripteinbindungen und Workflows) für den Plan. Objekte wie Richtlinien, Pools, MID-

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

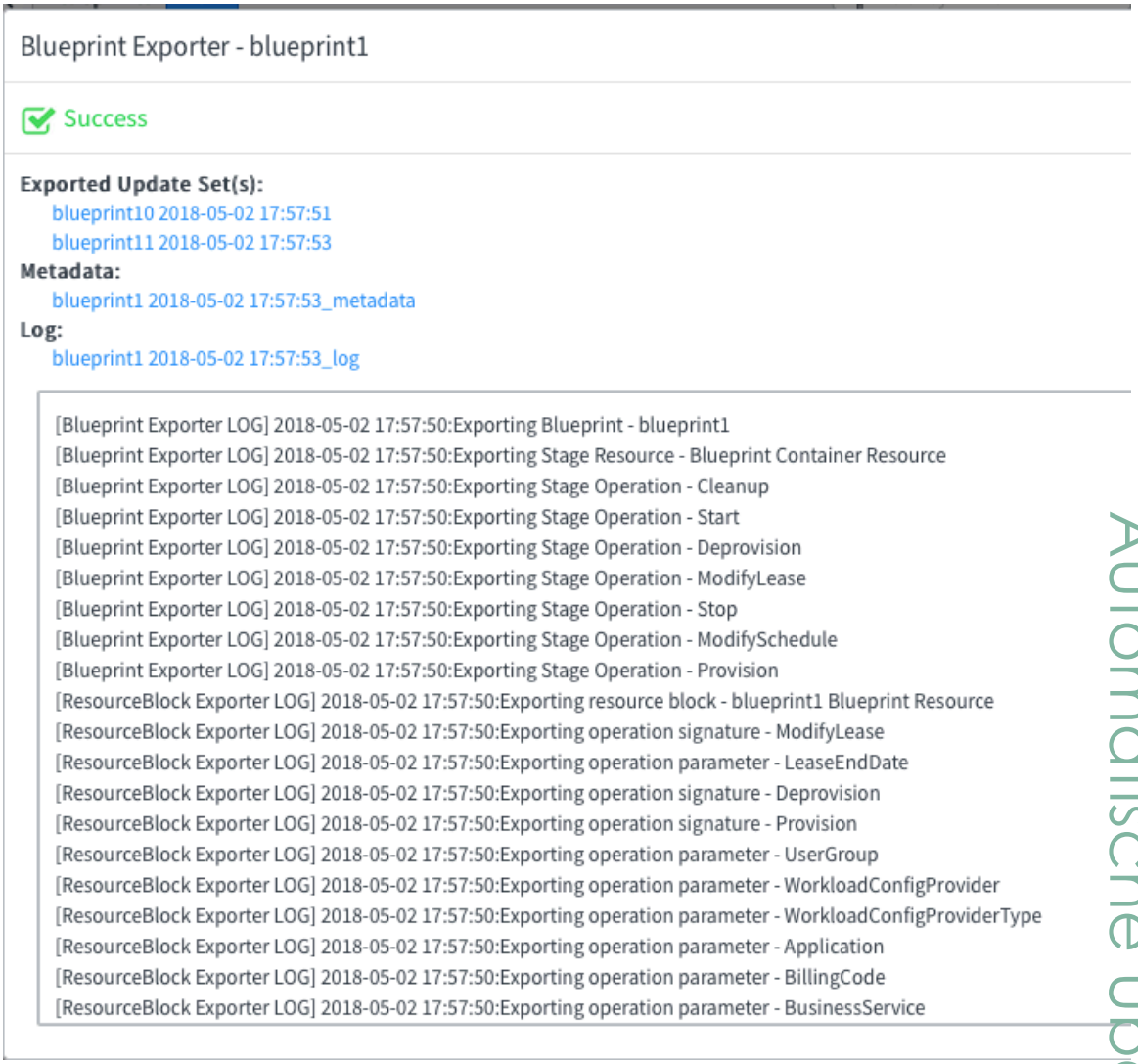
Skripts, Skripteinbindungen und Workflows sind nicht direkt Teil einer Blaupause, aber eine Blaupause kann davon abhängen, dass diese Objekte ordnungsgemäß funktionieren.

b. Klicken Sie im Fenster „Blueprint Exporter“ (Blaupausenexporteur) auf ein Objekt in der Spalte „Type“ (Typ).
Wählen Sie in der rechten Spalte die entsprechenden Einträge des Objekts aus, das Sie mit der Blaupause exportieren möchten. Wenn Sie beispielsweise MID Server-Skripteinbindungen auswählen, werden alle entsprechenden Skripteinbindungen in der rechten Spalte angezeigt. Wenn ein Workflow Subworkflows enthält, wählen Sie den übergeordneten Workflow und alle Subworkflows aus, damit der Workflow exportiert wird. Wenn einem Workflow benutzerdefinierte Aktivitäten zugeordnet sind, exportieren Sie diese zuerst und anschließend den Workflow.

c. Klicken Sie auf **Next** (Weiter).
Ein Fenster wird geöffnet, das eine Zusammenfassung der indirekten Abhängigkeiten aufführt, die Sie in das Export-Update Set aufgenommen haben.

d. Klicken Sie auf **Update Set exportieren**.
Das Fenster „Blueprint Exporter“ (Blaupausenexporteur) wird geöffnet. Das Kontrollkästchen **Success** (Erfolg) wird in Grün angezeigt. Dies zeigt an, dass die Blaupause mit allen zugehörigen Abhängigkeiten exportiert wurde. Standardmäßig werden alle unter „Exported Update Set(s)“ (Exportierte Update Sets) aufgeführten Dateien automatisch auf Ihr System heruntergeladen. Wenn die Dateien jedoch nicht automatisch heruntergeladen werden, führen Sie folgende Schritte aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Hinweis: Die Anzahl der erstellten Update Sets basiert auf dem Umfang der Datensätze, die exportiert werden. Beispiel: Angenommen, die Blaupause, die Sie exportieren, weist insgesamt 100 Datensätze auf – 60 Datensätze befinden sich in Umfang 1, 20 Datensätze befinden sich in Umfang 2, und die verbleibenden 20 Datensätze befinden sich in Umfang 3. In einem solchen Szenario werden drei Update Sets erstellt. Ein Update Set für jeden Umfang.

3. Stellen Sie sicher, dass die Dateien heruntergeladen werden.
   Wenn die Dateien nicht heruntergeladen werden, führen Sie die nachstehenden Schritte aus.

   a. Klicken Sie auf die Metadatendatei.
   Die Metadatendatei zeigt die Reihenfolge an, in der die exportierten Dateien importiert werden sollen. In diesem Beispiel ist die Datei `blueprint10` die erste zu exportierende Datei, gefolgt von der Datei `blueprint11`.

   b. Klicken Sie basierend auf der in der Metadatendatei angegebenen Reihenfolge auf die entsprechende Datei, um sie zu öffnen.
   Ein Fenster mit einer Liste aller im Update Set enthaltenen Dateien wird geöffnet.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Zum Herunterladen der ersten XML-Datei (in diesem Beispiel ist dies `blueprint10`) auf das System klicken Sie **Export to XML** (In XML exportieren).
Importieren Sie alle exportierten Dateien in eine andere Umgebung. Benutzer mit der Administratorrolle können die Dateien importieren. Beispiel: Sie haben das zu exportierende Update Set in einem System erstellt, das die Entwicklungsumgebung ausführt, und möchten das Update Set in ein anderes System importieren, auf dem die Produktionsumgebung ausgeführt wird.

d. Öffnen Sie die andere XML-Datei (im Beispiel ist dies `blueprint11`), und laden Sie diese Datei ebenfalls auf das System herunter.

4. Importieren Sie die Blaupause.

a. Geben Sie in der Umgebung und der neuen Instanz, in die Sie die Dateien importieren möchten, im Filternavigator `Retrieved Update Sets` (Abgerufene Update Sets) ein, und drücken Sie dann die Eingabetaste.

b. Klicken Sie auf den zugehörigen Link **Update Set aus XML importieren**.

c. Klicken Sie im daraufhin angezeigten Fenster „Import XML“ (XML importieren) auf **Choose File** (Dateiauswahl), wählen Sie die Exportdatei, und klicken Sie auf **Upload** (Hochladen).

Hinweis: Wenn in der Zielumgebung eine Blaupause vorliegt, die Sie aus der Quellumgebung exportiert haben und beide Blaupausen eine andere sys_id haben, wird beim Importieren der Blaupause ein Fehler angezeigt und der Importvorgang wird beendet. Exportieren Sie eine andere Blaupause aus der Quellumgebung oder löschen Sie in der Zielumgebung die Blaupause mit dem identischen Namen. Wenn in der Zielumgebung eine Blaupause vorliegt, die Sie aus der Quellumgebung exportiert haben und beide Blaupausen die gleiche sys_id haben, wird die Blaupause in der Zielumgebung mit der Blaupause aktualisiert, die Sie aus der Quellumgebung exportiert haben.

5. Um zu überprüfen, ob der Blueprint in die neue Umgebung importiert wurde, wechseln Sie in der neuen Umgebung zu Ihrer -Instanz und navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Blueprints**.
Die von Ihnen importierte Blaupause sollte in den aufgeführten Blaupausen angezeigt werden.

Einen Ressourcenblock aus einer Umgebung in die andere verschieben

Verwenden Sie Update-Sätze, um Ressourcenblöcke und ihre Abhängigkeiten mühelos zwischen Umgebungen zu übertragen. Gruppieren Sie sie in einem benannten Satz, um ein nahtloses Verschieben für Tests oder die Bereitstellung zu ermöglichen. Vereinfachen Sie Prozesse wie die Übertragung eines Ressourcenblocks von der Entwicklung an die Produktion, um effiziente und organisierte Übergänge zwischen verschiedenen Systemen zu gewährleisten.

Vorbereitungen

- Benutzer mit der Rolle „sn_cmp.cloud_service_designer“ können nur Update Sets exportieren.
- Benutzer mit der Administratorrolle können Update Sets exportieren und importieren.

Erforderliche Rolle: „sn_cmp.cloud_service_designer“ oder „admin“

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Warum und wann dieser Vorgang ausgeführt wird

Verpacken Sie den Ressourcenblock als Update Set. Exportieren Sie dann das Update Set aus seiner aktuellen Umgebung, und importieren Sie es in die andere Umgebung.

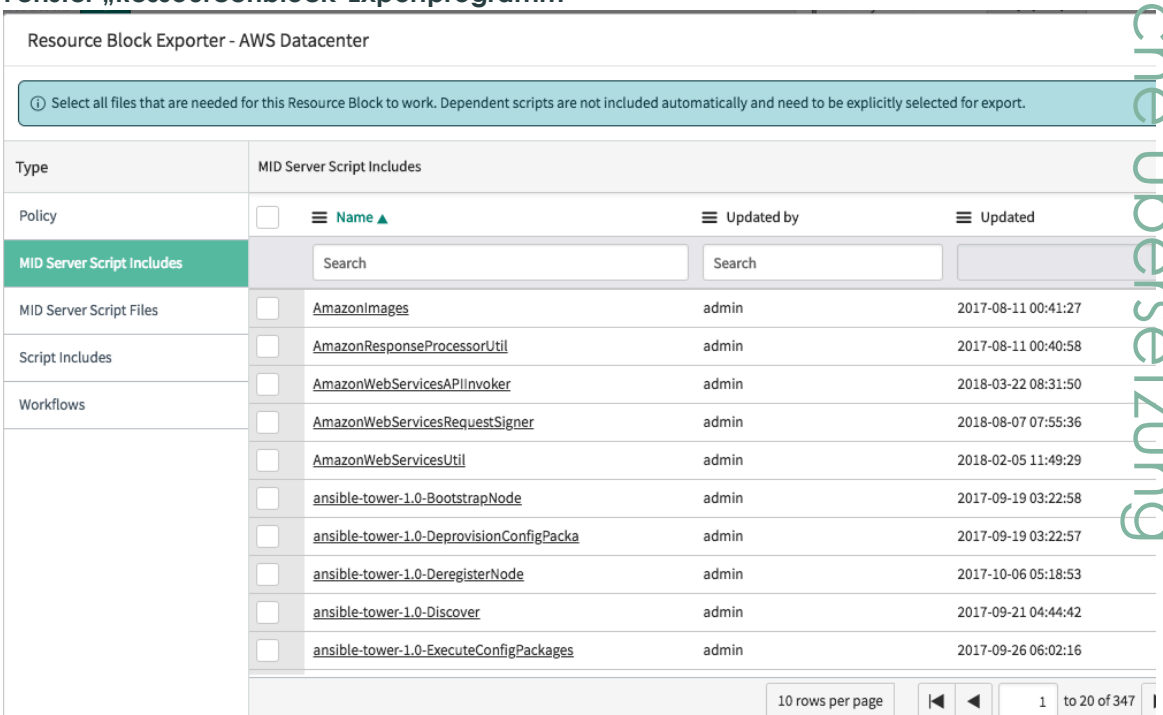
Hinweis: Wenn ein Ressourcenblock, den Sie aus der Quellumgebung exportieren, in der Zielumgebung vorhanden ist, führt der Import dieses Ressourcenblocks zu zwei Ressourcenblöcken mit demselben Namen: einem Ressourcenblock, der vor dem Import vorhanden war, und einem anderen Ressourcenblock, den Sie gerade importiert haben. Beispiel: Wenn Sie den Ressourcenblock „AWS-Rechenzentrum“ aus der Entwicklungsumgebung exportieren und bereits ein Ressourcenblock mit demselben Namen in der Produktionsumgebung vorliegt, liegen nach dem Import des Ressourcenblocks „AWS-Rechenzentrum“ in die Produktionsumgebung zwei Ressourcenblöcke mit dem identischen Namen „AWS-Rechenzentrum“ in der Produktionsumgebung vor.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Ressourcenblöcke**.
   Alle Blaupausen, egal ob veröffentlicht oder Entwurf, werden im Fenster „Resource Blocks“ angezeigt.
2. Exportieren Sie den Ressourcenblock.

   a. Klicken Sie für den zu exportierenden Ressourcenblock auf das Symbol „Export Resource Block“ (Ressourcenblock exportieren) ( ).

Fenster „Ressourcenblock-Exportprogramm“



   a. Klicken Sie im Fenster „Resource Block Exporter“ (Ressourcenblock-Exporteur) auf ein Objekt in der Spalte „Type“ (Typ).

      Wählen Sie in der rechten Spalte die entsprechenden Einträge des Objekts aus, das Sie mit der Blaupause exportieren möchten. Wenn Sie beispielsweise MID Server-Skripteinbindungen auswählen, werden alle entsprechenden Skripteinbindungen in der rechten Spalte angezeigt.

Automatische Übersetzung

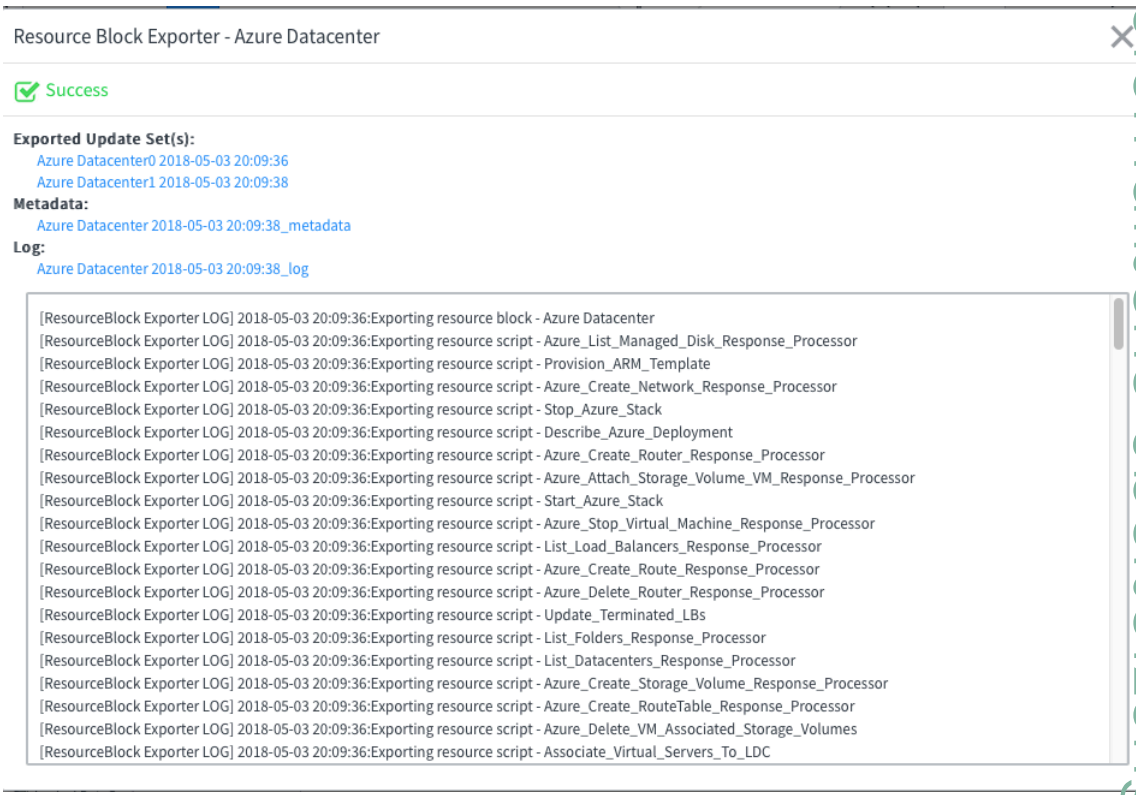
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn ein Workflow Unter-Workflows enthält, wählen Sie den übergeordneten Workflow und alle Unter-Workflows aus, damit der Workflow exportiert wird. Wenn einem Workflow benutzerdefinierte Aktivitäten zugeordnet sind, exportieren Sie diese zuerst und anschließend den Workflow.

b. Klicken Sie auf **Next** (Weiter).
Ein Fenster wird geöffnet, das eine Zusammenfassung der indirekten Abhängigkeiten aufführt, die Sie in das Export-Update Set aufgenommen haben.

c. Klicken Sie auf **Export Update Set** (Update Set exportieren).

Das Fenster „Resource Block Exporter" (Ressourcenblock-Exporteur) wird geöffnet. Das Kontrollkästchen **Success** (Erfolg) wird in Grün angezeigt. Dies zeigt an, dass der Ressourcenblock mit allen zugehörigen Abhängigkeiten exportiert wurde. Standardmäßig werden alle unter „Exported Update Set(s)" (Exportierte Update Sets) aufgeführten Dateien automatisch auf Ihr System heruntergeladen.



Automatische Übersetzung

Hinweis: Die Anzahl der erstellten Update Sets basiert auf dem Umfang der Datensätze, die exportiert werden. Beispiel: Angenommen, der Ressourcenblock, den Sie exportieren, weist insgesamt 100 Datensätze auf – 60 Datensätze befinden sich in Umfang 1, 20 Datensätze befinden sich in Umfang 2, und die verbleibenden 20 Datensätze befinden sich in Umfang 3. In einem solchen Szenario werden drei Update Sets erstellt. Ein Update Set für jeden Umfang.

3. Stellen Sie sicher, dass die Dateien heruntergeladen werden.
Wenn die Dateien nicht heruntergeladen werden, führen Sie die nachstehenden Schritte aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie auf die Metadatendatei.
Die Metadatendatei zeigt die Reihenfolge an, in der die exportierten Dateien importiert werden sollen. In diesem Beispiel ist die Datei `Azure Datacenter0` die erste zu exportierende Datei, gefolgt von der Datei `Azure Datacenter1`.

b. Klicken Sie basierend auf der in der Metadatendatei angegebenen Reihenfolge auf die entsprechende Datei, um sie zu öffnen.
Ein Fenster mit einer Liste aller im Update Set enthaltenen Dateien wird geöffnet.

c. Um die erste XML-Datei in das System herunterzuladen (in diesem Beispiel ist dies `Azure Datacenter0`), klicken Sie auf **In XML exportieren**.

d. Öffnen Sie die andere XML-Datei (im Beispiel ist dies `Azure Datacenter1`), und laden Sie diese Datei auf das System herunter.
Sie müssen alle exportierten Dateien in eine andere Umgebung importieren.
Beispiel: Sie haben das zu exportierende Update Set in einem System erstellt, das die Entwicklungsumgebung ausführt, und möchten das Update Set in ein anderes System importieren, auf dem die Produktionsumgebung ausgeführt wird.

4. Importieren Sie den Ressourcenblock.

a. Geben Sie in der Umgebung und der neuen Instanz, in die Sie die Dateien importieren möchten, im Filternavigator `Retrieved Update Sets` (Abgerufene Update Sets) ein, und drücken Sie dann die Eingabetaste.

b. Klicken Sie auf den zugehörigen Link **Update Set aus XML importieren**.

c. Klicken Sie im daraufhin angezeigten Fenster „Import XML“ (XML importieren) auf **Choose File** (Dateiauswahl), wählen Sie die Exportdatei, und klicken Sie auf **Upload** (Hochladen).

> **Hinweis:** Wenn in der Zielumgebung ein Ressourcenblock vorliegt, den Sie aus der Quellumgebung exportiert haben und beide Ressourcenblöcke eine andere sys_id haben, wird beim Import des Ressourcenblocks ein Fehler angezeigt und der Importvorgang wird beendet. Exportieren Sie einen anderen Ressourcenblock aus der Quellumgebung oder löschen Sie in der Zielumgebung den Ressourcenblock mit dem identischen Namen. Wenn in der Zielumgebung ein Ressourcenblock vorliegt, den Sie aus der Quellumgebung exportiert haben und beide Ressourcenblöcke die gleiche sys_id haben, wird der Ressourcenblock in der Zielumgebung mit dem Ressourcenblock aktualisiert, den Sie aus der Quellumgebung exportiert haben.

5. Um zu überprüfen, ob der Ressourcenblock in die neue Umgebung importiert wurde, wechseln Sie in der neuen Umgebung zu Ihrer -Instanz und navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Ressourcenblöcke**.
Der importierte Ressourcenblock sollte in den aufgeführten Ressourcenblöcken angezeigt werden.

Eine Cloud-API aus einer Umgebung in die andere verschieben

Mit Update Sets können Sie eine Cloud-API zwischen Umgebungen verschieben. Über Update Sets können Sie eine Cloud-API und ihre Abhängigkeiten in einem benannten Set gruppieren und dann als Einheit in andere Systeme verschieben, um sie dort zu testen oder bereitzustellen. Beispielsweise können Sie Cloud-APIs aus einer Entwicklungsumgebung in eine Produktionsumgebung verschieben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Benutzer mit der Rolle „sn_cmp.cloud_service_designer“ können nur Datensätze exportieren.
- Benutzer mit der Administratorrolle können Update Sets exportieren und importieren.

Erforderliche Rolle: „sn_cmp.cloud_service_designer“ oder „admin“

Warum und wann dieser Vorgang ausgeführt wird

Verpacken Sie die Cloud-API als Update Set. Exportieren Sie dann das Update Set aus seiner aktuellen Umgebung, und importieren Sie es in die andere Umgebung.

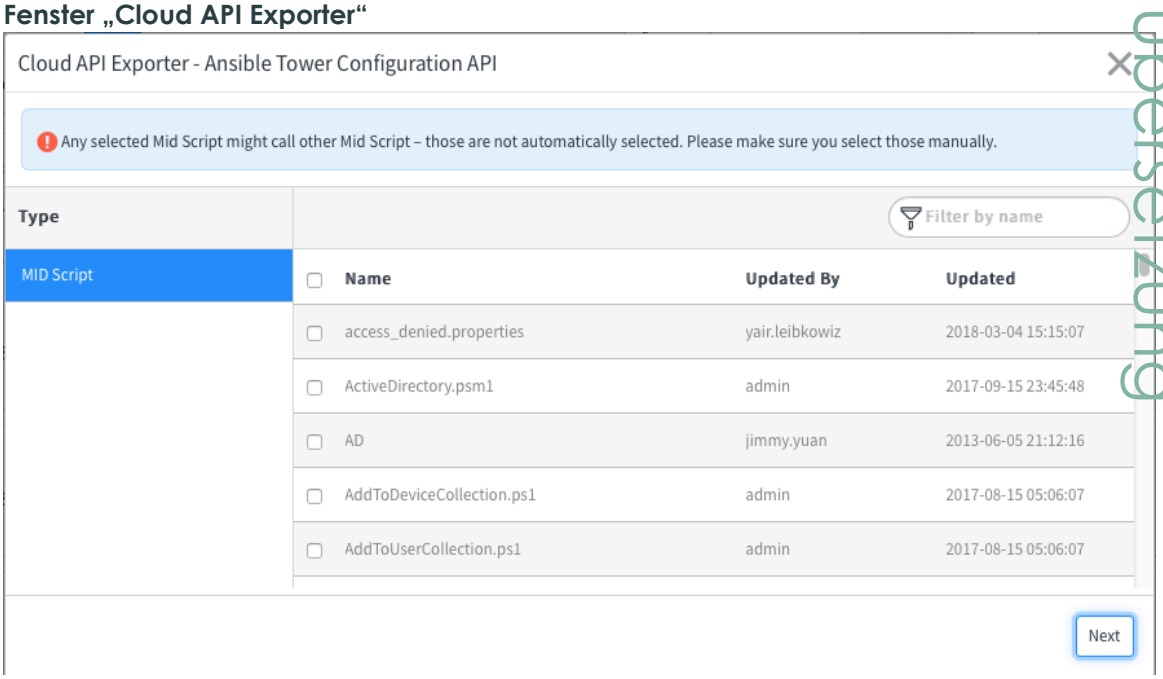
Hinweis: Wenn eine Cloud-API, die Sie aus der Quellumgebung exportieren, in der Zielumgebung vorhanden ist, führt der Import dieser Cloud-API zu zwei Cloud-APIs mit demselben Namen: einer Cloud-API, die vor dem Import vorhanden war, und einer anderen Cloud-API, die Sie gerade importiert haben. Beispiel: Wenn Sie die Ansible-Konfigurations-API aus der Entwicklungsumgebung exportieren und bereits eine Cloud-API mit demselben Namen in der Produktionsumgebung vorliegt, führt der Import der Ansible-Konfigurations-API in die Produktionsumgebung zu zwei Cloud-APIs mit demselben Namen, „Ansible Configuration API“, in der Produktionsumgebung.

Prozedur

1. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Cloud-API** > **API**.
   Alle Cloud-APIs werden im Cloud-API-Fenster angezeigt.
2. Exportieren Sie die Cloud-API.

   a. Klicken Sie auf das Symbol für den Export von Cloud-APIs (), damit die Cloud-API exportiert wird.

Fenster „Cloud API Exporter“



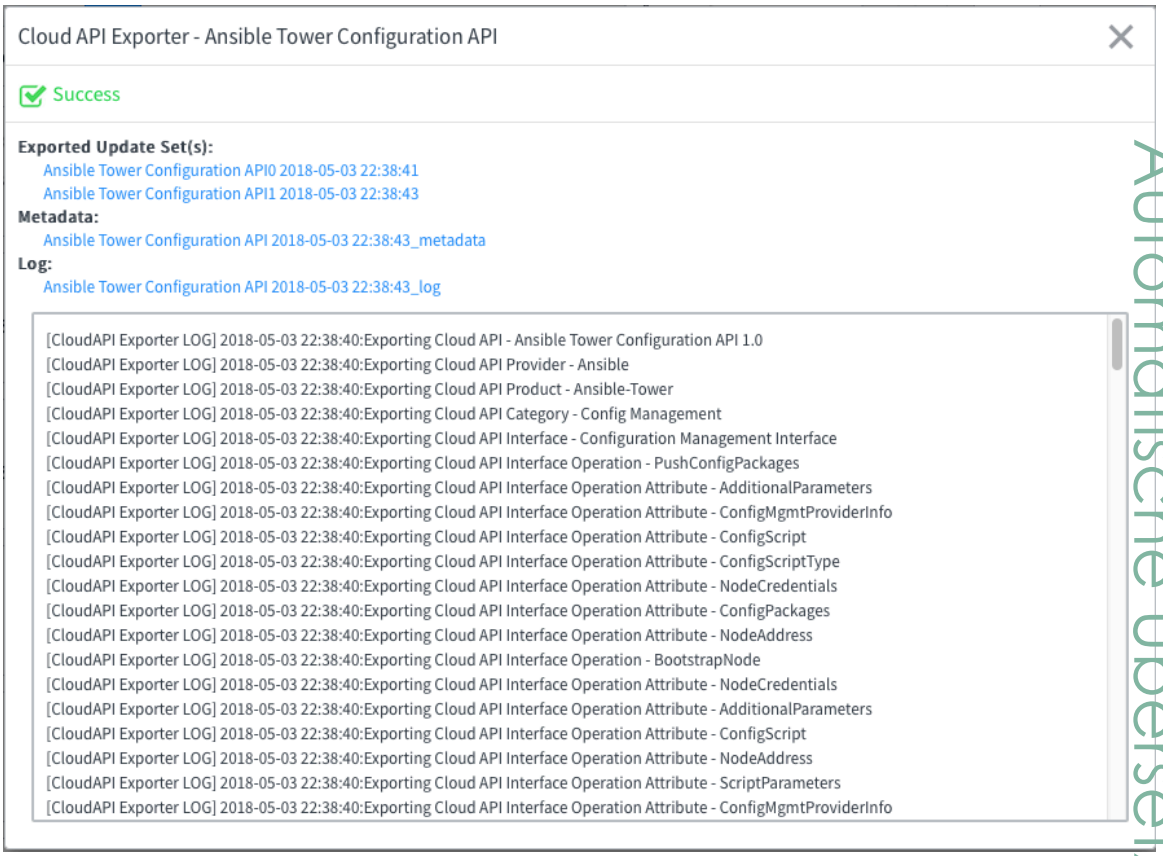
   b. Klicken Sie im Fenster „Cloud API Exporter“ (Cloud-API-Exporter) auf ein Objekt in der Spalte „Type“ (Typ).
   Wählen Sie in der rechten Spalte die entsprechenden Einträge des Objekts aus, das Sie mit der Cloud-API exportieren möchten. Wenn Sie beispielsweise „MID Script“ (MID-Skript) auswählen, werden alle entsprechenden MID-Skripts in der rechten Spalte angezeigt.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

c. Klicken Sie auf **Next** (Weiter).
Ein Fenster wird geöffnet, das eine Zusammenfassung der indirekten Abhängigkeiten der Cloud-API aufführt, die Sie in das Export-Update Set aufgenommen haben.

d. Klicken Sie auf **Export Update Set** (Update Set exportieren).
Das Fenster „Cloud API Exporter“ (Cloud-API-Exporteur) wird geöffnet. Das Kontrollkästchen **Success** (Erfolg) wird in Grün angezeigt. Dies zeigt an, dass die Cloud-API mit allen zugehörigen Abhängigkeiten exportiert wurde. Standardmäßig werden alle unter „Exported Update Set(s)“ (Exportierte Update Sets) aufgeführten Dateien automatisch auf Ihr System heruntergeladen.



Hinweis: Die Anzahl der erstellten Update Sets basiert auf dem Umfang der Datensätze, die exportiert werden. Beispiel: Die Cloud-API, die Sie exportieren, weist insgesamt 100 Datensätze auf – 60 Datensätze befinden sich in Umfang 1, 20 Datensätze befinden sich in Umfang 2, und die verbleibenden 20 Datensätze befinden sich in Umfang 3. In einem solchen Szenario werden drei Update Sets erstellt. Ein Update Set für jeden Umfang.

3. Stellen Sie sicher, dass die Dateien heruntergeladen werden.
Wenn die Dateien nicht heruntergeladen werden, gehen Sie wie folgt vor:

a. Klicken Sie auf die Metadatendatei.
Die Metadatendatei zeigt die Reihenfolge an, in der die exportierten Dateien importiert werden sollen. In diesem Beispiel ist die Datei namens `Ansible Tower-Konfiguration API0` die erste zu exportierende Datei, gefolgt von der Datei `Ansible Tower-Konfiguration API1`.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

b. Klicken Sie basierend auf der in der Metadatendatei angegebenen Reihenfolge auf die entsprechende Datei, um sie zu öffnen.
Ein Fenster mit einer Liste aller im Update Set enthaltenen Dateien wird geöffnet.

c. Zum Herunterladen der ersten XML-Datei (in diesem Beispiel ist dies `API0 2018-05-03`) auf das System klicken Sie **Export to XML** (In XML exportieren).

d. Öffnen Sie die andere XML-Datei (im Beispiel ist dies `API1 2018-05-03`), und laden Sie diese Datei auf das System herunter.
Importieren Sie alle exportierten Dateien in eine andere Umgebung. Beispiel:
Sie haben das zu exportierende Update Set in einem System erstellt, das die Entwicklungsumgebung ausführt, und möchten das Update Set in ein anderes System importieren, auf dem die Produktionsumgebung ausgeführt wird.

4. Importieren Sie die Cloud-API.

a. Geben Sie in der Umgebung und der neuen Instanz, in die Sie die Dateien importieren möchten, im Filternavigator `Retrieved Update Sets` (Abgerufene Update Sets) ein, und drücken Sie dann die Eingabetaste.

b. Klicken Sie auf den zugehörigen Link **Update Set aus XML importieren**.

c. Klicken Sie im daraufhin angezeigten Fenster „Import XML“ (XML importieren) auf **Choose File** (Dateiauswahl), wählen Sie die Exportdatei, und klicken Sie auf **Upload** (Hochladen).
Die Cloud-API wird in die neue Umgebung importiert.

5. Um zu überprüfen, ob der Blueprint in die neue Umgebung importiert wurde, wechseln Sie in der neuen Umgebung zu Ihrer -Instanz und navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Cloud-API** > **API**.
Die von Ihnen importierte Cloud-API sollte in der Liste der Cloud-APIs angezeigt werden.

Cloud-API (CAPI)

Die Cloud-API (CAPI) ermöglicht die Integration von Cloud Provisioning and Governance von Cloud-Providern mit REST APIs.

CAPI-Komponenten

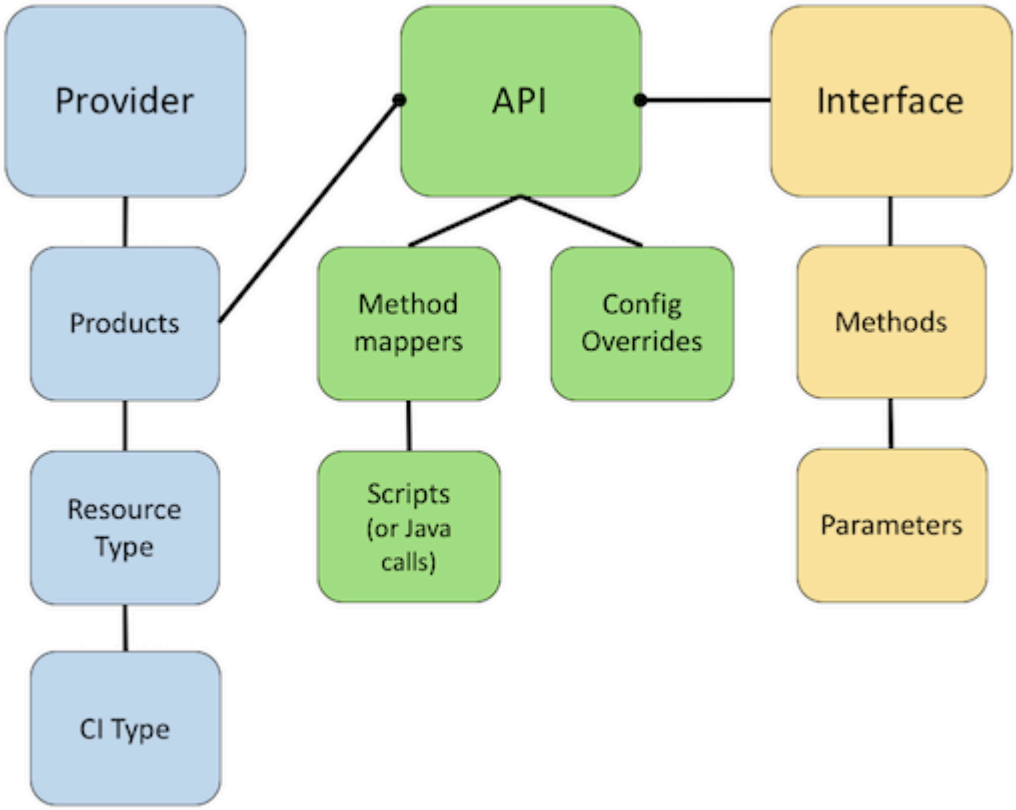
Die Integration mit Cloud-Providern erfolgt über REST-Aufrufe wie PUT, GET, POST und DELETE. CAPI bietet das Framework für die Integration einer REST API von Cloud-Anbietern, was Ihrer Instanz die Kommunikation mit dem Cloud-Anbieter ermöglicht, um Cloud-Ressourcen zu verwalten.

Weitere Informationen finden Sie unter Durchsuchen Sie die APIs nach Produkt .

CAPI umfasst folgende Komponenten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CAPI-Übersicht



Anbieter

Cloud-Anbieter sind die Clouds, mit denen Sie eine Verbindung herstellen können. Standardmäßig umfasst Cloud Provisioning and Governance die am häufigsten verwendeten Anbieter wie AWS, Azure und VMware. Jeder Anbieter verfügt über viele Produkte, von denen jedes Ressourcentypen bereitstellt. Jeder Ressourcentyp wird einem einzelnen CI-Typ zugeordnet. Zum Beispiel enthält *`AWS provider`* das Produkt *`AWS Elastic Compute Cloud`*, was den Ressourcentyp *`AWS::EC2::Instance`* umfasst. Dieser Ressourcentyp ist eine der gängigsten Cloud-Ressourcen, die Sie erstellen können. Der Ressourcentyp wird direkt dem CI-Typ der VM-Instanz [cmdb_ci_vm_instance] zugeordnet, wobei virtuelle Maschinen in der CMDB gespeichert werden.

Schnittstellen

Schnittstellen definieren das Framework, das das System benötigt, um die REST-Aufrufe zu strukturieren, die von den Cloud-Provider-APIs erwartet werden. Schnittstellen definieren den Betrieb, d. h. die Methoden, und die für die einzelnen Methoden erforderlichen Parameter.

Schnittstellen können wiederverwendet werden. Wenn Sie CAPI um neue Produkte und APIs erweitern, können Sie vorhandene Schnittstellen verwenden, um dieselben REST-Aufrufe durchzuführen.

APIs

CAPI-APIs sind die Kernkomponente von CAPI, über die ein Produkt und eine Schnittstelle miteinander verbunden sind. Die APIs enthalten den tatsächlichen Code, den das System ausführt.

Jede CAPI-API enthält die folgenden Komponenten:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- CAPI-Methodenzuordnungen stellen die Methoden bereit , die den in der Schnittstelle definierten Vorgängen zugeordnet sind. Über CAPI-Methodenzuordnungen erstellen Sie MID-Server Skripteinbindungen in JavaScript, um dem Cloud-Anbieter genau mitzuteilen, was zu tun ist. Über die Skripteinbindungen wird die Verbindung zum Cloud-Anbieter hergestellt.

  Hinweis: Wenn Sie benutzerdefinierte CAPI-APIs erstellen, stellt das System eine leere Skripteinbindung bereit, die Sie anpassen können. Sie können bei Bedarf auch vorhandene Skripteinbindungen in Methodenzuordnungen ändern. Allerdings verwenden viele der Standard-APIs, die mit der Anwendung Cloud Provisioning and Governance geliefert werden, keine änderbaren Skripteinbindungen. Die Verbindungen sind in Java fest codiert. Sie können diese APIs weiterhin in neuen von Ihnen erstellten Ressourcenblöcken verwenden, aber die APIs können nicht geändert werden.

- API-Konfigurationsüberschreibungen enthalten die Identität (z. B. einen Schlüssel) und Anmeldeinformationen (z. B. den geheimen Schlüssel) und andere wichtige Parameter, die der Cloud-Anbieter benötigt. Diese Parameter helfen dem Cloud-Anbieter, die Vorgänge in der den CAPI-Methodenzuordnungen zugehörigen Liste durchzuführen. API-Konfigurationsüberschreibungen sind erforderlich, da Anmeldeinformationsdaten nicht enthalten sind, wenn das System die API des Cloudanbieters über REST aufruft. Ressourcenblöcke verwenden die Parameter und Werte, die Sie in den API-Konfigurationsüberschreibungen definieren, um den Anmeldeinformationsspeicher abzufragen. Wenn die API ausgeführt wird, werden die Attribute für alle Methodenaufrufe in den von Ihnen verwendeten Skripteinbindungen verfügbar gemacht.

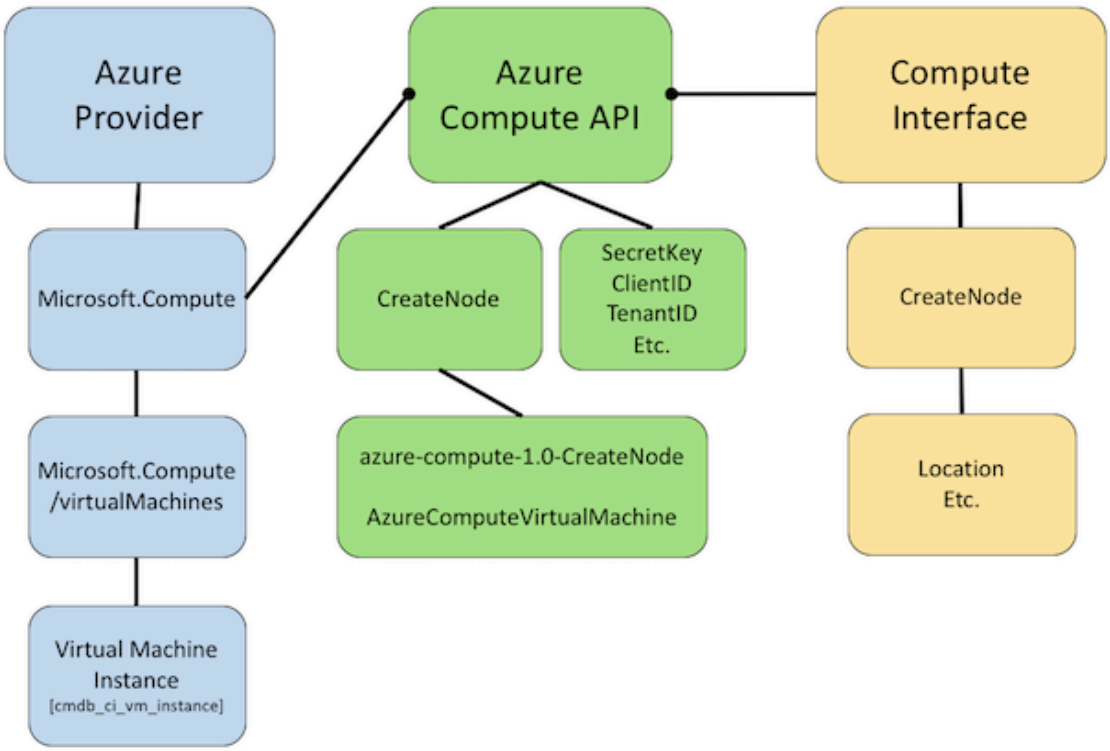
  Die Überschreibungen gelten nur für diese API. Die Überschreibungen überschreiben nichts in anderen APIs.

Da mehrere Versionen einer CAPI-API mit geringfügigen Abweichungen definiert werden können, kann eine vorhandene API erweitert werden (ohne sie zu überschreiben), während die gewünschte Funktionalität beibehalten wird.

Dieses Bild zeigt die Komponenten von CAPI, die verwendet werden, wenn ein virtueller Azure-Computer mit den Standard-CAPI-Einstellungen bereitgestellt wird, die mit Cloud Provisioning and Governance bereitgestellt werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CAPI Azure



In diesem Beispiel ist das Produkt *Microsoft.Compute* beim Anbieter *Azure* enthalten. Azure verwendet das Produkt *Microsoft.Compute* für virtuelle Computer. In Ihrem Fall ist das Produkt *Microsoft.Compute* dem Ressourcentyp *Microsoft.Compute/virtualMachines* zugeordnet, der mit dem CI-Typ *Virtual Machine Instance* in der CMDB verknüpft ist.

Die Schnittstelle *Compute* enthält Definitionen für Methoden wie *CreateNode*, die definiert, wie der tatsächliche virtuelle Computer erstellt wird. Von den vielen Parametern, die *CreateNode* verwendet, erfasst *Location* das Rechenzentrum, in der sich der virtuelle Computer befindet.

Azure Compute API verbindet das Produkt *Microsoft.Compute* und die in der Schnittstelle *Compute* definierte Struktur. Die Implementierung der Methode *CreateNode* ruft das Script Include *azure-compute-1.0-CreateNode* MID-Server auf , das das Script Include *AzureComputeVirtualMachine* MID-Server aufruft. Die Script Includes führen die tatsächlichen Aufrufe der Azure-API aus. Für den Zugriff auf das Azure-Konto werden die Methoden *SecretKey*, *ClientID*, *TenantID* sowie weitere Methoden in Konfigurationsüberschreibungen übergeben.

So führt CAPI eine Integration mit der Instanz durch

CAPI integriert die folgenden Komponenten in die Instanz:

Cloud Provisioning and Governance Ressourcenblöcke

Ein Ressourcenblock stellt eine einzelne Cloud-Ressource dar, z. B. einen virtuellen Server, virtuellen Serverspeicher oder ein Rechenzentrum. Ein Ressourcenblock kann auch als CI-Typ in der CMDB angesehen werden. Viele Ressourcenblöcke werden zu einer Blaupause zusammengefasst, die Benutzern im Cloud-Katalog als Katalogelement (auch Stapel genannt) angezeigt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Im System kann jeder Ressourcenblock als Container angesehen werden, der auf CAPI verweist und Antworten des Cloud-Anbieters mit einem bestimmten CI verknüpft. Ressourcenblöcke verwenden Folgendes:

- Operative Schritte, die CAPI für jeden Vorgang aufrufen, z. B. den Bereitstellungsvorgang, und erforderliche Parameterwerte weitergeben, die der Cloud-Anbieter zum Ausführen des Vorgangs benötigt.
- Antwortprozessoren, die die REST-Antwort des Anbieters verarbeiten und analysieren und Datensätze in der CMDB aktualisieren.

Die CMDB

Jeder Ressourcenblock basiert auf einem CI-Typ der CMDB. Für Cloud Provisioning and Governance basieren alle cloud-bezogenen CI-Typen auf der Klasse *Virtual Machine Object CI*, die alle Attribute bereitstellt, die für alle standardmäßig unterstützten Cloud-Ressourcen benötigt werden. Wenn in Basissystem kein CI-Typ für eine Cloudressource vorhanden ist, müssen eine neue CI-Klasse erstellt und die erforderlichen Attribute hinzugefügt werden.

Wenn Sie eine neue CI-Klasse erstellen, müssen Sie auch Folgendes erstellen:

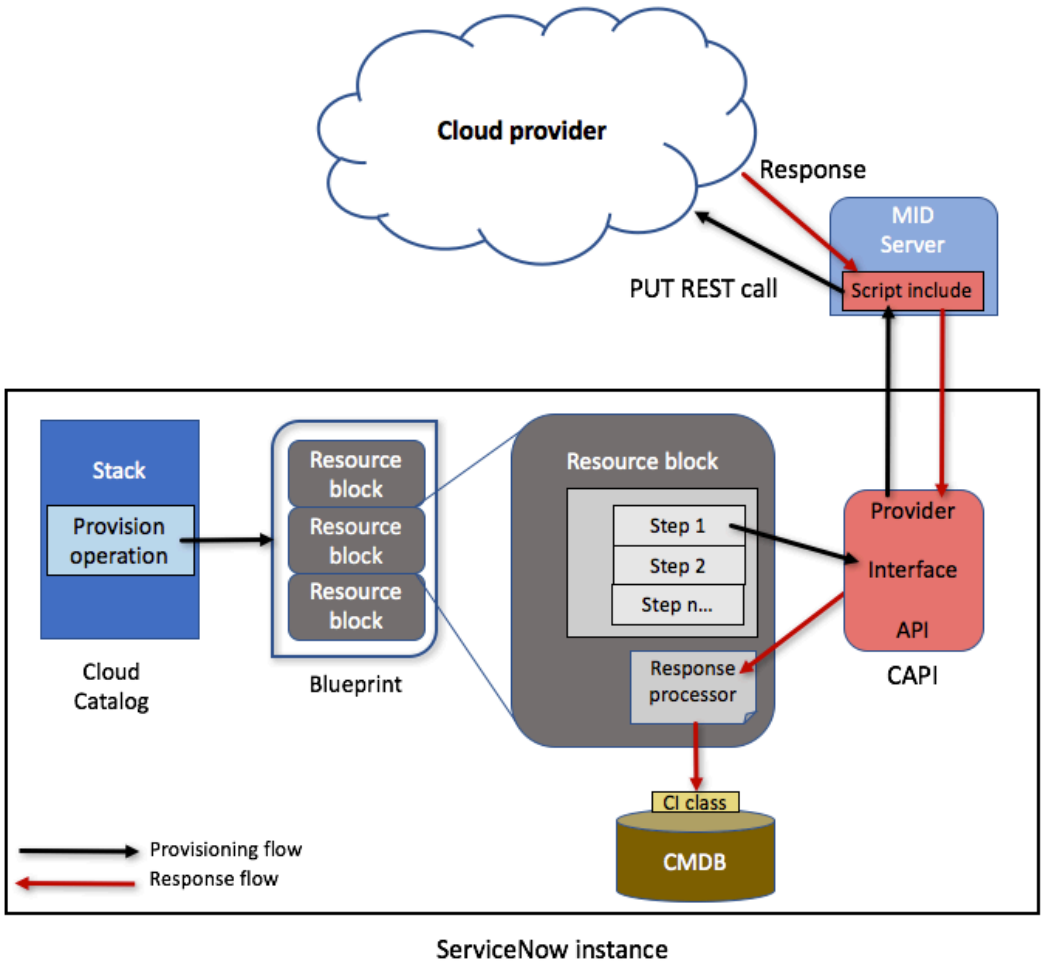
- Eine CI-Klasse für jede der Ressourcen, die den Benutzern zur Verfügung stehen. Alle CI-Klassen basieren auf der VM-Objektklasse.
- Eine Identifizierungsregel, die eine Objekt-ID angibt. Immer, wenn Komponenten von Cloud-Management auf eine bestimmte Cloud-Ressource in der CMDB verweisen, benötigen sie die Objekt-ID, um die richtige Cloud-Ressource zu finden.
- Eine Beziehungsregel, die angibt, wie die CI-Klasse für die Ressource mit anderen CI-Klassen verknüpft ist. Beispielsweise muss eine CI des Typs *virtual server* eine Beziehung des Typs *Hosted on::Hosts* mit einer CI des Typs *datacenter* haben. Diese Beziehungsregeln sind für die Eindeutigkeit von CIs erforderlich, wenn sie von der Engine für Identifizierung und Abgleich (Identification and Reconciliation Engine = IRE) verarbeitet werden. Die Kombination aus Servicekonto, Objekt-ID der Ressource und Datencenter (oder Standort), in dem sich die Ressource befindet, bestimmt die Eindeutigkeit.

Script Include MID-Server

Jeder Vorgang in der CAPI-API verfügt über eine Script Include MID-Server, die Sie konfigurieren. Die Script Include ruft die JavaScript-Klassen auf, die sich bereits in anderen Skripteinbindungen im System befinden, oder die von Ihnen erstellt wurden. Letzten Endes wird die Aufruferklasse aufgerufen, um den REST-Aufruf auszulösen. MID-Server-Skripteinbindungen werden auf der Instanz ServiceNow konfiguriert, aber auf MID-Server ausgeführt.

Dieses Bild zeigt, wie die Komponenten zusammenarbeiten, wenn ein Benutzer eine Ressource aus Cloudbenutzerportal bereitstellt:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



REST-Aufrufe zum Cloud-Anbieter

REST-Aufrufe zum Cloud-Provider werden über die Skripteinbindungen MID-Server ausgelöst, auf die von geskripteten CAPI-Methodenzuordnungen in CAPI-API-Datensätzen verwiesen wird. Zum Erstellen eigener CAPI-APIs oder zum Erstellen benutzerdefinierter MID-Server-Skripteinbindungen (die Teil der CAPI-Methodenzuordnungen sind) müssen Sie Folgendes berücksichtigen:

- Die Klassen, die Sie aus Skripteinbindungen des Typs MID-Server aufrufen können. Weitere Informationen finden Sie unter CAPI-Klassen in MID-Server-Skripteinbindungen.
- So implementiert der Cloud-Anbieter REST: Siehe:
  - Referenz zu Azure REST API
  - AWS-Handbücher und API-Referenzen

Um beispielsweise zu erfahren, wie ein REST-Aufruf an Azure zum Erstellen einer Ressourcengruppe zu tätigen ist, lesen Sie dieses Azure-Thema: Resource Groups - Creat Or Update (Ressourcengruppen – Erstellen oder Aktualisieren). Sie finden die von Azure benötigten Aspekte Endpunkt, Parameter und Anforderungstext sowie die von Azure bereitgestellten Antworten. Sie können Folgendes sehen:

- Der Endpunkt ist `management.azure.com`.
- Die Methode, die mit einem PUT-Vorgang aufgerufen wird, ist `subscriptions/{subscriptionId}/resourcegroups/{resourceGroupName}?api-version=2018-02-01`, wobei Sie die Abonnement-ID, den Ressourcengruppennamen und die API-Version angeben.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Denken Sie daran, dass die REST API-Aufrufe innerhalb der Skripteinbindungen vom Typ MID-Server stattfinden , die CAPI-API-Methodenzuordnungen zugeordnet sind. Sie rufen die Methoden auf, die CAPI bereits für Sie bereitstellt, indem Sie die von `CloudAPIBase` und `CloudRESTAPIInvoker` erweiterten Klassen verwenden. Sie können auch weitere Skripteinbindungen erstellen, um diese Basisklassen zu erweitern und eigene Klassen zu erstellen. Machen Sie sich mit diesen Basisklassen und den darin verfügbaren Methoden vertraut.

Hier geht es los

1. Überprüfen Sie die mit bereitgestellten CAPI-APIs Cloud Provisioning and Governance standardmäßig festgelegt.
2. Überprüfen Sie die CAPI-Klassen, die standardmäßig bereitgestellt werden. Diese Klassen können über die Skripteinbindungen von MID-Server in Ihren CAPI-API-Vorgängen aufgerufen werden.
3. Sehen Sie sich eine Vorstellung der Bereitstellung eines virtuellen Azure-Computers und eines virtuellen AWS-Computers an, um zu sehen, wie die Komponenten zusammenarbeiten. Die exemplarische Vorgehensweise für Azure verwendet eine Skripteinbindung von MID-Server, damit Sie die verschiedenen beim Bereitstellungsvorgang verwendeten CAPI-Klassen einsehen können. Die AWS-Vorstellung verwendet keine Skripteinbindung von MID-Server.
4. Einem vorhandenen Provider in CAPI ein Produkt hinzufügen.
5. Eine CI-Klasse für eine virtuelle Cloud-Ressource erstellen.
6. Eine CAPI-Schnittstelle erstellen oder erweitern.
7. Eine CAPI-API erstellen und eine benutzerdefinierte MID-Server-Skripteinbindung, die die REST-Aufrufe beim Cloud-Anbieter ausführt. Für neue CAPI-APIs wird immer eine leere Skripteinbindung von MID-Server generiert. Ändern Sie sie mit den Aufrufen anderer JavaScript-Klassen und -Methoden, z. B. den Methoden in der Aufrufer-Klasse.

Standard-CAPI-APIs

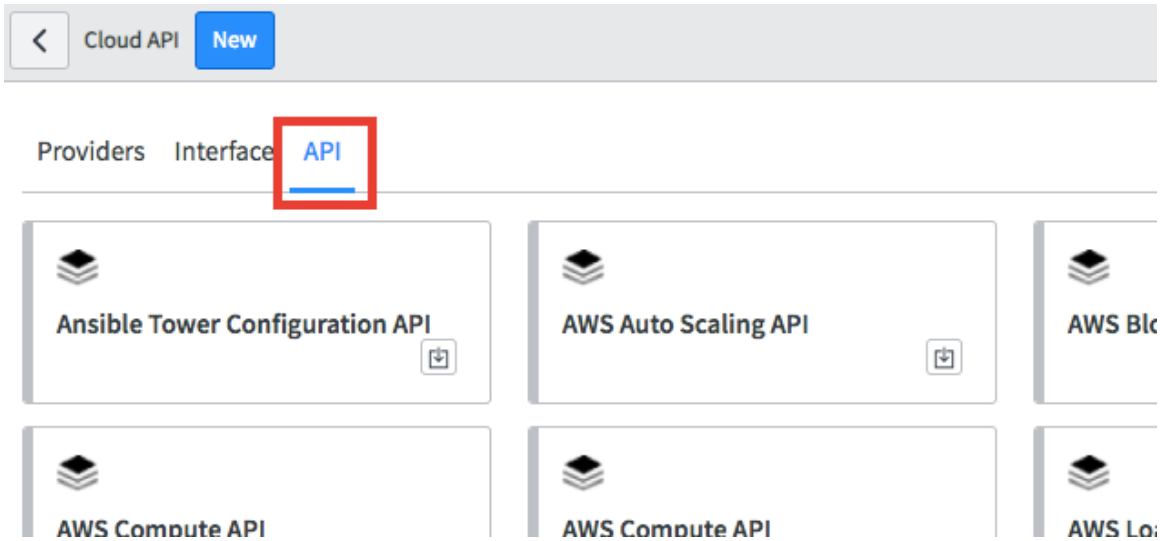
Mit der Anwendung Cloud Provisioning and Governance werden standardmäßig mehrere CAPI-APIs bereitgestellt.

CAPI-APIs beziehen sich auf die API-Datensätze, die ein CAPI-Produkt und eine CAPI-Schnittstelle verknüpfen. Sie verweisen nicht auf die CAPI-Klassen, die über Skripteinbindungen von MID-Server in CAPI-APIs aufgerufen werden können. Eine Übersicht über CAPI-Klassen finden Sie unter CAPI-Klassen in MID-Server-Skripteinbindungen.

Zeigen Sie Cloud-APIs an, indem Sie zu navigieren **Cloud-API** > **Bibliothek** in der Schnittstelle der Instanz Basissystem oder indem Sie zu navigieren **Entwurf** > **Cloud-API** in der Portal für Cloud-Admin..

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

CAPI-APIs



Hinweis: Geskriptete Connectors können Sie mit MID-Server-Skripteinbindungen anpassen.

API	Schnittstelle	Produkt	Geskriptet
Konfigurations-API von Ansible Tower	Schnittstelle zur Konfigurationsverwaltung	Ansible Tower	JA*
Automatisch skalierende AWS-API	Schnittstelle zur automatischen Skalierung	AWS Elastic Compute Cloud	JA*
AWS Blob Storage API	Blob Storage-Schnittstelle	AWS Simple Storage Service	NEIN
AWS Blob Storage API	Blob Storage-Schnittstelle	AWS Elastic Block Storage	NEIN
AWS Compute-API	Compute-Schnittstelle	AWS Elastic Compute Cloud	NEIN
AWS Compute-API	Compute-Schnittstelle	AWS Elastic Compute Cloud	JA*
AWS Load Balancer API	Load Balancer-Schnittstelle	AWS Elastic Load Balancer	NEIN
AWS-Netzwerk-API	Netzwerkschnittstelle	AWS Virtual Private Cloud	NEIN
AWS Stack Orchestration API	Stack-Orchestrierungsschnittstelle	AWS CloudFormation	JA*
Azure-Warnungs-API	Event-Schnittstelle	Azure-Warnung	JA*
Azure Blob Storage API	Blob Storage-Schnittstelle	Microsoft.Storage	JA*
Azure Block Storage API	Blob Storage-Schnittstelle	Microsoft.BlockStorage	JA*
Azure Compute-API	Compute-Schnittstelle	Microsoft.Compute	JA*

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

API	Schnittstelle	Produkt	Geskriptet
Azure-Erweiterungen-API	Azure-Erweiterungsschnittstelle	Microsoft.Compute	JA*
Azure Load Balancer API	Load Balancer-Schnittstelle	Microsoft.LoadBalancer	JA*
Azure-Netzwerk-API	Netzwerkschnittstelle	Microsoft.Network	JA*
Azure Stack Orchestration API	Stack-Orchestrierungsschnittstelle	Azure ARM	JA*
Infoblox IPAM-API	IPAM-Schnittstelle	Infoblox	NEIN
ServiceNow Store IPAM-API	IPAM-Schnittstelle	ServiceNow	JA*
SSH-API	SSH-Schnittstelle	SSH	NEIN
vSphere Block Storage-API	Blob Storage-Schnittstelle	VMware VDisk	NEIN
vSphere Compute-API	Compute-Schnittstelle	VMware vSphere	NEIN

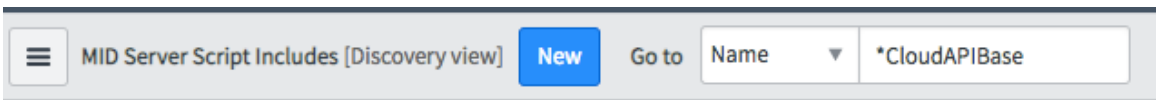
* Sie können anpassen, wie geskriptete APIs REST-Aufrufe an den Cloud-Anbieter tätigen.

CAPI-Klassen in MID-Server-Skripteinbindungen

Cloud Provisioning and Governance bietet mehrere JavaScript-Klassen, die REST-Aufrufe an Cloud-Anbieter durchführen. Diese Klassen werden von MID-Server-Skripteinbindungen (standardmäßig für Azure) oder von Java-Aufrufen im System (standardmäßig für AWS) aufgerufen. Wenn Sie benutzerdefinierte Anbieter, Schnittstellen oder CAPI-APIs (für alle Cloud-Anbieter) erstellen, können Sie die MID-Server-Skripteinbindungen zum Aufrufen der Klassen verwenden.

Hinweis: In CAPI-APIs gibt es keine MID-Server-Skripteinbindungen (in Methodenzuordnungen), die Sie anpassen können, um die AWS-Klassen aufzurufen. Standardmäßig führen die CAPI-APIs für AWS Java-Aufrufe durch, um dann die AWS-Klassen aufzurufen. Wenn Sie jedoch CAPI-APIs erstellen, können Sie auch benutzerdefinierte Skripteinbindungen zum Aufrufen der Klassen erstellen.

Zeigen Sie CAPI-Klassen an, indem Sie zu navigieren **MID-Server** > **Skripteinbindungen** in der Schnittstelle der Instanz Basissystem (nicht Portal für Cloud-Admin.). Den Namen einer Klasse suchen Sie im Suchfeld **Go to** (Wechseln zu) über die Spalte **Name**:



Basisklassen

Die folgenden Basisklassen sind standardmäßig verfügbar. Sie bilden eine Grundlage für die Azure- und AWS-Klassen, die die tatsächlichen REST-Aufrufe vornehmen.

CloudAPIBase

CloudAPIBase ist eine anbieterunabhängige API, die mit allen Arten von Cloud-APIs kommuniziert. Sie bietet Funktionen für das grundlegende Debugging und die Protokollierung sowie für das Sammeln von Proxyinformationen auf

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

MID-Server. Darüber hinaus definiert sie Header, Parameter, Endpunkte und `this.parameter`.

AWSCloudAPIBase

Diese Klasse wurde von CloudAPIBase erweitert und bietet Funktionen, die den Aufrufer auffordern, GET-, PUT-, POST- und DELETE-Anforderungen zu stellen. Die Klasse bietet die Option einer `executeAction`-Methode, die eine AWS-Implementierung von GET ist, oder der invoke-Methode, die REST API-Aufrufe bereitstellt.

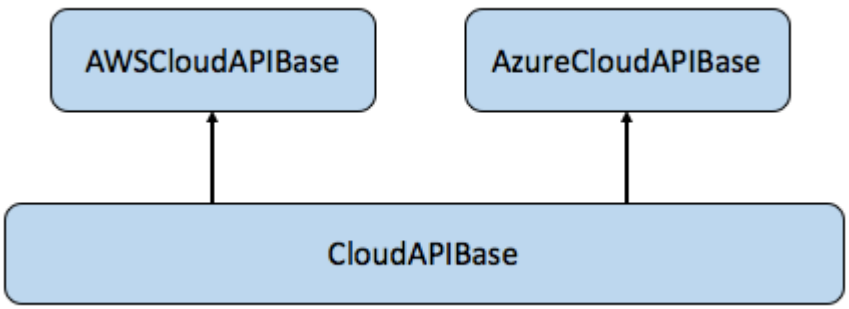
AzureCloudAPIBase

Diese Klasse wurde von CloudAPIBase erweitert und bietet Funktionen für die folgenden Aktionen:

- Ressourcen-IDs abrufen
- Endpunkteigenschaften abrufen
- Ressourcen auflisten
- Den Aufrufer aufrufen, GET-, PUT-, POST- und DELETE-Anforderungen zu senden.

AzureCloudAPIBase verwendet die Methode `_invokeRequest`, um REST API-Aufrufe an Azure mithilfe der Standard-REST API-Aufrufe zu tätigen.

Basis-APIs



Aufrufende Klassen

Aufruferklassen führen die tatsächlichen REST-Aufrufe an den Cloud-Anbieter durch. Wenn Sie benutzerdefinierte CAPI-Schnittstellen und APIs erstellen, sollten Sie *`CloudRestAPIInvoker`* erweitern, wenn Sie REST-Aufrufe erstellen möchten.

CloudRestAPIInvoker

Diese Klasse ist eine abstrahierte Klasse für REST API-Aufrufe. Wenn Header und/oder Parameter vorhanden sind, die mit einer Anforderung gesendet werden sollen, müssen Klassen, die den Aufrufer implementieren, dieses Objekt erweitern. Sie müssen auch Überschreibungen für *`getEndpointUrl`* bereitstellen, um den Zielendpunkt auszugeben, sowie für *`getHeaders`* und *`getParameters`*. Bei Azure REST APIs erfordert die Authentifizierung beispielsweise die Übergabe eines Tokens als Header. Die Erweiterung, die dies implementiert, sollte eine Antwort von *`getHeaders`* bereitstellen, die die Erstellung oder den Abruf des Tokens durchführt und dies festlegt. Dieses Basisobjekt ruft *`getHeaders`* auf und sendet alles, was auf die Anforderung zurückgegeben wird. Diese Klasse stellt auch eine *`getResponse`*-Methode für die Behandlung der Antwort des Cloud-Anbieters bereit.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie eine benutzerdefinierte CAPI-API erstellen, sollten Sie *CloudRestAPIInvoker* erweitern, um REST-Aufrufe an den Cloud-Provider zu tätigen.

AmazonWebServicesAPIInvoker

Diese Klasse wurde von *CloudRestAPIInvoker* erweitert und stellt Methoden für REST API-Aufrufe an den Cloud-Anbieter bereit.

AzureAPIInvoker

Diese Klasse wurde von *CloudRestAPIInvoker* erweitert und bietet Funktionen, die die folgenden REST API-Aufrufe an Azure Resource Manager vornehmen:

- Legt Dienstprinzipal, Header und Parameter für REST-Aufrufe fest.
- Ruft Endpunkt-URL, Token (Client-ID, Mandanten-ID und geheime Schlüssel) sowie Header/Parameter ab.
- Ruft den JSON-Antworttextkörper vom Cloud-Anbieter ab und decodiert ihn.

AzureEAAPIInvoker

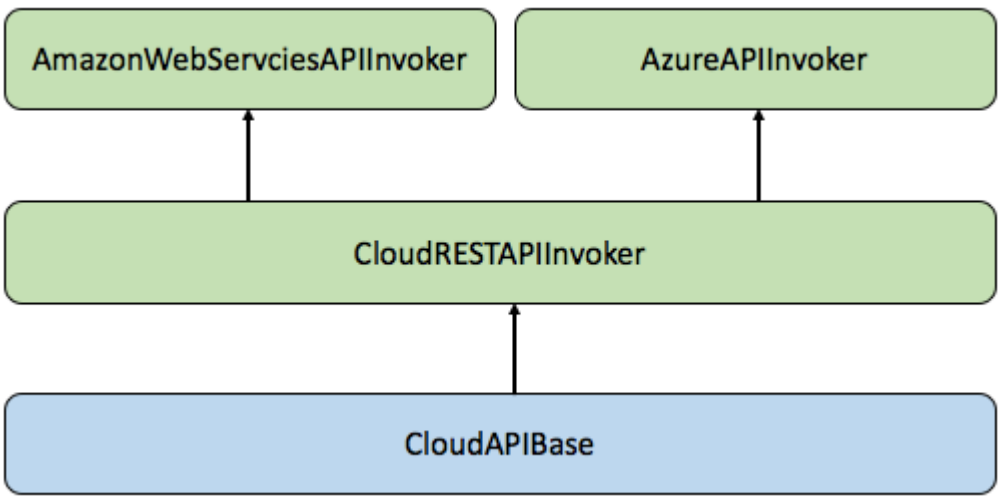
Diese Klasse gibt das Token für den Zugriff auf die REST API von Azure Enterprise Agreement (EA) zurück.

AzureStorageAPIInvoker

Diese Klasse führt REST-Aufrufe für Azure-Speicher durch. Die Funktionen in dieser Klasse können Token, Antwort, Header und Parameter abrufen.

Diese Grafik zeigt, wie die Basisklassen zur Erweiterung von AWS-spezifischen und Azure-spezifischen Klassen verwendet werden:

REST-Aufrufe werden aufgerufen



Ausnahmen

RESTAPIException

Diese Basisklasse behandelt Ausnahmen, die während des REST-Aufrufs auftreten können. Sie gibt den Antwortcode vom Cloud-Provider zurück.

AWSAPIException

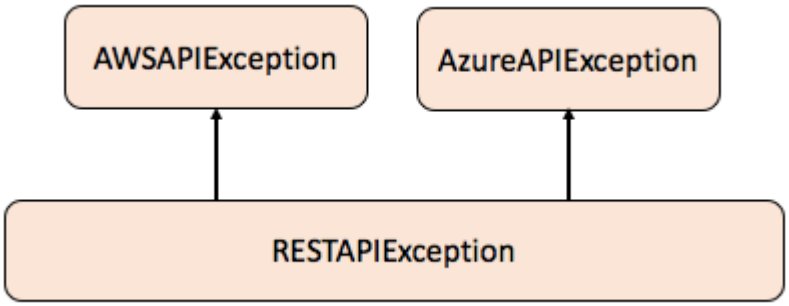
Diese Klasse behandelt Ausnahmen, die während des REST-Aufrufs auftreten können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AzureAPIException

Diese Klasse löst bei Bedarf während des Aufrufs der Azure-API eine Laufzeitausnahme aus.

Handhabung von Ausnahmen



Klassen für Anmeldeinformationen

CloudRESTRequestSigningUtil

Diese Klasse verwendet Überschreibungen, die in CAPI-API-Konfigurationsüberschreibungen angegeben sind. Die Klasse *AmazonWebServicesRequestSigner* erweitert diese Klasse. Für Azure sind viele Signierer in die Skripteinbindungen von MID-Server für Methodenzuordnungen in Azure-CAPI-APIs integriert.

AmazonWebServicesRequestSigner

Diese Klasse richtet eine sichere Sitzung für den REST API-Aufruf ein, indem Informationen zu einer Anforderung abgerufen und eine Zeichenfolge mit signature v4- -Signatur für die Anforderung erstellt wird. Diese Klasse wird von CloudRESTRequestSigningUtil erweitert.

Andere Azure-Klassen

Klassen, die AzureCloudAPIBase erweitern

Klasse	Beschreibung
AzureAlertRule	Klasse zum Erstellen und Löschen von Azure-Warnungsregeln.
AzureAuthorizationPolicy	Klasse zum Zuweisen von Tag-Richtlinien.
AzureComputeAvailabilitySet	Klasse für das Abrufen von Azure-Verfügbarkeitssätzen. Siehe: https://docs.microsoft.com/en-us/rest/api/compute/availabilitysets
AzureComputeHardware	Klasse zum Abrufen von Azure-Größen. Siehe: https://docs.microsoft.com/en-us/rest/api/compute/virtualmachinesizes
AzureComputeImage	Klasse für die Verarbeitung von Azure-API-Aufrufen zu Bildern. Siehe: https://docs.microsoft.com/en-us/rest/api/manageddisks/images/images-rest-api
AzureComputeVirtualMachine	Klasse für die Verarbeitung von Azure-API-Aufrufen zu virtuellen Computern. Siehe: https://docs.microsoft.com/en-us/rest/api/compute/

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassen, die AzureCloudAPIBase erweitern (Fortsetzung)

Klasse	Beschreibung
	virtualmachines VM-Größen und -Kapazitäten: https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-windows-sizes https://docs.microsoft.com/en-us/azure/virtual-machines/virtual-machines-linux-sizes Von Cloud-Init unterstützte Versionen: https://docs.microsoft.com/en-us/azure/virtual-machines/linux/using-cloud-init
AzureDeployment	Klasse für die Azure ARM-Vorlagenbereitstellung.
AzureDeploymentOperation	Klasse für den Betrieb der Azure ARM-Vorlagenbereitstellung.
AzureImages	Klasse für die Verarbeitung von Azure-Bildern.
AzureLoadBalancer	Klasse für die Verarbeitung von Azure-API-Aufrufen zu Lastenausgleichsmodulen. Siehe: https://msdn.microsoft.com/en-us/library/azure/mt163651.aspx
AzureLocalNetworkGateways	Klasse zum Erstellen und Abrufen von Gateways für lokale Netzwerke.
AzureNetworkNIC	Klasse für die Verarbeitung von Azure-API-Aufrufen zu Netzwerkschnittstellen-Karten. Siehe: https://msdn.microsoft.com/en-us/library/azure/mt163579.aspx
AzureNetworkPublicIP	Klasse für die Verarbeitung von Azure-API-Aufrufen zu öffentlichen IP-Adressen. Siehe: https://msdn.microsoft.com/en-us/library/azure/mt163638.aspx
AzureNetworkRouter	Klasse für die Verarbeitung von Azure-API-Aufrufen zur Routingtabelle. Siehe: https://docs.microsoft.com/en-us/rest/api/network/route-tables
AzureNetworkSecurityGroup	Klasse für die Verarbeitung von Azure-API-Aufrufen zu Netzwerkschnittstellen-Karten. Siehe: https://msdn.microsoft.com/en-us/library/azure/mt163579.aspx
AzureNetworkVirtualNetwork	Klasse für die Verarbeitung von Azure-API-Aufrufen zu virtuellen Netzwerken.
AzureProvider	Klasse zum Abrufen von Azure-Anbieterdetails, wie Anbieter-URL und Version.
AzureRegion	Klasse zum Abrufen von Azure-Regionen.
AzureResource	Behandelt das Objekt, auf das ObjectID in den Parametern verweist. Außerdem wird die API-Version abgerufen. Diese Klasse ist hauptsächlich zum Abrufen nicht unterstützter Typen oder zum Löschen von Ressourcen gedacht.
AzureResourceGroupManager	Klasse für die Verarbeitung von Azure ARM-Ressourcengruppen.
AzureResponseUtil	Klasse zum Übersetzen der Azure-API-Antwort in ein DTO-Objekt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Klassen, die AzureCloudAPIBase erweitern (Fortsetzung)

Klasse	Beschreibung
AzureStorageAccount	Klasse für die Verarbeitung von Azure-API-Aufrufen zum Speicherkonto. Siehe: //https://msdn.microsoft.com/en-us/library/azure/mt163638.aspx
AzureStorageBlob	Klasse zum Erstellen und Bearbeiten von Speichercontainern und Blobs.
AzureStorageManagedDisk	Klasse für die Verarbeitung von Azure-API-Aufrufen zum verwalteten Datenträger. Siehe: https://docs.microsoft.com/en-us/rest/api/manageddisks/disks/disks-create-or-update
AzureSubscription	Klasse zum Abrufen von Azure-Abonnements.
AzureVirtualNetworkGateways	Klasse zum Erstellen und Bearbeiten von Gateways für virtuelle Netzwerke.
AzureCloudEAAPIBase	Basisobjekt für Azure EA-API-Handler. Azure EA-APIs haben die Basis-URL https://consumption.azure.com und erfordern die Registrierungsnummer im Pfad. Diese Klasse verarbeitet das Aktivieren der Parameter „EnrollmentNumber“ und „EnrollmentToken“.

Andere AWS-Klassen

Klasse	Beschreibung
AmazonImages	Klasse für die Verarbeitung von Amazon Computerimages. http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html
AmazonResponseProcessorUtil	Klasse für die Verarbeitung der AWS REST API-Antwort.
AWSAutoScalingGroups	Klasse für die Verarbeitung von AWS API-Aufrufen zum Erstellen und Bearbeiten von Autoskalierungsgruppen .
AWSCloudFormation	Handler für AWS CloudFormation-API-Aufrufe.
AWSEC2	Handler für AWS EC2 API-Aufrufe.
AWSKeyValuePair	Klasse zum Importieren und Bearbeiten von Schlüsselpaaren.
AWSLaunchConfigurations	Hilfsklasse.
AWSS3	Handler für AWS S3 API-Aufrufe.
AWSTopics	Klasse mit AWS-Themen .

Azure VM-Bereitstellung – exemplarische Vorstellung

Dieses Beispiel führt Sie durch die Komponenten von Cloud Provisioning and Governance, die während der Bereitstellung eines virtuellen Computers in einem Azure-Rechenzentrum

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

in Betrieb sind. Zu den behandelten Themen gehören Blaupausen, Ressourcenblöcke, die Cloud-API (CAPI) und Skripteinbindungen MID-Server.

Vorbereitungen
Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird
Diese erläuternde Vorstellung beginnt mit einer Linux-VM, die ein Benutzer bereits in Azure bereitgestellt hat. Anschließend werden Ihnen die Blaupause mit der VM, den Ressourcenblöcken und den in den Ressourcenblöcken angegebenen CAPI-Aufrufen vorgestellt. Abschließend zeigt Ihnen die Vorführung, wie eine MID-Server-Skripteinbindung über mehrere CAPI-Aufrufe die tatsächlichen REST-Aufrufe an die Azure-API durchführt.

In diesem Beispiel werden Standardressourcenblocks und Skript Includes verwendet, die in Ihrer Instanz verfügbar sind. Deshalb können Sie, obwohl Sie möglicherweise keine bereitgestellte VM auf Ihrer Instanz haben, trotzdem diese Schritte befolgen und die in diesem Beispiel verwendeten Komponenten anzeigen, um die Arbeitsweise der Komponenten zu verstehen.

Ein Beispiel für einen virtuellen Computer in AWS finden Sie unter VM-Bereitstellung bei AWS – Beispiel-Vorstellung.

Hinweis: Die Begriffe virtueller Computer, VM (für „Virtual Machine“) und virtueller Server sind in diesem Beispiel synonym.

Prozedur

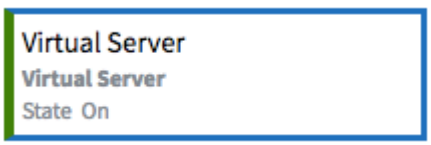
1. Betrachten Sie eine eingerichtete VM im Cloud User Portal und richten Sie den Fokus auf einige Details zur VM:

   a. Öffnen Sie auf der Schnittstelle der Basissystem -Instanz Cloudbenutzerportal (**Cloud-Anwenderportal**) an.

   b. Rufen Sie auf Cloudbenutzerportal eine bereitgestellte VM in einem Stapel auf, z. B. diese VM, indem Sie auf **Stapel** und dann auf den Namen des Stapels klicken.

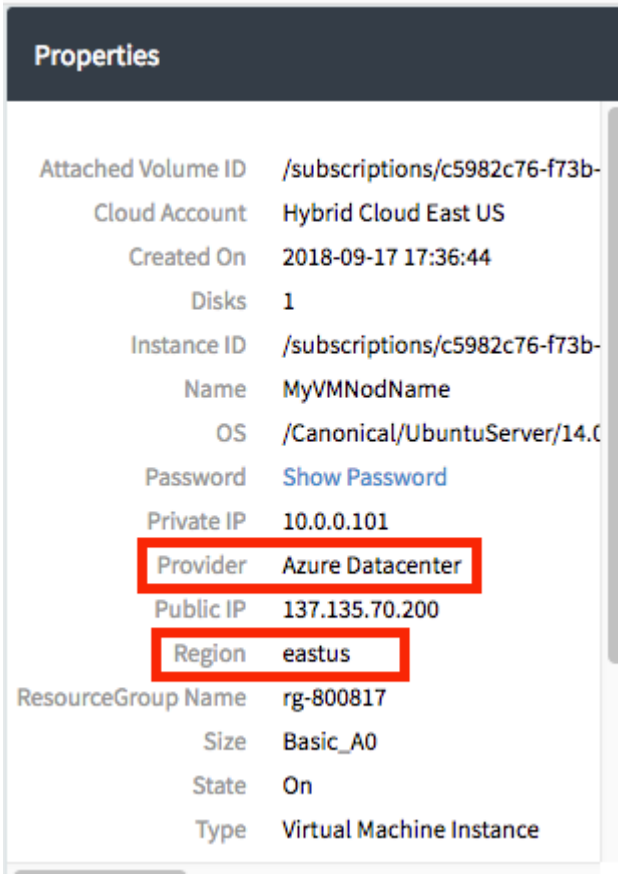
      In diesem Beispiel heißt der Stapel **MyAzureVM**.

   c. Klicken Sie unter **Resources**(Ressourcen) auf den virtuellen Computer im Stapel.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

d. Rufen Sie die Eigenschaften der VM auf; beachten Sie, dass sie sich in einem **Azure-Rechenzentrum** in der Region **Eastus** befindet.

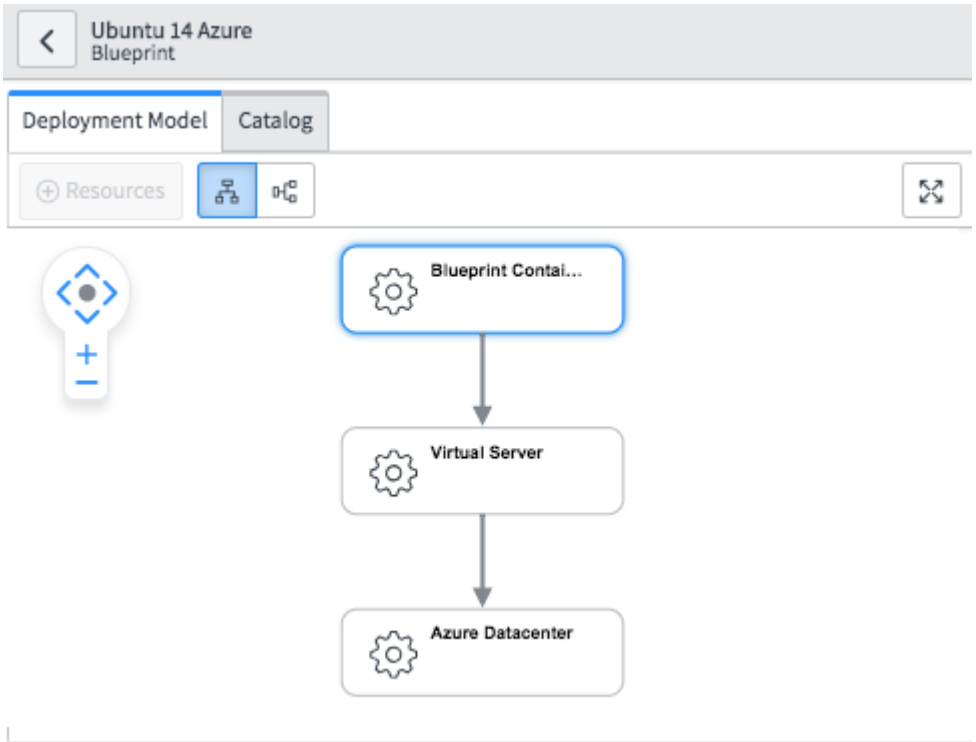


2. Sehen Sie sich die Blaupause an, auf der die VM basiert:

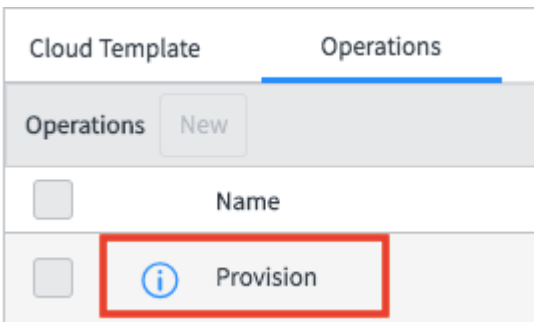
a. Navigieren zu **Entwurf** > **Blueprints**, und öffnen Sie dann einen Blueprint mit einem virtuellen Server im Azure-Rechenzentrum. Die Registerkarte **Bereitstellungsmodell** wird standardmäßig angezeigt und zeigt Ihnen die verschiedenen Komponenten des Blueprints.

Diese Beispiel-Blaupause hat drei Komponenten: den Container, den virtuellen Server, der die bereitgestellte VM ist, und das Azure-Rechenzentrum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

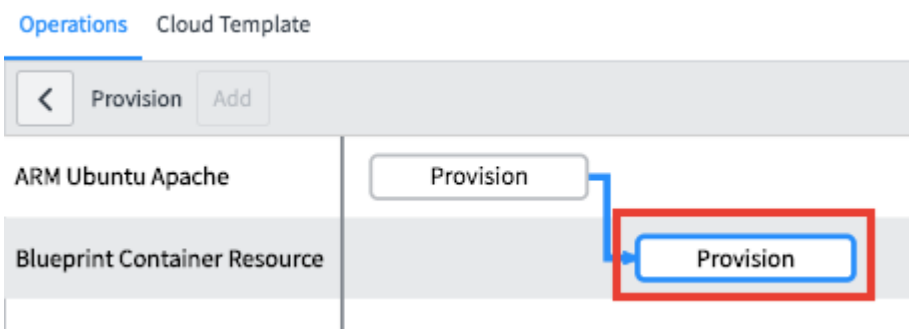


b. Klicken Sie unten auf die Registerkarte **Vorgänge** und dann auf **Bereitstellung**.



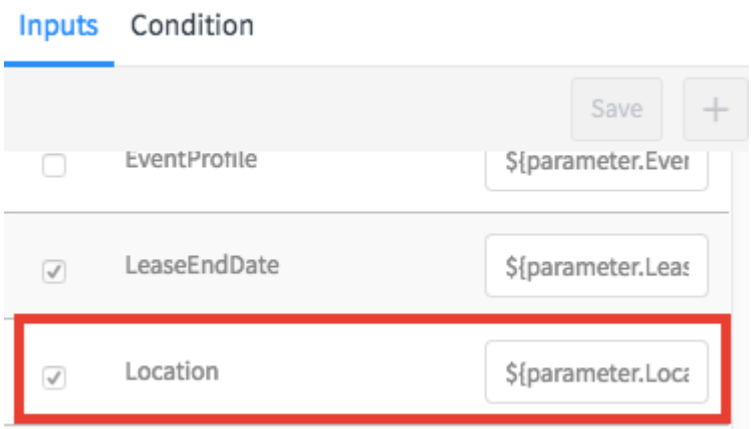
Der Bereitstellungsvorgang ist der Vorgang, den das System beim Erstellen der VM ausgelöst hat. Andere Standardvorgänge sind verfügbar, in diesem Beispiel konzentrieren wir uns aber auf den Bereitstellungsvorgang.

c. Klicken Sie auf den Block **Bereitstellung** für die Container-Ressource der Blaupause.



d. Beachten Sie, dass einer der Parameter auf der rechten Seite in der Inputs-Liste „Location“ lautet.
Dieser Parameter speichert den Statuswert, der aussagt, wo die VM im Datencenter lebt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

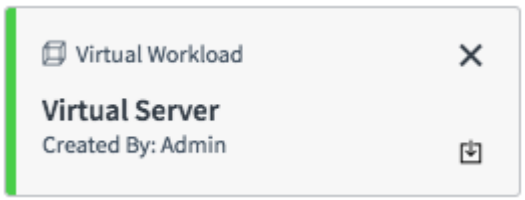


Eingaben können auf Container-Ebene festgelegt werden, wie in diesem Beispiel, oder auf einem beliebigen anderen Ressourcenblock. Standardmäßig ist der *location*-Parameter bereits für Sie im Blaupause-Container-Ressourcenblock festgelegt, sodass Sie ihn in jeder Blaupause wie dieser verwenden können. Wenn Sie den Status der Blaupause auf **Entwurf** wechseln, können Sie dem Container-Ressourcenblock der Blaupause weitere Parameter hinzufügen. Dem Ressourcenblock des virtuellen Servers können Sie keine Parameter hinzufügen. Für diese Anleitung werden keine weiteren Parameter benötigt.

3. Betrachten Sie die Ressourcenblöcke des virtuellen Servers und des Azure-Rechenzentrums, die in dieser Blaupause verwendet werden:

a. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Ressourcenblöcke**.

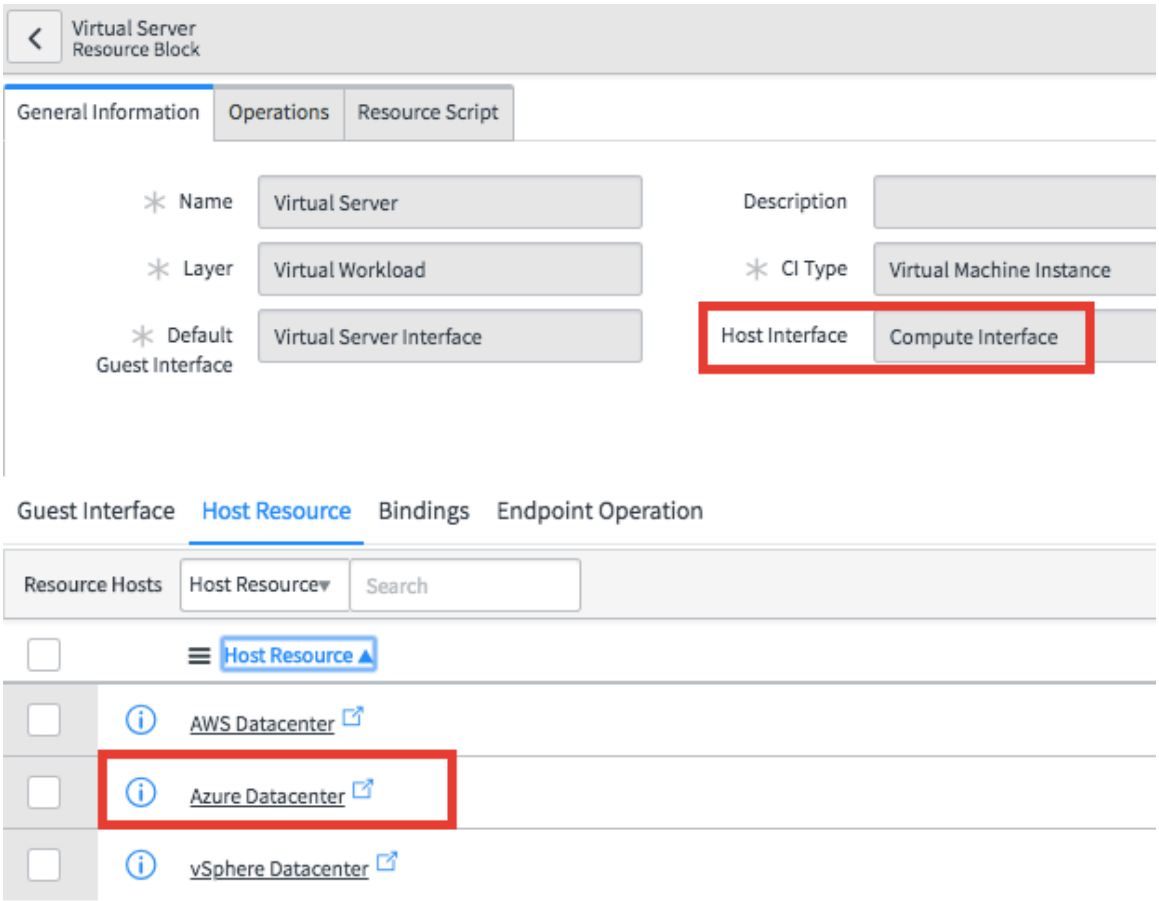
b. Suchen und öffnen Sie den Ressourcenblock **Virtueller Server**, der standardmäßig mit Cloud Provisioning and Governance bereitgestellt wird.



c. Klicken Sie im Ressourcenblock-Formular auf die zugehörige Liste **Hostressource**, um die Liste der unterstützten Host-Ressourcenblöcke anzuzeigen.

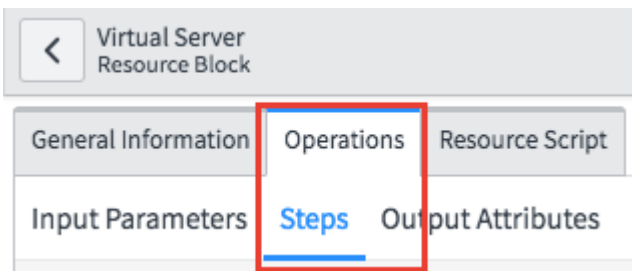
d. Beachten Sie die Host-Schnittstelle und die Host-Ressource, die bereits angegeben wurden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



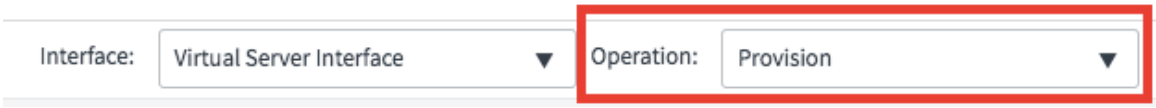
- Das Feld **Host Interface** (Host-Schnittstelle) gibt die Schnittstelle an, die mit der Gastschnittstelle im Ressourcenblock, der den virtuellen Computer hostet, übereinstimmen muss. In diesem Fall ist die Host-Schnittstelle die Compute-Schnittstelle, die auch die Gastschnittstelle auf dem Azure Datacenter-Ressourcenblock ist. Standardmäßig stellt der Rechenzentrum-Ressourcenblock mehrere Gastschnittstellen bereit, über die sich andere Ressourcenblöcke mit dem Datacenter verbinden können, beispielsweise der virtuelle Speicher.
- Die Spalte **HostResource** in der zugehörigen Liste **Host Resource** (Host-Ressource) gibt bereits **Azure Datacenter** (Azure-Rechenzentrum) an, was bedeutet, dass der Azure-Rechenzentrum-Ressourcenblock ein gültiger Host für diese VM ist.

e. Klicken Sie auf die Registerkarte **Vorgänge**, und klicken Sie dann auf die untergeordnete Registerkarte **Schritte**.



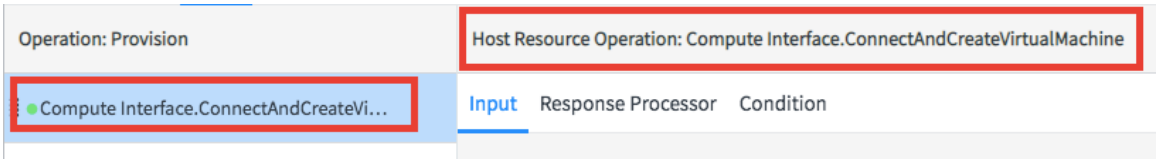
f. Wählen Sie in der Liste **Vorgang** die Option **Bereitstellung** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Denken Sie daran, dass es der Bereitstellungsvorgang ist, mit dem das System die VM erstellt. Andere Standardvorgänge sind verfügbar, in diesem Beispiel konzentrieren wir uns aber auf den Bereitstellungsvorgang.

g. Beachten Sie den Schritt, der in der Liste angezeigt wird, und die vollständige Schrittbeschreibung, die über den Eingabeparametern angezeigt wird:



(Schritt für Bereitstellung)

- **Host Resource Operation:** (Hostressourcenvorgang) gibt an, dass dieser Schritt einen Vorgang für die Hostressource (das Azure-Rechenzentrum in diesem Beispiel) aufruft.
- **Compute Interface** (Compute-Schnittstelle) ist die Gastschnittstelle im Azure-Rechenzentrum, die dieser Schritt verwendet.
- **ConnectAndCreateVirtualMachine** ist der Vorgang im Azure-Rechenzentrum, den dieser Schritt aufruft.

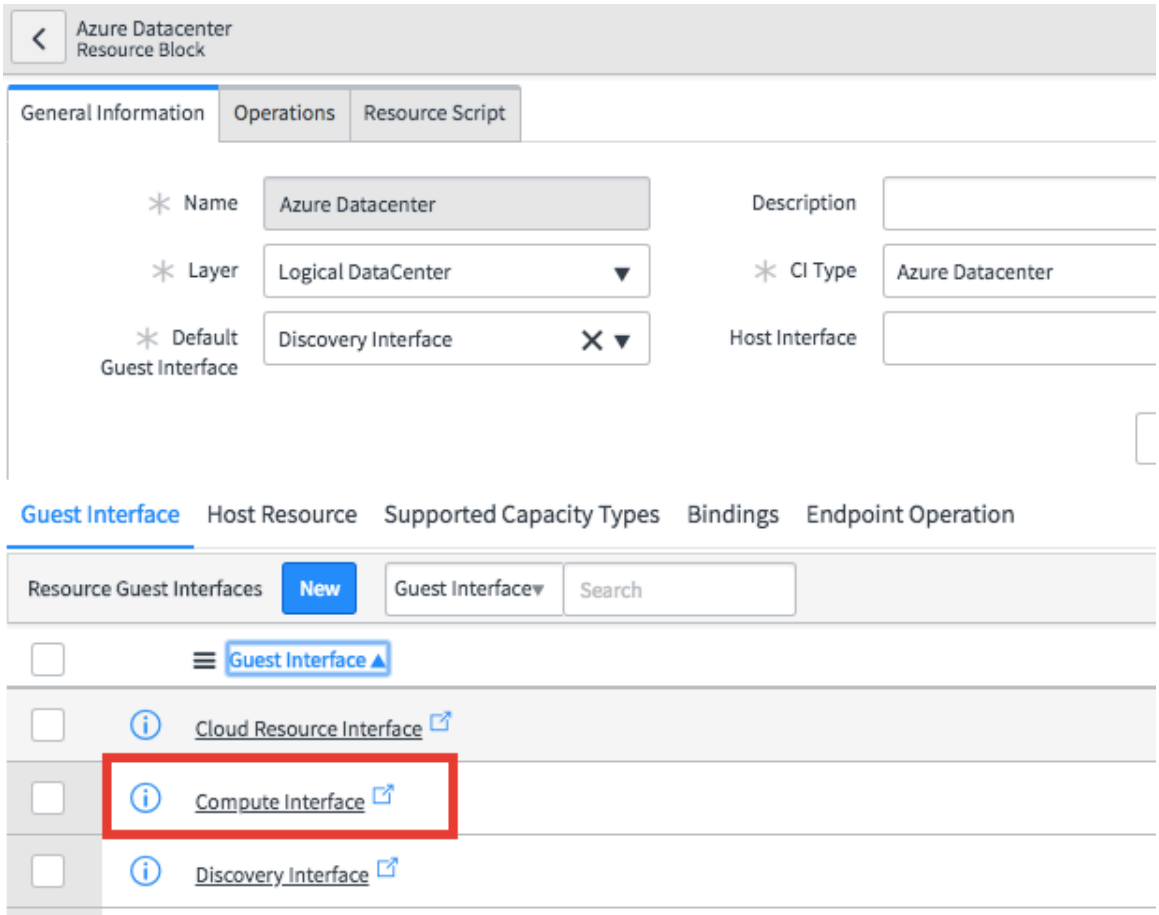
Hinweis: In diesem Fall ruft der Schritt einen Vorgang von einem anderen Ressourcenblock auf: dem Azure-Rechenzentrum. Schritte können CAPI auch direkt aufrufen, und dann kann CAPI REST-Aufrufe an die Cloud-Provider-API ausführen. Das sehen Sie, wenn Sie sich den Ressourcenblock des Azure-Rechenzentrums ansehen.

h. Navigieren Sie zurück zu **Entwurf** > **Ressourcenblöcke**.

i. Öffnen Sie den Ressourcenblock **Azure Datacenter** (Azure-Rechenzentrum), der den Host-Ressourcenblock darstellt, mit dem der virtuelle Server verbunden ist.

j. Beachten Sie die unterstützten Gastschnittstellen in der zugehörigen Liste **Guest Interface** (Gastschnittstelle):

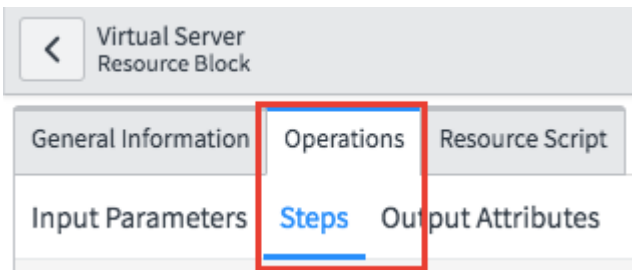
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



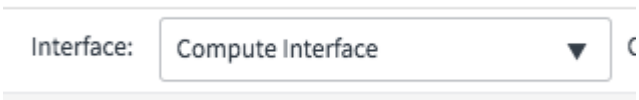
(Azure-Rechenzentrum mit Compute-API)

Diese Gastschnittstellen sind die Schnittstellen, die das Azure-Rechenzentrum anderen Ressourcenblöcken zur Verfügung stellt. Die Option **Compute Interface** (Compute-Schnittstelle) wird bereitgestellt, damit der Ressourcenblock des virtuellen Servers, der die Compute-Schnittstelle als Host-Schnittstelle angibt, eine Verbindung zum Rechenzentrum herstellen kann.

k. Klicken Sie auf die Registerkarte **Vorgänge**, und klicken Sie dann auf die untergeordnete Registerkarte **Schritte**.



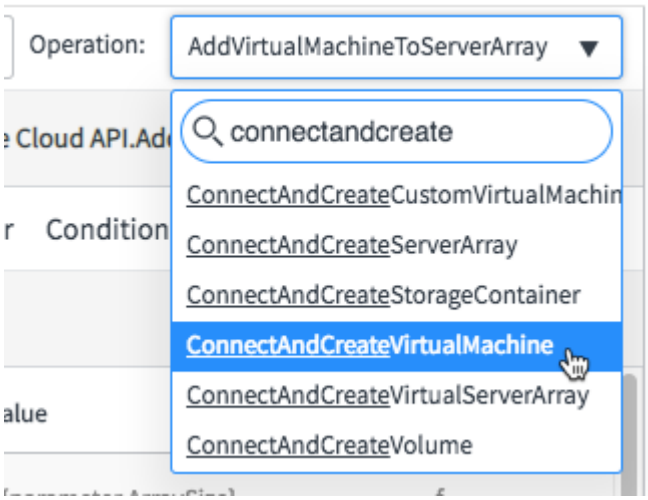
l. Wählen Sie in der Liste **Interface** (Schnittstelle) die Option **Compute Interface** (Compute-Schnittstelle) aus, wenn sie nicht bereits ausgewählt ist.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

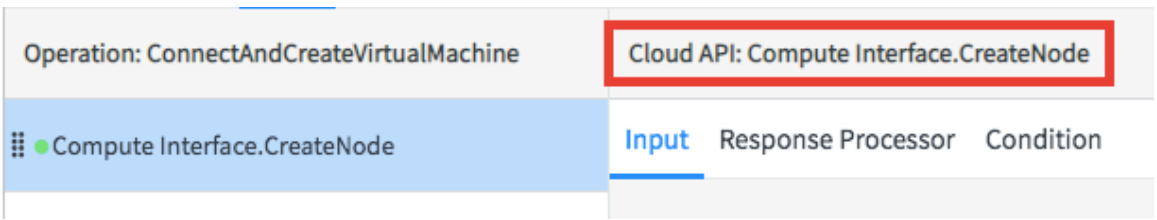
Denken Sie daran, dass diese Schnittstelle im Ressourcenblock des virtuellen Servers angegeben ist.

m. Suchen Sie in der Liste **Operation** (Vorgang) die Option **ConnectAndCreateVirtualMachine** und wählen Sie sie aus.



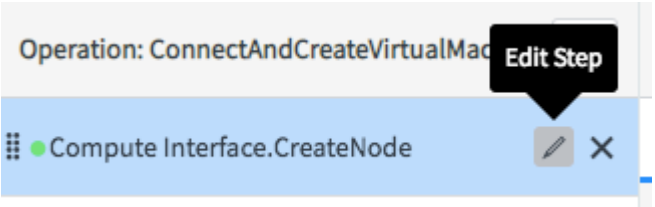
Dabei ist zu berücksichtigen, dass diese Schnittstelle im Ressourcenblock des virtuellen Servers angegeben ist.

n. Zu beachten ist der CAPI-Aufruf, der im einzigen Schritt für den Vorgang „ConnectAndCreateVirtualMachine“ verwendet wird:



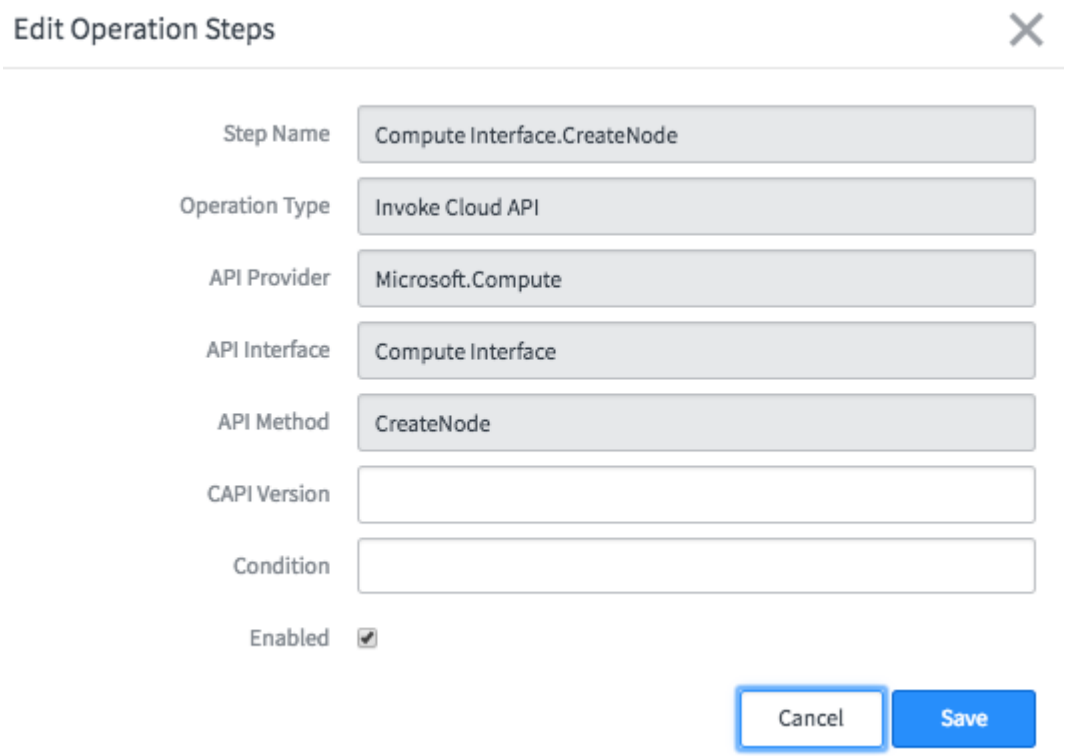
- **Cloud API:** (Cloud-API) Gibt an, dass dieser Schritt CAPI aufruft, sodass CAPI einen REST-Aufruf an den Cloud-Anbieter ausführen kann, der in diesem Fall Azure ist.
- **Compute Interface** (Compute-Schnittstelle) gibt die CAPI-Schnittstelle vor, die von diesem Schritt aufgerufen wird.
- **CreateNode** gibt die Methode an, die ausgeführt wird. Wie der Name schon sagt, weist diese Methode den Cloud-Anbieter an, den virtuellen Computer zu erstellen.

o. So öffnen Sie die Schrittkonfiguration: Der Ressourcenblock muss den Status **Draft** (Entwurf) aufweisen. Zeigen Sie dann auf den hervorgehobenen (blauen) Schritt, und klicken Sie auf das Symbol **Edit Step** (Schritt bearbeiten).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

p. Sehen Sie sich die Schrittkonfiguration an, und hier insbesondere die Einstellungen, die in CAPI integriert werden:



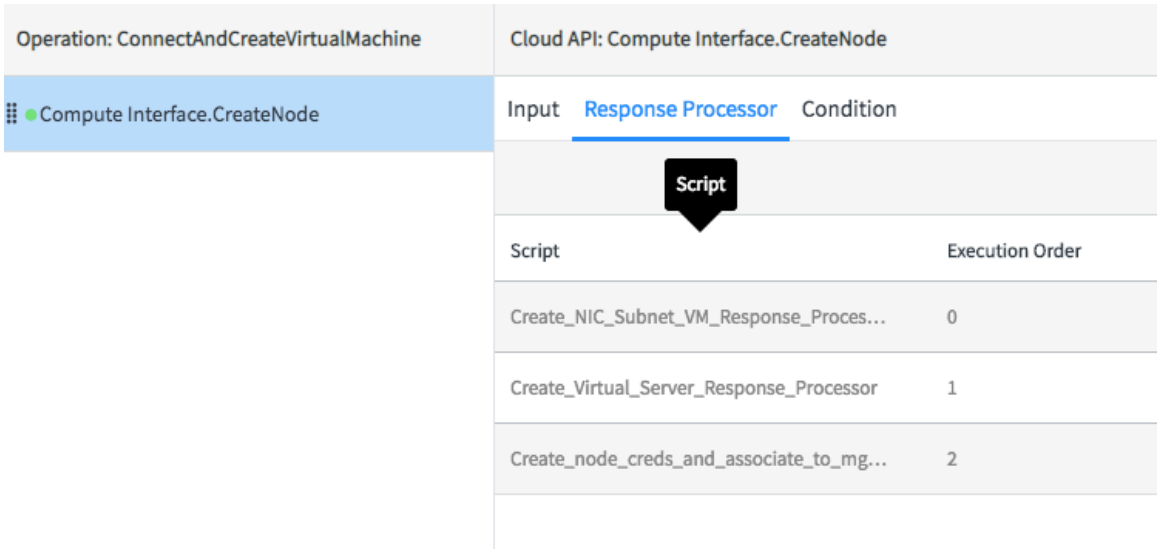
Feld	Beschreibung
Vorgangstyp	**Invoke Cloud API** (Cloud-API aufrufen) gibt an, dass dieser Schritt die CAPI über den angegebenen Anbieter, die angegebene Schnittstelle und die angegebene Methode aufrufen soll.
API-Anbieter (der eigentlich das Produkt ist)	**Microsoft.Compute** ist ein Produkt (nicht der tatsächliche Anbieter), das zum Azure-Anbieter gemäß der Definition in CAPI gehört.
API-Schnittstelle	**Compute Interface** (Compute-Schnittstelle) ist ein Produkt, das zum Azure-Anbieter gemäß der Definition in CAPI gehört.
API-Methode	**CreateNode** ist die Methode, die Azure zum Erstellen der VM aufruft.

Hinweis: Die CAPI-API-Definition verbindet den Anbieter (Azure), das Produkt (Microsoft.Compute), die Schnittstelle (Compute Interface) und die Methode (CreateNode).

q. Schließen Sie das Fenster.

r. Klicken Sie bei ausgewähltem Schritt **Compute Interface.CreateNode** auf **Response Processor** (Antwortprozessor); beachten Sie dabei das Skript **Create_Virtual_Server_Response_Processor**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieses Skript ist der Antwortprozessor, der die CMDB in Ihrer Instanz aktualisiert, nachdem der virtuelle Computer erstellt wurde.

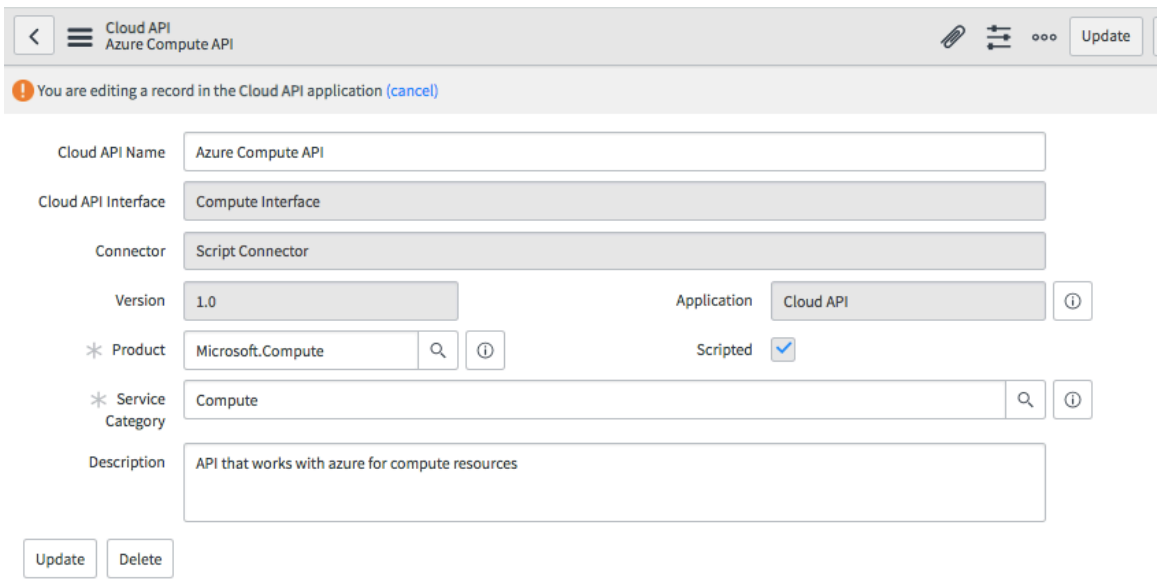
s. Zeigen Sie eine Erklärung des Skripts und das Beispiel an, das Teil des Themas unter Antwortprozessor erstellenist.
Wenn Sie die Überprüfung von diesem Themas abgeschlossen haben, kehren Sie zu diesem Thema zurück.

4. Sehen Sie sich die CAPI-Komponenten an, die zusammenarbeiten, um den virtuellen Computer bereitzustellen:

a. Navigieren Sie im Cloud-Administrationsportal zu **Entwurf** > **Cloud-API**.

b. Klicken Sie auf die Registerkarte **API** und suchen Sie dann nach einer offenen **Azure Compute-API**.

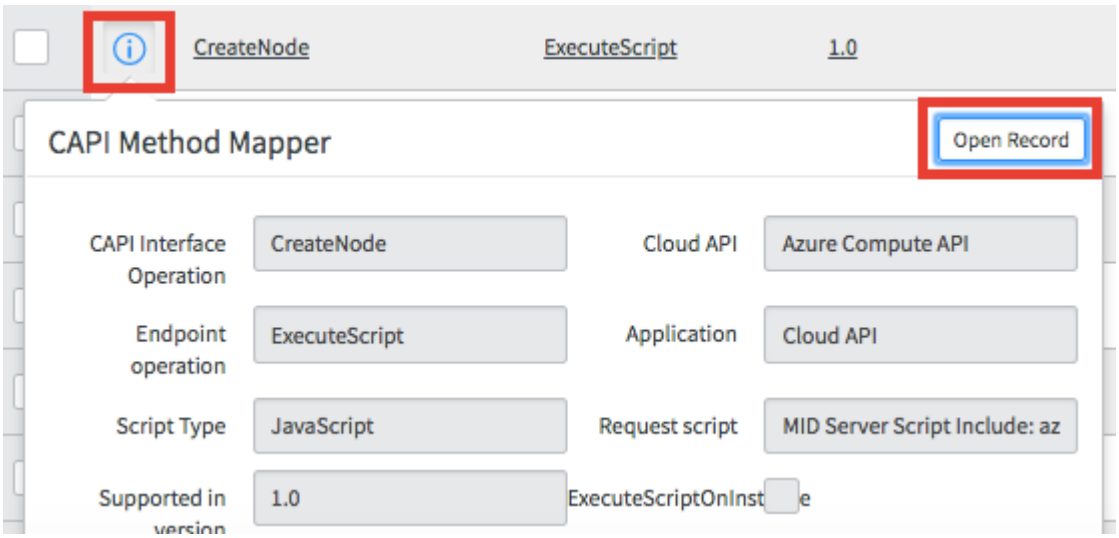
c. Sehen Sie sich an, wie diese CAPI-API eine Schnittstelle und ein Produkt miteinander verknüpft:



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

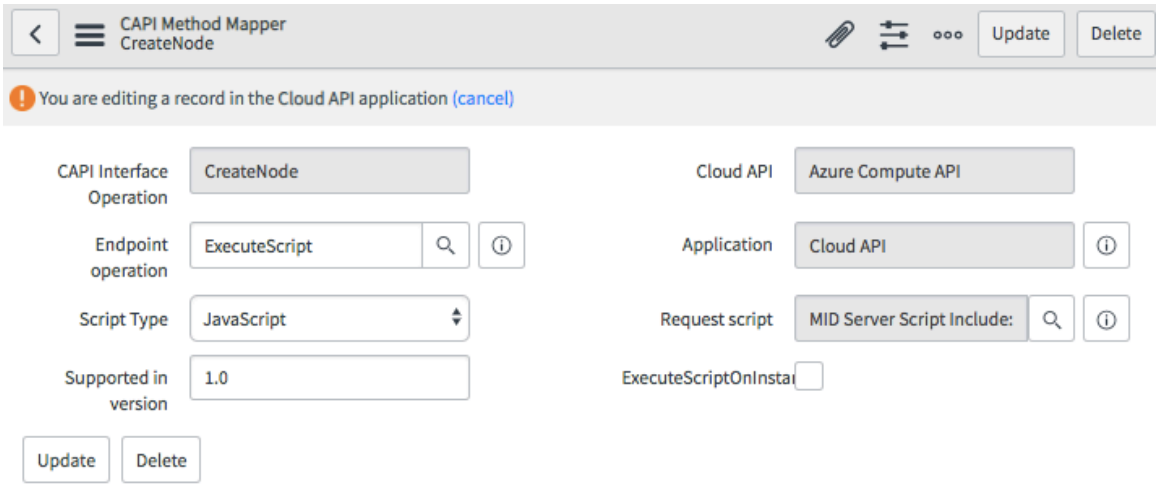
Feld	Beschreibung
Cloud-API-Schnittstelle	**Compute Interface** (Compute-Schnittstelle) ist die gleiche Schnittstelle, die im Ressourcenblock angegeben ist. Die Schnittstelle enthält die Definition für Methoden, einschließlich der Methode *CreateStack*.
Connector	**Script Connector** (Script-Connector) gibt an, dass diese CAPI eine Skripteinbindung MID-Server für jeden Vorgang bereitstellt. Die Skripteinbindung ruft die API auf. Sie können die Skripteinbindung ändern oder sogar eine neue erstellen.
Version	**1.0** gibt die Version der API an. Sie können über mehrere Versionen dieser API mit unterschiedlichen Versionsnummern verfügen. Beachten Sie, dass im Schritt im Ressourcenblock für das Rechenzentrum, den der virtuellen Computer erstellt, ein Versionsfeld bereitgestellt wird. Obwohl dieses Feld im Beispiel leer war, da nur eine Version dieser API vorhanden ist, können Sie eine andere Versionsnummer angeben.
Produkt	**Microsoft.Compute** ist das Produkt, das zum Anbieter in CAPI gehört. Dieses Produkt wird standardmäßig mit Cloud Provisioning and Governance geliefert und ist eines der am häufigsten verwendeten Produkte zum Erstellen virtueller Computer in Azure.

d. Klicken Sie in der zugehörigen Liste „CAPI Method Mappers“ (CAPI-Methodenzuordnungen) auf das Symbol für die Datensatzvorschau für den Datensatz *CreateNode*, und klicken Sie dann auf **Open Record** (Datensatz öffnen).



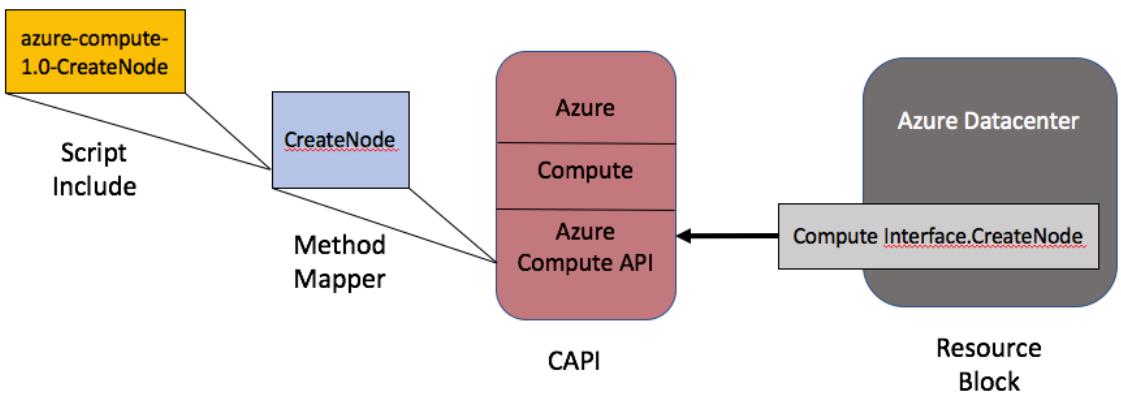
e. Sehen Sie sich die Methodenzuordnung für *CreateNode* an:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beachten Sie, dass **Endpoint Operation** (Endpunktvorgang) **Execute Script** (Skript ausführen) ist, was anzeigt, dass eine anpassbare Skripteinbindung zum Aufrufen von Funktionen in CAPI verwendet wird, die letztlich die REST-Aufrufe an Azure durchführt. Die Skripteinbindung *azure-compute-1.0-CreateNode* MID-Server ist im Feld **Request script** (Skript anfordern) angegeben.

Dieses Schaubild zeigt, wie die Komponenten – vom Ressourcenblock bis zur Skripteinbindung – verbunden sind:



f. Klicken Sie auf das Datensatzsymbol (ⓘ) für das **Anforderungsskript**.

Die Skripteinbindung *azure-compute-1.0-CreateNode* MID-Server wird geöffnet.

g. Überprüfen Sie den Inhalt des Skripts.

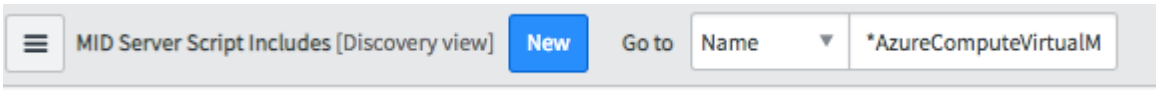
```
createNode();
function createNode(){
   var acp = new AzureComputeVirtualMachine(this.parameters,
 this.headers);
   var vm = acp.createVirtualMachine();

   return vm;
}
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das Skript ruft die Funktion *createVirtualMachine* in der Klasse *AzureComputeVirtualMachine* auf. Dies gibt den erstellten virtuellen Computer zurück. Die Klasse *AzureComputeVirtualMachine* erweitert *AzureCloudAPIBase*, eine der Basis-APIs in Cloud Provisioning and Governance.

h. Um die Klasse *AzureComputeVirtualMachine* anzuzeigen, bei der es sich um eine MID-Server -Skripteinbindung handelt, öffnen Sie die Instanzschnittstelle Basissystem (nicht Portal für Cloud-Admin.), und navigieren Sie dann zu **MID-Server** > **Skripteinbindungen**.

i. Suchen Sie nach *AzureComputeVirtualMachine* und öffnen Sie sie.



j. Überprüfen Sie die Funktion `createVirtualMachine`:

Die Funktion definiert viele Variablen, die zum Erstellen eines virtuellen Computers erforderlich sind, einschließlich *Location* (Rechenzentrum), den Namen des virtuellen Computers usw.

```
var location = this.parameters.get('Location');
var vmName = this.parameters.get('NodeName');
...
```

Diese Codezeile ruft die Funktion `_performVMOperation` in derselben Skripteinbindung auf und übergibt die erforderlichen Parameter. Beachten Sie, dass ein leerer Wert `''` für den Parameter `action` (Aktion) weitergeleitet wird:

```
var response = this._performVMOperation(subscriptionId, resourceGroup,
 vmName, '', 'PUT', jsonObj.encode(params));
```

Die Funktion `_performVMOperation` ruft die Funktion `_invokeRequest` auf, die sich in der Klasse *AzureCloudAPIBase* befindet:

```
return this._invokeRequest(this.pathDefault, param, method,
requestBody);
```

Die PUT-Methode für den REST-Aufruf wird im Parameter *method* angegeben.

Sehen Sie sich Skripteinbindung *AzureCloudAPIBase* MID-Server an . Die Funktion `_invokeRequest` ruft zuerst die Funktion `_getEndpoint` auf, um den Endpunkt abzurufen, sowie die Funktion `_getAPIInvoker` , um die Klasse *AzureAPIInvoker* als die Klasse zu identifizieren, die den tatsächlichen PUT-Aufruf aufruft:

```
var apiInvoker = this._getAPIInvoker(apiEndpoint, this.apiVersion);
```

AzureAPIInvoker ist von *CloudRESTAPIInvoker* erweitert, was die Basisfunktionen für alle Aufrufer bereitstellt. Sobald die richtige Aufruferklasse identifiziert ist, wird eine *response*-Variable erstellt, die den von der Funktion `invokePut` in *CloudRESTAPIInvoker* zurückgegebenen Wert enthält:

```
response = apiInvoker.invokePut(requestBody);
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Sehen Sie sich *CloudRESTAPIInvoker* an, die Basisklasse für alle Aufrufer. Die Funktion *invokePut* gibt die PUT-Methode an und ruft `getRequest` auf. Sie gibt die Antwort der Funktion *getResponse* zurück, die einen Statuscode und die Antwort von Azure abruft. In dieser Aufruferklasse wird die Verbindung zu Azure hergestellt.

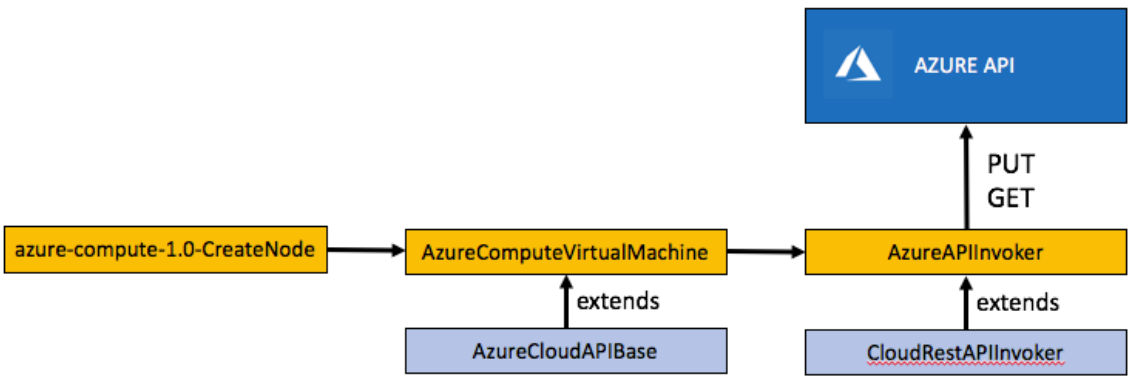
Kehren Sie zu Skripteinbindung *AzureComputeVirtualMachine* MID-Server zurück, und suchen Sie diese Zeilen:

```
var response = this._performVMOperation(subscriptionId, resourceGroup,
 vmName, '', 'PUT', jsonObj.encode(params));
this._compareVMState(response.id, 'PowerState/running');
var nodeResponse = this.getVirtualMachine(response.id);
```

Denken Sie daran, dass die Variable *response* vom Aufruf an `_performVMOperation` zurückgegeben wird, was die Antwort vom API-Aufrufer umfasst, der die PUT-Methode ausgelöst hat. Die Variable *nodeResponse* enthält die Antwort der Funktion `getVirtualMachine-`, die die ID des virtuellen Computers in der Antwort weiterleitet. Die Funktion `getVirtualMachine` ruft `_getVMInfo` auf, die ebenfalls die Funktion `_invokeRequest-` aufruft, die bereits zuvor aufgerufen wurde. Dieser Aufruf stellt eine weitere Verbindung zum Aufrufer dar, der die eigentlichen REST-Aufrufe durchführt. In diesem Fall ist der REST-Aufruf ein GET REST-Aufruf von Azure, um die Identität des virtuellen Computers zu erhalten.

Die Zeile `return nodeResponse;` gibt *nodeResponse* in der Funktion `createVirtualMachine` zurück, die von der Skripteinbindung MID-Server im Vorgang *createNode* aufgerufen wurde.

Diese Grafik zeigt die beteiligten Klassen:



k. Navigieren Sie zurück zum API-Formular von Azure Compute.

l. Klicken Sie auf die zugehörige Liste **API Config Overrides** (API-Konfigurationsüberschreibungen), und überprüfen Sie die für die Authentifizierung erforderlichen Elemente.

Konfigurationsparameter und Überschreibungswert	Beschreibung
ClientID	Die Client-ID ist erforderlich, um die Anwendung in Azure zu i

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Konfigurationsparameter und Überschreibungswert	Beschreibung
$(CloudCredential.client_id)	
EndpointURL $(CloudCredential.URL)	Die Endpunkt-URL ist die autorisierende Eingabe in Azure.
SecretKey $(CloudCredential.secret_key)	Der geheime Schlüssel wird zur Autorisierung des Clients verw
TenantID $(CloudCredential.tenant_id)	Die Mandanten-ID ist der global eindeutige Bezeichner für de
EnrollmentNumber $(CloudCredential.sn_cmp_ea_credential.enrollment_number) EnrollmentToken $(CloudCredential.sn_cmp_ea_credential.access_key)	Die Azure-Registrierungsnummer und das Token dienen dem Registrierungskonto.

Unter Anmeldeinformationen des Azure-Dienstprinzipals in der Instanz speichern finden Sie weitere Informationen zu den Azure-Informationen, die in diesen Überschreibungen verwendet werden.

m. Navigieren Sie zurück zu **Entwurf** > **Cloud-API**, und klicken Sie dann auf die Registerkarte **Schnittstelle**.

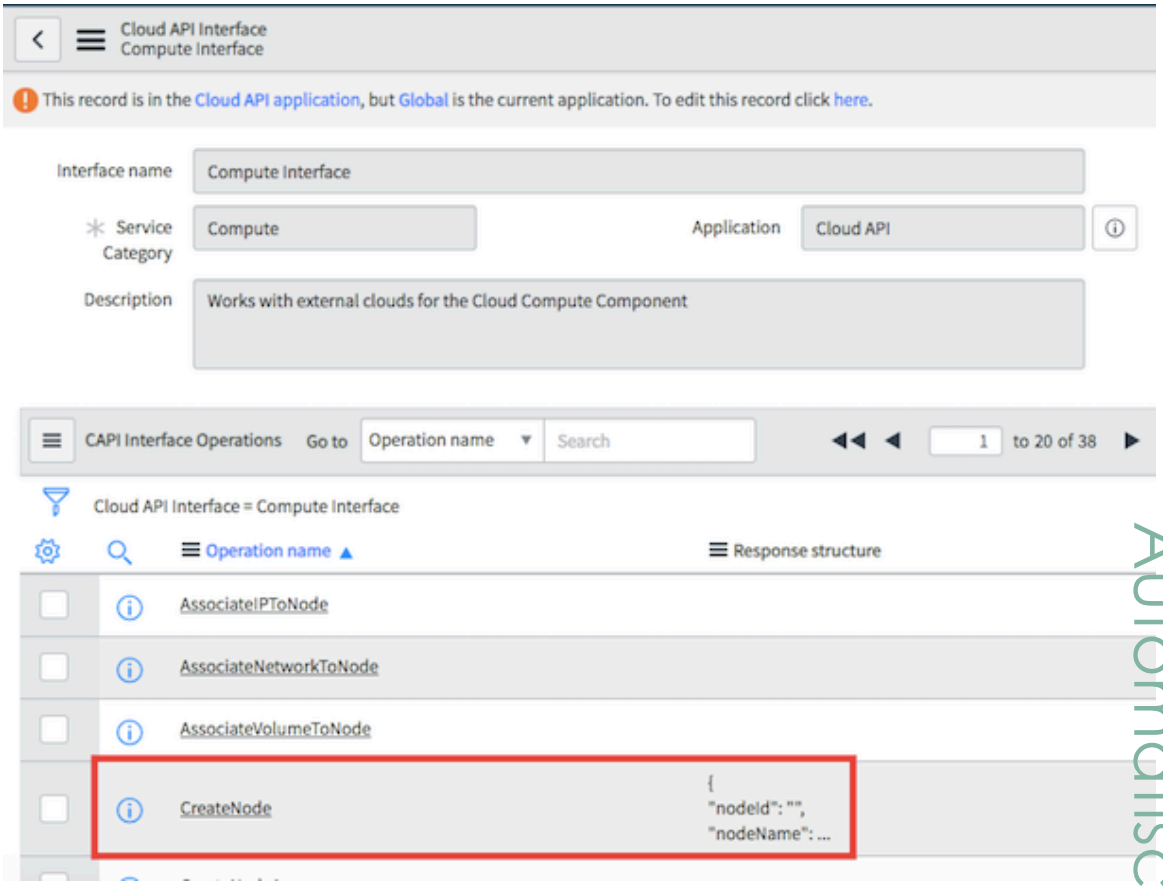
n. Suchen Sie nach **Compute Interface** (Compute-Schnittstelle) und öffnen Sie diese.

o. Überprüfen Sie den Inhalt der Schnittstelle.

Beachten Sie, dass die Schnittstelle REST-Antwortstrukturen für Methoden wie *CreateNode* bereitstellt. In der Regel müssen vorhandene Schnittstellen nicht geändert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Beachten Sie die Servicekategorie und die Vorgänge:

Feld oder zugehörige Liste	Beschreibung
Servicekategorie	Die Servicekategorie klassifiziert die Schnittstelle. Die Kategorie für die Compute-Schnittstelle ist ebenfalls **Compute**.
CAPI-Schnittstellenvorgänge	Die Schnittstellenvorgänge definieren die JSON-Struktur für den REST-Aufruf und die Parameter, die für die Schnittstelle erforderlich sind.

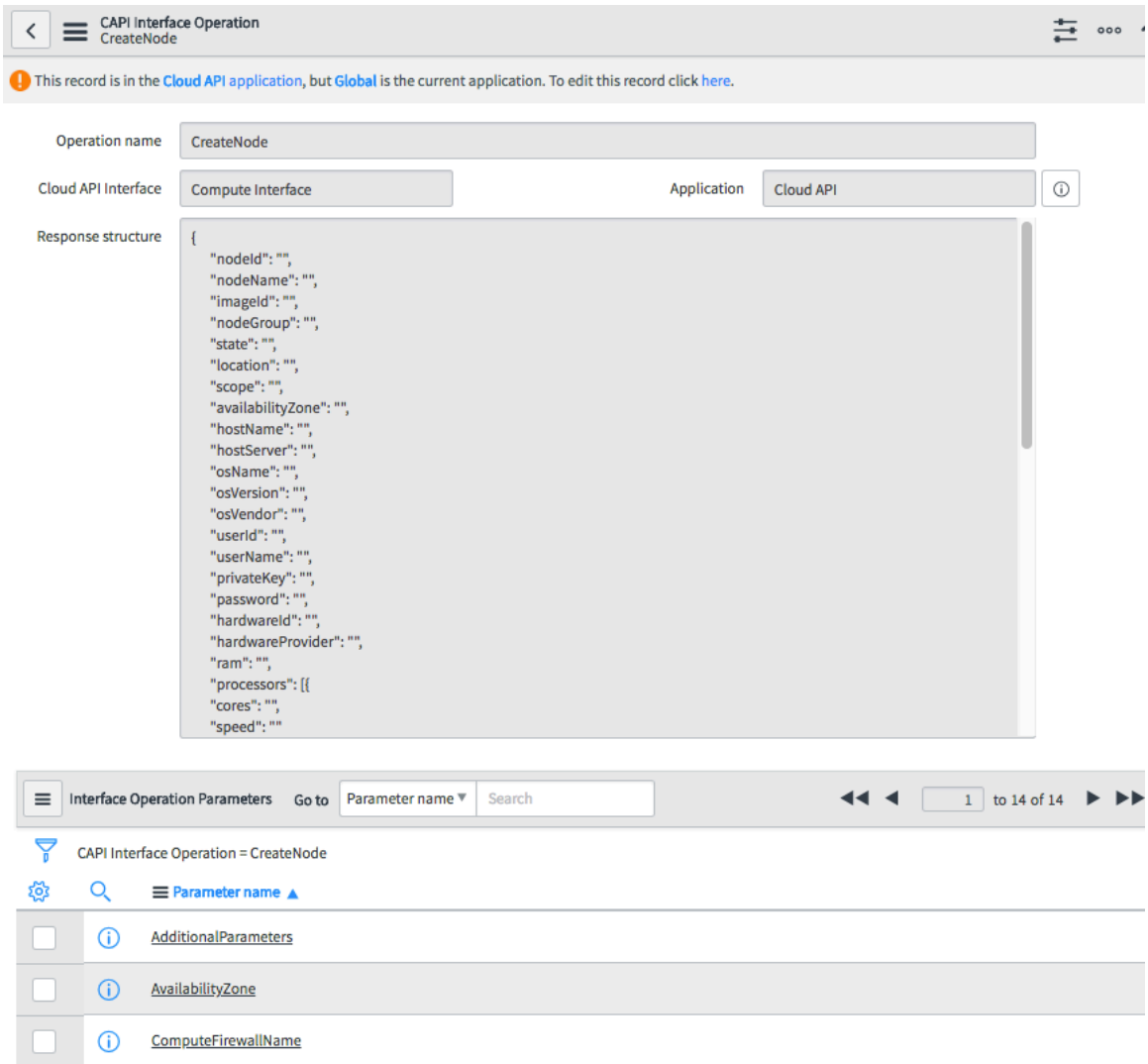
p. Klicken Sie auf den CAPI-Schnittstellenvorgang **CreateNode**.
Über diesen Vorgang wird das Framework für die Erstellung des virtuellen EC2-Servers bereitgestellt.

q. Überprüfen Sie die Komponenten des Vorgangs:

Feld oder zugehörige Liste	Beschreibung
Antwortstruktur	Die Antwortstruktur ist das JSON-Framework für den REST API-Aufruf. Diese Struktur bietet eine Liste von Attributen, die der Anbieter zum Erstellen der virtuellen Ressource mit leeren Werten verwenden kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld oder zugehörige Liste	Beschreibung
Parameter für Schnittstellenvorgänge	Diese Parameter sind auch die Parameter, die die CAPI-Schnittstelle vom System benötigt, damit sie die Struktur im REST-Aufruf an den Cloud-Anbieter übergeben kann.



r. Navigieren Sie zurück zu **Entwurf** > **Cloud-API** und klicken Sie dann auf die Registerkarte **Provider**.

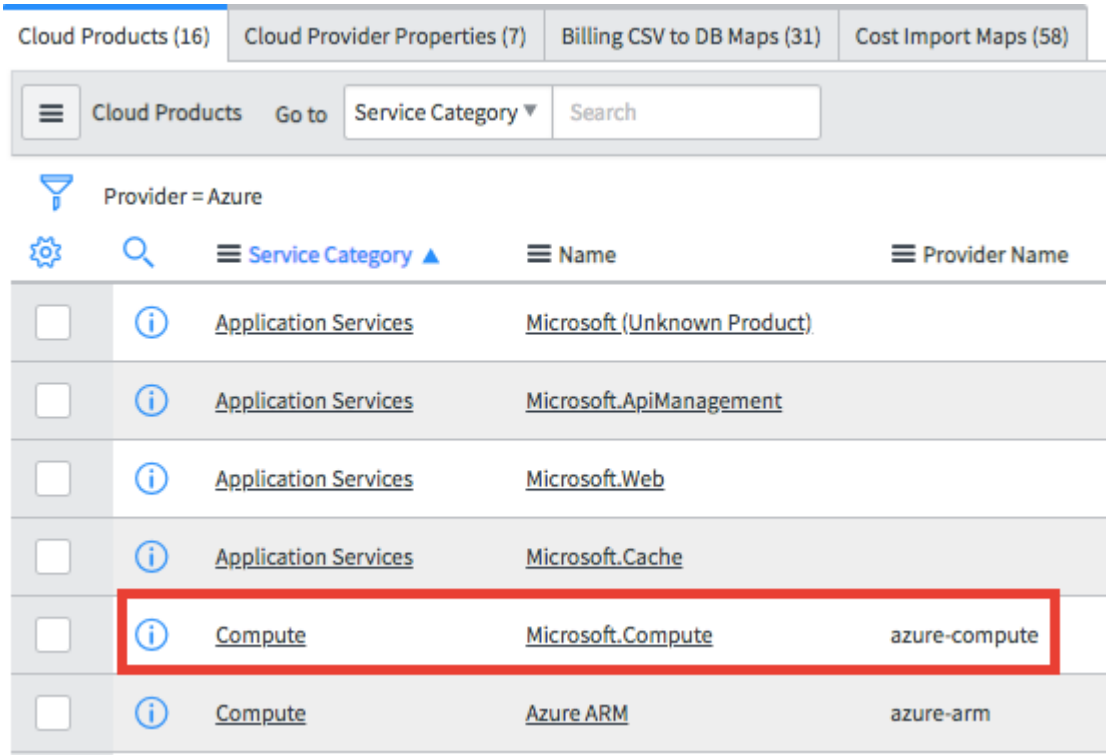
s. Öffnen Sie den Anbieter **Azure**.

Das Formular „Azure Cloud Provider“ (Azure-Cloud-Anbieter) wird geöffnet und zeigt an, dass dieser Anbieter auf einer vorhandenen CMDB-Klasse basiert: **Azure Datacenter [cmdb_ci_azure_datacenter]**.

t. Klicken Sie auf die zugehörige Liste „Cloud Products“ (Cloud-Produkte), und sortieren Sie die Liste nach der Spalte **Name**.

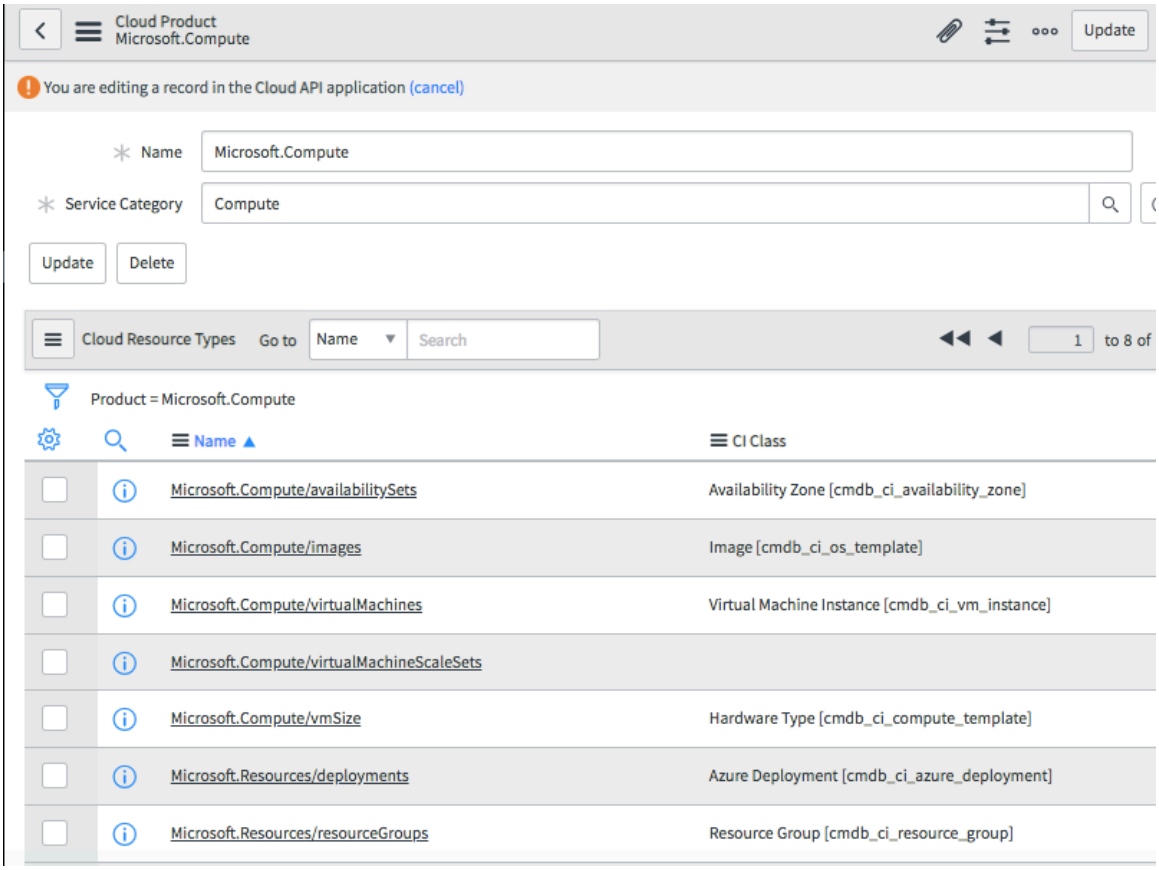
Beachten Sie, dass standardmäßig mehrere Azure-Produkte verfügbar sind. Eines der am häufigsten verwendeten Azure-Produkte, die aus Vorlagen erstellt werden, ist **Microsoft.Compute**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



u. Klicken Sie in der Spalte **Name** auf **Microsoft.Compute**.
Beachten Sie, dass das Produkt viele Ressourcentypen angibt, die jeweils einer CI-Klasse zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

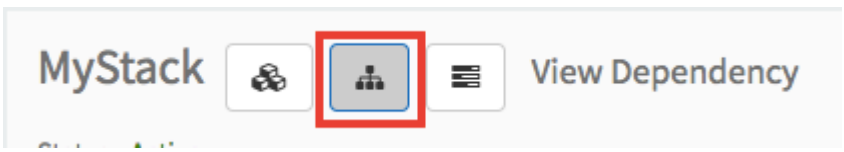


Diese Ressourcentypen geben einige, aber nicht alle CIs an, die sich auf den virtuellen Computer beziehen. Der Antwortprozessor im Ressourcenblock füllt CIs mit Daten aus, wenn der Cloud-Anbieter den virtuellen Computer bereitstellt.

5. So zeigen Sie die wichtigen mit der VM verbundenen CIs an:

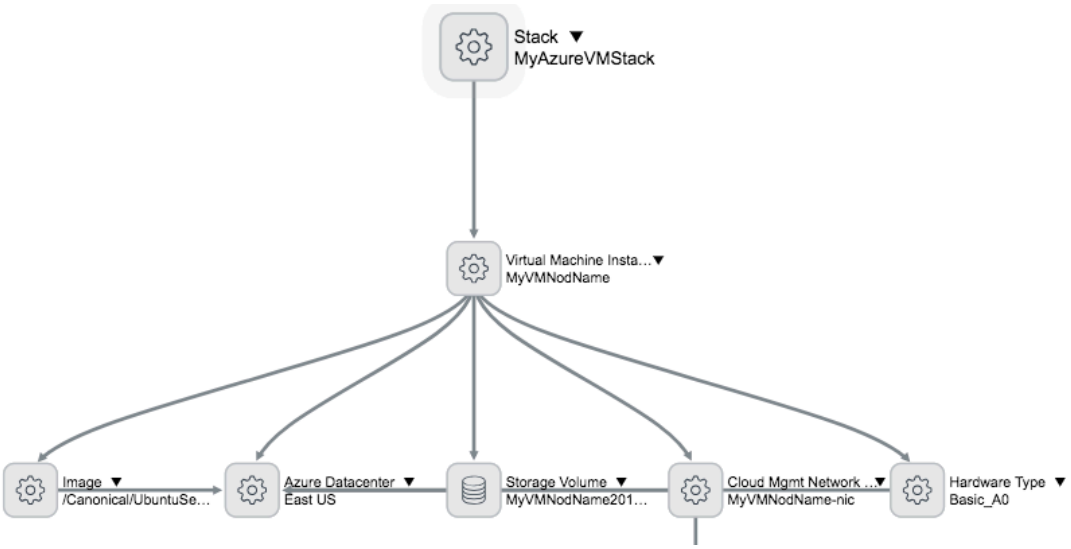
a. Klicken Sie in Cloudbenutzerportal auf **Stapel**, und öffnen Sie dann den Stapel, der die VM enthält.

b. Klicken Sie auf das Symbol **View Dependency** (Abhängigkeit anzeigen).



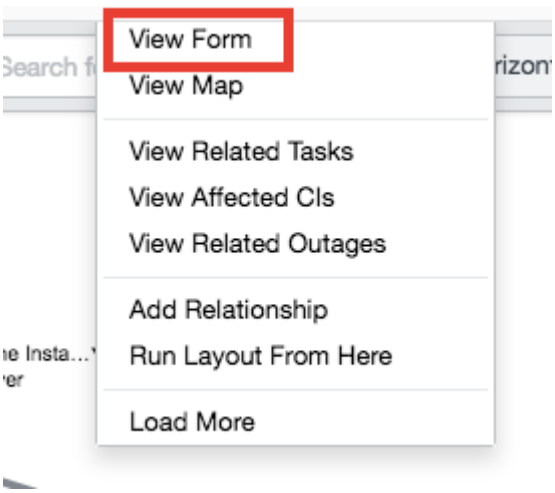
Die Abhängigkeitszuordnung zeigt das Stapel-CI oben, den virtuellen Computer in der Mitte und die verschiedenen zugehörigen CIs unten, z. B. das Bild.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



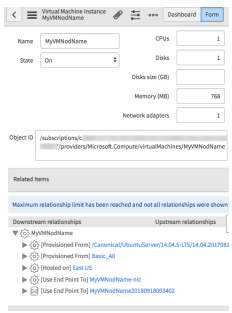
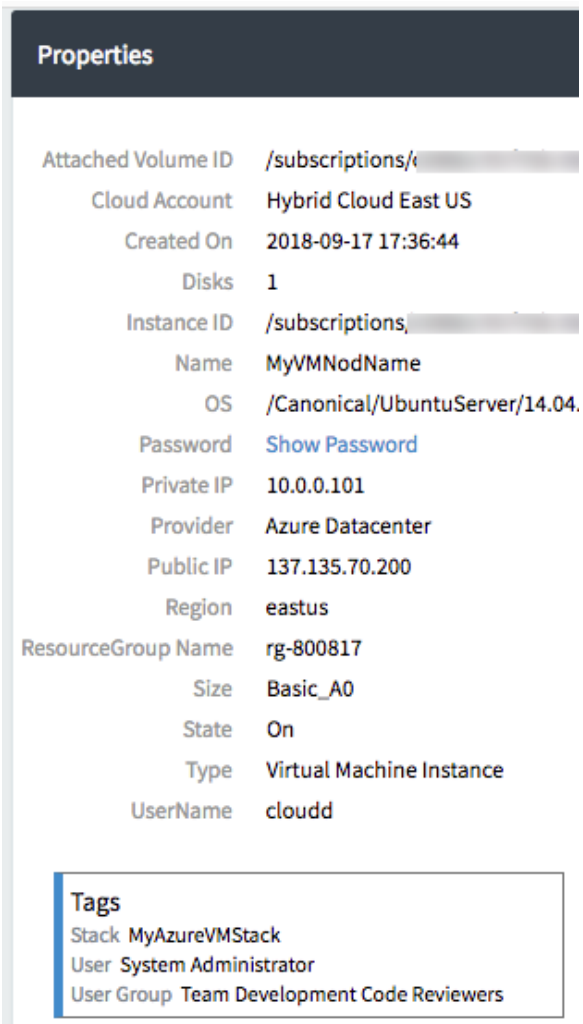
c. Sie rufen das Formular für den virtuellen Computer in der CMDB auf, indem Sie mit der rechten Maustaste auf den Pfeil neben einem CI klicken.

d. Wählen Sie im Menü **View Form** (Formular anzeigen).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das CI-Formular wird geöffnet und zeigt an, dass viele der Informationen bereits auf Cloudbenutzerportal verfügbar sind, wenn Sie die Eigenschaften des virtuellen Computers anzeigen lassen.

VM-CI-Formular	Eigenschaften des virtuellen Computers in Cloudbenutzerportal
	

VM-Bereitstellung bei AWS – Beispiel-Vorstellung

Dieses Beispiel führt Sie durch die Komponenten von Cloud Provisioning and Governance, die während der Bereitstellung eines virtuellen Computers in einem AWS-Rechenzentrum in Betrieb sind. Zu den behandelten Themen gehören Blaupausen, Ressourcenblöcke, die Cloud-API (CAPI) und Skripteinbindungen MID-Server.

Vorbereitungen

Erforderliche Rolle: admin

Warum und wann dieser Vorgang ausgeführt wird

Die Vorstellung beginnt mit einem virtuellen Computer unter Windows, den der Benutzer bereits in AWS bereitgestellt hat. Anschließend werden die Blaupause mit virtuellem Computer, Ressourcenblöcke und in den Ressourcenblöcken angegebene CAPI-Aufrufe vorgestellt. Abschließend zeigt die Vorstellung, wie eine MID-Server-Skripteinbindung die tatsächlichen Aufrufe an die AWS-API durchführt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

In diesem Beispiel werden Standardressourcenblocks und Skript Includes verwendet, die in Ihrer Instanz verfügbar sind. Deshalb können Sie, obwohl Sie möglicherweise keine bereitgestellte VM auf Ihrer Instanz haben, trotzdem diese Schritte befolgen und die in diesem Beispiel verwendeten Komponenten anzeigen, um die Arbeitsweise der Komponenten zu verstehen.

Ein Beispiel für einen virtuellen Computer in Azure finden Sie unter Azure VM-Bereitstellung – exemplarische Vorstellung.

Hinweis: Die Begriffe virtueller Computer, VM (für „Virtual Machine“) und virtueller Server sind in diesem Beispiel synonym.

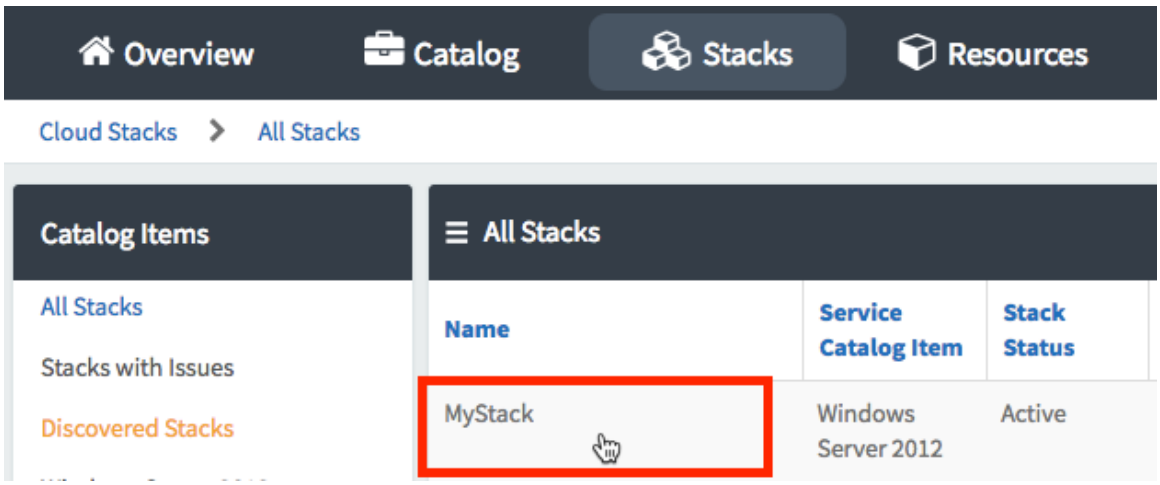
Prozedur

1. Betrachten Sie eine eingerichtete VM im Cloud User Portal und richten Sie den Fokus auf einige Details zur VM:

   a. Öffnen Sie in Ihrer Instanz Cloudbenutzerportal (Cloud Provisioning and Governance. **Cloud-Anwenderportal**) an.

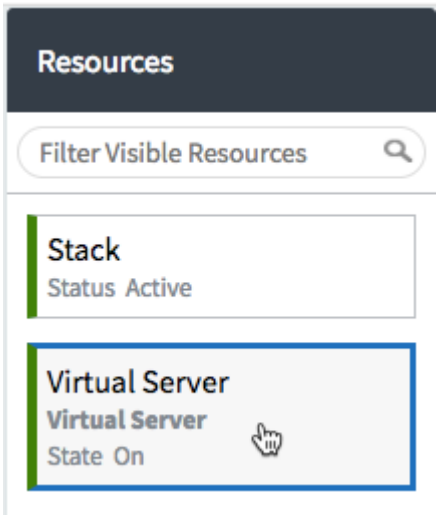
   b. Rufen Sie eine bereitgestellte VM in einem Stapel auf, z. B. diese Windows VM, indem Sie auf **Stapel** und dann auf den Namen des Stapels klicken.

   In diesem Beispiel heißt der Stapel **MyStack**.

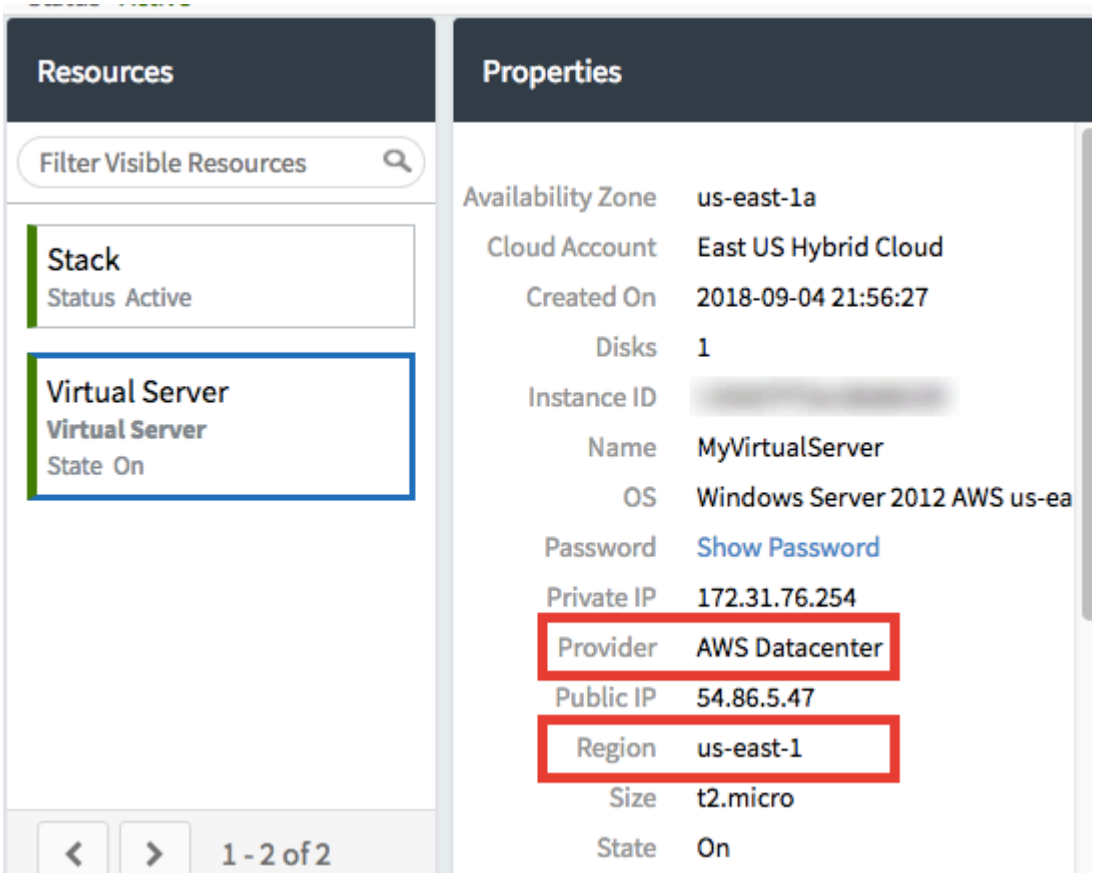


   c. Klicken Sie unter **Resources**(Ressourcen) auf den virtuellen Computer im Stapel.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



d. Rufen Sie die Eigenschaften der VM auf; beachten Sie, dass sich die VM in einem AWS-Rechenzentrum in der Region „us-east-1“ befindet.

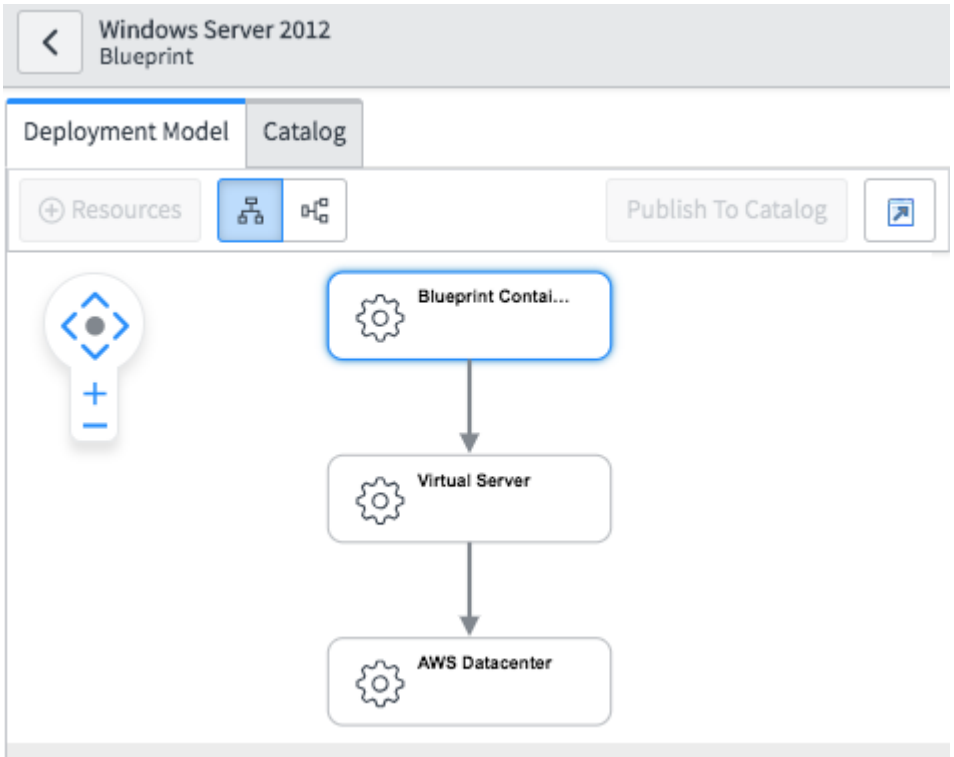


2. Sehen Sie sich die Blaupause an, auf der die VM basiert:

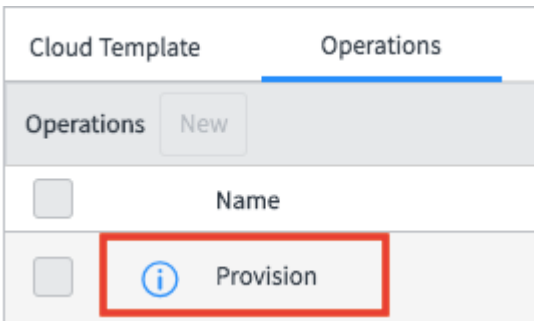
a. Navigieren zu **Entwurf** > **Blueprints**, und öffnen Sie dann einen Blueprint mit einem virtuellen Server im Azure-Rechenzentrum. Die Registerkarte **Bereitstellungsmodell** wird standardmäßig angezeigt und zeigt Ihnen die verschiedenen Komponenten des Blueprints.

Diese Beispiel-Blaupause hat drei Komponenten: den Container, den virtuellen Server, der die bereitgestellte VM ist, und das AWS-Rechenzentrum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

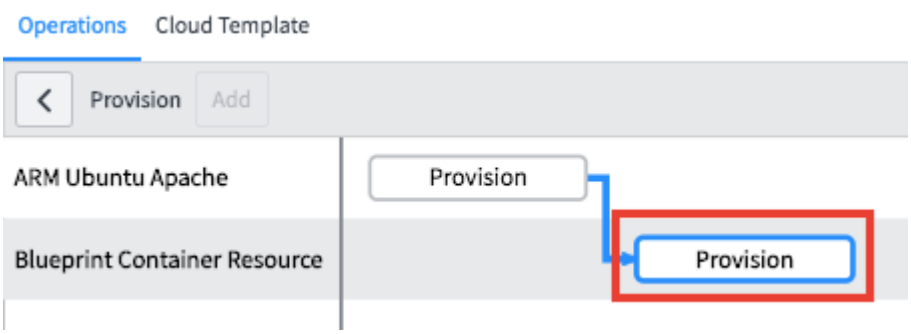


b. Klicken Sie unten auf die Registerkarte **Vorgänge** und dann auf **Bereitstellung**.



Der Bereitstellungsvorgang ist der Vorgang, den das System beim Erstellen der VM ausgelöst hat. Andere Standardvorgänge sind verfügbar, in diesem Beispiel konzentrieren wir uns aber auf den Bereitstellungsvorgang.

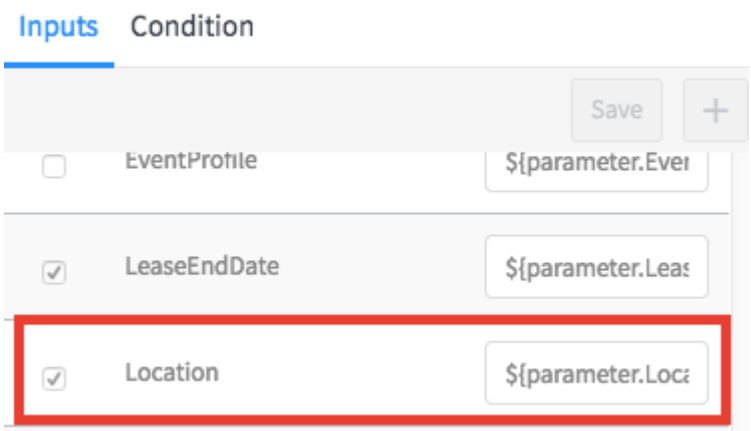
c. Klicken Sie auf den Block **Bereitstellung** für die Container-Ressource der Blaupause.



d. Beachten Sie, dass einer der Parameter auf der rechten Seite in der Inputs-Liste „Location“ lautet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Dieser Parameter speichert den Statuswert, der aussagt, wo die VM im Datencenter lebt.

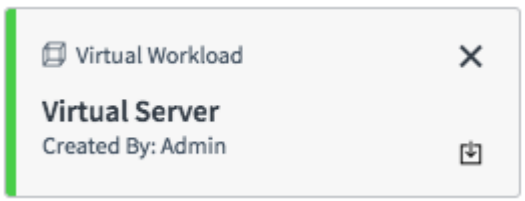


Eingaben können auf Container-Ebene festgelegt werden, wie in diesem Beispiel, oder auf einem beliebigen anderen Ressourcenblock. Standardmäßig ist der *Location*-Parameter bereits für Sie im Blaupause-Container-Ressourcenblock festgelegt, sodass Sie ihn in jeder Blaupause wie dieser verwenden können. Wenn Sie den Status der Blaupause auf **Entwurf** wechseln, können Sie dem Container-Ressourcenblock der Blaupause weitere Parameter hinzufügen. Dem Ressourcenblock des virtuellen Servers können Sie keine Parameter hinzufügen. Für diese Anleitung werden keine weiteren Parameter benötigt.

3. Betrachten Sie die Ressourcenblöcke des virtuellen Servers und des AWS-Rechenzentrums, die in dieser Blaupause verwendet werden:

   a. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Ressourcenblöcke**.

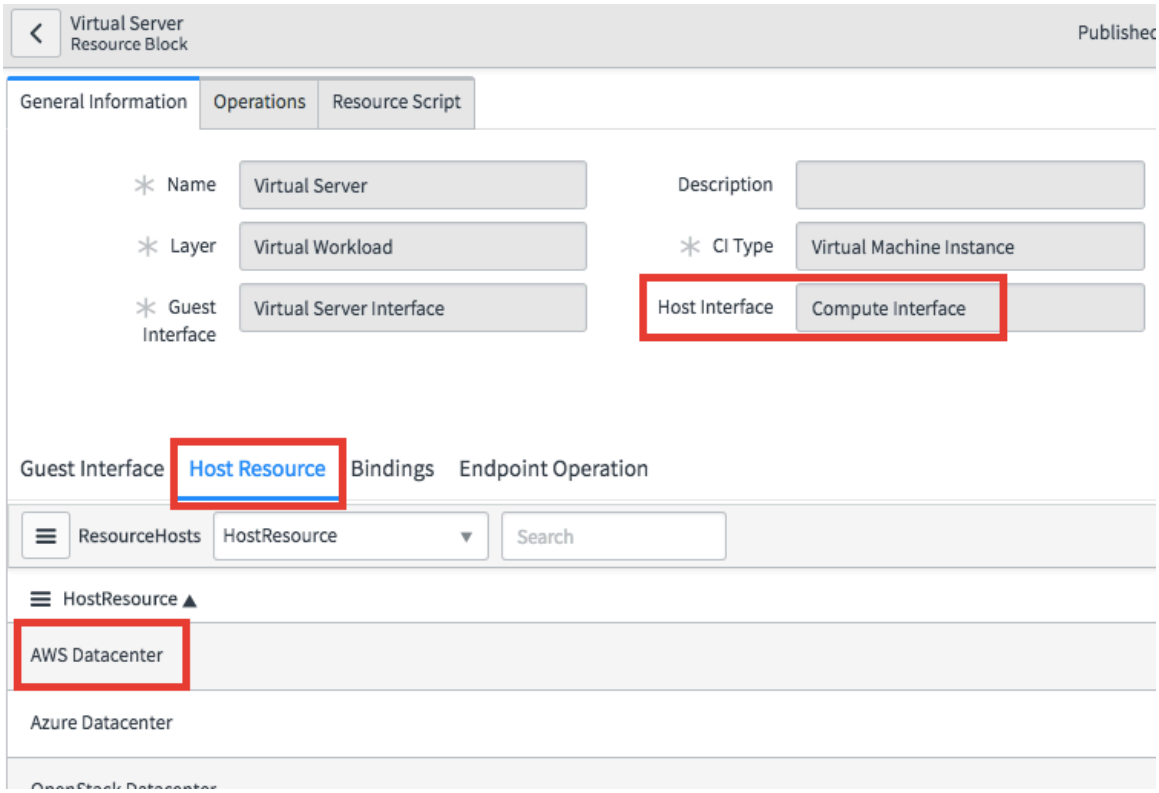
   b. Suchen und öffnen Sie den Ressourcenblock **Virtueller Server**, der standardmäßig mit Cloud Provisioning and Governance bereitgestellt wird.



   c. Klicken Sie im Ressourcenblock-Formular auf die zugehörige Liste **Hostressource**, um die Liste der unterstützten Host-Ressourcenblöcke anzuzeigen.

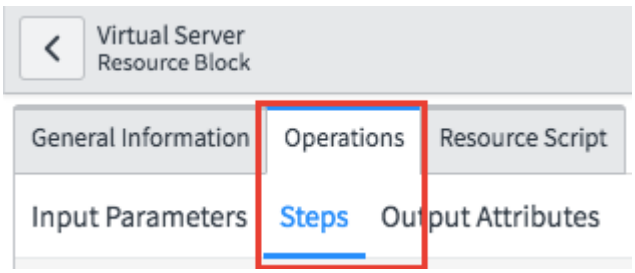
   d. Wie Sie erkennen können, wurden Host-Schnittstelle und Host-Ressource bereits angegeben:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

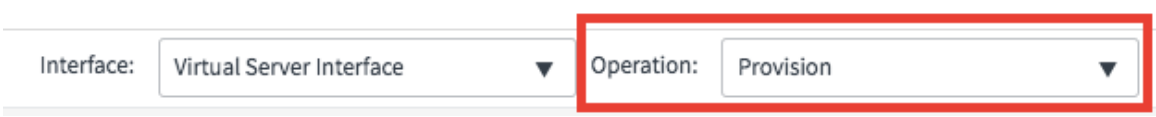


- Das Feld **Host Interface** (Host-Schnittstelle) gibt die Schnittstelle an, die mit der Gastschnittstelle im Ressourcenblock, der den virtuellen Computer hostet, übereinstimmen muss. In diesem Fall ist die Host-Schnittstelle die Compute-Schnittstelle, die auch die Gastschnittstelle auf dem Ressourcenblock des AWS-Rechenzentrums ist. Standardmäßig stellt der Rechenzentrum-Ressourcenblock mehrere Gastschnittstellen bereit, über die sich andere Ressourcenblöcke mit dem Datacenter verbinden können, beispielsweise der virtuelle Speicher.
- Die Spalte **HostResource** in der zugehörigen Liste **Host Resource** (Host-Ressource) gibt bereits **AWS Datacenter** (AWS-Rechenzentrum) an, was bedeutet, dass der Ressourcenblock des AWS-Rechenzentrums ein gültiger Host für diese VM ist.

e. Klicken Sie auf die Registerkarte **Vorgänge**, und klicken Sie dann auf die untergeordnete Registerkarte **Schritte**.



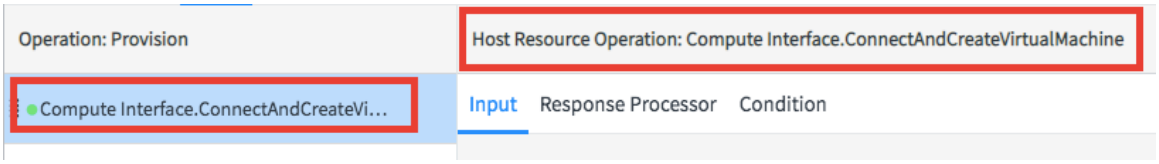
f. Wählen Sie in der Liste **Vorgang** die Option **Bereitstellung** aus.



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Denken Sie daran, dass es der Bereitstellungsvorgang ist, mit dem das System die VM erstellt. Andere Standardvorgänge sind verfügbar, in diesem Beispiel konzentrieren wir uns aber auf den Bereitstellungsvorgang.

g. Beachten Sie den Schritt, der in der Liste angezeigt wird, und die vollständige Schrittbeschreibung, die über den Eingabeparametern angezeigt wird:



(Schritt für Bereitstellung)

- **Host Resource Operation:** (Host-Ressourcenvorgang) gibt an, dass dieser Schritt einen Vorgang für die Host-Ressource (das AWS-Rechenzentrum in diesem Beispiel) aufruft.
- **Compute Interface** (Compute-Schnittstelle) ist die Gastschnittstelle im AWS-Rechenzentrum, die dieser Schritt verwendet.
- **ConnectAndCreateVirtualMachine** ist der Vorgang im AWS-Rechenzentrum, den dieser Schritt aufruft.

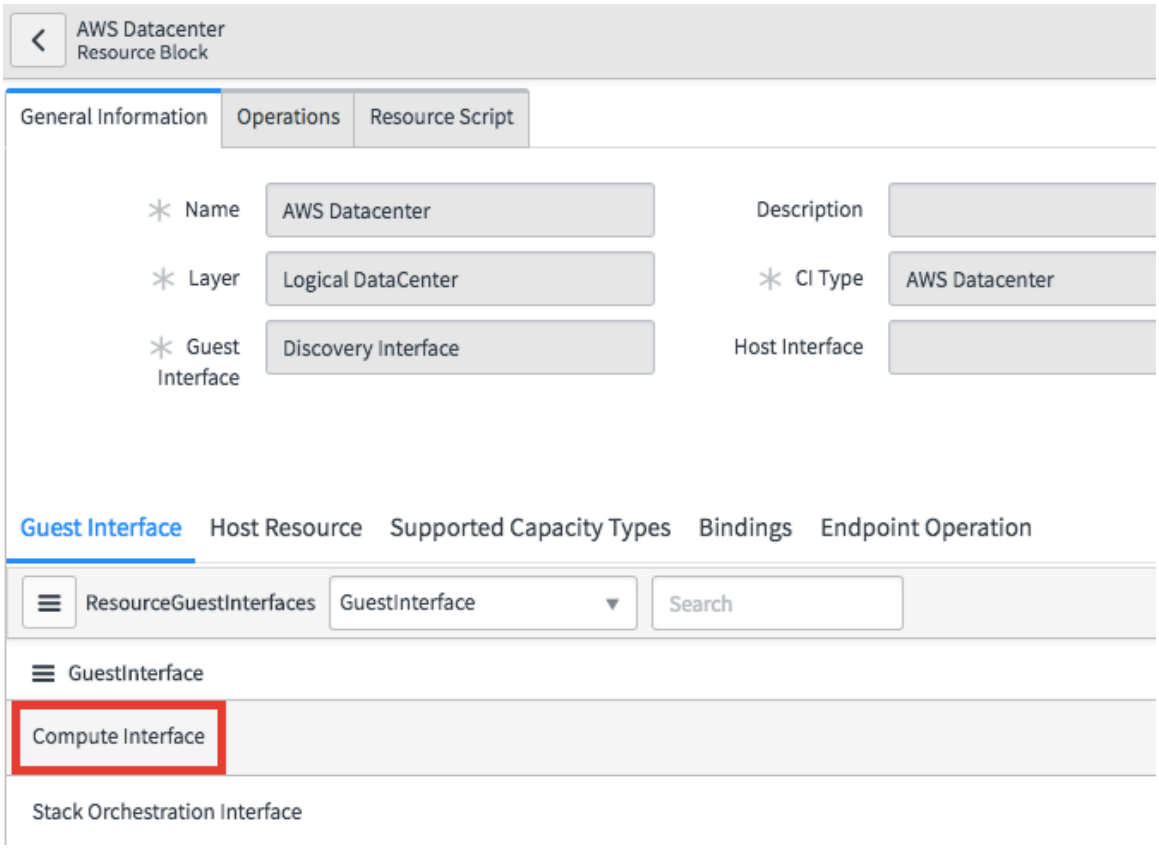
Hinweis: In diesem Fall ruft der Schritt einen Vorgang von einem anderen Ressourcenblock auf: dem AWS-Rechenzentrum. Schritte können CAPI auch direkt aufrufen, und dann kann CAPI REST-Aufrufe an die Cloud-Provider-API ausführen. Das sehen Sie, wenn Sie sich den Ressourcenblock des AWS-Rechenzentrums ansehen.

h. Navigieren Sie zurück zu **Entwurf** > **Ressourcenblöcke**.

i. Öffnen Sie den Ressourcenblock **AWS Datacenter** (AWS-Rechenzentrum), der den Host-Ressourcenblock darstellt, mit dem der virtuelle Server verbunden ist.

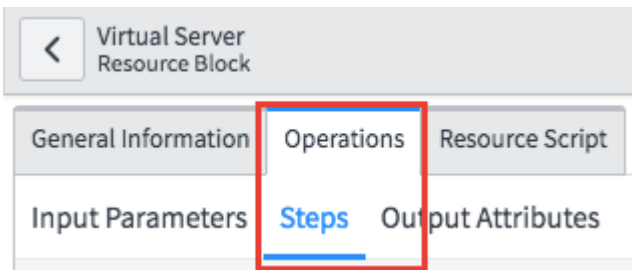
j. Beachten Sie die unterstützten Gastschnittstellen in der zugehörigen Liste **Guest Interface** (Gastschnittstelle):

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

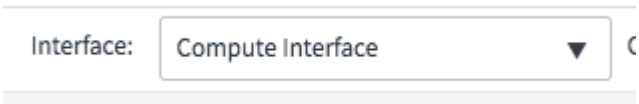


Diese Gastschnittstellen sind die Schnittstellen, die das AWS-Rechenzentrum anderen Ressourcenblöcken zur Verfügung stellt. Die Option **Compute Interface** (Compute-Schnittstelle) wird bereitgestellt, damit der Ressourcenblock des virtuellen Servers, der die Compute-Schnittstelle als Host-Schnittstelle angibt, eine Verbindung zum Rechenzentrum herstellen kann.

k. Klicken Sie auf die Registerkarte **Vorgänge**, und klicken Sie dann auf die untergeordnete Registerkarte **Schritte**.



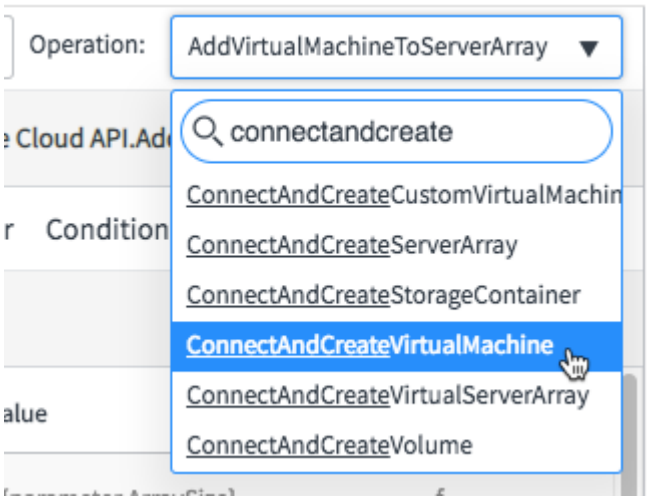
l. Wählen Sie in der Liste **Interface** (Schnittstelle) die Option **Compute Interface** (Compute-Schnittstelle) aus, wenn sie nicht bereits ausgewählt ist.



Denken Sie daran, dass diese Schnittstelle im Ressourcenblock des virtuellen Servers angegeben ist.

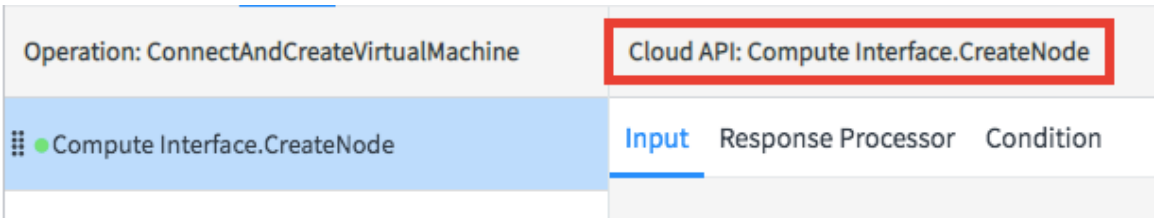
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

m. Suchen Sie in der Liste **Operation** (Vorgang) die Option **ConnectAndCreateVirtualMachine** und wählen Sie sie aus.



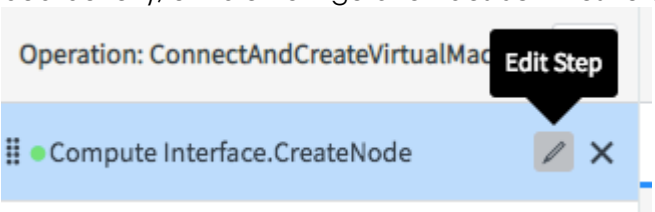
Dabei ist zu berücksichtigen, dass diese Schnittstelle im Ressourcenblock des virtuellen Servers angegeben ist.

n. Zu beachten ist der CAPI-Aufruf, der im einzigen Schritt für den Vorgang „ConnectAndCreateVirtualMachine“ verwendet wird:



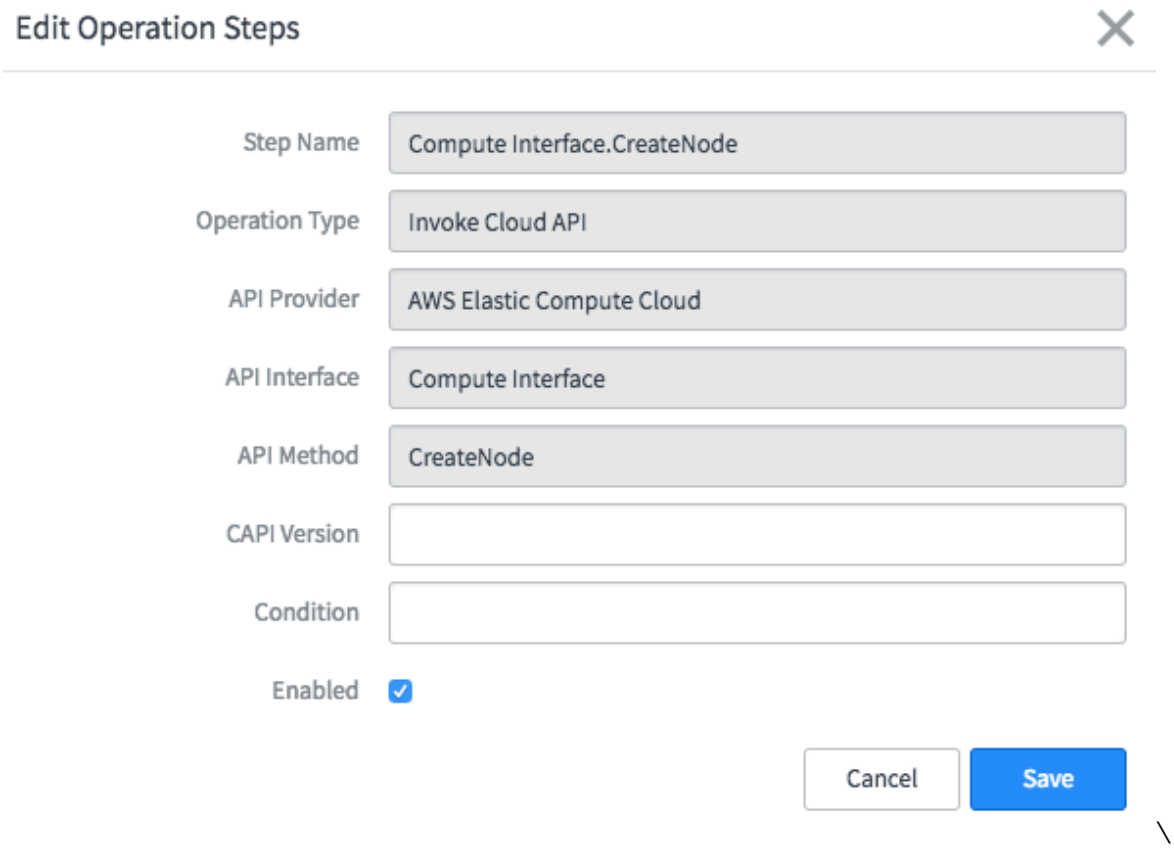
- **Cloud API:** (Cloud-API) Gibt an, dass dieser Schritt CAPI aufruft, sodass CAPI einen REST-Aufruf an den Cloud-Anbieter ausführen kann, der in diesem Fall AWS ist.
- **Compute Interface** (Compute-Schnittstelle) gibt die CAPI-Schnittstelle vor, die von diesem Schritt aufgerufen wird.
- **CreateNode** gibt die Methode an, die ausgeführt wird. Wie der Name schon sagt, weist diese Methode AWS an, den virtuellen Computer zu erstellen.

o. Der Ressourcenblock muss den Status **Draft** (Entwurf) aufweisen. Zeigen Sie dann auf den hervorgehobenen (blauen) Schritt, und klicken Sie auf das Symbol **Edit Step** (Schritt bearbeiten), um die Konfiguration des Schrittes zu öffnen.



p. Sehen Sie sich die Schrittkonfiguration an, und hier insbesondere die Einstellungen, die in CAPI integriert werden:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Feld	Beschreibung
Vorgangstyp	**Invoke Cloud API** (Cloud-API aufrufen) gibt an, dass dieser Schritt die CAPI über den angegebenen Anbieter, die angegebene Schnittstelle und die angegebene Methode aufrufen soll.
API-Anbieter	**AWS Elastic Compute Cloud** ist ein Produkt (nicht der tatsächliche Anbieter), das zum AWS-Anbieter gemäß der Definition in CAPI gehört.
API-Schnittstelle	**Compute Interface** (Compute-Schnittstelle) ist ein Produkt, das zum AWS-Anbieter gemäß der Definition in CAPI gehört.
API-Methode	**CreateNode** ist die Methode, die AWS zum Erstellen der VM aufruft.

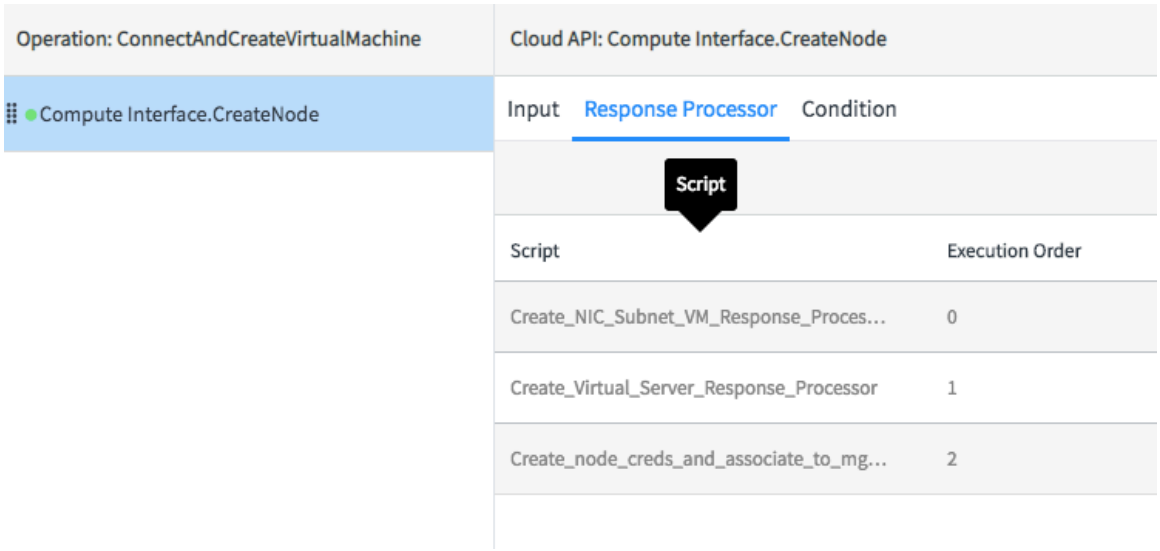
Hinweis: Die CAPI-API-Definition verbindet den Anbieter (Azure), das Produkt (AWS Elastic Compute Cloud), die Schnittstelle (Compute Interface) und die Methode (CreateNode).

q. Schließen Sie das Fenster.

r. Klicken Sie bei ausgewähltem Schritt **Compute Interface.CreateNode** auf **Response Processor** (Antwortprozessor); beachten Sie dabei das Skript **Create_Virtual_Server_Response_Processor**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Dieses Skript ist der Antwortprozessor, der die CMDB in Ihrer Instanz aktualisiert, nachdem der virtuelle Computer in AWS erstellt wurde.

s. Zeigen Sie eine Erklärung des Skripts und das Beispiel an, das Teil des Themas unter Antwortprozessor erstellenist.
Wenn Sie die Überprüfung von diesem Themas abgeschlossen haben, kehren Sie zu diesem Thema zurück.

4. Sehen Sie sich die CAPI-Komponenten an, die zusammenarbeiten, um den virtuellen Computer bereitzustellen:

a. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Cloud-API**.

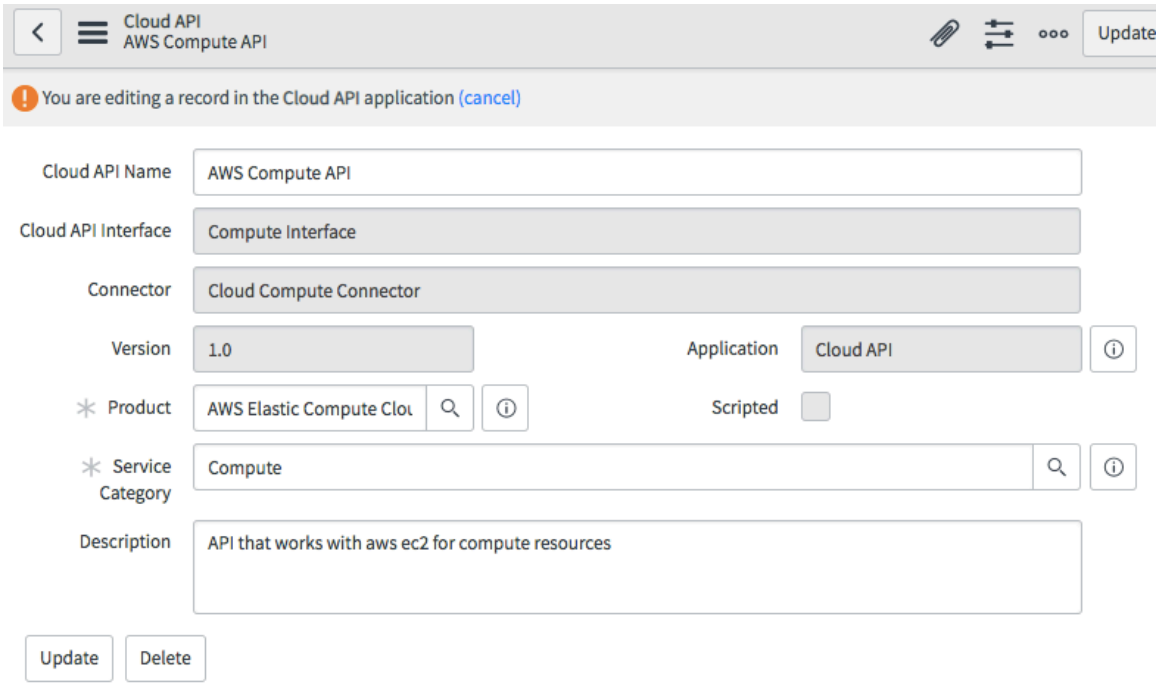
b. Klicken Sie auf die Registerkarte **API**.

c. Suchen Sie nach einer offenen **AWS Compute-API**.

Es gibt zwei AWS Compute-API-Datensätze. Öffnen Sie den ersten in der Liste, der dem Bild im nächsten Schritt entspricht.

d. Sehen Sie sich an, wie diese CAPI-API eine Schnittstelle und ein Produkt miteinander verknüpft:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

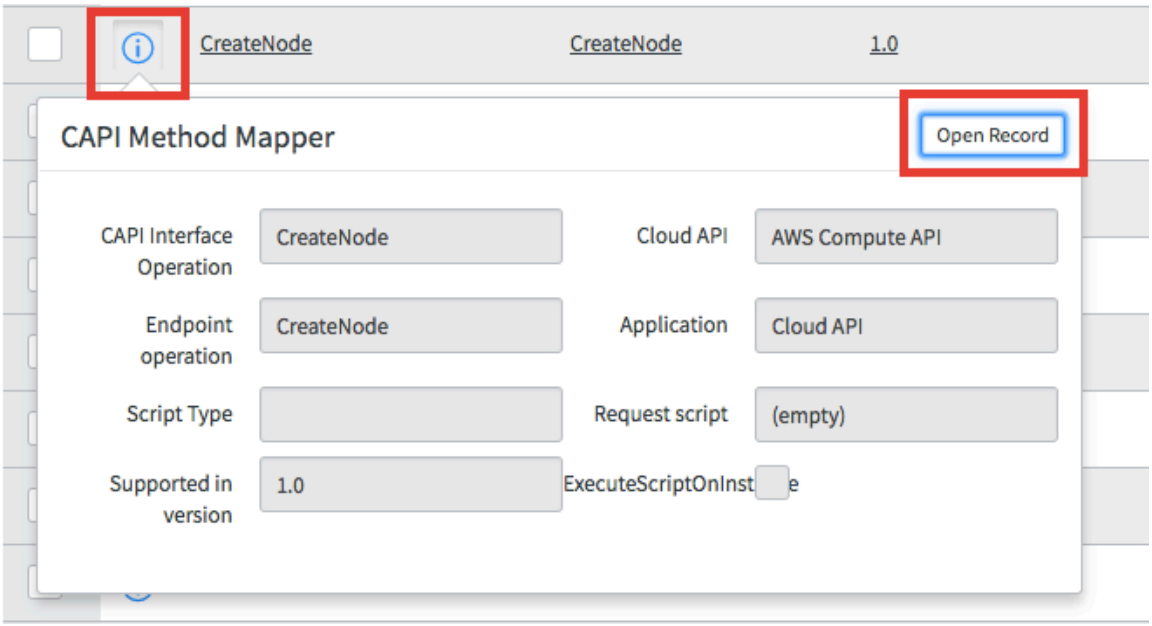


Feld	Beschreibung
Cloud-API-Schnittstelle	**Compute Interface** (Compute-Schnittstelle) ist die gleiche Schnittstelle, die im Ressourcenblock angegeben ist. Die Schnittstelle enthält die Definition für Methoden, einschließlich der Methode *CreateNode*.
Connector	**Cloud Compute Connector** gibt an, dass diese CAPI Java-Aufrufe an das System durchführt, das dann die AWS-API aufruft. Dieser Connector ist nicht geskriptet. Wenn es sich um einen skriptbasierten Connector handeln würde, würde er über eine Skripteinbindung MID-Server verfügen, die die AWS-API aufruft. **Hinweis:** Die meisten AWS-bezogenen APIs, die standardmäßig in der Anwendung Cloud Provisioning and Governance bereitgestellt werden, sind wie diese nicht geskriptet und können nicht geändert werden. Sie können jedoch eigene Skript-APIs erstellen.
Version	**1.0** gibt die Version der API an. Sie können über mehrere Versionen dieser API mit unterschiedlichen Versionsnummern verfügen. Beachten Sie, dass im Schritt im Ressourcenblock für das AWS-Rechenzentrums, den der virtuellen Computer erstellt, ein Versionsfeld bereitgestellt wird. Obwohl dieses Feld im Beispiel leer war, da nur eine Version dieser API vorhanden ist, können Sie eine andere Versionsnummer angeben.
Produkt	**AWS Elastic Compute Cloud** ist das Produkt, das zum AWS-Anbieter in CAPI gehört. Dieses Produkt wird standardmäßig mit Cloud Provisioning and Governance

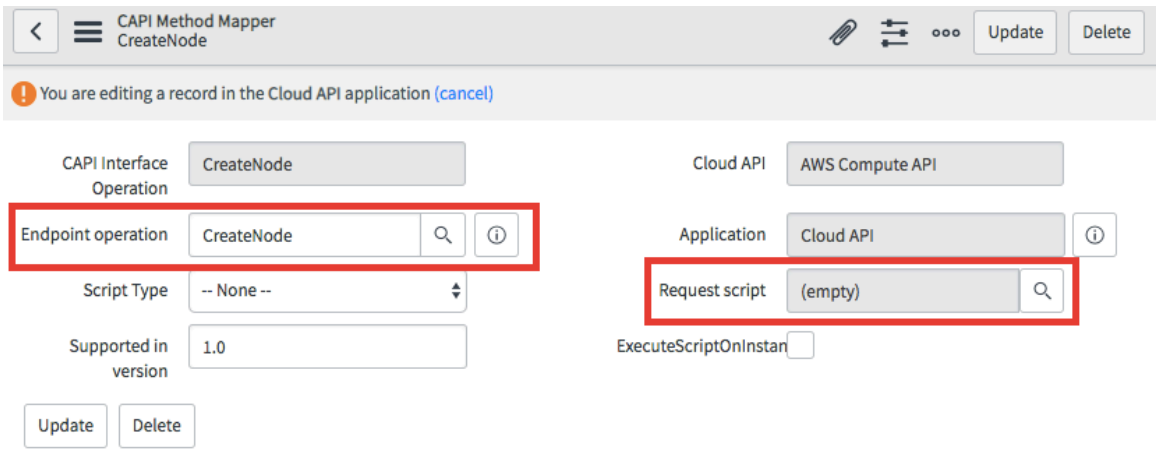
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	geliefert und ist eines der am häufigsten verwendeten Produkte zum Erstellen virtueller Computer in AWS.

e. Klicken Sie in der zugehörigen Liste „CAPI Method Mappers“ (CAPI-Methodenzuordnungen) auf das Symbol für die Datensatzvorschau für den Datensatz *`CreateNode`*, und klicken Sie dann auf **Open Record** (Datensatz öffnen).



f. Sehen Sie sich die Methodenzuordnung für *`CreateNode`* an:



Beachten Sie, dass der Endpunktvorgang nicht **Execute Script**(Skript ausführen) ist. Dieser Wert gibt an, dass die Methode „CreateNode“ einen Java-Aufruf innerhalb der Anwendung Cloud Provisioning and Governance auf Ihrer Instanz verwendet, um einen REST-Aufruf zur AWS-API durchzuführen. Daher können Sie die Funktionsweise der Methode „CreateNode“ nicht ändern. Wenn der Wert **Execute Script** (Skript ausführen) lauten würde, wäre eine MID-Server-Skripteinbindung im Skriptfeld **Request** (Anforderung) angegeben. Sie können diese Skripteinbindung ändern oder eine neue angeben, um die REST-Aufrufe an den AWS-Provider anzupassen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

g. Scrollen Sie nach unten, und sehen Sie sich Parameter in der zugehörigen Liste der CAPI-Parameterzuordnungen an.
Beachten Sie, dass wichtige Parameter wie **Location** (Standort) angegeben sind.

h. Navigieren Sie zurück zum API-Formular von AWS Compute.

i. Klicken Sie auf die zugehörige Liste **API Config Overrides** (API-Konfigurationsüberschreibungen), und überprüfen Sie die für die Authentifizierung erforderlichen Elemente.

Konfigurationsparameter und Überschreibungswert	Beschreibung
AccountAliasName $(CloudCredential.Alias)	Der Alias für das Konto ist ein optionaler Wert, den Sie in Ihrem AWS-Konto erstellen können. Es handelt sich um einen sekundären Namen für Ihre Konto-ID. In der Dokumentation zu AWS finden Sie weitere Informationen.
Berechtigungen $(CloudCredential.secret_key)	Der geheime Schlüssel wird mit dem Zugriffsschlüssel für die Authentifizierung verwendet. Sie haben diesen Wert während der Einrichtung in Ihrem AWS-Anmeldeinformationsdatensatz konfiguriert. Informationen zu diesem Verfahren finden Sie unter Zugriff auf AWS-Konten mit permanenten AWS-Anmeldeinformationen konfigurieren.
Endpunkt $(CloudCredential.URL)	Der Endpunkt ist die URL, bei der sich die Benutzer anmelden und authentifizieren müssen. Dazu werden Konto-ID oder Konto-Alias verwendet. In der Dokumentation zu AWS finden Sie weitere Informationen.
Identität $(CloudCredential.access_key)	Der Datensatz „Identify“ (Identifizieren) enthält den AWS-Zugriffsschlüssel, den AWS für die Authentifizierung benötigt.

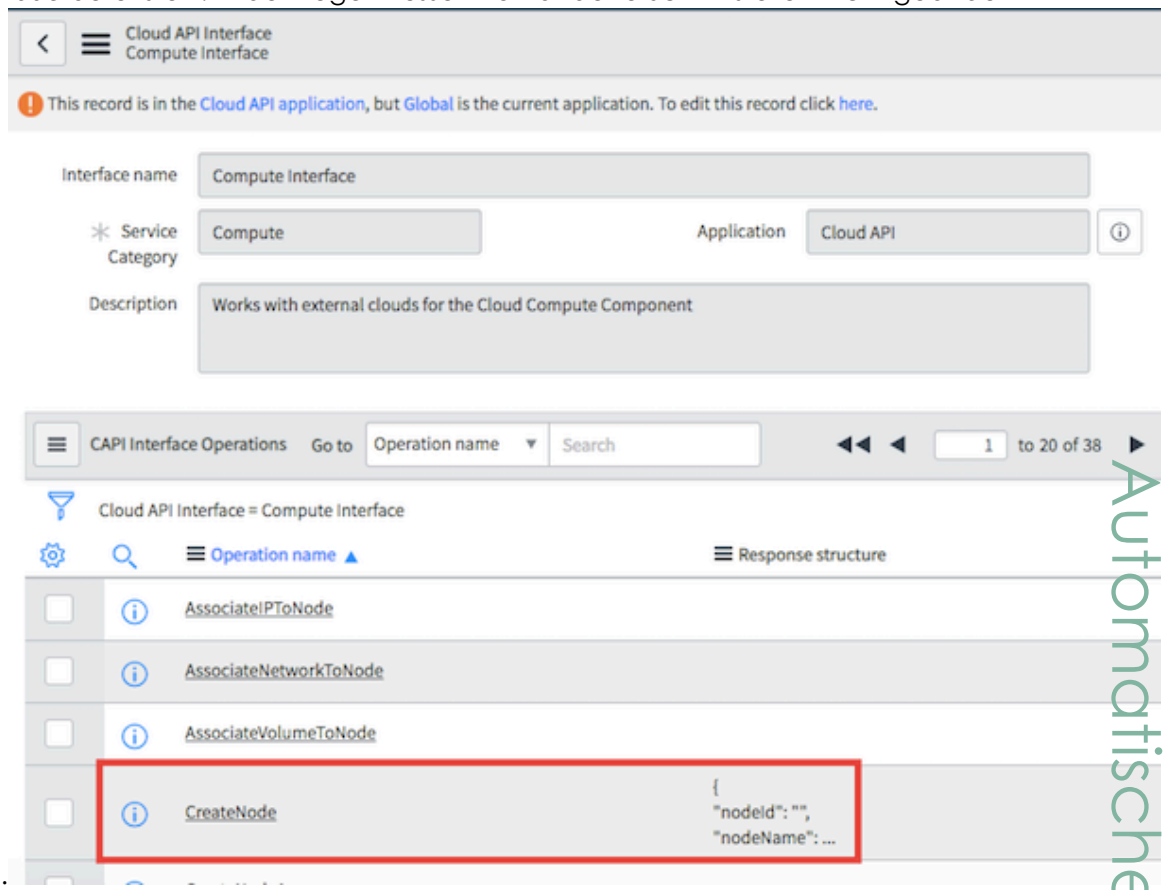
j. Navigieren Sie zurück zu **Entwurf** > **Cloud-API**, und klicken Sie dann auf die Registerkarte **Schnittstelle**.

k. Suchen Sie nach **Compute Interface** (Compute-Schnittstelle) und öffnen Sie diese.
Diese Schnittstelle ist die im Ressourcenblock und der CAPI-API unter **AWS Compute-API** angegebene Schnittstelle.

l. Überprüfen Sie den Inhalt der Schnittstelle.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Beachten Sie, dass die Schnittstelle REST-Antwortstrukturen für Methoden wie *CreateNode* bereitstellt. In der Regel müssen vorhandene Schnittstellen nicht geändert werden.



Beachten Sie die Servicekategorie und die Vorgänge:

Feld oder zugehörige Liste	Beschreibung
Servicekategorie	Die Servicekategorie klassifiziert die Schnittstelle. Die Kategorie für die Compute-Schnittstelle ist ebenfalls **Compute**.
CAPI-Schnittstellenvorgänge	Die Schnittstellenvorgänge definieren die JSON-Struktur für den REST-Aufruf und die Parameter, die für die Schnittstelle erforderlich sind.

m. Klicken Sie auf den CAPI-Schnittstellenvorgang **CreateNode**.
Über diesen Vorgang wird das Framework für die Erstellung des virtuellen EC2-Servers in AWS bereitgestellt.

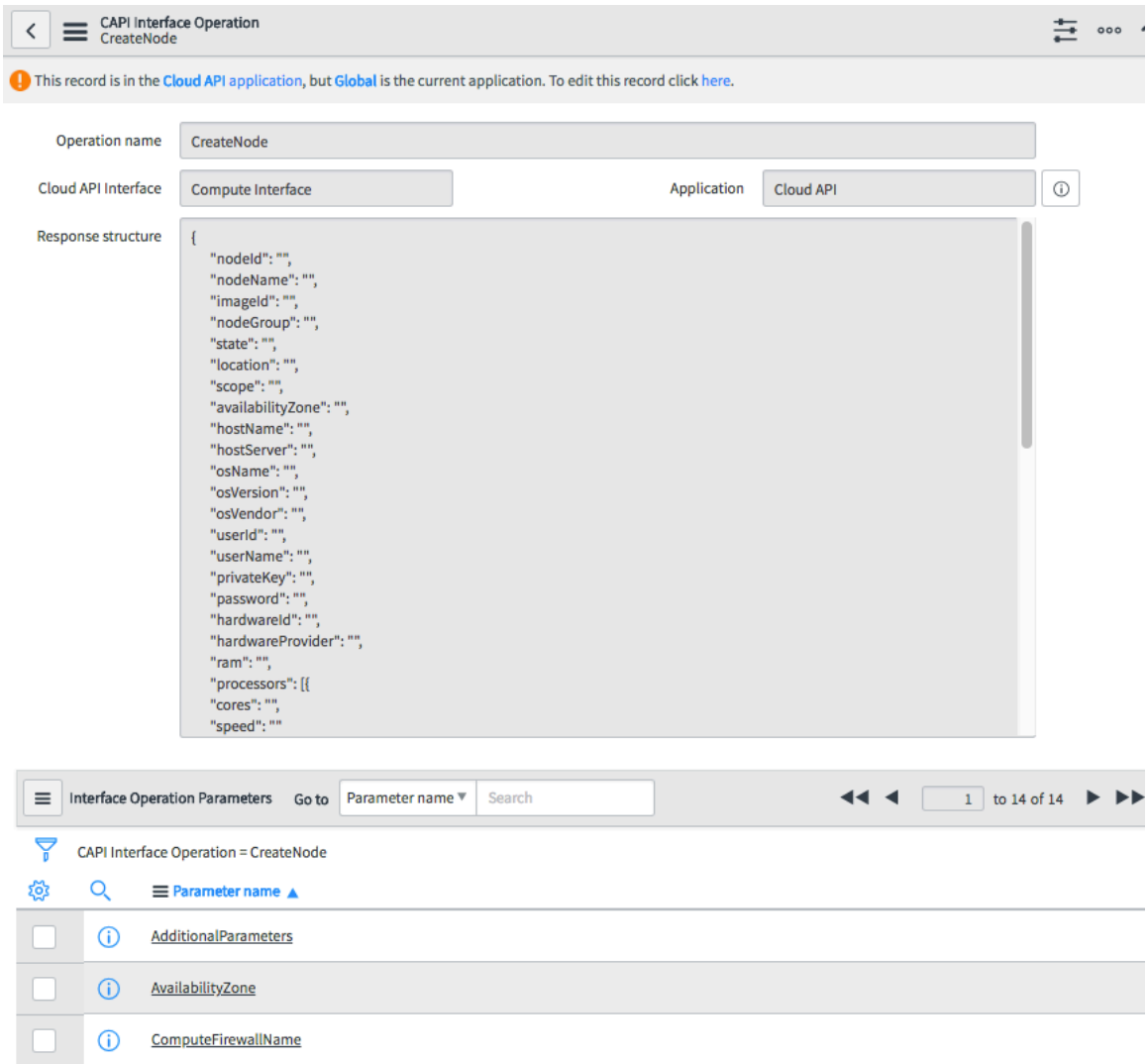
n. Überprüfen Sie die Komponenten des Vorgangs:

Feld oder zugehörige Liste	Beschreibung
Antwortstruktur	Die Antwortstruktur ist das JSON-Framework für den REST API-Aufruf. Diese Struktur bietet eine Liste von Attributen, die

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld oder zugehörige Liste	Beschreibung
	AWS zum Erstellen der virtuellen Ressource mit leeren Werten verwenden kann.
Parameter für Schnittstellenvorgänge	Diese Parameter sind auch die Parameter, die die CAPI-Schnittstelle vom System benötigt, damit sie die Struktur im REST-Aufruf an den Cloud-Anbieter übergeben kann.



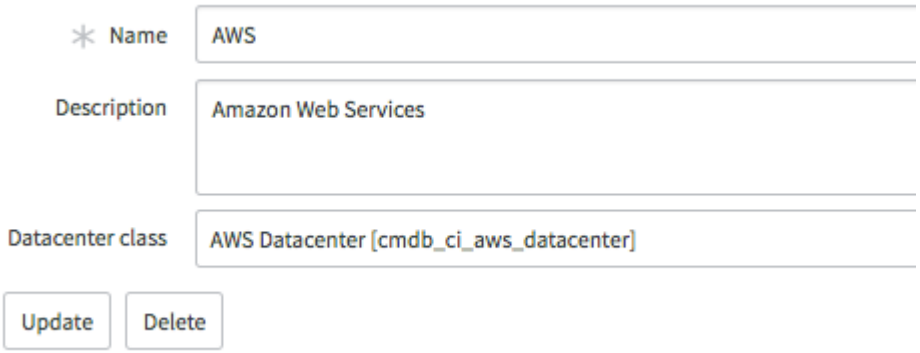
o. Navigieren Sie zurück zu **Entwurf** > **Cloud-API**, und klicken Sie dann auf die Registerkarte **Provider**.

p. Öffnen Sie den Anbieter **AWS**.

Das Formular „AWS Provider“ (AWS-Anbieter) wird geöffnet und zeigt an, dass dieser Anbieter auf einer vorhandenen CMDB-Klasse basiert: **AWS Datacenter [cmdb_ci_aws_datacenter]**.

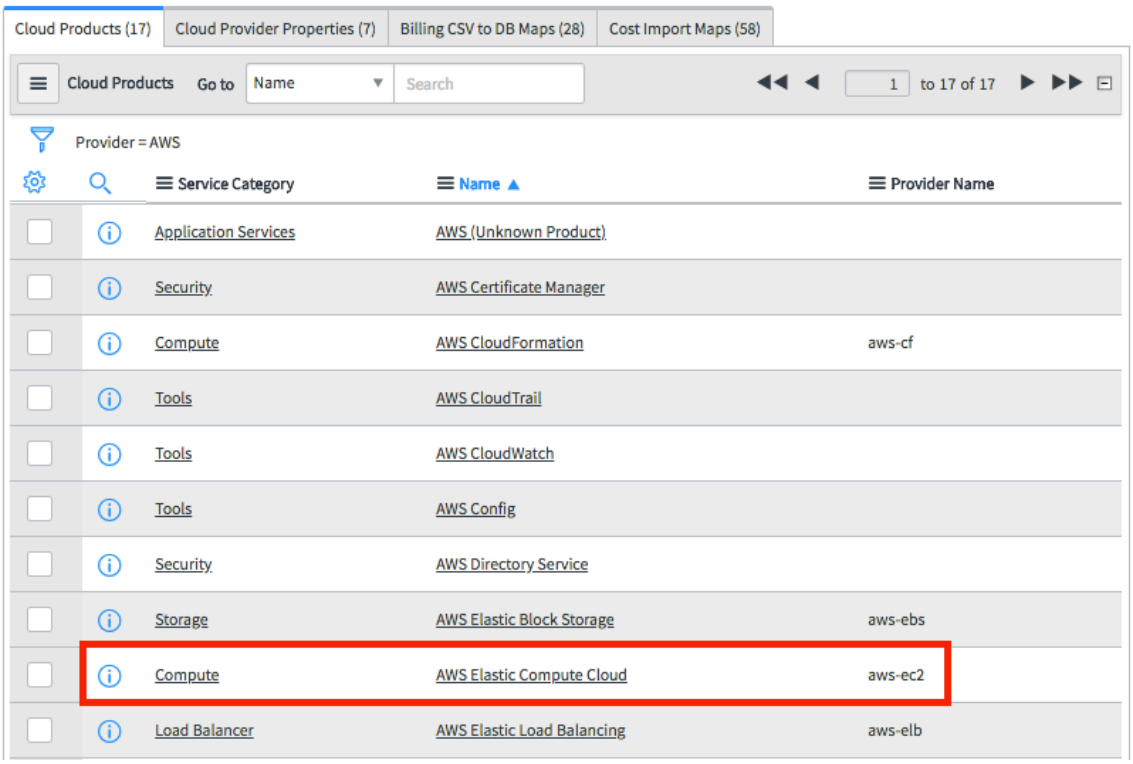
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



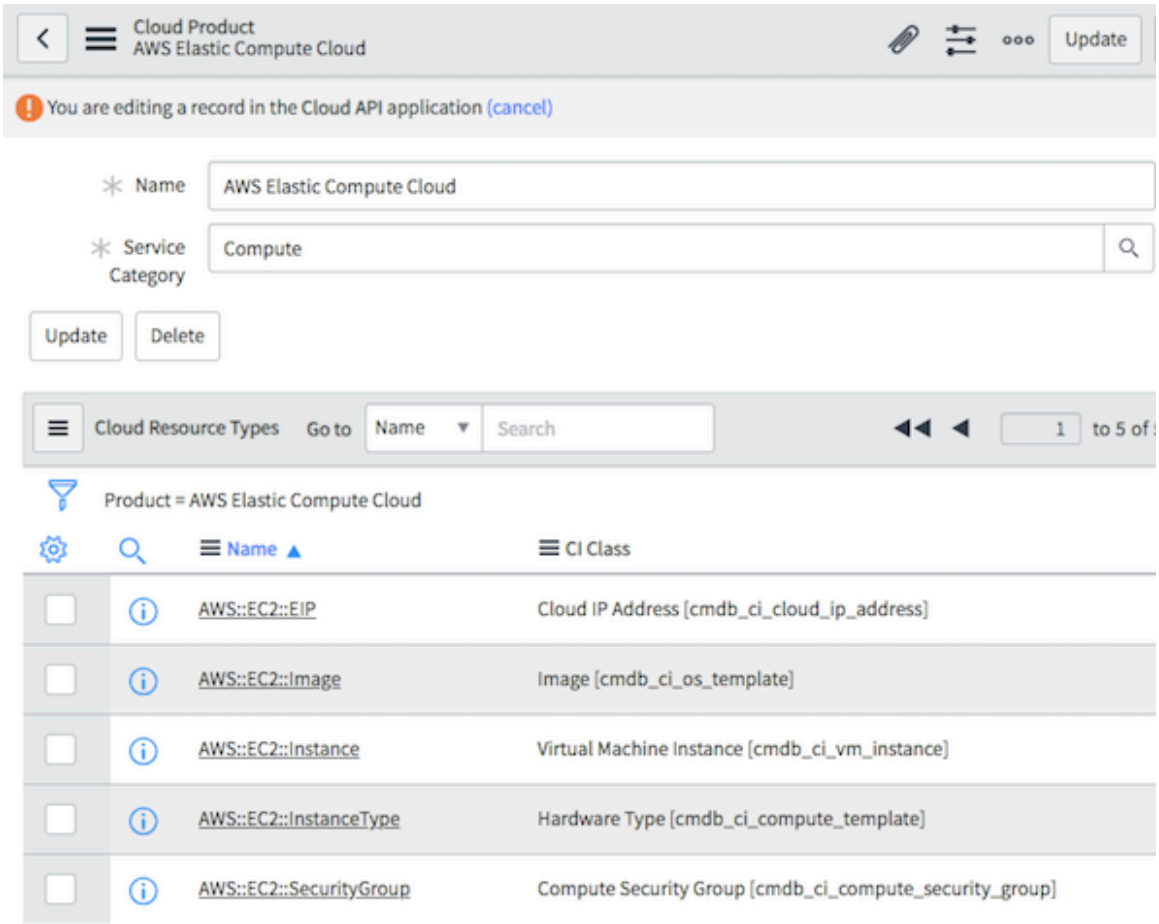
q. Klicken Sie auf die zugehörige Liste „Cloud Products“ (Cloud-Produkte), falls sie noch nicht ausgewählt ist, und sortieren Sie die Liste nach der Spalte **Name**.

Beachten Sie, dass standardmäßig bereits mehrere AWS-Produkte verfügbar sind. Eines der am häufigsten verwendeten AWS-Produkte ist **Elastic Compute Cloud (EC2)**.



r. Klicken Sie in der Spalte **Name** auf **AWS Elastic Compute Cloud**.
Beachten Sie, dass das Produkt viele Ressourcentypen angibt, die jeweils einer CI-Klasse zugeordnet sind.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

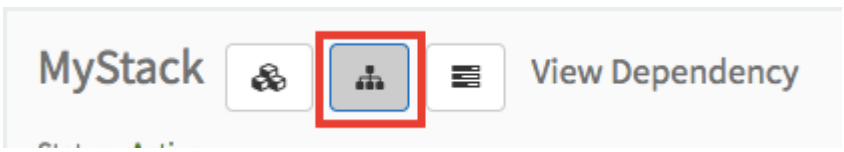


Diese Ressourcentypen geben einige, aber nicht alle CIs an, die sich auf den virtuellen Computer beziehen. Der Antwortprozessor im Ressourcenblock füllt CIs mit Daten aus, wenn AWS den virtuellen Computer bereitstellt.

5. So zeigen Sie die wichtigen mit der VM verbundenen CIs an:

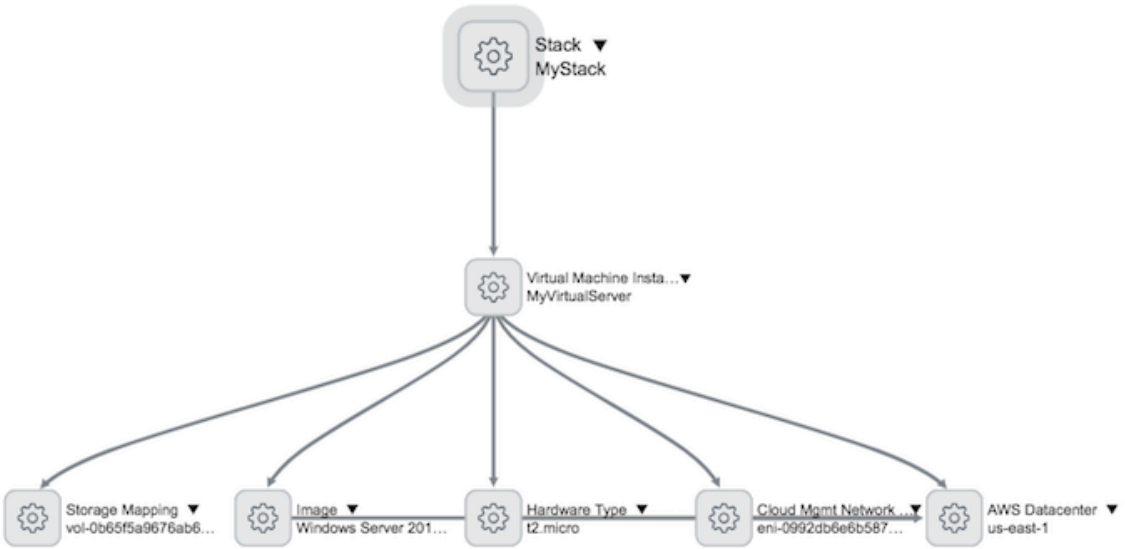
a. Klicken Sie in Cloudbenutzerportal auf **Stapel**, und öffnen Sie dann den Stapel, der die VM enthält.

b. Klicken Sie auf das Symbol View Dependency (Abhängigkeit anzeigen).



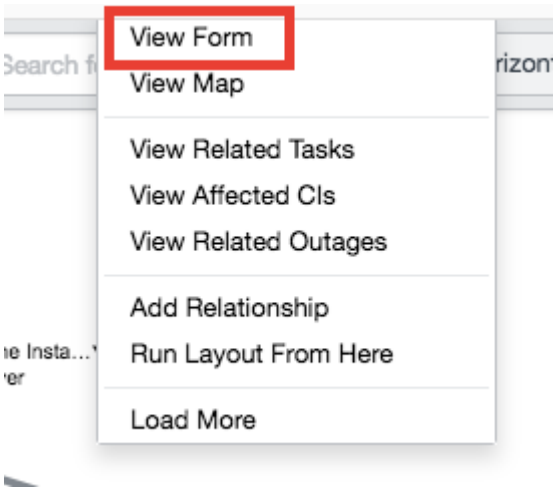
Die Abhängigkeitszuordnung zeigt das Stapel-CI oben, den virtuellen Computer in der Mitte und die verschiedenen zugehörigen CIs unten, z. B. das Bild.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



c. Sie rufen das Formular für den virtuellen Computer in der CMDB auf, indem Sie mit der rechten Maustaste auf den Pfeil neben einem CI, beispielsweise dem virtuellen Computer, klicken.

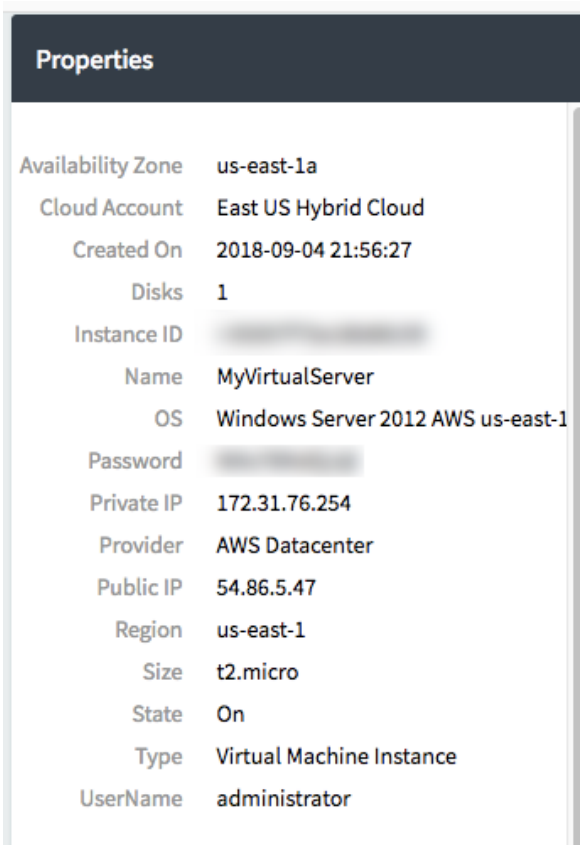
d. Wählen Sie im Menü **View Form** (Formular anzeigen).



© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Das CI-Formular wird geöffnet und zeigt an, dass viele der Informationen bereits auf Cloudbenutzerportal verfügbar sind, wenn Sie die Eigenschaften des virtuellen Computers anzeigen lassen.

Eigenschaften des virtuellen Computers in Cloudbenutzerportal



Einem vorhandenen Provider in CAPI ein Produkt hinzufügen

Die Cloud API (CAPI) Cloud Provisioning and Governance bietet viele Provider wie AWS und Azure und Produkte wie EC2-Instanzen. Sie können jedoch bestehenden Anbietern Produkte für neue Typen von Cloud-Ressourcen hinzufügen.

Vorbereitungen

- Erforderliche Rolle: Administrator
- Überprüfen Sie Standard-CAPI-APIs, und stellen Sie sicher, dass Anbieter und Produkte, die Sie erstellen möchten, nicht bereits angegeben sind.
- Machen Sie sich mit der Cloud-Anbieter-API vertraut, damit Sie wissen, wie REST-Aufrufe an den Anbieter erstellt werden. Wenn Sie mit Headern, Authentifizierungsanforderungen, Endpunkt und Daten, die Sie an die Provider-API übergeben können, nicht vertraut sind, können Sie keine eigenen CAPI-Komponenten erstellen.

Warum und wann dieser Vorgang ausgeführt wird

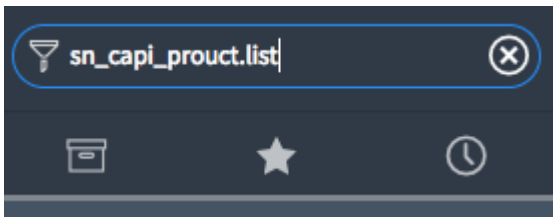
Dieses Thema enthält allgemeine Anweisungen für die Erweiterung eines vorhandenen Cloudanbietes, Produkts und Ressourcentyps.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Geben Sie in Ihrer Instanz (nicht Portal für Cloud-Admin.), den folgenden Text in den Applikationsfilter ein:

   `sn_capi_product.list`

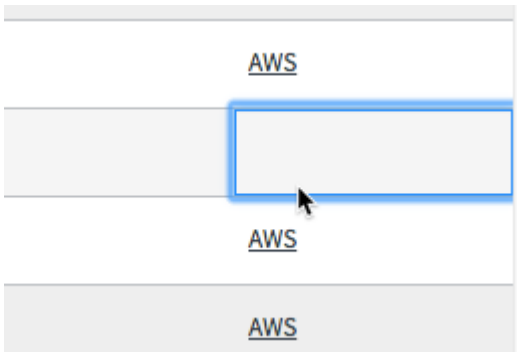
2. Drücken Sie die `EINGABETASTE`.

   Die Liste der Produkte, die zu allen Anbietern gehören, wird angezeigt. Sie können die Liste filtern, um sicherzustellen, dass das Produkt, das Sie erstellen möchten, nicht bereits bereitgestellt ist.

3. Klicken Sie auf **New** (Neu), geben Sie einen Namen ein und wählen Sie diejenige der vorhandenen Servicekategorien, die am besten geeignet ist.
4. Klicken Sie auf **Absenden**.

   Die Liste der Produkte wird erneut angezeigt.

5. Suchen Sie das von Ihnen erstellte Produkt, und doppelklicken Sie dann auf die leere Zelle in der Spalte **Provider** (Anbieter).

6. Fügen Sie den richtigen Anbieter hinzu.
7. Fügen Sie einen eindeutigen Anbieternamen hinzu: Doppelklicken Sie auf die Zelle im Feld **Provider Name** (Anbietername), und ändern Sie den Namen.

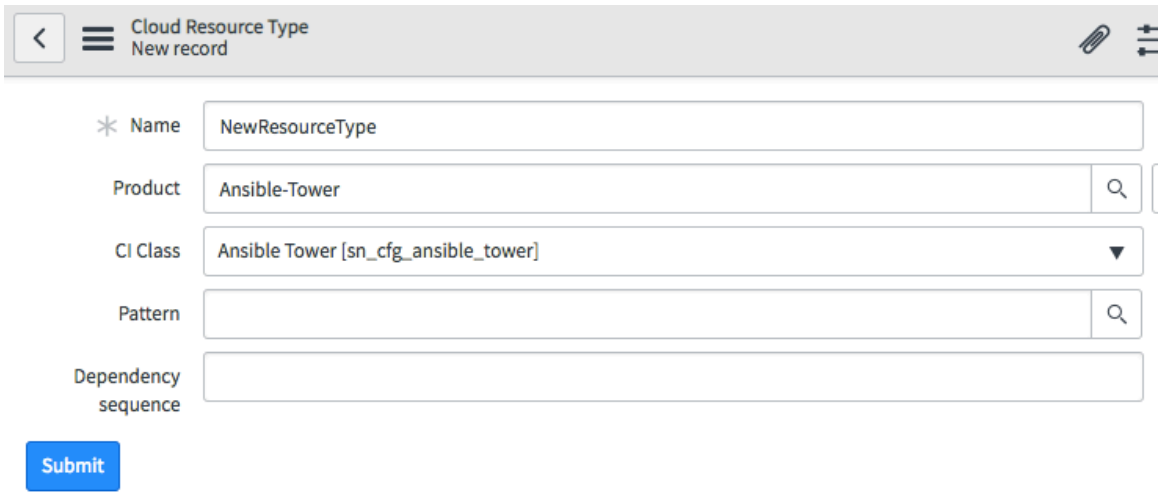
   Das System kann einen Anbieternamen automatisch für Sie generieren, Sie sollten ihn jedoch ändern, um Konflikte mit vorhandenen Anbieternamen zu vermeiden.

8. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Cloud-API**.
9. Klicken Sie auf die Kachel für den Anbieter, dem Sie das neue Produkt hinzugefügt haben.
10. Vergewissern Sie sich, dass sich Ihr Produkt in der zugehörigen Liste **Cloud Products** (Cloud-Produkte) befindet.
11. Klicken Sie auf das Informationssymbol (ⓘ) für das Cloud-Produkt, und klicken Sie dann auf **Open Record** (Datensatz öffnen).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

12. Klicken Sie in der zugehörigen Liste „Cloud Resource Types“ (Cloud-Ressourcentypen) auf **New** (Neu), und füllen Sie das Formular aus.

Feld	Beschreibung
Name	Ein eindeutiger und aussagekräftiger Name.
Produkt	Das Cloud-Produkt, für das Sie den Ressourcentyp erstellen. Wählen Sie aus der Nachschlageliste aus, oder erstellen Sie etwas neu.
CI-Klasse	Eine CMDB-Tabelle, die Sie dem Ressourcentyp zuordnen müssen. Wenn die richtige CMDB-Tabelle nicht angezeigt wird, finden Sie unter Eine CI-Klasse für eine virtuelle Cloud-Ressource erstellen Anweisungen dazu, wie Sie eine solche Tabelle erstellen können.
Muster	Das Muster, das zum Erkennen des Ressourcentyps verwendet wird. Wählen Sie in der Suchliste für Discovery-Muster aus, oder erstellen Sie ein neues Muster.
Abhängigkeitssequenz	Die Reihenfolge, in der der Ressourcentyp bereitgestellt oder erkannt wird. Geben Sie die Reihenfolge basierend auf gegenseitigen Abhängigkeiten von Ressourcen an. Beispiel: Wenn Sie über ein Netzwerk und ein Subnetz verfügen, die erkannt oder erstellt werden sollen, geben Sie einen höheren Rang für das Netzwerk als das Subnetz an, damit die Erkennung oder Erstellung von Ressourcen logisch und sequenziell erfolgt.



13. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Eine CI-Klasse für eine virtuelle Cloud-Ressource erstellen soweit nötig, oder Eine CAPI-Schnittstelle erstellen oder erweitern

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine CI-Klasse für eine virtuelle Cloud-Ressource erstellen

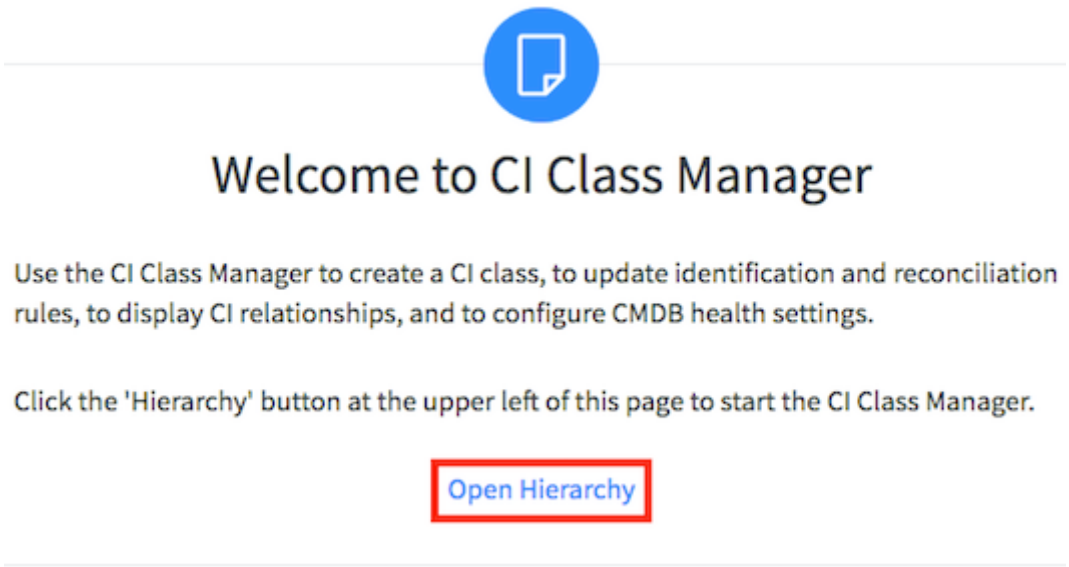
Wenn Basissystem keinen CI-Typ für cloudbasierte virtuelle Ressourcen bereitstellt, können Sie eine CI-Klasse basierend auf der Objektklasse des virtuellen Computers erstellen.

Vorbereitungen
Erforderliche Rolle: Administrator

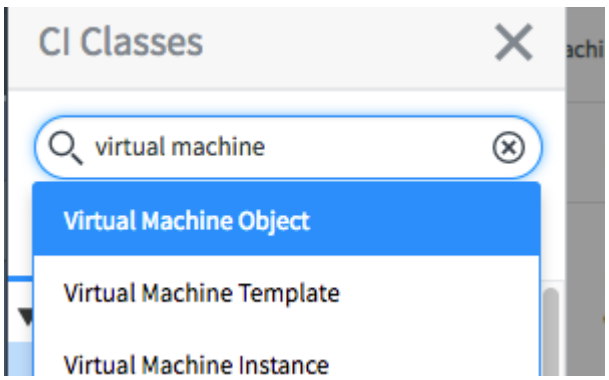
Warum und wann dieser Vorgang ausgeführt wird
Dieses Thema enthält allgemeine Anweisungen für die Erweiterung eines vorhandenen Cloudanbietes, Produkts und Ressourcentyps.

Prozedur

1. Navigieren zu **Alle** > **Konfiguration** > **CI-Klassen Manager**.
2. Klicken Sie auf **Open Hierarchy** (Hierarchie öffnen).



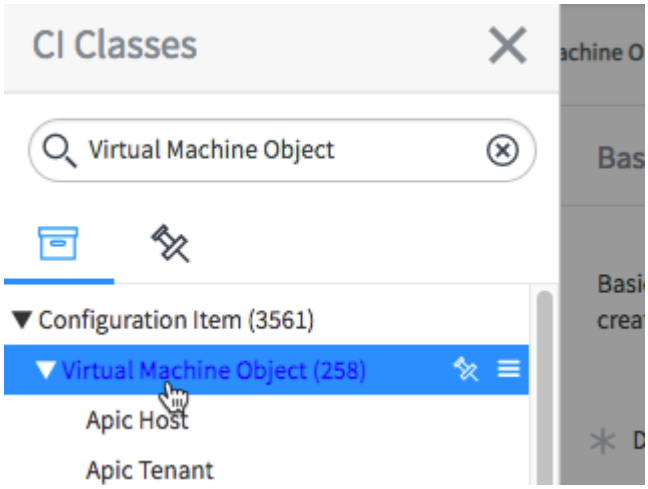
3. Geben Sie im Bereich **CI Classes** (CI-Klassen) im Suchfeld `Virtual Machine Object` (Objekt d. virtuellen Computers) ein, und wählen Sie dann **Virtual Machine Object**.



4. Klicken Sie auf den Link **Virtual Machine Object** (Objekt d. virtuellen Computers).

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



5. Klicken Sie auf **Nachfolgeklasse hinzufügen**.
6. Geben Sie im nun eingeblendeten Schritt **Provide Basic Info** (Grundlegende Informationen angeben) einen Namen und eine Beschreibung ein.

   Wenn Sie den Fokus des Cursors aus dem Feld **Display Name** (Anzeigename) entfernen, wird das Feld **Table Name** (Tabellenname) automatisch mit dem gleichen Namen in Kleinbuchstaben ausgefüllt. Bei einer Tabelle in einer bereichsbezogenen Anwendung wird dem Namen ein Namespace-Bezeichner vorangestellt, um anzuzeigen, dass er Teil einer Anwendung ist. Für eine Tabelle in der globalen Anwendung wird dem Namen die Zeichenfolge **u_cmdb_ci** vorangestellt. Sie können das Präfix nicht ändern. Sie können jedoch den Rest des Tabellennamens ändern. Der Name darf nur Kleinbuchstaben, alphanumerische ASCII-Zeichen und Unterstriche (_) enthalten. Die maximale Länge der Zeichenfolge beträgt 80 Zeichen.
7. Klicken Sie auf **Next** (Weiter).
8. Klicken Sie im Schritt **Add Attributes** (Attribute hinzufügen) auf **Derived** (Abgeleitet), und überprüfen Sie dann die Attribute, die von der VM-Objektklasse übernommen wurden.

   Die meisten benötigten Attribute werden bereitgestellt.
9. Wahlweise: So fügen Sie ein Attribut hinzu:

   a. Doppelklicken Sie im Feld **Collumn Label** (Spaltenbezeichnung) auf das Feld **Insert a new row** (Neue Zeile einfügen).

   b. Geben Sie einen Namen für die Spalte ein, und klicken Sie auf den grünen Pfeil.

   c. Füllen Sie die restlichen Felder der Zeile aus.
   Eine Beschreibung aller Felder finden Sie unter Formular „Wörterbucheintrag“. .
10. Klicken Sie auf **Next (Weiter)**.
11. Erstellen Sie im Schritt **Set Identification Rule** (Identifizierungsregel festlegen) eine Identifizierungsregel, die eine eindeutige Objekt-ID angibt, die für die Identifizierung erforderlich ist.

> **Wichtig:** Cloud Provisioning and Governance erfordert, dass die Objekt-ID eine Instanz des CI-Klassentyps eindeutig identifiziert.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Klicken Sie in der Standardregel unter **Identification Rule** (Identifizierungsregel) auf **Replace** (Ersetzen).

b. Geben Sie einen Namen für die Regel ein, und wählen Sie die Option **Dependent** (Abhängig).

c. Klicken Sie auf **Speichern**.

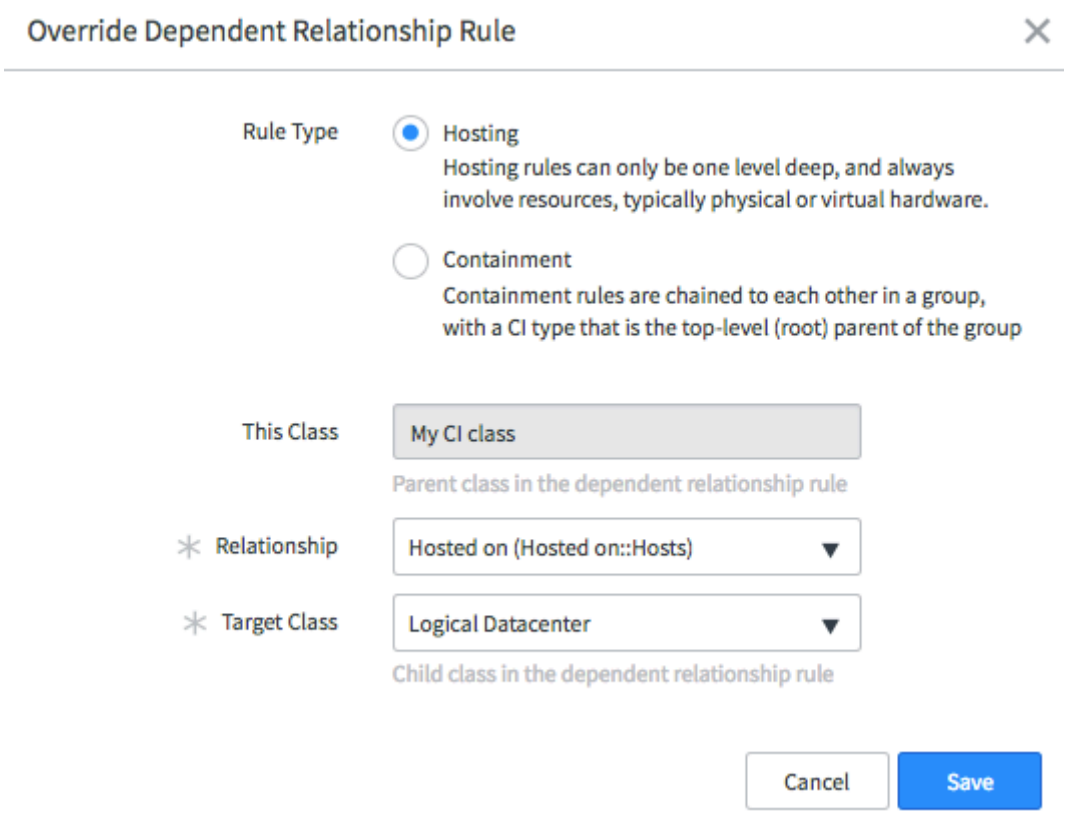
d. Klicken Sie unter **Bezeichner-Einträge** auf **Hinzufügen**.

e. Verschieben Sie die **Objekt-ID** aus der Spalte **Available** (Verfügbar) in die Spalte **Selected** (Ausgewählt).

f. Klicken Sie auf **Speichern**.

12. Klicken Sie auf **Next** (Weiter).
13. Klicken Sie im Schritt **Add Dependent Relationships** (Abhängige Beziehungen hinzufügen) auf **Override Dependencies** (Abhängigkeiten überschreiben).
14. Konfigurieren Sie die Beziehung zwischen dieser virtuellen Ressource und dem logischen Rechenzentrum, in dem sie sich befindet:

Feld	Wert
Regeltyp	**Hosting**
Beziehung	**Gehostet auf (Hosted on:Hosts)**
Zielklasse	**Logisches Rechenzentrum**



15. Klicken Sie auf **Speichern**.
16. Klicken Sie auf **Next** (Weiter).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

17. Klicken Sie erneut auf **Next** (Weiter), um den Schritt **Add Reconciliation Rules** (Abgleichregeln hinzufügen) zu überspringen, und klicken Sie dann auf **Done** (Fertig), um den Schritt **Add Suggested Relationships** (Vorgeschlagene Beziehungen hinzufügen) zu überspringen.

Nächste Maßnahme

Verwenden Sie die CI-Klasse in einem Ressourcentyp für einen Cloud-Anbieter. Anweisungen dazu finden Sie unter Einem vorhandenen Provider in CAPI ein Produkt hinzufügen.

Ihr Antwortprozessor, der Teil des Ressourcenblocks ist, muss auch die erforderlichen CI-Klassentypen angeben, damit er die CMDB aktualisieren kann. Normalerweise benötigt der Antwortprozessor die Objekt-ID, das spezifische Rechenzentrum und das Cloud-Servicekonto. Unter Beispiel für einen Antwortprozessor für einen virtuellen Server finden Sie Beispiele für Antwortprozessorcode, der CI-Klassen verwendet.

Eine CAPI-Schnittstelle erstellen oder erweitern

Sie können eine neue CAPI-Schnittstelle erstellen oder eine vorhandene erweitern, indem Sie neue Vorgänge hinzufügen.

Vorbereitungen

- Erforderliche Rolle: admin
- Überprüfen Sie Standard-CAPI-APIs und stellen Sie sicher, dass weder Anbieter noch Produkte, die Sie erstellen möchten, bereits vorliegen.
- Machen Sie sich mit der Cloud-Anbieter-API vertraut, damit Sie wissen, wie REST-Aufrufe an den Anbieter erstellt werden. Wenn Sie mit Headern, Authentifizierungsanforderungen, Endpunkt und Daten, die Sie an die Provider-API übergeben können, nicht vertraut sind, können Sie keine eigenen CAPI-Komponenten erstellen.

Warum und wann dieser Vorgang ausgeführt wird

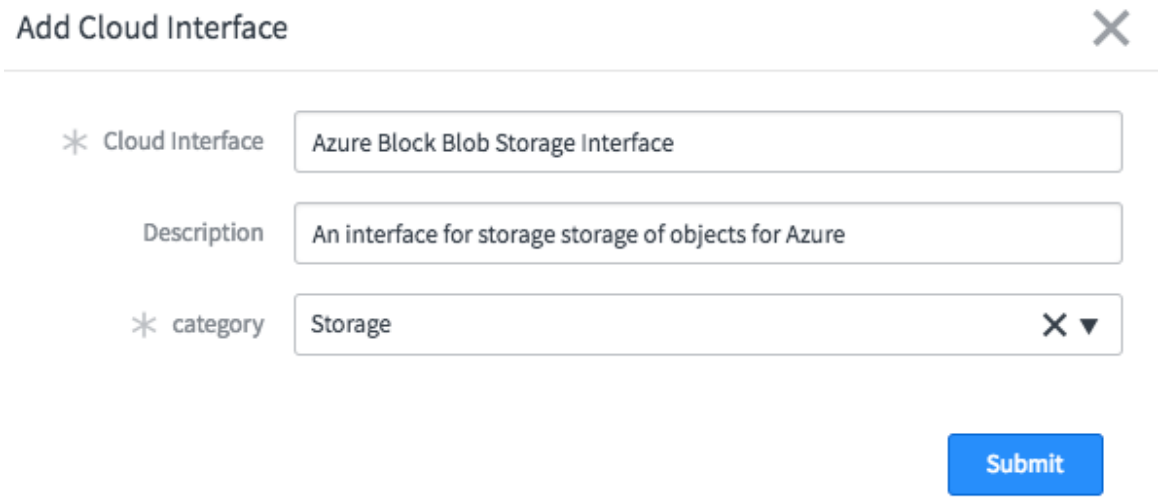
Normalerweise können Sie die Standardschnittstellen verwenden, die in der Anwendung Cloud Provisioning and Governance bereitgestellt werden. Für das Erstellen einer benutzerdefinierten Schnittstelle sollte eine ähnliche, bereits bestehende als Basis verwendet werden.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Cloud-API**, und klicken Sie dann auf die Registerkarte **Schnittstelle**.
2. Klicken Sie auf **Neu**.
3. Geben Sie im Fenster „Add Cloud interface“ (Cloudschnittstelle hinzufügen) einen Namen für die Schnittstelle und eine hilfreiche Beschreibung ein, und wählen Sie die relevanteste Kategorie aus, der die API-Schnittstelle angehören soll.

   Dieses Beispiel zeigt eine Schnittstelle für Azure-Speicher:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

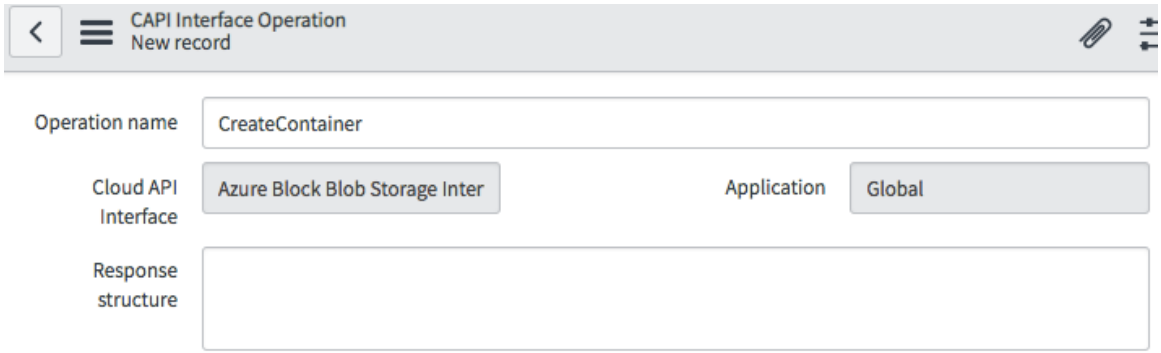


4. Klicken Sie in der zugehörigen Liste für CAPI-Schnittstellenvorgänge auf **New** (Neu).

   Jeder Vorgang, den Sie erstellen, entspricht einem anderen REST API-Aufruf.

5. Geben Sie einen Namen für den Vorgang an, der der API entspricht, die Sie im Anbieter aufrufen möchten.

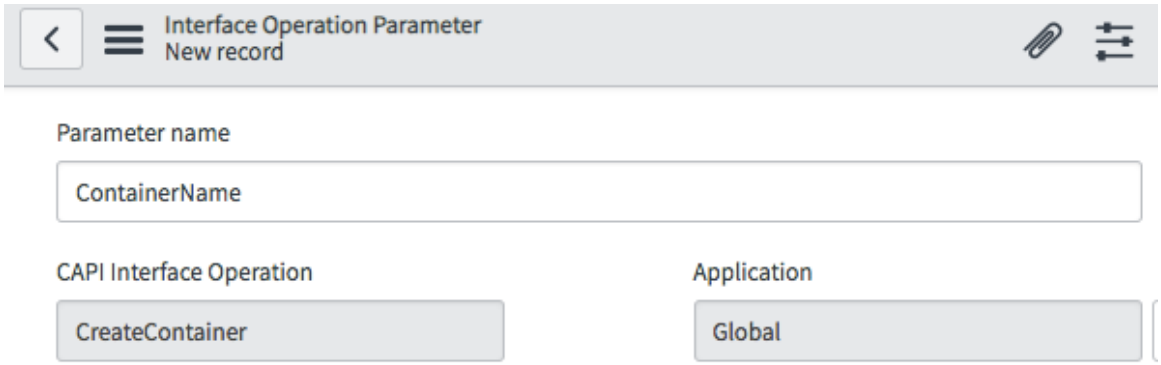
   Beispielsweise können Sie einen Vorgang namens *CreateContainer* erstellen, der dem Vorgang „Create Container“ (Container erstellen) in Azure entspricht.



6. Klicken Sie mit der rechten Maustaste auf die Kopfzeile und wählen Sie **Speichern**.
7. Klicken Sie in der zugehörigen Liste „Schnittstellen-Vorgangsparameter“ auf **Neu**.
8. Erstellen Sie einen Parameter, den der Vorgang gemäß der Definition der REST API-Dokumentation des Cloud-Anbieters benötigt.

   Wenn Sie die Parameter nicht kennen, schlägt der Vorgang fehl. Im Beispiel mit Azure-Speicher muss der Vorgang *CreateContainer* den Namen des Containers haben, der hier als *ContainerName* bezeichnet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



9. Klicken Sie auf **Absenden**.
10. Fügen Sie so viele Parameter hinzu, wie Sie für den Vorgang benötigen, und fügen Sie dann alle erforderlichen Vorgänge hinzu.

Nächste Maßnahme
Eine CAPI-API erstellen

Eine CAPI-API erstellen

Wenn die vorhandenen CAPI-APIs nicht in die CAPI-Schnittstelle für einen Anbieter integriert werden, können Sie eine API erstellen. Die Schritte in Ressourcenblöcken können die von Ihnen verwendeten API-Methoden aufrufen, wenn Vorgänge ausgeführt werden.

Vorbereitungen

- Erforderliche Rolle: admin
- Überprüfen Sie Standard-CAPI-APIs und stellen Sie sicher, dass weder Anbieter noch Produkte, die Sie erstellen, bereits vorliegen.
- Machen Sie sich mit der Cloud-Anbieter-API vertraut, damit Sie wissen, wie REST-Aufrufe an den Anbieter erstellt werden. Wenn Sie mit Headern, Authentifizierungsanforderungen, Endpunkt und Daten, die Sie an die Provider-API übergeben können, nicht vertraut sind, können Sie keine eigenen CAPI-Komponenten erstellen.

Warum und wann dieser Vorgang ausgeführt wird

Dieses Thema enthält Anweisungen zum Erstellen einer CAPI-API. Außerdem werden die Konfiguration von CAPI, Ressourcenblöcke, Blueprints und die Zuordnung von Anmeldeinformationen behandelt.

Prozedur

1. Navigieren Sie in Portal für Cloud-Admin.zu **Entwurf** > **Cloud-API**.
2. Klicken Sie auf die Registerkarte **API**.
3. Klicken Sie auf **Neu**.
4. Füllen Sie die Formularfelder aus (siehe Tabelle):

Feld	Beschreibung
Cloud-API	Geben Sie einen beschreibenden Namen an.
Schnittstelle	Wählen Sie eine der vorhandenen Schnittstellen aus, die die gewünschten Vorgänge bereitstellen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Connector	Der **Script Connector** (Skript-Connector) wird in diesem Feld angezeigt, wenn der Connector ein sofort verfügbarer Java-Connector ist, der nicht geändert werden kann. Sie müssen diese Skript-Connectors nicht ändern.
Produkt	Wählen Sie das Produkt aus, das Teil des Anbieters ist. Das Produkt enthält Ressourcentypen in der CMDB.
Version	Geben Sie eine Versionsnummer an, um diese API zu identifizieren. Geben Sie `1.0` ein, wenn diese API die erste Version ist. Sie können mehrere Versionen derselben API erstellen und dann in den Vorgangsschritten der Ressourcenblöcke auf die jeweiligen Versionen verweisen.
Geskriptet	Dieses Feld wird ausgewählt, wenn der Wert von **Interface** (Schnittstelle) **Script Connector** (Script-Connector) lautet.
Skripttyp	Wählen Sie die Sprache für das Skript aus. **Hinweis:** Es empfiehlt sich JavaScript. Die Methodenzuordnungen verwenden in Javascript geschriebene MID-Server-Skripteinbindungen.
ExecuteScriptOnInstance	
Beschreibung	Hier sollte sich die API-Beschreibung befinden.

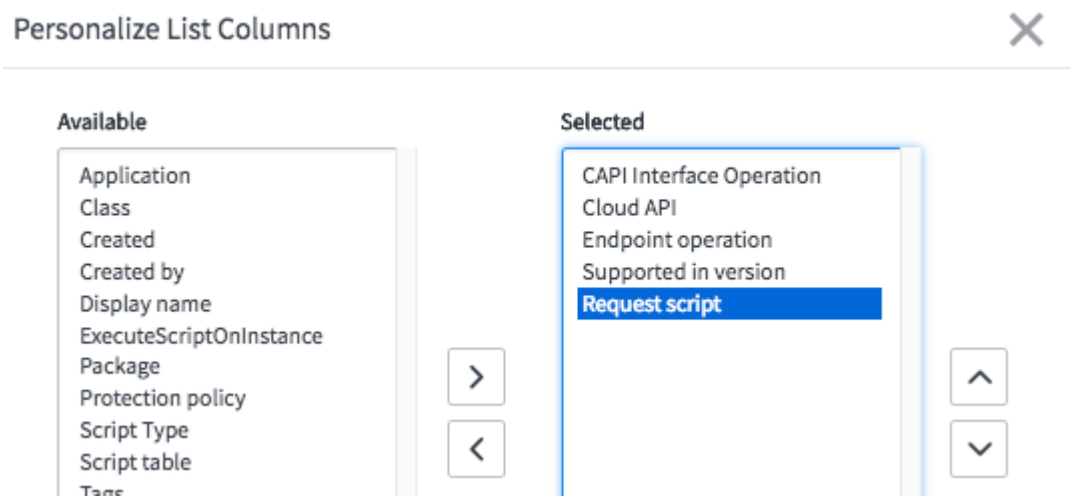
5. Stellen Sie sicher, dass alle erforderlichen Vorgänge in der zugehörigen Liste der **CAPI-Methodenzuordnungen** angezeigt werden.

   Die Vorgänge in der Liste CAPI-Methodenzuordnungen sind in der von Ihnen ausgewählten Schnittstelle die gleichen Vorgänge. Sie sind an diese API gebunden. Für diese Liste sind weder Hinzufügen noch Entfernen von Vorgängen möglich. Einige der Vorgänge, insbesondere Azure-Vorgänge, verwenden MID-Server-Skripteinbindungen, die die tatsächliche Implementierung für die API ausführen. Das Skript enthält einen Aufruf der REST API für den Anbieter, z. B. AWS oder Azure. Sie sollten die API in der Dokumentation des Anbieters finden.

6. So rufen Sie die Skripteinbindung für eine CAPI-Methodenzuordnung auf:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

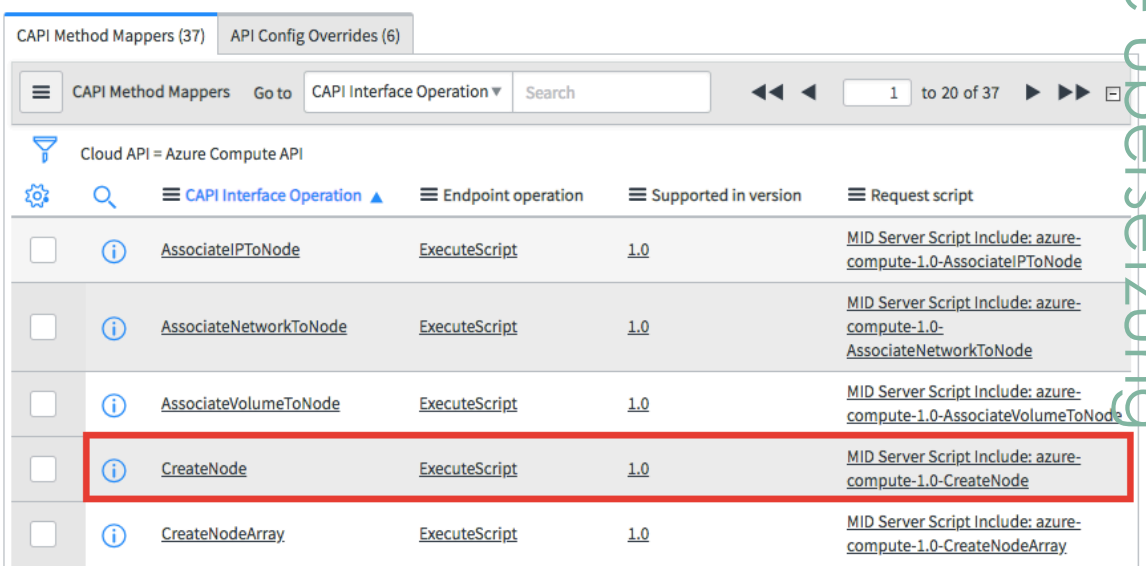
a. Klicken Sie auf das Zahnradsymbol ( ) auf der zugehörigen Liste **CAPI Method Mappers** (CAPI-Methodenzuordnungen), fügen Sie das Feld **Request Script** (Skript anfordern) der **ausgewählten** Spalte hinzu, und klicken Sie dann auf **OK**.



Die Skripteinbindungen von MID-Server werden jetzt in der Liste der Methodenzuordnungen angezeigt.

b. Klicken Sie auf den Namen eines Skripts, um die Skripteinbindung aufzurufen.

In diesem Beispiel verwendet der Vorgang **CreateNode** die Skripteinbindung *azure-compute-1.0-CreateNode*.



Diese Skripteinbindung enthält folgenden Code:

```
createNode();
function createNode(){
   var acp = new AzureComputeVirtualMachine(this.parameters,
 this.headers);
    //this passes the parameters and headers into the
 AzureComputeVirtualMachine script include.
   var vm = acp.createVirtualMachine();
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
    return vm;
}
```

Sie werden bemerken, dass der Code Skripteinbindung *AzureComputeVirtualMachine* aufruft, die standardmäßig mit der Anwendung Cloud Provisioning and Governance verfügbar ist. Sie enthält alle API-Aufrufe bei Azure mit virtuellen Computern.

7. Erstellen Sie eine Überschreibung der API-Konfiguration, um die erforderlichen Anmeldeinformationen an den Cloud-Anbieter zu übergeben.

   Sie müssen auch Header-Informationen übergeben, die für die REST API des Cloud-Anbieters erforderlich sind. API-Konfigurationsüberschreibungen sind erforderlich, da Anmeldeinformationsdaten nicht enthalten sind, wenn die Instanz den REST-Aufruf bei der Cloud-Anbieter-API durchführt.

   Tipp: Wenn Sie nicht wissen, welche API-Konfigurationsüberschreibungen erstellt werden sollen, suchen Sie nach einer ähnlichen API in CAPI, und verwenden Sie dieselben Überschreibungen. Wenn Sie beispielsweise eine API für AWS-Speicher erstellen, suchen Sie nach anderen AWS-APIs wie AWS Block Storage oder AWS Compute.

   a. Klicken Sie in der den API-Konfigurationsüberschreibungen zugehörigen Liste auf **New** (Neu).

   b. Klicken Sie auf das Suchsymbol, und wählen Sie einen vorhandenen Konfigurationsparameter aus.
   Viele nützliche Parameter werden standardmäßig bereitgestellt, z. B. **Identity** (Identität), **Credentials** (Anmeldeinformationen) usw.

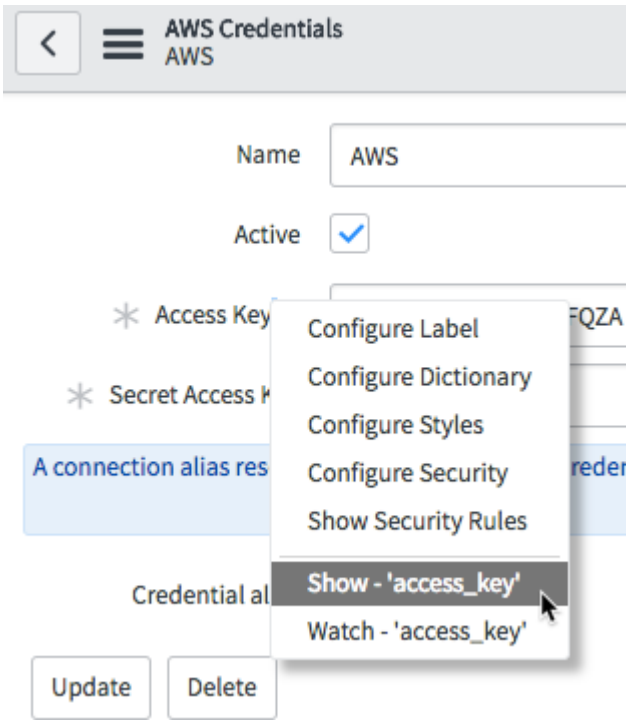
   c. Geben Sie einen **Überschreibungswert** ein.

      Sie können einen statischen Wert festlegen oder einen Wert im Format `$(CloudCredential.attribute_name)` aus dem System verwenden. Die Komponente `CloudCredential` entsperrt den Wert aus dem Anmeldeinformationsspeicher.
      Die Komponente `attribute_name` ist ein Attribut, das von den konkreten Anmeldeinformationen, Alias- oder Endpunkt-URLs abhängt, die Sie abrufen möchten.

      Wenn Sie zu navigieren **Verbindung und Anmeldeinformationen** > **Anmeldeinformationen** und öffnen Sie Ihre AWS-Anmeldeinformationen. Sie können mit der rechten Maustaste auf das Feld **Zugriffsschlüssel-ID** klicken und den Namen der Spalte in der Tabelle „Anmeldeinformationen“ anzeigen, in der der Zugriffsschlüssel gespeichert ist. In diesem

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Fall wird der Zugangsschlüssel in der Spalte `access_key` gespeichert. Daher muss der Überschreibungswert `$(CloudCredential.access_key)` sein.



8. Wenn Sie einen Konfigurationsparameter für die API-Konfigurationsüberschreibung erstellen müssen, gehen Sie wie folgt vor:

   a. Klicken Sie im Formular „API Config Override“ (API-Konfigurationsüberschreibung) auf das Suchsymbol im Feld **Config Parameter** (Konfigurationsparameter).

   b. Klicken Sie im Fenster „Config Parameter“ (Konfigurationsparameter) auf **New** (Neu) und füllen Sie das Formular aus.

Feld	Beschreibung
Konfigurationsparametername	Geben Sie einen beschreibenden Namen ein.
Standardwert	Sie können einen optionalen Standardwert festlegen.
Endpunkt	Dieses Feld ist schreibgeschützt.
Beschreibung	Geben Sie eine erläuternde Beschreibung ein.
Konfigurationsdatentypen	Wählen Sie den Datentyp aus: ▪ **Zeichenfolge** ▪ **DateTime** ▪ **Datum** ▪ **Lang** ▪ **Passwort** ▪ **Boolean**
Konfigurationstyp	Wählen Sie den Konfigurationstyp aus:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	▪ Header: Verwenden Sie diesen Wert, um die Überschreibungswerte als Header zu übergeben. Wenn Sie über eine MID-Server-Skripteinbindung als Teil der API verfügen, und diese `this.headers` als Parameter verwendet, werden die Überschreibungswerte der Anbieter-API übergeben. ▪ Config ▪ URI-Konfiguration

9. Ändern Sie bei Bedarf die Skripteinbindungen, die die Vorgänge für die Cloud-Anbieter-API ausführen:

a. Klicken Sie auf dem Cloud-API-Formular in der zugehörigen Liste der CAPI-Methodenzuordnungen auf das Informationssymbol ( ) neben dem CAPI-Schnittstellenvorgang.
Klicken Sie nicht auf den Namen des CAPI-Schnittstellenvorgangs.

b. Klicken Sie auf **Datensatz öffnen**.

c. Im Vorgangsformular können Sie die folgenden Feldwerte ändern:

Feld	Beschreibung
Endpunktvorgang	Behalten Sie den standardmäßigen Endpunktvorgang **Execute Script** (Skript ausführen) bei.
Unterstützt in Version	Üblicherweise muss dieser Wert nicht geändert werden. Ändern Sie die Version von **Supported in** (Unterstützt in), um die Methodenzuordnung in einer anderen Version der API zu verwenden. Standardmäßig ist für die Methodenzuordnungen dieselbe Versionsnummer festgelegt wie für die zugehörige API.

d. Klicken Sie im Feld **Request Script** (Skript anfordern) auf das Informationssymbol ( ) neben der Platzhalter-Skripteinbindung MID-Server, um Änderungen vorzunehmen.

e. Erstellen Sie mit dem Formular für Skripteinbindungen das gewünschte Skript.

Das folgende Beispiel-JavaScript listet Azure-Lastenausgleichsmodule auf. Beachten Sie die hilfreichen Kommentare:

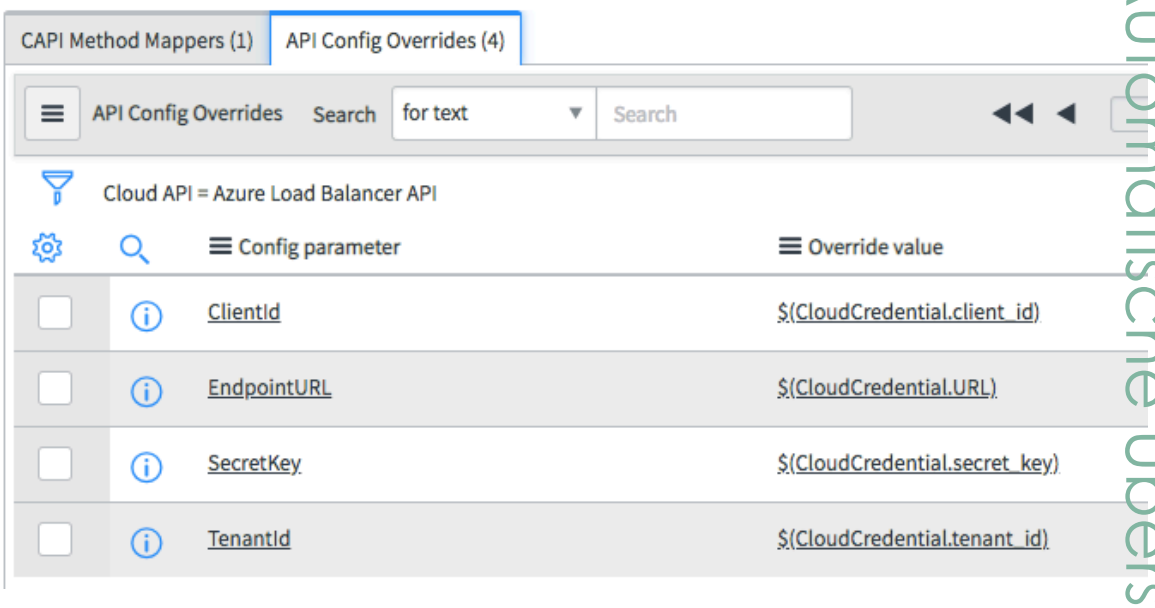
```
getResourceInfo();

function getResourceInfo() {
 var anpi = new AzureLoadBalancer(this.parameters, this.headers);

       //this calls the 'AzureLoadBalancer' MID-Server script include,
 which in turn
```

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
      //calls the 'AzureCloudAPIBase' script include, both of which
      //are already in your instance by default.
      //The 'AzureCloudBase' script include runs a query for
resources of a given type in a
//specified region.

var items = anpi.listResourcesByRegionOrIDs();
      //This function is in the 'AzureCloudAPIBase' script include.
It calls the Azure API.

return items;
}
```

Die für diesen Vorgang bereitgestellten Überschreibungen sind das, was Azure benötigt, um die Lastenausgleichsmodule zu finden: Client-ID, Mandanten-ID, geheimer Schlüssel und Endpunkt-URL:



Für das Integrationsbeispiel von Google Cloud ist auch eine MID-Server-JAR-Datei erforderlich.

f. Klicken Sie auf **Absenden**.

g. Ändern Sie die Skripteinbindung für jeden Vorgang.

Cloud-Benutzerportal

Das Cloud-Benutzerportal bietet Ihnen direkten Zugriff auf alle täglichen Cloud-Aktivitäten.

Cloud-Benutzerportal

Verwenden Sie das Cloud-Benutzerportal für folgende Vorgänge:

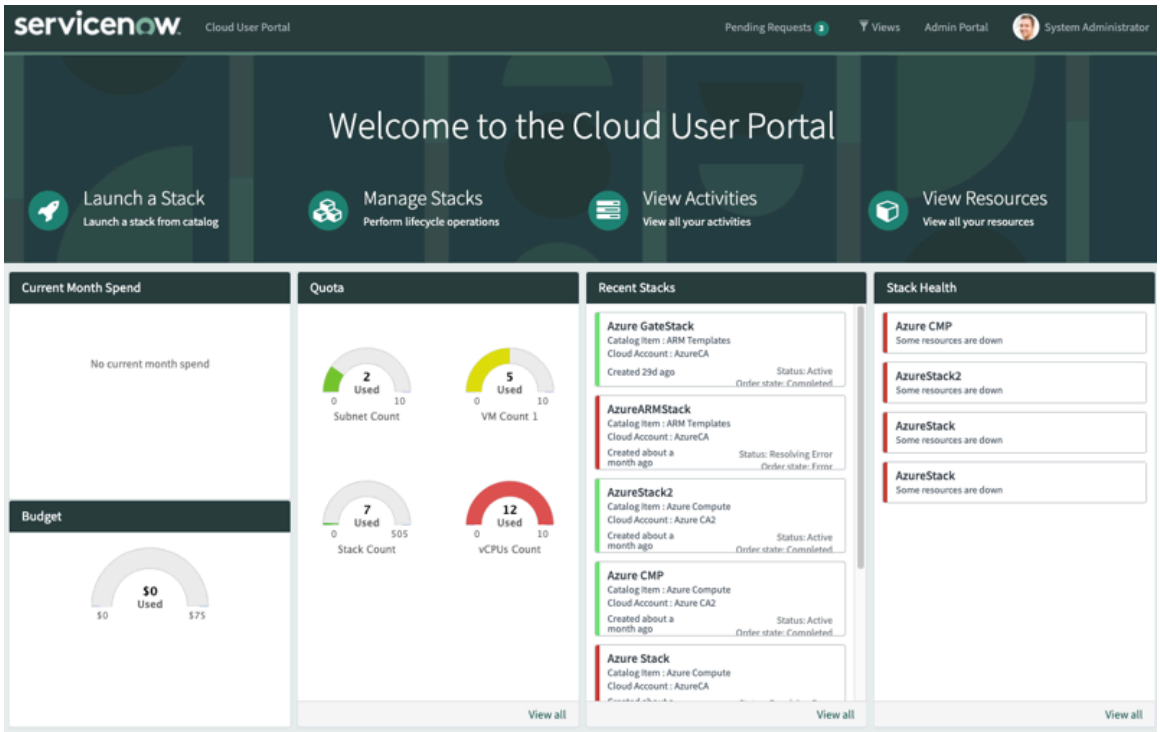
- Kontingente, Kosten, Budgets, Lebenszyklus-Events, Stapelintegrität und Anforderungen überwachen
- Stapel aus dem Servicekatalog anfordern und Anforderungen nachverfolgen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Lebenszyklusvorgänge für Stapel und Ressourcen anfordern (z. B. stoppen, starten oder Bereitstellung aufheben)
- Erstellen und Nachverfolgen von Incidents.

Seite „Overview“ (Übersicht) verwenden



Aufgaben auf der Seite „Overview“ (Übersicht)

Einen Stapel starten	Öffnen Sie den Servicekatalog von Elementen, die Sie anfordern können. Sie fordern ein Element an, und wenn die Anforderung genehmigt wird, startet das System den Stapel. Weitere Informationen finden Sie unter Einen Stapel starten.
Stapel verwalten	Sehen Sie die Ihnen zugewiesenen Stapel an. Weitere Informationen finden Sie unter Einen Stapel verwalten.
Aktivitäten anzeigen	Sehen Sie Aktivitäten für Ihre Stapel und Ressourcen an. Zu den Aktivitäten gehören Stapelanforderungen, Change-Anforderungen, Incidents, Cloud-Ereignisse und SSH-Schlüssel. Vgl. View Activities (Aktivitäten anzeigen).
Ressourcen anzeigen	Öffnet die Seite „Ressourcendetails“ zum Anzeigen von Details und Status einer Ressource. Weitere Informationen finden Sie unter Ressourcen verwalten.
Ausstehende Anforderungen	Wenn Sie eine Anforderung für einen Stapel übermitteln, zeigt die Seite **Acitivities** (Aktivitäten) Fortschritt und Status der Stapelanforderung an, und ein Link und ein Zähler für **Pending Requests** (ausstehende Anforderungen) werden angezeigt. Klicken Sie auf den Link, um eine Zusammenfassung der ausstehenden Stapelanforderungen aufzurufen. Weitere Informationen finden Sie unter Eine Stapel-Anforderung nachverfolgen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtig: Ab Release Yokohama sind die Widgets für aktuelle Monatsausgaben und Budget für nicht domänengetrennte Instanzen veraltet.

Schnellübersicht über Statusberichte auf der Seite „Overview“ (Übersicht)

Ansichten	Ein Filter zum Aufrufen und Verwalten Ihrer Ressourcen sowie der Ressourcen, die der Gruppe zugewiesen sind, der Sie angehören.
Aktuelle Monatsausgaben	Ein Diagramm, das die Kosten für Ihre Cloudressourcen nach Kategorie anzeigt.
Budget	Ein Bogendiagramm, das auf dem verbrauchten des Ihnen zugewiesenen Budgets basiert.
Mengen	In einem Diagramm wird der Kontingentverbrauch für kontingentdefinierte Ressourcentypen wie VM-Anzahl, vCPU-Anzahl, Größe des Speichervolume, Netzwerkanzahl und Stapelanzahl angezeigt. Sie können das von Ihnen verbrauchte Kontingent im Vergleich zu Ihrem maximal zugeteilten Kontingent anzeigen. Weitere Informationen finden Sie unter Kontingentgrenzen für Ressourcen anzeigen.
Letzte Stapel	Zehn Stapel, die Sie zuletzt angefordert haben. Jeder Eintrag zeigt **Namen**, angefordertes **Katalogelement**, das zum Anfordern des Stapels verwendete **Cloud-Konto** und den Auftragsstatus des angeforderten Stapels. Klicken Sie auf einen **Namen**, um die Stapeldetails aufzurufen.
Stapelintegrität	Zeigt die letzten 10 Elemente an: Für bereitgestellte Stapel erstellte Incidents oder aktive Stapel mit deaktivierter Ressource. Zeigt auch die Ressourcen an, die nicht verfügbar sind. Klicken Sie auf ein Element, um die Stapeldetails aufzurufen. Farbcodes für Incident-Typ: • Rot: Ausfall. • Orange: Leistungsproblem oder Funktionsstörung. • Grau: Frage oder Anforderung.

Verwenden der Taskleiste

Über die Taskleiste können Sie die folgenden Aktionen ausführen:

Übersicht	Rückkehr zur Homepage des Cloudbenutzerportals.
Katalog	Öffnet den Servicekatalog von Elementen, die Sie anfordern können. Wenn Sie eine **Servicekategorie** auswählen (VM, Compute, Netzwerk, Speicher usw.), werden im Abschnitt **All Items** (Alle Elemente) die Elemente in der ausgewählten Kategorie aufgelistet. Klicken Sie auf **Launch** (Starten), um ein Element anzufordern. Weitere Informationen finden Sie unter Einen Stapel starten.
Stapel	Listet alle Stapel auf, die Ihnen zugewiesen sind. Wählen Sie ein Katalogelement aus, um die vom Element gestarteten Stapel anzeigen zu lassen. Klicken Sie auf einen Stapel, um

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	Details aufzurufen – alle Ressourcen, Ressourceneigenschaften, Aktivitäten und Lebenszyklusvorgänge. Weitere Informationen finden Sie unter Einen Stapel verwalten.
Ressourcen	Listet einzelne Ressourcen der bereitgestellten Stapel auf, die Ihnen zugewiesen sind, unabhängig davon, wer den Stapel angefordert hat. Weitere Informationen finden Sie unter Ressourcen verwalten.
Aktivitäten	Stapel-Anforderungen, Change-Anforderungen, Cloud-Lebenszyklus-Events (falls konfiguriert) und Incidents, die Ihren Stapeln und Ressourcen zugeordnet sind. SSH-Schlüssel, die Sie erstellt haben oder die für Sie generiert wurden. Vgl. View Activities (Aktivitäten anzeigen).

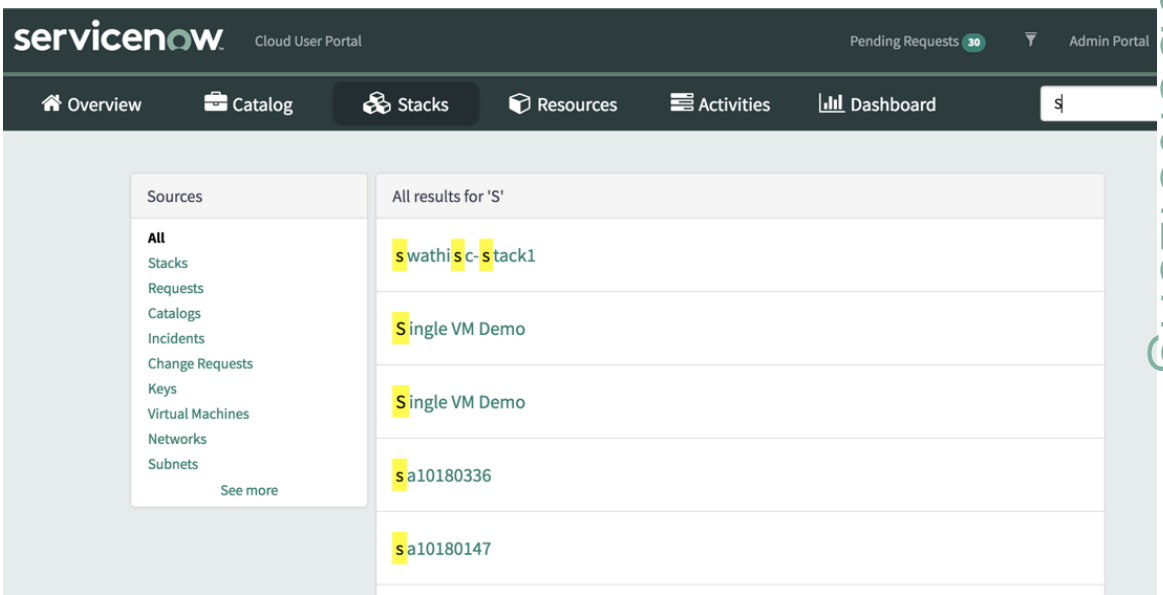
Das Cloud-Benutzerportal durchsuchen

Die Suchseite gibt Suchergebnisse zurück und bietet Filter, mit denen Sie Ergebnisse einschränken können.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Geben Sie auf einer beliebigen Portalseite Text in das Textfeld **Search** (Suchen) ein, und drücken Sie die **Eingabetaste**.
2. Zum Filtern der Suchergebnisse auf der Seite **Cloud Search** (Cloudsuche) klicken Sie auf eine Kategorie.
   In diesem Beispiel werden nur **Stapel**, die den Suchtext `s` umfassen, in der Liste **Search Results** (Suchergebnisse) angezeigt:



Einen Stapel starten

Starten Sie einen Stapel Cloud-Ressourcen, um eine Anforderung für ein Element im Servicekatalog zu übermitteln. Sie können einen Stapel über die Übersichtsseite des Cloud-Benutzerportals starten.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wenn Sie eine Anforderung für ein Element an den Servicekatalog übermitteln, stellt das System den Stapel in der Regel sofort bereit. Manchmal muss die Anforderung zuerst genehmigt werden.

Wenn für eine Ressource in einem Stapel beim Zugriff über SSH Anmeldeinformationen erforderlich sind, müssen Sie ein SSH-Schlüsselpaar erstellen, bevor Sie den Stapel starten können. Siehe Einen SSH-Schlüssel erstellen und Einen SSH-Schlüssel herunterladen.

Prozedur

1. Öffnen Sie das Anforderungsformular mit einer der folgenden Methoden:
   - Klicken Sie auf der Übersichtsseite auf **Einen Stapel starten**. Standardmäßig werden alle Katalogelemente in allen Servicekategorien aufgelistet. Wählen Sie eine **Servicekategorie**, und klicken Sie dann auf den **Namen** eines Katalogelements.
   - Öffnen Sie die Seite **Catalog** (Katalog). Standardmäßig werden alle Katalogelemente in allen Servicekategorien aufgelistet. Wählen Sie eine **Servicekategorie**, und klicken Sie dann auf **Launch** (Starten) für ein Katalogelement.
2. Geben Sie in jedem Abschnitt des Formulars die Werte ein, die Ihre Anforderung konfigurieren.

   Die Formularfelder unterscheiden sich für jedes Katalogangebot. Wenden Sie sich an Ihren Administrator für Cloud Provisioning and Governance, wenn Sie Fragen zu den Feldern haben.

   > **Wichtig:** Wenn Sie im Formular eine Benutzergruppe auswählen, werden die Kontingentgrenzen für Sie und die Benutzergruppe (zu der Sie gehören) im Abschnitt „Kontingent“ angezeigt.

   Die folgenden Unterschritte gelten nur, wenn Sie den Terraform-Connector und installierbare Terraform-Konfigurationen verwenden.

   a. Wählen Sie im Abschnitt „Allgemeine Informationen“ für die Option *UseExistingWorkspace* den Eintrag **Ja** aus, um vorhandene Arbeitsbereiche zu verwenden, die bereits erkannt wurden.

   b. Wählen Sie in der Liste **Arbeitsbereich** den Arbeitsbereich aus, in dem sich die installierbare Konfiguration befindet.

   > **Hinweis:** Wenn Sie eine Windows-VM konfigurieren, setzen Sie das Feld **IncludeManagementKey** auf **No** (Nein). Nach der Bereitstellung der VM können Sie den Vorgang des zweiten Tags namens „InfuseKey“ verwenden, um der VM Schlüsselanmeldeinformationen (**UserName** und **Password**) hinzuzufügen.

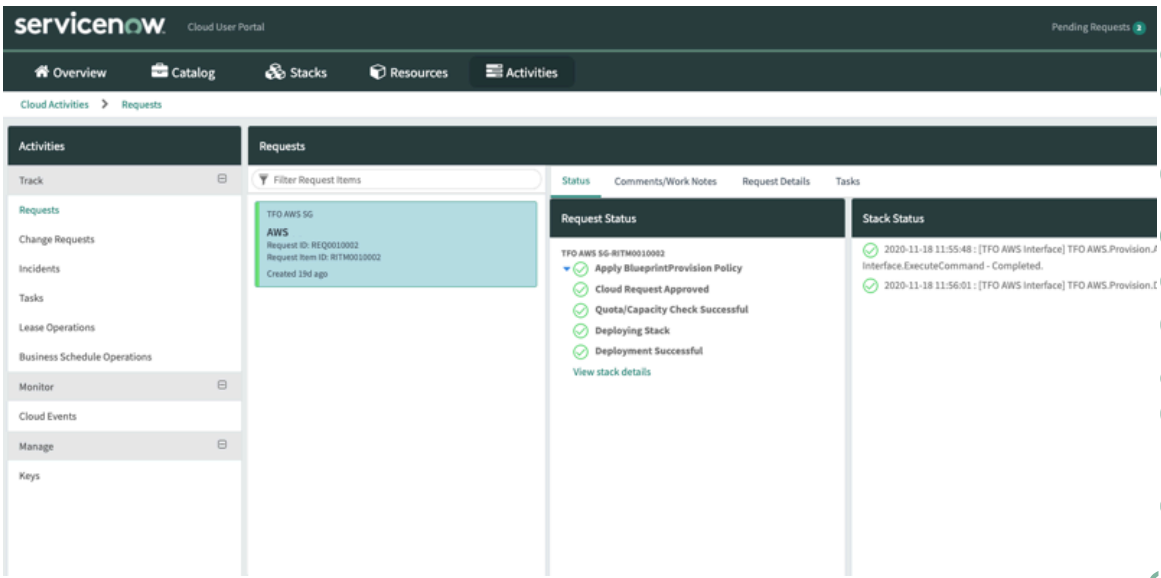
3. Wahlweise: Wählen Sie im Abschnitt „Allgemeine Informationen“ den Agent-Pool aus, den Sie in Ihrer Terraform Enterprise-Organisation für die Kommunikation mit einer privaten oder lokalen Infrastruktur erstellt haben.

   > **Hinweis:** Die Auswahl des Agent-Pools betrifft nur Bereitstellungs-Setups für VMware über Terraform Enterprise. Sie müssen in Ihrer Terraform Enterprise-Organisation Agent-Pools erstellt haben und in Ihrem Arbeitsbereich über VMware-Terraform Enterprise-Vorlagen verfügen, damit die Option für Agent-Pools in der GUI angezeigt wird.

4. Klicken Sie auf die Abschnittsüberschrift, um zum nächsten Abschnitt zu wechseln. Das verbleibende Kontingent wird basierend auf der von Ihnen ausgewählten Benutzergruppe aktualisiert. Für Pflichtfelder wird standardmäßig das erste Element in der Liste ausgewählt. Sie können dann einen beliebigen Wert auswählen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

5. Klicken Sie auf **Submit** (Absenden), um den Stapel anzufordern.
   - Die Seite **„Aktivitäten“** wird auf der Registerkarte **Status** im geöffnet **Titel** > **Anforderungen** Aktivität Die Registerkarte zeigt den Fortschritt und den Status der Anforderung an. Die folgenden Farbcodes zeigen die Phase der Anforderung an:
   - ▪ Grün: Abgeschlossen oder genehmigt.
     ▪ Orange: Wird verarbeitet.
     ▪ Rot: Abgelehnt, Fehler oder Abgebrochen.
   - Wenn eine Genehmigung erforderlich ist, startet das System den Stapel, nachdem der Administrator Ihre Anforderung genehmigt hat, und aktualisiert den **Anforderungsstatus**.
   - Wenn die Kontingentgrenze für Sie oder Ihre Benutzergruppe überschritten wird, wird eine Fehlermeldung angezeigt, oder es wird ein richtlinienbasierter Genehmigungs-Workflow ausgelöst. Weitere Informationen über Kontingentgrenzen finden Sie unter Kontingentgrenzen für Ressourcen anzeigen.
   - Wählen Sie eine andere Anforderung aus, um deren **Anforderungsstatus** und **Stapelstatus** anzeigen zu lassen.
   - Zum Anzeigen einer Zusammenfassung aller ausstehenden Anforderungen können Sie in der Titelleiste jederzeit auf den Link **Pending Requests** (Ausstehende Anforderungen) klicken.



Automatische Übersetzung

Kontingentgrenzen für Ressourcen anzeigen

Zeigen Sie Kontingentgrenzen an, um nachzuvollziehen, wie viele Ressourcen Sie verbraucht haben und wie viele Ressourcen Sie basierend auf den für Sie und Ihre Benutzergruppe festgelegten Kontingentgrenzen bereitstellen können.

Zugeteilte und verbrauchte Kontingentgrenzen

Um das von Ihnen für die Bereitstellung von Ressourcen verbrauchte Kontingent im Vergleich zu dem Ihnen zugeteilten Höchstkontingent anzuzeigen, navigieren Sie zur Seite „Übersicht“. Für die folgenden vordefinierten Ressourcentypen im System sind möglicherweise Kontingentgrenzen für Sie und die Benutzergruppen festgelegt, denen Sie angehören:

- Stapelanzahl
- VM-Anzahl

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- vCPU-Anzahl
- Größe des Speichervolume
- Netzwerkanzahl

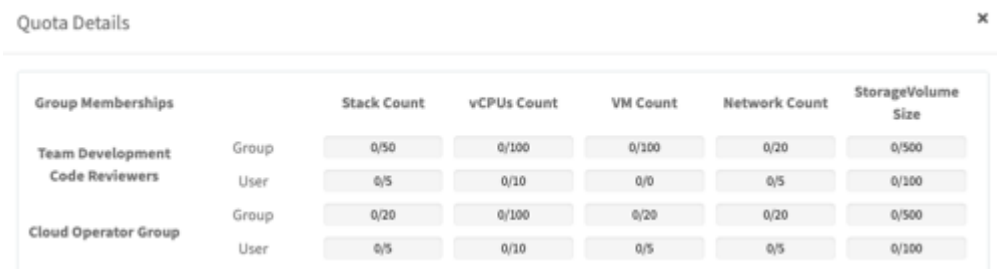
Hinweis: Die Stapelanzahl ist eine im Basissystem bestehende Standardkontingentgrenze, die seit Release Yokohama verfügbar ist. Sie wird auf der Seite „Übersicht“ angezeigt, wenn Ihr Cloud Provisioning and Governance-Administrator ein Kontingent für die Stapelanzahl für Sie oder Ihre Benutzergruppe festgelegt hat.

Auf der Seite „Übersicht“ werden im Abschnitt „Kontingent“ die Kontingentgrenzen in einem Diagramm angezeigt.

- Grün zeigt an, dass genügend Ressourcen verfügbar sind.
- Rot zeigt an, dass nicht genügend Ressourcen verfügbar sind.
- Wenn Kontingentgrenzen überschritten wurden, zeigt das System entweder eine Fehlermeldung an oder löst einen richtlinienbasierten Genehmigungs-Workflow aus, sobald Sie versuchen, einen Stapel bereitzustellen. Weitere Informationen finden Sie unter Stapel auf Basis von Kontingentgrenzen bereitstellen.

Die Kontingentgrenze, die im Abschnitt „Kontingent“ angezeigt wird, ist eine Zusammenfassung aller Benutzergruppen, denen Sie angehören. Um Kontingentgrenzen für Sie und Ihre Benutzergruppen separat anzuzeigen, klicken Sie auf **Alle anzeigen**. Das Popup-Fenster „Kontingentdetails“ wird angezeigt.

Popup-Fenster „Kontingentdetails“


Quota Details

Group Memberships		Stack Count	vCPUs Count	VM Count	Network Count	StorageVolume Size
Team Development Code Reviewers	Group	0/50	0/100	0/100	0/20	0/500
	User	0/5	0/10	0/0	0/5	0/100
Cloud Operator Group	Group	0/20	0/100	0/20	0/20	0/500
	User	0/5	0/10	0/5	0/5	0/100

Im Popup-Fenster „Kontingentdetails“ wird Ihr verbrauchtes Kontingent der zugeteilten Kontingentgrenze für jeden Ressourcentyp gegenübergestellt. Zum Beispiel bedeutet „0/5“ für einen Ressourcentyp, dass 0 Ressourcen verbraucht wurden und die zugeteilte Kontingentgrenze 5 Ressourcen beträgt.

Die Kontingentgrenze für einen Ressourcentyp wird entweder als Summe oder als Anzahl angezeigt. Beispielsweise wird die Größe von Speichervolumes als Summe in GB angezeigt, und die VM-Anzahl wird als Zahl angezeigt.

Sie können Kontingentgrenzen auch beim Starten von Stapeln anzeigen. Weitere Informationen finden Sie unter Einen Stapel starten.

Stapel auf Basis von Kontingentgrenzen bereitstellen

Wenn Sie Stapel bereitstellen, berechnet das System das Ihnen und Ihren Benutzergruppen zugeteilte Kontingent. Wenn Kontingentgrenzen überschritten wurden, zeigt das System entweder eine Fehlermeldung an oder löst einen richtlinienbasierten Genehmigungs-Workflow aus

Um Kontingentgrenzen anzuzeigen, navigieren Sie zur Seite „Übersicht“. Weitere Informationen finden Sie unter Kontingentgrenzen für Ressourcen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Kontingentberechnung für vorlagenbasierte Stapel

Die Stapelanzahl ist eine im Basissystem bestehende Standardkontingentgrenze, die seit Release Yokohama verfügbar ist. Die Grenze gilt für alle vorlagenbasierten Stapel im Servicekatalog.

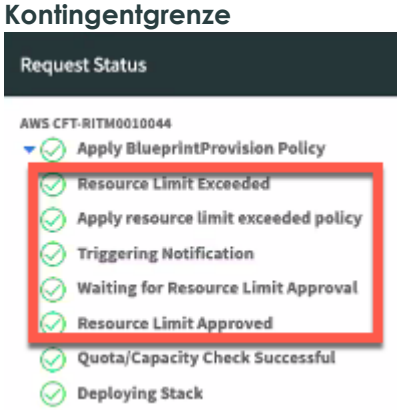
Wenn Ihr Cloud Provisioning and Governance-Administrator für Sie oder Ihre Benutzergruppe ein Stapelanzahl-Kontingent festgelegt hat, berechnet das System die Stapelanzahl, sobald Sie einen Stapel bereitstellen. Nach der Bereitstellung wird die Stapelanzahl des Kontingents für jeden bereitgestellten Stapel um den Wert 1 erhöht.

Stapelbereitstellung nach Überschreiten der Kontingentgrenzen

Wenn die für Sie oder Ihre Benutzergruppe festgelegte Kontingentgrenze überschritten wurde, zeigt das System entweder eine Fehlermeldung an oder löst einen zugeordnete Regel aus, sobald Sie versuchen, einen Stapel bereitzustellen.

- Falls das System eine Fehlermeldung anzeigt, die darauf hinweist, dass die Kontingentgrenze überschritten wurde, können Sie den Stapel nicht bereitstellen. Wenn Sie der Meinung sind, dass die Kontingentgrenze erhöht werden muss, wenden Sie sich an Ihren Cloud Provisioning and Governance-Administrator.
- Ist im System eine Richtlinie für die Überschreitung der Kontingentgrenze definiert, wird diese ausgelöst. Je nach Richtlinie löst das System eine Genehmigungsanforderung oder eine Benachrichtigung zur Erhöhung der Kontingentgrenze aus. Die Anforderung folgt einem im System vordefinierten Workflow für Genehmigungen. Wenn die Anforderung genehmigt wird, stellt das System den Stapel bereit.

Ausgelöste Richtlinie zur Bereitstellung eines Stapels nach Überschreiten der Kontingentgrenze



Eine Stapel-Anforderung nachverfolgen

Das System generiert eine Anforderung, wenn Sie das Formular zum Starten eines Stapels übermitteln.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird

Wenn keine Genehmigungsrichtlinie definiert ist, werden Anforderungen automatisch genehmigt. Wenn eine Richtlinie definiert ist, muss ein Benutzer auf der Genehmigerliste die Anforderung genehmigen.
Wenn die Kontingentgrenze für Sie oder Ihre Benutzergruppe überschritten wird, wird eine Fehlermeldung angezeigt, oder es wird ein richtlinienbasierter Genehmigungs-Workflow ausgelöst. Weitere Informationen über Kontingentgrenzen finden Sie unter Kontingentgrenzen für Ressourcen anzeigen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Wechseln Sie zur Seite **Aktivitäten**, oder navigieren Sie zu **Übersicht** > **Aktivitäten anzeigen**, und wählen Sie dann aus **Titel** > **Anforderungen**.
   Die folgenden Farbcodes zeigen den Status der Anforderung an:
   - Grün: Abgeschlossen oder genehmigt.
   - Orange: Wird verarbeitet.
   - Rot: Abgelehnt, Fehler oder Abgebrochen.
2. Klicken Sie in der Liste **Requests** (Anforderungen) auf einen Eintrag.

Registerkarte **Status**	
Anforderungsstatus	Für die Anforderung ausgeführte Aktionen. Durch Klicken auf den Abwärtspfeil (▼) wechseln Sie zwischen den folgenden Optionen: ◦ Ausführlicher Modus, der jede Aktion und den Status der Aktion beschreibt. ◦ Nur-Symbol-Modus, der nur den Status (Erfolg/Misserfolg) einer Aktion anzeigt.
Stapelstatus	Status der einzelnen Stapelanforderungen. Wenn die Bereitstellung fehlschlägt, werden Fehler von der Cloud-Orchestrierung aufgelistet.
Registerkarte **Comments / Work Notes** (Kommentare/Arbeitsnotizen)	
Angefordertes Element und Anforderungsnummer	Protokoll der Kommentare und Notizen, die für die Anforderung erstellt wurden. Die Rolle **itil** ist erforderlich, um einen Kommentar oder eine Arbeitsnotiz hinzuzufügen. So fügen Sie einen Kommentar oder eine Arbeitsnotiz hinzu: **a.** Geben Sie den Text ein. **b.** Wählen Sie das Kontrollkästchen **Work Notes** (Arbeitsnotizen), um eine Arbeitsnotiz hinzuzufügen. **c.** Klicken Sie auf **Senden**.
Registerkarte **Request Details** (Anforderungsdetails)	Werte, die der Anforderer auf dem Stapel-Anforderungsformular übermittelt hat.
Registerkarte **Tasks** (Aufgaben)	Listet alle Katalogaufgaben auf, die für Stapel erstellt wurden, welche nicht bereitgestellt werden konnten. Klicken Sie auf eine Katalogaufgabe, um weitere Details zu dieser Aufgabe anzuzeigen. Weitere Informationen finden Sie unter Eine fehlgeschlagene Stapel-Anforderung erneut übermitteln.

Eine fehlgeschlagene Stapel-Anforderung erneut übermitteln

Die Anwendung Cloud Provisioning and Governance erstellt eine Nachbesserungs- oder Katalogaufgabe, wenn die Anforderung für einen Stapel nicht bereitgestellt werden kann. Sie können die fehlgeschlagene Anforderung erneut übermitteln oder der Cloud-Operator-Gruppe zuweisen, damit diese sie für Sie bearbeitet.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen
Erforderliche Rollen: sn_cmp.cloud_service_user und sn_cmp.cloud_operator.

Warum und wann dieser Vorgang ausgeführt wird
Die Aufgabennachbesserung erfasst alle auf eine fehlgeschlagene Anforderung angewendeten Nachbesserungen. Sie können die für eine fehlgeschlagene Anforderung durchgeführte Nachbesserung und alle wichtigen Meilensteine auf der Unterregisterkarte **Comments/Work Notes** (Kommentare/Arbeitsnotizen) in Cloudbenutzerportal anzeigen lassen. Die Aufgabennachbesserung ist nur für die neue Bereitstellung von Stapeln und nicht für den Lebenszyklus oder andere Vorgänge verfügbar.

Die Bereitstellung eines Stapels kann aus vielen Gründen fehlschlagen. Ein Stapel schlägt möglicherweise fehl, wenn Sie Ihr Cloud-Kontingent oder die Kapazität Ihres Rechenzentrums überschritten haben oder einen ungültigen Parameter im Anforderungsformular eingegeben haben (z. B. doppelte NICs).

Wenn die Bereitstellung eines Stapels fehlschlägt, wird eine Katalogaufgabe erstellt und Ihnen zugewiesen. Eine Fehlermeldung zur fehlgeschlagenen Anforderung wird auf der Unterregisterkarte **Status** in Cloudbenutzerportal angezeigt.

Prozedur
1. Navigieren Sie in Cloudbenutzerportalzu **Aktivitäten anzeigen** > **Anforderungen** > **Aufgaben**.
2. Klicken Sie auf die Katalogaufgabe, die erneut zu übermitteln ist.
3. Wählen Sie eine Aktion nach Ihren Wünschen aus:
   - **Retry** (Wiederholen): Übermittelt die fehlgeschlagene Anforderung erneut. Sie können versuchen, die fehlgeschlagene Anforderung erneut zu übermitteln, indem Sie den Fehler nach Möglichkeit beheben. Wenn der Fehler auf das Überschreiten der Kontingentgrenze zurückzuführen ist, können Sie versuchen, die Bereitstellung einiger Ressourcen aufzuheben, die derzeit nicht verwendet werden, und dann auf **Retry** (Wiederholen) klicken. Wenn Sie auf **Retry** (Wiederholen) klicken, wird die ursprüngliche Anforderung erneut übermittelt. Es wird keine neue Anforderung erstellt.

     Hinweis: Alle Richtlinien, die einem Ressourcenvorgang zugeordnet sind, werden erneut ausgeführt.

   - **Ask for Help** (Um Hilfe bitten): Erstellt eine neue Katalogaufgabe und weist sie der Cloud-Operator-Gruppe zu, um die fehlgeschlagene Anforderung erneut zu übermitteln. Die Gruppe Cloud-Operator-Gruppe kann den Fehler genauer untersuchen und versuchen, ihn für Sie zu beheben. Jedes Mal, wenn die Kommentare oder Arbeitsnotizen in der Katalogaufgabe von der Cloud-Operator-Gruppe aktualisiert werden, werden die Änderungen auf der Unterregisterkarte **Comments/Work Notes** (Kommentare/Arbeitsnotizen) in Cloudbenutzerportal angezeigt. Bei Bedarf kann der Operator die fehlgeschlagene Anforderung abbrechen.
   - **Cancel Order** (Auftrag stornieren): Storniert die fehlgeschlagene Anforderung und hebt die Bereitstellung aller teilweise bereitgestellten Ressourcen auf.

Einen Stapel verwalten
Über die Seite „Stack Details“ (Stapeldetails) können Sie Details und Status für einen Stapel aufrufen und Lebenszyklusvorgänge für einen Stapel durchführen.

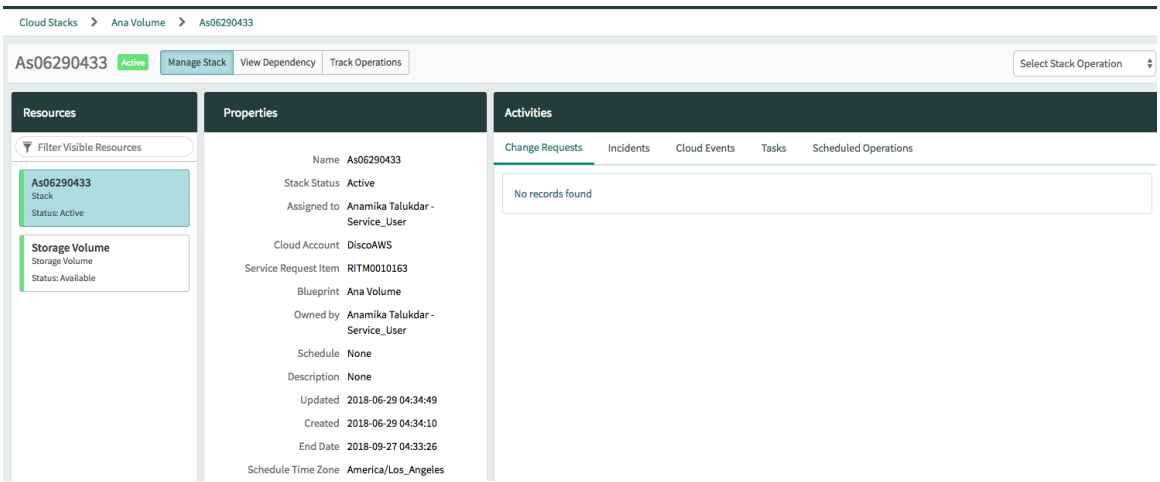
Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Über eine der folgenden Methoden öffnen Sie die Seite **Stack Details** (Stapeldetails):
   - Klicken Sie auf der Symbolleiste auf **Stapel**.
   - Verwenden Sie das Textfeld **Suchen**, um den Stapel zu suchen.
   - Klicken Sie auf der Homepage auf einen Stapel im Abschnitt **Letzte Stapel** oder **Stack-Integrität**.
   - Klicken Sie auf der Homepage auf **Stapel verwalten**.

   Standardmäßig werden alle Stapel in allen Servicekategorien aufgelistet.
2. Wählen Sie in der Liste **Stapel** eine Stapelkategorie, und klicken Sie dann auf den **Namen**eines Stapels.
   Auf der Seite **Stack Details** (Stapeldetails) werden die folgenden Informationen angezeigt:



   - Breadcrumb-Navigation
   - Name des Stapels. Klicken Sie auf **Abhängigkeit anzeigen**, um die Abhängigkeitszuordnung für den Stapel aufzurufen, auf **Stapel verwalten**, um Ressourcen, Eigenschaften und Aktivitäten des Stapels anzuzeigen, und auf **Vorgänge nachverfolgen**, um die Liste der Lebenszyklusvorgänge anzuzeigen, die für den Stapel und seine Ressourcen ausgeführt werden.
   - Statusinformationen
   - Liste aller Ressourcen im Stapel. Wenn Sie auf eine Ressource klicken, können Sie im Abschnitt **Properties** (Eigenschaften) Details einsehen. Farbcodes zeigen den Status des Stapels an:
     - Grün: Aktiviert/Aktiv.
     - Gelb: Deaktiviert oder Verarbeitung.
     - Rot: Beendet oder Fehler.
   - Liste der Stapeleigenschaften. Einige Eigenschaften werden im Stapelanforderungsformular festgelegt, andere werden durch Richtlinien festgelegt.
   - Aktivitäten, die dem Stapel zugeordnet sind. Klicken Sie auf eine Registerkarte, um Folgendes anzeigen zu lassen:
     - Change-Anforderungen, die dem Stapel zugeordnet sind. Weitere Informationen finden Sie unter Change-Anforderungen nachverfolgen.
     - Incidents, die für den Stapel ausgelöst wurden. Siehe Übermitteln eines Incidents für einen Stapel und Incidents nachverfolgen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Cloud-Events, die dem Stapel zugeordnet sind. Cloud-Events wird nur angezeigt, wenn eine Ressource ausgewählt ist. Weitere Informationen finden Sie unter Cloud-Events anzeigen.
- Katalogaufgaben die dem Stapel zugeordnet sind. Weitere Informationen finden Sie unter Eine fehlgeschlagene Stapel-Anforderung erneut übermitteln.
- Bevorstehende Zeitplanvorgänge für Geschäftszeiten, die dem Stapel zugeordnet sind. Sie können einen bevorstehenden Vorgang überspringen oder einen dem Stapel zugeordneten Zeitplan abbrechen. Weitere Informationen finden Sie unter Geschäftszeitplanvorgänge für einen Stapel ändern.

◦ Vorgänge, die Sie auf einem Stapel ausführen können. Weitere Informationen finden Sie unter Einen Lebenszyklusvorgang für einen Stapel oder eine Ressource durchführen.

◦ Textfeld, das zum Durchsuchen des Cloud-Benutzerportals nach Stapeln, Ressourcen basierend auf Typen, Stapelanforderungen, Change-Anforderungen, Incidents, Schlüsseln und Katalogelementen verwendet wird.

Stapeleigenschaften

Name	Name, den Sie bei der Anforderung des Stapels angegeben haben.
Stapelstatus	Aktueller Status des Stapels: ◦ Aktiv (bereitgestellte Stapel) ◦ Beendet (Stapel mit aufgehobener Bereitstellung) ◦ Nicht verwaltet (erfasste Stapel) ◦ Fehler (fehlerhafte Stapel) ◦ Wird verarbeitet (Stapel werden verarbeitet)
Zugewiesen an	Besitzer der Stapelkonfiguration. Dies beeinflusst die Zugriffssteuerungen und Ansichten im Cloud-Portal.
Cloud-Account	Cloud-Konto, dem der Stapel zugeordnet ist.
Serviceanforderungselement	Datensatz, der in der Tabelle „Request Item“ (Anforderungselement) erstellt wurde, als Sie den Katalog bestellt haben, der zu diesem Stapel geführt hat.
Blaupause	Blaupause, der der Stapel zugeordnet ist.
Eigentum von	Benutzername der anfordernden Person.
Besitzergruppe	Name der Gruppe, zu der der Besitzer des Stapels gehört.
Zeitplan	Der Zeitplan ist dem Stapel zugeordnet.
Ausgabe	Spezifische Details für ARM/CFT-Stapel, z. B. die URL einer Anwendung, Namen oder Speicherorte erstellter Ressourcen.
Aktualisiert	Datum und Uhrzeit der letzten Aktualisierung der Stapeldetails.
Erstellt	Datum und Uhrzeit der Anforderung des Stapels.
Enddatum	Datum und Uhrzeit der Beendigung (nicht bereitgestellt) des Stapels.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcen verwalten

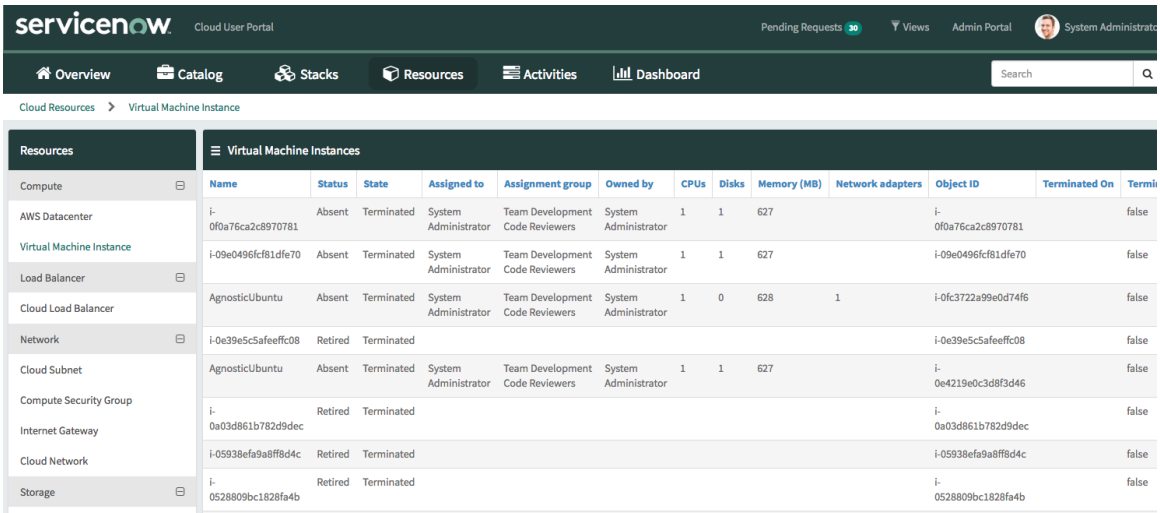
Über die Seite „Resource Details“ (Ressourcendetails) können Sie Details und Status für eine Ressource aufrufen und Lebenszyklusvorgänge für eine Ressource durchführen.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

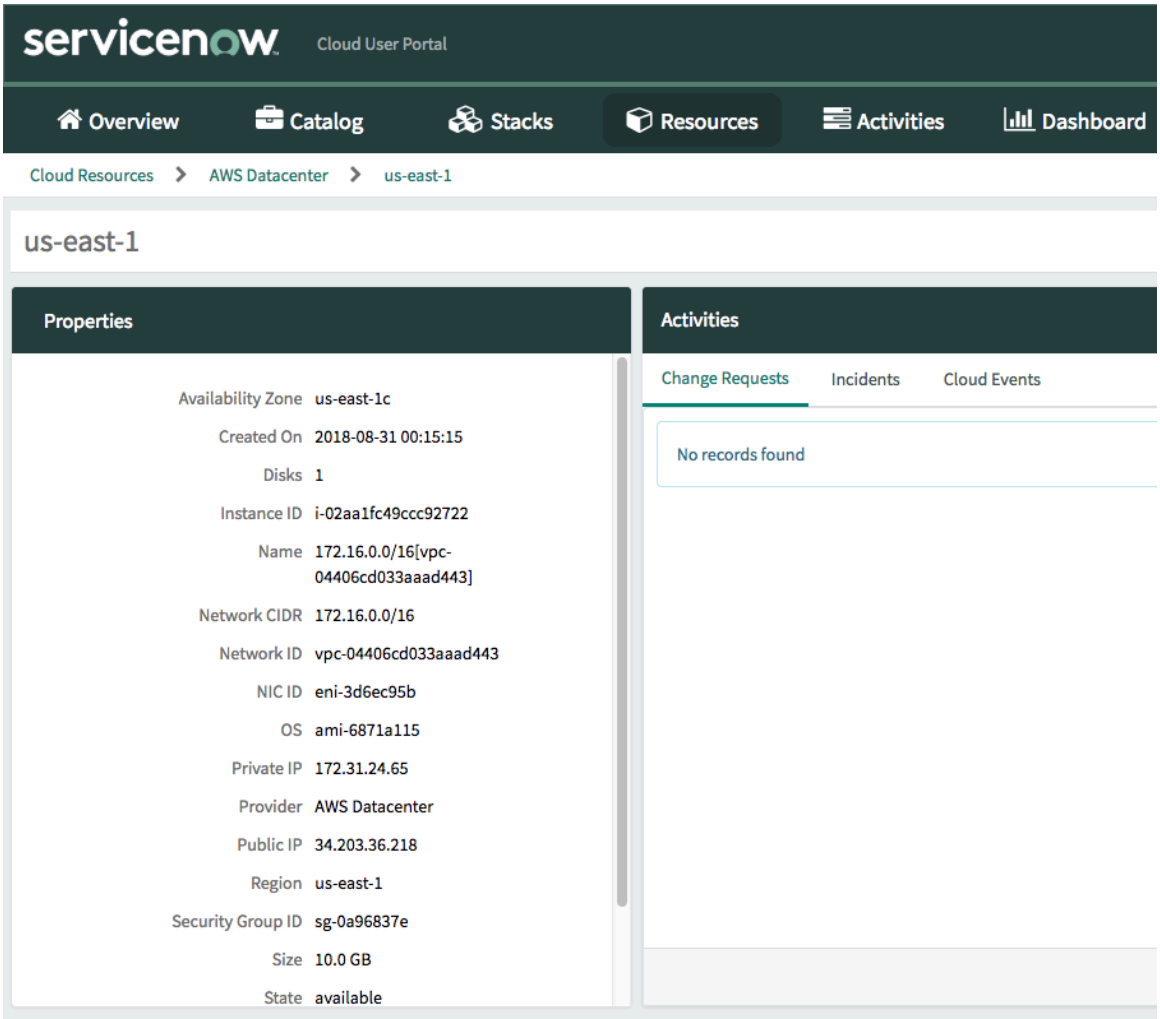
1. Klicken Sie auf der Symbolleiste auf **Resources** (Ressourcen).
   Die Seite **Resources** (Ressourcen) listet alle Ressourcentypen im linken Bereich auf.



2. Navigieren Sie zum entsprechenden Ressourcentyp, um die Liste der Ressourcen aufzurufen, die Sie interessieren, und klicken Sie dann auf einen Ressourcennamen, um spezifische Details zu dieser Ressource anzeigen zu lassen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.



Der Ressourcendetailbildschirm enthält folgende Informationen:

- Breadcrumb-Navigation
- Alle für die Ressource spezifischen Eigenschaften
- Aktivitäten, die der Ressource zugeordnet sind. Klicken Sie auf eine Registerkarte, um Folgendes anzeigen zu lassen:
  - Change-Anforderungen, die der Ressource zugeordnet sind. Weitere Informationen finden Sie unter Change-Anforderungen nachverfolgen.
  - Incidents, die für die Ressource ausgelöst wurden. Siehe Übermitteln eines Incidents für einen Stapel und Incidents nachverfolgen.
  - Cloud-Events, die bezüglich der Ressource eingetreten sind. Weitere Informationen finden Sie unter Cloud-Events anzeigen.
- Textfeld, das zum Durchsuchen des Cloud-Benutzerportals nach Stapeln, Ressourcen basierend auf Typen, Stapelanforderungen, Change-Anforderungen, Incidents, Schlüsseln und Katalogelementen verwendet wird.

Einen Lebenszyklusvorgang für einen Stapel oder eine Ressource durchführen

Vorgänge wie Start/Stopp, „Aufheben der Bereitstellung“ und „Skript ausführen“ werden Lebenszyklusvorgänge oder Tag-2-Vorgänge genannt. Wenn Sie einen Lebenszyklusvorgang für einen Stapel oder eine Ressource anfordern, wird vom System eine Change-Anforderung erzeugt. In einer Genehmigungsrichtlinie ist festgelegt, dass der Change entweder

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

automatisch genehmigt wird oder dass ein Benutzer auf der Genehmigerliste den Change genehmigen muss.

Vorbereitungen

Erforderliche Rolle:

Lebenszyklusvorgänge erfordern den Benutzer mit der Rolle `sn_cmp.cloud_service_user`, der die Ressource besitzt. Benutzer mit den Rollen „root_admin“, „admin“ oder `sn_cmp.cloud_admin` können den Vorgang ebenfalls ausführen.

Warum und wann dieser Vorgang ausgeführt wird

- Wie in den Beschreibungen erwähnt, werden nicht alle Vorgänge für alle Anbieter oder für alle Servicekategorien (Ressourcentypen) unterstützt.
- Für alle anderen Anbieter der Konfigurationsverwaltung gilt: Wenn für einen Stapel oder eine Ressource eine Anmeldung erforderlich ist, müssen Sie den zugehörigen SSH-Schlüssel herunterladen, bevor Sie auf die Ressource zugreifen können. Weitere Informationen finden Sie unter Einen SSH-Schlüssel herunterladen.

Prozedur

1. Wählen Sie einen Stapel oder eine Ressource aus.
2. Wählen Sie auf der Seite **Stack Details** (Stapeldetails) den Vorgang aus den Listen **Stapelvorgang auswählen** oder **Ressourcenvorgang auswählen** aus.
   Vollständige Beschreibungen der Vorgänge finden Sie unter Lebenszyklusvorgänge in Cloud Provisioning and Governance.

   Für einige Vorgänge sind Einstellungen erforderlich (z. B. der Name eines Skripts oder neue Zeitplaneinstellungen).
3. Geben Sie die Einstellungen ein, und klicken Sie auf **OK**.
   Das System übermittelt eine Change-Anforderung und die **Aktivitäten** > **Change-Anforderungen** Seite zeigt den Fortschritt und Status der Anforderung an.

Lebenszyklusvorgänge in Cloud Provisioning and Governance

Vorgänge wie Start/Stopp, „Aufheben der Bereitstellung“ und „Skript ausführen“ werden Lebenszyklusvorgänge oder Tag-2-Vorgänge genannt. Wenn Sie einen Lebenszyklusvorgang für einen Stapel oder eine Ressource anfordern, wird vom System eine Change-Anforderung erzeugt. In einer Genehmigungsrichtlinie ist festgelegt, dass der Change entweder automatisch genehmigt wird oder dass ein Benutzer auf der Genehmigerliste den Change genehmigen muss.

Um einen Vorgang durchzuführen, wählen Sie einen Stapel oder eine Ressource und klicken Sie dann auf **Stapelvorgang auswählen** oder **Ressourcenvorgang auswählen** aus. Die Liste enthält nur Vorgänge, die für die ausgewählte Ressource oder den ausgewählten Stapel einschlägig sind. Einige Vorgänge werden von Configuration Management Systems wie Ansible oder Terraform bereitgestellt.

Vorgänge in Basissystem

Start

Der Vorgang *`Start`* startet den ausgewählten virtuellen Computer. Der Ressourcenstatus wechselt auf „On“ (Aktiviert).

Keine Einstellung ist erforderlich.

Stoppen

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der Vorgang *Stop* hält den ausgewählten virtuellen Computer an. Der Ressourcenstatus wechselt auf „Off“ (Deaktiviert).

Keine Einstellung ist erforderlich.

Aufheben der Bereitstellung

Der Vorgang *Deprovision* (Aufheben der Bereitstellung) beendet den ausgewählten Stapel und sendet eine Benachrichtigung an den Stapelbesitzer.

Keine Einstellung ist erforderlich.

Vorgänge über die Erweiterungsschnittstelle des virtuellen Computers

Nur Google Cloud Platform und IBM Cloud unterstützen Vorgänge über die *Store-Erweiterungsschnittstelle für virtuelle Computer*. Die App Terraform Connector ServiceNow Store stellt die Vorgänge bereit.

Store-Erweiterungsschnittstelle des virtuellen Computers.ExecuteScript

Der Vorgang *ExecuteScript* führt ein Skript auf der ausgewählten Windows- oder Linux-VM aus. Beispielsweise kann ein Skript eine Anwendung auf einer Ressource installieren. Detaillierte Anweisungen finden Sie unter KB0756431 .

Hinweis: Zum Ausführen des Vorgangs *ExecuteScript* muss ein virtueller Computer Anmeldeinformationen enthalten. Virtuelle Computer unter Linux erben bei ihrer Bereitstellung Anmeldeinformationen für den Managementschlüssel. Verwenden Sie für virtuelle Computer unter Windows den Vorgang *InfuseKey*, um dem virtuellen Computer Anmeldeinformationen hinzuzufügen.

Geben Sie im Popup-Fenster Folgendes an:

- **ScriptType**: Shell- und PowerShell-Skripte werden unterstützt.
- **Script**: Name des Skripts.

Store-Erweiterungsschnittstelle des virtuellen Computers.InfuseKey

Der Vorgang *InfuseKey* fügt bei virtuellen Computern unter Windows Schlüsselanmeldeinformationen (öffentliche und private Schlüsselpaarwerte) hinzu.

Daher können Sie die Anmeldeinformationen in der Liste „Eigenschaften“ des virtuellen Computers unter Windows einsehen und die Anmeldeinformationen zum Ausführen von VM-Vorgängen verwenden. Anweisungen zum Generieren eines Schlüssels finden Sie unter Einen SSH-Schlüssel erstellen.

So fügen Sie einem virtuellen Computer unter Windows Schlüsselanmeldeinformationen hinzu:

1. Wählen Sie die Windows-VM aus.
2. Wählen Sie in der Liste **Select Resource Operation** (Ressourcenvorgang auswählen) die Option **Virtual Machine Store Extension Interface.InfuseKey**(Store-Erweiterungsschnittstelle des virtuellen Computers.InfuseKey).
3. Geben Sie im Popup-Fenster den zu verwendenden Schlüssel im Feld **UserKey** (Benutzerschlüssel) an, und klicken Sie dann auf **OK**.

Store-Erweiterungsschnittstelle des virtuellen Computers.Execute Job Template

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ansible liefert den Vorgang *Execute Job Template* (Auftragsvorlage ausführen). Mit diesem Vorgang können Sie einen Knoten einem Ansible-Server beifügen und ein Paket für diese VME ausführen. Beispielsweise kann ein Skript eine Anwendung auf einer Ressource installieren. Geben Sie im Popup-Fenster Folgendes an:

WorkloadConfigProviderType	
WorkloadConfigProvider	
Inventar	
HostGroup	Die Liste umfass alle möglichen Anwendungen (in Ansible als Gruppen bezeichnet), nicht nur die Anwendungen, die der Konfigurationsmanagement-Anbieter unterstützt. Daher schlägt die Bereitstellung fehl, wenn Benutzer eine nicht unterstützte Anwendung auswählen.
ApplicationProfile	Wählen Sie das Anwendungsprofil aus, das für die ausgewählte Ressource ausgeführt werden soll.

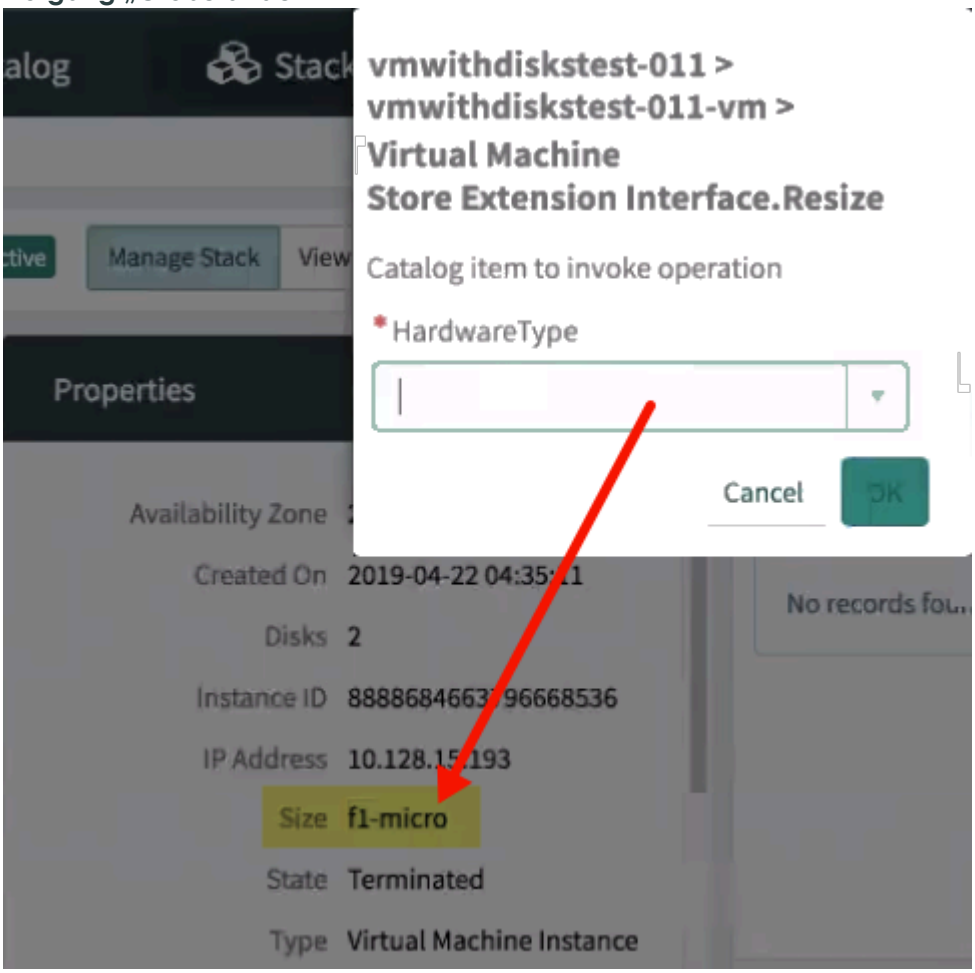
- **ScriptType**: Für Google Cloud Platform wird **Shell** unterstützt.
- **Script**: Name des Skripts.

Store-Erweiterungsschnittstelle des virtuellen Computers.Resize

Der Vorgang *Resize* (Größe ändern) ändert die Einstellung der **Größe** für einen virtuellen Computer (in der CI-Definition als **HardwareType** bezeichnet). Geben Sie im Popup-Fenster im Feld **HardwareType** die neue Größe an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorgang „Größe ändern“



Vorgänge des Typs „Compute-Sicherheitsgruppe – Store-Erweiterungsschnittstelle“

Die Vorgänge zur *Store-Erweiterungsschnittstelle der Compute-Sicherheitsgruppe* werden nur für IBM Cloud unterstützt. Die App Terraform ServiceNow Store stellt die Vorgänge bereit.

Compute-Sicherheitsgruppe – Store-Erweiterungsschnittstelle.Deprovision

Der Vorgang *Deprovision* (Aufheben der Bereitstellung) beendet die ausgewählte Compute-Sicherheitsgruppe und sendet eine Benachrichtigung an ihren Besitzer.

Keine Einstellung ist erforderlich.

Der **Status** der Netzwerkschnittstelle wechselt auf **Terminated** (Beendet). Im Abschnitt „Stack-Integrität“ der Homepage gibt der Status des Stapels an, dass einige Ressourcen nicht verfügbar sind.

Vorgänge des Typs „Lastenausgleichsmodul – Store-Erweiterungsschnittstelle“

Lastenausgleichsmodul – Store-Erweiterungsschnittstelle.Deprovision

Der Vorgang *Deprovision* (Aufheben der Bereitstellung) beendet das ausgewählte Lastenausgleichsmodul und sendet eine Benachrichtigung an den Stapelbesitzer.

Keine Einstellung ist erforderlich.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Der **Status** des Lastenausgleichsmoduls wechselt auf **Terminated** (Beendet). Im Abschnitt „Stack-Integrität“ der Homepage gibt der Status des Stapels an, dass einige Ressourcen nicht verfügbar sind.

Vorgänge des Typs „Netzwerk – Store-Erweiterungsschnittstelle“

Netzwerk – Store-Erweiterungsschnittstelle.Deprovision

Der Vorgang *Deprovision* (Aufheben der Bereitstellung) beendet das ausgewählte Netzwerk und sendet eine Benachrichtigung an den Stapelbesitzer.

Keine Einstellung ist erforderlich.

Der **Status** des Netzwerkspeichers wechselt auf **Terminated** (Beendet). Im Abschnitt „Stack-Integrität“ der Homepage gibt der Status des Stapels an, dass einige Ressourcen nicht verfügbar sind.

Vorgänge des Typs „Speicher-Laufwerk – Store-Erweiterungsschnittstelle“

Die Vorgänge zur *Store-Erweiterungsschnittstelle des Speicher-Laufwerks* werden nur für IBM Cloud unterstützt. Die App Terraform ServiceNow Store stellt die Vorgänge bereit.

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Create Snapshot

Der Vorgang *Create Snapshot* (Snapshot erstellen) generiert eine schreibgeschützte Kopie des angegebenen Laufwerks.

Legen Sie im Popup-Fenster den Parameter **SnapshotName** fest, der als Bezeichnung für den Snapshot verwendet werden soll.

Der Snapshot wird in der Tabelle [cmdbci.ci_storage_vol_snapshot_list] gespeichert.

Wenn keine Genehmigung erforderlich ist, erstellt das System den Snapshot sofort. Wenn eine Genehmigung erforderlich ist, kann es zu Verzögerungen kommen, bis ein Administrator die Änderung genehmigt. Sie erhalten eine E-Mail-Nachricht, wenn der Administrator die Genehmigung erteilt. Kehren Sie nach der Genehmigung durch den Administrator zum VM-Instanzformular zurück, und klicken Sie auf den zugehörigen Link **Proceed with Change** (Mit Änderung fortfahren).

Hinweis: Wenn die VM ausgeführt wird, wird die VM zu Beginn des Snapshot-Prozesses heruntergefahren und dann nach Abschluss des Prozesses neu gestartet. Das System löscht den ältesten Snapshot automatisch, wenn der Grenzwert der **Snapshot-Entfernungsrichtlinie** überschritten wird.

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Restore From Snapshot

Der Vorgang *Restore From Snapshot* (Aus Snapshot wiederherstellen) stellt das Bild aus dem angegebenen Snapshot wieder her.

Legen Sie den Parameter **SnapshotID** fest, der für die Wiederherstellung des Laufwerks verwendet werden soll.

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Delete Snapshot

Der Vorgang *Delete Snapshot* (Snapshot löschen) löscht den ausgewählten Snapshot.

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Attach

Der Vorgang *Attach* (Anfügen) fügt eine VM an das ausgewählte Laufwerk an.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

1. Wählen Sie das Laufwerk aus, dem etwas angehängt werden soll. Der **Status** des Laufwerks muss **Available** (Verfügbar) sein.
2. Wählen Sie den Vorgang **Storage Volume Store Extension Interface.Attach** (Speicher-Laufwerk –Store-Erweiterungsschnittstelle.Attach).
3. Wählen Sie im Popup-Fenster im Feld **NodeId** die **Instanz-ID** des Servers aus, der an das Laufwerk angefügt werden soll.

   Der Status des Laufwerks ändert sich von „Available“ (Verfügbar) in „In Use“ (In Verwendung).

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Detach

Der Vorgang `Detach` (Trennen) trennt eine VM vom ausgewählten Laufwerk.

1. Wählen Sie das Laufwerk aus, dem etwas angehängt werden soll. Der Status des Laufwerks muss „In Use“ (In Verwendung) sein.
2. Wählen Sie den Vorgang **Storage Volume Store Extension Interface.Detach** (Speicher-Laufwerk –Store-Erweiterungsschnittstelle.Detach).
3. Wählen Sie im Popup-Fenster im Feld **NodeId** die **Instanz-ID** des Hosts aus, der vom Laufwerk getrennt werden soll.

   Wenn diese VM die letzte oder einzige zu trennende VM ist, ändert sich der Status des Laufwerks von „In Use“ (In Verwendung) in „Available“ (Verfügbar).

Speicher-Laufwerk – Store-Erweiterungsschnittstelle.Deprovision

Der Vorgang `Deprovision` (Aufheben der Bereitstellung) beendet das ausgewählten Laufwerk und sendet eine Benachrichtigung an den Stapelbesitzer.

Keine Einstellung ist erforderlich.

- Das Abrechnungselement für die Speicherressource wird entfernt.
- Der **Status** des Laufwerks wechselt auf **Terminated** (Beendet). Im Abschnitt „Stack-Integrität“ der Homepage gibt der Status des Stapels an, dass einige Ressourcen nicht verfügbar sind.
- Für IBM Cloud: Das Speicher-Laufwerk ist für längere Zeit in IBM Cloud-Konsole verfügbar, damit der Benutzer es zurückfordern kann.

Übermitteln eines Incidents für einen Stapel

Senden Sie einen Incident für einen Stapel, wenn dieser nicht wie erwartet funktioniert oder Sie Fragen haben. Wenn der Benutzer antwortet oder das Problem behebt, wird der Incident geschlossen.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird

Sie können einen Incident für einen Stapel oder für eine einzelne Ressource übermitteln. Sie können Incident erstellen auch über die Incident-Anwendung ausführen. Stellen Sie sicher, dass das Feld **Category** auf den Wert Cloud Provisioning and Governance festgelegt ist. Das Configuration Item muss der Stapelname sein, für den der Incident ausgelöst werden soll, und der Name des Anrufers muss der Name der Person sein, für die der Incident erstellt wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Sie können die Seite mit Stapeldetails mit einer der folgenden Methoden anzeigen:

- Klicken Sie auf der Seite **Stack Details** (Stapeldetails) auf die Registerkarte **Incidents** im Abschnitt **Activities** (Aktivitäten).
- Klicken Sie auf der Seite **„Aktivitäten“** auf **Titel** > **Incidents**.

Der Abschnitt **Activities** (Aktivitäten) listet alle übermittelten Incidents für den Stapel auf.

Incidents	
Activities → Incidents (Aktivitäten → Incidents)	Lassen Sie Incidents aller Typen für jeden Stapel oder jede Ressource anzeigen, und übermitteln Sie sie.
Stacks → Stack Details → Incidents (Stapel → Stapeldetails → Incidents)	Lassen Sie Incidents für den ausgewählten Stapel anzeigen, und übermitteln Sie sie.
Resources → Resource Details → Incidents (Ressourcen → Ressourcendetails → Incidents)	Lassen Sie Incidents für die ausgewählte Ressource anzeigen, und übermitteln Sie sie.

2. Klicken Sie auf **New Incident** (Neuer Incident) und füllen Sie das Formular aus:

Incident Type (Incident-Typ)	Der Typ, der Ihren Bedürfnissen am ehesten entspricht.
Stack / Resource (Stapel/Ressource) [zusammenhängende Felder]	Stapel und Ressource, für die der Incident gilt. ◦ Wählen Sie auf der Seite **Activities** (Aktivitäten) den **Stapel** aus der Liste der aktiven Stapel aus. Lassen Sie das Feld **Resource** (Ressource) leer, wenn das Problem keiner konkreten Ressource zugeordnet ist. ◦ Auf der Seite **Stack Details** (Stapeldetails) ist der Wert für **Stapel** der aktuelle Stapel. ◦ Auf der Seite **Resources** (Ressourcen) ist der Wert **Resource** (Ressource) die aktuelle Ressource.
Das Problem beschreiben	Beschreiben Sie das aufgetretene Problem, oder geben Sie eine Frage ein. Geben Sie vollständige Informationen zum Verhalten an, das das Problem darstellt.
Was sind die Auswirkungen auf das Geschäft?	Geben Sie an, wie sich der Incident auf Ihre Arbeit und die Arbeit anderer, einschließlich Ihrer Kunden, auswirkt.
Fügen Sie Screenshots, Protokolle usw. an.	Durch Klicken oder Ablegen von Dateien können Problem bzw. Frage besser erläutert werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

3. Klicken Sie auf **Absenden**.
   Das System generiert den Incident. Die Registerkarte **Incidents** auf der Seite **Activities** (Aktivitäten) zeigt eine Zusammenfassung an.

Nächste Maßnahme

Um eine Liste aller übermittelten Incidents anzuzeigen, navigieren Sie zu **Aktivitäten** > **Incidents**.

Seite „Activities“ (Aktivitäten) verwenden

Über die Seite „Activities“ (Aktivitäten) können Sie Details Ihrer Cloud-Aktionen anzeigen lassen und verwalten.

Titel	
Anforderungen	Ihre Anforderungen für Katalogelemente (Stapel). Weitere Informationen finden Sie unter Eine Stapel-Anforderung nachverfolgen.
Change-Anforderungen	Change-Anforderungen, die für Stapel oder Ressourcen eingereicht wurden, die Ihnen zugewiesen sind. Das System generiert Change-Anforderungen, wenn Sie Lebenszyklusvorgänge für einen Stapel oder eine Ressource ausführen. Siehe Change-Anforderungen nachverfolgen und Einen Lebenszyklusvorgang für einen Stapel oder eine Ressource durchführen.
Incidents	Incidents für Stapel und die zugehörigen Ressourcen, die Ihnen zugewiesen sind. Weitere Informationen finden Sie unter Incidents nachverfolgen.
Aufgaben	Katalogaufgaben, die erstellt werden, wenn die Bereitstellung einer Anforderung für einen Stapel fehlschlägt. Weitere Informationen finden Sie unter Eine fehlgeschlagene Stapel-Anforderung erneut übermitteln.
Leasingvorgänge	Lassen Sie eine Liste aller Ihrer Stapel anzeigen, deren Mietenddatum in Kürze ansteht. Sie können das Enddatum einer Miete für alle aufgeführten Stapel verlängern. Weitere Informationen finden Sie unter Die Miete für einen Stapel ändern.
Geschäftsszeitplanvorgänge	Lassen Sie eine Liste aller in Kürze bevorstehenden Vorgängerschaftsrelation anzeigen, die den Stapeln zugewiesen sind. Sie können einen bevorstehenden Vorgang überspringen oder einen einem konkreten Stapel zugeordneten Zeitplan abbrechen. Weitere Informationen finden Sie unter Geschäftszeitplanvorgänge für einen Stapel ändern.
Überwachen	
Cloud-Events	Liste der Lebenszyklus-Events, die sich auf Ressourcen auswirken, die Ihnen oder einem Benutzer in Ihrer Gruppe

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

	zugewiesen sind. Weitere Informationen finden Sie unter Cloud-Events anzeigen.
Verwalten	
Keys	Lassen Sie vorhandene SSH-Schlüssel anzeigen, die Ihnen zugewiesen sind, oder generieren Sie einen Schlüssel. Weitere Informationen finden Sie unter Einen SSH-Schlüssel erstellen.

Change-Anforderungen nachverfolgen

Das System generiert Change-Anforderungen wenn Sie Lebenszyklusvorgänge für einen Stapel oder eine Ressource ausführen.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird
Jede Change-Anforderung wird entweder standardmäßig genehmigt oder, wenn eine Genehmigungsrichtlinie vorhanden ist, von einem Benutzer genehmigt, der auf der Genehmigerliste steht.

Prozedur

1. Wechseln Sie zur Seite **Aktivitäten**, oder navigieren Sie zu **Cloud-Anwenderportal** > **Aktivitäten anzeigen**, und wählen Sie dann aus **Titel** > **Change-Anforderungen**.

Nummer	Eindeutige automatisch generierte Nummer.
Konfigurationselement	Das betroffene CI.
Kategorie	Cloud Provisioning and Governance
Kurzbeschreibung	Text, der vom Anforderer eingegeben wurde.
Genehmigung	Status.

2. Klicken Sie in der Liste der **Change-Anforderungen** auf einen Eintrag, um alle Details aufzurufen.

Incidents nachverfolgen

Bevor ein Incident gelöst und geschlossen wird, können Sie den Status des Incidents anzeigen lassen.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Sie öffnen die Incidents-Seite mit einer der folgenden Methoden:
   - Klicken Sie auf der Seite **„Aktivitäten“** auf **Titel** > **Incidents**.
   - Klicken Sie auf der Seite **Stack Details** (Stapeldetails) auf die Registerkarte **Incidents** im Abschnitt **Activities** (Aktivitäten).

   Der Abschnitt **Activities** (Aktivitäten) listet alle übermittelten Incidents für den Stapel auf.
2. Klicken Sie in der Liste der **Incidents** auf einen Eintrag, um alle Details aufzurufen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Nummer	Eindeutige automatisch generierte Nummer.
Kategorie	Cloud Provisioning and Governance.
Unterkategorie	◦ Leistungsproblem: Das Problem ist der Vorgangsleistung zugeordnet. ◦ Anforderung: Anforderung eines Change.
Kurzbeschreibung	Text, den der Übermittler des Incidents eingegeben hat.
Konfigurationselement	CI der Ressource für den Incident.
Auswirkung	◦ Dringlichkeit, wie folgt bewertet: ◦ **1 - Hoch** ◦ **2 - Mittel** ◦ **3 - Niedrig**
Status	◦ **New** (Neu): kürzlich erstellter Incident. ◦ **Closed** (Geschlossen): Der Benutzer im Feld **Assigned to** (Zugewiesen an) hat auf das Problem reagiert oder es gelöst und den Incident als geschlossen markiert. ◦ **Abgebrochen**: Der Benutzer unter „Zugewiesen an“ hat das Problem geprüft, keine Maßnahmen ergriffen und den Incident abgebrochen.
Zugewiesen an	Der Benutzer, der auf den Incident reagieren muss.

Cloud-Events anzeigen

Wenn Ihr Administrator Cloud Provisioning and Governance so konfiguriert hat, dass Events überwacht werden, können Sie die aus Ihren Cloud-Ressourcen generierten Events anzeigen. Alle Events werden auf der Registerkarte „Cloud-Events“ auf der Stapeldetailseite aufgelistet.

Vorbereitungen

Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Sie öffnen die Cloud-Events-Seite mit einer der folgenden Methoden:
   - Klicken Sie auf der Seite **„Aktivitäten“** auf **Überwachen** > **Cloud-Ereignisse**.
   - Auf der Seite **Stack-Details** klicken Sie auf die Registerkarte **Cloud-Ereignisse** im Abschnitt **Aktivitäten**.

   Im Abschnitt **Cloud Events** werden alle Events für den Stapel aufgelistet.

Erstellt	Zeitstempel des Eintritts des Events.
Quelle	Quelle des Events: ◦ **azure**: Azure-Warnung ◦ **aws**: AWS-Konfig ◦ **vmware**: VMware-Events

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Event-Name	Name, der von Amazon, Azure oder VMware bereitgestellt wird.
Betreff	Text, der das Event beschreibt.
Event-Zeit	Zeitstempel des Events.
Ressourcen-ID	Eindeutige ID der Ressource, die das Event zum Lebenszyklusstatus oder zur Konfigurationsänderung empfangen hat.

2. Klicken Sie auf einen Eintrag, um die vollständigen Details anzeigen zu lassen.

Einen SSH-Schlüssel erstellen

Ein Stapel kann einen virtuellen Computer enthalten, der einen SSH-Schlüssel für den Zugriff erfordert. Zum Anfordern eines solchen Stapels können Sie entweder ein Ihnen zugewiesenes Schlüsselpaar verwenden oder einen anderen Schlüssel generieren.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Klicken Sie unter Cloudbenutzerportal auf **Activities** (Aktivitäten).
2. Wählen Sie in der Liste **Aktivitäten** die Option aus **Verwalten** > **Keys**.
3. Klicken Sie auf der Seite **SSH Key Pair** (SSH-Schlüsselpaar) auf **Generate Key Pair** (Schlüsselpaar generieren), geben Sie einen **Namen** für den Schlüssel an, und klicken Sie dann auf **OK**.

Ergebnisse
Das System erzeugt das Schlüsselpaar mit dem **Namen**, den Sie angegeben haben.

Einen SSH-Schlüssel herunterladen

Wenn für eine Ressource auf einem Stapel eine Anmeldung erforderlich ist, müssen Sie den zugehörigen SSH-Schlüssel herunterladen, bevor Sie auf die Ressource zugreifen können.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Prozedur

1. Klicken Sie im **Cloud-Benutzerportal** auf **Activities** (Aktivitäten).
2. Wählen Sie in der Liste **Aktivitäten** die Option aus **Verwalten** > **Keys**.
3. Klicken Sie in der Liste **SSH Key Pair** (SSH-Schlüsselpaar) auf einen Schlüssel und dann auf **Download Private Key** (Privaten Schlüssel herunterladen) im Abschnitt **SSH Private Key** (Privater SSH-Schlüssel).

Geschäftszeitpläne

Sie können auf allen virtuellen Computern in einem Stapel Geschäftszeitpläne einrichten. Geschäftszeitpläne können für Stapel zum Zeitpunkt der Bereitstellung oder für bereits vorhandene Stapel eingerichtet werden.

Zeitpläne können dafür festgelegt werden, wann ein Stapel gestartet, gestoppt und/oder seine Bereitstellung aufgehoben werden soll, indem Parameter wie Geschäftszeiten, Feiertage oder lange Wochenenden definiert werden.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: Für den auf Google Deployment Manager (GDM) basierenden Vorlagenkatalog werden die Planung von Geschäftszeiten und Vorgänge auf Stapelebene nicht unterstützt.

Der Administrator kann Zeitplanprofile im **Cloud Admin Portal** (Cloudverwaltungsportal) erstellen. Weitere Informationen finden Sie unter Ressourcenprofile.

Wählen Sie bei der Bereitstellung eines Stapels im Cloud-Benutzerportal mithilfe der Liste **Schedule Profile** (Zeitplanprofil) ein Profil aus, das bereits vom Administrator erstellt wurde. Wählen Sie in der Liste **Zeitzone des Zeitplans** eine Zeitzone aus, die standardmäßig der Zeitzone Ihres Systems entspricht und die Zeitzone angibt, in der die Geschäftszeiten des Zeitplans umgesetzt werden.

Sie können während der Bereitstellung auch den Mietendzeitpunkt für einen Stapel definieren. Der Mietendzeitpunkt für einen Stapel kann jederzeit geändert werden. Weitere Informationen finden Sie unter Die Miete für einen Stapel ändern.

Sobald Sie einen Stapel mit einem Zeitplan und/oder Mietzeitpunkten bereitgestellt haben, erfolgt eine Reihe von Vorgängen (Start, Stopp, Aufhebung der Bereitstellung) zum von Ihnen festgelegten Zeitpunkt. Sie können einen Geschäftszeitplanvorgang überspringen oder die einem Zeitplan zugeordneten Geschäftszeitplanvorgänge abbrechen. Weitere Informationen finden Sie unter Geschäftszeitplanvorgänge für einen Stapel ändern.

Die Miete für einen Stapel ändern

Wenn ein Stapel das Ende seiner Miete erreicht, benachrichtigt das System den Stapel-Besitzer und hebt die Stapel-Bereitstellung auf. Sie können die Miete für einen Stapel ändern, bevor das Enddatum erreicht ist.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird
Allen bereitgestellten Stapeln wird ein Mietendzeitpunkt zugewiesen. Eine integrierte Richtlinie mit dem Titel *Lease End ServiceNow* mit einem Richtlinienauslöser *on Lease end* weist Regeln auf, die Benachrichtigungen und Vorgänge definieren, die vor dem Enddatum der Miete, währenddessen und danach ausgeführt werden. Mietzeitpunkte können für aktive Stapel geändert werden. Das System sendet einen Tag vor Ende des Mietzeitraums eine Benachrichtigung an den Stapel-Besitzer. Am Tag, an dem die Miete endet, stoppt das System den Stapel und sendet eine weitere Benachrichtigung. Sieben Tage nach Ende der Miete wird der Stapel beendet und eine endgültige Benachrichtigung an den Stapel-Besitzer gesendet. Sie können die durchgeführten Aktionen und die Zeitpläne dieser Aktionen ändern, indem Sie die Richtlinie *Lease End ServiceNow* ändern. Sie können die Standardmietdauer für alle neuen Stapel ändern, indem Sie das zugehörige Aktionsskript in der integrierten Richtlinie *Scheduling Defaults* ändern.

Prozedur
1. Navigieren zu **Alle** > **Übersicht** > **Aktivitäten anzeigen**, und wählen Sie dann aus **Leasingvorgänge**.
   Eine Liste von Stapeln mit bevorstehenden Mietvorgängen wird angezeigt.
2. Klicken Sie auf die dem Stapel zugeordnete Liste **Select Action** (Aktion auswählen), und wählen Sie dann **Modify Lease** (Miete ändern).
   Die Option **Modify Lease** (Miete ändern) ist auch in der Liste der Stapeldetails unter **Stapel verwalten** verfügbar.
3. Legen Sie ein neues Datum und eine neue Uhrzeit für den Ablauf der Miete fest, und klicken Sie dann auf **OK**.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Geschäftszeitplanvorgänge für einen Stapel ändern

Geschäftszeitpläne können für Stapel zum Zeitpunkt der Bereitstellung oder für bereits vorhandene Stapel eingerichtet werden.

Vorbereitungen
Erfordert Rolle: sn_cmp.cloud_service_user

Warum und wann dieser Vorgang ausgeführt wird
Sobald ein Stapel mit einem Geschäftszeitplan eingerichtet wurde, generiert das System eine Reihe von Aufgaben zum Starten und Beenden des Stapels. Sie können diese Aufgaben anzeigen lassen und den Geschäftszeitplan für jeden Stapel ändern.

Prozedur

1. Navigieren zu **Alle** > **Übersicht** > **Aktivitäten anzeigen**, und wählen Sie dann aus **Geschäftsszeitplanvorgänge**.
   Eine Liste von Stapeln mit bevorstehenden Geschäftszeitplanvorgängen wird angezeigt.
2. Führen Sie in der dem Stapel zugeordneten Liste **Aktion auswählen** einen der beiden folgenden Vorgänge aus:
   - **Skip Operation** (Vorgang überspringen) – Klicken Sie hier, um einen einzelnen Geschäftszeitplanvorgang auf einem Stapel zu überspringen. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **OK**.
   - **Cancel Schedule** (Zeitplan abbrechen) – Klicken Sie hier, um die Geschäftszeitplanung auf einem Stapel abzubrechen. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **OK**.

   Wenn Sie den Zeitplan eines bestehenden Stapels ändern möchten, navigieren Sie zur Stapeldetailliste unter **Stapel verwalten** und wählen Sie **Modify Schedule** (Zeitplan ändern) aus der Liste **Stapelvorgang auswählen**.

Verwalten persönlicher Ressourcen und Gruppenressourcen

Sie können Ihre Ressourcen aufrufen und verwalten sowie die Ressourcen, die der Gruppe zugewiesen sind, der Sie angehören. Wenn Sie mehreren Gruppen angehören, können Sie alle diesen Gruppen zugewiesenen Ressourcen anzeigen lassen und verwalten.

Vorbereitungen
Erforderliche Rolle: Root-Administrator [sn_cmp.cmp_root_admin] und Systemadministrator [admin].

Warum und wann dieser Vorgang ausgeführt wird
Nur ein Stammadministrator und ein Systemadministrator haben Zugriff auf alle drei Filter: **Mining**, **Meine Gruppen**und **Alle**.

Prozedur

1. Wählen Sie unter Cloudbenutzerportalden Filter **Ansichten** auf der rechten Seite im Banner aus.
2. Wählen Sie eine Option aus:
   - **Mine** (Meine): Nur Ressourcen anzeigen und verwalten, die Ihnen zugewiesen sind.
   - **My Groups** (Meine Gruppen): Lassen Sie alle Ressourcen anzeigen, die Ihnen und allen Mitgliedern aller Gruppen, denen Sie angehören, zugewiesen sind, und verwalten Sie sie.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

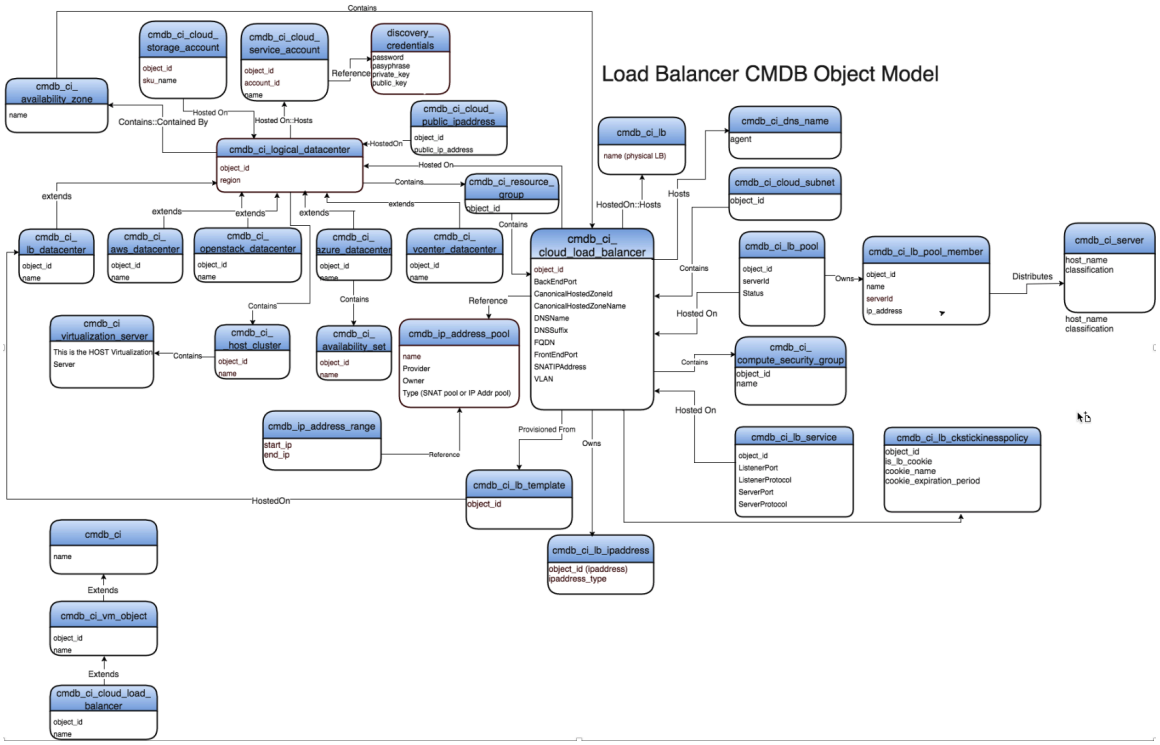
Schemata von Cloud Provisioning and Governance-Tabellen

Die Tabellen sind cloudagnostisch und können daher Daten für jeden Cloud-Anbieter enthalten.

Ressourcentabelle Lastenausgleich

Die Lastenausgleichstabelle [cmdb_ci_cloud_load_balancer] baut auf [cmdb_ci_vm_object auf], was auf [cmdb_ci] aufbaut. Klicken Sie, um das Bild zu vergrößern.

Schema-Lastenausgleichsmodul



Wichtige native Attribute der Tabelle „cmdb_ci_cloud_load_balancer“

Attribut	Beschreibung
object_id	Bezeichner, der normalerweise den Namen des Lastenausgleichsmoduls als Wert enthält.
canonical_hosted_zone_id	ID der von Amazon Route 53 gehosteten Zone für das Lastenausgleichsmodul.
canonical_hosted_zone_name	DNS-Name des Lastenausgleichmoduls.
dns_name	Öffentlicher DNS-Name des Lastenausgleichmoduls.
fqdn	DNS-Name als vollqualifizierter Domänenname. Kann auch ein CNAME-Datensatz sein, der auf den DNS-Namen verweist.
state	Status des Lastenausgleichmoduls: **available** (verfügbar) oder **terminated** (beendet).

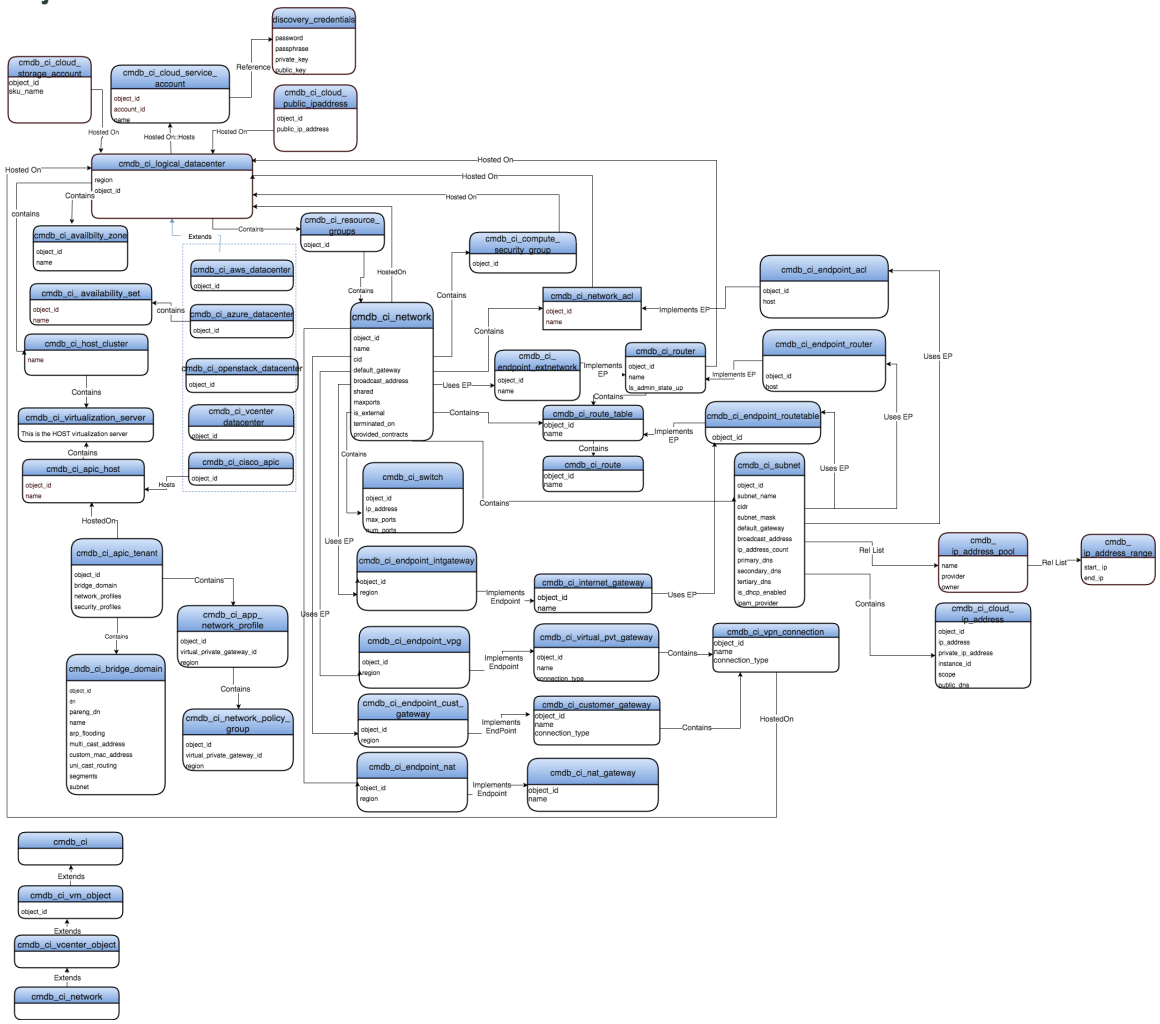
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Netzwerkressourcentabelle

Die Netzwerkressourcentabelle [cmdb_ci_network] baut auf [cmdb_ci_vcenter_object] auf, was auf [cmdb_ci_vm_object] aufbaut, und dies wiederum auf [cmdb_ci]. Klicken Sie, um das Bild zu vergrößern.

Objektmodell – Netzwerktabelle



Wichtige native Attribute der Tabelle „cmdb_ci_network“

Attribut	Beschreibung
object_id	Bezeichner, der normalerweise die Netzwerk-ID als Wert enthält. Bezeichnet eindeutig ein Objekt innerhalb einer Cloud.
name	Name des Netzwerks.
cidr	IP-Adressbereich. Klassenloses Inter-Domain-Routing setzt sich aus einer Reihe von Internetprotokollstandards zusammen, die zum Erstellen eindeutiger Bezeichner für Netzwerke verwendet werden.
default_gateway	Enthält InternetGatewayID, wenn IntenetGateway an das Netzwerk angefügt wird. Ein Standardgateway dient als Zugangspunkt oder IP-Router, über den ein vernetzter Computer Informationen an einen Computer in einem anderen Netzwerk oder Internet sendet. Das angegebene Gateway

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Wichtige native Attribute der Tabelle „cmdb_ci_network“ (Fortsetzung)

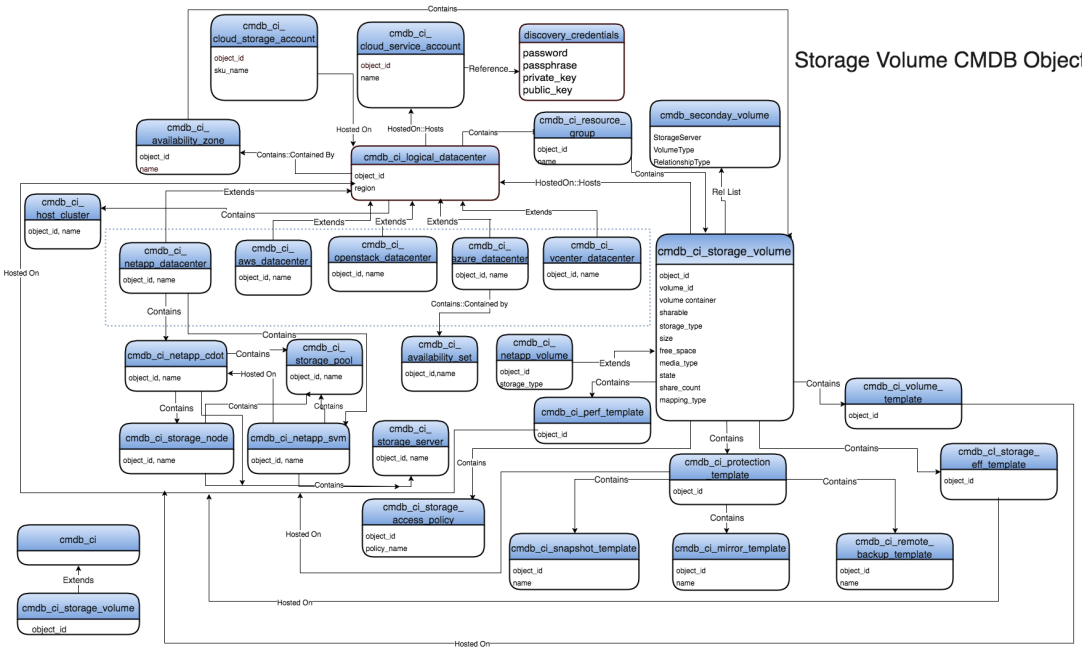
Attribut	Beschreibung
	wird standardmäßig verwendet, es sei denn, eine Anwendung gibt ein anderes Gateway an.
Broadcast_address	IP-Adresse, die zur Übertragung von Nachrichten und Datenpaketen an Netzwerksysteme verwendet wird.
Is_shared	Boolescher Wert. „true“: Netzwerk, das von anderen Projekten gemeinsam verwendet wird. false: Netzwerk, das nicht von anderen Projekten verwendet wird.
max_ports	Maximale Anzahl von Hosts, die mit dem Netzwerk verbunden werden können
is_external	Boolescher Wert. „true“: Netzwerk ist extern. „false“: Netzwerk ist intern.
terminated_on	Zeit, zu der die Bereitstellung des Netzwerks aufgehoben wurde.
state	Status des Netzwerks: **available** (verfügbar) oder **terminated** (beendet).
netmask	CIDR-Typ. 32-Bit-Maske, die eine IP-Adresse in Subnetze unterteilt und die im Netzwerk verfügbaren Hosts angibt.
dhcp_enabled	Boolescher Wert: „true“: Dynamische IP-Adresse wird dem Host zugewiesen „false“: Statische IP-Adresse wird dem Host zugewiesen

Speicher-Laufwerk-Ressourcentabelle

Die Ressourcentabelle [cmdb_ci_storage_volume] des Speicher-Laufwerks baut auf [cmdb_ci] auf. Klicken Sie, um das Bild zu vergrößern.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schemaspeicher-Volume



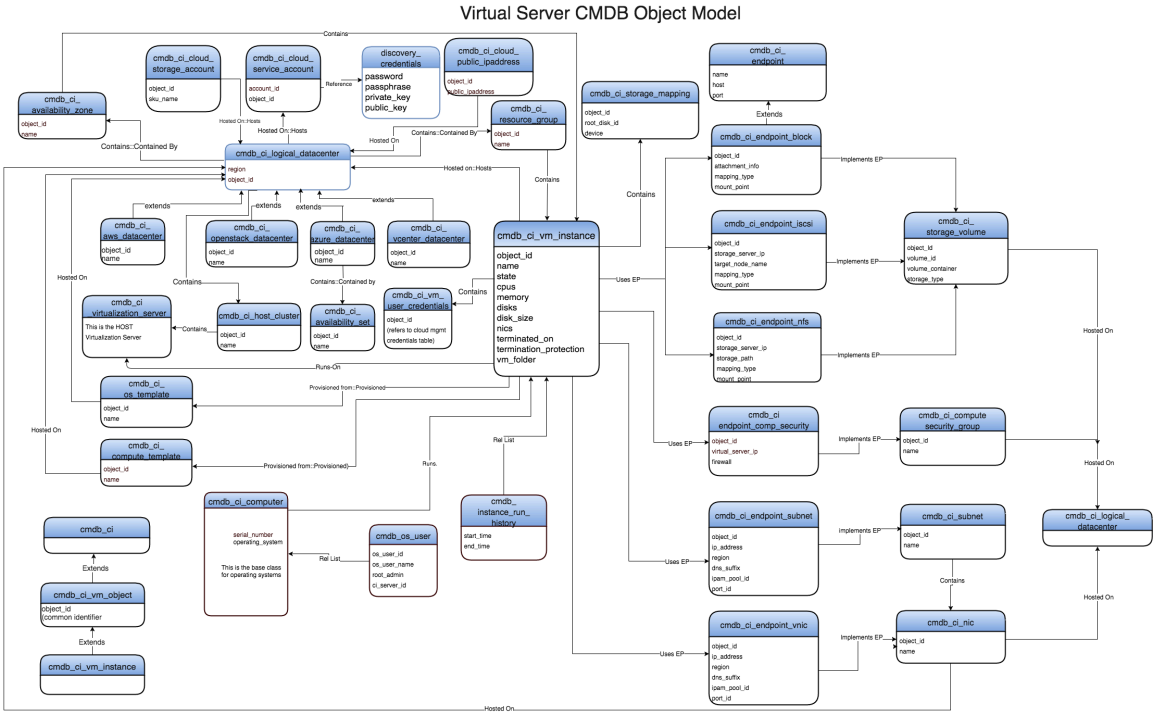
Wichtige native Attribute der Tabelle „cmdb_ci_storage_volume“

Attribut	Beschreibung
object_id	Bezeichner, der üblicherweise die Objekt-ID als Wert enthält. Bezeichnet eindeutig ein Objekt innerhalb einer Cloud.
volume_id	Bezeichner, der üblicherweise die Laufwerk-ID als Wert enthält. Bezeichnet eindeutig ein Objekt innerhalb einer Cloud.
volume_container	Nur für NetApp wird LUN zum Laufwerk und NetApp Volume wird zum Laufwerk-Container.
sharable	Boolescher Wert. „true“: Laufwerk wird von mehreren VMs gemeinsam verwendet. „false“: Laufwerk wird nicht von mehreren VMs gemeinsam verwendet.
storage_type	Typ des Speichers. • AWS: Block • Azure: PageBlob • vSphere: VMware vdisk
size	Gesamtkapazität des Laufwerks.
free_space	Verfügbarer Speicherplatz des Laufwerks
state	Status des Volumes: **available** (verfügbar) oder **in_use** (in Verwendung).
share_count	Anzahl der VMs, die vom Volume gemeinsam verwendet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Ressourcentabelle des virtuellen Servers

Die Ressourcentabelle des virtuellen Servers [cmdb_ci_vm_instance] baut auf [cmdb_ci_vm_object], was auf [cmdb_ci] aufbaut. Klicken Sie, um das Bild zu vergrößern.



Wichtige native Attribute der Tabelle „cmdb_ci_vm_instance“

Attribut	Beschreibung
object_id	Bezeichner, der normalerweise die ID der VM-Instanz enthält. Bezeichnet eindeutig ein Objekt innerhalb einer Cloud.
name	Name der VM
state	Status der VML: **on** (ein), **off** (aus) oder **terminated** (beendet).
cpus	Anzahl an CPUs
memory	Speichergröße in Megabyte
disks	Anzahl der Laufwerke
disk_size	Gesamtgröße der Datenträger in Gigabyte
nics	Anzahl der Netzwerkadapter
terminated_on	Zeit, zu der die Instanz beendet wurde.
termination_protection	Boolescher Wert. Der Standardwert ist „false“. „true“: Kann verhindern, dass die Instanz versehentlich mit Amazon EC2 beendet wird. „false“: Kann nicht verhindern, dass die Instanz versehentlich mit Amazon EC2 beendet wird.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Schnellstarttests für Cloud Provisioning and Governance

Überprüfen Sie, ob Cloud Provisioning and Governance noch funktioniert, nachdem Sie eine Konfigurationsänderung vorgenommen haben, z. B. das Anwenden eines Upgrades oder die Entwicklung einer Anwendung. Kopieren Sie diese Schnellstarttests und passen Sie sie an, um sie bei der Verwendung Ihrer instanzspezifischen Daten zu übergeben.

Cloud Provisioning and Governance

Cloud Provisioning and Governance-Schnellstarttests erfordern die Aktivierung der folgenden Cloud Provisioning and Governance-Plugins:

- Cloud Provisioning and Governance (com.snc.cloud.mgmt)
- Plugin „Domain Support – Domain Extensions Installer“ (com.glide.domain.msp_extensions.installer)
- Plugin „Servicekatalog – Domain Separation“ (glideapp.servicecatalog.domain_separation)

Cloud Provisioning and Governance: Azure-Test-Suite

Test	Beschreibung	Release-Version
CMP: Azure-Anmeldeinformationen hinzufügen	Fügt Azure-Anmeldeinformationen hinzu, indem die Felder in die Tabelle „Anmeldeinformationen“ eingefügt werden.	Orlando
CMP: Azure-Serviceaccount	Fügt einen Azure-Serviceaccount hinzu, indem die Felder in die Tabelle „Service-Account“ eingefügt werden.	Orlando
CMP: Rechenzentrumstyp aktualisieren	Aktualisiert das Cloud-Servicekonto mit dem Rechenzentrumstyp.	Orlando
CMP: Ressourcengruppe erstellen	Erstellt eine Ressourcengruppe zum Bereitstellen des Azure-Stack über eine ARM-Vorlage.	Orlando
CMP: Logisches Azure-Rechenzentrum erstellen	Erstellt ein logisches Azure-Rechenzentrum für die Bereitstellung von Ressourcen.	Orlando
CMP: „Contains: Contained by“-Beziehung erstellen	Erstellt eine „Contains: Contained by“-Beziehung zwischen Ressourcengruppe und Azure-Rechenzentrum.	Orlando
CMP: „Gehostet auf“-Beziehung erstellen	Erstellt eine „gehostet auf“-Beziehung zwischen logischem Rechenzentrum und Cloud-Serviceaccount.	Orlando

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance: Azure-Test-Suite (Fortsetzung)

Test	Beschreibung	Release-Version
CMP: Cloudaccount erstellen	Erstellt einen Cloudaccount, indem die Felder in die Cloudaccount-Tabelle eingefügt werden.	Orlando
CMP: Zuordnung zwischen Cloudaccount und logischem Rechenzentrum	Erstellt eine Zuordnung zwischen CMP-Cloud-Konto und logischem Rechenzentrum.	Orlando
CMP: Katalogelement erstellen	Erstellt ein Cloud-Katalogelement mit der ARM-Vorlage.	Orlando
CMP: Vorlagenversion erstellen	Erstellt eine Cloud-Vorlagenversion für das Cloud-Katalogelement.	Orlando
CMP: ARM-Vorlagentext	Aktualisiert die Cloud-Vorlagenversionen mit dem ARM-Vorlagentext.	Orlando
CMP: „ServiceNow-Cloud-Vorlagenversionen“ öffnen	Öffnet die GUI-Seite „ServiceNow-Cloud-Vorlagenversionen“.	Orlando
CMP: Cloud-Vorlagenversion aktivieren	Aktiviert die Cloud-Vorlagenversion, um Ressourcenblock, Blueprint und Katalog zu erstellen.	Orlando
CMP: Cloud-Vorlagenversion überprüfen	Validiert, ob der Status „Erfolg“ lautet und ob der Status in der Cloud-Vorlagenversionen nach dem Aktivierungsvorgang aktiv ist.	Orlando
CMP: Cloud-Katalogelement aktivieren	Aktiviert das Cloud-Katalogelement, um dem Cloud-Benutzer das Katalogbestellformular anzuzeigen.	Orlando
CMP: Stapel- und Ressourcengruppennamen in Katalogelement hinzufügen	Legt den Standardwert für Stapelnamen und Ressourcengruppe im Katalogelement fest.	Orlando
CMP: Überprüfen, ob Stapel vorhanden ist	Validiert, ob der Stapel mit dem Namen „ATFARMStack“ verfügbar ist.	Orlando
CMP: Cloud-Katalogelement-Seite öffnen	Öffnet die Seite „Cloud-Katalogelement“ im Serviceportal.	Orlando

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance: Azure-Test-Suite (Fortsetzung)

Test	Beschreibung	Release-Version
CMP: Katalogformular absenden	Sendet das Katalogformular, um die Bereitstellung des ARM-Stacks zu starten.	Orlando
CMP: Überprüfen, oder der Stapelstatus aktiv ist	Validiert den Status eines Stapels nach der Bereitstellung des Stapels.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang stoppen	Validiert, dass sich der Status des Stapels nach dem Stoppvorgang von „Ein“ in „Aus“ geändert hat.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang starten	Validiert, dass sich der Status des Stapels nach dem Startvorgang von „Aus“ in „Ein“ geändert hat.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang „Aufheben der Bereitstellung“	Validiert, dass sich der Stapelstatus nach dem Vorgang „Aufheben der Bereitstellung“ von „Aus“ in „Beenden“ geändert hat.	Orlando

Cloud Provisioning and Governance: AWS-Test-Suite

Test	Beschreibung	Release-Version
CMP: AWS-Anmeldeinformationen hinzufügen	Fügt AWS-Anmeldeinformationen hinzu, indem die Felder in die Tabelle „Anmeldeinformationen“ eingefügt werden.	Orlando
CMP: Serviceaccount für AWS	Fügt einen Serviceaccount für AWS hinzu, indem die Felder in die Tabelle „Servicekonto“ eingefügt werden.	Orlando
CMP: Rechenzentrumstyp aktualisieren	Aktualisiert das Cloud-Servicekonto mit dem Rechenzentrumstyp.	Orlando
CMP: Logisches Rechenzentrum erstellen	Erstellt ein logisches Rechenzentrum für die Bereitstellung von Ressourcen.	Orlando
CMP: „Gehostet auf“-Beziehung erstellen	Erstellt eine „gehostet auf“-Beziehung zwischen logischem Rechenzentrum und Cloud-Serviceaccount.	Orlando

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance: AWS-Test-Suite (Fortsetzung)

Test	Beschreibung	Release-Version
CMP: Cloudaccount erstellen	Erstellt einen Cloudaccount, indem die Felder in die Cloudaccount-Tabelle eingefügt werden.	Orlando
CMP: Zuordnung zwischen Cloudaccount und logischem Rechenzentrum	Erstellt eine Zuordnung zwischen CMP-Cloud-Konto und logischem Rechenzentrum.	Orlando
CMP: Katalogelement erstellen	Erstellt ein Cloud-Katalogelement mit der CFT-Vorlage.	Orlando
CMP: Vorlagenversion erstellen	Erstellt eine Cloud-Vorlagenversion für das Cloud-Katalogelement.	Orlando
CMP: CFT-Vorlagentext	Aktualisiert die Cloud-Vorlagenversionen mit dem CFT-Vorlagentext.	Orlando
CMP: ServiceNow-Cloud-Vorlagenversionen öffnen	Öffnet die GUI-Seite „ServiceNow-Cloud-Vorlagenversionen“.	Orlando
CMP: Cloud-Vorlagenversion aktivieren	Aktiviert die Cloud-Vorlagenversion, um Ressourcenblock, Blueprint und Katalog zu erstellen.	Orlando
CMP: Cloud-Vorlagenversion überprüfen	Validiert, ob der Status der Cloud-Vorlagenversionen „Erfolg“ lautet und ob der Status nach dem Aktivierungsvorgang aktiv ist.	Orlando
CMP: Cloud-Katalogelement aktivieren	Aktiviert das Cloud-Katalogelement, um dem Cloud-Benutzer das Katalogbestellformular anzuzeigen.	Orlando
CMP: Stapelnamen in Katalogelement hinzufügen	Legt den Standardwert für den Stapelnamen im Katalogelement fest.	Orlando
CMP: Überprüfen, ob Stapel vorhanden ist	Validiert, ob der Stapel mit dem Namen „ATFCFTStack“ verfügbar ist.	Orlando
CMP: Cloud-Katalogelement-Seite öffnen	Öffnet die Seite „Cloud-Katalogelement“ im Serviceportal.	Orlando

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Cloud Provisioning and Governance: AWS-Test-Suite (Fortsetzung)

Test	Beschreibung	Release-Version
CMP: Katalogformular absenden	Sendet das Katalogformular, um die Bereitstellung des CFT-Stacks zu starten.	Orlando
CMP: Überprüfen, oder der Stapelstatus aktiv ist	Validiert den Status des Stapels nach der Bereitstellung des Stapels.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang stoppen	Validiert, dass sich der Status des Stapels nach dem Stoppvorgang von „Ein“ in „Aus“ geändert hat.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang starten	Validiert, dass sich der Status des Stapels nach dem Startvorgang von „Aus“ in „Ein“ geändert hat.	Orlando
CMP: Stapelstatus nach Tag 2 verifizieren – Vorgang „Aufheben der Bereitstellung“	Validiert, dass sich der Stapelstatus nach dem Vorgang „Aufheben der Bereitstellung“ von „Aus“ in „Beenden“ geändert hat.	Orlando

Weitere Informationen zu Cloud Provisioning und Governance finden Sie unter Cloud Provisioning and Governance.

Zugehörige Informationen

Schnellstarttests

ITOM-Optimierung – Referenz

Referenzthemen enthalten zusätzliche Informationen zum Konfigurieren und Verwenden von ITOM-Optimierung.

Mit aktivierte Plugins ITOM-Optimierung

Tabelle, die die Plugins auflistet, die mit der Anwendung ITOM-OptimierungCloud Provisioning and Governanceaktiviert werden. Wenn Sie Ihre Anwendung aktualisieren, werden alle neu erforderlichen Anwendungsabhängigkeiten installiert.

Mit Cloud Provisioning and Governance (com.snc.cloud.mgmt) aktivierte Plugins

Plugin-Name	Beschreibung
Cloud Provisioning and Governance Core (com.snc.cloud.core)	Enthält Ressourcenblöcke und Cloud API-Zuordnungen (Cloud Application Programming Interface) im Zusammenhang mit der Cloud API-basierten Erkennung und Ereignissen, die entweder durch Antwortzuordnungs- oder Aufrufmuster verarbeitet werden.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Mit Cloud Provisioning and Governance (com.snc.cloud.mgmt) aktivierte Plugins (Fortsetzung)

Plugin-Name	Beschreibung
Verwaltung der Cloud-Konfiguration (com.snc.config.mgmt)	Ein Framework für die Konfigurationsverwaltung, das API-Implementierungen für die Integration mit Anbietern für die Konfigurationsverwaltung bereitstellt.
Orchestration (com.snc.runbook_automation)	Automatisiert häufig wiederholte manuelle Vorgänge wie Bereitstellungen, Konfigurationen und Informationssammlung. Orchestration nutzt Workflow- und MID-Server -Technologien, um Aktivitäten zum Ausführen von Befehlen auf Systemen innerhalb Ihres Unternehmensnetzwerks zu ermöglichen.
Serviceportal - Core (com.glide.service-portal)	Ein Portal-Framework, mit dem Administratoren eine für Mobilgeräte optimierte Selfservice-Experience für Benutzer erstellen können.
ITOM-Optimierung Lizenzierung (com.sn_itom_opt_licensing)	Eine Proxy-Anwendung, mit der Sie alle mit der Optimierung verbundenen Anwendungen installieren können. Sobald Sie die Optimierungslizenz erworben haben, können Sie diese Proxy-Anwendung installieren, mit der Sie jede Anwendung installieren können, die Teil der Optimierungslizenz ist.

Zugehörige Informationen

- Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate
- Mit installierte Plugins oder Anwendungen ITOM-Transparenz
- Mit installierte Plugins oder Anwendungen ITOM-Integrität
- Mit Now Assist für ITOM installierte Anwendungen

Konfiguration und Ausnahmebehandlung für MID Server

Sie können einen MID-Server mit zusätzlichen Konfigurationsparametern konfigurieren oder eine neue Eigenschaft erstellen, um das Standardverhalten zu ändern.

Mit der Systemeigenschaft „mid.property.probe.api.timeout.minutes“ können Sie festlegen, wie lange der MID-Server warten soll, bevor während der Bereitstellung ein Zeitüberschreitungsfehler ausgegeben wird.

Diese Cloud Provisioning and Governance MID-Server-Eigenschaft mit Name- und Wertparametern behandelt die Zeitüberschreitungsausnahme.

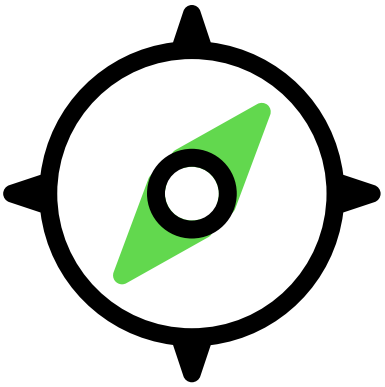
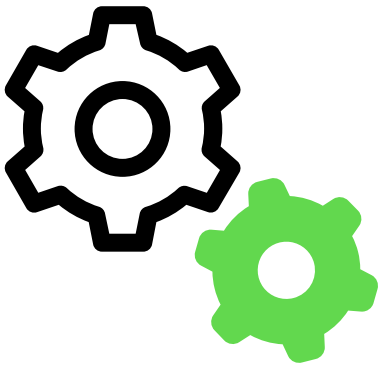
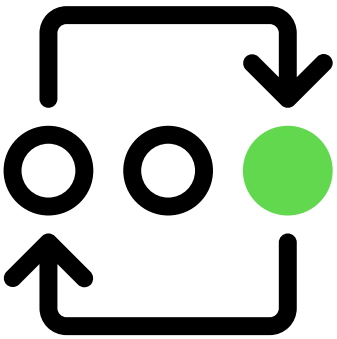
Weitere Informationen zum Erstellen einer MID-Server-Eigenschaft finden Sie unter MID Server-Eigenschaften .

Now Assist für IT Operations Management (ITOM)

Verwenden Sie die Anwendung ServiceNow® Now Assist für IT Operations Management (ITOM), um Warnungen in Ereignismanagementzu analysieren. Warnungsanalysen enthalten eine visuell lesbare Kurzbeschreibung der Warnung und technische Informationen, mit denen Sie Warnungen effektiver untersuchen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erste Schritte

Untersuchen	Konfigurieren	Verwenden
		
Erfahren Sie mehr über Now Assist für ITOM	Konfigurieren Sie die Anwendung Now Assist for ITOM, um zu beginnen	Verwenden Sie die generativen KI-Fähigkeiten von Now Assist für ITOM

Wichtig:

- Einige Now Assist -Produkte/-Funktionen sind derzeit für Kunden in FedRAMP-, NSC DOD IL5- oder Australia IRAP-geschützten Rechenzentren, für selbst gehostete Kunden oder in anderen eingeschränkten Umgebungen nicht verfügbar. Weitere Informationen finden Sie im Now Support Knowledge Base-Artikel KB0743854 . Achten Sie darauf, in zukünftigen Versionen nach Verfügbarkeitsaktualisierungen zu suchen.
- Einige Produkte/Funktionen Now Assist von sind derzeit nur für Kunden in bestimmten Regionen verfügbar. Weitere Informationen finden Sie in Artikel KB1699552 in der Now Support Knowledge Base. Achten Sie darauf, in zukünftigen Versionen nach Verfügbarkeitsaktualisierungen zu suchen.

Hinweis: Derzeit analysiert Now Assist für ITOM nur Tag-basierte, regelbasierte und Log Analytics-Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

Abhängigkeiten

Eine Liste der Now Assist für IT Operations Management (ITOM) Plugin-Abhängigkeiten finden Sie unter Mit Now Assist für ITOM installierte Anwendungen.

Problembehandlung und Hilfe

- KI und Intelligenz in der ServiceNow-Community
- Known Error-Portal nach Artikeln zu bekannten Fehlern durchsuchen
- Kontakt Kundenservice und Support

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

KI-Beschränkungen

Diese Anwendung nutzt künstliche Intelligenz (KI) und maschinelles Lernen, zwei sich schnell entwickelnde Studienbereiche, in denen Vorhersagen auf Grundlage von Datenmustern erstellt werden. Daher liefert diese Anwendung möglicherweise nicht immer präzise, vollständige und angemessene Informationen. Darüber hinaus gibt es keine Garantie dafür, dass diese Anwendung vollständig für Ihren Anwendungsfall trainiert und getestet wurde. Um diese Probleme zu minimieren, sind Sie dafür verantwortlich, Ihre Verwendung dieser Anwendung auf Genauigkeit, Schaden und Angemessenheit für Ihren Anwendungsfall zu testen und zu bewerten, die Ausgabe von Menschen beaufsichtigen zu lassen und sich bei der Entscheidungsfindung nicht ausschließlich auf KI-generierte Ergebnisse zu verlassen Zwecke. Dies ist besonders wichtig, wenn Sie diese Anwendung in Bereichen mit weitreichenden Auswirkungen wie Gesundheitswesen, Finanzen, Recht, Beschäftigung, Sicherheit und Infrastruktur einsetzen möchten. Sie erklären sich damit einverstanden, die Richtlinie zur zulässigen KI-Nutzung von ServiceNow einzuhalten, die von ServiceNow aktualisiert werden kann.

Wichtig: Verwenden Sie Now Assist für ITOM nicht für kritische Sicherheitswarnungen.

Datenverarbeitung

Bei dieser Anwendung müssen die Daten einzelner ServiceNow-Kundeninstanzen in eine zentrale ServiceNow-Umgebung übertragen werden, die sich in einer anderen Rechenzentrumsregion befinden kann als die, in der sich Ihre Instanz befindet, und möglicherweise an einen externen Cloud-Anbieter, z. B. Microsoft Azure. Diese Daten werden gemäß den internen Richtlinien und Verfahren von ServiceNow gehandhabt, einschließlich unserer Richtlinien, die über unser CORE-Compliance-Portal verfügbar sind.

Datenerfassung

ServiceNow sammelt und verwendet die Eingaben, Ausgaben und Ausgabenbearbeitungen dieser Anwendung, um ServiceNow-Technologien wie ServiceNow-Modelle und KI-Produkte zu entwickeln und zu verbessern. Kunden können der Datenerfassung für die Zukunft jederzeit widersprechen, wie auf der Now AssistAbwählseite beschrieben.

Weitere Informationen finden Sie unter Now Assist Dokumentation .

Zugehörige Informationen

Now Assist für IT Operations Management (ITOM) erkunden

Now Assist für IT Operations Management (ITOM) erkunden

Die Anwendung ServiceNow® Now Assist für IT Operations Management (ITOM) verwendet generative KI, um Warnungsanalysen in Ereignismanagementbereitzustellen. Warnungsanalysen enthalten eine visuell lesbare Kurzbeschreibung der Warnung und technische Informationen, mit denen Sie Warnungen effektiver untersuchen können.

In Ereignismanagementist die Warnungsanalyse eine wichtige Funktion, die den Prozess der Warnungsselektierung vollständig transformiert und zu einer schnelleren und nahtloseren Warnungsverwaltung beitragen kann. Basierend auf generativer KI verwendet sie ein Large Language Model (KI), um für Menschen lesbare Warnungstitel und detaillierte Beschreibungen basierend auf angereicherten und umsetzbaren Warnungsdaten zu generieren. Die KI-generierten Warnungsinformationen ermöglichen Ihrem Team eine schnelle Warnungsselektierung und effektive Analysen, was zu einer erheblichen Verkürzung der Lösungszeit führen kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Warnungsanalyse verbessert die Effizienz und Effektivität der Warnungsverwaltung in Ereignismanagement.

Zu den wichtigsten Funktionen gehören:

- Automatische Generierung von klaren, leicht verständlichen Warnungsbeschreibungen
- Verfügbarkeit der Analyse im Warnungsformular und in der Express-Liste
- Möglichkeit zum Aktualisieren und erneuten Generieren von Daten mithilfe der Kartenaktualisierung.

Hinweis: Warnungsanalysen werden in englischer Sprache bereitgestellt, unabhängig davon, welche Sprache in der Warnungsbeschreibung verwendet wird.

Hinweis: Derzeit analysiert Now Assist für ITOM nur Tag-basierte, regelbasierte und Log Analytics-Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

Now Assist für IT Operations Management (ITOM) konfigurieren

Ermöglichen Sie Anwendern Ereignismanagement, Warnungsanalysen anzuzeigen, die von Now Assist für ITOM mithilfe von generativer KI erstellt werden.

Installieren Sie das Plugin Now Assist for IT Operations Management (ITOM).

Installieren Sie das Plugin ITOM in der Funktion ServiceNow® Now Assist.

Vorbereitungen
Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Durch die Installation des Plugins ITOM können die Benutzer von Ereignismanagement Warnungsanalysen anzeigen, die von Now Assist mithilfe der generativen KI erstellt werden.

Prozedur

1. Rufen Sie die Website des ServiceNow Store auf.
2. Geben Sie in der Suchleiste Now Assist für ITOM ein, und wählen Sie **Suchen**aus.
3. Wählen Sie das Widget Now Assist für ITOM und dann **Abrufen** aus, um diese Anwendung für die Installation auf Ihren Instanzen verfügbar zu machen.
4. Navigieren Sie in Ihrer -Instanz zu **Alle** > **Systemdefinition** > **Plugins**.
5. Installieren Sie die Anwendung Now Assist -Administratorkonsole.
   a. Suchen Sie nach der Now Assist -Administratorkonsole.
      Die erforderliche Mindestversion ist 2.1.1.
   b. Wählen Sie **Installieren** aus.
6. Installieren Sie die Anwendung Now Assist für ITOM.
   a. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**.
   b. Suchen Sie nach Now Assist für IT Operations Management (ITOM).
   c. Wählen Sie **Installieren** aus.
7. Nur unter Yokohama Patch 3 und höher: Installieren Sie das Plugin „Glide Virtual Agent“.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

a. Navigieren zu **Alle** > **Systemdefinition** > **Plugins**.

b. Suchen Sie nach Glide Virtual Agent (com.glide.cs.chatbot).

c. Wählen Sie **Installieren** aus.

8. Aktivieren Sie in den Kompetenzen Now Assist für Technologiefunktionen die Kompetenz Warnungsanalyse, um die Verwendung Now Assist von zum Generieren von Warnungsanalysen zu aktivieren.
Aktivieren Sie außerdem die Kompetenz „Warnungsuntersuchung“, um mit Now Assist frühere zugehörige Incidents untersuchen zu können.

a. Navigieren zu **Alle** > **Now Assist Admin** > **Funktionen**.

b. Wählen Sie **Technologie**aus.

c. Wählen Sie auf der Seite „Kompetenzen für Technologiefunktionen Now Assist “ in der Dropdown-Liste des Produkts ITOM die Option aus.

d. Wählen Sie **Details anzeigen**.

e. Suchen Sie die Kompetenz Warnungsanalyse, und wählen Sie **Aktivieren**, um sie zu aktivieren.

f. Suchen und aktivieren Sie die Kompetenz Warnungsuntersuchung.

9. Nur unter Yokohama Patch 3 und höher: Aktivieren Sie die Anwendung KI-Suche in Ihrer Instanz.

a. Navigieren zu **Alle** > **KI-Suche** > **Status der KI-Suche**.

b. Lösen Sie den automatischen Aktivierungsprozess für die KI-Suche in Ihrer Instanz aus, indem Sie **KI-Suche anfordern**auswählen.

Hinweis: Das Aktivieren der KI-Suche in Ihrer Instanz kann bis zu 24 Stunden dauern.

Zugehörige Informationen

Warnungsanalyse von Now Assist in Express-Listeanzeigen

Now Assist für IT Operations Management (ITOM) verwenden

Als Benutzer Ereignismanagement von können Sie die Anwendung ServiceNow® Now Assist für ITOM verwenden, um Warnungsanalysen anzuzeigen, die von Now Assist mithilfe der generativen KI erstellt werden.

Warnungsanalysen umfassen visuell lesbare Kurzbeschreibungen der Warnung und zusätzliche technische Informationen, mit denen Sie Warnungen effektiver untersuchen können. Die Analysen werden in englischer Sprache bereitgestellt, unabhängig davon, welche Sprache in der Warnungsbeschreibung verwendet wird.

Weitere Informationen zur Anwendung ServiceNow® Now Assist für IT Operations Management (ITOM) finden Sie unter Now Assist für IT Operations Management (ITOM).

Warnungsanalyse von Now Assist in Service Operations-Arbeitsbereichanzeigen

Zeigen Sie für eine Warnung auf der Registerkarte Übersicht der Warnung in Service Operations-Arbeitsbereicheine Warnungsanalyse von Now Assist an. Warnungsanalysen enthalten eine visuell lesbare Kurzbeschreibung der Warnung und technische Informationen, mit denen Sie Warnungen effektiver untersuchen können.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in der Funktion Now Assist. Weitere Informationen finden Sie unter Installieren Sie das Plugin Now Assist for IT Operations Management (ITOM)..
- Zeigen Sie wichtige Informationen zur Anwendung ServiceNow® Now Assist für IT Operations Management (ITOM) in Now Assist für IT Operations Management (ITOM)an .

Hinweis: Derzeit analysiert Now Assist für ITOM nur Tag-basierte, regelbasierte und Log Analytics-Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

Erforderliche Rolle: evt_mgmt_user, evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereicherfahrung** > **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie das Listensymbol ( ).
3. Wählen Sie in der Liste „Warnungen“ die Option **Alle Warnungen** aus.
4. Wählen Sie eine Warnung aus.
   Die Warnung wird auf einer separaten Registerkarte geöffnet und zeigt die Unterregisterkarte **Übersicht** an.
5. Wählen Sie im Abschnitt **Analysedie Option Warnung analysieren**aus.
6. Überprüfen Sie die in der Warnungsanalyse bereitgestellten Informationen.

Hinweis: Warnungsanalysen werden in englischer Sprache bereitgestellt, unabhängig davon, welche Sprache in der Warnungsbeschreibung verwendet wird.

Warnungsanalyse von Now Assist in Express-Listeanzeigen

Zeigen Sie eine von ServiceNow® Now Assist erstellte Warnungsanalyse mit generativer KI an. Warnungsanalysen enthalten eine visuell lesbare Kurzbeschreibung der Warnung und technische Informationen, mit denen Sie Warnungen effektiver untersuchen können.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in der Funktion Now Assist. Weitere Informationen finden Sie unter Installieren Sie das Plugin Now Assist for IT Operations Management (ITOM)..
- Zeigen Sie wichtige Informationen zur Anwendung ServiceNow® Now Assist für IT Operations Management (ITOM) in Now Assist für IT Operations Management (ITOM)an .

Hinweis: Derzeit analysiert Now Assist für ITOM nur Tag-basierte, regelbasierte und Log Analytics Warnungsgruppen. Für alle anderen Warnungsgruppentypen wird nur die übergeordnete Warnung analysiert.

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol Express-Liste ( ) aus.
3. Wählen Sie in der Liste „Aktive Warnungen“ links neben einer Warnung das Informationssymbol ( ).

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wählen Sie auf der Registerkarte „Info“ des Vorschaubereichs **Analysieren** in Warnungsanalyse nach Now Assistaus.
5. Zeigen Sie die in der Warnungsanalyse bereitgestellten Informationen an.

   Hinweis: Warnungsanalysen werden in englischer Sprache bereitgestellt, unabhängig davon, welche Sprache in der Warnungsbeschreibung verwendet wird.

6. Wahlweise: Verwenden Sie die Warnungsanalysesymbole, um zugehörige Aufgaben auszuführen.

Symbole für Warnungsanalysen

Symbol	Beschreibung
	Kopieren Sie den Inhalt der Warnungsanalyse in die Zwischenablage.
	Aktualisieren Sie die Warnungsanalyse. **Hinweis:** Durch das Aktualisieren werden die Ergebnisse neu generiert. Vergangene Ergebnisse werden gelöscht.

Anzeigen einer Warnungsgruppenanalyse von Now Assist in Express-Liste

Zeigen Sie eine von ServiceNow® Now Assist erstellte Warnmeldungsgruppenanalyse mit generativer KI an. Die Analyse bietet eine vereinfachte, visuell lesbare Beschreibung der Warnmeldungsgruppe und technische Informationen, mit denen Sie die Warnmeldungsgruppe effizienter untersuchen können.

Vorbereitungen

Installieren Sie das ITOM-Plugin in der Funktion Now Assist. Weitere Informationen finden Sie unter Installieren Sie das Plugin Now Assist for IT Operations Management (ITOM)..

Zeigen Sie wichtige Informationen zur Anwendung ServiceNow® Now Assist für IT Operations Management (ITOM) in Now Assist für IT Operations Management (ITOM)an .

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol Express-Liste ( ) aus.
3. Wählen Sie in der Liste Aktive Warnungen das Informationssymbol ( ) links neben einer Warnungsgruppe, um den Vorschaubereich anzuzeigen.
4. Wählen Sie auf der Registerkarte „Info“ des Vorschaubereichs **Analysieren** in Warnungsanalyse nach Now Assistaus.
5. Zeigen Sie die in der Warnungsanalyse bereitgestellten Informationen an.

   Hinweis: Warnungsanalysen werden in englischer Sprache bereitgestellt, unabhängig davon, welche Sprache in den Warnungsbeschreibungen verwendet wird.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Wahlweise: Verwenden Sie die Warnungsanalysesymbole, um zugehörige Aufgaben auszuführen.

Symbole für Warnungsanalysen

Symbol	Beschreibung
	Kopieren Sie den Inhalt der Warnungsanalyse in die Zwischenablage.
	Aktualisieren Sie die Warnungsanalyse. **Hinweis:** Durch das Aktualisieren werden die Ergebnisse neu generiert. Vergangene Ergebnisse werden gelöscht.

Zugehörige Informationen

Anzeigen einer Warnungsgruppenanalyse durch Now Assist in Express-Liste

Speichern Sie die Zusammenfassung der Warnungsanalyse von Now Assist als Beschreibung der Warnungsgruppe in Express-Liste

Speichern Sie die visuell lesbare Zusammenfassung, die von Now Assist in der -Warnungsanalyse generiert wurde, als Beschreibung einer Warnmeldungsgruppe.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der linken Navigationsleiste das Symbol Express-Liste ( ) aus.
3. Wählen Sie in der Liste „Aktive Warnungen“ links neben einer Warnung das Informationssymbol ( ).
4. Wählen Sie auf der Registerkarte „Info“ des Vorschaubereichs **Analysieren** in Warnungsanalyse nach Now Assistaus.
5. Überprüfen Sie die visuell lesbare, KI-generierte Zusammenfassung der Warnungsanalyse.

   Hinweis: Warnungsanalysen werden in englischer Sprache bereitgestellt, unabhängig davon, welche Sprache in der Warnungsbeschreibung verwendet wird.

6. Wahlweise: Bearbeiten Sie den Zusammenfassungsinhalt.
7. Wählen Sie **Beschreibung speichern** aus, um den Zusammenfassungsinhalt als Beschreibung der Warnmeldungsgruppe zu speichern.
   Der KI-generierte Zusammenfassungsinhalt ersetzt die ursprüngliche Beschreibung der Warnmeldungsgruppe.

Warnmeldungsgruppenbeschreibung in Express-Liste mit Now Assistgenerieren

Verwenden Sie Now Assist, um eine aussagekräftige Beschreibung einer Warnmeldungsgruppe in Express-Liste zu generieren, die alle Warnungen innerhalb der

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Gruppe umfasst. Die generierte Beschreibung ersetzt die ursprüngliche Beschreibung der Gruppe.

Vorbereitungen

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der Navigationsleiste das Symbol Express-Liste ( ) aus.
3. Wählen Sie in der Liste Aktive Warnungen für eine Warnung das Informationssymbol ( ).
4. Wählen Sie unter der angezeigten Warnmeldungsgruppenbeschreibung **Beschreibung aktualisieren aus**.
   Now Assist generiert eine umfassende neue Beschreibung der -Warnungsgruppe, die alle Warnungen innerhalb der Gruppe umfasst. Wenn Sie **Aktualisieren**auswählen, ersetzt die generierte Beschreibung die ursprüngliche Beschreibung der Warnmeldungsgruppe, die aus der frühesten und schwerwiegendsten sekundären Warnung in der Gruppe übernommen wird.
5. Wahlweise: Stellen Sie die ursprüngliche Warnmeldungsgruppenbeschreibung wieder her, indem Sie das Rückgängigmachen-Symbol ( ) neben **Beschreibung aktualisieren** und dann **Wiederherstellen**wählen.

Starten Sie eine Warnungsanalyse im Bereich Now Assist .

Starten Sie im Bereich Now Assist eine Warnungsanalyse. Zur bequemen Überprüfung wird die Warnungsanalyse direkt im Bereich Now Assist angezeigt.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in der Funktion Now Assist. Weitere Informationen finden Sie unter Installieren Sie das Plugin Now Assist for IT Operations Management (ITOM)..
- Zeigen Sie wichtige Informationen zur Anwendung ServiceNow® Now Assist für IT Operations Management (ITOM) in Now Assist für IT Operations Management (ITOM)an .

Ausführliche Informationen zum Bereich Now Assist finden Sie unter Now Assist-Bereich .

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der Navigationsleiste das Listensymbol ( ) aus.
3. Auswahlvorgang **Listen** > **Warnungen** > **Alle Warnungen**.
4. Initiieren Sie mit einer der verfügbaren Methoden im Bereich Now Assist eine Warnungsanalyse.

Eine Warnungsanalyse starten	Verfahren
Aus der Liste	**a.** Wählen Sie das Bereichssymbol Now Assist ( ). Der Bereich Now Assist wird angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Eine Warnungsanalyse starten	Verfahren
	b. Geben Sie in das Feld unten im Bereich eine Warnungsanalyseanforderung einschließlich der Warnungsnummer ein. **Hinweis:** Wenn Sie unvollständige Informationen angeben, werden Sie von Now Assist aufgefordert, die fehlenden Details anzugeben. Die Warnungsanalyse wird im Bereich angezeigt.
Über ein Warnungsformular	**a.** Öffnen Sie eine Warnung. **b.** Wählen Sie das Bereichssymbol Now Assist ( ). Der Bereich Now Assist wird angezeigt. **c.** Wählen Sie **Warnungsanalyse durchführen aus**. Die Warnungsanalyse wird im Bereich angezeigt.

5. Wahlweise: Geben Sie Folgefragen oder Anforderungen ein.
Beispiel: `Analyse zusammenfassen` oder `Warnungsschweregrad anzeigen`.

Incident aus einer Warnung mit Now Assist in Express-Listeerstellen

Erstellen Sie mithilfe von Express-Liste im Bereich Now Assisteinen Incident mit einer visuell lesbaren, KI-generierten Beschreibung.

Vorbereitungen

Derzeit ist diese Funktion für Warnungen CMDBvom Typ , Log Analyticssowie für tagbasierte und komponentenbasierte Warnungen verfügbar.

Erforderliche Rolle: evt_mgmt_operator oder evt_mgmt_admin

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.

2. Wählen Sie in der linken Navigationsleiste das Symbol Express-Liste ( ) aus.

3. Erstellt einen Incident aus einer ausgewählten Warnung.

a. Wählen Sie im Bereich Express-Liste die Warnung aus.

Hinweis: Um die einzelnen Warnungen innerhalb einer Gruppe anzuzeigen, wählen Sie das Checker-Symbol ( ) am Anfang der Zeile der Warnmeldungsgruppe.

b. Wählen Sie in der Dropdown-Liste **Schließen** unter Korrekturaktionen **die Option Incident mit Now Assist erstellen aus**.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Aus der ausgewählten Warnung wird ein Incident mit einer visuell lesbaren, KI-generierten Beschreibung erstellt, und eine Bestätigungsmeldung wird angezeigt.

4. Wahlweise: Zeigen Sie den erstellten Incident an, indem Sie **Incident anzeigen** in der Bestätigungsnachricht oder im Warnungsvorschaubereich auswählen.

Beschleunigen Sie die Lösung von Warnungen mit einer Now Assist -Analyse vergangener zugehöriger Incidents

Verwenden Sie Now Assist, um relevante vergangene Incidents zu untersuchen und effektive Strategien zu ihrer Lösung vorzustellen.

Now Assist fragt historische Datensätze ab, um vergangene Incidents zu finden, und analysiert deren Häufigkeit, Relevanz, Arbeitsnotizen und Lösung. Sie enthält eine Zusammenfassung der relevantesten zugehörigen Incidents im Bereich Now Assist. Die Zusammenfassung enthält die verwendeten Lösungsstrategien sowie Kontaktdetails zu Personen oder Teams, die die Incidents gelöst haben und bei der aktuellen Warnung helfen könnten. Die bereitgestellten Informationen helfen Ihnen, den Kontext und die Bedeutung der aktuellen Warnung besser zu verstehen und effizienter an ihrer Lösung zu arbeiten.

Generieren Sie eine Zusammenfassung Now Assist vergangener zugehöriger Incidents

Zeigen Sie eine Now Assist -Zusammenfassung der vergangenen Incidents für dieselben oder verwandte Konfigurationselemente (Configuration Items, CI) und die zu ihrer Lösung verwendeten Strategien an.

Vorbereitungen

- Installieren Sie das ITOM-Plugin in der Funktion Now Assist. Weitere Informationen finden Sie unter Installieren Sie das Plugin Now Assist for IT Operations Management (ITOM)..
- Stellen Sie sicher, dass die Kompetenz „Warnungsuntersuchung“ aktiv ist. Weitere Informationen finden Sie unter Installieren Sie das Plugin Now Assist for IT Operations Management (ITOM)..
- Zeigen Sie wichtige Informationen zur Anwendung ServiceNow® Now Assist für IT Operations Management (ITOM) in Now Assist für IT Operations Management (ITOM)an .

Ausführliche Informationen zum Bereich Now Assist finden Sie unter Now Assist-Bereich .

Erforderliche Rolle: evt_mgmt_operator

Prozedur

1. Navigieren zu **Arbeitsbereiche** > **Service Operations-Arbeitsbereich**.
2. Wählen Sie in der Navigationsleiste das Listensymbol ( ).
3. Auswahlvorgang **Listen** > **Warnungen** > **Alle Warnungen**.
4. Öffnen Sie eine Warnung.
5. Wählen Sie das Bereichssymbol Now Assist ( ).
   Der Bereich Now Assist wird angezeigt.
6. Fordern Sie eine Untersuchung zu früheren Now Assist Incidents an, indem Sie **Zugehörige Incidents analysieren**auswählen.
   Im Bereich wird eine Zusammenfassung der relevantesten zugehörigen Incidents angezeigt.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Wahlweise: Überprüfen Sie die Details eines zugehörigen Incidents, indem Sie den entsprechenden Link unter Zugehörige Incidents auswählen.
   Die Incident-Seite wird geöffnet und zeigt die Registerkarte Übersicht an.

Now Assist für IT Operations Management (ITOM) – Referenz

Referenzthemen enthalten zusätzliche Informationen zum Konfigurieren und Verwenden der Anwendung Now Assist für ITOM.

Mit Now Assist für ITOM installierte Anwendungen

Tabelle, die mit der Anwendung Now Assist für IT Operations Management (ITOM) installierte Anwendungen auflistet. Wenn Sie Ihre Anwendung aktualisieren, werden alle neu erforderlichen Anwendungsabhängigkeiten installiert.

Mit Now Assist für ITOM installierte Anwendungen (sn_itom_gen_ai)

Anwendungsname	Beschreibung
UXC Generative KI (sn_uxc_gen_ai)	Aktiviert Plattformfähigkeiten zur Unterstützung von Funktionen der generativen künstlichen Intelligenz (GenAI) in Geschäftsbereichsanwendungen.
Warnmeldungsassistent (sn_alert_gen_ai)	Lässt sich in vorhandene Systeme integrieren, um kurze Warnungsbeschreibungen zu generieren, und ergänzt sie durch umfassende Analysen.

Zugehörige Informationen

- Mit installierte Plugins oder Anwendungen ITOM Cloud Accelerate
- Mit installierte Plugins oder Anwendungen ITOM-Transparenz
- Mit installierte Plugins oder Anwendungen ITOM-Integrität
- Mit aktivierte Plugins ITOM-Optimierung

Auf Cloud-Umgebungen für ITOM-Produkte zugreifen

Wenn Ihre Organisation IT-Assets in der Cloud bereitstellt, müssen ITOM-Produkte auf Ihre Cloud-Umgebung zugreifen, um Informationen über die IT-Infrastruktur zu sammeln.

Zugehörige Informationen

- Cloud-Discovery erkunden
- Cloud-Ressourcen-Erkennung

Installieren und konfigurieren Sie MID Servers für den Zugriff auf Cloud-Umgebungen

Installieren und konfigurieren Sie MID Servers richtig, um ITOM-Produkten den Zugriff auf Cloud-Ressourcen zu ermöglichen.

Vorbereitungen

Erforderliche Rolle: admin, discovery_admin oder sn_cmp.cloud_admin (für Cloud Provisioning and Governance)

Warum und wann dieser Vorgang ausgeführt wird

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Prozedur

1. Für die IP-basierte Discovery wird der MID Server auf einem Server in der Cloud-Umgebung in einer Virtual Private Cloud (VPC) installiert .

   Example
   Wenn Sie beispielsweise den Zugriff auf AWS-Servicekonten mit IAM-Rollen konfigurieren, installieren Sie MID-Server in der Amazon-EC2-Instanz.

   Wichtig: Wenn Sie AWS-Anmeldeinformationen für Now Platform konfigurieren, spielt der Standort des MID-Servers keine Rolle.

   Wenn Ihre Organisation über mehrere VPC-Segmente verfügt, stellen Sie MID Servers in einer Management-Mentor-Transit-VPC bereit.

2. Aktivieren Sie IP-basierte Erkennungsaufträge, um mit agentlosen Anmeldeinformationen auf die Rechenebene zuzugreifen.

3. Konfigurieren Sie MID-Server mit den Funktionen, die für die Cloud-Umgebung erforderlich sind, für die Sie eine Erkennung durchführen möchten.

   Sie können die Funktionalität `Alle` auswählen oder bestimmte Funktionen konfigurieren, um für eine höhere Sicherheit zu sorgen.

   Fügen Sie Cloud-Management in **der unterstützten Anwendung** in MID-Server für zu verarbeitende Anforderungen Cloud Provisioning and Governance von hinzu.

Cloud-Umgebung	**Von** Cloud-Discovery **benötigte** MID-Server**-Funktion**	**Von** Cloud Provisioning and Governance **benötigte** MID-Server**-Funktion**
Amazon AWS Cloud	`AWS`	`Cloud Management` und `AWS`
Google Cloud	`Google`	`Google` und `Cloud Management`
IBM Cloud Platform	`IBM`	`IBM` und `Cloud Management`
Microsoft Azure Cloud	`Azure`	`Azure` und `Cloud Management`

4. Wenn MID Servers für den Zugriff auf Cloud-Ressourcen einen nicht authentifizierten Proxy-Server verwenden muss, ändern Sie die Datei `agent\conf\wrapper-override.conf` wie folgt:

```
wrapper.java.additional.1=-Dhttp.proxySet=true
        wrapper.java.additional.2=-Dhttp.proxyHost=<proxyHost>
        wrapper.java.additional.3=-Dhttp.proxyPort=<proxyPort>
        wrapper.java.additional.4=-DuseProxy=true
```

Zugehörige Informationen

Proxy-Server-Konfiguration für MID Servers, die für Cloud-Discovery und Cloud Provisioning and Governance verwendet werden

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Proxy-Server-Konfiguration für MID Servers, die für Cloud-Discovery und Cloud Provisioning and Governance verwendet werden

Sie können den MID-Server für Cloud Provisioning and Governance für die Verwendung eines Proxy-Servers konfigurieren. Durch die Verwendung eines Proxy-Servers werden alle cloudbasierten Aktivitäten wie Ausführen von Discovery, Abrechnungsdownloads, Bereitstellen virtueller Computer und Ausführen von Lebenszyklusvorgängen auf virtuellen Computern unterstützt.

Einschränkungen für Proxy-Server

- VMware Cloud wird nicht unterstützt.
- Es werden ausschließlich Windows- oder Linux-Plattformen unterstützt.
- Die Integration mit Google Cloud Console bietet keine Unterstützung für das Herunterladen von Abrechnungsdaten.
- Remote-PowerShell-Skripts können nicht ausgeführt werden.
- Benutzerdefinierte APIs funktionieren möglicherweise nicht.

Hinweis:

SSH-Aufrufe dürfen nicht über einen Proxy-Server weitergeleitet werden, wenn eine Private Cloud-Umgebung verwendet wird, die sich auf derselben Seite des Proxy-Servers wie der MID-Server befindet.

Legen Sie „mid.capi.skip_proxy_for_ssh“ auf „wahr“ fest, um dies zu überspringen. Weitere Informationen finden Sie unter MID-Server-Eigenschaften, die von Service-Mapping verwendet werden.

mid.capi.überspringen_proxy_for_ssh:

- Bestimmt, ob der MID-Server den Proxy-Server bei der Weiterleitung von SSH-Anrufen überspringt.
- Typ: Wahr | Falsch
- Standardwert: falsch

Unterstützte Proxy-Server-Authentifizierung für Cloud Provisioning and Governance

Typ des Proxy-Servers	Authentifizierungstyp
HTTP/HTTPS	Keine Authentifizierung
SOCKS5	Keine Authentifizierung
HTTP/HTTPS	Basic Authentication
SOCKS5	Basic Authentication
HTTP/HTTPS	NTLM

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Proxy-Server-Konfigurationen für Cloud Provisioning and Governance

Unterstützte Konfigurationseinstellungen

Konfiguration	Betriebssystem	Proxy-Server	Authentifizierungsmodus
Konfiguration 1	Linux	Keine	Nicht zutreffend
Konfiguration 2	Windows	Squid (HTTPS)	Keine
Konfiguration 3	Linux	Squid (HTTPS)	Lokal
Konfiguration 4	Windows	Squid (HTTPS)	Active Directory

Unterstützte Konfigurationen

Cloud Provider	Funktionalität	Konfiguration 1	Konfiguration 2	Konfiguration 3	Konfiguration 4
Amazon AWS Cloud, Microsoft Azure Cloud und IBM Cloud Platform	Cloud-Discovery	Ja	Ja	Ja	Ja
	VM-Bereitstellung	Ja	Ja	Ja	Ja
	VM-Lebenszyklus	Ja	Ja	Ja	Ja
	CFT-Bereitstellung	Ja	Ja	Ja	Ja
	Abrechnungsdownload	Ja	Ja	Ja	Ja
	Skripts mit SSH	Ja	Ja	Ja	Ja
	Skripts mit PowerShell	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
	Cloud Events	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
Google Cloud Platform	Cloud-Discovery	Ja	Ja	Ja	Ja
	VM-Bereitstellung	Ja	Ja	Ja	Ja
	VM-Lebenszyklus	Ja	Ja	Ja	Ja
	CFT-Bereitstellung	Ja	Ja	Ja	Ja
	Abrechnungsdownload	Nein	Nein	Nein	Nein
	Skripts mit SSH	Ja	Ja	Ja	Ja
	Skripts mit PowerShell	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend
	Cloud Events	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Unterstützte Konfigurationen (Fortsetzung)

Cloud Provider	Funktionalität	Konfiguration 1	Konfiguration 2	Konfiguration 3	Konfiguration 4
VMware Cloud	Nicht zutreffend				

Zugehörige Informationen

MID Server unter Windows installieren

MID Server unter Linux installieren

Konfiguration für Wiederholung von Cloud-Anforderungen

Wenn eine Anforderung während der Discovery von einem Cloud-Anbieter gedrosselt wird, bietet die Wiederholungskonfiguration für Cloud-Anforderungen eine anpassbare Methode zur Wiederholung von Anforderungen. Muster für Discovery und Service-Mapping enthält eine Wiederholungskonfiguration für AWS und Azure. Sie können die enthaltene Konfiguration anpassen oder eine eigene erstellen.

Discovery-Administratoren und Cloud-Administratoren können unter auf die Konfiguration der Anforderungswiederholung zugreifen **Alle** > **Discovery** > **Konfiguration für Wiederholung von Cloud-Anforderungen**. Sie können eine Konfiguration für jeden Provider erstellen.

Wenn eine Anforderung eingeschränkt wird, wird vom Framework für Wiederholungen die für den Provider definierte Wiederholungskonfiguration dazu verwendet, Wiederholungen zu verarbeiten, bevor die endgültige Antwort an die ApiCommand-Klassen zurückgegeben wird:

- AwsApiCommand
- AzureApiCommand

Die Wiederholungskonfigurationen werden über die MID-Server-Eigenschaft *mid.cloud.discovery.retry.configuration* mit den MID Serversn synchronisiert.

Es gibt die folgenden Wiederholungsstrategien:

- Exponentielles Backoff
- Antwortheader – Backoff
- Benutzerdefinierter Backoff

Exponentielles Backoff

Für die folgende Beispielkonfiguration …

Einstellung	Wert
Max. Wiederholungen	3
Antwortcodes	429
Basisverzögerung in ms	1.000
Max. Verzögerung in ms	10000
Additional delay window in ms (Fenster „Weitere Verzögerung“ in ms)	1500

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

… funktioniert die Wiederholungsstrategie „Exponentielles Backoff“ wie folgt:

- 1. Wiederholung: Der Backoff-Multiplikator wird zufällig zwischen 0 und 1 ausgewählt. Der maximale Verzögerungswert beträgt 400 ms (400 * 1).
- 2. Wiederholung: Der Backoff-Multiplikator wird zufällig zwischen 0 und 3 ausgewählt. Der maximale Verzögerungswert beträgt 1.200 ms (400 * 3).
- 3. Wiederholung: Der Backoff-Multiplikator wird zufällig zwischen 0 und 7 ausgewählt. Der maximale Verzögerungswert beträgt 2.800 ms (400 * 7).

Wenn die Verzögerung bei nachfolgenden Wiederholungen 10.000 überschreitet (die maximale Verzögerung), wird der Wert 10.000 als anfängliche Verzögerung verwendet.

Sobald die anfängliche Verzögerung generiert wurde, wird der Verzögerung Jitter hinzugefügt. Das Fenster „Jitter“ wird durch das Feld **Additional delay window in ms** (Fenster „Weitere Verzögerung“ in ms) definiert. Vom System wird ein zufälliger Wert zwischen 0 und 1.500 ausgewählt und zur anfänglichen Verzögerung addiert.

Wenn die anfängliche Verzögerung 500 beträgt, kann die endgültige Verzögerung (mit Jitter) einen Wert zwischen 500 und 2.000 ms annehmen.

Antwortheader – Backoff

Für die folgende Beispielkonfiguration …

Einstellung	Wert
Max. Wiederholungen	3
Antwortcodes	429
Antwortheader	Retry-After (Wiederholen-nach)
Verzögerungseinheit für Antwortheader	Sekunden
Additional delay window in ms (Fenster „Weitere Verzögerung“ in ms)	1500

… funktioniert die Backoff-Strategie für Antwortheader wie folgt:

- Rufen Sie den Wert des Headers `Retry-After` aus der Serverantwort ab.
- Konvertieren Sie den Wert von `Retry-After` in Millisekunden, indem Sie ihn mit 1.000 multiplizieren.

Sobald die anfängliche Verzögerung generiert wurde, wird der Verzögerung Jitter hinzugefügt. Das Fenster „Jitter“ wird durch das Feld **Additional delay window in ms** (Fenster „Weitere Verzögerung“ in ms) definiert. Vom System wird ein zufälliger Wert zwischen 0 und 1.500 ausgewählt und zur anfänglichen Verzögerung addiert.

Wenn die anfängliche Verzögerung 2.000 beträgt, kann die endgültige Verzögerung (mit Jitter) einen Wert zwischen 2.000 und 3.500 ms annehmen.

Benutzerdefinierter Backoff

Mit einer anwenderdefinierten Backoff-Wiederholungsstrategie definieren Sie die **Max. Wiederholungen** und **Antwortcodes** und erstellen Ihre eigene **MID-Skripteinbindung,** die definiert, wie Anforderungen mit der Funktion `getDelay()` wiederholt werden. Weitere Informationen finden Sie unter Skripteinbindungen .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Richten Sie ein Cloud-Servicekonto ein

Erstellen und konfigurieren Sie ServiceNow-Cloud-Accounts unter Now Platform für die entsprechenden Servicekonten des Cloud-Lieferanten.

Richten Sie Servicekonten für Oracle Cloud Infrastructure (OCI) ein

Erstellen und konfigurieren Sie Cloud-Service-Accounts unter Now Platform für die entsprechenden Oracle Cloud Infrastructure(OCI)-Service-Accounts.

Der OCI-Serviceaccount ist ein Identitätstyp, der zum Authentifizierung und Autorisieren des Zugriffs auf OCI-Ressourcen und -Services verwendet wird. Sie bietet Anwendungen, Services und Benutzern die Möglichkeit, sicher mit OCI-Ressourcen zu interagieren. Servicekonten werden häufig für automatisierte Prozesse, Anwendungen oder Services verwendet, die innerhalb von OCI ausgeführt werden, sodass sie gemäß den definierten Berechtigungen und Richtlinien auf Ressourcen zugreifen können.

OCI-Zugriff und -Berechtigung mithilfe von Richtlinien

Oracle Zugriff auf die Cloud Infrastructure (OCI) und Berechtigungen mithilfe von Richtlinien bieten Berechtigungen für die sichere Nutzung und Verwaltung von Cloud-Ressourcen in OCI.

Laden Sie die Tabelle „OCI-Zugriff und -Berechtigung mithilfe von Richtlinien“ herunter, und verwenden Sie sie, um den erforderlichen Anwenderzugriff und die erforderliche Berechtigung zu gewähren.

Generieren Sie Ihre Oracle Cloud Infrastructure(OCI)-Anmeldeinformationen

Generieren Sie Ihre Oracle (OCI)-Anmeldeinformationen, um auf Ihr OCI-Erkennungskonto und ServiceNow Discoveryzuzugreifen.

Vorbereitungen

- Stellen Sie sicher, dass die App Cloud Access Interface (Cloud Access Interface) installiert ist (ab Version 1.0.0).
- Stellen Sie sicher, dass die Store-App CMDB CI-Klassenmodelle ab Version 1.23.0 installiert ist.
- Stellen Sie sicher, dass die Store-App Muster für Discovery und Service-Mapping ab Version 1.0.74 installiert ist.
- Erforderliche Rolle: Oracle Cloud-Benutzer, Oracle Cloud-Administrator

Warum und wann dieser Vorgang ausgeführt wird

Generieren Sie die folgenden OCI-Anmeldeinformationen, um auf Ihr OCI-Discovery-Konto zuzugreifen.

OCI-Anmeldeinformationen

Feld	Beschreibung
Mandanten-ID	Oracle Cloud-Bezeichner (OCID) für Ihren Mandanten. Die OCID ist das Stamm-Compartment, das alle Oracle Cloud Infrastructure-Ressourcen Ihrer Organisation enthält.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

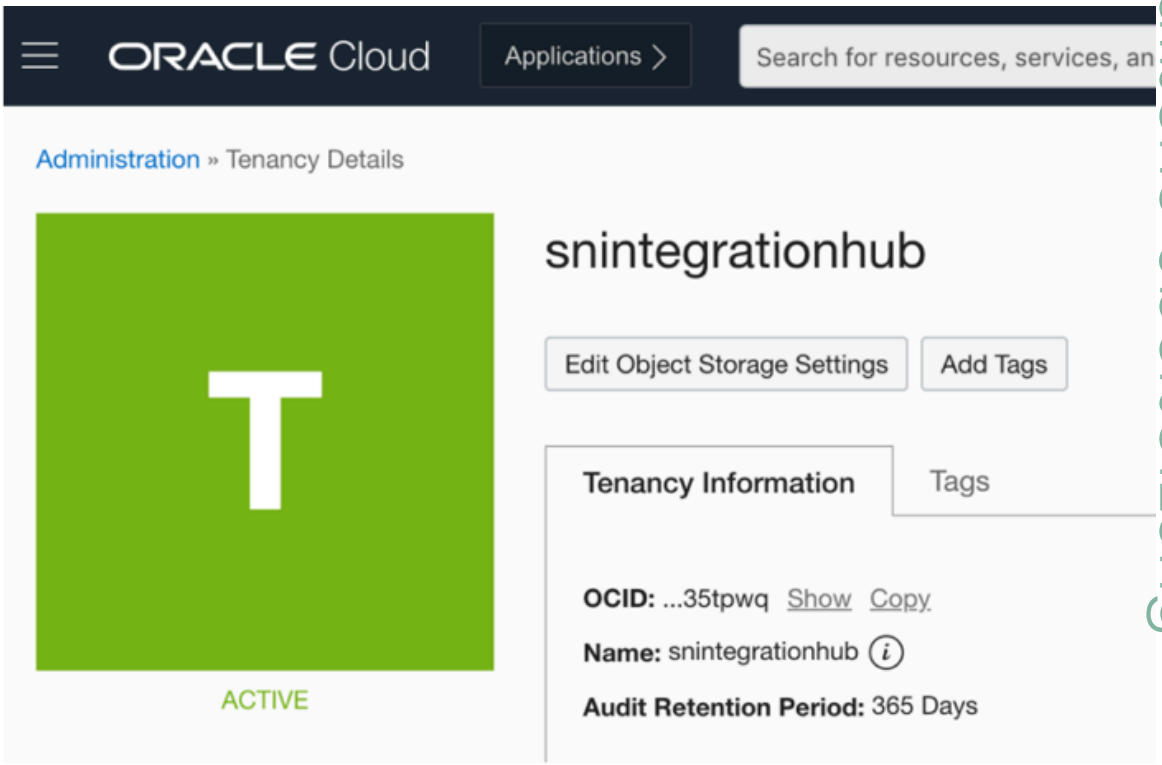
OCI-Anmeldeinformationen (Fortsetzung)

Feld	Beschreibung
Anwender-ID	OCID des Anwenders, der die Cloud-Infrastrukturressourcen Oracle verwalten oder verwenden muss.
Schlüssel-Fingerabdruck	Fingerabdruck des zuletzt hinzugefügten Schlüssels.
Privater Schlüssel	Privater RSA-Schlüssel, der für die API-Signaturauthentifizierung verwendet wird.

Prozedur

1. Melden Sie sich bei der OCI-Konsole an, und navigieren Sie zu **Governance und Administration** > **Administration**.
2. Wählen Sie in der Liste **Mandantendetails**aus.
   Das folgende Beispiel zeigt die OCID, den Namen und den Aufbewahrungszeitraum für die Mandanteninformationen.

Mandanteninformationen



3. Kopieren Sie die Mandanten-OCID in die Zwischenablage, indem Sie **Kopieren**auswählen.
4. Wechseln Sie in der OCI-Konsole zum Menü Profil, und wählen Sie **Anwendereinstellungen**aus.

> **Hinweis:** Wenn Sie Administrator sind, navigieren Sie zu **Governance und Administration** > **Identität** > **Anwender**. Wählen Sie den Anwender aus der Liste aus, um die Details anzuzeigen.

5. Kopieren Sie die Anwender-OCID in die Zwischenablage, indem Sie **Kopieren**auswählen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

6. Generieren Sie das API-Schlüsselpaar, indem Sie zum Menü „Profil“ wechseln und **Benutzereinstellungen**auswählen.
7. Navigieren zu **Ressourcen** > **API-Schlüssel** > **API-Schlüssel hinzufügen**.
8. Wählen Sie im Dialogfeld die Option **API-Schlüsselpaar generieren aus**.
9. Laden Sie aus dem Dialogfeld den privaten und den öffentlichen Schlüssel herunter, und speichern Sie die Schlüssel in Ihrem `.oci`– Verzeichnis.

   Wichtig: Wenn Ihr Browser den privaten Schlüssel in ein anderes Verzeichnis herunterlädt, verschieben Sie ihn in Ihr `.oci` -Verzeichnis.

   Hinweis: Sie können auch die für Linux, macOSoder Windows verfügbaren Befehlszeilentools verwenden, um einen API-Signaturschlüssel zu generieren. Weitere Informationen finden Sie unter Erforderliche Schlüssel und OCIDs auf der Dokumentationswebsite Oracle.

10. Konvertieren Sie den privaten und den öffentlichen Schlüssel mit den Ihnen zur Verfügung stehenden Onlinetools, z. B. decoder.link, in das RSA-Format.
    Weitere Informationen zum Konvertieren von Schlüsseln in das RSA-Format finden Sie im Artikel Oracle OCI – Musterrückgabefehler bei der Service-Account-Validierung: „JAVASCRIPT_CODE_FAILURE: RSA private key muss für die Authentifizierung angegeben werden“ [KB0966224] in der Now Support Knowledge Base.
11. Generieren Sie den **Schlüsselfingerabdruck**, indem Sie zu navigieren **Ressourcen** > **API-Schlüssel** > **API-Schlüssel hinzufügen**.
12. Wählen Sie im Dialogfeld die Option **Öffentlichen Schlüssel einfügen** aus.
13. Fügen Sie den öffentlichen Schlüssel im RSA-Format in das Dialogfeld ein, und wählen Sie **Hinzufügen**aus.

Ergebnisse

Der Fingerabdruck des Schlüssels wird angezeigt. Beispiel:
12:34:56:78:90:ab:cd:ef:12:34:56:78:90:ab:cd:ef ist der Fingerabdruck.

Hinweis: Nachdem Sie Ihren ersten öffentlichen Schlüssel hochgeladen haben, können Sie auch den API-Vorgang UploadApiKey verwenden, um zusätzliche Schlüssel hochzuladen. Weitere Informationen finden Sie unter UploadApiKey auf der Dokumentationswebsite Oracle.

AWS-Servicekonten einrichten

Erstellen und konfigurieren Sie Cloud-Servicekonten auf der Now Platform für die entsprechenden Amazon Web Services-Servicekonten (AWS).

Vorbereitungen

Sie müssen mit der Hierarchie der AWS-Servicekonten in Ihrer Umgebung vertraut sein. Wenn es beispielsweise AWS-Organisationen gibt, richten Sie in Now Platform Verwaltungs- und Mitgliedskonten ein, die diese Hierarchie abbilden. Sie können AWS-Servicekonten der folgenden Typen einrichten:

- **Diskretes Konto**: Eigenständiges Konto ohne Verwaltungskonto.
- **Verwaltungskonto**: Verwaltungskonto, das Mitgliedskonten (Unterkonten) enthalten kann.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Hinweis: In einigen UI-Bildschirmen in ServiceNow werden Verwaltungskonten als Master-Konten bezeichnet.

- **Mitgliedskonto**: Unterkonto, das zum (Verwaltungs-)Konto gehört.

Erforderliche Rolle:

- Für Cloud-Discovery: admin oder discovery_admin
- Für Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Ein Servicekonto ist ein sicherer Datensatz in Ihrer Instanz, in dem die Anmelde- und Zugriffsinformationen für Ihr Provider-Konto gespeichert sind. Von Discovery werden die Informationen für den Zugriff auf Ihr Provider-Konto dafür verwendet, Daten zu jeder Ressource in jedem angegebenen Rechenzentrum abzurufen. Ein Cloud-Konto ist die logische Darstellung der gesamten oder eines Teils Ihrer verwalteten Cloud-Infrastruktur in Cloud Provisioning and Governance. Ein Cloud-Konto kann mehrere Servicekonten – sogar Servicekonten verschiedener Provider – enthalten. Geben Sie für jedes Servicekonto an, welche Rechenzentren in das Cloud-Konto aufgenommen werden sollen.

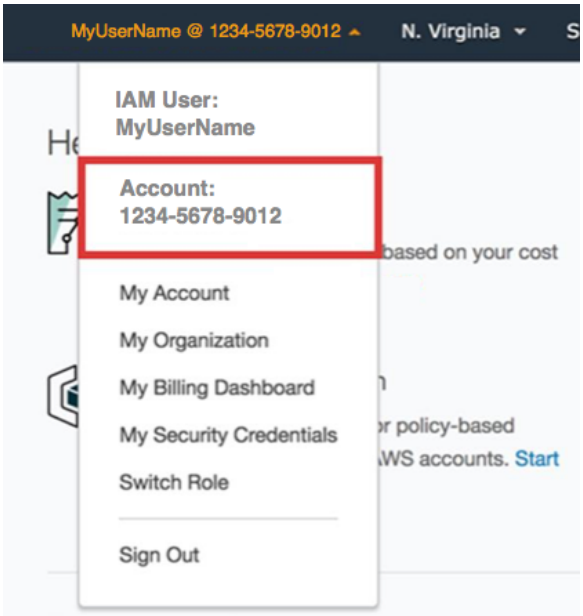
Prozedur

1. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Service-Accounts**.
2. Wählen Sie **Neu**.
3. Füllen Sie die Felder aus.

Formular für Cloud-Servicekonto

Feld	Beschreibung
Name	Eindeutiger und aussagekräftiger Name für dieses Servicekonto.
Account-ID	12-stellige Nummer des Benutzerkontos. Erweitern Sie die Liste unter dem AWS-Kontonamen in der AWS-Verwaltungskonsole, um die Nummer anzuzeigen. **Wichtig:** Entfernen Sie im Feld **Konto-ID** die Bindestriche (-) aus der Nummer.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Nummer des IAM-Benutzerkontos 
Discovery-Anmeldeinformationen	Anmeldeinformationen, die für ServiceNow-Anwendungen für den Zugriff auf dieses Konto erforderlich sind. Sie können dieses Feld zu einem späteren Zeitpunkt konfigurieren, während Sie den Zugriff auf AWS-Konten konfigurieren. ◦ Wenn Sie hat die AWS-Anmeldeinformationen unter konfiguriert Now Platform , wählen Sie das Lupensymbol und dann den Namen der entsprechenden AWS -Anmeldeinformationen aus. ◦ Um andere AWS-Konten für den Zugriff auf diesen Account zu verwenden, lassen Sie das Feld leer. Beispielsweise müssen Sie die AWS-Anmeldeinformationen nicht für Konten angeben, die IAM-Rollen oder Mitgliedskonten annehmen und ihr Verwaltungskonto für den Zugriff verwenden.
Rechenzentrums-URL	URL des Rechenzentrums. Dieses Feld ist für die Konten AWS Region China und AWS GovCloud (US) erforderlich. Zum Beispiel: ◦ AWS Region China: `https://organizations.cn-northwest-1.amazonaws.com.cn` ◦ AWS GovCloud (USA): `https://aws.amazon.com/ec2/`
Rechenzentrumstyp	Typ des Rechenzentrums, in dem das Konto gehostet wird. Wählen Sie das **AWS-Rechenzentrum**.
Status der Rechenzentrumserkennung	Automatisch generierter Wert: Status und Zeitstempel der letzten Ausführung von Discovery im Rechenzentrum.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Übergeordneter Account	Name des Verwaltungskontos, das die Organisation in AWS darstellt, zu der dieses Mitgliedskonto gehört. Dieser Name wird angezeigt, wenn Sie **AWS-Rechenzentrum** auswählen. Wenn dieses Konto nicht Teil einer AWS-Organisation ist, lassen Sie dieses Feld leer.
Ist Master-Konto	Kennzeichnung des Verwaltungskontos. Sie wird angezeigt, wenn Sie in der Dropdown-Liste „Rechenzentrumstyp“ die Option **AWS-Rechenzentrum** auswählen. Aktivieren Sie das Kontrollkästchen, um das AWS-Servicekonto dem Verwaltungskonto zuzuordnen. Aktivieren Sie dieses Kontrollkästchen nur für Konten, die Sie zuvor in der AWS-Verwaltungskonsole als Verwaltungskonten konfiguriert haben und zu denen einige Mitgliedskonten gehören. In der AWS-Dokumentation finden Sie weitere Informationen zu AWS-Organisationen. **Hinweis:** Sie müssen die richtige Berechtigung in AWS oder der Organisationsrolle für Standardanmeldeinformationen einrichten. Weitere Informationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern.
Account des Zugriffsberechtigten	Name des vertrauenswürdigen Kontos. Konfigurieren Sie dieses Feld nur für Konten, bei denen keine permanenten AWS-Anmeldeinformationen verwendet werden und bei denen IAM-Rollen für den Zugriff genutzt werden.

Zugriff für AWS-Servicekonten einrichten

Cloud-Discovery und Cloud Provisioning and Governance benötigen Zugriff auf Ressourcen in den AWS-Servicekonten (Amazon Web Services). Informieren Sie sich über verschiedene Methoden zur Konfiguration dieses Zugriffs.

Cloud-Discovery und Cloud Provisioning and Governance greifen auf Ressourcen in den AWS-Servicekonten über MID Servers zu. Sie müssen den eingehenden Datenverkehr an Amazon EC2-Instanzen vom MID-Server autorisieren, um die anfängliche Kommunikation einzurichten. Weitere Informationen hierzu finden Sie unter Eingehende Regeln für Sicherheitsgruppen mit der AWS-Verwaltungskonsole konfigurieren .

Typen von AWS-Anmeldeinformationen

Es gibt permanente und temporäre AWS-Anmeldeinformationen, die Sie zur Konfiguration des Zugriffs auf AWS-Servicekonten verwenden können.

Permanent

Die permanenten Anmeldeinformationen sind die eigentlichen AWS-Anmeldeinformationen für das Servicekonto, das Sie zum Modul Verbindungen und Anmeldeinformationen von Now Platform hinzufügen. Die Verwaltung der Anmeldeinformationen in Now Platform kann zwar zeitaufwendig sein, Sie

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

vermeiden jedoch die komplexen Konfigurationen, die mit der Verwendung temporärer Anmeldeinformationen verbunden sind.

Temporär

Die temporären Anmeldeinformationen werden vom AWS-Sicherheitstoken-Service (AWS STS) für IAM-Rollen generiert. Nachdem Sie IAM-Rollen für die Konten AWS konfiguriert haben, greift der MID-Server mit diesen temporären Anmeldeinformationen auf die Ressourcen AWS zu. Sie können die IAM-Standardrolle *OrganizationAccountAccessRole* verwenden oder benutzerdefinierte IAM-Rollen erstellen.

Die Annahme von IAM-Rollen in einer großen AWS-Organisation ist bequemer und bietet mehr Sicherheit als die Verwendung einer hohen Anzahl permanenter Anmeldeinformationen für alle AWS-Konten. Temporäre Anmeldeinformationen werden nur im Namen eines Servicekontos erworben, wenn für dieses Servicekonto in der Tabelle „Servicekonten“ [cmdb_ci_cloud_service_account] keine permanenten Anmeldeinformationen angegeben sind.

MID-Server verwendet die AssumeRole- Aktion in der AWS-Sicherheitstoken-Service-API, um die Rolle eines Mitgliedskontos anzunehmen. An diese API übergebene Parameter bestimmen, welche zusätzlichen Sicherheitsbeschränkungen auf die Rolle beim Zugriff auf AWS-Ressourcen angewendet werden.

Standardmäßig ist der MID-Server so konfiguriert, dass er die Rolle *OrganizationAccountAccessRole* übernimmt, mit der allen Mitgliedern eines Primärkontos temporäre Anmeldeinformationen gewährt werden. Diese Aktion erfolgt automatisch, wenn keine permanenten Anmeldeinformationen für die Mitgliedskonten vorhanden sind. Durch diese Konfiguration werden keine zusätzlichen Sicherheitseinstellungen angewendet; der Zugriff auf Ressourcen in Mitgliedskonten wird nicht eingeschränkt.

Standardmäßig werden temporäre Anmeldeinformationen für Mitgliedskonten 60 Minuten lang im Cache der ServiceNow-Instanz gespeichert. Dieses Intervall ermöglicht im Prozess der horizontalen Erkennung eine mehrmalige Ausführung, ohne dass bei jeder Erkennung neue Anmeldeinformationen generiert werden müssen. Sie können das Zwischenspeichern von Anmeldeinformationen verhindern oder den Caching-Zeitraum mithilfe der MID-Server-Eigenschaften ändern.

IAM-Rollen und -Berechtigungen

Um die Sicherheit der AWS-Standardrolle `OrganizationAccountAccessRole` zu verbessern, können Sie die AWS-Rollen anpassen, die MID Server annehmen können, um temporäre Anmeldeinformationen für Mitgliedskonten zu erhalten. Sie können zusätzliche Berechtigungen konfigurieren, um die Sicherheit zu verbessern und um anzupassen, wie die Rolle des Mitgliedskontos angenommen wird, wenn Cloud-Ressourcen erkannt werden.

Methoden zum Gewähren von Zugriff

Im Zusammenhang mit der Konfiguration des Zugriffs für AWS-Konten werden die folgenden Begriffe verwendet:

Vertrauende Konten

Vertrauende Konten haben keine permanenten AWS-Anmeldeinformationen. Sie konfigurieren die Vertrauensstellung für IAM-Rollen in diesen Konten so, dass sie für den Zugriff auf andere Konten zurückgreifen.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Vertrauenswürdige Konten

Die vertrauenswürdigen Konten werden von den vertrauenden Konten für den Zugriff verwendet. In der Benutzeroberfläche von ServiceNow werden die vertrauenswürdigen Konten als Accounts des Zugriffsberechtigten bezeichnet.

Normalerweise richten Sie den Zugriff auf die AWS-Konten in Ihrer Organisation mit den folgenden Methoden ein:

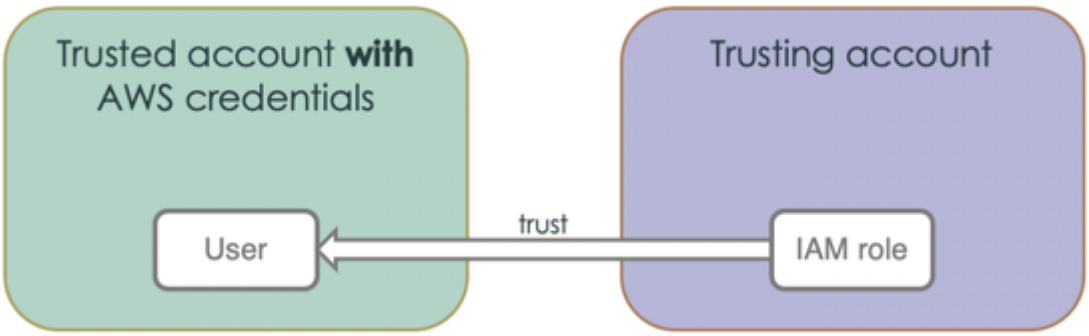
- Zugriff auf AWS-Konten mit permanenten AWS-Anmeldeinformationen konfigurieren

  Konfigurieren Sie die tatsächlichen AWS-Anmeldeinformationen auf der Now Platform, um die Komplexität beim Erstellen und Einrichten von IAM-Rollen zu vermeiden.

- Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren

  Konfigurieren Sie die AWS-Konten so, dass sie für den Zugriff auf das vertrauenswürdige Konto zurückgreifen. Dieses Setup funktioniert für jede Art von Konto: diskrete Konten (unabhängig), Verwaltungskonten oder Mitgliedskonten. Wenn Sie das vertrauenswürdige Konto mit den AWS-Anmeldeinformationen auf der Now Platform konfigurieren, können Sie eine IAM-Rolle konfigurieren, die zu den vertrauenden Konten gehört und die dem Benutzer des vertrauenswürdigen Kontos vertraut. Auf diese Weise können Sie nur einen Satz von AWS-Anmeldeinformationen für den Zugriff auf mehrere AWS-Konten verwenden.

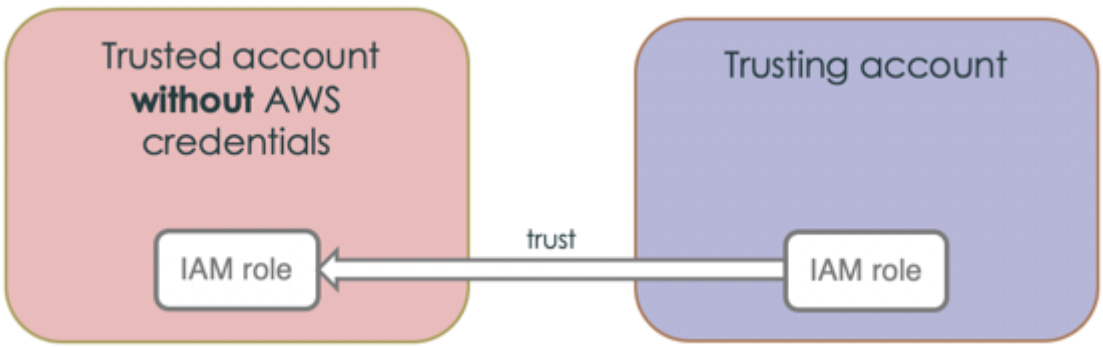
  AWS-Konten so einrichten, dass sie auf ein vertrauenswürdiges Konto mit AWS-Anmeldeinformationen zurückgreifen



- Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten ohne AWS-Anmeldeinformationen konfigurieren

  Um ein Konto ohne AWS-Anmeldeinformationen zu verwenden, müssen Sie dieses Konto zuerst mit einer IAM-Rolle und mit Berechtigungen für den Zugriff auf das vertrauende Servicekonto konfigurieren. Dann richten Sie die IAM-Rolle des vertrauenden Kontos ein, um Zugriff auf die IAM-Rolle des vertrauenswürdigen Kontos zu gewähren.

  AWS-Konten so einrichten, dass sie auf einem vertrauenswürdigen Konto ohne AWS-Anmeldeinformationen beruhen

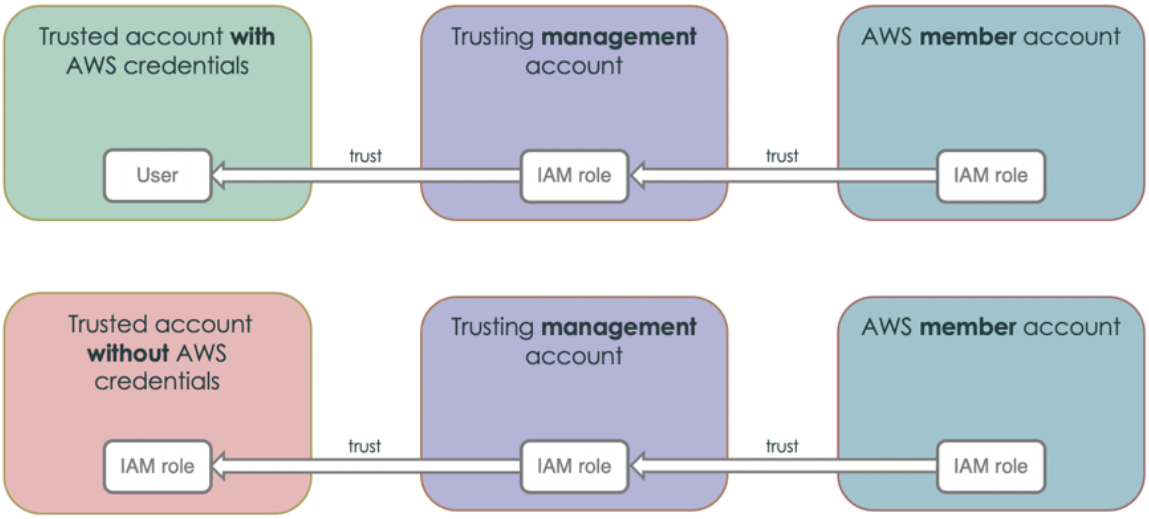


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Zugriff mithilfe temporärer Anmeldeinformationen für vertrauende AWS-Mitgliederkonten konfigurieren

  Wenn AWS-Organisationen vorhanden sind, können Sie AWS-Mitgliedskonten so konfigurieren, dass sie für den Zugriff auf das jeweilige Verwaltungskonto zurückgreifen. In diesem Fall konfigurieren Sie die IAM-Rollen der Mitgliedskonten so, dass sie der IAM-Rolle des jeweiligen Verwaltungskontos vertrauen. Es spielt keine Rolle, ob das Verwaltungskonto auf ein Konto mit oder ohne AWS-Anmeldeinformationen zurückgreift.

Mitgliedskonten so konfigurieren, dass sie für den Zugriff das jeweilige Verwaltungskonto nutzen



Wie Cloud-Discovery die zu verwendenden Anmeldeinformationen bestimmt

Cloud-Discovery verwendet die folgende Logik, um zu bestimmen, welche Anmeldeinformationen zum Erkennen von AWS-Cloud-Ressourcen in Mitgliedskonten verwendet werden:

1. Wenn für das Mitgliedskonto in der Tabelle „Cloud-Servicekonto“ [cmdb_ci_cloud_service_account] dauerhafte Anmeldeinformationen definiert sind, verwendet Discovery diese Anmeldeinformationen. Die Tabelle „Cloud-Servicekonten“ [cmdb_ci_cloud_service_account] enthält die Informationen zu den Servicekontotypen wie Verwaltungskonto oder Mitgliedskonto und deren Anmeldeinformationen.
2. Wenn für den Mitgliedsaccount keine permanenten Anmeldeinformationen definiert sind, überprüft Discovery die Tabelle „Cloud Servicekonto AWS-Org. – Parameter für Rollenübernahme“ [cloud_service_account_aws_org_assume_role_params] auf spezielle Parameter, die dem Mitgliedsaccount zugeordnet sind. Wenn in dieser Tabelle Parameter vorhanden sind, verwendet Discovery die temporären Anmeldeinformationen, die durch Angabe einer Rolle und deren Parameter in der Aktion „AssumeRole“ der AWS-Sicherheits-Token-Service-API abgerufen wurden.
3. Wenn dem Mitgliedskonto in der Tabelle [cloud_service_account_aws_org_assume_role_params] keine speziellen Parameter zugeordnet sind, überprüft Discovery diese Tabelle auf Parameter, die dem Verwaltungskonto zugeordnet sind. Wenn Parameter vorhanden sind, die eine Rolle für das Verwaltungskonto definieren, verwendet Discovery die von dieser Rolle bereitgestellten temporären Anmeldeinformationen.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

4. Wenn in der Tabelle [cloud_service_account_aws_org_assume_role_params] keine speziellen Parameter für Verwaltungs- oder Mitgliedskonten vorhanden sind, verwendet Discovery die Standardeinstellungen, die für die Rolle `OrganizationAccountAccessRole` definiert sind.

Zugriff auf AWS-Konten mit permanenten AWS-Anmeldeinformationen konfigurieren

Für den sicheren Zugriff auf Daten im Provider-Konto müssen mit dem Discovery-Prozess entsprechende Anmeldeinformationen bereitgestellt werden. Damit die Anmeldeinformationen für Discovery und Cloud Provisioning and Governance verfügbar sind, müssen Sie in der AWS-Verwaltungskonsole zunächst einen Benutzer mit programmgesteuertem Zugriff erstellen. Anschließend speichern Sie die Anmeldeinformationen sicher in einem Servicekonto in Now Platform.

Vorbereitungen

Erforderliche Rollen:

- AWS-Verwaltungskonsole Administrator
- Für Cloud-Discovery: admin oder discovery_admin
- Für Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Cloud-Anbieter verwenden oft unterschiedliche Namen für die Einstellungen für Accounts, Regionen und Anmeldeinformationen. Da die ServiceNow-Anwendung Unterstützung für mehrere Cloud Provider bietet, werden in der App allgemeine Namen für die Einstellungen verwendet.

Prozedur

1. Wahlweise: Um einen Benutzer für Cloud Provisioning and Governance zu erstellen (für den Zugriff des Programms auf Ihre AWS-Ressource und Abrechnungsdaten), gehen Sie wie folgt vor:

   a. Navigieren Sie im AWS-Verwaltungskonsolezu **Identity and Access Management (IAM)** > **Zugriffsverwaltung** > **Anwender**.

   b. Klicken Sie im IAM-Ressourcenportal auf **Anwender**.

   c. Wählen Sie **Anwender hinzufügen** aus.

   d. Konfigurieren Sie auf der Seite „Details“ die Benutzereinstellungen, und klicken Sie dann auf **Weiter**.

   Detailseite

Feld	Beschreibung
Benutzername	Name des Benutzers in Form eines Programms. Beispiel: `servicenowcloud`.
Zugriffstyp	Wählen Sie **Programmatic access** (Programmgesteuerter Zugriff) aus.

   e. Auf der Seite für die Berechtigungen fügen Sie den Benutzer einer Richtlinie hinzu. Konfigurieren Sie die folgenden Einstellungen, und wählen Sie dann **Weiter** aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
Berechtigungen für <Benutzername> festlegen	Wählen Sie **Attach existing policies directly** (Vorhandene Richtlinien direkt anhängen) aus.
Attach one or more policies … (Mindestens eine Richtlinie anhängen …)	Wählen Sie die entsprechende Richtlinie aus. **Hinweis:** Die Richtlinie **AdministratorAccess** hat die umfassendste Berechtigungsstufe, einschließlich der Berechtigung zum Bereitstellen von Cloud-Ressourcen. Die Richtlinie ermöglicht den gleichen Zugriff, der der Instanz gewährt würde, wenn Sie nicht IAM, sondern die Zugriffsschlüssel-ID und den geheimen Zugriffsschlüssel Ihres AWS-Kontos verwenden würden. Sie können stattdessen eine Richtlinie erstellen oder mehrere Richtlinien kombinieren, um die entsprechende Berechtigungsstufe zu gewähren. Weitere Detailinformationen finden Sie unter AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern.

f. Überprüfen Sie auf der Seite „Prüfung“ Ihre Auswahl, und wählen Sie dann **Benutzer erstellen** aus.

g. Kopieren Sie auf der Seite „Security Credentials“ (Sicherheitsanmeldeinformationen) den geheimen Zugriffsschlüssel und die Zugriffsschlüssel-ID.

Wichtig: Verlassen Sie die Seite erst, wenn Sie beide Schritte abgeschlossen haben. Der Wert des **geheimen Zugriffsschlüssels** wird nicht erneut angezeigt. Die in diesen Schritten generierten Werte müssen Sie in ein Cloud Provisioning and Governance-Formular einfügen.

i. Klicken Sie auf **Anzeigen**, um den geheimen Zugriffsschlüssel anzuzeigen. Kopieren Sie den Wert.

ii. Wählen Sie **Download .csv** (.csv herunterladen) aus, um die Datei, die den Benutzernamen, die Zugriffsschlüssel-ID und den Wert des geheimen Zugriffsschlüssels enthält, im CSV-Format zu speichern. Erstellen Sie die Datei als Sicherung für den Fall, dass Sie die Werte verlieren. Stellen Sie sicher, dass die Datei erstellt wurde, und speichern Sie sie dann sicher.

2. Navigieren Sie in der Instanz ServiceNow zu **Discovery** > **Anmeldeinformationen**.

3. Wählen Sie **Neu** und dann **AWS-Anmeldeinformationen** aus, geben Sie einen eindeutigen und aussagekräftigen **Namen** ein (z. B. `Cloud-Bereitstellungskonto`), und füllen Sie dann das Formular aus.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Formularfelder mit AWS-Anmeldeinformationen

Feld	Eingabewert
Name	Eindeutiger und beschreibender Name für die AWS-Anmeldeinformationen.
Aktiv	Option zur Verwendung dieser Anmeldeinformationen.
Zugangsschlüssel-ID	Die **Zugriffsschlüssel-ID**, die Sie in der AWS-Verwaltungskonsole generiert haben, z. B: APIAIOSFODNN7BEISPIEL.
Geheimer Zugangsschlüssel	Der **geheime Zugriffsschlüssel**, den Sie in der AWS-Verwaltungskonsole generiert haben, z. B.: wPalrXUtnFEMI/K7MDENG/bPxRfiCYBEISPIELSCHLÜSSEL.

4. Wählen Sie **Aktualisieren** oder **Absenden**.

Nächste Maßnahme

Ordnen Sie diese AWS-Anmeldeinformationen dem entsprechenden AWS-Konto zu, und testen Sie sie dann:

1. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**, und wählen Sie den Account AWS aus, den Sie zuvor wie in AWS-Servicekonten einrichtenbeschrieben erstellt haben.
2. Geben Sie im Formular „Cloud-Servicekonto“ die AWS-Anmeldeinformationen ein, die Sie im Feld **Discovery-Anmeldeinformationen** erstellt haben.
3. Wählen Sie unter **Zugehörige Links** die Option **Rechenzentren erkennen** aus.
4. Navigieren zu **Discovery** > **Dashboard „Cloudressourcen“**, und wählen Sie dann die Registerkarte **AWS** aus. Das Dashboard zeigt erkannte Ressourcen für das Konto, das Sie den neu erstellten AWS-Anmeldeinformationen zugeordnet haben.
5. Stellen Sie sicher, dass Cloud-Discovery den Erkennungsprozess erfolgreich ausgeführt hat.

Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren

Konfigurieren Sie das vertrauende Konto, auf dessen Ressourcen zugegriffen werden muss, so, dass es über die Identity and Access Management (IAM)-Rolle auf das vertrauenswürdige Konto zurückgreift.

Vorbereitungen

- Machen Sie sich mit der Amazon-Dokumentation zum Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer vertraut.
- Entscheiden Sie, welcher Amazon Web Services (AWS)-Account der vertrauenswürdige Account sein soll. Sie verwenden den vertrauenswürdigen Account zur Konfiguration temporärer Anmeldeinformationen für Cloud-Discovery mithilfe von IAM-Rollen. Der vertrauenswürdige Account, den Sie für den Zugriff auf andere Accounts mit IAM-Rollen verwenden, wird als Account eines Zugriffsberechtigten bezeichnet.
- Richten Sie das vertrauenswürdige und das vertrauende Konto wie in AWS-Servicekonten einrichten beschrieben ein.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

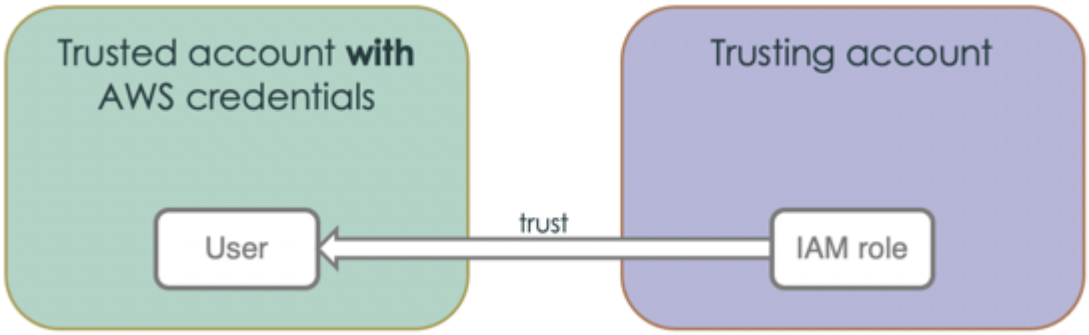
Erforderliche Rolle:

- Für Cloud-Discovery: admin oder discovery_admin
- Für Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Während dieser Konfiguration erstellen Sie eine IAM-Rolle für das vertrauende Konto und konfigurieren dann das vertrauenswürdige Servicekonto für das vertrauende Konto in Now Platform. Schließlich ordnen Sie die IAM-Rolle, die Sie für das vertrauende Konto erstellt haben, dem vertrauenden Konto selbst zu.

AWS-Konten so einrichten, dass sie auf ein vertrauenswürdiges Konto mit AWS-Anmeldeinformationen zurückgreifen



Prozedur

1. Erstellen Sie eine IAM-Rolle für das vertrauende Konto, und konfigurieren Sie die Vertrauensstellung zwischen dem Benutzer, der diese Rolle übernimmt, und dem vertrauenswürdigen Konto (Account des Zugriffsberechtigten).

   a. Melden Sie sich in der AWS-Managementkonsole bei dem vertrauenden Account an.

   b. Erstellen und konfigurieren Sie die IAM-Rolle, indem Sie im Feld **Account ID** die ID des vertrauenswürdigen Kontos (des Accounts des Zugriffsberechtigten) angeben. Informationen zum Erstellen von AWS -Rollen finden Sie unter Amazon Dokumentation .

   c. Wählen Sie auf der Seite „Zusammenfassung“ für die IAM-Rolle die Registerkarte **Trust Relationships** (Vertrauensstellungen).

   d. Klicken Sie auf **Edit trust relationship** (Vertrauensstellung bearbeiten). Die Seite zum Bearbeiten der Vertrauensstellung wird geöffnet und zeigt das Richtliniendokument an.

   e. Legen Sie den Parameter *AWS* auf den vollständigen Benutzer-ARN des vertrauenswürdigen Accounts (des Zugriffsberechtigten) fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Verifizieren Sie, ob der *Action*-Wert auf *sts:AssumeRole* festgelegt ist.

g. Klicken Sie auf **Update Trust Policy** (Vertrauensrichtlinie aktualisieren).

2. Konfigurieren Sie den vertrauenswürdigen Serviceaccount für das vertrauende Konto auf der Now Platform.

a. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**.

b. Öffnen Sie das vertrauende Konto.

c. Geben Sie im Formular „Cloud-Servicekonto“ den Namen des vertrauenswürdigen Kontos im Feld **Account des Zugriffsberechtigten** ein.

d. Wählen Sie **Aktualisieren**.

3. Weisen Sie die für den vertrauenden Account erstellte IAM-Rolle dem vertrauenden Account unter Now Platform zu.

> **Wichtig:** Führen Sie diesen Schritt nur aus, wenn Sie anwenderdefinierte IAM-Rollen erstellt haben. Es ist nicht erforderlich, die Standardrolle OrganizationAccountAccessRole einem Serviceaccount zuzuweisen.

a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Zugriffsparameter der Organisation** > **Cloud-Servicekonto AWS-Parameter für übergreifende Rollenübernahme**.

b. Wählen Sie **Neu**.

c. Konfigurieren Sie im Formular „Cloud-Service-Account: AWS-Parameter für übergreifende Rollenübernahme“ nur die folgenden Felder:

Feld	Definition
Name der Zugriffsrolle	Name der IAM-Rolle, die für den vertrauende Account erstellt wurde.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Definition
Cloud-Servicekonto	Name des vertrauenden Accounts, für den Sie mit der IAM-Rolle Zugriff bereitstellen.

d. Wählen Sie **Absenden**.
Das System fügt diesen Datensatz der Tabelle „Cloud-Serviceaccount AWS – Parameter für übergreifende Rollenübernahme“ [cloud_service_account_aws_cross_assume_role] hinzu.

Hinweis: Standardmäßig wird die Rolle OrganizationAccountAccessRole dem vertrauenswürdigen Verwaltungskonto des Mitglieds zugewiesen und von MID verwendet, wenn sie nicht der Tabelle „Cloud-Serviceaccount AWS-Org. – Parameter für Rollenübernahme“ [cloud_service_account_aws_org_assume_role_params] hinzugefügt wird. Wenn Sie die Standardrolle entfernt oder eine anwenderdefinierte IAM-Rolle erstellt haben, müssen Sie sie für jedes vertrauenswürdige Mitgliedskonto manuell der Tabelle „Cloud-Serviceaccount AWS-Org. – Parameter für Rollenübernahme“ [cloud_service_account_aws_org_assume_role_params] hinzufügen. Navigieren Sie dazu zu **Alle** > **Cloud Provisioning and Governance** > **Zugriffsparameter der Organisation** > **Cloud-Service-Account AWS-Org. – Parameter für Rollenübernahme** und führen Sie die vorherigen Schritte aus.

Nächste Maßnahme
Stellen Sie sicher, dass ServiceNow-Anwendungen mithilfe der IAM-Rolle auf das vertrauende Servicekonto zugreifen können:

1. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**.
2. Wählen Sie das vertrauende Konto aus, das Sie konfiguriert haben.
3. Klicken Sie unter **Zugehörige Links** auf **Rechenzentren erkennen**.
4. Navigieren zu **Discovery** > **Cloud-Discovery-Dashboard**, und klicken Sie dann auf die Registerkarte **AWS**.
5. Prüfen Sie, ob das Dashboard erkannte Ressourcen für das Konto zeigt, das Sie den neu erstellten AWS-Anmeldeinformationen zugeordnet haben.

Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten ohne AWS-Anmeldeinformationen konfigurieren

Richten Sie ein vertrauenswürdiges Konto ohne Anmeldeinformationen ein, auf das andere AWS-Konten für den Zugriff zurückgreifen können.

Vorbereitungen
Erstellen und konfigurieren Sie das vertrauenswürdige AWS-Konto.

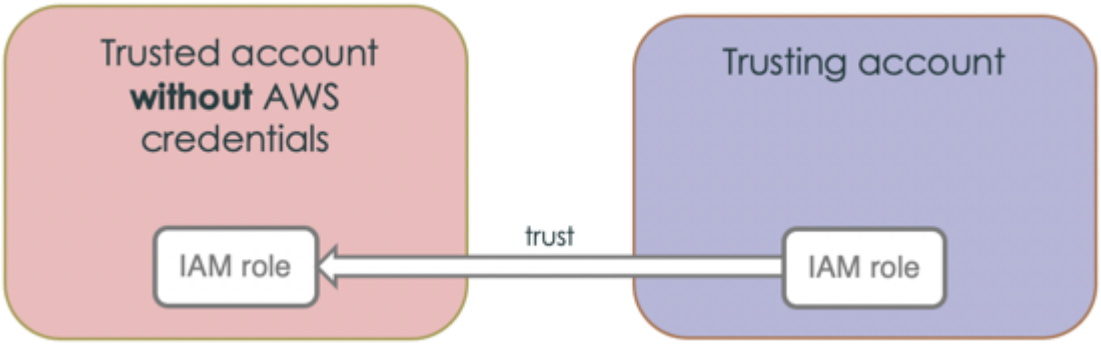
Erforderliche Rolle: admin, discovery_admin oder sn_cmp.cloud_admin (für Cloud Provisioning and Governance)

Erforderliche Rolle: Administrator

Warum und wann dieser Vorgang ausgeführt wird
Um ein Konto ohne AWS-Anmeldeinformationen zu verwenden, müssen Sie dieses Konto zuerst mit einer IAM-Rolle und mit Berechtigungen für den Zugriff auf das vertrauende Servicekonto konfigurieren. Dann richten Sie die IAM-Rolle des vertrauenden Kontos ein, um Zugriff auf die IAM-Rolle des vertrauenswürdigen Kontos zu gewähren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

AWS-Konten so einrichten, dass sie auf einem vertrauenswürdigen Konto ohne AWS-Anmeldeinformationen beruhen



Prozedur

1. Konfigurieren Sie eine IAM-Rolle für das vertrauende Konto.

a. Melden Sie sich in der AWS-Managementkonsole bei dem vertrauenden Konto an.

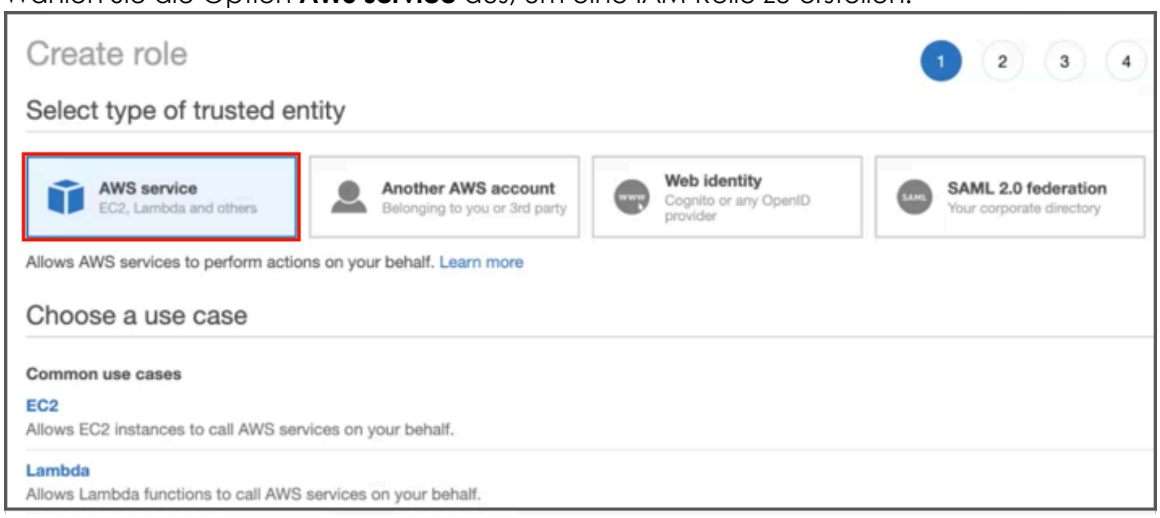
b. Erstellen Sie eine IAM-Rolle für dieses Konto.
Verwenden Sie beim Erstellen dieser IAM-Rolle die Konto-ID des vertrauenswürdigen Kontos. Bedienungsinformationen zum Arbeiten mit AWS-Rollen finden Sie in der Amazon-Dokumentation.

c. Erstellen Sie eine ReadOnlyAccess-Richtlinie, und hängen Sie sie an die neu erstellte IAM-Rolle an.

2. Konfigurieren Sie die IAM-Rolle für das vertrauenswürdige Konto.

a. Melden Sie sich bei der AWS-Managementkonsole mit den Anmeldeinformationen des Kontos an, das Sie als vertrauenswürdiges Konto einrichten möchten.

b. Wählen Sie die Option **AWS service** aus, um eine IAM-Rolle zu erstellen.



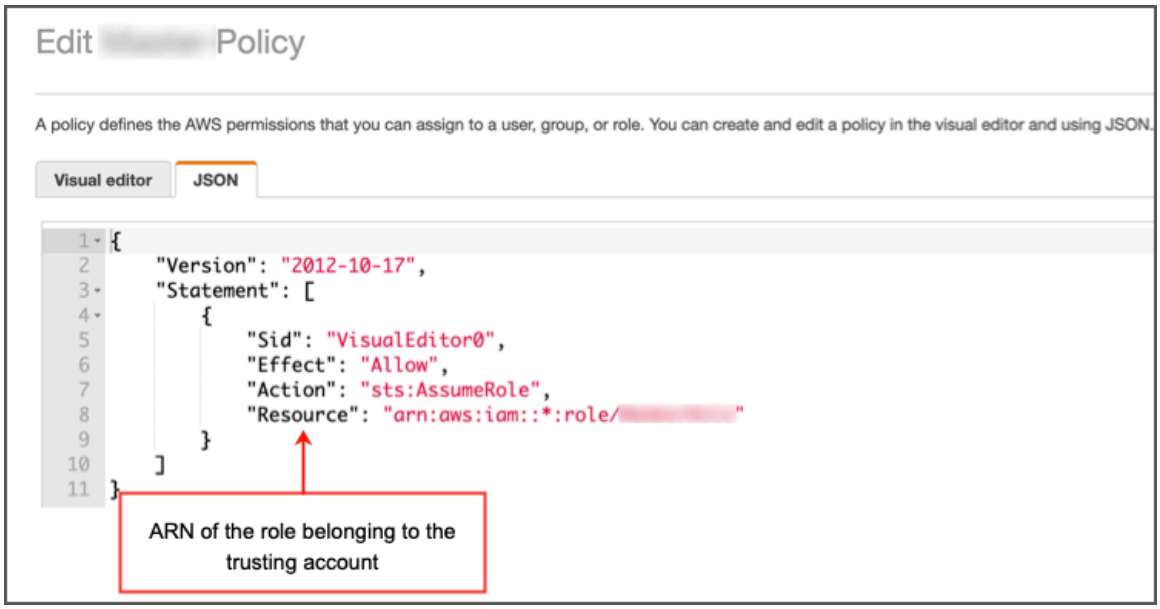
c. Erstellen Sie eine ReadOnlyAccess-Richtlinie für die IAM-Rolle des vertrauenswürdigen Kontos.

d. Erstellen Sie eine zusätzliche Richtlinie, um dieser IAM-Rolle Zugriff auf Ressourcen in vertrauenden Konten zu gewähren:

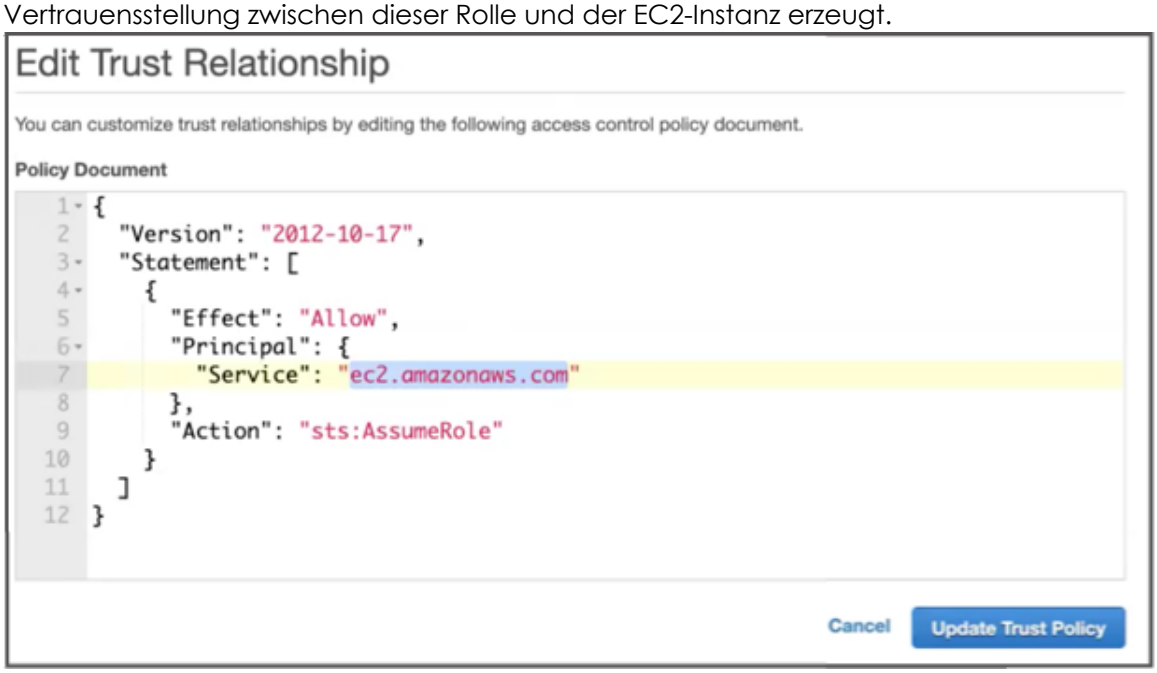
Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie den Parameter *Action* auf `sts:AssumeRole` fest.
- Legen Sie den Parameter *Resource* auf den ARN der Rolle des vertrauenden Kontos fest, die Sie in 1.b erstellt haben.



e. Hängen Sie die neu erstellte Rolle an die relevante Amazon EC2-Instanz an. Wenn Sie eine IAM-Rolle an eine EC2-Instanz anhängen, wird standardmäßig eine Vertrauensstellung zwischen dieser Rolle und der EC2-Instanz erzeugt.



3. Konfigurieren Sie das vertrauende Servicekonto, um Zugriff auf die IAM-Rolle zu gewähren, die zum vertrauenswürdigen Konto gehört.

a. Melden Sie sich in der AWS-Managementkonsole bei dem vertrauenden Konto an.

b. Navigieren Sie zu der IAM-Rolle, die Sie für dieses Konto in 1.b erstellt haben.

c. Bearbeiten Sie die Vertrauensstellung für diese IAM-Rolle wie folgt:

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

- Legen Sie den Parameter *Action* auf `sts:AssumeRole` fest.
- Legen Sie den Parameter *AWS* auf den ARN der Rolle des vertrauenswürdigen Kontos fest, die Sie in 2.b erstellt haben.

4. MID-Server für AWS-IAM-Rollen konfigurieren.
5. Konfigurieren Sie das vertrauenswürdige Servicekonto ohne Anmeldeinformationen für das vertrauende Konto in Now Platform.
   a. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**.
   b. Öffnen Sie das vertrauende Konto.
   c. Geben Sie im Formular „Cloud-Servicekonto“ den Namen des vertrauenswürdigen Kontos im Feld **Account des Zugriffsberechtigten** ein.
   d. Klicken Sie auf **Aktualisieren**.
6. Weisen Sie die für den vertrauenden Account erstellte IAM-Rolle dem vertrauenden Account unter Now Platform zu.

> **Wichtig:** Führen Sie diesen Schritt nur aus, wenn Sie anwenderdefinierte IAM-Rollen erstellt haben. Es ist nicht erforderlich, die Standardrolle OrganizationAccountAccessRole einem Serviceaccount zuzuweisen.

   a. Navigieren zu **Alle** > **Cloud Provisioning and Governance** > **Zugriffsparameter der Organisation** > **Cloud-Servicekonto AWS-Parameter für übergreifende Rollenübernahme**.
   b. Wählen Sie **Neu**.
   c. Konfigurieren Sie im Formular „Cloud-Service-Account: AWS-Parameter für übergreifende Rollenübernahme“ nur die folgenden Felder:

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Definition
Name der Zugriffsrolle	Name der IAM-Rolle, die für den vertrauende Account erstellt wurde.
Cloud-Servicekonto	Name des vertrauenden Accounts, für den Sie mit der IAM-Rolle Zugriff bereitstellen.

d. Wählen Sie **Absenden**.
Das System fügt diesen Datensatz der Tabelle „Cloud-Serviceaccount AWS – Parameter für übergreifende Rollenübernahme“ [cloud_service_account_aws_cross_assume_role] hinzu.

Hinweis: Standardmäßig wird die Rolle OrganizationAccountAccessRole dem vertrauenswürdigen Verwaltungskonto des Mitglieds zugewiesen und von MID verwendet, wenn sie nicht der Tabelle „Cloud-Serviceaccount AWS-Org. – Parameter für Rollenübernahme“ [cloud_service_account_aws_org_assume_role_params] hinzugefügt wird. Wenn Sie die Standardrolle entfernt oder eine anwenderdefinierte IAM-Rolle erstellt haben, müssen Sie sie für jedes vertrauenswürdige Mitgliedskonto manuell der Tabelle „Cloud-Serviceaccount AWS-Org. – Parameter für Rollenübernahme“ [cloud_service_account_aws_org_assume_role_params] hinzufügen. Navigieren Sie dazu zu **Alle** > **Cloud Provisioning and Governance** > **Zugriffsparameter der Organisation** > **Cloud-Service-Account AWS-Org. – Parameter für Rollenübernahme** und führen Sie die vorherigen Schritte aus.

Nächste Maßnahme
Stellen Sie sicher, dass ServiceNow-Anwendungen mithilfe der IAM-Rolle auf das vertrauende Servicekonto zugreifen können:

1. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**.
2. Wählen Sie das vertrauende Konto aus, das Sie konfiguriert haben.
3. Klicken Sie unter **Zugehörige Links** auf **Rechenzentren erkennen**.
4. Navigieren zu **Discovery** > **Cloud-Discovery-Dashboard**, und klicken Sie dann auf die Registerkarte **AWS**.
5. Prüfen Sie, ob das Dashboard erkannte Ressourcen für das Konto zeigt, das Sie den neu erstellten AWS-Anmeldeinformationen zugeordnet haben.

Zugriff mithilfe temporärer Anmeldeinformationen für vertrauende AWS-Mitgliederkonten konfigurieren

Konfigurieren Sie den Zugriff auf AWS-Mitgliedskonten mit dem Verwaltungskonto als vertrauenswürdigem Konto mithilfe der IAM-Rolle.

Vorbereitungen
Erforderliche Rolle: Administrator

- Machen Sie sich mit der Amazon-Dokumentation zum Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer vertraut.
- Vergewissern Sie sich, dass Sie wissen, welche AWS-Mitgliedskonten demselben Verwaltungskonto zugewiesen sind. Sie verwenden das Verwaltungskonto zur Konfiguration temporärer Anmeldeinformationen für die Cloud-Erkennung mithilfe von IAM-Rollen.
- Richten Sie die AWS-Verwaltungskonten und Mitgliedskonten wie in AWS-Servicekonten einrichten beschrieben ein.

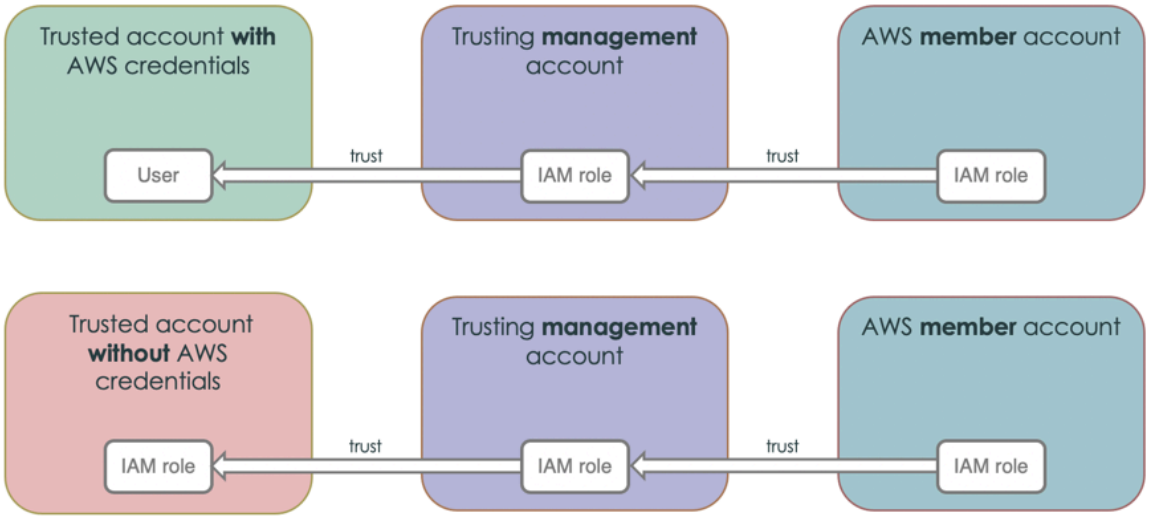
© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Erforderliche Rolle: admin, discovery_admin oder sn_cmp.cloud_admin (für Cloud Provisioning and Governance)

Warum und wann dieser Vorgang ausgeführt wird

Sie können den Zugriff auf Mitgliedskonten so konfigurieren, dass die Mitglieder auf das jeweilige Verwaltungskonto zurückgreifen. Es spielt keine Rolle, ob das Verwaltungskonto selbst permanente oder temporäre Anmeldeinformationen verwendet.

Mitgliedskonten so konfigurieren, dass sie für den Zugriff das jeweilige Verwaltungskonto nutzen



Prozedur

1. Erstellen Sie eine IAM-Rolle für das Mitgliedskonto, und konfigurieren Sie die Vertrauensstellung zwischen dem Benutzer, der diese Rolle übernimmt, und dem vertrauenswürdigen Konto (Account des Zugriffsberechtigten).

   a. Melden Sie sich bei der AWS-Managementkonsole mit den Anmeldeinformationen des Mitgliedskontos an, für das Sie den Zugriff konfigurieren.

   b. Erstellen und konfigurieren Sie die IAM-Rolle, indem Sie im Feld **Account ID** die ID des Verwaltungskontos angeben.
   Bedienungsinformationen zum Erstellen von AWS-Rollen finden Sie in der Amazon-Dokumentation.

   c. Klicken Sie auf der Seite **Summary** (Zusammenfassung) für die IAM-Rolle auf die Registerkarte **Trust Relationships** (Vertrauensstellungen).

   d. Klicken Sie auf **Edit trust relationship** (Vertrauensstellung bearbeiten).
   Die Seite zum Bearbeiten der Vertrauensstellung wird geöffnet und zeigt das Richtliniendokument an.

   e. Bearbeiten Sie die Vertrauensstellung wie folgt:

      - Legen Sie den Parameter *`Action`* auf `sts:AssumeRole` fest.
      - Legen Sie den Parameter `AWS` auf den vollständigen ARN der Rolle des Verwaltungskontos fest.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

f. Klicken Sie auf **Update Trust Policy** (Vertrauensrichtlinie aktualisieren).

2. Konfigurieren Sie das vertrauenswürdige Servicekonto für das vertrauende Konto in Now Platform.

a. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**.

b. Öffnen Sie das Mitgliedskonto.

c. Geben Sie im Formular „Cloud-Servicekonto“ im Feld **Übergeordneter Account** den Namen des Verwaltungskontos ein.

d. Klicken Sie auf **Aktualisieren**.

3. Weisen Sie dem Mitgliedskonto in Now Platform die für das Mitgliedskonto erstellte IAM-Rolle zu.

> **Wichtig:** Führen Sie diesen Schritt nur aus, wenn Sie benutzerdefinierte IAM-Rollen erstellt haben. Es ist nicht erforderlich, die Standardrolle OrganizationAccountAccessRole einem Serviceaccount zuzuweisen.

a. Navigieren zu **Cloud Provisioning and Governance** > **Zugriffsparameter der Organisation** > **AWS – Parameter für übergreifende Rollenübernahme**.

b. Klicken Sie auf **Neu**.

c. Konfigurieren Sie im Formular „Cloud-Service-Account: Parameter für Annahme der AWS-übergreifenden Rolle“ nur die folgenden Felder:

Feld	Definition
Name der Zugriffsrolle	Name der IAM-Rolle, die für den vertrauende Account erstellt wurde.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Definition
Cloud-Servicekonto	Name des vertrauenden Accounts, für den Sie mit der IAM-Rolle Zugriff bereitstellen.

d. Klicken Sie auf **Absenden**.

Nächste Maßnahme

Stellen Sie sicher, dass ServiceNow-Anwendungen mithilfe der IAM-Rolle auf das vertrauende Servicekonto zugreifen können:

1. Navigieren zu **Cloud Provisioning and Governance** > **Service-Accounts**, und wählen Sie den Account AWS aus, den Sie zuvor wie in AWS-Servicekonten einrichtenbeschrieben erstellt haben.
2. Wählen Sie das vertrauende Konto aus, das Sie mit der IAM-Rolle konfiguriert haben.
3. Klicken Sie unter **Zugehörige Links** auf **Rechenzentren erkennen**.
4. Navigieren zu **Discovery** > **Cloud-Discovery-Dashboard**, und klicken Sie dann auf die Registerkarte **AWS**.
5. Prüfen Sie, ob das Dashboard erkannte Ressourcen für das Konto zeigt, das Sie den neu erstellten AWS-Anmeldeinformationen zugeordnet haben.

MID-Server für AWS-IAM-Rollen konfigurieren

Konfigurieren Sie den MID-Server, um die temporären Sicherheitsanmeldeinformationen abzurufen, die einer IAM-Rolle zugeordnet sind.

Vorbereitungen

Erforderliche Rolle: admin, discovery_admin oder sn_cmp.cloud_admin (für Cloud Provisioning and Governance)

Erforderliche Rolle: Administrator

Prozedur

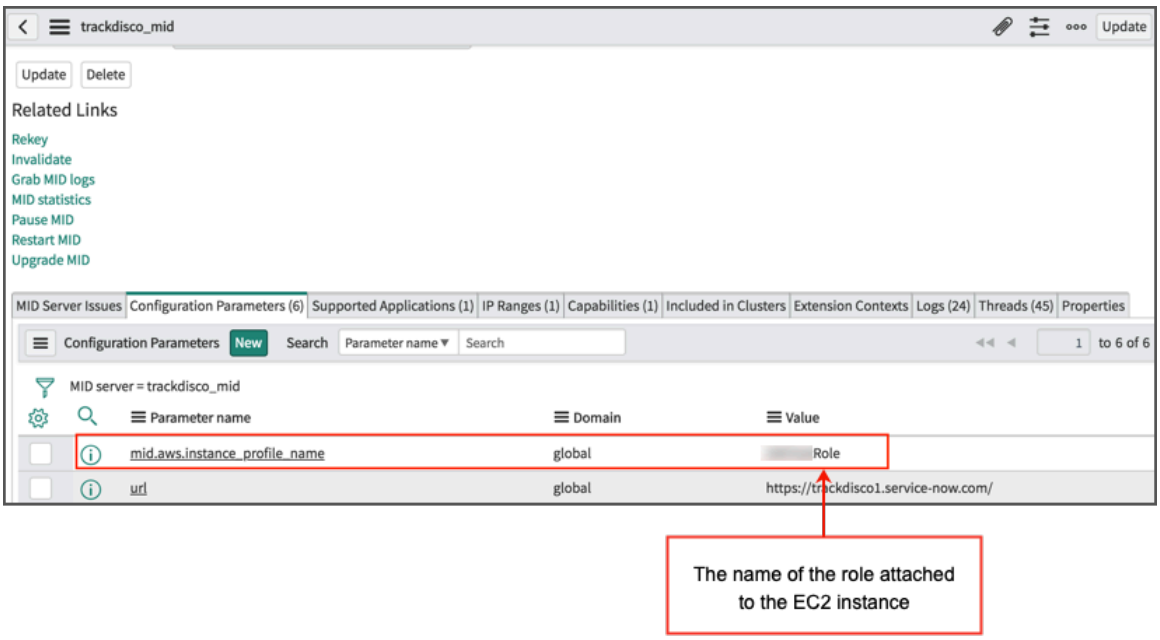
1. Navigieren zu **Alle** > **Discovery** > **MID-Server**.
2. Wählen Sie einen MID-Server aus, der auf einer Amazon EC2-Instanz innerhalb des betreffenden AWS-Servicekontos installiert ist.
3. Wählen Sie die zugehörige Liste **Konfigurationsparameter** aus.
4. Klicken Sie auf **Neu**.
5. Wählen Sie im Konfigurationsparameterformular *mid.aws.instance_profile_name* im Feld **Parametername** aus.
6. Geben Sie in das Feld **Wert** den Namen der IAM-Rolle ein, die mit der EC2-Instanz verbunden ist.

Hinweis: Der MID-Server verwendet dieselbe IAM-Rolle, die für den entsprechenden Service-Account AWS von eingerichtet ist. Weitere Informationen finden Sie unter Zugriff mit temporären Anmeldeinformationen basierend auf vertrauenswürdigen AWS-Konten mit AWS-Anmeldeinformationen konfigurieren.

Betriebsinformationen zum Erstellen von AWS -Rollen finden Sie in der Amazon-Dokumentation unter Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer .

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

7. Klicken Sie auf **Absenden**.
   Der neue Parameter wird im MID-Server-Datensatz aufgelistet.



AWS-Zugriff und -Berechtigungen mithilfe von Richtlinien steuern

Konfigurieren Sie Richtlinien mit der erforderlichen Berechtigungsstufe, um Zugriff auf die AWS-Ressourcen für Cloud-Discovery und Cloud Provisioning and Governance bereitzustellen.

Vorbereitungen

Machen Sie sich mit dem Erstellen von IAM-Benutzern und Benutzerrichtlinien vertraut. Konsultieren Sie dazu die AWS-Dokumentation .

Identifizieren Sie die Berechtigungsstufe, die zum Erkennen der Ressourcen mit Cloud-Discovery und zum Verwalten der Ressourcen mit Cloud Provisioning and Governance erforderlich ist. Zum Beispiel:

- Zusätzliche S3-Berechtigungen sind erforderlich, da AWS einen S3-Bucket zum Speichern und Ausführen der CloudFormation-Vorlagen verwendet, um Stapel mit CloudFormation bereitzustellen. Diese Berechtigungen sind auch dann erforderlich, wenn Sie dieselbe CloudFormation-Vorlage über die AWS-Konsole ausführen.
- Für die Muster-Discovery über mit der anwenderdefinierten Richtlinie ist schreibgeschützter Zugriff erforderlich.

Mit AWS CloudFormation werden Ressourcen bereitgestellt und konfiguriert, indem die in der Vorlage beschriebenen AWS-Services aufgerufen werden. Weitere Informationen hierzu finden Sie unter Funktionsweise von AWS CloudFormation .

Erforderliche Rollen:

- AWS-Verwaltungskonsole Administrator
- Für Cloud-Discovery: admin oder discovery_admin
- Für Cloud Provisioning and Governance: admin oder sn_cmp.cloud_admin

Warum und wann dieser Vorgang ausgeführt wird

Mit der von Ihnen konfigurierten Richtlinie werden die AWS-Berechtigungen definiert, die Sie einem Benutzer, einer Gruppe oder einer Rolle zuweisen können. Geben Sie abhängig von

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

den AWS-Services, die Sie verwenden, Aktionen für den Service an, um mit Cloud Provisioning and Governance Erkennungs-, Bereitstellungs- und Lebenszyklusaktionen auszuführen.

Prozedur

1. Melden Sie sich bei der AWS -Verwaltungskonsole mit den Anmeldeinformationen des entsprechenden Servicekontos an.
   Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwendet haben, um Zugriff mit temporären Anmeldeinformationen bereitzustellen, melden Sie sich mit demselben IAM-Benutzer oder derselben IAM-Rolle an.
2. Öffnen Sie den Benutzerdatensatz in der Instanz für den entsprechenden Benutzer.
3. Definieren Sie eine Benutzerrichtlinie in der AWS-Managementkonsole mit einer der folgenden Methoden:
   - Gewähren Sie dem Administrator Zugriff auf die Instanz. Diese Methode bietet die gleiche Zugriffsebene wie die Verwendung der Zugriffsschlüssel-ID und des geheimen Zugriffsschlüssels. Hängen Sie die Richtlinie `AdministratorAccess` an das Benutzerprofil an.

     Hinweis: Zum Erstellen einer Benutzerrichtlinie, die nur Cloud-Discovery und nicht die Bereitstellung von Cloud-Ressourcen unterstützt, hängen Sie stattdessen die Richtlinie `ReadOnlyAccess` an.

   - Erstellen Sie eine benutzerdefinierte Richtlinie mit einem beschreibenden Namen. Geben Sie im Feld für das Richtliniendokument den Code ein, der die APIs enthält, deren Ausführung durch diese Richtlinie erlaubt wird.

     Hinweis: Das folgende JSON-Beispiel enthält Berechtigungen für Cloud-Discovery.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"PermissionsNeededForDiscovery",
         "Effect":"Allow",
         "Action":[
            "account:ListRegions",
            "apigateway:GET",
            "application-autoscaling:Describe*",
            "autoscaling-plans:Describe*",
            "autoscaling:Describe*",
            "autoscaling:DescribeAutoScalingGroups",
            "autoscaling:DescribeLaunchConfigurations",
            "cloudformation:Describe*",
            "cloudformation:DescribeStack*",
            "cloudformation:List*
            "cloudwatch:Get*",
            "cloudwatch:List*",
            "config:ListDiscoveredResources",
            "dynamodb:Describe*",
            "dynamodb:DescribeTable",
            "dynamodb:ListGlobalTables",
            "dynamodb:ListTables",
            "ec2:Describe*",
            "ec2:ReportInstanceStatus",
            "ecs:Describe*",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
            "ecs:List*",
            "eks:Describe*",
            "eks:List*",
            "elasticache:Describe*",
            "elasticache:List*",
            "elasticfilesystem:Describe*",
            "elasticloadbalancing:Describe*",
            "lambda:Get*",
            "lambda:List*",
            "organizations:Describe*",
            "organizations:DescribeOrganization",
            "organizations:List*",
            "rds:Describe*",
            "redshift:Describe*",
            "route53:GetHostedZone",
            "route53:List*",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucket*",
            "s3:GetBucketLocation",
            "s3:List*",
            "sdb:GetAttributes",
            "sns:GetEndpointAttributes",
            "sns:GetSubscriptionAttributes",
            "sns:List*",
            "sns:ListPlatformApplications",
            "sns:ListSubscriptions",
            "sns:ListSubscriptionsByTopic",
            "sns:ListTopics",
         ],
         "Resource":"*"
      }
   ]
}
```

- Das folgende JSON-Beispiel enthält Berechtigungen für Cloud-Discovery und Cloud Provisioning and Governance.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PermissionsNeededForCPG",
            "Effect": "Allow",
            "Action": [
                "account:ListRegions",
                "apigateway:GET",
                "application-autoscaling:Describe*",
                "autoscaling-plans:Describe*",
                "autoscaling:Describe*",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeLaunchConfigurations",
                "cloudformation:Describe*",
                "cloudformation:DescribeStack*",
                "cloudwatch:Get*",
                "cloudwatch:List*",
                "config:ListDiscoveredResources"
                "dynamodb:Describe*",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                "dynamodb:DescribeTable",
                "dynamodb:ListGlobalTables",
                "dynamodb:ListTables",
                "ec2:Describe*",
                "ec2:ReportInstanceStatus",
                "ecs:Describe*",
                "ecs:List*",
                "eks:Describe*",
                "eks:List*",
                "elasticache:Describe*",
                "elasticache:List*",
                "elasticfilesystem:Describe*",
                "elasticloadbalancing:Describe*",
                "lambda:Get*",
                "lambda:List*",
                "organizations:Describe*",
                "organizations:DescribeOrganization",
                "organizations:List*",
                "rds:Describe*",
                "redshift:Describe*",
                "route53:GetHostedZone",
                "route53:List*",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucket*",
                "s3:GetBucketLocation",
                "s3:List*",
                "sdb:GetAttributes",
                "sns:GetEndpointAttributes",
                "sns:GetSubscriptionAttributes",
                "sns:List*",
                "sns:ListPlatformApplications",
                "sns:ListSubscriptions",
                "sns:ListSubscriptionsByTopic",
                "sns:ListTopics",
            ],
            "Resource": "*"
        },
        {
            "Sid":
"MinimalPermissionsNeededForEc2ProvisioningThroughCloudFormation",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:CreateUploadBucket",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStackResources",
                "cloudformation:DescribeStacks",
                "cloudformation:GetTemplate",
                "cloudformation:GetTemplateSummary",
                "cloudformation:List*",
                "cloudformation:UpdateStack",
                "cloudformation:ValidateTemplate"
                "ec2:*",
                "s3:CreateBucket",
                "s3:DeleteBucket",
                "s3:DeleteObject",
```


© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

```
                "s3:GetObject",
                "s3:ListBucket",
                "s3:PutObject",
            ],
            "Resource": "*"
        }
    ]
}
```

Zugehörige Informationen

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_create-console.html#access_policies_create-start

https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_understand-service-summary.html

Richten Sie Servicekonten für die Google Cloud Platform ein

Erstellen und konfigurieren Sie Cloud-Service-Accounts unter Now Platform für die entsprechenden Service-Accounts von Google Cloud Platform (GCP).

GCP Der Serviceaccount ist ein eindeutiger Account, der normalerweise von einer Anwendungs- oder Computing-Arbeitsauslastung, z. B. einer Compute Engine-Instanz, und nicht von einem Benutzer verwendet wird. Ein Serviceaccount wird durch seine E-Mail-Adresse identifiziert, die für den Account eindeutig ist. Es wird verwendet, um Interaktionen zwischen Ihrer Anwendung und verschiedenen GCP-Services zu authentifizieren und zu autorisieren.

Konfigurieren Sie die Google API-Anmeldeinformationen für Cloud-Discovery

Erstellen Sie API-Anmeldeinformationen für Google, damit Cloud-Discovery sicher auf die Daten in Ihrem Konto Google zugreifen kann.

Vorbereitungen

Vergewissern Sie sich, dass die Anwendungen aktuell sind

- Muster für Discovery und Service-Mapping
- Visibility Content
- CMDB CI-Klassenmodelle

Erforderliche Rolle: Administrator

Prozedur

Konfigurieren Sie die GCP -Anmeldeinformationen entweder durch Importieren einer JSON-Datei oder durch manuelles Eintragen in den -Datensatz.

Option	Aktionen
Importieren Sie die JSON-Datei	**a.** Wenn Sie die E-Mail von GCPerhalten, laden Sie die JSON-Datei herunter. **b.** Navigieren zu **Discovery** > **Anmeldeinformationen**. **c.** Wählen Sie **Neu** und dann **Google API-Anmeldeinformationen**aus.

Automatische Übersetzung

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Option	Aktionen
	d. Wählen Sie **JSON-Datei importieren aus** **e.** Wählen Sie **Datei wählen aus**, und wählen Sie die heruntergeladene JSON-Datei aus. **f.** Wählen Sie **Anmeldeinformationsdaten hochladen aus**.
Konfigurieren Sie die Anmeldeinformationen manuell	**a.** Navigieren zu **Discovery** > **Anmeldeinformationen**. **b.** Wählen Sie **Neu** und dann **Google API-Anmeldeinformationen**aus. **c.** Wählen Sie **Neu**. **d.** Füllen Sie im Formular die Felder gemäß der Formularbeschreibung aus. Eine Beschreibung der Formularfelder finden Sie unter Formular für Anmeldeinformationen für Google API. **e.** Wählen Sie **Absenden**.

Formular für Anmeldeinformationen für Google API

Füllen Sie das Formular „Anmeldeinformationen für Google-API-Anmeldeinformationen“ aus, um die Anmeldeinformationen zu konfigurieren.

Feld	Beschreibung
Name	Legen Sie einen eindeutigen Namen für die Google Cloud API-Anmeldeinformationen fest.
Aktiv	Option zum Aktivieren dieser Anmeldeinformationen für die Erkennung. Aktivieren Sie dieses Kontrollkästchen, um die Erkennung zu aktivieren.
Betrifft	MID-Server, auf den Sie die Anmeldeinformationen anwenden. Wählen Sie **Alle MID Server**.
Auftrag	Reihenfolge, in der die Plattform diese Anmeldeinformationen ausführt, wenn versucht wird, sich bei Geräten anzumelden. Eine kleinere Zahl gibt an, dass die Anmeldeinformationen in der Liste weiter oben angezeigt werden. Richten Sie die Reihenfolge der Anmeldeinformationen ein, wenn Sie eine große Anzahl von Anmeldeinformationen verwenden oder wenn die Sicherheitsvorkehrung Benutzer nach drei fehlgeschlagenen Anmeldeversuchen sperrt. Wenn alle

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.

Feld	Beschreibung
	Anmeldeinformationen dieselbe oder keine Nummer für die Reihenfolge haben, geht die Instanz die Anmeldeinformationen in zufälliger Reihenfolge durch. Der Standardwert ist 100.
E-Mail	Ihre E-Mail-Adresse GCP.
Geheimer Schlüssel	Geheimer Schlüssel, den Sie in der Konsole Google Cloud generiert haben.
Anmeldeinformationsalias	Ein Anmeldeinformationsalias, der von den Anmeldeinformationen zum Autorisieren von Aktionen verwendet wird.

GCP-Zugriff und -Berechtigung mithilfe von Richtlinien

Der Zugriff auf und die BerechtigungGoogle Cloud Platform (GCP) mithilfe von Richtlinien bieten Berechtigungen für die sichere Nutzung und Verwaltung von Cloud-Ressourcen in GCP.

Laden Sie die Tabelle „GCP-Zugriff und -Berechtigung mithilfe von Richtlinien“ herunter, und verwenden Sie sie, um den erforderlichen Anwenderzugriff und die erforderliche Berechtigung zu gewähren.

© 2025 ServiceNow. Alle Rechte vorbehalten.
ServiceNow, das ServiceNow-Logo, Now und andere ServiceNow-Marken sind Marken und/oder eingetragene Marken von ServiceNow, Inc.,in den USA und/oder anderen Ländern.
Andere Firmen- und Produktnamen können Marken der jeweiligen Unternehmen sein, mit denen sie verbunden sind.